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

Gerrit Kruitbosch
Silicon Engineering Group

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 modules. 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 products that are FIPS 140-validated to protect sensitive or valuable information in computer and telecommunication systems (including voice systems).

Additionally, many industries worldwide embrace FIPS 140 in their security requirements (e.g., the Payment Card Industry and the Digital Cinema Initiative). FIPS 140-3's adoption of the ISO/IEC 19790 and ISO/IEC 24759 standards on information technology security increased international involvement.

The FIPS standard has been revised twice. FIPS 140-2 was established in 2001. FIPS 140-3 referencing ISO/IEC 19790/2012 became effective September 22, 2019. Modules validated under 140-2 may remain on the validated modules list through September 21, 2026, and will remain acceptable for purchase until that time. It is anticipated that NIST will eventually release 140-4 referencing ISO/IEC 19790/2025.

FIPS 140 Fundamentals

FIPS 140 security 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 Introduction....1
FIPS 140 Fundamentals....1
Customer Value of FIPS Validation....3
How FIPS Validation Works....3
FIPS at Intel....4
FIPS and International Standards....5
Definitions....5

	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 is applicable. In essence, if cryptography is required, then it must be validated. Should the cryptographic module validation 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 independent Cryptographic and Security Testing (CST) laboratories, accredited by the National Voluntary Laboratory Accreditation Program (NVLAP, Lab Code: 600342). 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 transit is a typical application of cryptography and is critical for protecting sensitive and valuable data. Intel is aware that its Federal customers are required to purchase FIPS 140 validated products; so naturally, compliance with FIPS 140 is necessary for Intel components and validation to FIPS 140 for products sold directly to Federal customers. **The value of FIPS 140 validation is that it provides assurance from an independent 3rd-party that the cryptographic module complies with the requirements of ISO/IEC 19790.** When an Intel product is FIPS validated, customers can be assured 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 as described in the module Security Policy.

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 page *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 validation process includes the following steps: contracting an approved CST lab, providing design evidence, Cryptographic Algorithm Validation testing, Entropy Source Validation, source code review, operational testing, documentation and report generation, submission and NIST review. The entire process **typically takes more than one year**. Historically, there has been a significant backlog in the FIPS 140 review process, so the time frame for validation can sometimes exceed 2 years. A validation certificate is only valid for 5 years. Combined with the frequent release of many products, this can create quite a validation effort.

NIST has a rigorous methodology for selecting and specifying encryption algorithms, testing implementations for correctness, and testing their use within a larger context (modules). There are three related validation programs: 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. This validation is a prerequisite for cryptographic modules that will undergo FIPS 140 validation through the CMVP. It is also a prerequisite for validations performed by the U.S. National Information Assurance Partnership, which oversees a national program to evaluate Commercial Off-The-Shelf Information Technology products for conformance to the International Common Criteria.

The CAVP tests specific cryptographic algorithm Implementations against established standards to ensure they are implemented correctly. These algorithms include, but are not limited to, cryptographic key generation, key establishment schemes, symmetric and asymmetric encryption algorithms, hash functions, and digital signature algorithms.

Validation Process:

- CAVP validates the correctness of a given algorithm implementation, not the entire cryptographic module or system. If changes are made to the implementation, the new version must be validated.
- NIST has created an automated test system that provides input test data, which is processed by the implementation under test. The test output is then sent back to NIST for validation.
- Official testing must be performed through a test lab accredited by the National Voluntary Laboratory Accreditation Program. Vendors may establish a first-6[[party lab to do their own testing, or they must perform testing through a third-party test lab.
- Once an algorithm implementation passes CAVP testing, it receives an algorithm certificate indicating compliance with the relevant standard.
- An algorithm validation certificate 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

Cryptography and security applications extensively use random numbers and bits. When random values are required, the security of cryptographic methods can be directly affected by their randomness. Entropy sources play a crucial role in the generation of random numbers. NIST provides comprehensive guidelines and requirements for random number generation, including recommendations for entropy sources, deterministic random bit generators (DRBGs), and hybrid random number generators.

The Entropy Source Validation (ESV) program validates that a given source of entropy is compliant with the NIST standard (NIST SP 800-90B). ESV is also a prerequisite for cryptographic modules that undergo FIPS 140 validation as well as Common Criteria validations through the NIAP Scheme.

Validation Process:

- A rigorous model of the source must be analyzed to establish the minimum entropy under operational conditions.
- Substantial sampling of raw noise data and other operational parameters must be collected and analyzed to corroborate the model.
- Conditioning elements that consist of NIST-approved algorithms must be tested and validated through the CAVP.
- All results must be independently assessed by an accredited test lab that sends them to NIST for final validation.

The output of an entropy source should contain a sufficient amount of randomness (entropy) to provide the required security. Random number generation is nuanced, difficult, and at times even counterintuitive. As such, it is crucial that entropy sources have an ESV to provide assurance that the entropy source meets the NIST requirements.

CMVP

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 determined by the company seeking validation and within the guidelines established by the CMVP. When Intel submits a module to CVMP for validation, Intel defines the hardware, software, and firmware. Note, however, that Intel often provides module components and documentation to OEMs for inclusion in their modules, which they validate. When Intel does this, they seek to ensure the component(s) are "FIPS certifiable", meaning they will not prevent validation at a larger cryptographic module boundary. This may include working with our OEMs to provide CAVP, ESV, documentation, and even operational test support.

FIPS at Intel

Executive Mandate

Intel has issued 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, industry forum, and FIPS-related standards bodies. The COE 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 products are either:

a. FIPS Validated – Intel works with a third-party lab to fully validate the module.

b. FIPS Certifiable – products have been designed with compliance to FIPS 140 with the intent that our partners or customers may validate, typically as part of a larger module boundary.

FIPS Validated

Intel defines a module, performs testing with a third-party lab, and submits for full validation through the NIST CMVP.

1. Intel architects/engineers design their IP or products to be FIPS 140 compliant.
2. Intel defines a module boundary and module type as deemed appropriate.
3. 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 validation.
4. Intel, working with a NIST-accredited test lab, provides documentation, evidence of implementation, and tests the product. The test lab submits the results to the validation authority (CMVP).

FIPS Certifiable

As a component manufacturer, Intel's products are often just a part of a larger product where OEMs and partners add additional security functionality. In this context, validation is often more appropriate at a larger product boundary. Intel's approach is to make products "certifiable", meaning the component is fully compatible and compliant with the requirements of ISO/IEC 19790 when applied at the larger boundary. This is accomplished by ensuring the component is designed and implemented to meet applicable FIPS 140-3 requirements, pre-tested, including FIPS approved algorithm validation under the CAVP, with the capability to perform required self-tests and other operations, and documented as necessary. This enables Intel or customers/partners to later acquire FIPS 140-3 validation from the CMVP, if desired.

.

1. Intel architects/engineers design their IP or products to be FIPS 140 compliant at a broader product boundary.
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 validation.
3. As negotiated: Intel provides architecture and design documentation and implementation evidence to a partner or OEM and supports validation testing.

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 tested by an accredited Cryptographic and Security Testing Laboratory and validated by the NIST CMVP.
- **FIPS "Module In Process List":** A list maintained by the CMVP indicating that a complete set of testing documents have been submitted to NIST and CCCS for review. Each submission has a status indicating the modules progress through the review process. 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
- **Security Policy**: A required public document accompanying each validated module indicating the precise specification of the security rules under which a cryptographic module shall operate, including the rules derived from the requirements of the Standard and additional rules imposed by the module or validation authority.
- **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.

Copyright © 2025 Intel Corporation. All rights reserved. Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and other countries.

* Other names and brands may be claimed as the property of others.

intel®