FIPS for the Future

July 2023

About the Authors

Michael Burke, Coalfire

Michael is a Principal Consultant in the Payments Advisory and Product Guidance Practices at Coalfire, which includes workshops, fit-for-purpose reviews/whitepapers, gap analyses, and larger customer support efforts
(remediation and staff augmentation).

Michael came to Coalfire from a long career that included leadership positions on Wall Street, Global Systems Integrators, Government Agencies, and Compliance Assessment. On Wall Street, Michael was responsible for leading Front Office Trading Technology and overseeing integrations with back office and risk management. He helped Government Agencies, Educational Institutions, and Transportation firms strategically apply technology to solve business challenges and maintain regulatory compliance.

Michael has extensive experience working with large financial firms, as well as other highly regulated organizations, consulting with clients building compliance programs. Recent work has focused on coordinated advisory and assessment efforts, program management and the reduction of audit fatigue. Having experience in multiple frameworks as an assessor (PCI, SOC, HITRUST, FedRAMP, NIST, ISO, GDPR), Michael brings a pragmatic approach to solving compliance challenges.

Cloud Service Providers - Advisory Board

The Cloud Service Providers - Advisory Board (CSP-AB) represents the world's leading cloud companies and supports standards and policies that promote and enable secure cloud adoption in the public and private sectors. Our member companies are global leaders in the drive to provide safe, scalable, and accredited digital government services, with a focus on both the civil servants delivering those services and the end-users receiving them.

The CSP supports the Federal Government in developing more agile, effective, and innovative standards, while maintaining the highest levels of information security; serves as a technical resource to FedRAMP, governmental, and industry stakeholders to help inform policies that support efficient and secure adoption of cloud technology; and provides a forum for CSPs to engage and collaborate on technical and policy matters pertaining to the secure adoption of cloud technology.

To find out more, visit https://www.csp-ab.com/

Contents

FIPS for the Future

Abstract

Validated conformance testing against the Federal Information Processing Standards (FIPS) specification gives important assurances to end-users. The most recent update of FIPS 140 incorporates testing methodology from the International Organization for Standardization (ISO) to validate cryptographic modules, further enhancing the security protections for end-users. However, while FIPS 140 is crucial and critical, the process of validation has been long, complex, and further complicated by delays.

This paper outlines some of the challenges and proposes solutions to improve the FIPS Cryptographic Module Validation Program (CMVP) validation process, and some of the methods by which vendors and consumers interact with the validation process. Several ideas are provided to improve the process in which cryptographic modules (CMs) are validated and reported, with the intention to make improvements without lowering the standard of quality or security, which is integral to ensure the effectiveness of cryptography and risk management.

The primary recommendation is to create a recommended order of implementations for downstream certifications that indicates modules should be used in a specific order of preference.

Overview of FIPS 140

Federal Information Processing Standards (FIPS) 140 is a mandatory standard required for all U.S. federal government agencies that use cryptography-based security systems (hardware, firmware, and/or software) for the protection of their data.[1] The standard was published as FIPS 140-1 in January 1994 and has been revised twice. FIPS 140-3 is an incremental advancement of FIPS 140-2, which standardizes on the International Organization for Standards (ISO), ISO 19790:2012 and ISO 24759:2017 specifications.[2] The decision to keep FIPS 140-3 as a separate standard will still allow the U.S. National Institute of Standards and Technology (NIST) to mandate additional requirements on top of what the ISO standards contain, when needed. Cryptographic modules are required to be tested by independent laboratories that adhere to the FIPS 140 testing requirements maintained by the Cryptographic Module Validation Program (CMVP), a joint effort between NIST and the Canadian Centre for Cyber Security, a branch of the Communications Security Establishment (CSE) of Canada.[3]

Why FIPS 140 is important

The goal of FIPS 140 is to establish a cryptographic-based security standard that must be met by systems storing certain types of data. The FIPS 140 standard has emerged as the benchmark for a high level of security and is explicitly required in some use cases. Organizations must use FIPS 140 validated cryptography to protect data under NIST 800-171, and is a Defense Federal Acquisition Regulation Supplement (DFARS)and Cybersecurity Maturity Model Certification (CMMC) 2.0 requirement.[4,5,6] Mandated through the Federal Information Security Modernization Act (FISMA), validated modules are required to be used in federal government departments that collect, store, transfer, share and disseminate sensitive but unclassified (SBU) information.[7] This applies to all federal agencies as well as their contractors and service providers, including networking and cloud service providers.

Validation Testing

Testing under FIPS 140 is split across two areas: the module's architecture and criteria for testing that architecture under NIST SP 800–140. How a cryptographic module is implemented, or the module architecture, is critical to how it is tested under FIPS 140. Cryptographic modules fall into three distinct categories: a hardware only implementation, carried entirely within the firmware of a hardware appliance (i.e. a Hardware Security Module (HSM)); a software driven API library, that may utilize common architecture, or a combination of the two; or a "hybrid" module, which is a new concept within the FIPS 140-3 standard. Based upon this distinction, the architecture determines the test requirements. These test

1 National Institute of Standards and Technology, *FIPS 140-2 Security requirements for cryptographic modules*, accessed February 2023, https://csrc.nist.gov/publications/detail/fips/140/2/final

2 National Institute of Standards and Technology, *FIPS 140-3 Security requirements for cryptographic modules*, accessed February 2023, https://csrc.nist.gov/publications/detail/fips/140/3/final

3 National Institute of Standards and Technology, *Cryptographic Module Validation Program, Validated Modules,* accessed February 2023, https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules

4 National Institute of Standards and Technology, *Compliance faqs: Federal Information Processing Standards (FIPS),* accessed February 2023, https://www.nist.gov/standardsgov/compliance-faqs-federal-information-processing-standards-fips

5 National Institute of Standards and Technology, *Protecting controlled unclassified information, FAQs*, accessed February 2023, from https://csrc.nist.gov/Projects/protecting-controlled-unclassified-information/faqs

6 Carnegie Mellon University and The Johns Hopkins University Applied Physics Laboratory LLC, *Cybersecurity Maturity Model Certification Assessment Guide Level 2,* December 2021, https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf

7 Cybersecurity and Infrastructure Security Agency, *Federal Information Security Modernization Act*, accessed February 2023, https://www.cisa.gov/federal-information-security-modernization-act

requirements are defined in new SP 800-140x publications[8] that are specifically referenced within the FIPS 140-3 standards.

The SP 800–140x documents are a series of testing requirements that define how CMVP algorithms are implemented as well as handling the generation, transmission, and protection of key and key material for those algorithms. Additionally, a module's security level is utilized in the assessment of a crypto module under FIPS 140. FIPS 140 defines four levels of security that measure how that crypto module responds to tampering. The four security levels under FIPS 140–3 (See chart in appendix A) arise from being robust conceivable tampering (Level 1), to passively and actively resisting tampering (Levels 2 and 3). The most aggressive level of FIPS 140–3 is Level 4, which requires that a system resist tampering against environmental attacks from physical access. Typically, this has been in the context of physically accessing the hardware, but as the environments become increasingly virtual, it could be interpreted as access under duress.

Challenges with FIPS 140 and the CMVP

FIPS 140 and the CMVP are challenged through environmental, political, and geographical constraints. Critics often refer to the history of issues with the FIPS 140 validation process as cause for immediate replacement, including concerns about quantum computing, as well as extended backlogs in the validation process. These challenges to the FIPS certification process are well documented and fall into several key areas.

Updating Existing Validations

First, maintenance of the certification under FIPS 140 is extremely difficult.[9] Code changes, including maintenance and bug fixes to a crypto module, necessitate a new crypto module certification. This certification can take months or even years to complete, due to the specified nature of the testing and the backlog of certified labs. As crypto modules are validated as a system, any change, including changes to hardware, including storage, or an operating system module or library, will require the system to be revalidated.

As a result, certified crypto modules are consistently several versions behind the current commercial versions.[10] This can lead to serious problems where exploits or vulnerabilities cannot be immediately patched without a waiver, as doing so would require an update and re-certification of that product. This has led to a number of major exploits in crypto modules that have effectively been left unpatched due to a combination of vendors being unable to recertify quickly.

Additionally, there is a concern that the requirement to use FIPS validated cryptographic modules, while ensuring that strong cryptographic algorithms are used, also potentially introduces security risk from vulnerabilities on the cryptographic module itself. For example, the OpenSSL FIPS Object Module 2.0 was first validated in 2012, with subsequent validations in later years.[11] The 2.0 module only worked with OpenSSL releases 1.0.1 and 1.0.2, and nothing else, such as OpenSSL 1.1 which was not able to support FIPS. OpenSSL 1.0.2 went end-of-support in December 2019, except for premium customers.[12] However,

8 National Institute of Standards and Technology Special Publication 800-140, *FIPS 140-3 derived test requirements (DTR)*, March 2020, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140.pdf

9 Progress, *What you need to know about FIPS 140-2 validation,* September 28, 2018, https://www.ipswitch.com/blog/what-you-need-to-know-about-fips-140-2-validation

10 Speeds and feeds, *Secure or Compliant: pick one,* July 23, 2009 http://veridicalsystems.com/blog/secure-or-compliant-pick-one/index.html

11 Open SSL, *FIPS Module 2.0,* accessed May 2023, *https://wiki.openssl.org/index.php/FIPS_module_2.0*

12 Open SSL, *FIPS Modules,* accessed May 2023, https://wiki.openssl.org/index.php/FIPS_modules#:%7E:text=The%202.0%20FIPS%20module%20is,2%2C%20and%20no%20others

OpenSSL 3.0 was not yet validated at that time, leaving CSPs with a suboptimal option of running an End of Support software in their FedRAMP environments. Additionally, there are known vulnerabilities in the OpenSSL 1.0.2 cryptographic module which could have been avoided by CSPs running a later version of OpenSSL.[13]

As well as the technical process backlog, an often-underestimated challenge is related to the human capital required to prepare for validation. The precise nature of the material contained within, and the specific process itself present additional challenges to the validation process. The process of preparing the validation package often requires organizations to hire consultants with expert knowledge.[14] Additionally, this skill set is becoming increasingly rare, forcing organizations to compete for an ever-shrinking resource. These structural requirements continue to increase the cost of the validation, increasing the time to market for validated solutions.

NIST reported the backlog for FIPS validation to be roughly nine months in late 2020, and a year later in 2021, with laboratories reporting the same nine-month delay. However, there are currently modules that have been "in process" in various stages of validation for over a year. Additionally, an analysis of the current queue shows that the average time to completion for modules undergoing 140-2 validation is 376 days, and the average time for completion for 140-3 validation was 577 days.[15] Looking at the currently reported in process queue, you will find four statuses, *Review Pending, In Review, Finalization, or Coordination*. The first three status messages are straight forward, and Coordination indicates that the CVMP and the applicant are iterating findings, information, and other items discovered during the testing process. NIST currently acknowledges a significant backlog in the validation process, and encourages use of modules that are currently on the active list.[16] NIST has established a three-to-nine month timeframe for validation completion, but the current queue is four to eight times longer than the established timeframe.

Technology Advances vs. Validation Processes

The speed at which technology advances, and the speed at which vulnerabilities and exploitable threats are discovered, is in direct conflict with the delays in the validation process. In the current state, the mean time from submission to validation is in excess of nine months. A nine-month cycle for validation equals the entire supported time period of a regular release of Ubuntu[17]. In many cases, by the time validation is complete, the underlying operating system and software components have been either patched, updated with a minor revision, or a new major version has been released. This timeline means that validated modules are released effectively with vulnerabilities or defects.

Additionally, supply chain challenges are poised to further complicate the technology ecosystem in a post COVID world. Because FIPS 140 validations are tied to both specific software and *specific hardware*, some vendors are forced to maintain older equipment to ensure that the validation remains in place. In a specific example, certificate #3739 requires that the Cortex ARMv8 processor be utilized.[18] The Cortex-A57 processor was released in 2013 and will be more than a decade old when the validation expires in 2025.

---

13 National Institute of Standards and Technology, *National Vulnerability Database*, accessed May 2023, https://nvd.nist.gov/vuln/search/results?cpe_version=cpe%3A%2Fa%3Aopenssl%3Aopenssl%3A1.0.2k&startIndex=0

14 Corsec, *Decisions in a FIPS 140-2 Validation*, November 27, 2013 https://www.corsec.com/fips-validation-steps/

15 National Institute of Standards and Technology, Cryptographic Module Validation Program, accessed May 2023 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List

16 Ibid.

17 Ubuntu, *The Ubuntu lifecycle and release cadence,* accessed February 2023, https://ubuntu.com/about/release-cycle

18 National Institute of Standards and Technology, Cryptographic Module Validation Program, accessed February 2023 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List

The issues of hardware, software, and hybrid (a combination of both hardware and software) validations provides a fair amount of confusion when evaluating the status of validations. Software only validations, as in the case of OpenSSL, are tested on a representative hardware platform for the process of being able to run the software during the validation. This hardware platform becomes part of the validation description and often leads to some confusion when organizations are ensuring that FIPS 140 validated modules are being utilized[19]. Clearly, the idea of improving clarity when reporting the status of FIPS 140 validated modules is something that can be improved upon and should be part of any improvement in the FIPS validation process.

Recommendations - Addressing the Backlog

Addressing backlog in the validation process is not straightforward. For example, adding more resources to solve supply and demand issues does not provide a sustainable longer-term solution. As such, justification for the backlog is often sought, for example by citing the release of FIPS 140-3 and its impact on the workload of validation labs. Instead, this paper attempts to identify potential opportunities to advance the process of validation through the introduction of new processes or procedures that will shorten the time from submission through validation, thereby providing a sustainable solution.

Looking at the implementation of the Automated Cryptographic Module Validation Program (ACMVP)[20] as a guide, it appears that there are some leverage points within the program to address both the rapid implementation of updates, and the maintenance of validation status. The process of testing components is largely repetitive, which makes it a good candidate for automation. Understanding the nature of the changes is an important part of validating an update to a platform. This concept is already being utilized in the introduction of certain replacement hardware within FIPS 140 validated systems, such as disk drives, and could logically be extended to software components. This may require the decoupling of components and establishing an interface standard between validated components.

Divide and Conquer

The decoupling of components has two avenues for improvement. First, we have the issue of validated hardware platforms that are undergoing updates as technology evolves. This presents a challenge if the validation has stipulations that require certain components to be in place for the validated solution. In the same vein, software that undergoes updates, or patching to resolve vulnerabilities, may affect the status of the validation for that particular solution. As a potential improvement for these scenarios, the components in the critical path for the validated solution could be enumerated, minimizing the impact of hardware or software updates on the validation. As an example of this, establishing hardware equivalence standards would allow vendors to update hardware with updated models and not require an additional validation cycle. A second variation of this concept would be that vendors are permitted to explicitly allow next generation processors to be added to certificates with proven equivalence standards.

Improving Visibility and Facilitating Data Driven Decision Making

In order to improve current budgetary and vendor selection and management challenges, a procedural change is possible that could enable organizations to make decisions with an understanding of what is in the validation queue. In this case, providing information to entities through the queue process regarding

19 National Institute of Standards and Technology, *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program,* accessed February 2023, from https://csrc.nist.rip/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/fips140-2/FIPS1402IG.pdf

20 National Institute of Standards and Technology, *Automation of the NIST Cryptographic Module Validation Program,* accessed February 2023, https://csrc.nist.gov/Projects/Automated-Cryptographic-Validation-Testing

applications for validation, particularly in instances where some component is being updated and the likelihood of passing validation testing is high. This presents an opportunity for the entity themselves to provide some self-testing results, in accordance with an updated guideline, which would enable entities to make implementation and purchase decisions for these “future state” validations. This would require some procedural change, and the establishment of a self-testing standard that would enable this type of reporting. A furthering of this concept would be a roadmap for a standard for interactions between hardware and software components.

Improving the visibility into the process of validation, the status of modules in progress (MIP), and the Scenario in which the module is undergoing revalidation may also assist in understanding the process queues. Understanding that Scenario 1 and 3 validation updates have a shorter time frame, a consumer organization making a purchasing decision may elect to wait for the process to finish before looking for other options.[21] Additionally, integrators who are making decisions on validated solutions that employ validated hardware may elect to incorporate hardware that is on the MIP listings, if this information is available. The provision of this information regarding the queue status does not lessen the security but enables organizations to make informed decisions that will influence their organizations for years to come.

The visibility into the queue and the historical lists are important for organizations on both the vendor and consumer sides of the equation. The following is a proposed order of implementation for certifications of modules for use: (1) Validated modules from the CMVP listing with Active Status; (2) Modules in Process with CMVP that are replacing a module that went historical, with caveats to note that regular updates should be sought to ensure validation completes; (3) Modules in Process with CMVP that are net new, with caveats to note that regular updates should be sought to ensure that the validation completes; (4) Modules on the Historical list, with caveats to ensure support for bug closure from the vendor and settings for disabling the now-deprecated algorithms, key sizes, and primitives that were supported by the module. Primitives include hashing, randomization, and initialization vectors that establish the building blocks of cryptographic solutions.

Integration is an important part of developing a validated solution, so the visibility of the queue is crucial. This integration provides additional opportunities in establishing a standard for interfaces between validated components, possibly making the case where more granular decisions are available. In this case, the industry may have to step back to the concepts of cryptographic primitives. NIST has already started the journey toward the concept of establishing Multi-Party Threshold Cryptography (MPTC).[22] MPTC holds the promise to enable organizations to distribute trust across multiple operators, in order to establish a fault tolerant secrecy. Distribution can ensure that the compromise of some of the parties used in the cryptography will not lead to the compromise of the encryption itself. This may require that the primitives provide mechanisms to provide for distribution, self-testing, trust, and deprecation. Embracing MPTC may address the issues related to an aversion to utilizing cryptographic solutions that are validated by a particular geopolitical entity.

Getting Prepared for the Quantum Age

When considering future proofing, some attention must be paid to FIPS 140 validation in the presence of quantum computing. It is suspected that advances in quantum computing will render current cryptographic standards obsolete. In the current FIPS 140 standard, a module validated in 2024, when the new post-quantum cryptographic standard (PQCS) is published, will be validated until 2029. Naturally, the FIPS

21 Safelogic, *Don't Let Lightning Strike Twice: FIPS 140-2 Re-Validation*, July 2013, https://www.safelogic.com/blog/lightningstrikes

22 National Institute of Standards and Technology, *Multi-Party Threshold Cryptography,* accessed February 2023. https://csrc.nist.gov/Projects/threshold-cryptography/presentations

140 testing methodology is not aligned to test for attacks by a Cryptanalytically-Relevant Quantum Computer (CRQC), one must think that this testing will be the subject for at least an update to the FIPS standards.[23] The NSA has introduced some aggressive timelines for a Commercial National Security Algorithm Suite (CNSA 2.0)[24] to address Post Quantum (PQ) cryptography, but the certification of these will require that CAVP testing be developed and the appropriate implementation guides be developed by vendors, before these can be certified by the CMVP. NIST SP 800-208 has recommended PQ algorithms, but the requisite conformance testing under CAVP and CMVP has not been fully developed.

The White House recently released NSM-10 to address threats to current cryptographic methods from quantum computing. According to NSM-10, a CRQC "will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world." A CRQC, "could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure, and defeat security protocols for most Internet-based financial transactions." Due to this, "Any digital system that uses existing public standards for public-key cryptography, or that is planning to transition to such cryptography, could be vulnerable." The NSM-10 promotes "a balanced approach to technology promotion and protection."[25] Further, it states, "the United States must prioritize the timely and equitable transition of cryptographic systems to quantum-resistant cryptography" and that "central to this migration effort will be an emphasis on cryptographic agility, both to reduce the time required to transition and to allow for seamless updates for future cryptographic standards." As stated in the preceding paragraph, quantum computing is expected to break widely used encryption methods within the decade.

While the use of modern cryptography ought to continue to be enforced, relying solely on FIPS 140 validation for implementing NIST 800-53 controls related to encryption, such as SC-13, becomes an increasingly risky approach versus leveraging the *most advanced* modern cryptography, which will increasingly include quantum-resistant cryptographic algorithms as they gain broader adoption within the information technology space. The latter approach is in line with the spirit of the Revision 5 SC-13 guidance, which clarifies that "moving to non-FIPS CM or product is acceptable when the FIPS validated version has a known vulnerability and a non-FIPS version fixes the vulnerability." A vulnerability which will be exploitable soon is still a vulnerability all the same, especially when one considers the risk from "harvest now, decrypt later" campaigns by nation-state level actors. "Harvest now, decrypt later" campaigns collect and store data encrypted with existing cryptography, anticipating that within a few years, existing encryption algorithms will be able to be decrypted by quantum computers.[26]

Considering the above, it is imperative that commercial organizations implement encryption from a risk-based approach. Such an approach must include the ability for organizations to leverage modern cryptographic modules that better protect them from the latest threats. Similarly, agencies must be empowered to make risk-based decisions when partnering with Cloud Service Offerings.

---

23 National Institute of Standards and Technology, *Post-Quantum Cryptography Standardization,* accessed February 2023, https://csrc.nist.gov/projects/post-quantum-cryptography/post-quantum-cryptography-standardization

24 National Security Agency, *NSA Releases Future Quantum-Resistant (QR) Algorithm Requirements for National Security Systems,* September 07, 2022, https://www.nsa.gov/Press-Room/News-Highlights/Article/Article/3148990/nsa-releases-future-quantum-resistant-qr-algorithm-requirements-for-national-se/

25 The White House, *National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems,* May 04, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/05/04/national-security-memorandum-on-promoting-united-states-leadership-in-quantum-computing-while-mitigating-risks-to-vulnerable-cryptographic-systems/

26 PR Newswire, *Harvest Now, Decrypt Later Attacks Pose a Security Concern as Organizations Consider Implications of Quantum Computing,* September 20, 2022, https://www.prnewswire.com/news-releases/harvest-now-decrypt-later-attacks-pose-a-security-concern-as-organizations-consider-implications-of-quantum-computing-301628445.html

Conclusion

The backlog that exists within the FIPS 140 validation process is not only affecting the vendors ability to bring validated solutions to market but is also affecting the purchasing and budgeting decisions of entities that are required to utilize validated solutions. This paper provides several suggestions for potential relief for an already congested process of validation. While the congestion could potentially be described as the “perfect storm” combination of an update to the validation standard, which forced many modules onto the historical list, it also exacerbated issues related to procurement time to market for many solutions. The importance of FIPS 140 validation is not in question, and in no way is this paper seeking to diminish the critical nature of the process.

As technology continues to evolve, to maintain the critical function of FIPS as the highest standard of security, the validation process will need to establish a more agile solution in order to match the pace of technology growth.

Appendix A – An Overview of FIPS 140

The Federal Information Processing Standard (FIPS) 140 is a U.S. government standard that defines minimum security requirements for cryptographic modules in information technology products and systems. Testing against the FIPS 140 standard is maintained by the Cryptographic Module Validation Program (CMVP), a joint effort between the U.S. National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security, a branch of the Communications Security Establishment (CSE) of Canada.

FIPS 140 is a mandatory standard required for all U.S. federal government agencies that use cryptography-based security systems (hardware, firmware, software, or a combination of those) for the protection of sensitive or valuable data within Federal systems, the standard was initially published as FIPS 140-1 in January 1994 and has been revised twice. The FIPS 140-2 standard, has security requirements covering 11 areas related to the design and implementation of a cryptographic module. Each module has its own security policy — a precise specification of the security rules under which it operates — and employs approved cryptographic algorithms, cryptographic key management, and authentication techniques. For each area, a cryptographic module receives a security level rating 1 to 4 (from lowest to highest, see Table-1) depending on the requirements met. NIST publishes a searchable list of vendors and their cryptographic modules validated for FIPS 140-2.[27]

Table A1 – Summary of Security Requirements

	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, approved security functions, and normal and degraded modes of 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 an approved manner.			
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data 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, or EDC based integrity test. Defined SFMI, HFMI and HSMI. Executable code	Approved digital signature or keyed message authentication code-based integrity test.	Approved digital signature-based integrity test.	
Operational Environment	Non-Modifiable, Limited, or Modifiable. Control of SSPs.	Modifiable. Role-based or discretionary access control. Audit mechanism.		

27 National Institute of Standards and Technology, Cryptographic Module Validation Program, accessed February 2023 https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/Modules-In-Process-List

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. EFP. Fault injection mitigation.
Non-Invasive Security		Module is designed to mitigate against non-invasive attacks specified in Annex F.			
		Documentation and effectiveness of mitigation techniques specified in Annex F.		Mitigation Testing.	Mitigation Testing.
Sensitive 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 either 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.			
Life-Cycle Assurance	**Configuration Management**	Configuration management system for cryptographic module, components, and documentation. Each uniquely identified and tracked throughout lifecycle.		Automated configuration management system.	
	Design	Module designed to allow testing of all provided security related services.			
	FSM	Finite state model.			
	Development	Annotated source code, schematics, or HDL.	Software high-level language. Hardware high-level descriptive language.		Documentation annotated with pre-conditions upon entry into module components and post- conditions expected to be true when components is completed.
	Testing	Functional Testing.		Low-level Testing.	
	Delivery and Operation	Initialization procedures.	Delivery Procedures.		Operator authentication using vendor provided authentication information.
	Guidance	Administrator and non-administrator guidance.			
Mitigation of other attacks		Specification of mitigation of attacks for which no testable requirements are currently available.			Specification of mitigation of attacks with testable requirements.

FIPS 140-3 is an incremental advancement of FIPS 140-2, which now standardizes on the International Organization for Standards (ISO), ISO 19790:2012 and ISO 24759:2017 specifications. Historically, ISO 19790 was based on FIPS 140-2, but the ISO standard has continued to advance since its initial publication. FIPS 140-3 will now point back to ISO 19790 for security requirements and to ISO 24759 for

the testing requirements. Keeping FIPS 140-3 as a separate standard will still allow NIST to mandate additional requirements on top of what the ISO standards contain when needed.

The ISO 19790:2012 standard applies to a wide spectrum of data sensitivity, a diversity of application environments and specifies four security levels, along with the 11 requirement areas. In these security levels, as the level increases from 1 through 4, the security level required increases as well. The standard is specifically intended to maintain the security provided by the cryptographic module. The process of testing these requirements is the subject of another standard, ISO 24759:2017. This standard specifies the methods that are to be utilized by testing laboratories in the testing of requirements. It specifies the requirements for information to be provided to laboratories, and the requirements that must be satisfied prior to the submission of applications to the testing laboratories for validation. ISO 24759 is designed to ensure consistency amongst the testing laboratories and establish to the requirements for the vendors to ensure that the cryptographic modules meet requirements established by ISO 19790.

As part of the validation process, the vendors must include appropriate direction for the implementation of the validated solution. Compliance with the testing standards alone do not ensure that the module or that the security of information protected by that module is at a level that may be sufficient or acceptable to the information owner. Consumers of the validated solutions must ensure their implementation is done in accordance with the Implementation Guides and Security Policies for each validated solution. Proper implementation of validated solutions ensures that the protection of the information is effective and acceptable.

FIPS 140 History

FIPS 140-1, first published in 1994, was developed by a government and an industry working group comprised of both users and vendors. The working group identified requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity and a diversity of application environments. The FIPS standard specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems as defined in Section 5131 of the Information Technology Management Reform Act of 1996, (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

In 2001, when FIPS 140-2 superseded FIPS 140-1, the new standard incorporated changes in applicable standards and technology, as well as changes that were based on comments received from the vendor, laboratory, and user communities. A review of the FIPS 140-2 standard was undertaken after 5 years, in 2007, however, consensus to move toward a revised standard was not achieved until publication of the 2012 revision of International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 19790.

FIPS 140-2 validated modules continue to be valid through 2026, although development to support and validate FIPS 140-3 modules were established and required to be utilized by September 2021, which coincided with the first date in which FIPS 140-3 validation packages were accepted. The transition from FIPS 140-2 to FIPS 140-3 includes organizational, documentation, and procedural changes necessary to update and efficiently manage the increasing list of security products that are tested for use in the US and Canadian governments. Changes also support the migration of internally developed security standards towards a set of standards developed and maintained by ISO, an international body, while also referencing government standards.

FIPS 140-3 became effective September 22, 2019, permitting CMVP to begin accepting validation submissions under the new scheme beginning September 2020. The CMVP continues to validate

cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules for applications received prior to March 31, 2022.

Major changes in FIPS 140-3 testing are limited to the introduction of non-invasive physical requirements, these non-invasive physics attacks are side-channel attacks that exploit weak channels. These types of attacks include attacks through electromagnetic interference or power interference. Non-invasive physical attacks were not previously tested under FIPS 140-2. The new standard introduces some significant procedural changes. Rather than encompassing the module requirements directly, FIPS 140-3 references ISO/IEC 19790:2012. The testing for these requirements will be in accordance with, and as defined by, ISO/IEC 24759:2017. The use of the ISO standard dictates the procedural changes in the management and execution of the validation program and process.

Status of FIPS 140-2

FIPS 140-2 modules can remain active for 5 years after validation or until September 21, 2026, when the FIPS 140-2 validations will be moved to the historical list. Even on the historical list, CMVP supports the use of these modules for existing systems. CMVP recommends that implementers consider all modules that appear on the Validated Modules Search Page and meet their requirements for the best selection of cryptographic modules, regardless of whether the modules are validated against FIPS 140-2 or FIPS 140-3.

FIPS 140-3 aligns the standard with the with ISO/IEC 19790:2012(E) and includes modifications of the Annexes that are allowed to the CMVP as a validation authority. The Annexes provide a list of integral items that are part of the cryptographic process, for example, FIPS 140-2, Annex D, discusses key establishment techniques that have been approved for FIPS validated use. Annexes A-D from FIPS 140-2 have been replaced with NIST SP800-140 A-F. The NIST SP 800-140 annexes define the testing requirements and establish the CVMP requirements in accordance with ISO/IEC 24759:2017(E), and, in the instances of NIST SP800-140 Annexes B and E, additional requirements in ISO 19790 annex B and E respectively.

Transition schedule from FIPS 140-2 to FIPS 140-3

The time of the transition is shown below:

- March 22, 2019: FIPS 140-3 Approved
- September 22, 2019: FIPS 140-3 Effective Date. Drafts of SP 800-140x (Public comment closed 12-9-2019)
- March 20, 2020: Publication of SP 800-140x documents
- May 20, 2020: Updated CMVP Program Management Manual for FIPS 140-2
- July 1, 2020: Tester competency exam updated to include FIPS 140-3
- September 21, 2020: FIPS 140-3 Implementation Guidance, CMVP Management Manual for FIPS 140-3
- September 22, 2020: CMVP accepts FIPS 140-3 submissions
- September 21, 2021: CMVP stops accepting FIPS 140-2 submissions for new validation certificates
- April 1, 2022: CMVP only accepts FIPS 140-2 reports that do not change the validation sunset date, i.e., Scenarios 1, 1A, 3A, 3B, and 4 as defined in FIPS 140-2 Implementation Guidance G.8.
    - These scenarios are specific in that they represent: 1) Changes that do not affect any FIPS 140-2 relevant items, 1A) Only represent the rebranding of an OEM module, 1B) a 1SUB testing of an already validated module with non-security relevant changes, 3A & B)

Less than 30% of the security relevant items of an already validated module can qualify for revalidation, and 4) modifications are made only to the physical enclosure of the validated module.

- September 21, 2026: Remaining FIPS 140-2 certificates are moved to the Historical List

Table A2 - FIPS 140-2 Vs. FIPS 140-3

Specifications	FIPS 140-2	FIPS 140-3
Cryptographic Module	The FIPS 140-2 standard was written with the idea that all modules were hardware modules. Later different types of modules (hybrid, software, and firmware) were added and defined in the IG (IGs 1.9, 1.16 and 1.17).	FIPS 140-3 will include the hardware module, firmware module, software module, hybrid-software module, and hybrid-firmware module
Cryptographic Boundary	FIPS 140-2 IG 1.9 restricted hybrid modules to a FIPS 140-2 Level 1 validation	There is also no restriction as to the level at which a hybrid module may be validated in the new standard.
Roles	The FIPS 140-2 standard (section 4.3.1), requires that a module support both a crypto officer role, and a user role, and the support of a maintenance role was optional.	FIPS 140-3 still has these same three roles, but only the crypto officer role is required (section 7.4.2). The user role and the maintenance role are now optional.
Authentication	**ISO 19790:** Level 1 -no authentication requirements Level 2 – minimum role-based authentication Level 3 – identity-based authentication	**ISO 19790:** FIPS 140-3 is similar to FIPS 140-2 for authentication at security levels 1-3. Level 4 is also added in FIPS 140-3, For level 4 authentication, it must be multi-factor identity based.

Appendix B: Cryptographic Algorithms

FIPS 140 validated Cryptographic Algorithms

A FIPS approved algorithm generally refers to an algorithm or technique that is either specified in a FIPS or NIST recommendation or adopted in a FIPS or NIST recommendation (specified in an appendix or in a document referenced by the FIPS or NIST recommendation). These algorithms must be used by cryptographic modules that are undergoing FIPS validation. A cryptographic module is a set of hardware, software, firmware, or a combination that implements cryptographic functions or processes. The testing of cryptographic algorithms is completed through the Cryptographic Algorithm Validation Program (CAVP). The CAVP maintains a list of FIPS approved and NIST recommended cryptographic algorithms and their individual components. CAVP validation is a prerequisite for CMVP validation.

Table B1: Status of Validated Algorithms

Algorithm	Status
Two-key TDEA Encryption	Disallowed
Two-key TDEA Decryption	Legacy use
Three-key TDEA Encryption	Deprecated through 2023 Disallowed after 2023
Three-key TDEA Decryption	Legacy use
SKIPJACK Encryption	Disallowed
SKIPJACK Decryption	Legacy use
AES-128 Encryption and Decryption	Acceptable
AES-192 Encryption and Decryption	Acceptable
AES-256 Encryption and Decryption	Acceptable

Table B2: Digital Signature Process Status

Digital Signature Process	Status
Digital Signature Generation	
<112 bits of security strength: DSA: (L, N) ≠ (2048, 224), (2048,256) or (3072, 256) ECDSA: len(n) < 224 RSA: len(n) < 2048	Disallowed
≥ 112 bits of security strength: DSA: (L, N) = (2048, 224), (2048,256) or (3072, 256) ECDSA or EdDSA: len(n) ≥ 224 RSA: len(n) ≥ 2048	Acceptable
Digital Signature Verification	
< 112 bits of security strength: DSA32: ((512 ≤ L < 2048) or (160 ≤ N < 224)) ECDSA: 160 ≤ len(n) < 224 RSA: 1024 ≤ len(n) < 2048	Legacy use
≥ 112 bits of security strength: DSA: (L, N) = (2048, 224), (2048,256) or (3072, 256) ECDSA and EdDSA: len(n) ≥ 224 RSA: len(n) ≥ 2048	Acceptable

Table B3: Hash Function Usage

Hash Function	Use
SHA-1	
Digital signature generation	Disallowed, except where specifically allowed by NIST protocol-specific guidance
Digital signature verification	Legacy use
Non-digital signature applications	Acceptable
SHA-2 family (SHA224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)	Acceptable for all hash function applications
SHA-3 family (SHA3-224, SHA3- 256, SHA3-384, and SHA3-512)	Acceptable for all hash function applications
TupleHash and ParallelHash	Acceptable for the purposes specified in **SP 800-185**