

---

# Understanding the Federal Information Processing Standards FIPS 140-3 Validation Process





## Introduction

UL Solutions recognizes the importance that Federal Information Processing Standards (FIPS) 140-3 validation certificates hold for our customers and the vital role that both the Cryptographic Module Validation Program (CMVP) and the FIPS 140-3 requirements have for the U.S. and Canadian governments. There are also organizations in the IT security industry that value the security assurance that comes from the independent expert testing and validation of cryptographic modules against the FIPS 140-3 standard.

FIPS 140 has been around for three decades, with thousands of modules validated through the CMVP. UL Solutions (NVLAP Code 100432-0) has worked with the CMVP since its inception, yielding more than 1,000 validation certificates. We are confident in offering some essential guidance that is valuable for cryptographic module developers and testing laboratories.

This ebook will describe the end-to-end process you will follow when developing and validating cryptographic modules for the U.S. and Canadian governments from the beginning to when you receive your certificate.

Next, we will describe the FIPS 140-3 requirements and answer some questions: Where is everything that comprises the standard? Where can I find the information, and what are the names of the standard publications? What does the standard include that I need to know, and will additional requirements be developed over time?

We will also discuss ways to improve your probability of successfully receiving the validation certificate. Finally, we present lessons we have learned, including some you should know from the beginning.

# Participants in the FIPS 140-3 process

There are four active participants in the FIPS 140 validation process:



Vendor



Laboratory



CMVP



End customer  
(the user of the validated module)

The vendor is the company that designs and produces a product for purchase by the government as a cryptographic module.

The vendor sends what they believe to be a product that complies with the FIPS 140-3 standard to a laboratory. The laboratory's job is to test and verify that the module meets the standard and provide test reports to the CMVP.

The CMVP, joined by the Cryptographic Algorithm Validation Program (CAVP), is run by the U.S. National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS). NIST is also responsible for maintaining the cryptography standards and testing against those standards according to U.S. law, i.e., the Federal Information Security Management Act (FISMA).

The CMVP is responsible for reviewing and approving all cryptographic modules maintained in a validation list. This list is updated when modules successfully receive a FIPS 140-2/140-3 certificate number or when updates to an existing certificate are approved.

The final participant is the end user of the validated module. This organization or government agency specifies and procures validated cryptographic modules. For procurement and deployment, they verify that the versions in use match the identical versions posted on the CMVP website and the published security policies for those products.

## The FIPS 140-3 validation process – preparation

There are some essential elements you need to take care of to get ready, and the first is getting educated about the FIPS 140-3 standard itself. You can do that with self-training, and there are also educational workshops to help people quickly learn the standard.

Build funds into your budget to pay a laboratory to test your module and NIST for the certification. Just as important is your staffing budget for the validation project and various milestones. Some laboratories may have multiple milestones that can occur in parallel and simultaneously. Do you, as a vendor, have the resources to facilitate and take advantage of parallel processes to speed up testing?

Compliance consulting is valuable in helping vendors understand the standard's requirements and how they apply to their products. Most laboratories and other individual consulting agencies offer such consulting. This service can help reduce the burden on vendors, who would otherwise need to spend substantial time researching the requirements.

The most critical preparation is understanding your customers' needs. Make sure you know the FIPS 140-3 security level (1, 2, 3 or 4) your product's end users require.



There is an essential distinction between the security level (1, 2, 3 or 4) and the FIPS 140 version (140-1, 140-2 or 140-3). A greater security level indicates higher security assurance. The version numbers increment over the history of the standard. It started with FIPS 140-1, which was replaced by FIPS 140-2 and, in turn, FIPS 140-2 was replaced by FIPS 140-3 — the current version of the standard.



## Important milestones

There are several important milestones — vendor-laboratory partner milestones, laboratory milestones and CMVP milestones.

### Important milestones

The vendor creates a documentation package that includes a security policy and other evidence backing the vendor's claim of compliance. The vendor requirements — abbreviated as "VEs" in the standard — are found in the SP 800-140 Derived Test Requirements and ISO/IEC 24759:2017. The vendor submits the documentation to the laboratory to be reviewed and to ensure that it is accurate and complete. There is also Entropy Source Validation (ESV), algorithm testing, and physical security testing (for hardware modules).

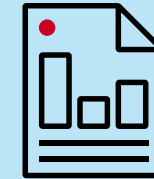
After those milestones are complete, there is a guided source code review where the vendor and laboratory work together to analyze the source code to ensure that it meets all the applicable requirements. Finally, the module undergoes operational/functional testing.

### Laboratory milestones

Once joint testing is complete, the laboratory prepares a validation test report and physical security test report (where applicable) for submittal, along with the security policy and other pertinent documentation, to the CMVP.

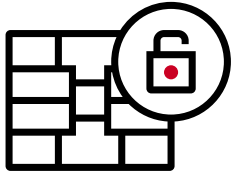
### CMVP milestones

The CMVP publishes the following status milestones on the Modules in Process (MIP) list on the CMVP website. The first milestone is the Review Pending phase, which can seem lengthy at four to nine months in duration. Next is the In Review phase, in which assigned reviewers evaluate the test documents. Then comes the Coordination phase between the laboratory and the CMVP. This is where comments, questions and answers are worked out until the CMVP agrees that the module complies. After the Finalization phase, the module information is posted to the CMVP website along with the published security policy.



## What comprises the FIPS 140-3 standard?

- ISO/IEC 19790:2012/Cor 1:2015, Information Technology – Security Techniques – Security Requirements for Cryptographic Modules
- ISO/IEC 24759:2017, Information Technology – Security Techniques – Test Requirements for Cryptographic Modules – includes vendor and tester evidence
- NIST FIPS 140-3 publications
- NIST FIPS cryptographic algorithms
- NIST special publications – A specific subset of guidance and requirements from the 800 series



## FIPS 140-3 publications

FIPS 140-3 Security Requirements for Cryptographic Modules covers ISO/IEC standards 19790 and 24759.

### **FIPS 140-3 special publications**

SP 800-140 – Derived Test Requirements (DTR)

The following documents correspond directly to ISO/IEC 19790 standard Annexes A through F.

- SP 800-140A – Documentation
- SP 800-140B – Security policy
- SP 800-140C – Approved security functions
- SP 800-140D – Key generation and establishment
- SP 800-140E – Approved authentication mechanisms
- SP 800-140F – Non-invasive attack mitigation



# FIPS 140-3 approved algorithms

## FIPS publications – Cryptographic algorithm standards

- FIPS 180-4 – Secure Hash Standard (SHS) (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512, SHA-512/224 and SHA-512/256)
- FIPS 186-4 – Digital Signature Standard (DSS) (DSA, RSA and ECDSA)
- FIPS 197 – Advanced Encryption Standard (AES)
- FIPS 198-1 – Keyed-Hash Message Authentication Code (HMAC)
- FIPS 202 – SHA-3
  - Standard (SHA3-224, SHA3-256, SHA3-384 and SHA3-512)
  - Extendable-output functions (XOF) (SHAKE128 and SHAKE256)
  - Derived functions (cSHAKE, TupleHash and ParallelHash)

## Block ciphers – AES and triple-DES

- SP 800-38A – Block cipher modes of operation
- SP 800-38A addendum – Ciphertext stealing for CBC mode
- SP 800-38B – CMAC
- SP 800-38C – CCM
- SP 800-38D – GCM and GMAC
- SP 800-38E – XTS-AES
- SP 800-38F – Methods for key wrapping
- SP 800-38G – Format-preserving encryption
- SP 800-67 Rev.2 – Triple-DES encryption algorithm (TDEA)
- IEEE 802.1AEbw-2013 – Media access control (MAC)

## Digital signature

- FIPS 186-4 – Digital Signature Standard (DSS) (DSA, RSA, ECDSA)
- SP 800-208 – Stateful hash-based signature schemes (LMS, HSS, XMSS, XMSSMT)

## Secure hash algorithms

- SP 800-185 – SHA-3 derived functions (cSHAKE, KMAC, TupleHash and ParallelHash)
- SP 800-107 Rev.1 – Applications using approved hash algorithms

## Random bit generators

- SP 800-90A Rev.1 – Deterministic random bit generator (DRBG)
- SP 800-90B – Entropy source

## Key agreement

- SP 800-56A Rev. 3 – Pair-wise key-establishment schemes using discrete logarithm
- SP 800-56B Rev. 2 – Pair-wise key-establishment schemes using integer factorization

## Key derivation and generation

- SP 800-56C Rev.2 – Key-derivation methods in key-establishment schemes
- SP 800-108 – Key-based key derivation using pseudorandom functions
- SP 800-132 – Password-based key derivation (PBKDF)
- SP 800-135 Rev.1 – Application-specific key derivation functions
- SP 800-133 Rev. 2 – Key generation
- IETF RFC 8446 – Transport Layer Security (TLS) Protocol Version 1.3, Section 7.1

## Other sensitive security parameter establishment methods

FIPS 140-3 – Implementation Guidance (IG), Section D.A

## Cryptographic algorithm transitions

SP 800-131Ar2 – Describes the life cycle for various cryptographic algorithms, when they expire, when they are deprecated and when they fall into disuse



## Critical items not readily apparent from the FIPS 140 standard

You will not find some things in the standard itself, the additional requirements or special publications. The CMVP provides additional documentation on the NIST website to fill in the gaps. Specifically, there could be some surprises if you do not stay closely connected with NIST regarding FIPS 140-3 implementation guidance (IG).

### **IG draft reviews**

The IG document released by the CMVP provides programmatic guidance and clarifications on ISO/IEC 24759:2017(E) and FIPS PUB 140-3, Derived Test Requirements. The guidance in this living document stems from NIST and CCCS answers to questions from Cryptographic and Security Testing (CST) laboratories, vendors, and other organizations/individuals. The CMVP publishes IG drafts before publishing the final version. Reading the IG drafts will help you stay ahead of the publications and understand new requirements. Also, during the draft review phase, communicate any comments and questions so the CMVP can act on your feedback. The CMVP does not want to be surprised any more than you do, so they like to keep an open flow of information.

### **Special publication draft reviews**

Similarly, there are opportunities to review the drafts of NIST special publications and algorithm transitions, which are updated periodically.

### **CAVP frequently asked questions (FAQ) document**

The CAVP FAQ is a compilation of frequently asked questions from the cryptographic security testing laboratories about validating

cryptographic algorithm implementations. This document has critical information about obtaining your algorithm certificates.

### **CMVP management manual**

This manual is for the laboratories and the CMVP, but you should also read it. It provides the CMVP and laboratories' perspectives and can help you understand the activities of the validation process so you can ensure that you meet the FIPS 140-3 standard requirements. Knowing this information in advance will make it easier for you to move through the process.

### **NIST handbook 150-17e2022**

Like the management manual, this handbook provides guidance for the accreditation of laboratories by NIST. It describes rules, procedures, organizations and how NIST operates. Annex G is significant because it is about automated cryptographic validation testing (ACVT). You can help facilitate the process when you understand what is expected of the accredited laboratories. Similarly, Annex H has information about entropy source validation (ESV), which is a mandatory testing program for compliance with SP 800-90B.






## Increase your probability of success

Here are some suggestions to help improve your probability of successfully receiving a validation certificate:

- Ask the laboratory and consultants questions early in the process before the formal validation starts. You will likely save more time and money the more questions you get answered early on.
- Learn about compliance issues as early as possible in the validation process. Finding compliance issues during source code review or with operational testing can get expensive in terms of time and money.
- Eliminate any areas of uncertainty that you may have regarding the module's implementation and its compliance with the standard. You can do this by making sure you have a clear understanding of the FIPS 140-3 requirements and which ones apply to your module, as well as documenting the details about how your module meets those requirements. As you do so, assume nothing. Proceeding with an assumption that turns out to be incorrect can prove extremely costly. Ask questions and get definitive answers. You must be sure the module meets every applicable requirement to be able to make a strong assertion and present your supporting vendor evidence to the laboratory to verify it.



- 
- Treat standards compliance as a design objective rather than trying to see what you can get away with after your product has shipped. Although it is possible to validate a product that has already shipped, it will be much harder and much more expensive to try to do it that way. It is more difficult to bring something into compliance after the fact than initially designing it with the proper security compliance in mind from the product's inception.
  - Keep a close eye on changes made to the CMVP program; do not rely on the laboratories to do this for you. You have the best understanding of how changes would impact your product life cycle — more than test laboratories do — so keep track of any changes by regularly monitoring the NIST website.
  - Attend the annual International Cryptographic Modules Conference (ICMC), especially for their speaker track about certification programs. NIST, CMVP and CCCS organizations generally present these. If you can't attend the ICMC in person, consider watching the video presentations after the event.
  - Become an active member of the Cryptographic Module Users Forum (CMUF), a monthly consortium of vendors and laboratories, with participation from the CMVP. There, you will gain insight into other vendors' experiences and from different laboratories, and you'll have an opportunity to provide input on NIST programmatic updates. It's an excellent place for Q&As with other vendors. The CMUF has monthly conference calls and steering committees for special interest work groups (SIGs). The entropy SIG is a popular group.
  - Finally, if, after research and consulting, you still have questions about compliance with the standard, ask your laboratory to submit a request for guidance (RQFG) to NIST if necessary. NIST is responsive to such requests.



## Lessons learned

Finally, here are lessons we have learned (some of them the hard way) from our FIPS experience:

- Provide input to the CMVP before decisions have been finalized and published. Once something is completed and published as a standard, as a special publication or as IG, it is challenging to change them or reverse the decisions. Refrain from debating about changes to cryptographic algorithm standards that NIST has already published.
- Set your management's expectations about accelerating the CMVP queue time (Review Pending phase). The queue time is when you are waiting in line for four to nine months for a reviewer to be assigned to you. That queue time is a function of how many modules are in validation and how many reviewers are available to the CMVP, which can prove challenging for the project manager and management. It is not possible to affect the queue time; it is entirely outside the vendor and laboratory's control. Planning and setting expectations for this time in the queue can help ease frustrations.
- Stay connected with the MIP list or your laboratory to learn how long modules have been in the CMVP queue because laboratories can observe patterns that aren't necessarily apparent to vendors. The laboratories track when modules are submitted and when the CMVP returns comments.
- Consider outsourcing items like algorithm testing harness coding. Consider focusing your highly compensated cryptographers on cryptographic modules instead of working on things that a developer can handle at a lower cost — for example, writing a JSON parser for an algorithm test file format.
- Automate operational testing as much as possible before you reach the actual operational testing event. This is particularly important if you will be testing more than one module. Each operational environment must undergo thorough testing, so you will likely increase the speed and decrease the cost of test labor by automating the tests.
- Write and maintain a source code review plan describing how you will demonstrate your source code files, function names and a list of which requirements are being met. Remember that there is natural turnover in the laboratory and in your organization. Consequently, a written plan is necessary to help ensure the shortest time to market for your module in future validations. The same should be helpful in your operational test plan. Document all the requirements and how you will test to those requirements.

# What differentiates UL Solutions from other laboratories?

## Proven history

Following its inception in 1993, InfoGard was the first private IT security laboratory accredited by NIST, and completed the first FIPS 140-1 Security Level 4 validation. UL Solutions acquired InfoGard in 2015. We have completed more than 1,000 cryptographic module validations. With our history and resources, we should be a top choice as your laboratory partner.

## Prevalidation services

Before the validation phase of the process, UL Solutions provides workshops, compliance consulting and training services that are vital for vendors delivering a cryptographic module to any laboratory for FIPS 140-3 validation.

- **Product profile workshop** – In this workshop, you work with our compliance experts to understand the FIPS 140-3 requirements and review your product against the 12 areas of the FIPS 140-3 standard, section by section. A product profile report is a deliverable that provides specific status and guidance concerning a cryptographic module's readiness for formal validation. Compliance issues found in the product during the workshop, if any, are identified for the vendor to resolve. If you have previously completed a FIPS 140-2 validation,

we can provide this workshop as a gap analysis to the new FIPS 140-3 requirements in which we identify the applicable changes to the standard that impact the module's compliance.

- **Documentation workshop** – Vendor-provided documentation is evidence that must meet the standard requirements. You must also present a security policy that complies with the required CMVP content and format. We can help you draft the security policy, a compliance summary, the finite state model and configuration management information. We will also introduce you to the templates and forms we provide for algorithm testing, source code review and operational testing.
- **Compliance consulting** – You may have further questions once you complete our workshops. Our compliance consulting will help bridge that knowledge gap and is particularly useful for anyone new to the validation process.
- **Entropy source consulting** – We often see vendors struggle when preparing entropy source documentation as evidence ready for validation. It is a new and complicated process that can require the expertise of someone with a postgraduate degree in mathematics or statistics. UL Solutions has employees and partners who can help guide you toward success.

## Proven processes

Given that we have been testing modules for decades, we have built an optimized and proven process comprising multiple teams to accomplish the following milestones:

- Algorithm testing
- Documentation review
- Entropy source validation
- Physical security testing
- Source code review
- Operational testing

We typically have four teams working concurrently on a given project, thus optimizing the process to reduce time to market.



## Conclusion

You now have a better idea of the process to follow when developing and validating cryptographic modules. We have listed all the FIPS 140-3 standard publications with their attendant standards for approved cryptographic algorithms. We have shared ways to improve the probability of success as well as some lessons learned.

Finally, UL Solutions has proven to be a leading laboratory since the inception of the FIPS 140 standard. Having validated more than 1,000 cryptographic modules using a refined process over several decades of experience, UL Solutions is uniquely positioned with the services and resources that can help you succeed in testing and certifying your products.

[BACK TO THE FIRST PAGE](#)



[UL.com/FIPS](https://www.ul.com/FIPS)

© 2023 UL LLC. All Rights Reserved.

The policies and third-party statements presented here are those of the corresponding third party, and are not necessarily those of UL Solutions.

IMS22CS573983  
060.01.0523.EN.CYB