**Draft NIST Special Publication 800-140**

# FIPS 140-3 Derived Test Requirements (DTR):

*CMVP Validation Authority Updates to ISO/IEC 24759*

Kim Schaffer

INFORMATION SECURITY

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

# Draft NIST Special Publication 800-140

# FIPS 140-3 Derived Test Requirements (DTR):

*CMVP Validation Authority Updates to ISO/IEC 24759*

Kim Schaffer
*Computer Security Division*
*Information Technology Laboratory*

October 2019


U.S. Department of Commerce
*Wilbur L. Ross, Jr., Secretary*

National Institute of Standards and Technology
*Walter Copan, NIST Director and Under Secretary for Standards and Technology*

## Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-140
Natl. Inst. Stand. Technol. Spec. Publ. 800-140, 16 pages (October 2019)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

**Public comment period: *October 9, 2019* through *December 9, 2019***

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sp800-140-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

## Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

## Abstract

NIST Special Publication (SP) 800-140 specifies the Derived Test Requirements (DTR) for Federal Information Processing Standard (FIPS) 140-3. SP 800-140 modifies the test (TE) and vendor (VE) evidence requirements of International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 24759. As a validation authority, the Cryptographic Module Validation Program (CMVP) may modify, add, or delete TEs and/or VEs as specified under paragraph 5.2 of ISO/IEC 24759. This NIST Special Publication should be used in conjunction with ISO/IEC 24759 as it modifies only those requirements identified in this document.

## Keywords

Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140; ISO/IEC 19790; ISO/IEC 24759; testing requirement; vendor evidence.

## Audience

This document is focused toward the vendors, testing labs, and CMVP for the purpose of addressing CMVP-specific requirements in ISO/IEC 24759, *Test requirements for cryptographic modules*.

116 **Table of Contents**


137

# 1 Scope

This document specifies the Cryptographic Module Validation Program (CMVP) modifications of the methods to be used by a Cryptographic and Security Testing Laboratory (CSTL) to demonstrate conformance. It also specifies the modification of methods for evidence that vendors provide to the testing laboratories as supporting evidence to demonstrate conformity. Unless otherwise specified in this document, the test requirements are specified in ISO/IEC 24759.

# 2 Normative references

This section identifies additional references to the normative references cited in ISO/IEC 24759. For dated references (e.g., ISO/IEC 19790:2012/Cor.1:*2015*(E)), only the edition cited applies. For undated references (e.g., ISO/IEC 19790), the latest edition of the referenced document (including any amendments) applies.

National Institute of Standards and Technology (2019) *Security Requirements for Cryptographic Modules*. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

# 3 Terms and definitions

The following terms and definitions supersede or are in addition to those defined in ISO/IEC 19790 and ISO/IEC 24759:

*None at this time*

# 4 Symbols and abbreviated terms

The following symbols and abbreviated terms supersede or are in addition to ISO/IEC 19790 and ISO/IEC 24759 throughout this document:

| | |
|---|---|
| CCCS | Canadian Centre for Cyber Security |
| CMVP | Cryptographic Module Validation Program |
| CSD | Computer Security Division |
| CSTL | Cryptographic and Security Testing Laboratory |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management/Modernization Act |
| NIST | National Institute of Standards and Technology |

| | |
|---|---|
| SP 800-XXX | NIST Special Publication 800 series document |
| TE | Test Evidence |
| VE | Vendor Evidence |

# 5 Document organization

## 5.1 General

Section 6 of this document specifies any modifications to the requirements for information that vendors shall provide to testing laboratories and the requirements that shall be used by testing laboratories. Following ISO/IEC 24759, Section 6 includes a general area of security followed by 11 specific areas of security.

Each Annex is addressed in a similarly labeled SP 800-140*X*, such that:

Annex A – Documentation requirements
are addressed in SP 800-140A.

Annex B – Cryptographic module security policy
is addressed in SP 800-140B.

Annex C – Approved security functions
are addressed in SP 800-140C.

Annex D – Approved sensitive parameter generation and establishment methods
are addressed in SP 800-140D.

Annex E – Approved authentication mechanisms
are addressed in SP 800-140E.

Annex F – Approved non-invasive attack mitigation test metrics
are addressed in SP 800-140F.

## 5.2 Modifications

Modifications will follow a similar format as in ISO/IEC 24759. For additions to test requirements, new Test Evidence (TEs) or Vendor Evidence (VEs) will be listed by increasing the "sequence_number." Modifications can include a combination of additions using underline and deletions using ~~strikethrough~~. If no changes are required, the paragraph will indicate "No change."

# 6 Security requirements

In responding to test evidence (TE), a yes/no answer does not provide sufficient assurance. Therefore, CMVP requires the following information when responding to a documentation, operational testing, or verify/verify by inspection requirement.

Documentation:

Reference/cite the applicable vendor documentation, and summarize the contents per the TE.

Operational Testing:

Describe the test method and tools, and summarize the results per the TE.

Verify or Verify by Inspection:

Describe the test or inspection method used to verify the requirement, and provide detailed results of the inspection per the TE.

## 6.1 General

No change.

## 6.2 Cryptographic module specification

No change.

## 6.3 Cryptographic module interfaces

No change.

## 6.4 Roles, services, and authentication

AS04.54: (Operator authentication — Levels 2, 3, and 4)

Feedback of authentication data to an operator shall be obscured during authentication to anyone other than the operator. ~~(e.g. no visible display of characters when entering a password)~~.

Required Vendor Information

VE04.54.01: The vendor documentation shall specify the method used to obscure feedback of the authentication data ~~to an operator~~ during entry of the authentication data.

VE04.54.02: The vendor documentation shall specify how, if implemented, the vendor allows an operator to view authentication data at the time of entry while obscuring any useful information

to all others.

Required Test Procedures

TE04.54.01: The tester shall verify from the vendor documentation that the authentication data is obscured during data entry.

TE04.54.02: The tester shall enter authentication data and verify that there is no visible display of authentication data during data entry.

TE04.54.03: The tester shall verify that, if implemented, the operator can view authentication data at the time of entry while obscuring any useful information to all others.

### 6.5 Software/Firmware security

No change.

### 6.6 Operational environment

No change.

### 6.7 Physical security

**AS07.37: (Single-chip cryptographic modules – Levels 3 and 4)**

***{Either}*** **the module shall be covered with a hard opaque tamper-evident coating (e.g. a hard opaque epoxy covering the passivation) {*or AS07.38 shall be satisfied*}.**

**Required Vendor Information**

VE07.37.01: The vendor documentation shall state clearly that the approach specified in AS07.37 is used to meet the requirement.

VE07.37.02: The vendor documentation shall provide supporting detailed design information, especially the type of coating that is used and its characteristics.

Required Test Procedures

TE07.37.01: The tester shall verify by inspection and from the vendor documentation that the module is covered with a hard opaque tamper evident coating.

TE07.37.02: The tester shall verify that the vendor documentation does sufficiently provide supporting detailed design information, especially specifying the type of coating that is used and its characteristics.

TE07.37.03: The tester shall verify that the coating cannot be easily penetrated to the depth of the underlying circuitry, and that it leaves tamper evidence. The inspection has to verify that the coating completely covers the module, is visibly opaque, and deters direct observation, probing,

or manipulation.

TE07.37.04: The security policy shall specify the nominal and high/low temperature range at which the module hardness testing was performed. If the module hardness testing was only performed at a single temperature (e.g., vendor provided only a nominal temperature, or the vendor did not provide a specification), the security policy shall clearly state that the module hardness testing was only performed at a single temperature, and no assurance is provided for hardness conformance at any other temperature.

**AS07.77: (Environmental failure protection features — Levels 3 and 4)**

If the temperature or voltage falls outside of the cryptographic module's normal operating range, the protection capability shall either

— shut down the module to prevent further operation,

or

— immediately zeroise all unprotected SSPs

Required Vendor Information

VE07.77.01: If EFP is chosen for a particular condition, the module shall monitor and correctly respond to fluctuations in the operating temperature or voltage outside of the module's normal operating range for that condition. The protection features shall continuously measure these environmental conditions. If a condition is determined to be outside of the module's normal operating range, the protection circuitry shall either:

a) Shut down the module, or

b) Zeroise all plaintext SSPs

Documentation shall state which of these approaches was chosen and provide a specification description of the EFP features implemented within the module.

VE07.77.02: The security policy addresses whether EFP forces module shutdown or zeroises all plaintext SSPs and specifies the normal operating temperature range this requirement meets.

Additional Required Test Procedures

TE07.77.04: The tester shall verify that the vendor-provided security policy defines how EFP forces module shutdown or zeroises all plaintext SSPs and specifies the normal operating temperature range.

AS07.81: (Environmental failure testing procedures — Level 3)

The temperature range to be tested shall be from a temperature within the normal operating temperature range to the lowest (i.e. coldest) temperature that either (1) shuts down the module

to prevent further operation or (2) immediately zeroises all unprotected SSPs; and from a temperature within the normal operating temperature range to the highest (i.e. hottest) temperature that either (1) shuts down or goes into an error state or (2) zeroises all unprotected SSPs.

**Required Vendor Information**

VE07.81.01: If EFT is chosen for a particular condition, the module shall be tested within the temperature range specified in AS07.82 and voltage ranges specified in AS07.85 and AS07.86. The module shall either:

a) Continue to operate normally, or

b) Shut down, or

c) Zeroise all plaintext SSPs.

Documentation shall state which of these approaches was chosen and provide a specification description of the EFT.

**Additional Required Test Procedures**

VE07.81.02: The security policy addresses EFT, whether the module continues to operate normally or shut down or zeroise all plaintext SSPs, and specifies the normal operating temperature range this requirement meets.

**Required Test Procedures**

TE07.81.03: The tester shall verify that the vendor-provided security policy defines how either EFT forces module shutdown or zeroises all plaintext SSPs and specifies the normal operating temperature range.

### 6.8 Non-invasive security

No change.

### 6.9 Sensitive security parameter management

**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.**

**Required Vendor Information**

VE09.28.01: The vendor documentation shall specify the zeroisation information of the following SSPs:

a. Zeroisation techniques
b. Restrictions when plaintext SSPs can be zeroised
c. Plaintext SSPs that are zeroised
d. Plaintext SSPs that are not zeroised and rationale
e. Rationale explaining how the zeroisation technique is performed in a time that is not sufficient to compromise plaintext SSPs

VE09.28.02: The vendor documentation shall specify how the zeroization method(s) are employed such that the secret and private cryptographic keys and other CSPs within the module cannot be obtained by an attacker.

VE09.28.03: If SSPs are zeroized procedurally while under the control of the operator (i.e., present to observe the method has completed successfully or controlled via a remote management session), vendor documentation and the module security policy must specify how the methods shall be performed.

**Required Test Procedures**

TE09.28.01: The tester shall verify in the vendor documentation that the information specified in VE09.30.01 is included. The tester shall verify the accuracy of any rationale provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.

TE09.28.02: The tester shall verify which keys are present in the module and initiate the zeroise command. Following the completion of the zeroise command, the tester shall attempt to perform cryptographic operations using each of the plaintext SSPs that were stored in the module. The tester shall verify that each plaintext SSP cannot be accessed.

TE09.28.03: The tester shall initiate zeroisation and verify the key destruction method is performed in a time that is not sufficient to compromise plaintext SSPs.

TE09.28.04: The tester shall verify that all plaintext SSPs that are not zeroised by the zeroise command are either 1) encrypted using an approved algorithm or 2) physically or logically protected within an embedded, validated cryptographic module (validated as conforming to ISO/IEC 19790:2012/Cor.1:2015).

TE09.28.05: If procedural zeroization methods are used, the tester shall verify that the vendor-provided documentation, including the security policy, specifies that the procedure must be performed under the control of the operator.

TE09.28.06: If the procedural zeroization method is not under the direct control of the operator, the tester shall verify the accuracy of any rationale provided by the vendor as to why secret and private cryptographic keys and other CSPs within the module cannot be obtained by an attacker. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.

~~NOTE 1 This assertion is tested AS09.30.~~

NOTE 2 Temporarily stored SSPs and other stored values owned by the module should be zeroised when they are no longer needed for future use.

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

**A zeroised SSP shall not be retrievable or reusable.**

**Required Vendor Information**

VE09.29.01: The vendor documentation shall specify how a zeroised SSP cannot be retrievable or reusable.

**Required Test Procedures**

TE09.29.01: The tester shall verify that the vendor provides documentation specifies how a zeroised SSP cannot be retrievable or reusable.

TE09.29.02: The tester shall verify the accuracy of any rationale provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed

NOTE 1 Zeroisation of protected PSPs, encrypted CSPs, or CSPs otherwise physically or logically protected within an additional embedded validated module (meeting the requirements of this International Standard) is not required.

NOTE 2 SSPs need not meet these zeroisation requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialisation key).

**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).**

NOTE 1 This assertion is tested in AS09.28.

~~**Required Vendor Information**~~

~~VE09.30.01: The vendor documentation shall specify the following SSPs zeroisation information:~~

a) ~~Zeroisation techniques~~
b) ~~Restrictions when plaintext SSPs can be zeroised~~
c) ~~Plaintext SSPs that are zeroised~~

d) ~~Plaintext SSPs that are not zeroised and rationale~~
e) ~~Rationale explaining how the zeroisation technique is performed in a time that is not sufficient to compromise plaintext SSPs~~

~~**Required Test Procedures**~~

~~TE09.30.01: The tester shall verify the vendor documentation that the information specified in VE09.30.01 is included. The tester shall verify the accuracy of any rationale provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.~~

~~TE09.30.02: The tester shall verify which keys are present in the module and initiate the zeroise command. Following the completion of the zeroise command, the tester shall attempt to perform cryptographic operations using each of the plaintext SSPs that were stored in the module. The tester shall verify that each plaintext SSPs cannot be accessed.~~

~~TE09.30.03: The tester shall initiate zeroisation and verify the key destruction method is performed in a time that is not sufficient to compromise plaintext SSPs.~~

~~TE09.30.04: The tester shall verify that all plaintext SSPs that are not zeroised by the zeroise command are either 1) encrypted using an approved algorithm, or 2) physically or logically protected within an embedded validated cryptographic module (validated as conforming to ISO/IEC 19790:2012/Cor.1:2015).~~

### 6.10 Self-tests

No change.

### 6.11 Life-cycle assurance

**AS11.38: (Guidance documents – Levels 1, 2, 3, and 4)**

**Administrator guidance shall specify:**
**- the administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the Crypto Officer and/or other administrative roles;**
**- procedures required to keep operator authentication data and mechanisms functionally independent;**
**- procedures on how to administer the cryptographic module in an approved mode of operation; and**
**- assumptions regarding User behavior that are relevant to the secure operation of the cryptographic module.**

**Required Vendor Information**

VE11.38.03: The vendor shall provide evidence that there is no vulnerability identified on the CVE list associated with the module that will affect the module.

**Required Test Procedures**

TE11.38.03: The tester shall verify the vendor's claim that no libraries or similar vendor equipment have a vulnerability on the CVE list that will affect the module.

### 6.12 Mitigation of other attacks

No change.

455 **Document Revisions**

| Date | Change |
|---|---|
| | |
| | |

456

457