AUTOMATA LLC

Navigating CMVP Security Policy Requirements

The common security policy template introduced through NIST SP 800-140B Revision 1: how a policy is now assembled, why some active FIPS 140-3 validations retain earlier formats, and published policies from Apple, Microsoft and Red Hat compared.

Published November 15, 2026.

FIPS 140 | CMVP | CRYPTOGRAPHY

Abstract

A FIPS 140 validation certificate establishes that a cryptographic module was tested. The security policy published alongside it explains how that module must be installed, configured and used for the validation to apply. For years, each vendor organized that document in its own way, leaving implementers to learn a new layout for every module they deployed. This whitepaper examines the common security policy template introduced through NIST SP 800-140B Revision 1 and what it changes for the people who rely on these documents.

Organized around the questions implementers bring to a security policy, the paper traces the release and adoption of the revision, explains how a policy is now assembled, and compares published policies from Apple, Microsoft, and Red Hat across earlier and newer formats. It focuses on the most important security policy sections and explains why some active FIPS 140-3 validations retain earlier formats.

The objective is to help implementers, system owners and assessors navigate a standardized policy efficiently, recognize an earlier format when they encounter one, and identify where additional interpretation remains necessary to configure a module and verify approved operation.

1 Introduction and Scope

Purpose and Audience

For many organizations, FIPS validation begins and ends with the certificate. A product either appears on the Cryptographic Module Validation Program's list of validated modules or it does not. What can receive less attention is the security policy linked from that certificate. The certificate states that a module was validated. The policy states which versions and environments were tested, how the module enters its approved mode, and what an operator must do or avoid for that validation to hold.

This paper is intended for implementers, system owners and assessors who deploy or evaluate validated modules. Anyone who has opened a policy looking for a single configuration step and found it thirty pages later under a heading no other vendor uses will recognize the problem. The aim is to show where a standardized policy keeps that information and where it still does not.

Scope and Basis for Review

This paper covers NIST SP 800-140B Revision 1, referred to here as Br1, along with the Cryptographic Module Validation Program (CMVP) guidance and tooling that put it into practice. Automata reviewed the publication, the CMVP's supporting material and nine published security policies from Apple, Microsoft, and Red Hat, covering FIPS 140-2, early FIPS 140-3 and Br1 formats. [1], [2]

Those policies all describe Security Level 1 software or software-hybrid modules. The physical security and authentication sections that matter more for hardware modules at higher levels therefore receive less attention here. Laboratory submission mechanics, the underlying ISO/IEC test requirements and the cryptographic strength of any module are outside the scope of this paper. Certificates and policies also change, so the references identify the certificates and documents reviewed. Organizations should read the current policy for the exact module version they deploy.

2 Security Policies Before the Common Template

Before getting into the revision itself, it helps to look at what implementers were working with. Microsoft's FIPS 140-2 policy for the Windows Cryptographic Primitives Library is a useful example. It runs to fourteen numbered sections, including a Finite State Model and a Security Levels table near the end. The instructions for configuring Windows to use FIPS-approved algorithms sit in section 1.3 of the introduction, while the steps for verifying the Windows version and binary signatures are in an appendix. An operator had to know that layout to find either one. [3]

TABLE OF CONTENTS

1 INTRODUCTION 8

1.1 LIST OF CRYPTOGRAPHIC MODULE BINARY EXECUTABLES 9
1.2 VALIDATED PLATFORMS 9
1.3 CONFIGURE WINDOWS TO USE FIPS-APPROVED CRYPTOGRAPHIC ALGORITHMS 11

2 CRYPTOGRAPHIC MODULE SPECIFICATION 11

3 CRYPTOGRAPHIC MODULE PORTS AND INTERFACES 22

4 ROLES, SERVICES AND AUTHENTICATION 34

5 FINITE STATE MODEL 40

6 OPERATIONAL ENVIRONMENT 40

7 CRYPTOGRAPHIC KEY MANAGEMENT 43

8 SELF-TESTS 47

9 DESIGN ASSURANCE 49

10 MITIGATION OF OTHER ATTACKS 49

11 SECURITY LEVELS 50

12 ADDITIONAL DETAILS 50

13 APPENDIX A – HOW TO VERIFY WINDOWS VERSIONS AND DIGITAL SIGNATURES 51

14 APPENDIX B – REFERENCES 52

Figure 1. Contents of Microsoft's FIPS 140-2 policy for the Cryptographic Primitives Library, shown as selected excerpts from pages 4 to 7. Configuration guidance sits in section 1.3 and the verification steps in an appendix. Source: Microsoft, CMVP certificate #4825. [3]

FIPS 140-3 brought more order. The original SP 800-140B, published in March 2020, allowed the CMVP to specify the order of the security policy against ISO/IEC 19790 Annex B. [4] Apple's 2022 policy for corecrypto v11.1 follows the twelve sections that result. Below those twelve headings, though, the subsections were still the vendor's and laboratory's choice. [5]

Table of Contents

1. General 5

2. Cryptographic Module Specification 6

3. Cryptographic Module Interfaces 12

4. Roles, services, and authentication 13

5. Software/Firmware security 19

5.1. Integrity Techniques 19

5.2. On-Demand Integrity Test 19

6. Operational Environment 20

6.1. Applicability 20

7. Physical Security 21

8. Non-invasive Security 22

9. Sensitive Security Parameter Management 23

9.1. Random Number Generation 24

9.2. Key / SSP Generation 25

9.3. Keys/SSPs Establishment 25

9.4. Keys/SSPs Import/Export 25

9.5. Keys/SSPs Storage 25

9.6. Keys/SSPs Zeroization 25

10. Self-tests 26

10.1. Pre-operational Software Integrity Test 26

10.2. Conditional Self-Tests 26

10.2.1. Conditional Cryptographic Algorithm Self-Tests 26

10.2.2. Conditional Pairwise Consistency Test 27

10.3. Error Handling 27

11. Life-cycle assurance 28

11.1. Delivery and Operation 28

11.2. Crypto Officer Guidance 28

12. Mitigation of other attacks 29

Figure 2. Contents of Apple’s 2022 policy for corecrypto v11.1. The twelve top-level sections follow Annex B, while the subsections are Apple’s own. Source: Apple, CMVP certificate #4392. [5]

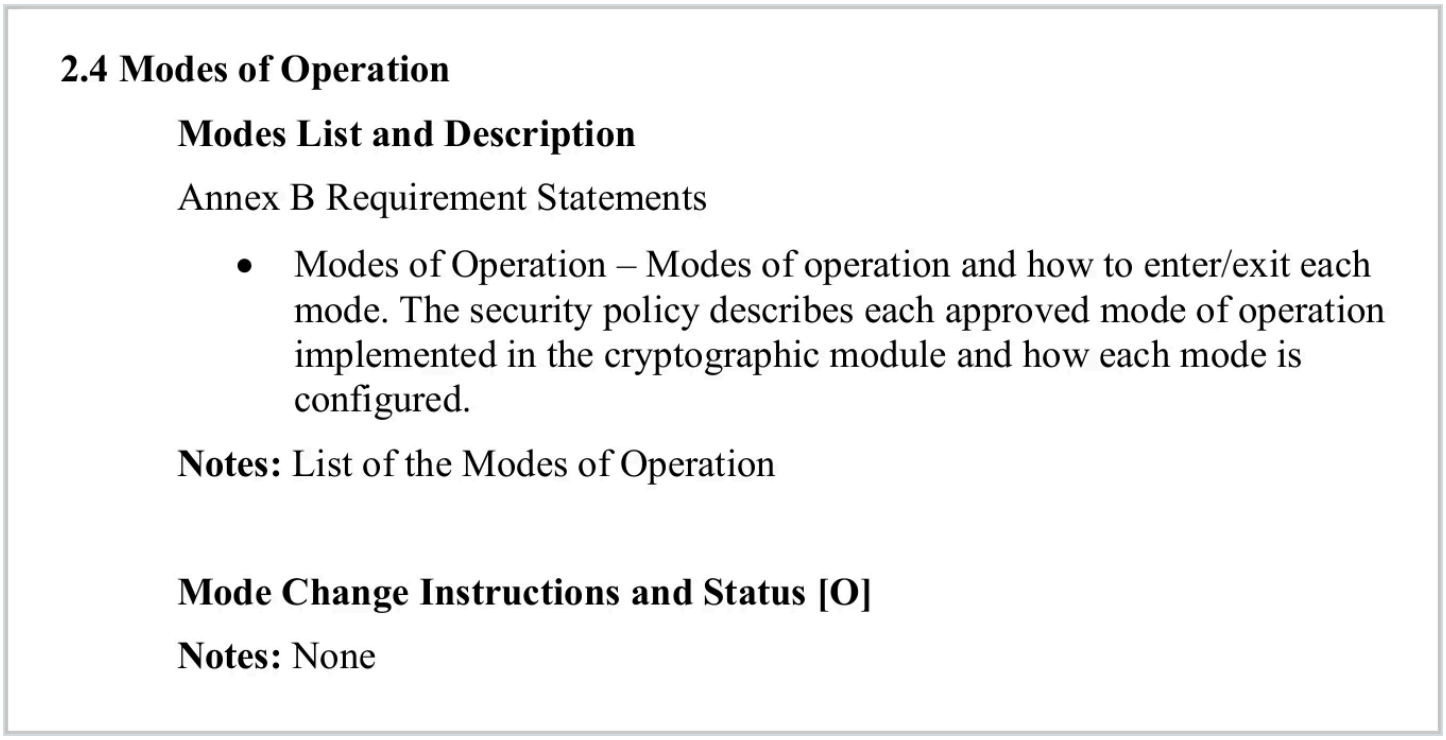
So the early FIPS 140-3 format addressed the top level and left the rest. Two policies could share the same twelve headings and still disagree on where to find the modes of operation or the installation steps. That is the gap the revision set out to close.

3 What SP 800-140B Revision 1 Changed

NIST published SP 800-140B Revision 1 on 17 November 2023 and withdrew the 2020 edition the same day. [1], [4] Its announcement identifies four significant changes. The revision defines a more detailed structure for the security policy, captures requirements defined outside the ISO/IEC documents, builds the policy as a combination of subsection information, and generates the approved algorithm table from the algorithm test selections. [6]

A Fixed Structure

The revision keeps the twelve Annex B sections and requires them in order, from General through Mitigation of Other Attacks. Sections that do not apply must be marked as such. [1] Beneath them it defines a common set of subsections. In every policy that follows the template, 2.4 is Modes of Operation, 4.3 is Approved Services and 11.1 is Installation, Initialization, and Startup Procedures.



2.4 Modes of Operation

Modes List and Description

Annex B Requirement Statements

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

Notes: List of the Modes of Operation

Mode Change Instructions and Status [O]

Notes: None

Figure 3. Section 2.4 as defined in SP 800-140B Revision 1. Each subsection lists its requirement statements and notes, and optional parts carry the [O] marker. Source: NIST. [1]

Some subsections carry an [O] marker, which the publication itself does not define. The CMVP's template completion instructions do. The number and text of each heading must be kept. Optional sections are deleted entirely when they do not apply, while required sections that do not apply stay in place with a statement saying so. [7] This distinction matters later, since a missing optional section is not an oversight. Table 1 lists the full structure, with the optional subsections in their own column.

Table 1. Sections and subsections of a Br1 security policy.

Section	Always present	Optional, marked [O]

Section	Always present	Optional, marked [O]
1 General	1.1 Overview. 1.2 Security Levels.	1.3 Additional Information.
2 Cryptographic Module Specification	2.1 Description. 2.2 Tested and Vendor Affirmed Module Version and Identification. 2.3 Excluded Components. 2.4 Modes of Operation. 2.5 Algorithms. 2.6 Security Function Implementations. 2.7 Algorithm Specific Information. 2.8 RBG and Entropy. 2.9 Key Generation. 2.10 Key Establishment. 2.11 Industry Protocols.	2.12 Additional Information.
3 Cryptographic Module Interfaces	3.1 Ports and Interfaces.	3.2 Trusted Channel Specification. 3.3 Control Interface Not Inhibited. 3.4 Additional Information.
4 Roles, Services, and Authentication	4.1 Authentication Methods. 4.2 Roles. 4.3 Approved Services. 4.4 Non-Approved Services. 4.5 External Software/Firmware Loaded.	4.6 Bypass Actions and Status. 4.7 Cryptographic Output Actions and Status. 4.8 Additional Information.
5 Software/Firmware Security	5.1 Integrity Techniques. 5.2 Initiate on Demand.	5.3 Open-Source Parameters. 5.4 Additional Information.
6 Operational Environment	6.1 Operational Environment Type and Requirements.	6.2 Configuration Settings and Restrictions. 6.3 Additional Information.
7 Physical Security	7.1 Mechanisms and Actions Required.	7.2 User Placed Tamper Seals. 7.3 Filler Panels. 7.4 Fault Induction Mitigation. 7.5 EFP/EFT Information. 7.6 Hardness Testing Temperature Ranges. 7.7 Additional Information.
8 Non-Invasive Security	None.	8.1 Mitigation Techniques. 8.2 Effectiveness. 8.3 Additional Information.
9 Sensitive Security Parameters Management	9.1 Storage Areas. 9.2 SSP Input-Output Methods. 9.3 SSP Zeroization Methods. 9.4 SSPs.	9.5 Transitions. 9.6 Additional Information.
10 Self-Tests	10.1 Pre-Operational Self-Tests. 10.2 Conditional Self-Tests. 10.3 Periodic Self-Test Information. 10.4 Error States.	10.5 Operator Initiation of Self-Tests. 10.6 Additional Information.

Section	Always present	Optional, marked [O]
11 Life-Cycle Assurance	11.1 Installation, Initialization, and Startup Procedures. 11.2 Administrator Guidance. 11.3 Non-Administrator Guidance.	11.4 Design and Rules. 11.5 Maintenance Requirements. 11.6 End of Life. 11.7 Additional Information.
12 Mitigation of Other Attacks	None.	12.1 Attack List. 12.2 Mitigation Effectiveness. 12.3 Guidance and Constraints. 12.4 Additional Information.

Sources: SP 800-140B Revision 1 and the CMVP's example security policy. Subsection numbers follow the example policy. [1], [8]

How the Policy Is Assembled

The less visible change is who produces the document. Previously, the entire policy was written by hand. [9] Under Br1, structured information is submitted as JSON in what the CMVP calls the Module Information Structure, or MIS. The vendor enters the remaining text and images into a Word template supplied by the CMVP, and the CMVP merges the two to produce the final policy. [2] The template and the MIS schema are published and versioned separately from the Special Publication, so they can change without a new revision of SP 800-140B. [2]

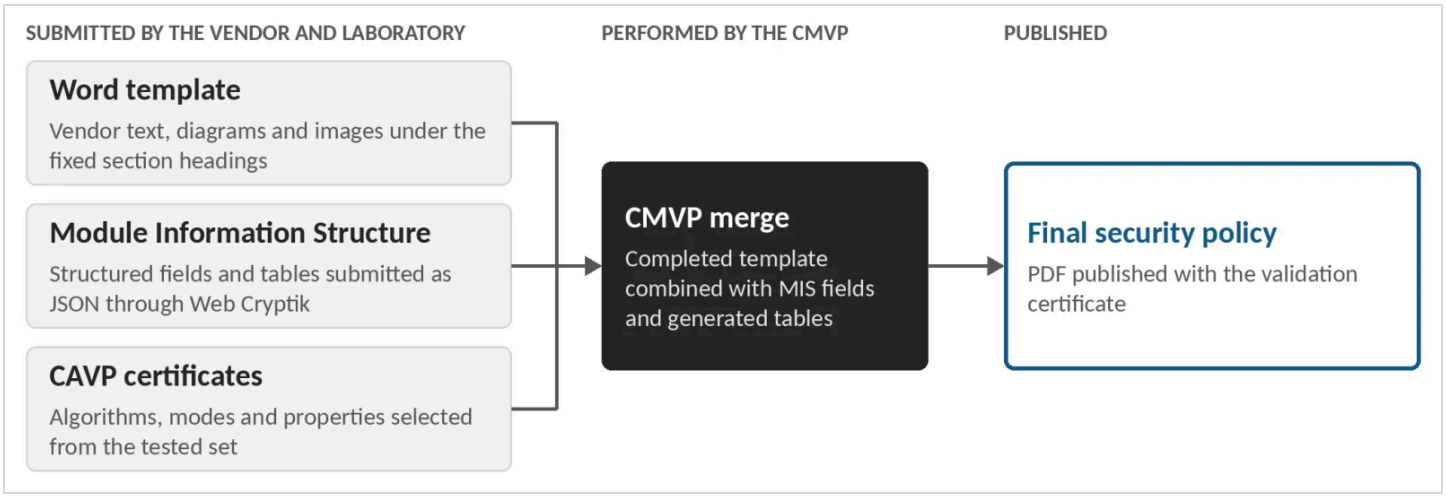


Figure 4. How a Br1 security policy is assembled. Vendors and laboratories can preview the merged result with the CMVP's builder tool, although that output is unofficial. Source: Automata, based on CMVP guidance. [2], [7]

Several tables are generated and no longer written. The approved algorithm table comes from the algorithms, modes and properties selected from the module's CAVP certificates, and the security level table is generated from information already entered. [1] For the reader, this means the tables in two Br1 policies share the same columns. The Approved Services table, for example, lists each service's name, description, indicator, inputs, outputs, security functions and SSP access. [8]

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
T16 Name	T16 Descrip	T16 Indicator	T16 Inputs	T16 Outputs	T10 Name	T15 Name - T24 Name: G,W,Z

Table 14: Approved Services

<Text>

4.4 Non-Approved Services

Name	Description	Algorithms	Role
T17 Name	T17 Descrip	T9 Algo	T17 Role

Table 15: Non-Approved Services

<Text>

Figure 5. Approved and Non-Approved Services tables in the CMVP's example security policy. The columns are generated and are the same in every Br1 policy. Source: NIST CMVP. [8]

4 Release and Adoption Timeline

With the changes covered, the discussion can turn to how they reached published certificates. The revision went through two public drafts and a pilot, then met a validation queue that already held a backlog of submissions prepared in the earlier format. [10], [11]

Table 2. SP 800-140B Revision 1 release and adoption milestones.

Date	Milestone
20 March 2020	SP 800-140B is published with the rest of the SP 800-140 series
22 September 2020	CMVP begins accepting FIPS 140-3 submissions
12 May 2022	Initial public draft of Revision 1 is released
17 October 2022	Second public draft is released
June 2023	CMVP begins a Br1 pilot with testing laboratories
17 November 2023	Revision 1 is published and SP 800-140B is withdrawn. The template completion instructions carry the same date

Date	Milestone
1 January 2024	Cutoff for interim validation. Only submissions received before this date are eligible
29 January 2024	Web Cryptik Br1 User's Guide version 1.0 is issued
6 June 2024	CMVP begins two-year interim validations
11 July 2024	First three certificates from the Br1 pilot are posted
1 October 2024	Window to elect interim validation closes
16 October 2025	Management Manual version 2.6 adds the Br1 Update to Interim scenario

Sources: NIST and CMVP publications, and atsec's account of the pilot, which dates its start by month only. [1], [4], [10], [7], [11], [12], [9], [13]

Why Earlier Formats Remain Active

At first glance, a withdrawn publication and a new template might suggest that every FIPS 140-3 policy now looks the same. It is not quite that simple. The publication sets no cutover date of its own, so adoption is enforced through the submission process. [1], [13] Automata's review found three reasons an active certificate can still carry an earlier format.

- Full validations completed before the revision keep their five-year sunset dates. Apple's corecrypto v11.1 was validated on 7 December 2022 and remains active until 6 December 2027 with its original policy. [5]
- Submissions received before 1 January 2024 could elect interim validation. These carry a two-year sunset date and an interim validation caveat, and the examples reviewed were published in the earlier format. [11], [14], [15]
- The Management Manual marks only full submissions, updates and the Br1 Update to Interim scenario as needing to meet all latest guidance. Other revalidation scenarios are held to the requirements that applied at the original validation. [13] Automata reads this to mean an earlier policy format can persist through those scenarios, although the manual does not say so directly.

The interim path also explains how a module moves from one format to the other. A follow-up submission in the Br1 format must reach the CMVP before the two-year sunset date. On completion, the CMVP issues a new Br1-compliant certificate without the interim caveat. The sunset date becomes five years from the interim validation, and the interim certificate moves to the Historical list with a pointer to its replacement. [13], [11]

5 Comparing Published Policies

That process has now produced something useful for anyone studying the template, which is the same module published in both formats. The table below lists two such pairs, along with a third that crosses from FIPS 140-2.

Table 3. Published policies in earlier and Br1 formats.

Module	Earlier format	Br1 format
Apple corecrypto v13.0 [Intel, Kernel, Software, SL1]	Certificate #4919. Interim validation on 17 December 2024. 33 pages. Now Historical.	Certificate #5347. Validated 19 June 2026. 54 pages. Sunset 16 December 2029.
Red Hat Enterprise Linux 9 OpenSSL FIPS Provider	Certificate #4857. Interim validation on 29 October 2024. 48 pages. Now Historical.	Certificate #5573. Validated 9 November 2026. 90 pages. Sunset 28 October 2029.
Microsoft Cryptographic Primitives Library	Certificate #4825 under FIPS 140-2. 53 pages.	Certificate #5410 under FIPS 140-3. Validated 31 August 2026. 101 pages.

Sources: CMVP certificate pages and the security policies linked from them. [14], [16], [15], [17], [3], [18]

The Apple and Red Hat pairs are consistent with the interim path described above. In both cases the CMVP lists the interim certificate as Historical and replaced, and the replacement's sunset date falls five years after the interim validation. [14], [16], [15], [17] The Microsoft pair is a different kind of comparison, since it crosses from FIPS 140-2 to FIPS 140-3 and is not a conversion of a single validation. It is included because it shows the largest change in layout.

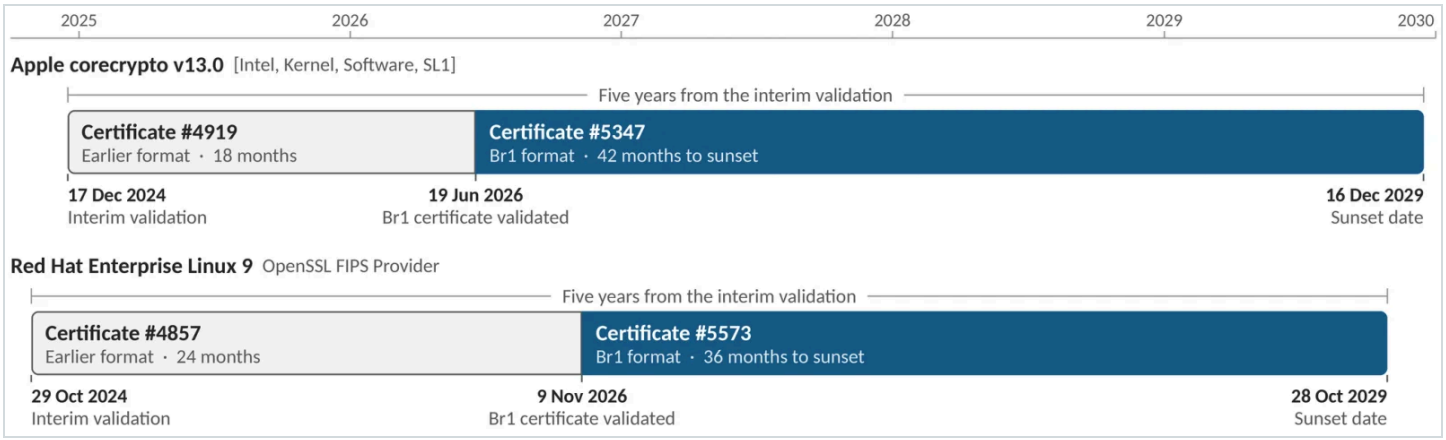


Figure 6. Validation timelines for the Apple and Red Hat modules. Each Br1 certificate keeps the sunset date set five years after the interim validation. Source: Automata, based on the CMVP entries. [14], [16], [15], [17]

The first thing these pairs show is that standardized does not mean shorter. Each Br1 policy in Table 3 is longer than its predecessor, and a good part of that growth appears to come from the generated tables. The contents pages show the change most directly. The next figure maps the contents of the same Apple module's policy before and after conversion. The twelve top-level sections are unchanged, while the subsection headings grow from 16 to 36 and four topics change section.



Figure 7. Contents of Apple's corecrypto v13.0 policy before and after conversion. Lines link each earlier subsection to its Br1 location. Source: Automata, based on the policies for certificates #4919 and #5347. [14], [16]

The second is that content moved to a common home. In Red Hat's earlier policy, the steps for placing the system in FIPS mode sat under a Crypto Officer guidance heading in section 11.2, alongside the conditions for AES-GCM, AES-XTS and PBKDF2. In the Br1 policy, the FIPS mode steps are in section 11.1 and the algorithm conditions are in section 2.7, under the same subsection titles that Apple and Microsoft now use. [15], [17], [16], [18] This even shows up on the certificate. Red Hat's interim certificate directed operators to Section 11.2 of its policy for installation and configuration. Microsoft's Br1 certificate points to Section 11.1, which is where the template places that content for every module. [15], [18]

11.2 Crypto Officer guidance

Before the RPM package is installed, the RHEL 9 system must operate in the approved mode. This can be achieved by:

- Starting the installation in the approved mode. Add the fips=1 option to the kernel command line during the system installation. During the software selection stage, do not install any third-party software. More information can be found at the vendor documentation.
- Switching the system into the approved mode after the installation. Execute the fips-mode-setup –enable command. Restart the system. More information can be found at the vendor documentation.

In both cases, the Crypto Officer must verify the RHEL 9 system operates in the approved mode by executing the fips-mode-setup --check command, which should output “FIPS mode is enabled.”
After installation of the RPM package, the Crypto Officer must execute the openssl list -providers command. The Crypto Officer must ensure that the fips provider is listed in the output as follows:

```
 fips
   name: Red Hat Enterprise Linux 9 - OpenSSL FIPS Provider
   version: 3.0.7-395c1a240fbfffd8
   status: active
```

The cryptographic boundary consists only of the FIPS provider as listed. If any other OpenSSL or third-party provider is invoked, the user is not interacting with the module specified in this Security Policy.
The crypto policies package provided as part of the RHEL OS should be set with no restrictions, any options selected will reduce the available services.

Figure 8. Crypto Officer guidance in Red Hat’s earlier policy, where the FIPS mode steps appear in section 11.2. Source: Red Hat, CMVP certificate #4857. [15]

11.1 Installation, Initialization, and Startup Procedures

The module is distributed as a part of the Red Hat Enterprise Linux 9 (RHEL 9) by means of one the following RPM packages:

- openssl-fips-provider-3.0.7-11.el9_0
- openssl-fips-provider-3.0.7-11.el9_8

Before the openssl-fips-provider-3.0.7-11.el9_0 RPM package or the openssl-fips-provider-3.0.7-11.el9_8 RPM package is installed, the RHEL 9 system must operate in the approved mode. This can be achieved by:

- Starting the installation in the approved mode. Add the fips=1 option to the kernel command line during the system installation. During the software selection stage, do not install any third-party software.
- Switching the system into the approved mode after the installation. Execute the fips-mode-setup –enable command. Restart the system. More information can be found from the vendor documentation.

In both cases, the Crypto Officer must verify the RHEL 9 system operates in the approved mode by executing the fips-mode-setup --check command, which should output “FIPS mode is enabled.”

Figure 9. The same steps in Red Hat’s Br1 policy, now under section 11.1. Source: Red Hat, CMVP certificate #5573. [17]

6 Navigating a Standardized Policy

With the format established, this section turns to the practical question of where to look. Most implementers come to a security policy with a short list of questions. Is the deployed version the one that was tested? What needs to be configured? Which algorithms can be used, and how does an application know that a given operation was approved? The template gives each of these a predictable home.

Table 4. Where a Br1 security policy answers common implementer questions.

Question	Section	What to look for
Which versions and environments were tested?	2.2 Tested and Vendor Affirmed Module Version and Identification	Exact module versions, tested operating environments and any vendor-affirmed environments
How does the module enter approved mode?	2.4 Modes of Operation	The modes table and the status indicator for each mode
Which algorithms are approved, allowed or not allowed?	2.5 Algorithms and 2.6 Security Function Implementations	Separate tables for approved, vendor-affirmed, allowed and not allowed algorithms
What must the calling application do?	2.7 Algorithm Specific Information	Conditions attached to specific algorithms, such as AES-GCM, AES-XTS and PBKDF2
How is an approved operation confirmed?	4.3 Approved Services and 4.4 Non-Approved Services	The Indicator column for each approved service
Are there restrictions on the environment?	6.2 Configuration Settings and Restrictions	Settings and restrictions on the operating environment. Optional, so it may be absent
How is the module installed and verified?	11.1 through 11.3	Installation, initialization and startup procedures, then administrator and non-administrator guidance
What happens on failure or at end of life?	9.3 SSP Zeroization Methods, 10.4 Error States and End of Life	Zeroization methods, error indicators, recovery and sanitization steps

Sources: SP 800-140B Revision 1 and the CMVP’s example security policy. [1], [8]

One caution applies to these section numbers, because numbering below an optional heading can drift. The publication itself numbers two different subsections 11.4. The CMVP’s example and Red Hat’s policy place End of Life at 11.6, Apple’s policy for corecrypto 18.3 has it at 11.5, and Apple’s policy for v13.0 on Apple silicon goes from 11.4 to 11.6. [1], [8], [17], [19], [20] For optional subsections, it is safer to navigate by title than by number.

Start With the Certificate

The certificate page is the place to begin, not the policy. Its caveat states the conditions attached to the validation and, where installation or configuration matters, names the policy section that holds them. Microsoft's certificate for the Cryptographic Primitives Library points to Section 11.1 and names the other Windows module certificates it must operate alongside. [18] That is a reminder that a product may depend on several validated modules, each with its own policy.

> **Caveat on CMVP certificate #5410**
> When operated in approved mode. When installed, initialized and configured as specified in **Section 11.1 of the Security Policy**. When operated in approved mode with module Kernel Mode Cryptographic Primitives Library validated to FIPS 140-3 under **Cert. #5408** operating in approved mode and Code Integrity validated to FIPS 140-3 under **Cert. #5406** operating in approved mode or Secure Kernel Code Integrity validated to FIPS 140-3 under **Cert. #5407** operating in approved mode. No assurance of minimum security of SSPs (e.g., keys, bit strings) that are externally loaded, or of SSPs established with externally loaded SSPs. No assurance of FIPS 140-3 requirements met for the components of the RBG construct that are external to the module boundary (e.g., DRBG, ESV) except for SP 800-90C compliance and security strength of the provided random bits

Source: CMVP entry for certificate #5410. Emphasis added. [18]

Module Identity and Approved Mode

Section 2.2 settles whether the deployed version is the validated one. Microsoft's policy lists specific Windows 11 and Windows Server 2022 builds, so a version check means comparing build numbers and not just product names. [18]

Section 2.4 is where many readers expect to find a switch, and often there is not one. In the Br1 policies reviewed, approved mode is implicit. Apple's module is in approved mode by default and leaves it only when a non-approved service is called. Microsoft describes approved mode as normal operation with approved algorithms. Red Hat's module enters approved or non-approved mode automatically according to the service requested. [19], [18], [17] The mode follows what the application calls. It is not a setting an administrator applies once.

2.4 Modes of Operation

Modes List and Description:

Table Name	Description	Type	Status Indicator
T5 Name	T5 Descrip	Approved	T5 Status

Table 3: Modes List and Description

Figure 10. Modes List and Description table in the CMVP's example security policy. The Status Indicator column states how each mode is identified. Source: NIST CMVP. [8]

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved mode	Automatically entered whenever an approved service is requested	Approved	Equivalent to the indicator of the requested service
Non-approved mode	Automatically entered whenever a non-approved service is requested	Non-Approved	Equivalent to the indicator of the requested service

Table 5: Modes List and Description

After passing all pre-operational self-tests and cryptographic algorithm self-tests executed on start-up, the module automatically transitions to the approved mode. No operator intervention is required to reach this point. The module operates in the approved mode of operation by default and can only transition into the non-approved mode by calling one of the non-approved services listed in the Non-Approved Services table of the Security Policy.

In the operational state, the module accepts service requests from calling applications through its logical interfaces. At any point in the operational state, a calling application can end its process, causing the module to end its operation.

Mode Change Instructions and Status:

The module automatically switches between the approved and non-approved modes depending on the services requested by the operator. The status indicator of the mode of operation is equivalent to the indicator of the service that was requested.

Figure 11. Modes List and Description table from section 2.4 of Red Hat's Br1 policy. Source: Red Hat, CMVP certificate #5573. [17]

Algorithms and Services

That makes sections 2.5 through 2.7 and 4.3 more important than they might first appear. The algorithm tables state what is approved, and section 2.7 adds the conditions that come with specific algorithms. In the policies reviewed, these included how AES-GCM IVs are constructed, the restriction of AES-XTS to storage, the parameters required for PBKDF2 and the RSA key sizes limited to legacy verification. [19], [18], [17] These are obligations on the calling application. Apple's policy makes the point directly in section 11.4, where the Crypto Officer is told to follow the requirements in section 2.7. [19] The revision gives section 2.7 no requirement statements of its own, so its depth depends on the vendor and laboratory. [1]

The Indicator column in the Approved Services table is how an application confirms that a given operation was approved. The form varies by vendor. Apple documents API functions whose return value reports whether an algorithm is approved. Red Hat documents named indicator values tied to its API calls, along with a function that reports whether an operation is approved. [19], [17]

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
HKDF Key derivation	Perform key derivation	EVP_KDF_REDHAT_FIPS_INDICATOR_APPROVED	Shared secret	HKDF Derived Key	Key derivation with HKDF	Crypto Officer - Shared secret: W,E - HKDF Derived Key: G,R
Key derivation with TLS 1.3 KDF	Perform key derivation	EVP_KDF_REDHAT_FIPS_INDICATOR_APPROVED	Shared secret	TLS 1.3 Derived Key	Key derivation with TLS 1.3 KDF	Crypto Officer - Shared secret: W,E - TLS 1.3 KDF Derived key: G,R

Figure 12. Approved Services table from section 4.3 of Red Hat's Br1 policy, including the Indicator column. Source: Red Hat, CMVP certificate #5573. [17]

Configuration and Operator Guidance

Section 6.2 and sections 11.1 through 11.3 hold what most people mean by configuration. Red Hat's policy is the clearest example in this review. Section 6.2 rules out debugging and tracing tools such as ptrace, gdb and strace in the operational environment. Section 11.1 gives two ways to place the system in FIPS mode, either the fips=1 kernel option during installation or the fips-mode-setup command afterward, followed by the command that verifies the result. Section 11.2 then tells the administrator how to confirm that the FIPS provider is the one in use. [17]

Microsoft's sections 11.1 and 11.2 cover a different kind of task. They describe how Windows is delivered and updated, then give the steps for verifying the installed Windows version and the module binary's version and digital signature. [18] Both are answers to the same heading, and they are quite different answers.

7 Where Interpretation Remains

A common layout tells the reader where to look. It does not guarantee that what they need is there. Automata's review found one area where the reader still has work to do.

Configuration Outside the Policy

Microsoft's FIPS 140-2 policy told operators to enable the Windows FIPS security policy setting, or its registry value, in section 1.3. A full-text search of the FIPS 140-3 policy for the same library finds no mention of that setting, the registry value or an MDM policy, and section 2.4 describes approved mode as implicit. [3], [18] The layout is now standard, but what an administrator should configure at the operating system level is no longer answered in the same place. Organizations should check current vendor guidance and not assume that the earlier instruction either carried over or was retired.

1.3 Configure Windows to use FIPS-Approved Cryptographic Algorithms

There are two methods to enable FIPS-Approved mode for the Cryptogrpahic Primitives Library.

The first is to use FIPS Local/Group Security Policy setting or a Mobile Device Management (MDM) to enable FIPS-Approved mode for the Cryptographic Primitives Library. The Windows operating system provides a group (or local) security policy setting, "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing".

The second method to enable FIPS-Approved mode for the Cryptographic Primitives Library is to set the following registry key to 1: HKLM\System\CurrentControlSet\Control\Lsa\FIPSAlgorithmPolicy\STE. When this registry key exists and is set to 1, the selftests in Cryptogaphic Primitives Library will run in compliance with FIPS 140-2 Implementation Guidance section 9.11 and the module will be in FIPS Approved mode.

In addition to these methods, Consult the MDM documentation for information on how to enable FIPS-Approved mode. The Policy CSP - Cryptography includes the setting **AllowFipsAlgorithmPolicy**.

Changes to either Approved mode security policy setting do not take effect until the computer has been rebooted.

Figure 13. Section 1.3 of Microsoft's FIPS 140-2 policy, which describes how to configure Windows to use FIPS-approved algorithms. Source: Microsoft, CMVP certificate #4825. [3]

Guidance can also sit outside the policy by design. The requirement behind sections 11.2 and 11.3 allows administrator guidance to be a separate document. [1] Apple's section 11.2 refers administrators to two of its own platform guides for verifying module integrity. [19] The policy then becomes a pointer, and the reader needs the referenced document as well.

8 Conclusion and Recommendations

SP 800-140B Revision 1 delivers what it promises to the reader. Policies built on the template share one order, one set of subsection headings and one set of table layouts, and a reader who learns them once can apply that knowledge to the next module. What the template cannot do is decide how much a vendor writes under each heading, or bring guidance back into the policy once a vendor has placed it elsewhere.

Key Findings

The common structure is visible in published policies. The same module published before and after conversion shows matching subsection titles and generated tables in place of each vendor's own arrangement.

Adoption follows CMVP process and not a date in the publication. Earlier formats remain active through validations completed before 2024 and through interim validations, and conversions were still reaching the validated modules list in November 2026.

Approved operation is increasingly a question asked per service. In the policies reviewed, approved mode was implicit and confirmed through service indicators, which shifts attention from a one-time setting to what applications call.

Recommendation

Automata recommends starting with the certificate caveat, then confirming the module version and tested environment in section 2.2 before reading further. A policy for a different version or platform does not describe the deployed module.

Organizations should then read sections 2.4, 2.7, 6.2 and 11.1 through 11.3 together, and treat the conditions in section 2.7 as requirements on their own applications. Where the policy refers to external guidance, that guidance should be obtained and kept alongside it.

Finally, the policy should be treated as the starting point for verification and not as proof of it. Organizations should confirm the installed version, run the documented verification steps and record the result against the exact certificate their system depends on. Where a policy is silent on a configuration question, the answer should come from the vendor and not from an assumption.

Toward a Second Revision

Revision 1 is a good start, and it settled where information goes. Automata's review points to three things a second revision should add, so that what sits under each heading is as dependable as the layout.

The configuration an operator needs should be in the policy. Where approved operation depends on a system setting, the policy should state it, and where none is needed it should say so. Where guidance sits in a separate document, the policy should identify that document by title and version.

Every subsection should carry requirement statements. Section 2.7 Algorithm Specific Information has a heading but none of its own, which leaves the conditions an application must meet to the judgment of each vendor and laboratory. [1]

Section numbers should be stable. The publication should define the [O] marker, correct the two subsections numbered 11.4, and keep numbering fixed when an optional section is omitted, so that a certificate caveat or a procedure can cite a section number safely. [1]

Ultimately, standardizing the sections was a strong start. The next step for NIST and the CMVP is to standardize the content by requiring specific information from vendors in the sections they write themselves, so that implementers can read every policy the same way.

References

Numbered references support the main discussion. Citation numbers link to the entries below. Source titles link to the original publications.

[1] Hawes, David, Alexander Calis and Roy Crombie. *Cryptographic Module Validation Program (CMVP) Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B*. NIST Special Publication 800-140B Revision 1. November 2023. See Security Requirements and the document history on the publication page.

[2] NIST CMVP. *SP 800-140B: CMVP Security Policy Requirements*. SP 800-140 Series Supplemental Information. See Module Information Structure, Security Policy and Process Support Applications.

[3] Microsoft. *Cryptographic Primitives Library Security Policy Document*. FIPS 140-2. CMVP certificate #4825. Version 1.1, 23 August 2024.

[4] Schaffer, Kim. *CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B*. NIST Special Publication 800-140B. March 2020. Withdrawn 17 November 2023.

[5] NIST CMVP. *Certificate #4392: Apple corecrypto Module v11.1 [Apple silicon, Kernel, Software]*. FIPS 140-3. Validated 7 December 2022. Security policy version 1.3, November 2022.

[6] NIST. *NIST Publishes SP 800-140Br1 on CMVP Security Policy Requirements*. Computer Security Resource Center. 17 November 2023.

[7] NIST CMVP. *SP800-140Br1 Security Policy Template Completion Instructions*. 17 November 2023.

[8] NIST CMVP. *Example Finalized Security Policy*. Document 99-0280. Linked from the SP 800-140B supplemental information page.

[9] atsec information security. *First SP800-140Br1 Compliant FIPS 140-3 Certificates*. 12 July 2024.

[10] NIST CMVP. *Cryptographic Module Validation Program*. See Status of CMVP validation effort.

[11] NIST CMVP. *Programmatic Transitions*. See Program Related Transitions for the interim validation process.

[12] NIST CMVP. *Web-Cryptik Br1 User's Guide*. Version 1.0.0, 29 January 2024.

[13] NIST and the Canadian Centre for Cyber Security. *FIPS 140-3 Cryptographic Module Validation Program Management Manual*. Version 2.7, 9 April 2026. See sections 7.1.2.1, 7.1.2.2 and 7.1.14.

[14] NIST CMVP. *Certificate #4919: Apple corecrypto Module v13.0 [Intel, Kernel, Software, SL1]*. FIPS 140-3. Interim validation, 17 December 2024. Historical, replaced by certificate #5347. Security policy version 2.0, December 2024.

[15] NIST CMVP. *Certificate #4857: Red Hat Enterprise Linux 9 - OpenSSL FIPS Provider*. FIPS 140-3. Interim validation, 29 October 2024. Historical, replaced by certificate #5573. Security policy version 1.5, 8 July 2025.

[16] NIST CMVP. *Certificate #5347: Apple corecrypto Module v13.0 [Intel, Kernel, Software, SL1]*. FIPS 140-3. Validated 19 June 2026. Security policy version 1.0, 21 May 2026.

[17] NIST CMVP. *Certificate #5573: Red Hat Enterprise Linux 9 - OpenSSL FIPS Provider*. FIPS 140-3. Validated 9 November 2026. Security policy version 1.1, 9 November 2026.

[18] NIST CMVP. *Certificate #5410: Cryptographic Primitives Library*. Microsoft Corporation. FIPS 140-3. Validated 31 August 2026. Security policy version 1.0, 4 May 2026.

[19] Apple. *Apple corecrypto Module 18.3 [Apple silicon, User, Software, SL1] FIPS 140-3 Non-Proprietary Security Policy*. CMVP certificate #5184.

[20] NIST CMVP. *Certificate #5065: Apple corecrypto Module v13.0 [Apple silicon, User, Software, SL1]*. FIPS 140-3. Validated 22 September 2025.