National Institute of Standards and Technology
U.S. Department of Commerce

FIPS 140-3 Validation

Timothy A. Hall
Computer Security Division, Information Technology Lab
National Institute of Standards and Technology (NIST)

FIPS 140 Introduction

- FIPS 140 “Security Requirements for Cryptographic Modules”

- If a US Federal agency specifies that Controlled Unclassified Information (CUI) needs to be cryptographically protected, then it must use a FIPS 140 validated module.

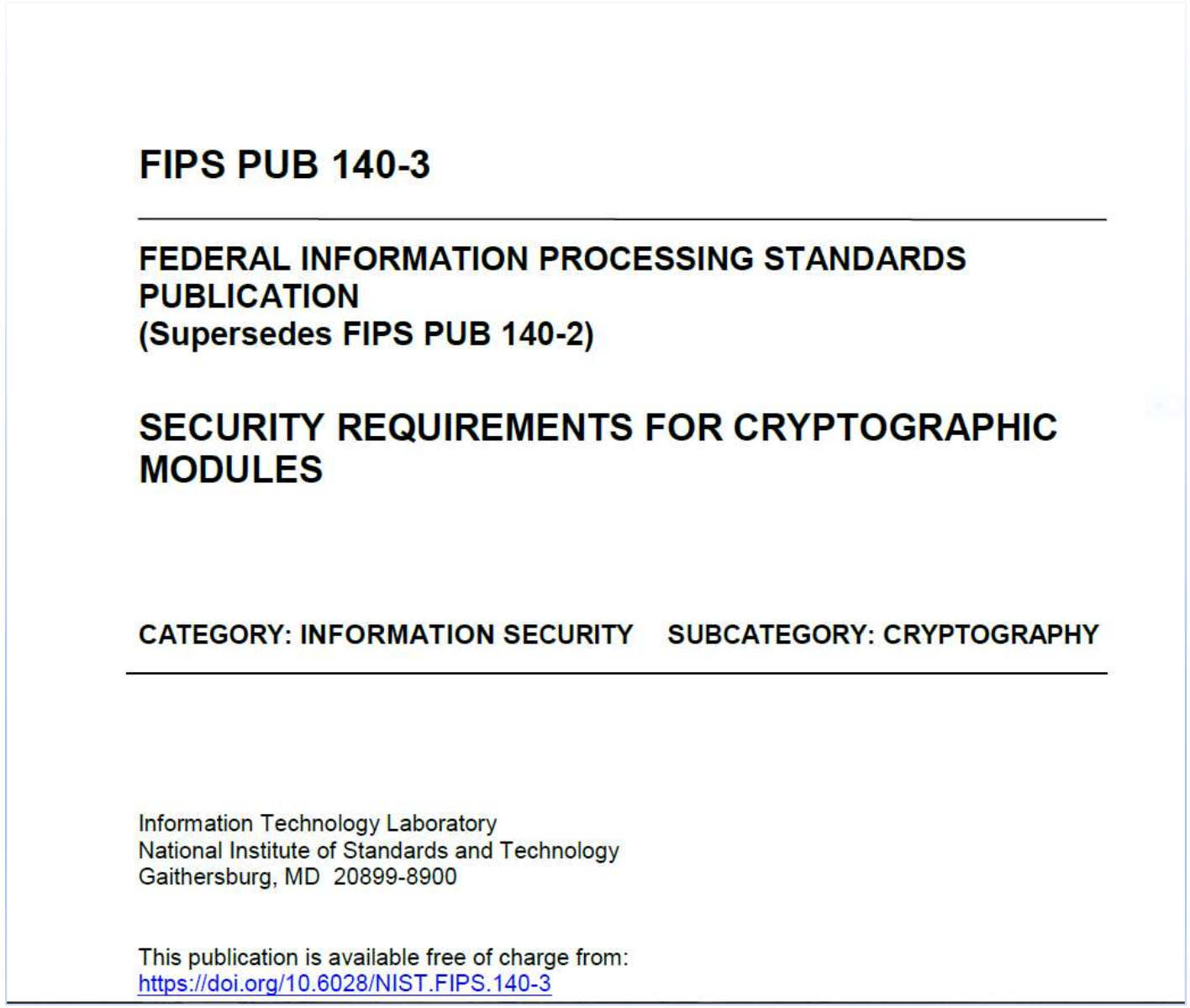
- A cryptographic module is any software, hardware, hybrid, system, etc. that has at least one approved security function, e.g., AES-CBC, HMAC SHA2-256, ECDSA, PBKDF.

- The Cryptographic Module Validation Program (CMVP), a joint effort between NIST (US) and CCCS (Canada), is the validation authority for FIPS 140

- FIPS 140 first published in 1994; CMVP established in 1995

- FIPS 140-3 (2019) is current version

FIPS 140-3



FIPS PUB 140-3

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

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: INFORMATION SECURITY SUBCATEGORY: CRYPTOGRAPHY

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

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

FIPS 140-3 and NIST SP 800-140 series

FIPS 140-3 modifies *ISO/IEC 19790* "Security Requirements for Cryptographic Modules"

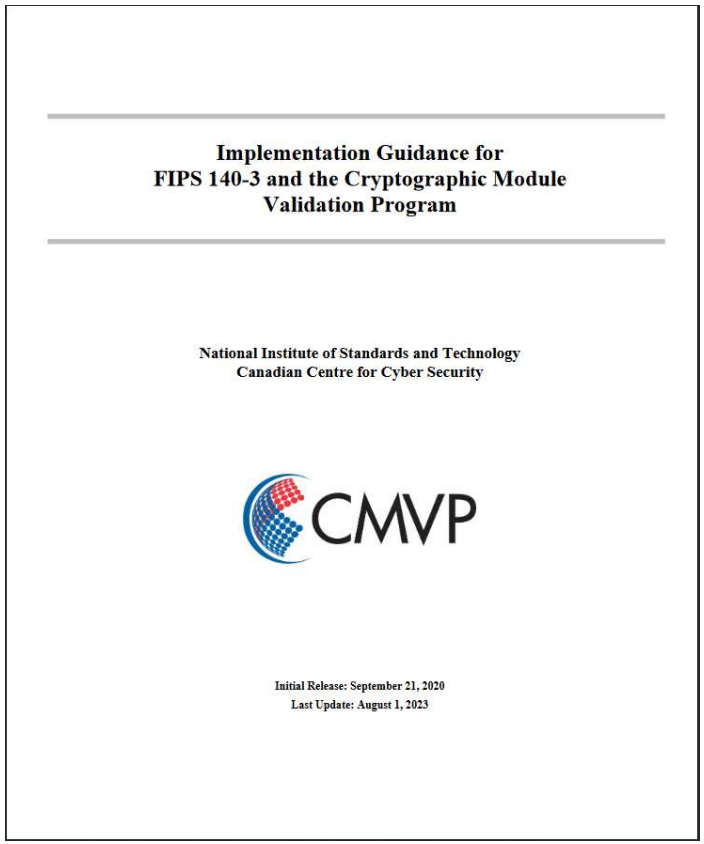
NIST SP 800-140 Series:

- SP 800-140 "Derived Test Requirements (DTR): CMVP Validation Authority Updates to *ISO/IEC 24759*"
- SP 800-140A, B: Requirements for *documentation*, *security policy*
- SP 800-140C, D: Approved *security functions*, *SSP generation and establishment* methods
- SP 800-140E: Approved *authentication methods*
- SP 800-140F: Approved Non-Invasive Attack Mitigation Test Metrics

Security Requirements (from DTR)

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-140.pdf , Table of Contents

Implementation Guidance (IG)

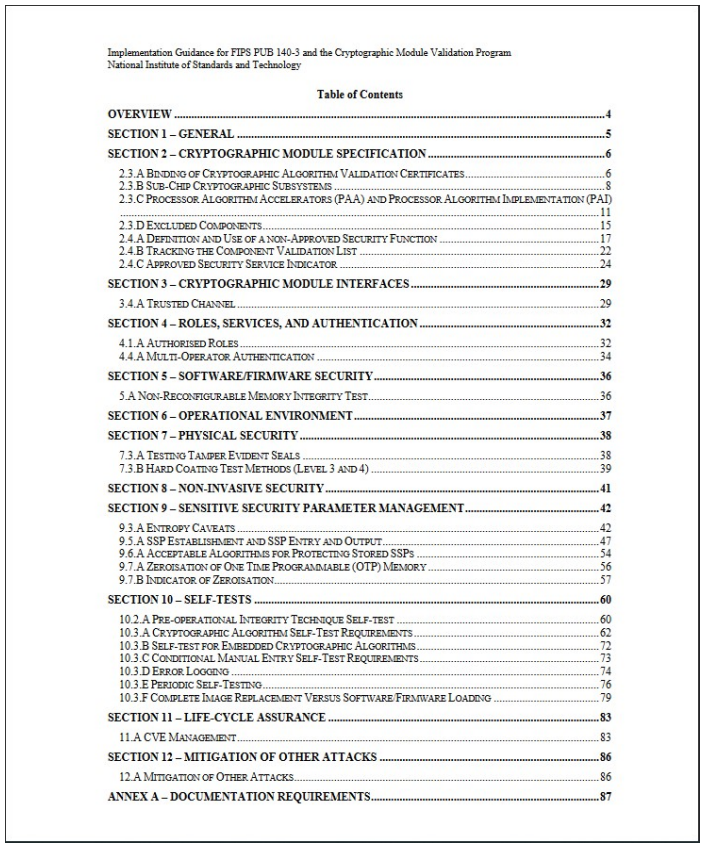


Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program

National Institute of Standards and Technology
Canadian Centre for Cyber Security

CMVP

Initial Release: September 21, 2020
Last Update: August 1, 2023

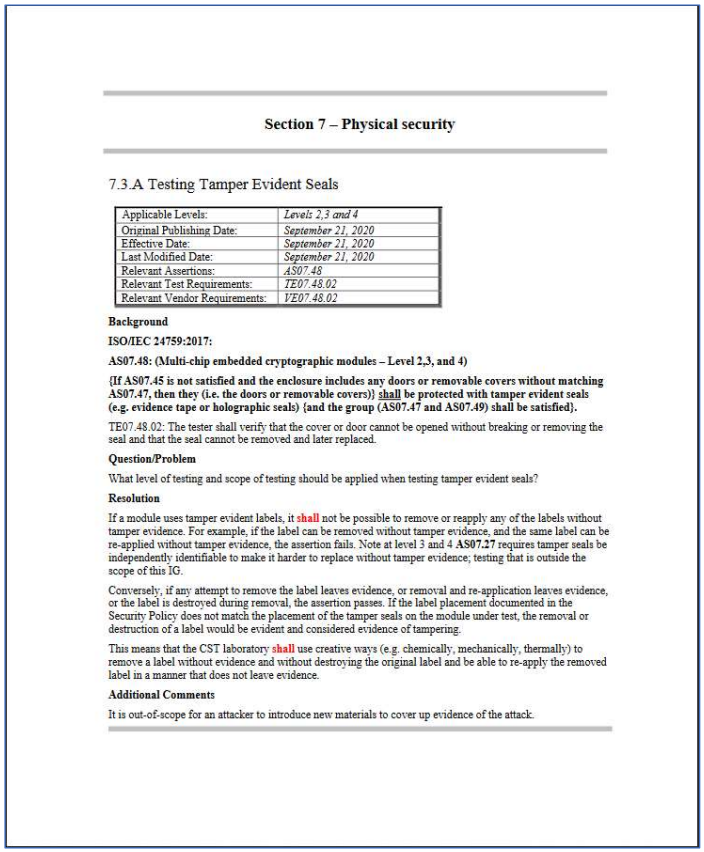


Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program
National Institute of Standards and Technology

Table of Contents

https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf

Implementation Guidance (IG) Examples



Section 7 – Physical security

7.3.A Testing Tamper Evident Seals

Applicable Levels:	*Levels 2,3 and 4*
Original Publishing Date:	*September 21, 2020*
Effective Date:	*September 21, 2020*
Last Modified Date:	*September 21, 2020*
Relevant Assertions:	*AS07.48*
Relevant Test Requirements:	*TE07.48.02*
Relevant Vendor Requirements:	*VE07.48.02*

Background

ISO/IEC 24759:2017:

AS07.48: (Multi-chip embedded cryptographic modules – Level 2,3, and 4)

{If AS07.45 is not satisfied and the enclosure includes any doors or removable covers without matching AS07.47, then they (i.e. the doors or removable covers)} shall be protected with tamper evident seals (e.g. evidence tape or holographic seals) {and the group (AS07.47 and AS07.49) shall be satisfied}.

TE07.48.02: The tester shall verify that the cover or door cannot be opened without breaking or removing the seal and that the seal cannot be removed and later replaced.

Question/Problem

What level of testing and scope of testing should be applied when testing tamper evident seals?

Resolution

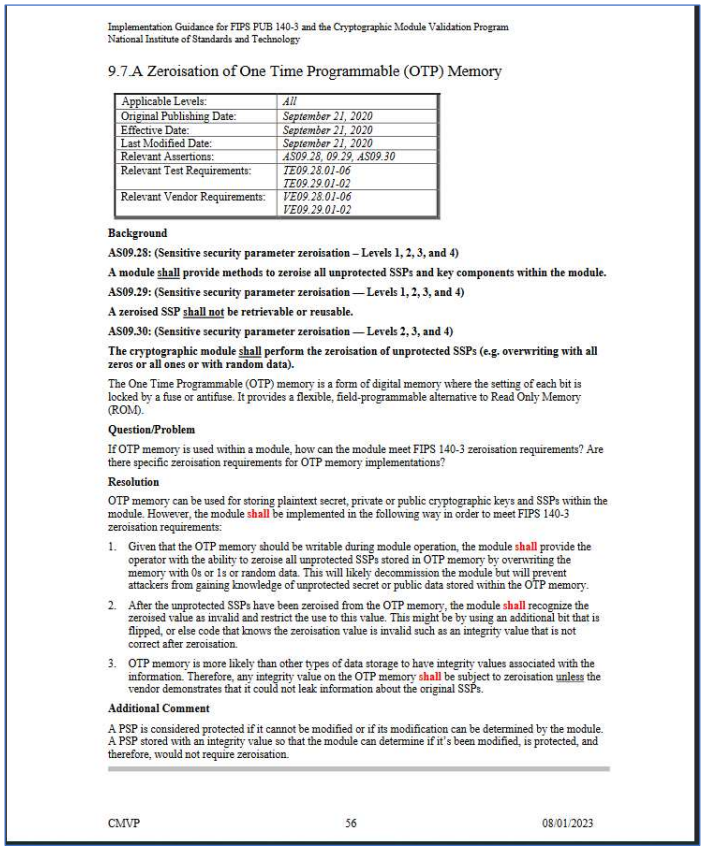
If a module uses tamper evident labels, it **shall** not be possible to remove or reapply any of the labels without tamper evidence. For example, if the label can be removed without tamper evidence, and the same label can be re-applied without tamper evidence, the assertion fails. Note at level 3 and 4 **AS07.27** requires tamper seals be independently identifiable to make it harder to replace without tamper evidence; testing that is outside the scope of this IG.

Conversely, if any attempt to remove the label leaves evidence, or removal and re-application leaves evidence, or the label is destroyed during removal, the assertion passes. If the label placement documented in the Security Policy does not match the placement of the tamper seals on the module under test, the removal or destruction of a label would be evident and considered evidence of tampering.

This means that the CST laboratory **shall** use creative ways (e.g. chemically, mechanically, thermally) to remove a label without evidence and without destroying the original label and be able to re-apply the removed label in a manner that does not leave evidence.

Additional Comments

It is out-of-scope for an attacker to introduce new materials to cover up evidence of the attack.



9.7.A Zeroisation of One Time Programmable (OTP) Memory

Applicable Levels:	*All*
Original Publishing Date:	*September 21, 2020*
Effective Date:	*September 21, 2020*
Last Modified Date:	*September 21, 2020*
Relevant Assertions:	*AS09.28, 09.29, AS09.30*
Relevant Test Requirements:	*TE09.28.01-06* *TE09.29.01-02*
Relevant Vendor Requirements:	*VE09.28.01-06* *VE09.29.01-02*

Background

AS09.28: (Sensitive security parameter zeroisation – Levels 1, 2, 3, and 4)

A module shall provide methods to zeroise all unprotected SSPs and key components within the module.

AS09.29: (Sensitive security parameter zeroisation — Levels 1, 2, 3, and 4)

A zeroised SSP shall not be retrievable or reusable.

AS09.30: (Sensitive security parameter zeroisation — Levels 2, 3, and 4)

The cryptographic module shall perform the zeroisation of unprotected SSPs (e.g. overwriting with all zeros or all ones or with random data).

The One Time Programmable (OTP) memory is a form of digital memory where the setting of each bit is locked by a fuse or antifuse. It provides a flexible, field-programmable alternative to Read Only Memory (ROM).

Question/Problem

If OTP memory is used within a module, how can the module meet FIPS 140-3 zeroisation requirements? Are there specific zeroisation requirements for OTP memory implementations?

Resolution

OTP memory can be used for storing plaintext secret, private or public cryptographic keys and SSPs within the module. However, the module **shall** be implemented in the following way in order to meet FIPS 140-3 zeroisation requirements:

1. Given that the OTP memory should be writable during module operation, the module **shall** provide the operator with the ability to zeroise all unprotected SSPs stored in OTP memory by overwriting the memory with 0s or 1s or random data. This will likely decommission the module but will prevent attackers from gaining knowledge of unprotected secret or public data stored within the OTP memory.
2. After the unprotected SSPs have been zeroised from the OTP memory, the module **shall** recognize the zeroised value as invalid and restrict the use to this value. This might be by using an additional bit that is flipped, or else code that knows the zeroisation value is invalid such as an integrity value that is not correct after zeroisation.
3. OTP memory is more likely than other types of data storage to have integrity values associated with the information. Therefore, any integrity value on the OTP memory **shall** be subject to zeroisation unless the vendor demonstrates that it could not leak information about the original SSPs.

Additional Comment

A PSP is considered protected if it cannot be modified or if its modification can be determined by the module. A PSP stored with an integrity value so that the module can determine if it's been modified, is protected, and therefore, would not require zeroisation.

https://csrc.nist.gov/CSRC/media/Projects/cryptographic-module-validation-program/documents/fips%20140-3/FIPS%20140-3%20IG.pdf , IG 7.3.A, IG 9.7

FIPS 140-3 Transition

Transition Schedule

Updated - 06-02-2021

Date	Activity
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	Released FIPS 140-3 Implementation Guidance Released CMVP Management Manual for FIPS 140-3
September 22, 2020	CMVP accepted FIPS 140-3 submissions
September 22, 2021	*CMVP no longer accepts FIPS 140-2 submissions for new validation certificates unless the vendor is under contract with a CSTL prior to June 15, 2021, the CSTL has submitted an extension request, and the CSTL has received acceptance by the CMVP.* *The CMVP continues to accept FIPS 140-2 reports that do not change the validation sunset date, i.e. Scenarios 1, 1A, 1B, 3A, 3B and 4 from FIPS 140-2 Implementation Guidance G.8.*
April 1, 2022	*CMVP no longer accepts FIPS 140-2 submissions for new validation certificates.*
September 22, 2026	*All FIPS 140-2 certificates are placed on the Historical List*

https://csrc.nist.gov/projects/fips-140-3-transition-effort

FIPS 140-3 Validation

- CMVP is the FIPS 140-3 Validation Authority
- National Voluntary Laboratory Accreditation Program (NVLAP)
  - 20+ international (N. America, Europe, Asia, Australia) accredited testing laboratories
- Supporting programs and activities
  - Cryptographic Algorithm Validation Program (CAVP)
  - Entropy Source Validation (ESV) Testing
- Implementations Under Test (IUTs), Modules in Process (MIPs) and validation certificates posted on NIST CSRC website

Cryptographic Module Validation Program

- **CMVP is joint program between NIST and the Canadian Centre for Cyber Security (CCCS)**
- Validation consists of conformance testing to FIPS 140 "Security Requirements of Cryptographic Modules"

A cryptographic module is any software, hardware, hybrid, system, etc. that has at least one approved security function (cryptographic algorithm), such as encryption, authentication, digital signatures, key exchange

Vendors, Labs, and CMVP

- Vendors of cryptographic modules use independent, **NVLAP-accredited Cryptographic and Security Testing (CST) laboratories** to test their modules. Over 20 labs worldwide.
- CST laboratories use the Derived Test Requirements (DTR), Implementation Guidance (IG) and other CMVP programmatic guidance to test conformance against FIPS 140.
- FIPS 140-3 and NIST SP 800-140 modify ISO/IEC 19790 and ISO/IEC 24759.

Cryptographic Algorithm Validation Program

Automated Cryptographic Validation Testing System (ACVTS) provides automated validation testing of Approved security functions and sensitive security parameter generation and establishment methods.

ACVTS Prod used by accredited labs to conduct validation testing.

ACVTS Demo is a sandbox-style environment for labs, vendors and other users to test implementations at any stage of development cycle.

Approved (i.e, FIPS-approved and NIST Recommended) security functions and SSP generation and establishment methods for FIPS 140-3 are found in SP 800-140Cr1 and SP 800-140Dr1.

- Over 1 M vector sets served between Demo and Prod.
- Testing for draft publications available on Demo
- ACVT scope open to first party test labs.
- Source code at https://github.com/usnistgov/ACVP-Server

Entropy Source Validation Testing

Entropy Source Validation Testing (ESVT) is part of the CMVP but decouples entropy source validation from module validation.

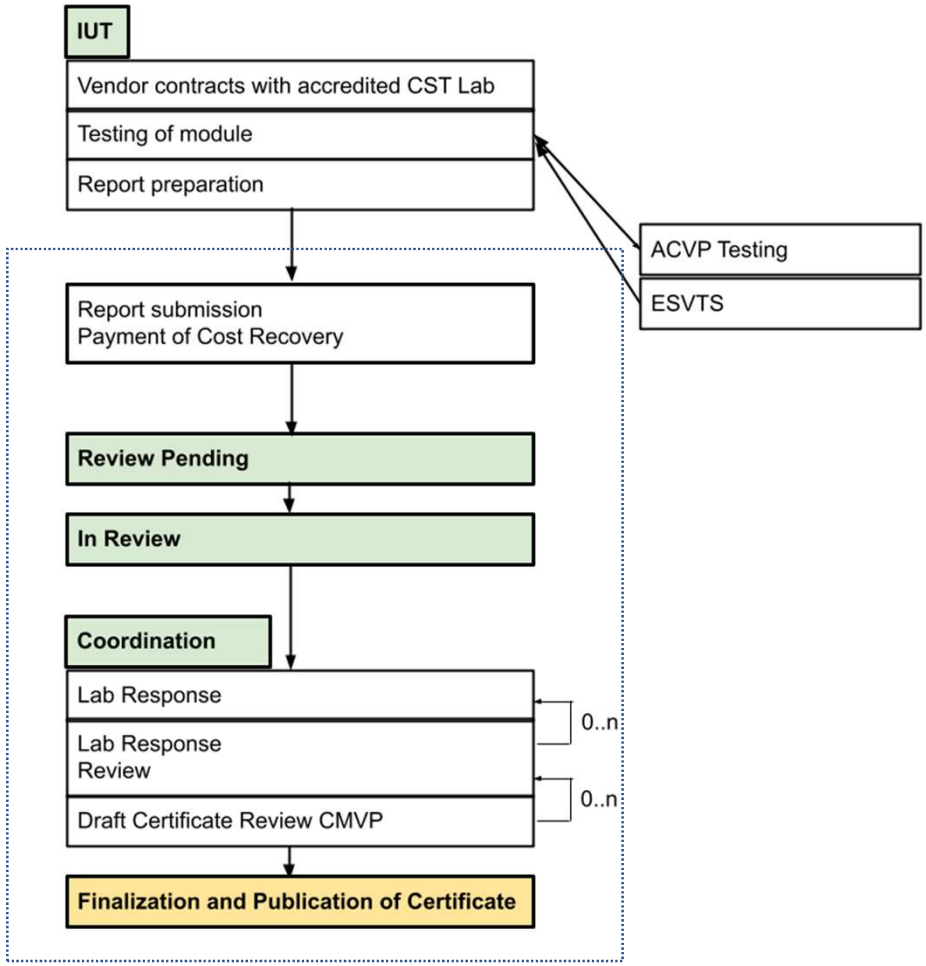
ESVTS (ESV Testing System) processes submission of entropy reports. Runs SP 800-90B entropy estimators on submitted raw noise, restart test and conditioned samples.

NIST SP 800-90B "Recommendation for the Entropy Sources Used for Random Bit Generation"

- Reference ESV Cert in similar manner to CAVP Certs.
- First ESV Certificate (E1) issued 29 Aug 2022.
- Separate validation scope (17ESV) in process.

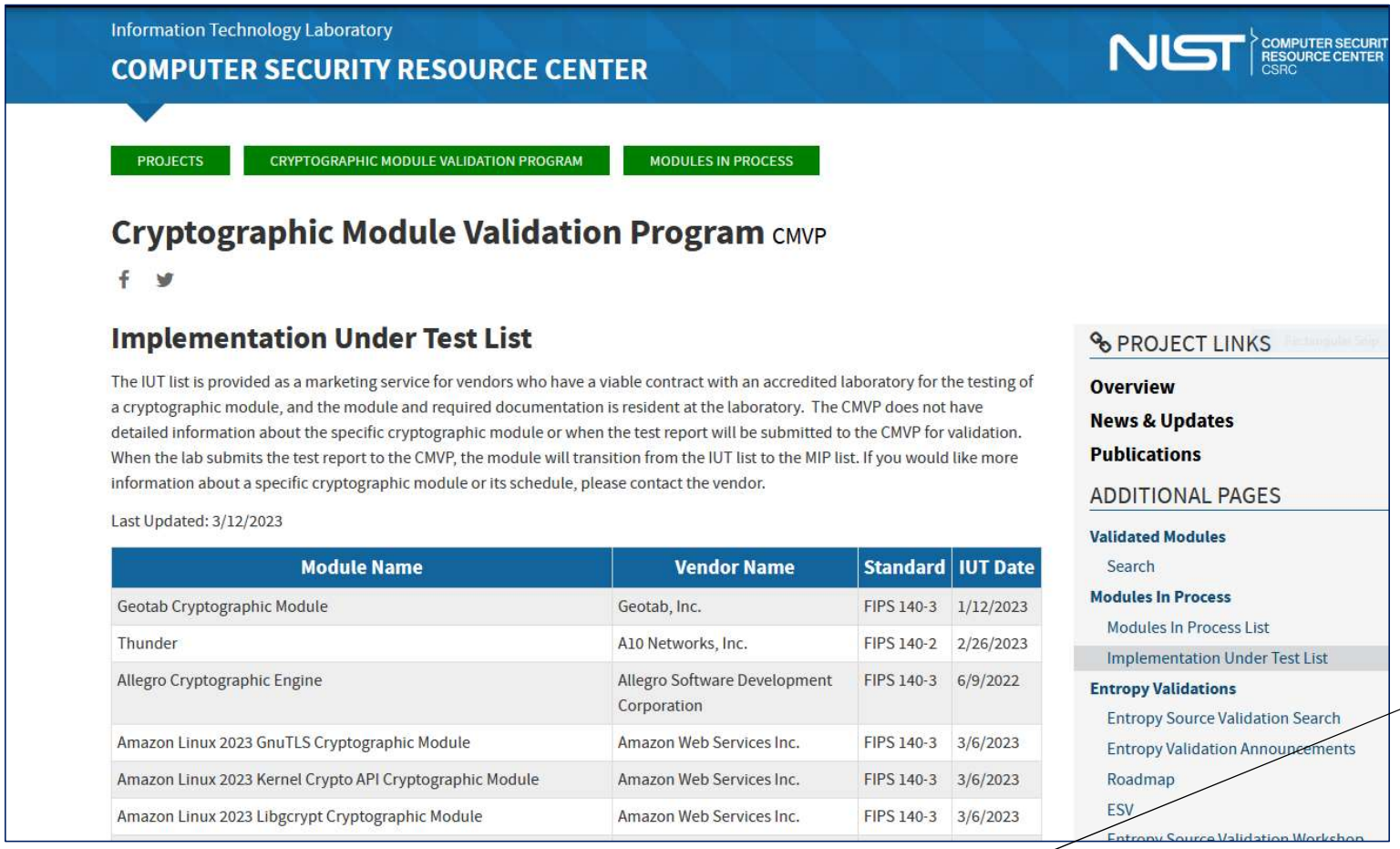
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations

Module Validation Process Flowchart



- Green/Gold boxes correspond to Status on CSRC (IUT List or "Status" column on MIP List)
- CAVP and ESV processes managed separately, "out of band"; certs are pre-requisites
- A few states (status) not shown, e.g., "Hold"

Implementation Under Test (IUT) List



Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

PROJECTS | CRYPTOGRAPHIC MODULE VALIDATION PROGRAM | MODULES IN PROCESS

Cryptographic Module Validation Program CMVP

Implementation Under Test List

The IUT list is provided as a marketing service for vendors who have a viable contract with an accredited laboratory for the testing of a cryptographic module, and the module and required documentation is resident at the laboratory. The CMVP does not have detailed information about the specific cryptographic module or when the test report will be submitted to the CMVP for validation. When the lab submits the test report to the CMVP, the module will transition from the IUT list to the MIP list. If you would like more information about a specific cryptographic module or its schedule, please contact the vendor.

Last Updated: 3/12/2023

Module Name	Vendor Name	Standard	IUT Date
Geotab Cryptographic Module	Geotab, Inc.	FIPS 140-3	1/12/2023
Thunder	A10 Networks, Inc.	FIPS 140-2	2/26/2023
Allegro Cryptographic Engine	Allegro Software Development Corporation	FIPS 140-3	6/9/2022
Amazon Linux 2023 GnuTLS Cryptographic Module	Amazon Web Services Inc.	FIPS 140-3	3/6/2023
Amazon Linux 2023 Kernel Crypto API Cryptographic Module	Amazon Web Services Inc.	FIPS 140-3	3/6/2023
Amazon Linux 2023 Libgcrypt Cryptographic Module	Amazon Web Services Inc.	FIPS 140-3	3/6/2023

PROJECT LINKS

Overview

News & Updates

Publications

ADDITIONAL PAGES

Validated Modules

Search

Modules In Process

Modules In Process List

Implementation Under Test List

Entropy Validations

Entropy Source Validation Search

Entropy Validation Announcements

Roadmap

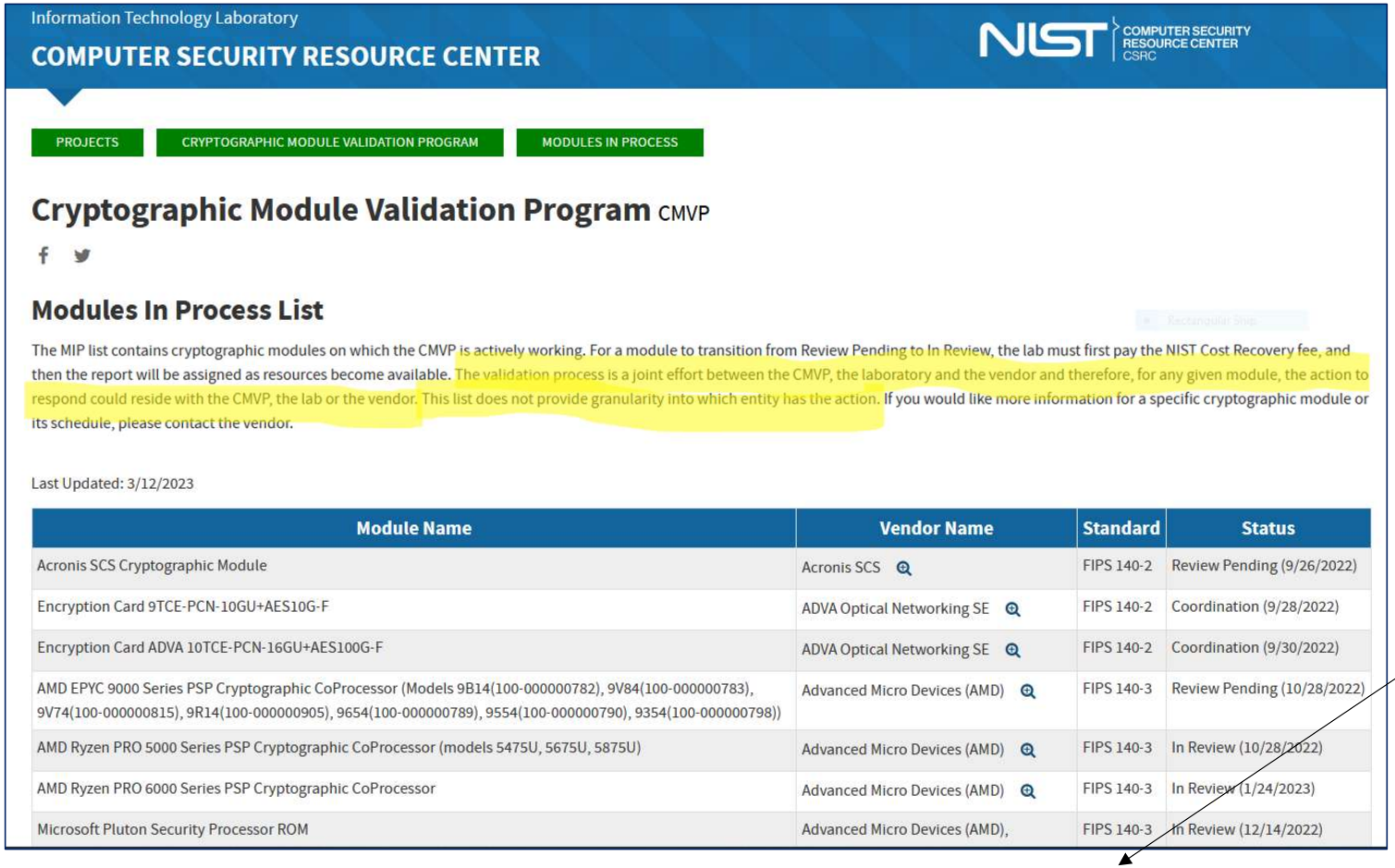
ESV

Displayed	**176**
Not Displayed	**4**
Total	**180**

at bottom of page

https://csrc.nist.gov/Projects/cryptographic-module-validation-program/modules-in-process/IUT-List

Modules In Process (MIP) List



Information Technology Laboratory

COMPUTER SECURITY RESOURCE CENTER

NIST COMPUTER SECURITY RESOURCE CENTER CSRC

PROJECTS | CRYPTOGRAPHIC MODULE VALIDATION PROGRAM | MODULES IN PROCESS

Cryptographic Module Validation Program CMVP

Modules In Process List

The MIP list contains cryptographic modules on which the CMVP is actively working. For a module to transition from Review Pending to In Review, the lab must first pay the NIST Cost Recovery fee, and then the report will be assigned as resources become available. The validation process is a joint effort between the CMVP, the laboratory and the vendor and therefore, for any given module, the action to respond could reside with the CMVP, the lab or the vendor. This list does not provide granularity into which entity has the action. If you would like more information for a specific cryptographic module or its schedule, please contact the vendor.

Last Updated: 3/12/2023

Module Name	Vendor Name	Standard	Status
Acronis SCS Cryptographic Module	Acronis SCS	FIPS 140-2	Review Pending (9/26/2022)
Encryption Card 9TCE-PCN-10GU+AES10G-F	ADVA Optical Networking SE	FIPS 140-2	Coordination (9/28/2022)
Encryption Card ADVA 10TCE-PCN-16GU+AES100G-F	ADVA Optical Networking SE	FIPS 140-2	Coordination (9/30/2022)
AMD EPYC 9000 Series PSP Cryptographic CoProcessor (Models 9B14(100-000000782), 9V84(100-000000783), 9V74(100-000000815), 9R14(100-000000905), 9654(100-000000789), 9554(100-000000790), 9354(100-000000798))	Advanced Micro Devices (AMD)	FIPS 140-3	Review Pending (10/28/2022)
AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor (models 5475U, 5675U, 5875U)	Advanced Micro Devices (AMD)	FIPS 140-3	In Review (10/28/2022)
AMD Ryzen PRO 6000 Series PSP Cryptographic CoProcessor	Advanced Micro Devices (AMD)	FIPS 140-3	In Review (1/24/2023)
Microsoft Pluton Security Processor ROM	Advanced Micro Devices (AMD),	FIPS 140-3	In Review (12/14/2022)

Displayed	**263**
Not Displayed	**42**
Total	**305**

at bottom of page

https://csrc.nist.gov/projects/cryptographic-module-validation-program/modules-in-process/modules-in-process-list

FIPS 140-3 Certificates

8 certificates match the search criteria

Certificate Number	Vendor Name	Module Name	Module Type	Validation Date	Status
4555	Advanced Micro Devices (AMD)	AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor (models 5475U, 5675U, 5875U)	Firmware-hybrid	07/31/2023	Active
4442	VMware, Inc.	VMware's ESXboot Cryptographic Module	Software	02/23/2023	Active
4402	Advanced Micro Devices (AMD)	AMD Ryzen PRO 4000 Series PSP Cryptographic CoProcessor	Firmware-hybrid	12/30/2022	Active
4401	Advanced Micro Devices (AMD)	AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor	Firmware-hybrid	12/30/2022	Active
4392	Apple Inc.	Apple corecrypto Module v11.1 [Apple silicon, Kernel, Software]	Software	12/07/2022	Active
4391	Apple Inc.	Apple corecrypto Module v11.1 [Apple silicon, User, Software]	Software	12/07/2022	Active
4390	Apple Inc.	Apple corecrypto Module v11.1 [Intel, Kernel, Software]	Software	12/07/2022	Active
4389	Apple Inc.	Apple corecrypto Module v11.1 [Intel, User, Software]	Software	12/07/2022	Active

Search results for FIPS 140-3 (Search Type="Advanced", Standard="FIPS 140-3") from:
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/search

FIPS 140-3 Certificate

Certificate #4401

Details

Module Name	AMD Ryzen PRO 5000 Series PSP Cryptographic CoProcessor
Standard	FIPS 140-3
Status	Active
Sunset Date	12/29/2027
Overall Level	1
Caveat	When installed, initialized and configured as specified in Section 11.1 of the Security Policy.
Security Level Exceptions	• Non-invasive security: N/A • Mitigation of other attacks: N/A
Module Type	Firmware-hybrid
Embodiment	Single Chip
Description	The AMD PSP Cryptographic CoProcessor provides cryptographic algorithm support for the Ryzen PRO 5000 Series processor.
Tested Configuration(s)	• AMD Ryzen PRO 5350G • AMD Ryzen PRO 5350GE • AMD Ryzen PRO 5450U • AMD Ryzen PRO 5650G • AMD Ryzen PRO 5650GE • AMD Ryzen PRO 5650U • AMD Ryzen PRO 5750G • AMD Ryzen PRO 5750GE • AMD Ryzen PRO 5850U
Approved Algorithms	RSA SigVer (FIPS186-4) A1719 SHA2-384 A1719
Hardware Versions	bc0c0140FIPS001
Firmware Versions	bc0c0140FIPS001

Vendor

Advanced Micro Devices (AMD)
2485 Augustine Drive
Santa Clara, CA 95054
USA

FIPS Contact
FIPS@amd.com
Phone: 1408-749-4000

Related Files

Security Policy
Consolidated Certificate

Validation History

Date	Type	Lab
12/30/2022	Initial	ATSEC INFORMATION SECURITY CORP

Click on 4401 from list on previous slide

Entropy Source Validation Certificates

Showing **51** through **55** of **55** matching records.

<< < 1 | 2 | **3**

Vendor	Implementation	Certificate Number	Validation Date
Red Hat, Inc.	RHEL Kernel CPU Time Jitter RNG Entropy Source	E54	6/20/2023
Kingston Technology Company, Inc.	Crypto Library FW	E55	7/20/2023
Juniper Networks	Junos OS Non-Physical Entropy Source	E56	7/21/2023
Intel Corporation	Intel DRNG Entropy Source	E57	7/21/2023
Quadient Technologies France	Quadient Postal Security Device Entropy Source	E58	7/24/2023

<< first < previous 1 2 **3**

Page 3 (most recent) of search results for Entropy Source Validation Search (all fields blank) from:
https://csrc.nist.gov/Projects/cryptographic-module-validation-program/entropy-validations/search

FIPS 140-3 and 5G?

FIPS 140-3 validation is a requirement for US Federal Government agencies using cryptographic protection of CUI data.

There are different security levels (1 – 4) and different module types (software, hardware, firmware-hardware hybrid, etc.)

However, there is nothing analogous to (for example) Common Criteria's categories such as "mobility" or "network and network-related devices and systems"