Technical Paper

Product Security
FIPS 140-3 Certification

FIPS 140-3 Primer

Intel's Approach to Cryptographic Module Validation

Intel's commitment to product security includes focus on compliance with regulatory requirements including Federal Information Processing Standard (FIPS) 140-3.

Authors

Adesola Adegboye
Intel FIPS Center of Excellence

Anna Scott
Intel Government Center of Excellence

FIPS 140-3 Introduction

Federal Information Processing Standard (FIPS) 140-3 is the latest National Institute of Standards and Technology (NIST) developed standard for validating the effectiveness of cryptographic hardware. Since 1994, the US and Canadian federal departments and agencies that operate or are operated for them under contract are required by law to purchase hardware that is FIPS 140-validated to protect sensitive or valuable information in computer and telecommunication systems (including voice systems).

Additionally, many governments worldwide leverage FIPS 140 in their security requirements (e.g. Common Criteria in the European Union). This interaction was strengthened by alignment between FIPS 140-3 and the ISO 19790 and ISO 24759 standards on information technology security.

There have been two revisions of the FIPS standard. FIPS 140-3, became effective September 22, 2019. FIPS 140-2, which will reach end of life September 21, 2026, is still widely used.

FIPS 140 Fundamentals

FIPS 140 requirements cover areas related to the secure design, implementation and operation of a cryptographic module. The standard provides four increasing, qualitative levels (L1 - L4) of security intended to cover a wide range of potential applications and environments (see table below). Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module.

Table of Contents

	FIPS 140-3 Security Level			
Requirement Area	**L1**	**L2**	**L3**	**L4**
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes or operation. Description of cryptographic module including all hardware, software and firmware components, all services provide status information to indicate when the service utilizes an approved cryptographic algorithm, security function or process in a n approved manner.			
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output paths		Trusted channel	
Roles, Services, and Authentication	Logical separation of required and optional roles and services	Role-based or identity-based operator authentication	Identity-based operator authentication	Multi-factor authentication
Software / Firmware Security	Approved integrity technique.	Approved digital signature or keyed message authentication code-based integrity test	Approved digital signature-based integrity test	
Operational Environment	Non-modifiable.	Modifiable. Role-based or discretionary access control. Audit mechanism		
Physical Security	Production grade components	Tamper evidence. Opaque covering or enclosure.	Tamper detection and response for covers and doors. Strong enclosure or coating. Protection from direct probing EFP or EFT.	Tamper detection and response envelope. Fault injection mitigation.
Non-invasive Security	Module is designed to mitigate against non-invasive attacks			
	Documentation and effectiveness of mitigation techniques		Mitigation testing	Mitigation testing
Security Parameter Management	Random bit generators, SSP generation, establishment, entry and output, storage and zeroization			
	Automated SSP transport or SSP agreement using approved methods			
	Manually established SSPs may be entered or output in plaintext form		Manually established SSPs may be entered or output in encrypted form via a trusted channel or using split knowledge procedures	
Self-Tests	Pre-operational: software/firmware integrity, bypass, and critical functions test			
	Conditional: cryptographic algorithm, pair-wise consistency, software/firmware loading, manual entry, conditional bypass and critical functions test			

Non-validated cryptography is viewed by NIST as providing ***no protection*** to information or data—in effect, data would be considered unprotected plaintext. ***If the agency specifies that information or data be cryptographically protected***, then FIPS 140-2 or FIPS 140-3 is applicable. In essence, if cryptography is required, then it must be validated. Should the cryptographic module be revoked, use of that module is no longer permitted. (ref NIST CMVP)

Accredited Lab Validation

FIPS 140-3 requires that cryptographic modules be validated through the independent Cryptographic and Security Testing (CST) laboratories, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP). The CST labs perform cryptographic module conformance testing and protect each vendor's Intellectual Property (IP) while assuring high quality assessment. (From ITL Bulletin)

On December 1, 2023, the Intel CST Lab was accredited as a first-party laboratory approved to validate its own algorithm implementations, a non-commercial service.

FIPS Validated Modules

NIST maintains a website with all validates modules, modules in process, and modules at an accredited lab waiting for testing:

- Validated Modules
- Modules in Process
- Implementation Under Test
- Entropy Validation

FIPS Transition Timeline

The FIPS 140 standard has evolved over time. The first version was published in 1994. It was updated in 2001 as FIPS 140-2. FIPS 140-3 was published March 22, 2019, and became effective September 22, 2019. Note that:

- FIPS 140-2 submissions are no longer being accepted.
- All FIPS 140-2 certifications will be sunset (moved to the "Historical" state) on **September 22, 2026**.
- See the Transition Timeline from FIPS 140-2 to 140-3

Customer Value of FIPS 140 Validation

Encrypting data at rest and in motion is critical for protecting sensitive and valuable data, especially now when environments assume an adversary is present. Intel is aware that federal customers are required to purchase FIPS-compliant hardware; so naturally, compliance with FIPS is expected for Intel to sell hardware to these customers. However above and beyond this requirement, FIPS 140-validated hardware provides a clear benefit to all companies and organizations, because FIPS 140-validated hardware has been rigorously tested and shown to meet the NIST standards of encryption for data protection. **The value of FIPS 140 validation is that it ensures that the cryptography implementation actually works as required.** When an Intel product is FIPS validated, then customers know that the product is designed with strong cryptographic algorithms (NIST approved), key management schemes, self-tests, authentication of users, and physical designs in a standard manner.

There are several key values and benefits for organizations, governments, and end users that are using or validating cryptographic modules. This includes enhanced security, support with compliance efforts, supply chain of trust, government endorsement and market access, competitive advantage, cost savings and most importantly data integrity, non-repudiation, and crypto proofing. By leveraging FIPS 140-3 validated modules, organizations can ensure a robust cryptographic foundation for their information security infrastructure.

Legal Requirements for FIPS 140-3

All US and Canadian Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) are required by law to purchase system(s) that are FIPS 140-validated. This requirement is spelled out in the FIPS 140-3 document Abstract. The exact language is:

- This standard (FIPS 140-3) shall be used in designing and implementing **cryptographic modules** that federal departments and agencies operate or are operated for them under contract.
- This standard is applicable to **all federal agencies that use cryptographic-based security systems** to provide adequate information security for all agency operations and assets as defined in 15 U.S.C. § 278g-3.

The US laws that make this a requirement are also called out in the FIPS 140-3 Standard on p *iv*, Section 6. Applicability:

- Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 140-106)
- Federal Information Security Management Act of 2002 (Public Law 107-347)

How FIPS Validation Works

The FIPS 140 validations process **typically takes more than one year** and requires testing by a CSTL lab. Currently, there is a significant backlog on FIPS 140-3 testing, so the time frame for validation is even longer (in some cases up to 2 years). Although CMVP has been accepting submissions against FIPS 140-3 since September 2020, only 259 certifications have been approved as of March 2025, compared to 400+ that are still in the queue.

NIST has a rigorous methodology for selecting the best encryption algorithms, tests them for performance and then test and validate their use within platforms (modules). There are three main elements of the validation process: Cryptographic Algorithm Validation Program (CAVP), Entropy Source Validation (ESV), and the Cryptographic Module Validation Program (CMVP).

CAVP

The CAVP provides validation testing for cryptographic algorithms to ensure they are implemented correctly and securely. This validation is a prerequisite for cryptographic modules that will undergo FIPS 140-2 or FIPS 140-3 certification through the CMVP.

CAVP tests specific cryptographic algorithms against established standards to ensure they are implemented correctly. These algorithms include, but are not limited to, symmetric and asymmetric encryption algorithms, hash functions, digital signature algorithms, and random number generators.

Validation Process:

- Vendors with first party labs (such as Intel) may complete the algorithm validation within their lab. While vendors without labs may submit their implementations to be tested by accredited third-party laboratories.
- Once an algorithm implementation passes CAVP testing, it receives an algorithm certificate indicating compliance with the relevant standard. This certificate is often a requirement for further certification of the cryptographic module under CMVP.
- CAVP only validates the correctness of the algorithm implementation, not the entire cryptographic module or system. Other aspects of a cryptographic module, such as ESV, its physical security or overall design, are outside the scope of CAVP and are addressed by CMVP. If changes are made to the implementation, it may need to be re-validated.
- An algorithm validation does not have a defined expiration date, but it can be superseded by new standards or withdrawn if vulnerabilities are discovered in the algorithm.

ESV

The Entropy Source Validation (ESV) program is a prerequisite of the CMVP managed by NIST. The ESV program specifically focuses on the validation of entropy sources used in cryptographic systems. Entropy sources are mechanisms that generate random values, which are crucial for the security of cryptographic operations, such as key generation, nonce generation, and random padding.

Encryption and random number generation must be done using NIST-approved algorithms and random number generators:

- Entropy – A measure of disorder, randomness or variability in a closed system.
- Entropy Source – The combination of a noise source, health tests, and an optional conditioning component that produce random bitstrings to be used by an RBG.
- Random Bit Generators (RBG) – A device or algorithm that outputs a random sequence that is effectively indistinguishable from statistically independent and unbiased bits. An RBG is classified as either Deterministic (DRBG) or Non-deterministic (NRBG).

All entropy sources should have an ESV to prove that the entropy source meets the NIST requirements:

- Encryption must be done using NIST-approved hash functions or block cipher algorithms per NIST SP800-90A rev1, which specifies several DRBG mechanisms based on cryptographic algorithms.
- Random number generation must follow NIST SP 800-90B, which provides guidance for the development and validation of entropy sources used by the DRBG.

This is important because random numbers are used for key generation and weak keys create security vulnerabilities. The CAVP can be in hardware, software, or firmware or any combination of these.

CMVP

To be FIPS validated, a module boundary must be defined and this module must be submitted and approved through NIST's CMVP. This process can be done by Intel or by partners.

A cryptographic module can be defined as a set of **hardware, software, firmware,** or some **combination** thereof, that **at a minimum**, implements a **defined cryptographic service** employing an **approved cryptographic algorithm, security function,** or **process** and is contained within a **defined cryptographic boundary**.

A cryptographic module is defined by a boundary. This boundary is determined by the company that is submitting the module for validation. When Intel submits a module to CVMP for validation Intel defines the hardware, software, and firmware. Note that Intel often provides module components and documentation to OEMs for inclusion in their modules. When we do this, we consider our component to be "FIPS certifiable" since it does not have full FIPS validation, but it can be validated since it uses NIST-approved algorithms.

FIPS at Intel

Executive Mandate

Intel is under an executive leadership mandate to be FIPS 140-3 certifiable across all platform lines beginning in 2024. The FIPS Center of Excellence (COE) was launched in July of 2021 to provide the resources and support needed for Intel to follow this mandate. The FIPS COE has deep technical/FIPS talent from across the Intel technical community, and it supports Intel Business Units (BUs) and engineering teams in their compliance with this mandate.

Intel FIPS Process

The Intel FIPS COE is responsible for helping BUs apply for FIPS certifiability/validation. Intel can either pursue:

a. FIPS Validated: Create a fully certified module (CVMP) that will be delivered to partners along with needed documentation.

b. FIPS Certifiable: Create an artifact that is certifiable that will be delivered to partners along with needed documentation so partners can certify the Intel component as a part of their module.

FIPS Validated

Intel defines a module and applies for CVMP validation for a hardware, software, and firmware (or a combination (hybrid) of these) module.

1. Intel architects/engineers design their IP or products to be FIPS certified.
2. Intel produces necessary architecture/design documentation and evidence of implementation (e.g. RTL, code, entropy tests, etc.) within the cryptographic boundary to be used by an approved FIPS lab in certification.
3. Intel, working through a FIPS-approved lab, provides documentation, evidence of implementation, testing the product, and submitting results to certifying bodies (e.g., NIST and Canadian authority). Intel can determine, in coordination with the lab, what documentation we produce and what the lab produces.

FIPS Certifiable

Intel's definition of "certifiable" is the identification of a cryptographic module, designed and implemented to meet applicable FIPS 140-3 requirements, documented, pre-tested, including FIPS approved algorithms, with the capability to perform required self-tests and other operations, and eventually acquire FIPS 140-3 validation from the CMVP by Intel or customers/partners, if desired.

Validation that a module meets those requirements is evaluated and tested by an accredited third-party lab and the authorization and certificate is provided by the CMVP based on an independent written report of that lab.

1. Intel architects/engineers design their IP or products to be FIPS certifiable.
2. Intel produces necessary architecture/design documentation and evidence of implementation (e.g. RTL, code, entropy tests, etc.) within the cryptographic boundary to be used by an approved FIPS lab in certification. Note: Intel can work with a lab to support this process of document and evidence creation.
3. Optional: Intel provides architecture and design documentation and implementation evidence to a partner or OEM and certifies our component in their product or platform.

Intel may in the future decide, based on business requirements, to pursue validation.

FIPS and International Standards

FIPS 140-3 is based on the following international standards:

- ISO/IEC 19790:2012/Cor.1:2015(E) *Information technology — Security techniques — Security requirements for cryptographic modules*
- ISO/IEC 24759:2017(E). *Information technology — Security techniques — Test requirements for cryptographic modules*

Definitions

- **FIPS**: Federal Information Processing Standards
- **NIST:** National Institute of Standards and Technology
- **FIPS 140-3:** Security Requirements for Cryptographic Modules
- **FIPS Module:** A cryptographic module can be defined as a set of **hardware, software, firmware,** or some **combination** thereof, that **at a minimum**, implements a **defined cryptographic service** employing an **approved cryptographic algorithm, security function,** or **process** and is contained within a **defined cryptographic boundary.**
- **FIPS Certifiable:** Intel has defined the term "Certifiable" as the identification of cryptographic module, designed and implemented to meet applicable FIPS 140-3 requirements, documented, pre-tested, that includes one or more FIPS Approved Algorithms (CAVP), with the capability to perform required self-tests and other operations, and eventually acquire FIPS 140-3 validation from CMVP by Intel customers/partners (e.g. OEMs)
- **FIPS 140-3 Validated**: A module that has been reviewed and validated by an accredited Cryptographic and Security Testing Laboratory.
- **FIPS "Module In Process":** Complete set of testing documents submitted to NIST and CCCS for review but the review is not yet complete. Documentation includes draft certificate, summary module description, detailed test report, nonproprietary security policy, web-site information. In addition, some CST labs include a separate physical testing report. Signed letter from laboratory stating recommendation for validation received by NIST and CCCS.
- **CAVP:** Cryptographic Algorithm Validation Program
- **CMVP:** Cryptographic Module Validation Program.
- **ESV**: Entropy Source Validation
- **SP** (for CAVP only): Security Policy - Appropriate documentation has been prepared to allow our customers/partners to certify the cryptography implemented in our products either as its own FIPS 140 cryptographic module or as a component in the customer/partner's bigger FIPS cryptographic module.
- **EFP:** Environmental Failure Protection
- **EFT:** Environmental Failure Testing
- **SSP:** Sensitive Security Parameter

Disclosures

[1] All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Intel technology's features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No product or component can absolutely be secure.