Introduction to FIPS 140-2 and FIPS 140-3

Federal agencies and cloud service providers must run any encryption that protects federal information in a module validated under NIST's Cryptographic Module Validation Program (CMVP). A strong algorithm such as AES or SHA-256 is not enough on its own.

Published September 15, 2025.

FIPS 140 | CRYPTOGRAPHY | CMVP | FEDRAMP | CMMC

NOTE

If you are not familiar with the distinction between cryptographic modules and cryptographic algorithms, we recommend reading our short primer on Cryptographic Modules vs Cryptographic Algorithms first. It clarifies the terminology and scope used throughout this whitepaper.

Introduction

Federal agencies and cloud service providers in the federal systems space are required to use FIPS-validated cryptography to protect sensitive data. This mandate is codified through federal laws, regulations, and frameworks for protecting data at rest and in transit. In practice, this means that any encryption employed to secure federal information must be performed by cryptographic modules that have been tested and validated under NIST's Cryptographic Module Validation Program (CMVP). Simply using strong algorithms like AES or SHA-256 is not sufficient as the implementation of the underlying cryptographic module which provides those algorithms must be formally validated.

This whitepaper provides an overview of FIPS 140-2 and 140-3 standards, the concept of FIPS-validated cryptography, the Cryptographic Module Validation Program (CMVP), and Security Policies.

The target audience includes compliance teams and engineers aiming to bring commercial offerings into FedRAMP, FISMA, DISA CC SRG, or CMMC compliance. The focus of this whitepaper is on industry standards and best practices relevant to achieving FIPS 140-3 validated cryptography in real-world systems rather than on any specific product or tool that may be referenced.

Who requires FIPS 140-3 Validation and Why does it Matter?

Federal Information Processing Standards-validated cryptography is a term that might or might not be immediately familiar to those reading this whitepaper. For the readers who have worked in federal systems, maintained authorizations for systems which have achieved authorizations/certifications such as FedRAMP, GovRAMP, or CMMC

L2, they will certainly be familiar with this terminology. On the other hand, to readers who are new to federal systems and the associated compliance frameworks, FIPS-validated cryptography is a term which was introduced as a requirement which they must meet.

Whether a seasoned veteran or fresh to the industry, many who work to implement FIPS validated cryptography must struggle to read through dozens of NIST Special Publications, assessor guidance, and articles from their peers. The first question everyone who has faced this struggle asks is, "What is the authoritative source that says FIPS validated cryptography is required?"

The following table answers that question.

FIPS-Validated Cryptography Mandates

Framework / Industry	Requirement	Authoritative Source
All U.S. Federal agencies (FISMA scope)	If an agency specifies that information must be cryptographically protected, the cryptography **must be FIPS 140-2/140-3 validated** (non-validated cryptography is treated as *no protection*).	NIST CMVP overview page ("Use of Cryptographic Modules by Federal Agencies and Departments").
OMB Circular A-130 (implements FISMA)	Requires agencies to use only cryptographic modules that are validated under **FIPS 140** when protecting Federal information systems covered by FISMA.	OMB Circular A-130, Appendix I & III.
FedRAMP - Low, Moderate, High	FedRAMP policy sets **normative** requirements for cryptographic module **selection and use**, aligning with FIPS 140 validation for protections in scope.	FedRAMP "Policy for Cryptographic Module Selection and Use".
CUI environments via NIST SP 800-171 (e.g., DFARS 252.204-7012 contractors)	**3.13.11:** "Employ **FIPS-validated cryptography** when used to protect the confidentiality of **CUI**."	NIST SP 800-171 Rev. 2 control text (and the Rev. 3 mapping).
CMMC 2.0 (Level 2)	**SC.L2-3.13.11** mirrors NIST 800-171: use **FIPS-validated** cryptography when protecting **CUI**.	DIB SCC CyberAssist explainer of SC.L2-3.13.11.
FBI CJIS Security Policy (criminal justice information)	When CJI is transmitted outside a physically secure location, encryption **must use a FIPS 140-validated module** (≥128-bit symmetric key); applies to LMR and data in transit/at rest per current guidance.	CJIS Security Policy docs & state CJIS guidance summarizing the FIPS mandate.

Readers responsible for systems subject to these frameworks often ask why they must use FIPS-validated cryptography rather than simply rely on a strong algorithm such as AES-256.

FIPS 140-3 validation matters because it verifies much more than the presence of a strong algorithm. It provides assurance that the entire cryptographic module is designed, implemented, and operated correctly. Modules are tested by accredited laboratories and certified through the NIST CMVP, which produces auditable evidence that satisfies FedRAMP, FISMA, and many DoW and state procurement requirements. Using a non validated library that

implements a strong algorithm still leaves risk from implementation bugs, insecure modes, weak entropy, mishandled keys, and configuration drift. It can also block an Authorization to Operate. A validated module simplifies assessments and reduces compliance and liability risk.

NIST FIPS 140-2 and FIPS 140-3: What Are They?

FIPS 140-2 and FIPS 140-3 are successive versions of the Federal Information Processing Standards (FIPS) that specifies security requirements for cryptographic modules. FIPS 140 (current version 140-3) defines the minimum security requirements that a cryptographic module must meet if it is to be used for protecting sensitive information in U.S. government systems. The standard covers 11 different areas of cryptographic module design/implementation, with each area rated from Security Level 1 (lowest) to 4 (highest) based on the robustness of the controls.

FIPS PUB 140-2

CHANGE NOTICES (12-03-2002)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supercedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

Issued May 25, 2001



U.S. Department of Commerce
Donald L. Evans, Secretary

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Arden L. Bement, Jr., Director



FIPS PUB 140-3

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS PUB 140-2)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: INFORMATION SECURITY SUBCATEGORY: CRYPTOGRAPHY

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

This publication is available free of charge from:
https://doi.org/10.6028/NIST.FIPS.140-3

March 22, 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary for Standards and Technology

FIPS 140-2 was published in 2001 and remained the standard in use for roughly two decades. FIPS 140-3 is the newer standard released by NIST in 2019. The CMVP has accepted no FIPS 140-2 submissions for new certificates since April 1, 2022, and from September 22, 2021 it accepted them only in limited cases. Existing FIPS 140-2 module certificates remained valid for up to five years after validation and could still be used by federal agencies, but that transition period ended on September 21, 2026, the final date the Cryptographic Module Validation Program (CMVP) set for any FIPS 140-2 validations:

> FIPS 140-2 active modules can be used until [**September 21, 2026**] for new systems. After this date, FIPS 140-2 validation certificates will be moved to the Historical List.
> *National Institute of Standards and Technology Cryptographic Module Validation Program*

After that date the CMVP places FIPS 140-2 validated modules on the Historical List: agencies may keep using them in existing systems, on their own risk determination, but should not include them in new systems. FIPS 140-3 does not radically change the cryptographic requirements from 140-2, but it updates the testing and documentation processes and adopts the ISO framework.

For readers looking to implement FIPS-validated cryptography in a new system, the phase out of FIPS 140-2 cryptographic modules leaves one strong implication: Use FIPS 140-3 validated cryptographic modules whenever possible, and avoid FIPS 140-2 validated cryptographic modules at all costs.

For those maintaining current systems which might use many FIPS 140-2 validated cryptographic modules, this same information comes with the strong recommendation to review the full list of all cryptographic modules in use, their current FIPS 140 version, and the sunset date for each module. If a plan to transition modules has not been implemented, immediate action should be taken to:

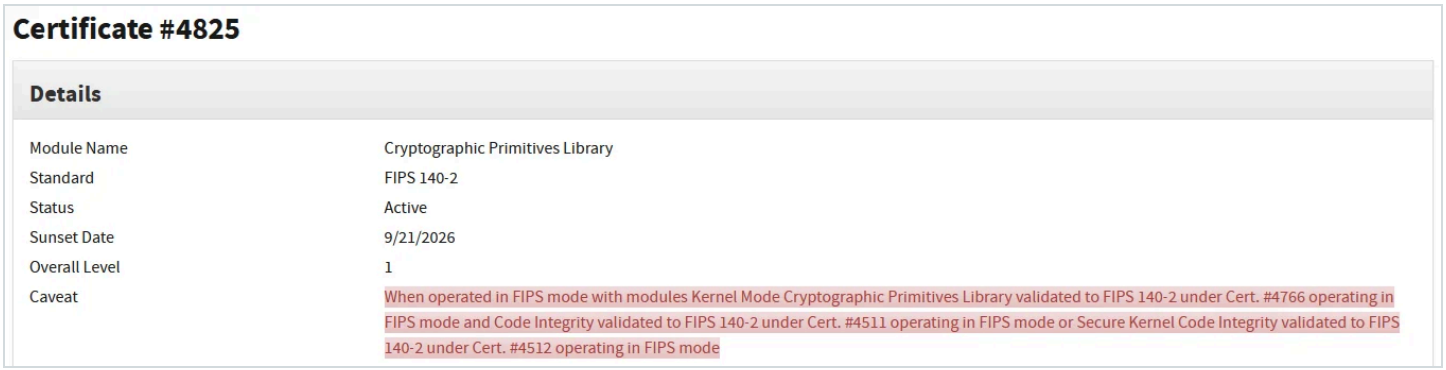
1. Identify if the current vendor providing the cryptographic module has a newer certification for the FIPS 140-3 validated version of the cryptographic module.
2. If no currently validated version for FIPS 140-3 is available, review the CMVP In Process list to determine if they are currently working on achieving a FIPS 140-3 certification on the cryptographic module and where in the process that module currently is.
3. If neither a current certification for FIPS 140-3 nor an In Process certification is present, begin identifying next steps to migrate to an alternative FIPS 140-3 validated cryptographic module, following your change management and significant change processes, and migrating to the new module before your current module's sunset date.
4. If you are unable to migrate cryptographic modules prior to the sunset date, begin tracking on your Plan of Action and Milestones and identifying any mitigating factors or justifications to provide to your federal agency for any potential risk adjustments or operational requirements to extend the remediation window. This step is entirely dependent on your federal agency's risk tolerance and the scope of impact of the cryptographic module in question to your system's security and privacy posture.

What is FIPS-Validated Cryptography?

FIPS-validated cryptography refers to cryptographic operations performed by a module (software library, hardware device, or firmware) that has undergone independent lab testing and government validation per the FIPS 140 standards. It is not enough to simply use FIPS-approved algorithms (like AES, RSA, SHA) in principle; the implementation of those algorithms must be validated by the CMVP. FIPS-validated cryptography means using a cryptographic module that appears on NIST's validated modules list and operating it in an Approved Mode in accordance with the security policy.

To achieve validation, a vendor submits their cryptographic module to an accredited laboratory for testing against all applicable FIPS 140 criteria. Upon passing tests and review, NIST issues a certificate for that module. The module is then identified by a certificate number on the NIST CMVP validated modules list, along with a published Security

Policy document describing its proper usage.



Certificate #4825

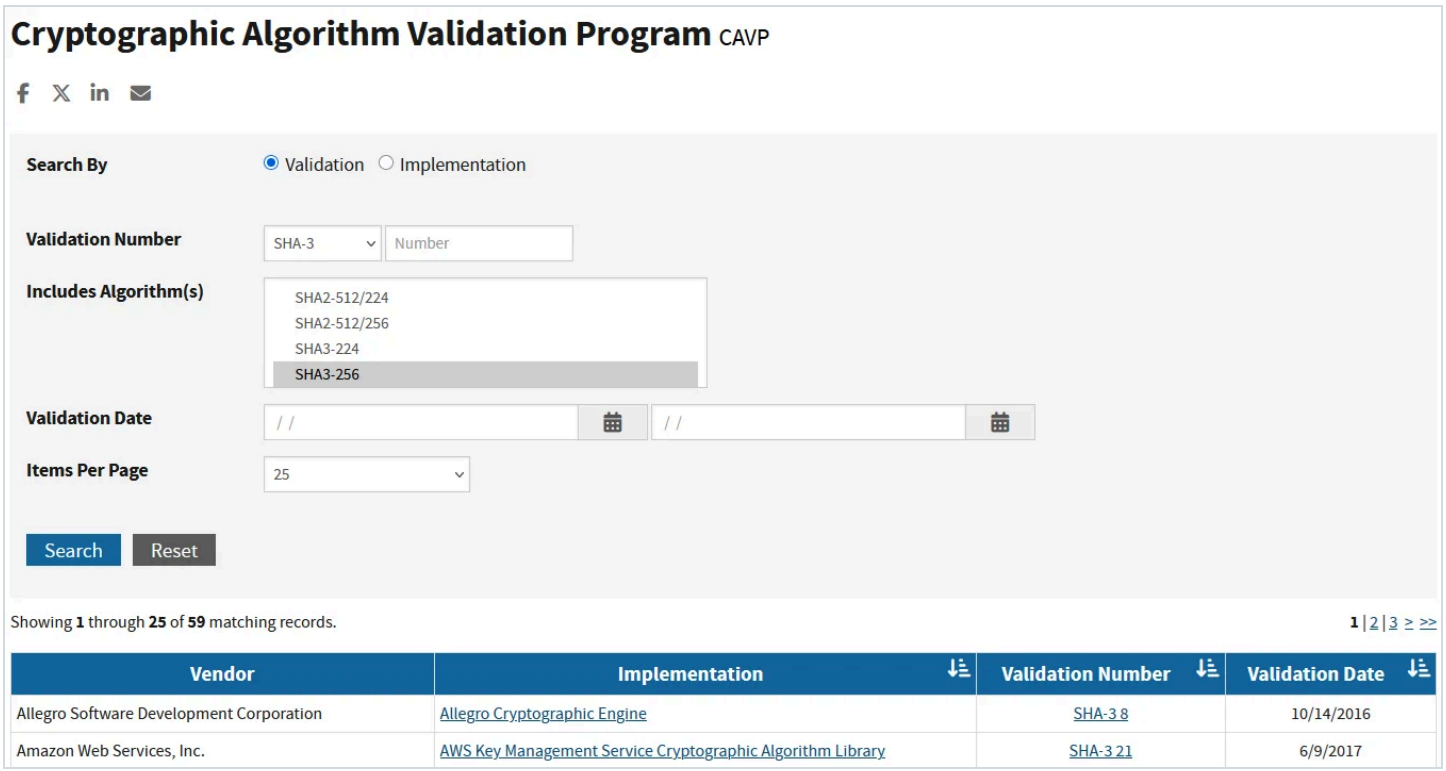
Details

Module Name	Cryptographic Primitives Library
Standard	FIPS 140-2
Status	Active
Sunset Date	9/21/2026
Overall Level	1
Caveat	When operated in FIPS mode with modules Kernel Mode Cryptographic Primitives Library validated to FIPS 140-2 under Cert. #4766 operating in FIPS mode and Code Integrity validated to FIPS 140-2 under Cert. #4511 operating in FIPS mode or Secure Kernel Code Integrity validated to FIPS 140-2 under Cert. #4512 operating in FIPS mode

Terms like “FIPS-compliant” or “FIPS-capable” do not mean FIPS-validated. Many software libraries might claim they use “FIPS-approved algorithms” or have a “FIPS mode,” but unless the module has actually gone through CMVP testing and received a certificate, it is not FIPS-validated. True FIPS validation gives assurance that the implementation of algorithms (and the module's overall design) meets the standard, including aspects like generating keys properly, protecting key material, running self-tests, resisting tampering, etc. This assurance is why FedRAMP and government policies insist on validated modules rather than just trusting any library that implements AES.

NIST Cryptographic Algorithm Validation Program (CAVP)

The CAVP is the NIST program that validates implementations of approved cryptographic algorithms. Where the CMVP assesses an entire cryptographic module, the CAVP focuses on algorithm correctness. Vendors receive algorithm certificates when an implementation conforms to NIST test requirements.



Cryptographic Algorithm Validation Program CAVP

Search By ◉ Validation ○ Implementation

Validation Number SHA-3 | Number

Includes Algorithm(s) SHA2-512/224, SHA2-512/256, SHA3-224, SHA3-256

Validation Date / / | / /

Items Per Page 25

Search | Reset

Showing **1** through **25** of **59** matching records.

1 | 2 | 3 > >>

Vendor	Implementation	Validation Number	Validation Date
Allegro Software Development Corporation	Allegro Cryptographic Engine	SHA-3 8	10/14/2016
Amazon Web Services, Inc.	AWS Key Management Service Cryptographic Algorithm Library	SHA-3 21	6/9/2017

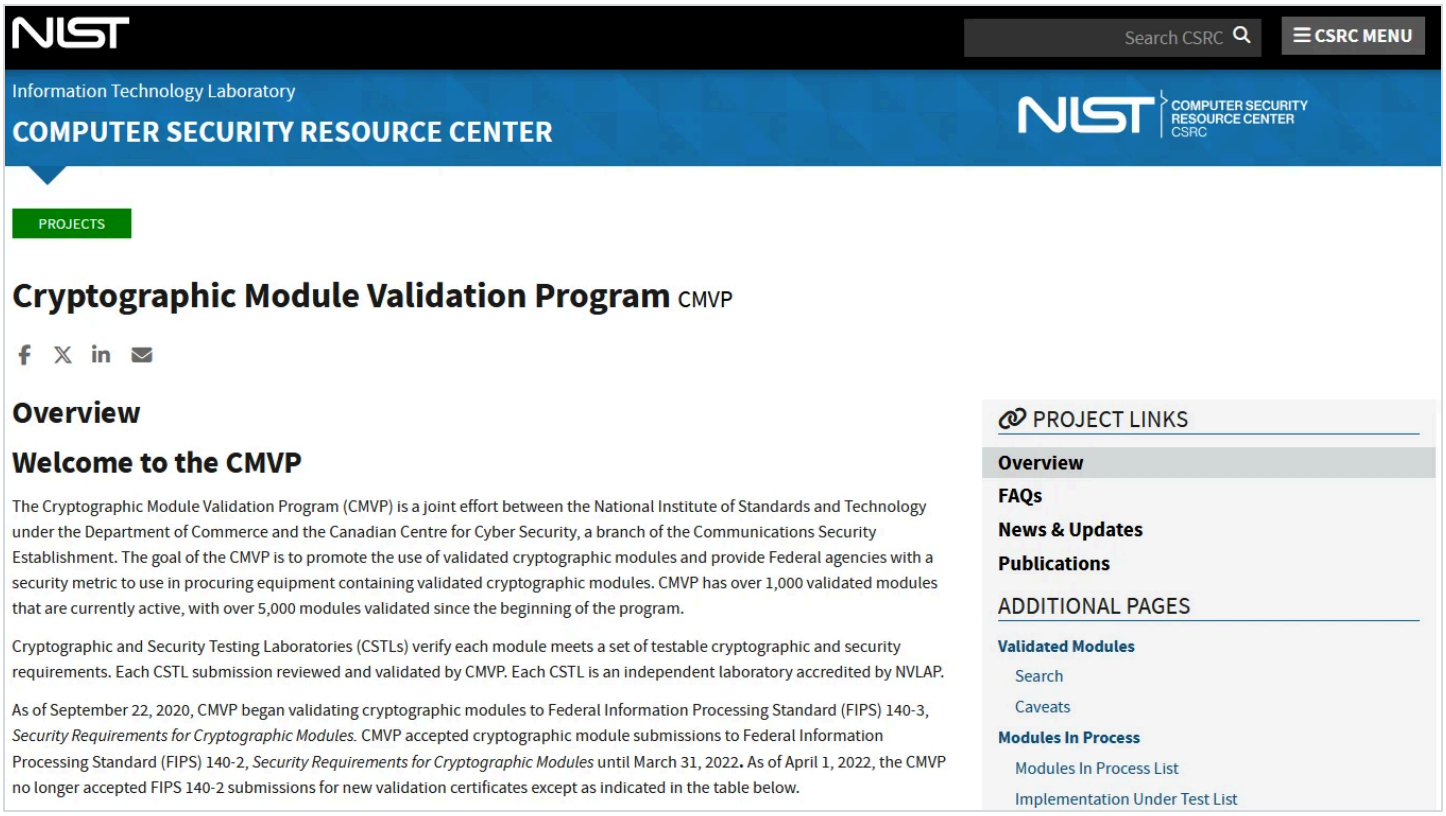
Each entry on the validated algorithms list identifies the vendor, the specific algorithm and mode, supported parameters such as key sizes, the certificate number, and any caveats or operational notes. Practitioners can use this list to confirm that a library or hardware core has a validated implementation of an approved algorithm.

CAVP validation is a prerequisite for CMVP module validation. A module submitted to the CMVP must incorporate algorithm implementations that already hold matching CAVP certificates for the claimed algorithms, modes, and key sizes. Algorithm validation alone does not satisfy FIPS 140-3 because it does not evaluate module-level design, key management, entropy sources, or physical and operational controls.

In practice, review the module's CMVP certificate together with the underlying CAVP algorithm certificates to verify that the algorithms in the deployed build are validated. This reduces the risk of relying on non-validated builds that would not meet compliance requirements.

NIST Cryptographic Module Validation Program (CMVP)

The CMVP is the joint NIST (U.S.) and CCCS (Canada) program that conducts and coordinates these FIPS 140 validations. Under CMVP, independent labs perform the actual testing of cryptographic modules against the FIPS 140 criteria. The CMVP then validates the results and issues a certification if the module passes. The program maintains a searchable public list of all validated cryptographic modules on the NIST Computer Security Resource Center site. This list is the definitive reference that auditors and compliance officers will check to confirm whether a given product's cryptography is FIPS validated.



Each entry on the validated modules list includes details such as: the vendor, module name/version, certificate number, validation level for each area, and a PDF of the module's Security Policy. For example, if Microsoft says that Windows 11 cryptography is FIPS 140-3 validated, one can go to NIST's CMVP site and find Microsoft's validated modules listed with their certificate numbers.

When building or assessing a federal system, one must identify which cryptographic module is being used for each security function and verify its CMVP validation status. Fortunately, CMVP makes this straightforward via its public listings and documentation. Many operating systems and libraries used in cloud and enterprise environments already have validated modules available.

Cryptographic Module Security Policy

For each validated cryptographic module, a Security Policy document is published to describe how the module meets FIPS requirements and how it should be used securely.

FIPS 140-3 Non-Proprietary Security Policy

Google, LLC.

BoringCrypto

Software Version:
2023042800

Date: January 10, 2025

Public Material – May be reproduced only in its original entirety (without revision).

2. Cryptographic Module Specification

Google, LLC BoringCrypto module is an open-source, general-purpose cryptographic library which provides FIPS 140-3 approved cryptographic algorithms to serve BoringSSL and other user-space applications.

The boundary of the module is defined as a single object file, bcm.o, and its instantiation in memory. The module version is: 2023042800.

The module was tested on the following operational environments:

#	Operating System	Hardware Platform	Processor	PAA/Acceleration
1	Android 14	Google Pixel 8	Google Tensor G3 64-bit	With and without PAA
2	Android 14	Google Pixel 7	Google Tensor G2 64-bit and 32-bit	With and without PAA
3	Android 14	Google Pixel 6	Google Tensor 64-bit and 32-bit	With and without PAA
4	Android 14	Google Pixel 5a	Qualcomm Snapdragon 765 64-bit and 32-bit	With and without PAA
5	Google Prodimage with Linux 5.15.110	IN762	IN762	With and without PAA
6	Google Prodimage with Linux 5.10.0	Tau t2a	Ampere Altra	With and without PAA
7	Ubuntu 23.04	Gigabyte GA-Z170X-UD5	Intel Core i7-6700K	With and without PAA
8	Debian Linux 6.4.4	n2d	AMD EPYC 7B12	With and without PAA

Table 2 - Tested Operational Environments

The cryptographic module is also supported on the following operational environments for which operational testing and algorithm testing was not performed:

#	Operating System	Hardware Platform
1	Linux 4.X	x86_64 architecture ARMv7 architecture ARMv8 architecture
2	Linux 5.X	x86_64 architecture ARMv7 architecture ARMv8 architecture
3	Linux 6.X	x86_64 architecture ARMv7 architecture ARMv8 architecture

Table 3 - Vendor Affirmed Operational Environments

Public Material – May be reproduced only in its original entirety (without revision).

The Security Policy is essentially the manual for a FIPS-validated module's proper operation. It includes:

- A description of the module and its boundaries (hardware, software, firmware components).
- The cryptographic algorithms it implements.
- The FIPS-approved modes of operation, the roles and services.
- The rules that must be followed such as how to initialize in FIPS mode and what to avoid to stay in compliance.

- The list of both Approved algorithms and any Non-approved but allowed algorithms.
- Self-test procedures, error states, and any physical security mechanisms.

An important part of the security policy is the delineation of mode of operation. There are two modes which any FIPS validated cryptographic module can be in:

1. Approved Mode.
2. Non-Approved Mode.

A cryptographic module must be running in its approved mode of operation, as described in the security policy, to be considered "FIPS validated." If the cryptographic module is running in a non-approved mode, the vendor provides no guarantee to the FIPS validation of the cryptographic module or the functions run by the module.

Typically, the security policy will explicitly state how to configure or instantiate the module such that it runs in FIPS-approved mode, and it will list which algorithms are FIPS-approved versus which are non-approved. For example, a module's policy might list SHA-256, SHA-384, AES, RSA, DRBG, etc. as FIPS-approved algorithms available, while also listing MD5 or SHA-1 for non-digital-signature use as “non-approved algorithms” that are present but not to be used in FIPS mode. The policy will often note if some non-approved algorithms are only allowed in specific circumstances. The most common example of this is the usage of SHA-1 which may be allowed for hashing but disallowed for digital signatures.

The security policy matters to implementers and assessors because it tells you how to deploy the module in compliance. For instance, if you have a FIPS-validated OpenSSL module, its Security Policy will explain that you must call a specific FIPS_mode() enabling function or load a FIPS provider, and that certain algorithms must not be used or the module will transition to a non-approved state. It will also enumerate any configuration settings required.

The security policy is where one finds the allowed configurations and cryptographic primitives for a given module. When ensuring your system is FIPS validated, you often need to consult these documents to verify that you are using the module correctly. The security policy also provides the mapping of the module's certificate number and version. In practice, a good starting point is to locate the Security Policy PDF for each crypto module in your product and review the “FIPS Approved algorithms” and “Non-Approved algorithms” sections, as well as any guidance about module initialization.

Conclusion

Federal programs and sector frameworks require FIPS-validated cryptography where they govern your system. Validation attaches to a cryptographic module, not to an algorithm name by itself, and it only counts when the module is operating in its Approved mode as defined in its Security Policy. The CMVP list and the module's published Security Policy are the authoritative sources for what is validated and how it must be configured.

Implementing FIPS validated cryptography across your stack is one of the largest engineering tasks associated with configuring systems to meet federal requirements. Cryptography spans all layers of a system's technology stack, from operating systems, to containers, to data at rest.

Automata has published The Automata FIPS (AFIPS) Model to provide the first industry standard and best practices on mapping Federal Information Processing Standards (FIPS) 140 validated cryptography within a system.

Glossary

A-130: OMB Circular A-130, which implements FISMA requirements for federal information systems.

ATO: Authorization to Operate, the formal management decision that authorizes a system to operate and accepts risk.

CJIS: Criminal Justice Information Services program and policy set that governs protection of criminal justice information.

CAVP: The NIST Cryptographic Algorithm Validation Program (CAVP) provides validation testing of Approved (i.e., FIPS-approved and NIST-recommended) cryptographic algorithms and their individual components.

CMVP: Cryptographic Module Validation Program, the joint NIST and CCCS program that validates cryptographic modules and publishes certificates.

CMMC: Cybersecurity Maturity Model Certification.

CNG: Cryptography API: Next Generation, Microsoft's cryptographic platform.

CSP: Cloud Service Provider.

Cryptographic module: The hardware, software, or firmware that implements cryptographic functions and is assessed as a unit under FIPS 140. The module's boundary and services are defined in its Security Policy.

Controlled Unclassified Information: Information that law, regulation, or governmentwide policy requires to have safeguarding or disseminating controls, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

FedRAMP: Federal Risk and Authorization Management Program for assessing and authorizing cloud services for use by federal agencies.

FIPS: Federal Information Processing Standards.

FIPS 140-2: Earlier version of the cryptographic module standard. Its certificates move to the Historical List after September 21, 2026.

FIPS 140-3: Current cryptographic module standard. Builds on ISO and uses validation levels 1 through 4.

FISMA: Federal Information Security Modernization Act.

NIST: National Institute of Standards and Technology.

OMB: Office of Management and Budget.

Security Policy: The published document for a validated module that defines the module boundary, roles, services, Approved mode configuration, allowed algorithms, and self-tests.

SP: Special Publication, a NIST series of guidance documents.

TLS: Transport Layer Security protocol for network encryption.