NIST Special Publication 800-140

FIPS 140-3
Derived Test Requirements (DTR):

CMVP Validation Authority Updates to ISO/IEC 24759

Kim Schaffer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140

INFORMATION SECURITY

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

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140

March 2020

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, 23 pages (March 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140

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 http://csrc.nist.gov/publications.

Comments on this publication may be submitted to:

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 modifications of 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.

Table of Contents

1 Scope 1
2 Normative references 1
3 Terms and definitions 1
4 Symbols and abbreviated terms 1
5 Document organization 2
5.1 General 2
5.2 Modifications 2
6 Security requirements 2
6.1 General 3
6.2 Cryptographic module specification 3
6.3 Cryptographic module interfaces 6
6.4 Roles, services, and authentication 7
6.5 Software/Firmware security 8
6.6 Operational environment 8
6.7 Physical security 9
6.8 Non-invasive security 11
6.9 Sensitive security parameter management 11
6.10 Self-tests 15
6.11 Life-cycle assurance 15
6.12 Mitigation of other attacks 17

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 to the required documentation vendors are to 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 the normative references cited as ISO/IEC 19790 and ISO/IEC 24759. The specific editions to be used are ISO/IEC 19790:2012 and ISO/IEC 24759:2017. Please note that the version 19790:2012 referenced here includes the corrections made in 2015.

Federal Information Processing Standard Publication (FIPS) 140-3, *Security Requirements for Cryptographic Modules*

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 symbols and abbreviated terms:

CMVP	Cryptographic Module Validation Program
CSD	Computer Security Division
CCCS	Canadian Centre for Cyber Security
CSTL	Cryptographic and Security Testing Laboratory
CVE	Common Vulnerabilities and Exposures
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

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 for testing that shall be used by testing laboratories. Following the format of ISO/IEC 24759, Section 6 includes a general area of security, followed by eleven specific areas of security.

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

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

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

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

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

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

Annex F – Approved non-invasive attack mitigation test metrics
is 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. 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 test or inspection, per the TE.

6.1 General

No change.

6.2 Cryptographic module specification

AS02.15: (Specification – Levels 1, 2, 3, and 4)

The cryptographic boundary of a hardware cryptographic module shall delimit and identify:

- **The set of hardware components which may include:**
  - **physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between components,**
  - **active electrical components such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc.**
  - **physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces,**
  - **firmware, which may include an operating system,**
  - **other components types not listed above.**

Required Vendor Information

VE02.15.05 For each processor in the module, the vendor shall identify, by major services, the software or firmware that are executed by the processor, and the memory devices that contain the executable code and data.

VE02.15.06 For each processor, the vendor shall identify any hardware with which the processor interfaces.

Required Test Procedures

TE02.15.10 The tester shall verify the documentation provided under assertion AS02.02, with a focus on the block diagram depicting all of the major hardware components of a cryptographic module and component interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory.

TE02.15.11 The tester shall verify that the block diagram indicates all significant interconnections and data flow among major components of the module, and between the module and outside equipment. In particular, each line on the block diagram indicating an interconnection must be labeled with the type of information it transmits.

TE02.15.12 The tester shall verify that the block diagram indicates the cryptographic boundary for the cryptographic module, as required under this assertion.

TE02.15.13 The tester shall verify that, for each processor, the vendor has identified the software or firmware code modules executed by that processor, the services performed by that processor and associated code, and the memory devices containing the executable code and data.

TE02.15.14 The tester shall verify that, for each processor, the vendor has identified any hardware with which the processor interfaces. This must include, as applicable, any hardware components that provide input, control, or status data to the processor and associated software/firmware, and any hardware components that receive output, control, or status data from the processor and associated software/firmware. Such hardware components may be within the cryptographic module or may be user equipment outside the module such as input/output devices.

AS02.17: (Specification – Levels 1, 2, 3, and 4)

The cryptographic boundary of a firmware cryptographic module shall delimit and identify:

- **The set of executable file or files that constitute the cryptographic module; and**
- **The instantiation of the cryptographic module saved in memory and executed by one or more processors.**

Required Vendor Information

VE02.17.04 For each processor in the computing platform of the operational environment bound to the firmware module, the vendor shall identify, by major services, the firmware that is executed by the processor, and the memory devices that contain the executable code and data.

VE02.17.05 For each processor in the computing platform of the operational environment bound to the firmware module, the vendor shall identify any hardware with which the processor interfaces.

Required Test Procedures

TE02.17.06 The tester shall verify the documentation provided under assertion AS02.02, with a focus on the block diagram depicting all of the major hardware components of a cryptographic module and component interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory.

TE02.17.07 The tester shall verify that the block diagram indicates all significant interconnections and data flows among major components of the module, and between the module and outside equipment. In particular, each line on the block diagram indicating an interconnection must be labeled with the type of information it transmits.

TE02.17.08 The tester shall verify that the block diagram indicates the cryptographic boundary for the cryptographic module, as required under this assertion.

TE02.17.09 The tester shall verify that, for each processor in the computing platform of the operational environment bound to the firmware module, the vendor has identified the firmware code modules executed by that processor, the services performed by that processor and associated code, and the memory devices containing the executable code and data.

TE02.17.10 The tester shall verify that, for each processor in the computing platform of the operational environment bound to the firmware module, the vendor has identified any hardware with which the processor interfaces. This must include, as applicable, any hardware components that provide input, control, or status data to the processor and associated firmware, and any hardware components that receive output, control, or status data from the processor and associated firmware. Such hardware components may be within the cryptographic module or may be user equipment outside the module such as input/output devices.

AS02.18: (Specification – Levels 1, 2, 3, and 4)

The cryptographic boundary of a hybrid cryptographic module shall:

- **be the composite of the module's hardware component boundary and the disjoint software or firmware component(s) boundary; and**
- **include the collection of all ports and interfaces from each component.**

NOTE In addition to the disjoint software or firmware component(s), the hardware component can also include embedded software or firmware.

Required Vendor Information

VE02.18.01: The cryptographic module shall be identified in the vendor documentation as either a Hybrid Software Module or a Hybrid Firmware Module.

a) For Hybrid Software Module components, the vendor documentation shall provide information required under VE02.15.01 through ~~VE02.15.04~~ VE02.15.06 and VE02.16.01 through VE02.16.03.

b) For Hybrid Firmware Module components, the vendor documentation shall provide information required under VE02.15.01 through ~~VE02.15.04~~ VE02.15.06 and VE02.17.01 through ~~VE02.17.03~~ VE02.17.05.

Required Test Procedures

TE02.18.01: The tester shall verify that the documentation identifies the module as either a Hybrid Software Module or a Hybrid Firmware Module.

a) For Hybrid Software Module components, the tester shall follow procedures required under TE02.15.01 through ~~TE02.15.09~~ TE02.15.14 and TE02.16.01 through TE02.16.05.

b) For Hybrid Firmware Module components, the tester shall follow procedures required under TE02.15.01 through ~~TE02.15.09~~ TE02.15.14 and TE02.17.01 through ~~TE02.17.05~~ TE02.17.10.

AS02.20: (Specification – Levels 1, 2, 3, and 4)

An approved mode of operation shall be defined as the set of services which include at least one service that utilises an approved cryptographic algorithm, security function or process and those services or processes specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* 7.4.3.

Required Vendor Information

VE02.20.03 The vendor shall provide a list of all vendor affirmed security methods.

VE02.20.04 The vendor provided non-proprietary security policy shall include a list of all vendor affirmed security methods.

Required Test Procedures

TE02.20.03 The tester shall verify that the vendor has provided the list of vendor affirmed security methods as described above.

TE02.20.04 The tester shall verify that the vendor provided documentation specifies how the implemented vendor affirmed security methods conform to the relevant standards.

6.3 Cryptographic module interfaces

AS03.07: (Data output interface – Levels 1, 2, 3, and 4)

All data output via the "data output" interface shall be inhibited while performing manual entry, pre-operational self-tests, software/firmware loading and zeroisation; or when the cryptographic module is in an error state.

Required Vendor Information

VE03.07.03: The vendor documentation shall specify how the physical and logical paths used by all major categories of output data exiting the cryptographic module are logically or physically disconnected from the processes performing SSP generation, manual SSP entry, and zeroisation of SSPs.

VE03.07.04: If the physical and logical paths followed by the output data and SSP information are physically shared, the vendor documentation shall specify how the cryptographic module enforces logical separation of the output data and SSP information.

VE03.07.05: The vendor documentation shall specify how the cryptographic module does not allow the specified SSP processes to pass SSP information to the output data path, and does not allow output data exiting the module to interfere with the SSP processes.

Required Test Procedures

TE03.07.06: The tester shall verify that the vendor documentation specifies how the physical and logical paths used by all major categories of output data exiting the cryptographic module are logically or physically disconnected from the processes performing SSP generation, manual SSP entry, and zeroisation of SSPs.

TE03.07.07: If the physical and logical paths followed by the output data and SSP information are physically shared, the tester shall verify that the vendor documentation specifies how the cryptographic module enforces logical separation of the output data and SSP information.

TE03.07.08: The tester shall verify that the output data path is logically or physically disconnected from the processes performing SSP generation, manual SSP entry, and zeroisation of SSPs.

6.4 Roles, services, and authentication

AS04.44: (Operator authentication – Levels 1, 2, 3, and 4)

Authentication data within a cryptographic module shall be protected against unauthorised use, disclosure, modification, and substitution.

NOTE Approved security functions can be used as part of the authentication mechanism.

Required Vendor Information

VE04.44.01: The vendor documentation shall describe the protection of all authentication data within the module. Protection shall include the implementation of mechanisms that protect against unauthorised use, disclosure, modification, and substitution.

Required Test Procedures

TE04.44.01: The tester shall verify the vendor documentation that describes the protection of authentication data. The tester shall verify that the documentation describes how the data will be protected against unauthorised use, disclosure, modification, and substitution.

AS04.45: (Operator authentication – Levels 2, 3, and 4)

If a cryptographic module does not contain the authentication data required to authenticate the operator for the first time the module is accessed, then other authorised

methods (e.g. procedural controls or use of factory-set or default authentication data) shall be used to control access to the module and initialise the authentication mechanisms.

Required Test Procedures

TE04.45.02: If access to the module before initialisation is procedurally controlled, the tester shall initiate an error on an uninitialised module and shall verify that the module denies access. The tester shall assume the authorised role and verify that the required authentication complies with the documented procedures. The tester shall attempt to assume other roles before the module has been initialised and verify that the module denies access to the roles.

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 confirm 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 access of authentication data during data entry, except, as an option, to the operator.

TE04.54.03: If the vendor allows an operator to confirm authentication data at the time of entry, the tester shall verify that this information is obscured from other entities.

6.5 Software/Firmware security

No change.

6.6 Operational environment

AS06.11: (Operational environment – Level 2)

The operating system shall be configured to protect against unauthorised execution, unauthorised modification, and unauthorised reading of SSPs, control and status data.

Required Vendor Information

VE06.11.01: The vendor shall provide operating system documentation which provides a description of the operating system control mechanisms which can be configured to protect against unauthorised execution, unauthorised modification, and unauthorised reading of SSPs, control and status data.

Required Test Procedures

TE06.11.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechanisms, that the operating system can be configured to protect against unauthorised execution, unauthorised modification, and unauthorised reading of SSPs, control and status data.

TE06.11.02: The tester shall configure the operating system to protect against unauthorised execution, unauthorised modification, and unauthorised reading of SSPs, control and status data. During execution of a cryptographic process, the tester shall attempt to execute, modify or read SSPs, control or status data which the tester has authorised access.

TE06.11.03: The tester shall configure the operating system to protect against unauthorised execution, unauthorised modification, and unauthorised reading of SSPs, control and status data. During execution of a cryptographic process, the tester shall attempt to execute, modify or read SSPs, control or status data which the tester has unauthorised access.

6.7 Physical security

AS07.26: (Physical security – Levels 3 and 4)

Strong or hard conformal or non-conformal enclosures, coatings or potting materials shall maintain strength and hardness characteristics over the module's intended temperature range of operation, storage and distribution.

Required Vendor Information

VE07.26.01: The vendor documentation shall describe the strength or hardness of the~~,~~ ~~hard~~ conformal or non-conformal enclosure, coatings or potting materials and the rationale that the strength or hardness is appropriate for the module design.

VE07.26.02: The vendor provided security policy shall specify the nominal and high/low temperature range.

Required Test Procedures

TE07.26.01: The tester shall verify from the vendor documentation and ~~inspection~~ testing of the module that the strength or hardness of the~~,~~ ~~hard~~ conformal or non-conformal enclosure, coatings or potting materials is ~~the one designed~~ implemented as specified. The tester shall verify the module hardness at the following temperatures:

- the lowest temperature of the module's intended temperature range of operation, storage and distribution;

- the highest temperature of the module’s intended temperature range of operation, storage and distribution.

TE07.26.02: The tester shall verify that the vendor provided security policy specifies the high/low temperature range.

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

— shutdown 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) shutdown the module, or

b) zeroise all ~~plaintext~~ unprotected 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 shall address whether the employed EFP feature forces module shutdown or zeroises all unprotected SSPs and shall specify the temperature range met.

Additional Required Test Procedures

TE07.77.04 The tester shall verify that the security policy specifies the normal operating temperature and voltage range, and whether the module shuts down or zeroises all unprotected SSPs if the operating temperature or voltage falls outside the normal operating range of the module.

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) shutdown the module to prevent further operation or (2) immediately zeroise 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) shutdown, or

c) zeroise all ~~plaintext~~ unprotected SSPs.

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

VE07.81.02: The security policy shall address whether the employed EFT feature forces module shutdown or zeroises all unprotected SSPs and shall specify the temperature range met.

Required Test Procedures

TE07.81.03: The tester shall verify that the non-proprietary security policy specifies the normal operating temperature and voltage range, and whether the module forces shut down or zeroises all unprotected SSPs if the operating temperature or voltage falls outside the normal operating range of the module.

6.8 Non-invasive security

No change.

6.9 Sensitive security parameter management

AS09.23: (Sensitive security parameter entry and output – Level 3)

{If the module employs split knowledge procedures, the module shall employ separate identity-based operator authentication for entering or outputting each key component,} and at least two key components shall be required to reconstruct the original cryptographic key.

Required Vendor Information

VE09.23.01: The vendor documentation shall specify the number of components that are required to construct the original CSP.

VE09.23.02: If knowledge of the number of key components is required to reconstruct the original key, the vendor provided documentation shall include rationale stating how knowledge of any one less than the number of key components provides no information about the original key other than the length.

Required Test Procedures

TE09.23.01: The tester shall verify in the vendor provided documentation that the split knowledge procedure requires at least two components to construct the original CSP.

TE09.23.02: The tester shall verify the vendor provided documentation provides a rationale that no information is gained without knowing all the necessary split keys. ~~that the output of CSPs under split knowledge procedures does not result in the output of a single component that can be used to construct the original CSP~~.

TE09.23.04: 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.

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 following zeroisation information for SSPs:

a. Zeroisation techniques

b. Restrictions when unprotected SSPs can be zeroised

c. Unprotected SSPs that are zeroised

d. Unprotected 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 unprotected SSPs

VE09.28.02 The vendor documentation shall specify how the zeroisation method(s) are employed such that unprotected SSPs within the module cannot be obtained by an attacker.

VE09.28.03: If SSPs are zeroised 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 the vendor documentation includes the information specified in VE09.30.01. 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 SSPs 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 unprotected SSPs that were stored in the module. The tester shall verify that each unprotected SSP cannot be accessed.

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

TE09.28.04: The tester shall verify that all unprotected 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).

TE09.28.05: If procedural zeroisation 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 zeroisation 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 unprotected SSPs 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 provided 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 document ~~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

AS10.01: (Self-tests – Levels 1, 2, 3, and 4)

All self-tests shall be performed, {and determination of pass or fail shall be made by the module, without external controls, externally provided input ~~text~~ test vectors, expected output results, or operator intervention or whether the module will operate in an approved or non-approved mode}.

NOTE This assertion is not separately tested.

AS10.02: (Self-tests – Levels 1, 2, 3, and 4)

***{All self-tests shall be performed,}* and determination of pass or fail shall be made by the module, without external controls, externally provided input ~~text~~ test vectors, expected output results, or operator intervention or whether the module will operate in an approved or non-approved mode.**

NOTE The intention of this assertion is that the determination of pass or fail will be made by the module, without external controls, primarily for pre-operational self-tests and (conditional) cryptographic algorithm self-test. It is known that a software/firmware load test into a validated module involves the software or firmware that is loaded from an external source, and that a manual entry test involves SSPs or key components manually entered by a human operator; however, the essence is the same.

AS10.07: (Self-tests – Levels 1, 2, 3, and 4)

If a cryptographic module fails a self-test, the module shall enter an error state *{and shall output an error indicator as specified in {ISO/IEC 19790:2012/Cor.1:2015 subclause} 7.3.3}*.

Required Test Procedures

TE10.07.05: The tester shall verify by inspection and from the vendor documentation that determination of pass or fail of each self-test is made by the module, without external controls, externally provided input ~~text~~ test vectors, expected output results, or operator intervention.

6.11 Life-cycle assurance

AS11.13: (Finite state model – Levels 1, 2, 3, and 4)

Changing to the Crypto Officer state from any other role other than the Crypto Officer shall be prohibited.

NOTE: The intention of this assertion is to remove/avoid privilege escalation to a Crypto Officer role.

AS11.29: (Vendor testing – Levels 1, 2, 3, and 4)

Documentation shall specify the functional testing performed on the cryptographic module.

Required Vendor Information

VE11.29.01: The vendor shall provide documentation that specifies the functional testing performed on the cryptographic module, providing assurance that the cryptographic module behaves in accordance with the module security policy and functional specifications.

Required Test Procedures

TE11.29.01: The tester shall verify that the vendor provided documentation ~~that~~ specifies the functional testing performed on the cryptographic module.

TE11.29.02: The tester shall verify that the vendor provided documentation provides assurance that the cryptographic module behaves in accordance with the module security policy and functional specifications.

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 list any CVEs associated with the module, and either

- provide assurance that they are not security relevant;
- or, for any CVE's that are considered security relevant, the vendor shall describe how they have been mitigated.

Required Test Procedures

TE11.38.03: The tester shall verify that any CVEs associated with the module:

- are not security relevant, or,
- if they are security relevant, mitigations provided by the vendor are appropriate.

6.12 Mitigation of other attacks

No change.

Document Revisions

Date	Change