1
2

3

CMVP Security Policy Requirements:

4

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

5
6

7

David Hawes
Alexander Calis
Roy Crombie

8
9
10
11

12

13

14
15
16

17

18

19

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
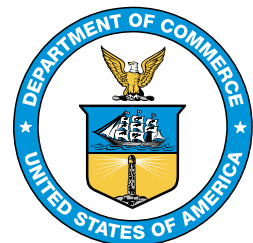*ISO/IEC 24759 and ISO/IEC 19790 Annex B*

Initial Public Draft

David Hawes
Alexander Calis
Computer Security Division
Information Technology Laboratory

Roy Crombie
Canadian Centre for Cyber Security

May 2022

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.

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.

90 **Reports on Computer Systems Technology**

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

101 **Abstract**

102 NIST Special Publication (SP) 800-140Br1 is to be used in conjunction with ISO/IEC 19790
103 Annex B and ISO/IEC 24759 section 6.14. The special publication modifies only those
104 requirements identified in this document. SP 800-140Br1 also specifies the content of the
105 information required in ISO/IEC 19790 Annex B. As a validation authority, the Cryptographic
106 Module Validation Program (CMVP) may modify, add, or delete Vendor Evidence (VE) and/or
107 Test Evidence (TE) specified under paragraph 6.14 of the ISO/IEC 24759 and specify the order
108 of the security policy as specified in ISO/IEC 19790:2012 B.1.

113 **Audience**

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

118

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

165	FISMA	Federal Information Security Management/Modernization Act
166	NIST	National Institute of Standards and Technology
167	SP 800-XXX	NIST Special Publication 800 series document
168	TE	Test Evidence
169	VE	Vendor Evidence

170 **5 Document organization**

171 **5.1 General**

172 Section 6.1 of this document specifies any modifications to ISO/IEC 19790 Annex B and
173 ISO/IEC 24759 section 6.14.

174 **5.2 Modifications**

175 Modifications to ISO/IEC 24759 section 6.14 - Cryptographic module security policy - will
176 follow a similar format as in ISO/IEC 24759. For additions to test requirements, new Test
177 Evidence (TEs) or Vendor Evidence (VEs) will be listed by increasing the "sequence_number."
178 Modifications can include a combination of additions using underline and deletions using
179 ~~strikethrough~~. If no changes are required, the paragraph will indicate "No change."

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

186 **6   Security requirements**

187 **6.1   Changes to ISO/IEC 24759 section 6.14 and ISO/IEC 19790 Annex B Requirements**

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

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

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

198 No Change.

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

200 **B.2.1 General**
201
202 No Change.
203
204 **B.2.2 Cryptographic module specification**
205
206 No Change.
207
208 **B.2.3 Cryptographic module interfaces**
209
210 No Change.
211
212 **B.2.4 Roles, services, and authentication**
213
214 No Change.
215
216 **B.2.5 Software/Firmware security**
217
218 No Change.
219
220 **B.2.6 Operational environment**
221
222 No Change.
223
224 **B.2.7 Physical security**

225
226   No Change.
227
228   **B.2.8 Non-invasive security**
229
230   No Change.
231
232   **B.2.9 Sensitive security parameters management**
233
234   • Provide a ~~key~~ <u>SSP</u> table specifying the ~~key~~ SSP type(s), strength(s) in bits, security
235   function(s), security function certification number(s), where and how the ~~key(s)~~ <u>SSP(s)</u> is
236   generated, whether the ~~key(s)~~ <u>SSP(s)</u> is imported or exported, any SSP generation and
237   establishment method used and indicate any related ~~keys~~ <u>SSPs</u>.
238   • Specify the electronic and manual ~~key~~ <u>SSP</u> I/O method(s).
239
240   **B.2.10 Self-tests**
241
242   No Change.
243
244   **B.2.11 Life-cycle assurance**
245
246   No Change.
247
248   **B.2.12 Mitigation of other attacks**
249
250   No Change.
251
252   **6.2   Documentation requirement additions**

253   In addition to ISO/IEC 24759 section 6.14 and ISO/IEC 19790 Annex B, other publications and
254   documents specify documentation requirements for the Security Policy. Many of these
255   requirements relate to specific conditions and configurations of modules and would not be
256   applicable in many cases.

257   These additional requirements are listed for each section of the Security Policy, grouped by the
258   source publication or document and reference the specific section from the document where the
259   requirement is stated. Where possible, they are direct statements from the source documents and
260   would often require the original context to best understand the requirement.

261   # B.2.1 General
262
263   No Additions.
264
265   # B.2.2 Cryptographic module specification
266
267   **SP800-140:VE02.20.04**

268   1. Vendor Affirmed Security Methods - The vendor provided non-proprietary security
269   policy shall include a list of all vendor affirmed security methods.
270

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

271
272   1. Non-Approved No Security Claimed - If a non-approved cryptographic algorithm is used
273   by the module in the approved mode but is not a security function, the algorithm shall be
274   included in the list of non-approved but allowed algorithms in the Security Policy with
275   the caveat "(no security claimed)"
276   2. Tested Components (CVL) - The Security Policy shall individually list the tested
277   components shown in the module's CVL certificates that may be called during the
278   operation of the module.
279

IG:2.4.C - Approved Security Service Indicator

280
281   1. List of Services and Indicators - The Security Policy shall provide a complete list of all
282   approved and non-approved services along with details on each service and their
283   respective indicators (if applicable).
284

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

285
286   1. List of Curves - The Security Policy shall list all approved and non-approved curves that
287   are implemented.
288   2. Security Strength of Curves - The Security Policy shall indicate the associated security
289   strength for all non-approved curves that are implemented.
290

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

291
292
293   1. Vendor Affirmation of SHA-3 - If the module implemented the same higher-level
294   algorithm with a FIPS 180-4 hash function and there is a corresponding entry on the
295   approved line of the module's validation certificate, then the vendor affirmation of the
296   same algorithm using SHA-3 does not need to be shown separately on the certificate's
297   approved line but shall be documented in the module's Security Policy.
298

IG:C.D - Use of a Truncated HMAC

299
300   1. Use of a Truncated HMAC - The use of the truncated HMAC shall be shown in the
301   module's Security Policy.
302

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

303
304   1. KAS-RSA Scheme Listing - When implementing a key agreement scheme (or a shared
305   secret computation as part of a key agreement scheme), the vendor shall indicate in the
306   module's Security Policy whether the scheme is of the Diffie-Hellman or the MQV
307   variety. If a key agreement scheme (FFC or ECC-based) is documented on the module's
308   certificate's non-approved line, the vendor is encouraged to state there if this is a Diffie-
309   Hellman or an MQV scheme.
310

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

311
312

313   1. Triple-DES within IETF Protocol - The limit of 2^20 encryptions with the same Triple-
314   DES key applies when keys are generated as part of one of the recognized IETF
315   protocols. To use this provision, the Security Policy shall say which of the IETF
316   protocols governs the generation of the Triple-DES keys and list the IETF RFC(s) where
317   the details of this protocol, relevant to the generation of the Triple-DES encryption keys,
318   are documented.
319   2. Triple-DES Limit Enforcement - The Security Policy shall explain how the module
320   performs the enforcement.
321
322   **IG:C.H - Key/IV Pair Uniqueness Requirements from SP 800-38D**
323   1. Compatibility with TLS 1.2 - If the vendor claims that the IV generation is in compliance
324   with the TLS 1.2 specification and only for use within the TLS 1.2 protocol, then the
325   module's Security Policy shall explicitly state the module's compatibility with TLS 1.2
326   and the module's support for acceptable AES-GCM ciphersuites from Section 3.3.1 of SP
327   800-52 rev1 or SP 800-2rev2.
328   2. TLS 1.2 - Trigger Statement - A statement concerning the triggering or a handshake to
329   establish a new encryption key shall be included in the Security Policy and Validation
330   Test Report.
331   3. IPsec-v3 Compatibility Statement - The Security Policy shall explicitly state the
332   module's compliance with RFC 4106 and/or RFC 5282 (depending on the protocols
333   supporting GCM).
334   4. IPsec-v3 Compliant IKEv2 Statement - The Security Policy shall state that the module
335   uses RFC 7296 compliant IKEv2 to establish the shared secret SKEYSEED from which
336   the AES-GCM encryption keys are derived.
337   5. IPsec-v3 Rekey Trigger Statement - A statement indicating a rekeying trigger shall be
338   included in the Security Policy.
339   6. MACsec Statements - The Security Policy shall tell what this module's role is in the
340   MACsec protocol, explain what the module does in support of the IV generation for the
341   MACsec's use of AES-GCM, and state that when supporting the MACsec protocol in the
342   approved mode, the module should only be used together with the CMVP-validated
343   modules providing the remaining <Peer, Authenticator, …> functionalities.
344   7. MACsec Link Configuration - All configuration instructions for the link between the
345   Authenticator and the Authentication Server shall be provided in the Security Policy of
346   the module.
347   8. MACsec Link Secure - The Peer and the Authenticator Modules Security Policies shall
348   state that the link between the Peer and the Authenticator should be secured to prevent
349   the possibility for an attacker to introduce foreign equipment into the local area network
350   9. SSHv2 Compliance - If the vendor claims that the IV generation is in compliance with
351   the SSHv2 specification and only for use within the SSHv2 protocol, then the module's
352   Security Policy and the Validation Test Report shall explicitly state the module's
353   compliance with RFCs 4252, 4253 and 5647.
354   10. Case 2: Internal, Random Generation - If the IV is generated internally at its entirety
355   randomly, the Security Policy shall include a statement that the generation uses an
356   Approved DRBG that is internal to the module's boundary and the IV length is at least 96
357   bits (per SP 800-38D).

358 11. Case 3: Generated Deterministically - Human Operator Reset - There will be a human
359   operator who will reset the IV to the last one used in case the module's power is lost and
360   then restored. (This condition is not enforced but shall be stated in the module's Security
361   Policy, under the "User Guide" heading.)
362 12. Case 3: Generated Deterministically - Power Lost and Restored - In case the module's
363   power is lost and then restored, a new key for use with the AES-GCM
364   encryption/decryption shall be established. (This condition may or may not be enforced
365   but shall be stated in the module's Security Policy, under the "User Guide" heading.)
366 13. Case 3: Generated Deterministically - Generation and Restoration Statement - A
367   statement explaining how the deterministic IV generation is performed and how the IV
368   restoration conditions are met shall be included in the Security Policy and Validation Test
369   Report.
370 14. Case 5: Industry Protocol Not in Case 1 - Name and Version - The module's Security
371   Policy shall state the protocol's name and version number and confirm that the IV is
372   generated and used within this protocol's implementation.
373 15. Case 5: Industry Protocol Not in Case 1 - Document List - The Security Policy shall list
374   the documents (such as the IETF RFCs) where the protocol and, specifically, the use of
375   the AES-GCM encryption within the protocol are defined.
376

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

378 1. Parameter Lengths - The vendor shall document, in the module's Security Policy, the
379   lengths of the following parameters from SP 800-38G: radix, radix^minlen, minlen,
380   maxlen, and maxTlen.
381

IG:D.A - Acceptable SSP Establishment Protocols

383 1. SSP Establishment Caveat - If the comparable strength of the largest SSP (taken at face
384   value) that can be established by a cryptographic module is greater than the largest
385   comparable strength of the implemented SSP establishment method, then the module
386   certificate and Security Policy will be annotated with, in addition to the other required
387   caveats, the caveat "(SSP establishment methodology provides xx bits of encryption
388   strength)" for that SSP establishment method.
389

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

391 1. Not Validated, Not Listed - If the module implements a KDF from SP 800-135rev1 and
392   this KDF has not been validated by the CAVP, then the module's certificate shall not list
393   this function. The module's Security Policy shall make it clear that the corresponding
394   protocol shall not be used in an approved mode of operation.
395 2. Validated, Listed with Statement - If the module's Security Policy claims that the module
396   supports or uses the corresponding protocol, then the Security Policy shall state that no
397   parts of this protocol, other than the approved cryptographic algorithms and the KDFs,
398   have been tested by the CAVP and CMVP.
399 3. KDF Not Implemented - If the module does not implement any KDFs from SP 800-
400   135rev1 but the module's Security Policy claims that the module supports or uses parts of
401   the corresponding protocol(s) then no entry on the certificate's approved or allowed
402   algorithms lines is required. As in the case considered above (2), the Security Policy shall
403   state that this protocol has not been reviewed or tested by the CAVP and CMVP.

404
405   **IG:D.E - Assurance of the Validity of a Public Key for SSP establishment**
406   1. No Ephemeral Public Key Validation - If a cryptographic module implements a key
407   agreement / shared secret computation scheme whereby the recipient of an ephemeral
408   public key omits the explicit ephemeral public key validation, the modules Security
409   Policy shall indicate the appropriate protocol listed above that allows the omission of the
410   validation in order to claim conformance to this Implementation Guidance.
411
412   **IG:D.F - Key Agreement Methods**
413   1. Scenario 1, Path 2 Requirements - The module's Security Policy shall state which key
414   agreement algorithms and algorithm components have been implemented and CAVP-
415   tested.
416   2. Scenario 2, Path 2 Requirements - The module's Security Policy shall state which key
417   agreement algorithms and algorithm components have been implemented and CAVP-
418   tested.
419   3. Scenario 3 Requirements - An ECC scheme using the elliptic curves compliant with IG
420   C.A. This scheme shall be shown as allowed in the module's Security Policy and
421   documented on the certificate's non-approved line.
422   4. Scenario 1, Options List - For Scenario 1, KAS1 may be implemented as either a basic
423   scheme (no key confirmation) or a Party_V-Confirmation scheme. KAS2 may be
424   implemented as either a basic, or a Party_V-Confirmation, or a Party_U-Confirmation or
425   a bilateral-confirmation scheme. The module's Security Policy shall state which of the
426   following schemes have been implemented and tested.
427
428   **IG:D.G - Key Transport Methods**
429   1. RSA Details - The Security Policy shall document the tested RSA modulus sizes, the
430   method (from FIPS 186-4) of RSA key generation, the tested key confirmation (if
431   applicable) and assurances, as defined in Sections 5 and 6 of SP 800-56Brev2, and
432   whether the encapsulation, un-encapsulation or both methods are supported.
433   2. RSA OAEP Support - The Security Policy shall indicate the module's support for the
434   KTS-OAEP scheme and, if applicable, document the module's readiness to use the
435   transported key in a hybrid scheme defined in Section 9.3 of SP 800-56Brev2.
436   3. RSA Non-Approved but Allowed - The module's Security Policy shall state that the
437   PKCS#1-v1.5 padding is performed as shown in Section 8.1 of RFC 2313.
438   4. Approved Annotation with Caveat - The module's compliance with either the symmetric
439   or the asymmetric key based approved key transport techniques shall be annotated in the
440   approved cryptographic algorithms list in the Security Policy, with the caveats, as
441   necessary and as shown in the Management Manual - Annex A.
442   5. Allowed Annotation with Caveat - The use of the allowed methods for key transport shall
443   be annotated in the allowed algorithms list in the Security Policy.
444
445   **IG:D.H - Requirements for Vendor Affirmation to SP 800-133**
446   1. Method Details - The Security Policy shall provide the details of each method.
447
448   **IG:D.J - Entropy Estimation and Compliance with SP 800-90B**

449   1. Amount Generated and Entropy per Bit - When entropy source testing to SP 800-90B is
450   applicable, the module's Security Policy shall document the overall amount of generated
451   entropy and the estimated amount of entropy per the source's output bit.
452   2. Deterioration Action - If the source may deteriorate to the point when the generation of
453   the sufficient amount of entropy (sufficient to support the claims about the strengths of
454   the generated cryptographic keys) can no longer be guaranteed, the module's Security
455   Policy shall explain what action is to be taken.
456

IG:D.N - SP 800-132 Password-Based Key Derivation for Storage Applications
458   1. Designate Option - Four options (1a, 1b, 2a and 2b) are given for deriving a Data
459   Protection Key from the Master Key. The vendor shall specify in the cryptographic
460   module's Security Policy which option or options are used by the module.
461   2. Option 1b Requirements - The Security Policy shall indicate for option 1b – the approved
462   key derivation function (KDF) used.
463   3. Option 2a Requirements - The Security Policy shall indicate for option 2a – the approved
464   authenticated encryption algorithm or approved authentication technique and approved
465   encryption algorithm used.
466   4. Option 2b Requirements - The Security Policy shall indicate for option 2b – the approved
467   authenticated encryption algorithm or approved authentication technique and approved
468   encryption algorithm and the approved KDF used.
469   5. Password Length and Probability - Therefore, the vendor shall document in the module's
470   Security Policy the length of a password/passphrase used in key derivation and establish
471   an upper bound for the probability of having this parameter guessed at random.
472   6. Iteration Count and Justification - The vendor shall document in the module's Security
473   Policy, a justification for the iteration count value used. If multiple iteration count values
474   are used, the vendor shall document the conditions that lead to the various values.
475   7. Storage Only Statement - The vendor shall indicate in the module's Security Policy that
476   keys derived from passwords, as shown in SP 800-132, may only be used in storage
477   applications.
478

IG:D.O - Combining Entropy from Multiple Sources
480   1. Combined Entropy Explanation - The Security Policy shall further explain the nature of
481   the module's entropy sources, specify which of them are creditable, and indicate if
482   Method 1 or Method 2 is used for entropy calculation.
483

IG:D.P - SP 800-56Crev2 One-Step Key Derivation Function Without a Counter
485   1. SP800-56Crev2 One-Step Use - The Security Policy shall explain how each KDA is used
486   by the module.
487

B.2.3 Cryptographic module interfaces

489

IG:3.4.A - Trusted Channel
491   1. Trusted Channel Physical Characteristics - The Security Policy shall specify the physical
492   characteristics of the Trusted Channel, with an explanation of how the Trusted Channel
493   will protect the plaintext CSPs

494   2. Trusted Channel Controls - The Security Policy shall specify the controls that are used to
495   maintain the Trusted Channel, including the list of any physical tools (wires, cables, etc.)
496   needed to establish the Trusted Channel
497   3. Trusted Channel Operator Instructions - The Security Policy shall specify operator
498   instructions for setup and operation of the Trusted Channel
499   4. Trusted Channel Source or Target - The Security Policy shall specify the specific
500   characteristics and specification of the source or target of the Trusted Channel relative to
501   the cryptographic module.
502   5. Trusted Channel Path Control - The Security Policy shall specify how the operator stays
503   in control over the physical path and is able to prevent any unauthorized tampering.
504

B.2.4 Roles, services, and authentication

506

IG:4.4.A - Multi-Operator Authentication
508   1. Case 1 Requirements - For Case 1, the Security Policy shall identify all roles, and for
509   each role, the authentication method (i.e. either role-based or identity-based).
510   2. Case 3 Requirements - For Case 3, the Security Policy shall explain how the
511   authentication may be performed for each role.
512   3. Case 4 Requirements - For Case 4, the Security Policy shall identify all roles, and for
513   each role, the authentication method (i.e. either multi-factor identity-based or identity-
514   based).
515

B.2.5 Software/Firmware security

517

IG:5.A - Non-Reconfigurable Memory Integrity Test
519   1. End of Life Procedures - The security policy shall state the module's end of life
520   procedures and the timeline for these procedures.
521

B.2.6 Operational environment

523

524 No Additions.

525

B.2.7 Physical security

527

SP800-140:VE07.26.02
529   1. High and Low Temperature - The vendor provided security policy shall specify the
530   nominal and high/low temperature range.
531

SP800-140:VE07.77.02
533   1. Temperature Shutdown/Zeroise - The security policy shall address whether the employed
534   EFP feature forces module shutdown or zeroises all unprotected SSPs and shall specify
535   the temperature range met.
536

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

660
661 **B.2.1.1 Overview**
662 Requirement Statements - None
663
664 **Notes:** Overview information desired by the vendor
665
666 **Input Method:** Web Cryptik
667
668
669 **B.2.1.2 Security Levels**
670 Requirement Statements
671   1. Security Level Table - A table indicating the individual clause levels and overall
672   level. [AnnexB:]
673   2. Security Rating - Overall Security Rating of the module and the Security Levels
674   of individual areas [AnnexB:]
675
676 **Notes:** None
677
678 **Input Method:** Web Cryptik
679
680
681 **B.2.1.3 Additional Information**
682 Requirement Statements - None
683
684 **Notes:** Additional Vendor Information
685
686 **Input Method:** Separate Vendor Doc
687

B.2.2 Cryptographic module specification

688
689
690 **B.2.2.1 Purpose or Use**
691 Requirement Statements
692   1. Purpose - Intended purpose or use of the module including intended use
693   environment [AnnexB:]
694
695 **Notes:** None
696
697 **Input Method:** Web Cryptik
698
699
700 **B.2.2.2 Diagram, Schematic, or Photograph**
701 Requirement Statements
702   1. Diagram, Schematic, or Photograph - Illustrative diagram, schematic or
703   photograph of the module. A photograph included for hardware modules. If the
704   security policy encompasses multiple versions of the module, each version is

705   represented separately or annotated that the representation is illustrated for all
706   versions. For a software or firmware cryptographic module, the security policy
707   includes a block diagram that illustrates [AnnexB:]
708   2. Location of Logical Object - the location of the logical object of the software or
709   firmware module with respect to the operating system, other supporting
710   applications and the cryptographic boundary so that all the logical and physical
711   layers between the logical object and the cryptographic boundary are clearly
712   defined [AnnexB:]
713   3. Interactions of the Logical Object - the interactions of the logical object of the
714   software or firmware module with the operating system and other supporting
715   applications resident within the cryptographic boundary. [AnnexB:]
716   4. Block Diagram - Block Diagram, as applicable. [AnnexB:]
717
718   **Notes:** The image will show the disjoint hardware component of the hybrid module.
719
720   **Input Method:** Separate Vendor Doc
721
722
723   **B.2.2.3 Description**
724   Requirement Statements
725   1. Description - Description of Module [AnnexB:]
726
727   **Notes:** None
728
729   **Input Method:** Web Cryptik
730
731
732   **B.2.2.4 Version Information**
733   Requirement Statements
734   1. Version Information - Provide version/identification of the module(s) and all
735   components (hardware, software or firmware). [AnnexB:]
736
737   **Notes:** None
738
739   **Input Method:** Web Cryptik
740
741
742   **B.2.2.5 Module Type**
743   Requirement Statements
744   1. Module Type - Hardware, Software, Firmware, or Hybrid designation: [AnnexB:]
745
746   **Notes:** None
747
748   **Input Method:** Web Cryptik
749
750

751 **B.2.2.6 Operating Environments**
752 Requirement Statements
753   1. Operating Systems - for software, firmware and hybrid cryptographic modules,
754   list the operating system(s) the module was tested on and list the operating
755   system(s) that the vendor affirms can be used by the module. [AnnexB:]
756
757 **Notes:** See Appendix A - Security Policy Detailed Information Description
758
759 **Input Method:** Web Cryptik
760
761
762 **B.2.2.7 Vendor Affirmed Operating Environments**
763 Requirement Statements
764   1. Operating Systems - for software, firmware and hybrid cryptographic modules,
765   list the operating system(s) the module was tested on and list the operating
766   system(s) that the vendor affirms can be used by the module. [AnnexB:]
767
768 **Notes:** See Appendix A - Security Policy Detailed Information Description
769
770 **Input Method:** Web Cryptik
771
772
773 **B.2.2.8 Cryptographic Boundary**
774 Requirement Statements
775   1. Physical and Cryptograpic Boundaries - Precise definition of the module's
776   physical and cryptographic boundaries: [AnnexB:]
777
778 **Notes:** None
779
780 **Input Method:** Web Cryptik
781
782
783 **B.2.2.9 Physical Perimeter**
784 Requirement Statements
785   1. Physical and Cryptograpic Boundaries - Precise definition of the module's
786   physical and cryptographic boundaries: [AnnexB:]
787
788 **Notes:** None
789
790 **Input Method:** Web Cryptik
791
792
793 **B.2.2.10 Excluded Components**
794 Requirement Statements
795   1. Excluded Components - the hardware, software or firmware excluded from the
796   cryptographic boundaries specified in the security policy. [AnnexB:]

797
798   **Notes:** Enter "None" instead of leaving blank
799
800   **Input Method:** Web Cryptik
801
802
803   **B.2.2.11 Modes of Operation**
804   Requirement Statements
805   1. Modes of Operation - Modes of operation and how to enter/exit each mode. The
806   security policy describes each approved mode of operation implemented in the
807   cryptographic module and how each mode is configured. [AnnexB:]
808
809   **Notes:** None
810
811   **Input Method:** Web Cryptik
812
813
814   **B.2.2.12 Degraded Mode**
815   Requirement Statements
816   1. Degraded Mode - Description of degraded operation [AnnexB:]
817
818   **Notes:** Enter "None" instead of leaving blank
819
820   **Input Method:** Web Cryptik
821
822
823   **B.2.2.13 Approved Algorithms**
824   Requirement Statements
825   1. Tested Components (CVL) - The Security Policy shall individually list the tested
826   components shown in the module's CVL certificates that may be called during the
827   operation of the module. [IG:2.4.A]
828   2. Security Functions Table - Table of all security functions, with specific key
829   strengths employed for approved services, as well as the implemented modes of
830   operation (e.g. CBC, CCM), if appropriate. [AnnexB:]
831
832   **Notes:** This table is generated from the selected CAVP Tested algorithms, modes, and properties
833
834   **Input Method:** CAVP Algorithm-Mode-Property Selection
835
836
837   **B.2.2.14 Vendor Affirmed Algorithms**
838   Requirement Statements
839   1. Vendor Affirmed Security Methods - The vendor provided non-proprietary
840   security policy shall include a list of all vendor affirmed security methods.
841   [SP800-140:VE02.20.04]

842   2. Security Functions Table - Table of all security functions, with specific key
843   strengths employed for approved services, as well as the implemented modes of
844   operation (e.g. CBC, CCM), if appropriate. [AnnexB:]
845
846 **Notes:** A list of the vendor affirmed algorithms allowed in the approved mode of operation - See
847 Appendix A - Security Policy Detailed Information Description
848
849 **Input Method:** Web Cryptik
850
851

852 **B.2.2.15 Non-Approved, Allowed Algorithms**
853 Requirement Statements
854   1. Security Functions Table - Table of all security functions, with specific key
855   strengths employed for approved services, as well as the implemented modes of
856   operation (e.g. CBC, CCM), if appropriate. [AnnexB:]
857
858 **Notes:** A list of the non-approved algorithms allowed in the approved mode of operation - See
859 Appendix A - Security Policy Detailed Information Description
860
861 **Input Method:** Web Cryptik
862
863

864 **B.2.2.16 Non-Approved, Allowed Algorithms with No Security Claimed**
865 Requirement Statements
866   1. Non-Approved No Security Claimed - If a non-approved cryptographic algorithm
867   is used by the module in the approved mode but is not a security function, the
868   algorithm shall be included in the list of non-approved but allowed algorithms in
869   the Security Policy with the caveat "(no security claimed)" [IG:2.4.A]
870   2. Security Functions Table - Table of all security functions, with specific key
871   strengths employed for approved services, as well as the implemented modes of
872   operation (e.g. CBC, CCM), if appropriate. [AnnexB:]
873
874 **Notes:** A list of the non-approved algorithms allowed in the approved mode of operation with no
875 security claimed. These algorithms do not claim any security and are not used to meet FIPS 140-
876 3 requirements. Therefore, SSPs do not map to these algorithms. - See Appendix A - Security
877 Policy Detailed Information Description
878
879 **Input Method:** Web Cryptik
880
881

882 **B.2.2.17 Security Function Implementations**
883 Requirement Statements
884   1. Security Functions Table - Table of all security functions, with specific key
885   strengths employed for approved services, as well as the implemented modes of
886   operation (e.g. CBC, CCM), if appropriate. [AnnexB:]
887

888   **Notes:** See Appendix A - Security Policy Detailed Information Description
889
890   **Input Method:** Web Cryptik
891
892

893   **B.2.2.18 Non-Approved, Not Allowed Algorithms**
894   Requirement Statements - None
895
896   **Notes:** See Appendix A - Security Policy Detailed Information Description
897
898   **Input Method:** Web Cryptik
899
900

901   **B.2.2.19 Algorithm Specific Information**
902   Requirement Statements

903   1. List of Curves - The Security Policy shall list all approved and non-approved
904   curves that are implemented. [IG:C.A]
905   2. Security Strength of Curves - The Security Policy shall indicate the associated
906   security strength for all non-approved curves that are implemented. [IG:C.A]
907   3. Vendor Affirmation of SHA-3 - If the module implemented the same higher-level
908   algorithm with a FIPS 180-4 hash function and there is a corresponding entry on
909   the approved line of the module's validation certificate, then the vendor
910   affirmation of the same algorithm using SHA-3 does not need to be shown
911   separately on the certificate's approved line but shall be documented in the
912   module's Security Policy. [IG:C.C]
913   4. Use of a Truncated HMAC - The use of the truncated HMAC shall be shown in
914   the module's Security Policy. [IG:C.D]
915   5. KAS-RSA Scheme Listing - When implementing a key agreement scheme (or a
916   shared secret computation as part of a key agreement scheme), the vendor shall
917   indicate in the module's Security Policy whether the scheme is of the Diffie-
918   Hellman or the MQV variety. If a key agreement scheme (FFC or ECC-based) is
919   documented on the module's certificate's non-approved line, the vendor is
920   encouraged to state there if this is a Diffie-Hellman or an MQV scheme. [IG:C.F]
921   6. Triple-DES within IETF Protocol - The limit of 2^{20} encryptions with the same
922   Triple-DES key applies when keys are generated as part of one of the recognized
923   IETF protocols. To use this provision, the Security Policy shall say which of the
924   IETF protocols governs the generation of the Triple-DES keys and list the IETF
925   RFC(s) where the details of this protocol, relevant to the generation of the Triple-
926   DES encryption keys, are documented. [IG:C.G]
927   7. Triple-DES Limit Enforcement - The Security Policy shall explain how the
928   module performs the enforcement. [IG:C.G]
929   8. Compatibility with TLS 1.2 - If the vendor claims that the IV generation is in
930   compliance with the TLS 1.2 specification and only for use within the TLS 1.2
931   protocol, then the module's Security Policy shall explicitly state the module's
932   compatibility with TLS 1.2 and the module's support for acceptable AES-GCM
933   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

1114   1. Not Validated, Not Listed - If the module implements a KDF from SP 800-
1115   135rev1 and this KDF has not been validated by the CAVP, then the module's
1116   certificate shall not list this function. The module's Security Policy shall make it
1117   clear that the corresponding protocol shall not be used in an approved mode of
1118   operation. [IG:D.C]
1119   2. Validated, Listed with Statement - If the module's Security Policy claims that the
1120   module supports or uses the corresponding protocol, then the Security Policy shall
1121   state that no parts of this protocol, other than the approved cryptographic
1122   algorithms and the KDFs, have been tested by the CAVP and CMVP. [IG:D.C]
1123   3. KDF Not Implemented - If the module does not implement any KDFs from SP
1124   800-135rev1 but the module's Security Policy claims that the module supports or
1125   uses parts of the corresponding protocol(s) then no entry on the certificate's
1126   approved or allowed algorithms lines is required. As in the case considered above
1127   (2), the Security Policy shall state that this protocol has not been reviewed or
1128   tested by the CAVP and CMVP. [IG:D.C]
1129
1130 **Notes:** None
1131
1132 **Input Method:** Web Cryptik
1133
1134

1135 **B.2.2.24 Key Generation**
1136 Requirement Statements
1137   1. Method Details - The Security Policy shall provide the details of each method.
1138   [IG:D.H]
1139
1140 **Notes:** None
1141
1142 **Input Method:** Web Cryptik
1143
1144

1145 **B.2.2.25 Design and Rules**
1146 Requirement Statements
1147   1. Design and Rules - Overall security design and the rules of operation [AnnexB:]
1148
1149 **Notes:** As part of this requirement, algorithm-specific guidance, rules, and security policy-
1150 specific requirements shall be included.
1151
1152 **Input Method:** Web Cryptik
1153
1154

1155 **B.2.2.26 Initialisation**
1156 Requirement Statements
1157   1. Initialisation - Initialisation requirements, as applicable. [AnnexB:]
1158
1159 **Notes:** None

1160
1161   **Input Method:** Web Cryptik
1162
1163
1164   **B.2.2.27 Additional Information**
1165   Requirement Statements - None
1166
1167   **Notes:** Additional Vendor Information
1168
1169   **Input Method:** Separate Vendor Doc
1170

1171 B.2.3 Cryptographic module interfaces

1172
1173   **B.2.3.1 Ports and Interfaces**
1174   Requirement Statements
1175   1. Ports and Intefaces Table - Table listing of all ports and interfaces (physical and
1176   logical). [AnnexB:]
1177   2. Information Passing - Define the information passing over the five logical
1178   interfaces. [AnnexB:]
1179   3. Physical Ports - Specify physical ports and data that pass over them [AnnexB:]
1180
1181   **Notes:** The physical ports here should map to the physical ports shown in the module
1182   images/diagrams. If the ports are different per module within the same submission, then this
1183   table should indicate the differences. - See Appendix A - Security Policy Detailed Information
1184   Description
1185
1186   **Input Method:** Web Cryptik
1187
1188
1189   **B.2.3.2 Trusted Channel Specification**
1190   Requirement Statements
1191   1. Trusted Channel Physical Characteristics - The Security Policy shall specify the
1192   physical characteristics of the Trusted Channel, with an explanation of how the
1193   Trusted Channel will protect the plaintext CSPs [IG:3.4.A]
1194   2. Trusted Channel Controls - The Security Policy shall specify the controls that are
1195   used to maintain the Trusted Channel, including the list of any physical tools
1196   (wires, cables, etc.) needed to establish the Trusted Channel [IG:3.4.A]
1197   3. Trusted Channel Operator Instructions - The Security Policy shall specify
1198   operator instructions for setup and operation of the Trusted Channel [IG:3.4.A]
1199   4. Trusted Channel Source or Target - The Security Policy shall specify the specific
1200   characteristics and specification of the source or target of the Trusted Channel
1201   relative to the cryptographic module. [IG:3.4.A]
1202   5. Trusted Channel Path Control - The Security Policy shall specify how the
1203   operator stays in control over the physical path and is able to prevent any
1204   unauthorized tampering. [IG:3.4.A]

1205   6.   Trusted Channel - Specify Trusted Channel [AnnexB:]
1206
1207   **Notes:** None
1208
1209   **Input Method:** Web Cryptik
1210
1211
1212   **B.2.3.3 Control Interface Not Inhibited**
1213   Requirement Statements
1214   1.   Control Interface Not Inhibited - Specification of the exceptions and rationale if
1215   the control output interface is not inhibited during the error state, [AnnexB:]
1216
1217   **Notes:** None
1218
1219   **Input Method:** Web Cryptik
1220
1221
1222   **B.2.3.4 Additional Information**
1223   Requirement Statements - None
1224
1225   **Notes:** Additional Vendor Information
1226
1227   **Input Method:** Separate Vendor Doc
1228

1229   ## B.2.4 Roles, services, and authentication

1230
1231   **B.2.4.1 Authentication Methods**
1232   Requirement Statements
1233   1.   Authentication Methods - Specify each authentication method, whether the
1234   method is Identity or Role-based and the method is required. [AnnexB:]
1235   2.   Strength of Authentication - How is the strength of authentication requirement
1236   met? [AnnexB:]
1237   3.   Service Info - For each service, the service name, a concise description of the
1238   service purpose and/or use (the service name alone may, in some instances,
1239   provide this information), a list of approved security functions (algorithm(s), key
1240   management technique(s) or authentication technique) used by, or implemented
1241   through, the invocation of the service, and a list of the SSPs associated with the
1242   service or with the approved security function(s) it uses. For each operator role
1243   authorised to use the service info [AnnexB:]
1244
1245   **Notes:** See Appendix A - Security Policy Detailed Information Description
1246
1247   **Input Method:** Web Cryptik
1248
1249

1250   **B.2.4.2 Roles**
1251   Requirement Statements
1252   1. Roles List - Specify all roles [AnnexB:]
1253   2. Roles Table - Table of Roles, with corresponding service commands with input
1254   and output [AnnexB:]
1255
1256   **Notes:** See Appendix A - Security Policy Detailed Information Description
1257
1258   **Input Method:** Web Cryptik
1259
1260
1261   **B.2.4.3 Bypass Actions and Status**
1262   Requirement Statements
1263   1. Bypass Actions - If there is a bypass capability, what are the two independent
1264   actions and how is the status checked? [AnnexB:]
1265
1266   **Notes:** None
1267
1268   **Input Method:** Web Cryptik
1269
1270
1271   **B.2.4.4 Cryptographic Output Actions and Status**
1272   Requirement Statements
1273   1. Cryptographic Output - If there is a self-initiated cryptographic output capability,
1274   what are the two independent actions how is the status indicated? [AnnexB:]
1275
1276   **Notes:** None
1277
1278   **Input Method:** Web Cryptik
1279
1280
1281   **B.2.4.5 External Software/Firmware Loaded**
1282   Requirement Statements
1283   1. External Software/Firmware Loadded - If external software or firmware is loaded,
1284   specify the controls on loading and the isolation of code that deter unauthorised
1285   access to and use of the module. [AnnexB:]
1286
1287   **Notes:** None
1288
1289   **Input Method:** Web Cryptik
1290
1291
1292   **B.2.4.6 Approved Services**
1293   Requirement Statements

1294   1. List of Services and Indicators - The Security Policy shall provide a complete list
1295   of all approved and non-approved services along with details on each service and
1296   their respective indicators (if applicable). [IG:2.4.C]
1297   2. List of Services and Indicators - The Security Policy shall provide a complete list
1298   of all approved and non-approved services along with details on each service and
1299   their respective indicators (if applicable). [IG:2.4.C]
1300   3. Approved and Non-Approved Services - Separately list the security and non-
1301   security services, both approved and non-approved. [AnnexB:]
1302   4. Service Info - For each service, the service name, a concise description of the
1303   service purpose and/or use (the service name alone may, in some instances,
1304   provide this information), a list of approved security functions (algorithm(s), key
1305   management technique(s) or authentication technique) used by, or implemented
1306   through, the invocation of the service, and a list of the SSPs associated with the
1307   service or with the approved security function(s) it uses. For each operator role
1308   authorised to use the service info [AnnexB:]
1309   5. Roles List - Specify all roles [AnnexB:]
1310
1311   **Notes:** See Appendix A - Security Policy Detailed Information Description
1312
1313   **Input Method:** Web Cryptik
1314
1315

1316   **B.2.4.7 Non-Approved Services**
1317   Requirement Statements
1318   1. Approved and Non-Approved Services - Separately list the security and non-
1319   security services, both approved and non-approved. [AnnexB:]
1320   2. Service Info - For each service, the service name, a concise description of the
1321   service purpose and/or use (the service name alone may, in some instances,
1322   provide this information), a list of approved security functions (algorithm(s), key
1323   management technique(s) or authentication technique) used by, or implemented
1324   through, the invocation of the service, and a list of the SSPs associated with the
1325   service or with the approved security function(s) it uses. For each operator role
1326   authorised to use the service info [AnnexB:]
1327
1328   **Notes:** See Appendix A - Security Policy Detailed Information Description
1329
1330   **Input Method:** Web Cryptik
1331
1332

1333   **B.2.4.8 Installation Process**
1334   Requirement Statements
1335   1. Installation Process and Authentication Mechanisms - Describe the installation
1336   process and the cryptographic authentication mechanism(s). [AnnexB:]
1337
1338   **Notes:** None
1339

1340   **Input Method:** Web Cryptik
1341
1342
1343   **B.2.4.9 Multi-Operator Authentication**
1344   Requirement Statements
1345   1. Case 1 Requirements - For Case 1, the Security Policy shall identify all roles, and
1346   for each role, the authentication method (i.e. either role-based or identity-based).
1347   [IG:4.4.A]
1348   2. Case 3 Requirements - For Case 3, the Security Policy shall explain how the
1349   authentication may be performed for each role. [IG:4.4.A]
1350   3. Case 4 Requirements - For Case 4, the Security Policy shall identify all roles, and
1351   for each role, the authentication method (i.e. either multi-factor identity-based or
1352   identity-based). [IG:4.4.A]
1353
1354   **Notes:** None
1355
1356   **Input Method:** Web Cryptik
1357
1358
1359   **B.2.4.10 Additional Information**
1360   Requirement Statements - None
1361
1362   **Notes:** Additional Vendor Information
1363
1364   **Input Method:** Separate Vendor Doc
1365
1366   # B.2.5 Software/Firmware security
1367
1368   **B.2.5.1 Integrity Techniques**
1369   Requirement Statements
1370   1. Integrity Techniques - Specify the approved integrity techniques or EDC
1371   employed [AnnexB:]
1372
1373   **Notes:** None
1374
1375   **Input Method:** Web Cryptik
1376
1377
1378   **B.2.5.2 Initiate on Demand**
1379   Requirement Statements
1380   1. Initiate on Demand - Specify how the operator can initiate the integrity test on
1381   demand. [AnnexB:]
1382   2. Executable Code - Specify the form and each component of executable code
1383   provided. [AnnexB:]
1384

1385   **Notes:** None
1386
1387   **Input Method:** Web Cryptik
1388
1389
1390   **B.2.5.3 Executable Code**
1391   Requirement Statements - None
1392
1393   **Notes:** None
1394
1395   **Input Method:** Web Cryptik
1396
1397
1398   **B.2.5.4 Open Source Parameters**
1399   Requirement Statements
1400   1. Open Source Parameters - If the module is open source, specify the compilers and
1401   control parameters required to compile the code into an executable format.
1402   [AnnexB:]
1403
1404   **Notes:** None
1405
1406   **Input Method:** Web Cryptik
1407
1408
1409   **B.2.5.5 Non-Reconfigurable Memory**
1410   Requirement Statements
1411   1. End of Life Procedures - The security policy shall state the module's end of life
1412   procedures and the timeline for these procedures. [IG:5.A]
1413
1414   **Notes:** None
1415
1416   **Input Method:** Web Cryptik
1417
1418
1419   **B.2.5.6 Additional Information**
1420   Requirement Statements - None
1421
1422   **Notes:** Additional Vendor Information
1423
1424   **Input Method:** Separate Vendor Doc
1425
1426   ## B.2.6 Operational environment
1427
1428   **B.2.6.1 Operational Environment Type**
1429   Requirement Statements

1430   1. Operational Environment Type - Identify the operational environment (e.g. non-
1431   modifiable, limited, or modifiable). [AnnexB:]
1432
1433 **Notes:** Include an explanation supporting the OE type
1434
1435 **Input Method:** Web Cryptik
1436
1437

1438 **B.2.6.2 Operating Environments**
1439 Requirement Statements
1440   1. Operational Enviornment List - Identify the operating system(s) and tested
1441   platform(s). [AnnexB:]
1442
1443 **Notes:** See Appendix A - Security Policy Detailed Information Description
1444
1445 **Input Method:** Web Cryptik
1446
1447

1448 **B.2.6.3 Operational Environment Requirements**
1449 Requirement Statements
1450   1. Software Module Operating Environment Restrictions - Restrictions to the
1451   configuration of the operational environment shall be documented in the Security
1452   Policy of the cryptographic module. [IG:9.5.A]
1453   2. Op Env Requirements - For each applicable level, explain how requirements are
1454   satisfied. [AnnexB:]
1455
1456 **Notes:** None
1457
1458 **Input Method:** Web Cryptik
1459
1460

1461 **B.2.6.4 Vendor Affirmed Operating Environments**
1462 Requirement Statements
1463   1. Vendor Affirmed OE Claim - The vendor may provide claims of porting to other
1464   OS's not specifically tested yet vendor affirmation of correct operation is claimed.
1465   [AnnexB:]
1466
1467 **Notes:** See Appendix A - Security Policy Detailed Information Description
1468
1469 **Input Method:** Web Cryptik
1470
1471

1472 **B.2.6.5 Configuration Settings**
1473 Requirement Statements
1474   1. Config Settings - Specification of the security rules, settings or restrictions to the
1475   configuration of the operational environment. [AnnexB:]

1476
1477 **Notes:** None
1478
1479 **Input Method:** Web Cryptik
1480
1481
1482 **B.2.6.6 Restrictions**
1483 Requirement Statements
1484   1. Restrictions - Specification of any restrictions to the configuration of the
1485   operational environment. [AnnexB:]
1486
1487 **Notes:** None
1488
1489 **Input Method:** Web Cryptik
1490
1491
1492 **B.2.6.7 Additional Information**
1493 Requirement Statements - None
1494
1495 **Notes:** Additional Vendor Information
1496
1497 **Input Method:** Separate Vendor Doc
1498
1499 ## B.2.7 Physical security
1500
1501 **B.2.7.1 Embodiment**
1502 Requirement Statements
1503   1. Embodiment - Specify the embodiment (single-chip, multi-chip embedded or
1504   multi-chip standalone). [AnnexB:]
1505
1506 **Notes:** None
1507
1508 **Input Method:** Web Cryptik
1509
1510
1511 **B.2.7.2 Mechanisms and Actions Required**
1512 Requirement Statements
1513   1. Mechanisms - Specify the physical security mechanisms that are implemented in
1514   the module (e.g. tamper evident seals, locks, tamper response and zeroisation
1515   switches, and alarms). [AnnexB:]
1516   2. Actions Required - Specify the actions required by the operator(s) to ensure that
1517   the physical security is maintained (e.g. periodic inspection of tamper-evident
1518   seals or testing of tamper response and zeroisation switches). [AnnexB:]
1519
1520 **Notes:** See Appendix A - Security Policy Detailed Information Description

1521
1522   **Input Method:** Web Cryptik
1523
1524
1525   **B.2.7.3 Reference Photos Include Tamper Seals**
1526   Requirement Statements
1527   1. Reference Photos Include Tamper Seals - Specify the following information if the
1528   module requires operator applied tamper evident seals or security appliances that
1529   the operator will apply or modify over the lifecycle of the module: The reference
1530   photo or illustrations required in B 2.2 will reflect the module configured or
1531   constructed as specified. Additional photos/illustrations may be provided to
1532   reflect other configurations. [AnnexB:]
1533
1534   **Notes:** None
1535
1536   **Input Method:** Separate Vendor Doc
1537
1538
1539   **B.2.7.4 Filler Panel Info**
1540   Requirement Statements
1541   1. Filler Panel Info - If filler panels are needed to cover unpopulated slots or
1542   openings to meet the opacity requirements, they will be included in the photo or
1543   illustrations with tamper seals affixed as needed. The filler panels will be included
1544   in the list of parts. [AnnexB:]
1545
1546   **Notes:** None
1547
1548   **Input Method:** Separate Vendor Doc
1549
1550
1551   **B.2.7.5 Photos of Tamper Seal Placement**
1552   Requirement Statements
1553   1. Photos of Tamper Seal Placement - Photos or illustrations will indicate the precise
1554   placement of any tamper evident seal or security appliance needed to meet the
1555   physical security requirements. [AnnexB:]
1556
1557   **Notes:** None
1558
1559   **Input Method:** Separate Vendor Doc
1560
1561
1562   **B.2.7.6 Total Number to Place**
1563   Requirement Statements
1564   1. Total Number to Place - The total number of tamper evident seals or security
1565   appliances that are needed will be indicated (e.g. 5 tamper evident seals and 2
1566   opacity screens). The photos or illustrations which provide instruction on the

1567   precise placement will have each item numbered in the photo or illustration and
1568   will equal the total number indicated (the actual tamper evident seals or security
1569   appliances are not required to be numbered). [AnnexB:]
1570

1571 **Notes:** None

1572

1573 **Input Method:** Separate Vendor Doc

1574

1575

1576 **B.2.7.7 Part Numbers**
1577 Requirement Statements
1578   1. Part Numbers - If the tamper evident seals or security appliances are parts that can
1579   be reordered from the module vendor, the security policy will indicate the module
1580   vendor part number of the seal, security appliance or applicable security kit. After
1581   reconfiguring, the operator of the module may be required to remove and
1582   introduce new tamper evident seals or security appliances. [AnnexB:]
1583

1584 **Notes:** None

1585

1586 **Input Method:** Separate Vendor Doc

1587

1588

1589 **B.2.7.8 Unused Seals**
1590 Requirement Statements
1591   1. Unused Seals - Specify the operator role responsible for securing and having
1592   control at all times of any unused seals, and the direct control and observation of
1593   any changes to the module such as reconfigurations where the tamper evident
1594   seals or security appliances are removed or installed to ensure the security of the
1595   module is maintained during such changes and the module is returned to an
1596   Approved mode of operation. [AnnexB:]
1597

1598 **Notes:** None

1599

1600 **Input Method:** Separate Vendor Doc

1601

1602

1603 **B.2.7.9 Prepare Surface**
1604 Requirement Statements
1605   1. Prepare Surface - If tamper evident seals or security appliances can be removed or
1606   installed, clear instructions will be included regarding how the surface or device
1607   shall be prepared to apply a new tamper evident seal or security appliance.
1608   [AnnexB:]
1609

1610 **Notes:** None

1611

1612 **Input Method:** Separate Vendor Doc

1613
1614
1615   **B.2.7.10 Fault Induction Mitigation**
1616   Requirement Statements
1617   1. Fault Induction Mitigation - Specify the fault induction mitigation methods
1618   implemented. [AnnexB:]
1619
1620   **Notes:** None
1621
1622   **Input Method:** Separate Vendor Doc
1623
1624
1625   **B.2.7.11 EFP/EFT Information**
1626   Requirement Statements
1627   1. EFT Shutdown/Zeroise - The security policy shall address whether the employed
1628   EFT feature forces module shutdown or zeroises all unprotected SSPs and shall
1629   specify the temperature range met. [SP800-140:VE07.81.02]
1630
1631   **Notes:** For physical Security Level 3 and above - See Appendix A - Security Policy Detailed
1632   Information Description
1633
1634   **Input Method:** Web Cryptik
1635
1636
1637   **B.2.7.12 Hardness Testing Temperature Ranges**
1638   Requirement Statements
1639   1. High and Low Temperature - The vendor provided security policy shall specify
1640   the nominal and high/low temperature range. [SP800-140:VE07.26.02]
1641   2. Temperature Shutdown/Zeroise - The security policy shall address whether the
1642   employed EFP feature forces module shutdown or zeroises all unprotected SSPs
1643   and shall specify the temperature range met. [SP800-140:VE07.77.02]
1644
1645   **Notes:** For modules covered by strong or hard conformal or non-conformal enclosures, coatings,
1646   or potting materials - See Appendix A - Security Policy Detailed Information Description
1647
1648   **Input Method:** Web Cryptik
1649
1650
1651   **B.2.7.13 Additional Information**
1652   Requirement Statements - None
1653
1654   **Notes:** Additional Vendor Information
1655
1656   **Input Method:** Separate Vendor Doc
1657

1658   **B.2.8 Non-invasive security**
1659
1660   **B.2.8.1 Mitigation Techniques**
1661   Requirement Statements
1662   1. Mitigation Techniques - Specify all of the non-invasive mitigation techniques
1663   referenced in Annex F employed by the module to protect the module's CSPs
1664   from non-invasive attacks. [AnnexB:]
1665
1666   **Notes:** Per IG 12.A: Until requirements of SP 800-140F are defined, non-invasive mechanisms
1667   fall under ISO/IEC 19790:2012 Section 7.12 Mitigation of other attacks
1668
1669   **Input Method:** Web Cryptik
1670
1671
1672   **B.2.8.2 Effectiveness**
1673   Requirement Statements
1674   1. Effectiveness - Describe the effectiveness of the non-invasive mitigation
1675   techniques referenced in Annex F employed by the module to protect the
1676   module's CSPs from non-invasive attacks. [AnnexB:]
1677
1678   **Notes:** See B.2.8.1 above.
1679
1680   **Input Method:** Web Cryptik
1681
1682
1683   **B.2.8.3 Additional Information**
1684   Requirement Statements - None
1685
1686   **Notes:** Additional Vendor Information
1687
1688   **Input Method:** Separate Vendor Doc
1689
1690   **B.2.9 Sensitive security parameters management**
1691
1692   **B.2.9.1 Storage Areas**
1693   Requirement Statements
1694   1. SSP Storage - Specify the SSP storage technique(s). [AnnexB:]
1695
1696   **Notes:** See Appendix A - Security Policy Detailed Information Description
1697
1698   **Input Method:** Web Cryptik
1699
1700
1701   **B.2.9.2 SSP Input-Output Methods**
1702   Requirement Statements

1703   1. SSP I/O Methods - Specify the electronic and manual ~~key~~
1704   <ins>SSP</ins> I/O method(s). [AnnexB:]
1705
1706   **Notes:** See Appendix A - Security Policy Detailed Information Description
1707
1708   **Input Method:** Web Cryptik
1709
1710
1711   **B.2.9.3 SSP Zeroization Methods**
1712   Requirement Statements
1713   1. SSP Procedural Zeroisation - If SSPs are zeroised procedurally while under the
1714   control of the operator (i.e., present to observe the method has completed
1715   successfully or controlled via a remote management session), vendor
1716   documentation and the module security policy must specify how the methods
1717   shall be performed. [SP800-140:VE09.28.03]
1718   2. Level 1 Procedures - The Security Policy shall document these procedures to
1719   zeroise unprotected SSPs and how the operator will determine whether the
1720   procedures were successful. [IG:9.7.B]
1721   3. Implicit or Explicit Zeroisation - The "Sensitive security parameters
1722   management" section of the Security Policy shall indicate and provide details on
1723   whether a SSP is zeroised implicitly or explicitly. [IG:9.7.B]
1724   4. SSP Zeroization - Specify the unprotected SSP zeroisation method(s) and
1725   rationale, and operator initiation capability. [AnnexB:]
1726
1727   **Notes:** See Appendix A - Security Policy Detailed Information Description
1728
1729   **Input Method:** Web Cryptik
1730
1731
1732   **B.2.9.4 SSPs**
1733   Requirement Statements
1734   1. SSP Key Table - Provide a SSP table specifying the SSP type(s), strength(s) in
1735   bits, security function(s), security function certification number(s), where and
1736   how the SSP(s) is generated, whether the SSP(s) is imported or exported, any SSP
1737   generation and establishment method used and indicate any related SSPs.
1738   [AnnexB:]
1739   2. SSP Other Table - Present a table of other SSPs and how they are generated.
1740   [AnnexB:]
1741   3. SSP Zeroization - Specify the unprotected SSP zeroisation method(s) and
1742   rationale, and operator initiation capability. [AnnexB:]
1743
1744   **Notes:** See Appendix A - Security Policy Detailed Information Description
1745
1746   **Input Method:** Web Cryptik
1747
1748

1749 **B.2.9.5 Entropy Sources**
1750 Requirement Statements
1751   1. ESV Public Use Document - Indicate that the module is compliant to the ESV
1752   entropy source public use document, if applicable. [ESV:]
1753   2. Scenario 1 - Generated or Well-Defined - The SP shall state the minimum number
1754   of bits of entropy generated by the module or requested per each function call for
1755   use in SSP generation. [IG:9.3.A]
1756   3. Scenario 2 - Passively Receiving - The SP shall state the minimum number of bits
1757   of entropy believed to have been loaded and justify the stated amount (from the
1758   length of the entropy field and from any other factors known to the vendor).
1759   [IG:9.3.A]
1760   4. Scenario 3a - Hybrid Passively Adds - The SP shall state the minimum number of
1761   bits of entropy that can be guaranteed to be actively obtained and, in addition, it
1762   shall state the number of bits believed to have been loaded and justify the stated
1763   amounts (from the lengths of the entropy fields and from any other factors known
1764   to the vendor). [IG:9.3.A]
1765   5. Scenario 3b - Hybrid Passively Preempts - The SP shall state the minimum
1766   number of bits of entropy believed to have been loaded and justify the stated
1767   amount (from the length of the entropy field and from any other factors known to
1768   the vendor). [IG:9.3.A]
1769   6. Estimation and Porting to Untested Platform - The module's SP shall contain a
1770   statement that if porting to an untested platform is allowed then when running a
1771   module on such an untested platform the "No assurance of the minimum strength
1772   of generated SSPs" caveat applies regardless of what caveat, if any, is applicable
1773   to the original validation. [IG:9.3.A]
1774   7. Generating Random Strings, not SSPs - If the module generates random strings
1775   that are not SSPs and the security strength of a generated string is less than the bit
1776   length of the string due to limited entropy,
1777   8. the module's SP shall state the guaranteed amount of entropy for both the SSPs
1778   and the random strings generated by the module using the available entropy
1779   source(s). [IG:9.3.A]
1780   9. Random String Length and Key Strength - The module's SP shall inform the
1781   reader about the length of a random string loaded into the module and explain, if
1782   applicable, the effect of the random string length on the strengths of the generated
1783   keys. [IG:9.3.A]
1784   10. Entropy Sources - Specify the RBG entropy source(s). [AnnexB:]
1785
1786 **Notes:** Per IG 9.3.A, this should include the minimum number of bits of entropy generated,
1787 requested, and/or believed to have been loaded. See Appendix A - Security Policy Detailed
1788 Information Description
1789
1790 **Input Method:** ESV and Web Cryptik
1791
1792
1793 **B.2.9.6 RNGs and Output**
1794 Requirement Statements

1795   1. RNGs - Specify the approved and non-approved random bit generators [AnnexB:]
1796   2. RNG Output - Describe the uses of RBG output(s). [AnnexB:]
1797
1798 **Notes:** Table generated from previously entered information
1799
1800 **Input Method:** N/A
1801
1802
1803 **B.2.9.7 Transitions**
1804 Requirement Statements
1805   1. Transitions - Specify applicable transition periods or timeframes where an
1806   algorithm or key length transitions from approved to non-approved [AnnexB:]
1807
1808 **Notes:** None
1809
1810 **Input Method:** Web Cryptik
1811
1812
1813 **B.2.9.8 Additional Information**
1814 Requirement Statements - None
1815
1816 **Notes:** Additional Vendor Information
1817
1818 **Input Method:** Separate Vendor Doc
1819

1820 ## B.2.10 Self-tests
1821
1822 **B.2.10.1 Pre-Operational Self-Tests**
1823 Requirement Statements
1824   1. Pre-Operational and Conditional List - Provide the list of pre-operational and
1825   conditional self-tests with defined parameters and list conditions under which the
1826   tests are performed. [AnnexB:]
1827
1828 **Notes:** Separate the Pre-Operational from the Conditional - See Appendix A - Security Policy
1829 Detailed Information Description
1830
1831 **Input Method:** Web Cryptik
1832
1833
1834 **B.2.10.2 Conditional Self-Tests**
1835 Requirement Statements
1836   1. Pre-Operational and Conditional List - Provide the list of pre-operational and
1837   conditional self-tests with defined parameters and list conditions under which the
1838   tests are performed. [AnnexB:]
1839

1840   **Notes:** Separate the Pre-Operational from the Conditional - See Appendix A - Security Policy
1841   Detailed Information Description
1842
1843   **Input Method:** Web Cryptik
1844
1845
1846   **B.2.10.3 Self-test Interruption**
1847   Requirement Statements
1848   1. Self-test Interruption - Specify the time period and the policy regarding any
1849   conditions that may result in the interruption of the module's operations during
1850   the time to repeat the period self-tests. [AnnexB:]
1851
1852   **Notes:** None
1853
1854   **Input Method:** Web Cryptik
1855
1856
1857   **B.2.10.4 Error States**
1858   Requirement Statements
1859   1. Error State List - Describe all error states and status indicators [AnnexB:]
1860
1861   **Notes:** See Appendix A - Security Policy Detailed Information Description
1862
1863   **Input Method:** Web Cryptik
1864
1865
1866   **B.2.10.5 Operator Initiation Self-test**
1867   Requirement Statements
1868   1. Operator Initiation Self-test - Describe operator initiation, if applicable.
1869   [AnnexB:]
1870
1871   **Notes:** None
1872
1873   **Input Method:** Web Cryptik
1874
1875
1876   **B.2.10.6 Periodic Self-Tests**
1877   Requirement Statements
1878   1. Levels 3 and 4 Requirements - The time period and any conditions that may result
1879   in the interruption of the module's operations during the time to repeat the pre-
1880   operational or conditional self-tests shall be specified in the security policy
1881   [IG:10.3.E]
1882   2. Met Inherently Claim - Rationale - If a vendor wishes to claim that a module
1883   meets the periodic self-testing requirements inherently based on module design or
1884   limitations and falls into one of the cases above, the vendor shall provide rationale

1885   in the module's security policy as to how the module is protected against faults or
1886   errors that may occur over time. [IG:10.3.E]
1887   3. Met Inherently Claim - Timeframe - The module's security policy shall explicitly
1888   state what the expected timeframe is for the periodic self-test. [IG:10.3.E]
1889   4. Different Execution Triggers - In the event that multiple triggers for periodic self-
1890   test are defined, each mechanism shall be clearly stated in the module's security
1891   policy along with the self-tests that correspond to each. [IG:10.3.E]
1892

1893 **Notes:** Additional Vendor Information
1894

1895 **Input Method:** Separate Vendor Doc
1896

1897

1898 **B.2.10.7 Additional Information**
1899 Requirement Statements - None
1900

1901 **Notes:** None
1902

1903 **Input Method:** Web Cryptik
1904

1905 ## B.2.11 Life-cycle assurance
1906

1907 **B.2.11.1 Startup Procedures**
1908 Requirement Statements
1909   1. Startup Procedures - Specify the procedures for secure installation, initialization,
1910   startup and operation of the module. [AnnexB:]
1911

1912 **Notes:** None
1913

1914 **Input Method:** Rich Text Box
1915

1916

1917 **B.2.11.2 Maintenance Requirements**
1918 Requirement Statements
1919   1. Maintenance Requirements - Specify any maintenance requirements [AnnexB:]
1920

1921 **Notes:** None
1922

1923 **Input Method:** Rich Text Box
1924

1925

1926 **B.2.11.3 Administrator Guidance**
1927 Requirement Statements
1928   1. ESV Public Use Reference - Within the Administrator Guidance, include a
1929   reference to the ESV entropy source public use document, if applicable. [ESV:]

1930   2. Administrator and non-Administrator Guidance - Provide the Administrator and
1931   non-Administrator guidance (may be a separate document). [AnnexB:]
1932

1933   **Notes:** None

1934

1935   **Input Method:** Rich Text Box

1936

1937

1938   **B.2.11.4 Non-Administrator Guidance**
1939   Requirement Statements
1940   1. Administrator and non-Administrator Guidance - Provide the Administrator and
1941   non-Administrator guidance (may be a separate document). [AnnexB:]
1942

1943   **Notes:** None

1944

1945   **Input Method:** Rich Text Box

1946

1947

1948   **B.2.11.5 Additional Information**
1949   Requirement Statements - None

1950

1951   **Notes:** Additional Vendor Information

1952

1953   **Input Method:** Separate Vendor Doc

1954

1955   ## B.2.12 Mitigation of other attacks

1956

1957   **B.2.12.1 Attack List**
1958   Requirement Statements
1959   1. Attack List - Specify what other attacks are mitigated. [AnnexB:]

1960

1961   **Notes:** The level of detail describing the security mechanism(s) implemented to mitigate other
1962   attacks must be similar to what is found on advertisement documentation (product glossies).

1963

1964   **Input Method:** Web Cryptik

1965

1966

1967   **B.2.12.2 Mitigation Effectiveness**
1968   Requirement Statements
1969   1. Mitigation Effectiveness - Describe the effectiveness of the mitigation techniques
1970   listed. [AnnexB:]

1971

1972   **Notes:** None

1973

1974   **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

1996 **Appendix A—Security Policy Detailed Information Description**

1997 This appendix to SP800-140B contains detailed descriptions of the tables of information
1998 required.

1999
2000 **Operating Environments (B.2.2.6 & B.2.6.2)**

2001

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1				

2002
2003 Notes
2004 • No links to other tables
2005
2006
2007 **Operating Environments – Hardware (B.2.2.6)**

2008

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

2009
2010 Notes
2011 • Examples of distinguishing features may be ports and interfaces, memory storage devices
2012 and sizes, field replaceable and stationary accessories (power supplies, fans), etc.
2013
2014
2015 **Vendor Affirmed Operating Environments (B.2.2.7 & B.2.6.4)**

2016

#	Operating System	Hardware Platform
1		

2017

2018 Notes
2019 • No links to other tables
2020

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

2045   **Non-Approved, Allowed Algorithms with No Security Claimed (B.2.2.16)**

2046

Algorithm	Caveat	Use/Function

2047
2048   Notes
2049   • No links to other tables
2050
2051
2052   **Security Function Implementations (SFI) (B.2.2.17)**

2053

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

2054

2055   Notes
2056   • Column Information
2057   o Name – a unique name that relates to the Security Function. It can be KTS1, or
2058   KTS xxx
2059   o Type – a value from the defined set of Security Functions
2060   o Description – how this is used
2061   o SF Properties – If there are specific properties or characteristics associated with
2062   this SF implementation. This could include a reference to a specific Publication
2063   Section, IG, etc. This is where appropriate bit strength caveats should be included.
2064   o Algorithms – what Algorithms from the tested and allowed lists are part of the
2065   implementation. Include prerequisites.
2066   o Algorithm Properties – If a subset of the available properties are used, specify.
2067   • What is meant by Implementations of Security Functions

2068   o A module can (and often does) have more than one implementation for a given
2069   Security Function type
2070   ▪ A KTS that uses an authenticated encryption mode vs. separate encryption
2071   and authentication would both be KTS but would have two
2072   implementation entries
2073   ▪ A SigVer could be used for role/identity authentication and also for an
2074   integrity test
2075   ▪ Block Cipher could include modes for storage (XTS) or as part of a KTS
2076   ▪ The same algorithm could be used with different key sizes to support
2077   different sizes
2078   o For many modules, there would likely be one SFI for a SF type.
2079   • Why these wouldn't just map directly to Services
2080   o At times, these could map directly to services, particularly for modules like
2081   software libraries.
2082   o Documenting in this manner will clarify which algorithms are actual services
2083   provided and which are supporting or prerequisite
2084   o When the same category SF algorithms are used for different functions and
2085   therefore different services, there should be separate SFIs. Many modules have
2086   multiple DigSigVer implementations. For example, one for authentication during
2087   an SSH connection and one for the module startup integrity test. These should be
2088   separately defined as implementations and then mapped to different services.
2089   o Requiring the Services to map directly to the Security Functions seems to
2090   overreach into the vendor's design of their module. The Services and
2091   corresponding level of granularity should be left to the vendor to determine.
2092   • There should only be entries for top-level functions. For example, if SHA2-256 is only
2093   used for Hash DRBG, then it shouldn't be included as a separate Secure Hash entry. And,
2094   if the DRBG is only a supporting function (for example, just a prerequisite to Symmetric
2095   Key Generation), then DRBG shouldn't be a separate entry in this table. The Services
2096   table will include the Security Function Implementations, so often that will likely
2097   determine what is a top-level entry.
2098   • All the supporting and prerequisite algorithms for that implementation would be included
2099   in the Algorithms column.
2100   • Every tested and allowed algorithm should be included somewhere in this table.
2101   • Every SFI should be included in the Services table.
2102
2103

2104 **Non-Approved, Not Allowed Algorithms (B.2.2.18)**

2105

Algorithm	Use/Function

2106
2107 Notes

2108   • No links to other tables
2109
2110
2111   **Ports and Interfaces (B.2.3.1)**

2112

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

2113
2114   Notes
2115   • No links to other tables
2116

2117
2118   **Authentication Methods (B.2.4.1)**

2119

Name	Description	Mechanism	Strength Each	Strength Per Minute

2120

2121   Notes
2122   • Mechanism can be module algorithm, SFI, or alternative
2123

2124   **Roles (B.2.4.2)**

2125

Name	Type	Operator Type	Authentication Methods

2126
2127   Notes
2128   • Type – Role, Identity, or Multi-Factor Identity
2129   • Operator Type – CO, Owner, or other
2130   • Authentication Methods selected from existing table entries
2131

2132   **Approved Services (B.2.4.6)**

2133

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

2134

2135 Notes
2136   • Security Function Implementations - selected from existing SFI table entries
2137   • Roles
2138   ○ selected from existing Roles table entries
2139   ○ could have multiple entries
2140   ○ could also be "Unauthenticated"
2141   • Roles SSP Access
2142   ○ For each role entry, this column has entries for each SSP accessed by that role
2143   using that service with the appropriate access indicators
2144   ▪ Generate: The module generates or derives the SSP.
2145   ▪ Read: The SSP is read from the module (e.g. the SSP is output).
2146   ▪ Write: The SSP is updated, imported, or written to the module.
2147   ▪ Execute: The module uses the SSP in performing a cryptographic
2148   operation.
2149   ▪ Zeroise: The module zeroises the SSP.
2150   ○ SSPs are selected from entries in SSP Table
2151
2152 Example
2153

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

2154
2155 **Non-Approved Services (B.2.4.7)**

2156

Name	Description	Algorithms Accessed	Role	Indicator

2157

2158 Notes

2159 • Algorithms Accessed are selected from existing table (Non-Approved Algorithms)
2160 entries

2161

2162

2163 **Mechanisms and Actions Required (B.2.7.2)**

2164

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

2165

2166 Notes

2167 • None

2168

2169

2170 **EFP/EFT Information (B.2.7.11)**

2171

	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			

2172

2173 Notes

2174 • EFP is required for modules with physical Security Level 4.

2175

2176

2177 **Hardness Testing Temperature Ranges (B.2.7.12)**

2178

	Hardness tested temperature measurement
Low Temperature	
High Temperature	

2179

2180 Notes
2181 • The module is hardness tested at the lowest and highest temperatures within the module's
2182 intended temperature range of operation
2183

2184
2185 **Storage Areas (B.2.9.1)**

2186

Name	Description	Type

2187
2188 Notes
2189 • Type – Persistent or Volatile
2190 • Name maps to a specific item in the block diagram
2191

2192
2193 **SSP Input-Output Methods (B.2.9.2)**

2194

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

2195
2196 Notes
2197 • Name – Unique, descriptive name
2198 • From/To
2199   o Clearly indicate one as inside and the other as outside the cryptographic boundary
2200   o Include any input/output devices
2201   o For internal references, provide a component/structure that is clearly identified in
2202   the block diagram and/or a storage area from the list
2203 • Format Type - Encrypted or Plaintext
2204 • Distribution Type – Manual, Automated, Wireless (Reference IG 9.5.A)
2205 • Entry Type – Direct, Electronic (Reference IG 9.5.A)
2206 • 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

2239   o   Indicate relationship to current SSP – "Derived From", "Wrapped By", "Wraps",
2240   "Paired With", etc.
2241
2242 **Entropy Sources (B.2.9.5)**

2243

Name	Type	Minimum bits	Details

2244

2245 Notes
2246   •   Type
2247   o   Physical or Non-Physical
2248   •   Minimum Bits - The minimum number of bits of entropy generated, requested, and/or
2249   believed to have been loaded
2250
2251
2252 **Pre-Operational Self-Tests (B.2.10.1)**

2253

Algorithm	OE	Test Properties	Type	Details

2254
2255 Notes
2256   •   Algorithm and OE from set of tested/allowed algorithms
2257   •   Test Properties – the key length, signature, etc. used for the test
2258   •   Type – KAT, PCT, etc.
2259   •   Details – any other information related to the test
2260   •   Any relevant information related to the different implementations should be included in
2261   the "Notes" section following the table.
2262
2263
2264 **Conditional Self-Tests (B.2.10.2)**

2265

Algorithm	OE	Test Properties	Type	Details	Condition

2266
2267 Notes
2268   •   Algorithm and OE from set of tested/allowed algorithms
2269   •   Test Properties – the key length, signature, etc. used for the test
2270   •   Type – KAT, PCT, etc.
2271   •   Details – any other information related to the test
2272   •   Condition – what condition triggers the test

2273   •   Any relevant information related to the different implementations should be included in
2274   the "Notes" section following the table.
2275
2276
2277 **Error States (B.2.10.4)**

2278

State Name	Description	Indicator

2279
2280 Notes
2281   •   No links to other tables
2282

2283 **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

2284