International Standard

ISO/IEC 24759

Fourth edition
2025-02

Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules

Sécurité de l'information, cybersécurité et protection de la vie privée — Exigences d'essai pour modules cryptographiques

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

Reference number
ISO/IEC 24759:2025(en)

© ISO/IEC 2025

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2025

All rights reserved. Unless otherwise specified, or required in the context of its implementation, no part of this publication may be reproduced or utilized otherwise in any form or by any means, electronic or mechanical, including photocopying, or posting on the internet or an intranet, without prior written permission. Permission can be requested from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
CP 401 • Ch. de Blandonnet 8
CH-1214 Vernier, Geneva
Phone: +41 22 749 01 11
Email: copyright@iso.org
Website: www.iso.org

Published in Switzerland

Contents

Page

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

ISO and IEC draw attention to the possibility that the implementation of this document may involve the use of (a) patent(s). ISO and IEC take no position concerning the evidence, validity or applicability of any claimed patent rights in respect thereof. As of the date of publication of this document, ISO and IEC had not received notice of (a) patent(s) which may be required to implement this document. However, implementers are cautioned that this may not represent the latest information, which may be obtained from the patent database available at www.iso.org/patents and https://patents.iec.ch. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

This document was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *Information security, cybersecurity and privacy protection*.

This fourth edition cancels and replaces the third edition (ISO/IEC 24759:2017), which has been technically revised.

The main changes are as follows:

— new terminology has been added;

— ASs, VEs and TEs have been updated according to ISO/IEC 19790:2025; and

— VEs and TEs have been corrected or updated to improve efficiency.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Introduction

In information technology there is an ever-increasing need to use cryptographic mechanisms, such as for the protection of data against unauthorized disclosure or manipulation, for entity authentication, and for non-repudiation. The security and reliability of such mechanisms are directly dependent on the cryptographic modules in which they are implemented.

ISO/IEC 19790 provides four increasing, qualitative levels of security requirements intended to cover a wide range of potential applications and environments. The cryptographic techniques are identical over the four security levels defined in this document. The security requirements cover areas relative to the design and implementation of a cryptographic module. These areas include:

— cryptographic module specification;

— cryptographic module interfaces;

— roles, services and authentication;

— software/firmware security;

— operational environment;

— physical security;

— non-invasive security;

— sensitive security parameter management;

— self-tests;

— life-cycle assurance; and

— mitigation of other attacks.

This document specifies the test requirements for cryptographic modules conforming to ISO/IEC 19790:2025.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Information security, cybersecurity and privacy protection — Test requirements for cryptographic modules

1 Scope

This document specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2025. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This document also specifies the information that vendors are required to provide testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2025.

Vendors can also use this document to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2025 before applying to a testing laboratory for testing.

2 Normative references

The following documents are referred to in the text in such a way that some or all of their content constitutes requirements of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19790:2025, *Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules*

ISO/IEC 20085-1, *IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 1: Test tools and techniques*

ISO/IEC 20085-2, *IT Security techniques — Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part 2: Test calibration methods and apparatus*

ISO/IEC 20543, *Information technology — Security techniques — Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19790 and the following apply.

ISO and IEC maintain terminology databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at www.iso.org/obp;

— IEC Electropedia: available at www.electropedia.org.

3.1
validation certificate
assertion by a certification body that a cryptographic function has been tested and found to be a correct implementation of the target cryptographic function

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

3.2
vendor affirmation
statement from a vendor that a given implementation of a security function is correct and meets all relevant requirements from related standards, based on their own internal assurance activities

Note 1 to entry: Rules on acceptable vendor affirmations are set by individual certification bodies who independently define evidence requirements for a given vendor affirmation and can require review by an independent testing laboratory.

4 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms apply.

ACL	access control list
API	application programming interface
CBC	cipher block chaining
CPLD	complex programmable logic device
CSP	critical security parameter
ECB	electronic codebook
EDC	error detection code
EFP	environmental failure protection
EFT	environmental failure testing
FPGA	field programmable gate array
FSM	finite state model
HDL	hardware description language
IC	integrated circuit
PC	personal computer
PIN	personal identification number
PSP	public security parameter
RBG	random bit generator
SSP	sensitive security parameter

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

5 Document organization

5.1 General

Clause 6 specifies the methods that shall be used by testing laboratories and the requirements for documentation that vendors shall provide to testing laboratories.

6.2 to 6.12 includes eleven subclauses corresponding to the eleven areas of security requirements from ISO/IEC 19790:2025. Clause 7 corresponds to ISO/IEC 19790:2025, Annex A, and Clause 8 corresponds to ISO/IEC 19790:2025, Annex B.

© ISO/IEC 2025 – All rights reserved

ISO/IEC 19790:2025, Annexes C, D, E, F and G do not currently include any assertions and are not covered by this document.

5.2 Assertions and security requirements

In Clauses 6, 7 and 8, the corresponding security requirements from ISO/IEC 19790:2025 are presented in Table 1 to 429, each dedicated to an individual assertion (i.e. statements that shall be true for the module to satisfy the requirement of a given area at a given level).

All of the assertions are direct quotations from ISO/IEC 19790:2025, however what is quoted in each table can be part of a longer sentence or list that is not replicated in this document. For this reason, it is important that the entire text of ISO/IEC 19790:2025 be used to fully understand every assertion's definition, context and conditions.

The assertions are denoted by the form:

AS⟨requirement_number⟩.⟨requirement_number⟩

where "requirement_number" is the number of the corresponding area specified in ISO/IEC 19790:2025 (i.e. 1 to 11 and A to G), and "sequence_number" is a sequential identifier for assertions within a subclause. After the statement of each assertion, the security levels to which the assertion applies (i.e. levels 1 to 4) are listed in parentheses.

Following each assertion in its corresponding table is a set of requirements levied on the vendor. These requirements describe the types of documentation or explicit information that the vendor shall provide in order for the tester to verify conformity to the given assertion. These requirements are denoted by the form:

VE⟨requirement_number⟩.⟨assertion_sequence_number⟩.⟨sequence_number⟩

where "requirement_number" and "assertion_sequence_number" are identical to the corresponding assertion requirement number and sequence number, and "sequence_number" is a sequential identifier for vendor requirements within the assertion requirement.

Following each assertion and the requirements levied on the vendor in the table, there are a set of requirements levied on the tester of the cryptographic module. These requirements instruct the tester as to what he or she shall do in order to test the cryptographic module with respect to the given assertion. These requirements are denoted by the form:

TE⟨requirement_number⟩.⟨assertion_sequence_number⟩.⟨sequence_number⟩

where "requirement_number" and "assertion_sequence_number" are identical to the corresponding assertion requirement number and sequence number, and "sequence_number" is a sequential identifier for tester requirements within the assertion requirement.

Tables give the assertions ASs, the requirements levied on the vendor VEs, the requirements levied on the tester TEs, notes if applicable and examples if applicable.

A certification body may modify, add, or delete either VEs or TEs, or both, in this document.

5.3 Assertions with cross references

For clarity, some assertions have been provided and cross references to other assertions and related text have been put between curly brackets "{" and "}".

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6 Security requirements

6.1 General

Table 1 — VE and TE of AS01.01

General — levels 1, 2, 3 and 4	
AS01.01 ISO/IEC 19790:2025, 7.1	This clause specifies the security requirements that cryptographic modules shall follow.
Required test procedures	
This assertion is not separately tested.	

Table 2 — VE and TE of AS01.02

General — levels 1, 2, 3 and 4	
AS01.02 ISO/IEC 19790:2025, 7.1	A cryptographic module shall be tested against the requirements of each area addressed in this clause.
Required test procedures	
This assertion is not separately tested.	
NOTE 1 The tests can be performed in one or more of the following manners. a) The tester performs tests at the tester's facility. b) The tester performs tests at the vendor's facility. c) The tester supervises vendor performing tests at the vendor's facility. 1) Rationale is included that explains why the tester could not perform the tests. 2) The tester develops the required test plan and required tests. 3) The tester directly observes the tests being performed. d) The tester can reference existing evidence of compliance (e.g. third party certificate or test report) where permitted by a given certification body or accreditation body for the testing laboratory. NOTE 2 An assertion fails if any of its subsequent tests fail. NOTE 3 The accreditation body for testing laboratory refers to ISO/IEC TS 23532-2.	

Table 3 — VE and TE of AS01.03

General — levels 1, 2, 3 and 4	
AS01.03 ISO/IEC 19790:2025, 7.1	The cryptographic module level shall be independently determined in each area.
Required test procedures	
This assertion is not separately tested.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 4 — VE and TE of AS01.04

General — levels 1, 2, 3 and 4	
AS01.04 ISO/IEC 19790:2025, 7.1	All documentation, including copies of the user and installation manuals, design specifications and life cycle documentation shall be provided for a cryptographic module that undergoes independent testing.
Required test procedures	
This assertion is not separately tested.	

6.2 Cryptographic module specification

6.2.1 Cryptographic module specification general requirements

Table 5 — VE and TE of AS02.01

Cryptographic module specification general requirements — levels 1, 2, 3 and 4	
AS02.01 ISO/IEC 19790:2025, 7.2.1	A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof, which at a minimum, implements a defined cryptographic service employing an approved security function as specified in ISO/IEC 19790:2025, Annex C, or process, and is contained within a defined cryptographic boundary.
Required test procedures	
This assertion is not separately tested.	

Table 6 — VE and TE of AS02.02

Cryptographic module specification general requirements — levels 1, 2, 3 and 4	
AS02.02 ISO/IEC 19790:2025, 7.2.1	The documentation for cryptographic module specification specified in ISO/IEC 19790:2025, A.2.1 shall be provided.
Required test procedures	
This assertion is tested as part of ASA.01.	

6.2.2 Types of cryptographic modules

Table 7 — VE and TE of AS02.03

Types of cryptographic modules — levels 1, 2, 3 and 4	
AS02.03 ISO/IEC 19790:2025, 7.2.2	A cryptographic module shall be defined as either a hardware module, firmware module, hybrid firmware module, software module, or hybrid software module.
Required vendor information	
VE02.03.01	The vendor shall provide a description of the cryptographic module describing the type of cryptographic module. It will explain the rationale of the module type selection.
VE02.03.02	The vendor shall provide a specification of the cryptographic module identifying all hardware and either software and firmware components of the cryptographic module as applicable.
Required test procedures	
TE02.03.01	The tester shall verify that the documentation provided by the vendor identifies one of the module types listed in AS02.03.
TE02.03.02	The tester shall review the specific documentation provided by the vendor, by identifying all hardware and either software or firmware components (AS02.13 to AS02.16), to verify that the cryptographic module is consistent with the type of the cryptographic module.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 8 — VE and TE of AS02.04

Types of cryptographic modules — levels 1, 2, 3 and 4	
AS02.04 ISO/IEC 19790:2025, 7.2.2	For hardware, firmware or hybrid firmware modules, the applicable physical security and non-invasive security requirements specified in ISO/IEC 19790:2025, 7.7 and ISO/IEC 19790:2025, 7.8 shall apply.
Required test procedures	
This assertion is not separately tested.	

6.2.3 Cryptographic boundary

6.2.3.1 Cryptographic boundary general requirements

Table 9 — VE and TE of AS02.05

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.05 ISO/IEC 19790:2025, 7.2.3.1	A cryptographic boundary shall consist of an explicitly defined perimeter (i.e. set of hardware, software or firmware components) that establishes the boundary of all components of the cryptographic module.
Required vendor information	
VE02.05.01	The vendor-provided documentation shall specify all components within the cryptographic boundary.
Required test procedures	
TE02.05.01	The tester shall review the vendor-provided documentation and inspect the cryptographic module to verify that all the components specified in AS02.13 to AS02.16 are within the cryptographic boundary.
TE02.05.02	The tester shall review the vendor-provided documentation and inspect the cryptographic module to verify that there are no unidentified components which are not specified in AS02.13 to AS02.16 within the cryptographic boundary.

Table 10 — VE and TE of AS02.06

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.06 ISO/IEC 19790:2025, 7.2.3.1	The requirements of this document shall apply to all security functions, processes and components within the module's cryptographic boundary.
Required test procedures	
This assertion is not separately tested.	

Table 11 — VE and TE of AS02.07

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.07 ISO/IEC 19790:2025, 7.2.3.1	The cryptographic boundary shall, at a minimum, encompass all security relevant security functions, processes and components of a cryptographic module as defined in ISO/IEC 19790:2025, Clause 7.
Required vendor information	
VE02.07.01	The vendor shall provide a list of all the security relevant security functions, processes, and components within the cryptographic boundary.
Required test procedures	
TE02.07.01	The tester shall verify that the documentation provided by the vendor clearly identifies and lists all the security relevant security functions, processes, and components of the module within the cryptographic boundary.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 12 — VE and TE of AS02.08

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.08 ISO/IEC 19790:2025, 7.2.3.1	Non-security relevant security functions, processes or components which are used in approved services shall be implemented in a manner so as to not interfere or compromise the approved operation of the cryptographic module.
Required vendor information	
VE02.08.01	The vendor-provided documentation shall list the non-security relevant functions used in an approved service and justify that they are not interfering with the approved service of the module.
Required test procedures	
TE02.08.01	The tester shall review documentation and inspect the module to verify that the non-security relevant functions do not interfere or compromise the approved service of the module.
TE02.08.02	The tester shall verify the correctness of any rationale provided by the vendor for not interfering nor compromising the service. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall ask the vendor to produce additional information as needed.

Table 13 — VE and TE of AS02.09

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.09 ISO/IEC 19790:2025, 7.2.3.1	The defined name of a cryptographic module shall be representative of the composition of the components within the cryptographic boundary and not representative of a larger composition or product.
Required vendor information	
VE02.09.01	The vendor shall provide the defined name of the module.
Required test procedures	
TE02.09.01	The tester shall verify that the module name provided by the vendor is consistent with the composition of the components within the cryptographic boundary.
TE02.09.02	The tester shall verify that the module name does not represent a composition of components or functions that are not consistent with the composition of the components within the cryptographic boundary.

Table 14 — VE and TE of AS02.10

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.10 ISO/IEC 19790:2025, 7.2.3.1	The cryptographic module shall have, at minimum, specific versioning information representing the distinct individual hardware and software or firmware components as applicable.
Required vendor information	
VE02.10.01	The vendor shall provide the versioning information of the module's distinct individual hardware and either software or firmware components.
Required test procedures	
TE02.10.01	The tester shall verify that the versioning information represents the modules distinct individual hardware and either software or firmware components.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 15 — VE and TE of AS02.11

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.11 ISO/IEC 19790:2025, 7.2.3.1	The excluded hardware, software or firmware components shall be implemented in such a manner to not interfere or compromise the approved secure operation of the cryptographic module.
Required vendor information	
VE02.11.01	The vendor shall describe the excluded components of the module and justify that these components will not interfere with the approved secure operation of the module.
VE02.11.02	The vendor-provided documentation shall provide the rationale for excluding each of the components. The rationale shall describe how each excluded component, when working properly or when it malfunctions, shall not interfere with the approved secure operation of the module. Rationale that can be acceptable, if adequately supported by documentation, includes the following. a) The component is not connected with security relevant components of the module that would allow inappropriate transfer of SSPs, plaintext data, or other information that could interfere with the approved secure operation of the module. b) All information processed by the component is strictly for internal use of the module, and does not in any way impact the correctness of control, status or data outputs.
Required test procedures	
TE02.11.01	The tester shall review the documentation provided by the vendor to inspect that the excluded components within the cryptographic boundary will not interfere with the approved secure operation of the module.
TE02.11.02	The tester shall verify the correctness of any rationale for exclusion provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall ask the vendor to produce additional information as needed.
TE02.11.03	The tester shall manipulate (e.g. to cause the component to operate not as designed) the excluded components in a manner to cause incorrect operation of the excluded component. The tester shall verify that the incorrect operation of the excluded component shall not interfere with the approved secure operation of the module. NOTE 1 Testing can rely on either code review, documentation, or both, if behavioural or physical methods which cause the incorrect operation of the excluded component are infeasible or impractical for a given module. Behavioural methods include using a debugger, code manipulator/injector, simulator, or another tool to manipulate data that can impact the behaviour of an excluded component; physical methods include shorting/removing pins and voltage manipulations. Testing is considered infeasible or impractical when such manipulations are understood to permanently damage the module, or the system in which it is contained, without achieving any desired security goals beyond simply rendering the entire module inoperable. NOTE 2 The tests are intended to focus on the secure operation of the module and not on other aspects such as reliability or quality, unless they help prove lack of interference with the approved secure operation of the module.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 16 — VE and TE of AS02.12

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.12 ISO/IEC 19790:2025, 7.2.3.1	Any excluded hardware, software or firmware residing within the module's cryptographic boundary shall be specified in accordance with ISO ISO/IEC 19790:2025, Annex A and listed in the module security policy in accordance with ISO ISO/IEC 19790:2025, Annex B.
Required vendor information	
VE02.12.01	Any components that are excluded from the security requirements shall be explicitly listed in the vendor-provided documentation as specified in ISO ISO/IEC 19790:2025, Annex A.
VE02.12.02	Any components that are excluded from the security requirements shall be explicitly listed in the non-proprietary security policy.
Required test procedures	
TE02.12.01	The tester shall verify based on the vendor-provided documentation whether the vendor indicates that any components of the module are excluded from the requirements of ISO ISO/IEC 19790:2025.

6.2.3.2 Definitions of cryptographic boundary

Table 17 — VE and TE of AS02.13

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.13 ISO/IEC 19790:2025, 7.2.3.2	The cryptographic boundary of a hardware cryptographic module shall delimit and identify: a) the set of hardware elements which may include: 1) physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between elements; 2) active electrical elements such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc; and 3) physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces. b) a limited or non-modifiable OE; c) firmware, which may include an operating system; and d) other element types not listed in a), b) or c), (e.g. configuration files for a CPLD).
Required vendor information	
VE02.13.01	All hardware elements of the cryptographic module shall be identified in the vendor-provided documentation. Elements to be listed shall include all of the following: a) physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between elements: 1) circuit boards, substrates and mounting surfaces;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 17 *(continued)*

	b) active electrical elements such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc.: 1) processors, including microprocessors, digital signal processors, custom processors, microcontrollers, or any other types of processors (identify manufacturer and type); 2) read-only memory (ROM) integrated circuits for program executable code and data [this may include mask-programmed ROM, programmable ROM (PROM) such as ultraviolet, erasable PROM (EPROM), electrically erasable PROM (EEPROM), or Flash-memory]; 3) random-access memory (RAM) or other integrated circuits for temporary data storage; 4) semi-custom, application-specific integrated circuits, such as gate arrays, programmable logic arrays, field programmable gate arrays, or other programmable logic devices; 5) fully custom, application-specific integrated circuits, including any custom cryptographic integrated circuits; 6) power supply elements, including power supply, power converters (e.g. AC-to-DC or DC-to-DC modules, transformers), input power connectors and output power connectors; 7) other active electronic circuit elements (passive circuit elements such as pull up/pull down resistors or bypass capacitors are not necessary to include if they do not provide security relevant function as part of the cryptographic module); c) physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces: 1) physical structures and enclosures, including any removable access doors or covers; 2) potting or encapsulation materials; 3) boundary connectors; 4) connectors between major independent sub-assemblies within the module; d) firmware, which can include an operating system: 1) executable code: i) non-modifiable; ii) limited; e) other elements types not listed above: 1) cooling or heating arrangements, such as conduction plates, cooling airflow, heat exchanger, cooling fins, fans, heaters, or other arrangements for removing or adding heat.
VE02.13.02	The vendor-provided documentation shall indicate the internal layout and assembly methods (e.g. fasteners and fittings) of the module, including drawings that are at least approximately to scale.
VE02.13.03	The vendor-provided documentation shall describe the primary physical parameters of the module, including descriptions of the enclosure, access points, circuit boards, location of power supply, inter-connection wiring runs, cooling arrangements, and any other significant parameters.
VE02.13.04	The vendor-provided documentation shall include a block diagram which represents the module's cryptographic boundary and relationship of the hardware elements.
VE02.13.05	For each processor in the 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.
VE02.13.06	For each processor, the vendor shall identify any hardware with which the processor interfaces.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 17 *(continued)*

TE02.13.01	The tester shall identify all hardware elements of the cryptographic module. Elements to be listed shall include all of the following: a) physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between elements: 1) circuit boards, substrates and mounting surfaces; b) active electrical elements such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc: 1) processors, including microprocessors, digital signal processors, custom processors, microcontrollers, or any other types of processors (identify manufacturer and type); 2) read-only memory (ROM) integrated circuits for program executable code and data [this can include mask-programmed ROM, electrically erasable PROM (EEPROM), or Flash-memory]; 3) random-access memory (RAM) or other integrated circuits for temporary data storage; 4) custom (ASIC), semi-custom (FPGA, CPLD), or off-the-shelf elements such as gate arrays, programmable logic arrays, field programmable gate arrays, or other programmable logic devices; 5) fully custom, application-specific, integrated circuits, including any custom cryptographic integrated circuits; 6) power supply elements, including power supply, power converters (e.g. AC-to-DC or DC-to-DC modules, transformers), input power connectors, and output power connectors; 7) other active electronic circuit elements (passive circuit elements such as pull up/pull down resistors or bypass capacitors are not necessary to be included if they do not provide security relevant function as part of the cryptographic module); c) physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces: 1) physical structures and enclosures, including any removable access doors or covers; 2) potting or encapsulation materials; 3) boundary connectors; 4) connectors between major independent sub-assemblies within the module; d) firmware, which can include an operating system: 1) executable code: i) non-modifiable; ii) limited; e) other elements types not listed above: 1) cooling or heating arrangements, such as conduction plates, cooling airflow, heat exchanger, cooling fins, fans, heaters, or other arrangements for removing or adding heat.
TE02.13.02	The tester shall verify that the elements list is consistent with the information provided for other assertions of 6.2.3, as defined below.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 17 *(continued)*

	a) The specification of the cryptographic boundary under assertion AS02.05. Verify that all elements inside the cryptographic boundary are included in the elements list and vice versa. Also verify that any elements outside the cryptographic boundary are not listed as elements of the cryptographic module. b) The specification of the block diagram under assertion ISO/IEC 19790:2025, A.2.1. Verify that any individual elements identified in the block diagram (e.g. processors, application specific integrated circuits) are also listed in the elements list. c) Any elements that shall be excluded from the requirements of ISO/IEC 19790:2025 under the provisions of assertions AS02.11 and AS02.12. Verify that excluded elements are still listed in the elements list.
TE02.13.03	The tester shall verify that the cryptographic boundary is physically contiguous, such that there are no gaps that could allow uncontrolled input, output, or other access into the cryptographic module. The tester shall verify that there are no uncontrolled interfaces into or out of the cryptographic module in the module design. NOTE Physical protection and tamper protection are covered separately in requirements under ISO/IEC 19790:2025, 7.7.
TE02.13.04	The tester shall verify that the cryptographic boundary encompasses all elements that are identified in the block diagram under assertion ISO/IEC 19790:2025, A.2.1 as inputting, outputting, or processing SSPs, plaintext data, or other information.
TE02.13.05	As a partial exception to AS02.13, the vendor is allowed to exclude certain elements from the requirements of ISO/IEC 19790:2025 after satisfying the requirements under assertions AS02.11 and AS02.12 in 6.2.3. The tester shall verify that any interfaces or physical connections between such excluded elements and the rest of the module do not allow the following: a) uncontrolled release of Critical Security Parameters (CSP), plaintext data, or other information that if misused could lead to a compromise; b) uncontrolled modifications of SSPs or other information that could lead to a compromise.
TE02.13.06	The tester shall verify that the vendor's documentation shows the internal layout of the module, including the placement and approximate dimensions of major identifiable elements of the module. This shall include drawings that are at least approximately to scale.
TE02.13.07	The tester shall verify that the vendor's documentation indicates the major physical assemblies of the module and how they are assembled or inserted into the module.
TE02.13.08	The tester shall verify that the vendor's documentation describes the primary physical parameters of the module. This description shall include at least the following: a) enclosure shape and approximate dimensions, including any access doors or covers; b) circuit board(s) approximate dimensions, layout, and interconnections; c) location of power supply, power converters, and power inputs and outputs; d) interconnection wiring runs: routing and terminals; e) cooling or heating arrangements, such as conduction plates, cooling airflow, heat exchanger, cooling fins, fans, heaters, or other arrangements for removing heat from or adding heat to the module; f) other element types not listed above.
TE02.13.09	The tester shall verify that the block diagram provided by the vendor represents the module's cryptographic boundary and relationship of the hardware elements.
TE02.13.10	The tester shall verify the documentation provided under assertion AS02.02, with a focus on the block diagram depicting all of the major hardware elements of a cryptographic module and element interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory and program memory.
TE02.13.11	The tester shall verify that the block diagram indicates all significant interconnections and data flow among major elements of the module, and between the module and outside equipment. In particular, each line on the block diagram indicating an interconnection shall be labelled with the type of information it transmits.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 17 *(continued)*

TE02.13.12	The tester shall verify that the block diagram indicates the cryptographic boundary for the cryptographic module, as required under this assertion.
TE02.13.13	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.
TE02.13.14	The tester shall verify that, for each processor, the vendor has identified any hardware with which the processor interfaces. This shall include, as applicable, any hardware elements that provide input, control, or status data to the processor and associated software/firmware, and any hardware elements that receive output, control, or status data from the processor and associated software/firmware. Such hardware elements may be within the cryptographic module or may be user equipment outside the module such as input/output devices.

Table 18 — VE and TE of AS02.14

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.14 ISO/IEC 19790:2025, 7.2.3.2	The cryptographic boundary of a software cryptographic module shall delimit and identify: a) the set of executable files or other files that constitute the cryptographic module; and b) the instantiation of the cryptographic module saved in memory and executed by one or more processors.
Required vendor information	
VE02.14.01	All software files of the cryptographic module shall be identified in the vendor-provided documentation. Files to be listed shall include all of the following: a) the set of executable file or other files that constitute the cryptographic module; b) other security relevant file types not listed above.
VE02.14.02	The vendor-provided documentation shall indicate the internal software architecture, including how the software files interact.
VE02.14.03	The vendor-provided documentation shall indicate the operational environment (e.g. operating system, run-time library, etc.) on which the module executes.
Required test procedures	
TE02.14.01	The tester shall verify that the documentation includes a files list that includes all software files of the cryptographic module.
TE02.14.02	The tester shall verify that the files list includes all occurrences of the following types of files, excluding only file types that are not used in the module: a) the set of executable file or other files that constitute the cryptographic module; b) other security file types not listed above.
TE02.14.03	The tester shall verify that the files list is consistent with information provided for other assertions of 6.2.3, as defined below. a) The specification of the cryptographic boundary under assertion AS02.05. Verify that all files inside the cryptographic boundary are included in the files list and vice versa. Also verify that any files outside the cryptographic boundary are not listed as files of the cryptographic module. b) The specification of the software under assertion ISO/IEC 19790:2025, A.2.1. Verify that the list of software files is the same as in the specifications under assertion AS02.05. c) The specification of the block diagram under assertion ISO/IEC 19790:2025, A.2.1. Verify that any individual files identified in the block diagram are also listed in the files list. d) Any files that shall be excluded from the requirements of ISO/IEC 19790:2025 under the provisions of assertions AS02.13 and AS02.14. Verify that excluded files are still listed in the files list.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 18 *(continued)*

TE02.14.04	As a partial exception to the above requirements, the vendor is allowed to exclude certain files from the requirements of ISO/IEC 19790:2025 after satisfying the requirements under assertions AS02.11 and AS02.12 in 6.2.3. The tester shall verify that any interfaces or physical connections between such excluded files and the rest of the module do not allow the following: a) uncontrolled release of CSPs, plaintext data, or other information that if misused can lead to a compromise; b) uncontrolled modifications of SSPs or other information that can lead to a compromise.
TE02.14.05	The tester shall verify that the vendor's documentation indicates the major software files of the module and how they are linked together forming the module.

Table 19 — VE and TE of AS02.15

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.15 ISO/IEC 19790:2025, 7.2.3.2	The cryptographic boundary of a firmware cryptographic module shall delimit and identify: a) the set of executable files or other files that constitute the cryptographic module; and b) the instantiation of the cryptographic module saved in memory and executed by one or more processors.
Required vendor information	
VE02.15.01	All firmware files of the cryptographic module shall be identified in the vendor-provided documentation. Files to be listed shall include all of the following: a) the set of executable files or other files that constitute the cryptographic module; b) other security relevant file types not listed above.
VE02.15.02	The vendor-provided documentation shall indicate the internal firmware architecture, including how the firmware files interact.
VE02.15.03	The vendor-provided documentation shall indicate the operational environment (e.g. operating system, run-time library) on which the module executes.
VE02.15.04	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.
VE02.15.05	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	
TE02.15.01	The tester shall verify that the documentation includes a files list that includes all firmware files of the cryptographic module.
TE02.15.02	The tester shall verify that the files list includes all occurrences of the following types of files, excluding only file types that are not used in the module: a) the set of executable file or other files that constitute the cryptographic module; b) other security file types not listed in a).
TE02.15.03	The tester shall verify that the files list is consistent with information provided for other assertions of 6.2.3, as defined below.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 19 *(continued)*

	a) The specification of the cryptographic boundary under assertion AS02.07. Verify that all files inside the cryptographic boundary are included in the files list and vice versa. Also verify that any files outside the cryptographic boundary are not listed as files of the cryptographic module. b) The specification of the firmware under assertion ISO/IEC 19790:2025, A.2.1. Verify that the list of firmware files is the same as in the specifications under assertion AS02.05. c) The specification of the block diagram under assertion ISO/IEC 19790:2025, A.2.1. Verify that any individual files identified in the block diagram are also listed in the files list. d) Any files that shall be excluded from the requirements of ISO/IEC 19790:2025 under the provisions of assertions AS02.11 and AS02.12. Verify that the excluded files are still listed in the files list.
TE02.15.04	As a partial exception to the above requirements, the vendor is allowed to exclude certain files from the requirements of ISO/IEC 19790:2025 after satisfying the requirements under assertions AS02.11 and AS02.12 in 6.2.3. The tester shall verify that any interfaces or physical connections between such excluded files and the rest of the module do not allow the following: a) uncontrolled release of CSPs, plaintext data, or other information that if misused can lead to a compromise; b) uncontrolled modifications of SSPs or other information that can lead to a compromise.
TE02.15.05	The tester shall verify that the vendor's documentation indicates the major firmware files of the module and how they are linked together forming the module.
TE02.15.06	The tester shall verify the documentation provided under assertion AS02.02, with a focus on the block diagram depicting all of the major hardware elements of a cryptographic module and element interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory.
TE02.15.07	The tester shall verify that the block diagram indicates all significant interconnections and data flows among major elements of the module, and between the module and outside equipment. In particular, each line on the block diagram indicating an interconnection shall be labelled with the type of information it transmits.
TE02.15.08	The tester shall verify that the block diagram indicates the cryptographic boundary for the cryptographic module, as required under this assertion.
TE02.15.09	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.
TE02.15.10	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 shall include, as applicable, any hardware elements that provide input, control, or status data to the processor and associated firmware, and any hardware elements that receive output, control, or status data from the processor and associated firmware. Such hardware elements can be within the cryptographic module or can be user equipment outside the module such as input/output devices.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 20 — VE and TE of AS02.16

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.16 ISO/IEC 19790:2025, 7.2.3.2	The cryptographic boundary of a hybrid cryptographic module shall: a) be the composite of the module's hardware component and the disjoint software or firmware component(s); and b) include the collection of all ports and interfaces from each component.
Required vendor information	
VE02.16.01	The cryptographic module shall be identified in the vendor-provided 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 VE02.13.01 to VE02.13.06 and VE02.14.01 to VE02.14.03. b) For hybrid firmware module components, the vendor documentation shall provide information required under VE02.13.01 to VE02.13.06 and VE02.15.01 to VE02.15.05.
Required test procedures	
TE02.16.01	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 TE02.13.01 to TE02.13.14 and TE02.14.01 to TE02.14.05. b) For hybrid firmware module components, the tester shall follow procedures required under TE02.13.01 to TE02.13.14 and TE02.15.01 to TE02.15.10.
NOTE In addition to the disjoint software or firmware component(s), the hardware component can also include embedded software or firmware.	

6.2.4 Module operations

6.2.4.1 Module operations general requirements

Table 21 — VE and TE of AS02.17

Module operations — levels 1, 2, 3 and 4	
AS02.17 ISO/IEC 19790:2025, 7.2.4.1	The operator shall be able to operate the module utilising approved services.
Required vendor information	
VE02.17.01	The vendor-provided non-proprietary security policy shall provide a description of the approved services.
VE02.17.02	The vendor-provided non-proprietary security policy shall provide instructions for invoking the approved services.
Required test procedures	
TE02.17.01	The tester shall verify that the vendor-provided non-proprietary security policy contains a description of the approved services.
TE02.17.02	The tester shall invoke the approved services using the vendor-provided instructions found in the non-proprietary security policy. The tester shall verify, by inspection and from the vendor-provided documentation, that the cryptographic module utilizes the approved services as a result of documented instructions.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 22 — VE and TE of AS02.18

Module operations — levels 1, 2, 3 and 4	
AS02.18 ISO/IEC 19790:2025, 7.2.4.1	An approved service shall be defined as a service that includes at least one approved security function or process, and can include non-security relevant functions or processes.
Required vendor information	
VE02.18.01	The vendor shall provide a validation certificate if available for each approved security function.
VE02.18.02	The vendor shall provide a list of all non-approved security functions.
VE02.18.03	The vendor shall provide a list of all vendor affirmed security functions.
VE02.18.04	The vendor-provided non-proprietary security policy shall include a list of all vendor affirmed security functions.
Required test procedures	
TE02.18.01	The tester shall verify that the vendor has provided a validation certificate if available for each approved security function issued by a certification body.
TE02.18.02	The tester shall verify that the vendor has provided the list of non-approved security functions.
TE02.18.03	The tester shall verify that the vendor has provided the list of vendor affirmed security functions.
TE02.18.04	The tester shall verify that the documentation provided by the vendor specifies how the implemented vendor affirmed security functions conform to the relevant standards.

Table 23 — VE and TE of AS02.19

Module operations — levels 1, 2, 3 and 4	
AS02.19 ISO/IEC 19790:2025, 7.2.4.1	Non-approved security functions and processes shall not be utilized by the operator in an approved service unless the non-approved security function or process is not security relevant to the approved process or service's operation (e.g. a non-approved security function or non-approved generated key may be used to obfuscate data or CSPs but the result is considered plaintext and provides no security relevant functionality until it is protected with an approved security function).
Required vendor information	
VE02.19.01	The vendor-provided documentation shall identify all of non-approved security functions or processes utilized for each approved service or process.
VE02.19.02	The vendor-provided documentation shall provide a rationale for why utilized non-approved security functions or processes are considered non-security relevant to the approved processes' or service's operation. This rationale shall address how approved algorithm CSPs are kept exclusive to the approved algorithms within the service and protected from the non-approved algorithms within that same service.
Required test procedures	
TE02.19.01	The tester shall inspect the module to verify that the vendor-provided documentation identifies all of the non-approved security functions or processes utilized for each approved service or process.
TE02.19.02	The tester shall verify the correctness 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 ask the vendor to produce additional information as needed.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.2.4.2 Normal operation

Table 24 — VE and TE of AS02.20

Module operations — levels 1, 2, 3 and 4	
AS02.20 ISO/IEC 19790:2025, 7.2.4.2	CSPs shall be exclusive between approved and non-approved services (e.g. not shared or accessed).
Required vendor information	
VE02.20.01	The vendor shall provide a list of all CSPs within the module and identify their usage between approved and non-approved services.
VE02.20.02	The vendor shall provide a description of how each CSP becomes exclusive between approved and non-approved services.
VE02.20.03	The vendor shall provide a list of CSPs that are accessible both approved and non-approved services, and shall document how the shared access cannot weaken the security of the CSP or increase its risk of compromise.
Required test procedures	
TE02.20.01	The tester shall verify that the documentation provided by the vendor contains a description of the usage of each CSP between approved and non-approved services.
TE02.20.02	The tester shall inspect the module and review the vendor-provided documentation to verify that the CSPs are exclusive between approved and non-approved services.
TE02.20.03	The tester shall verify that any CSPs that are accessible by both approved and non-approved services cannot weaken the security of the CSP or increase its risk of compromise.

Table 25 — VE and TE of AS02.21

Module operations — levels 1, 2, 3 and 4	
AS02.21 ISO/IEC 19790:2025, 7.2.4.2	The module's security policy shall define the complete set of services: approved, non-approved, and non-security related.
Required test procedures	
This assertion is tested as part of ASB.01.	
NOTE The complete set of services is defined as all of the services provided by the module. This includes both approved and non-approved services.	

Table 26 — VE and TE of AS02.22

Module operations — levels 1, 2, 3 and 4	
AS02.22 ISO/IEC 19790:2025, 7.2.4.2	Each service shall provide an output indicator upon completion of the service to indicate whether the service executed an approved security function or process, or not.
Required vendor information	
VE02.22.01	The documentation provided by the vendor shall specify the output indicator for each service.
VE02.22.02	If a single encryption service supports both approved and non-approved key strengths, or approved and non-approved security functions, the vendor-provided documentation shall describe how the output indicator changes to indicate an approved or non-approved service.
Required test procedures	
TE02.22.01	The tester shall verify that the vendor-provided documentation contains a description of the output indicator indicating whether the service executes an approved security function or process in an approved manner or not.
TE02.22.02	The tester shall execute all services and verify that the output indicator provides an unambiguous indication of whether the service utilizes an approved security function or process in an approved manner or not.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 26 *(continued)*

TE02.22.03	If a single encryption service supports both approved and non-approved key strengths, or approved and non-approved security functions, the tester shall verify that the vendor documentation describes how the output indicator changes to indicate an approved or non-approved service.
TE02.22.04	If a single encryption service supports both approved and non-approved key strengths, the tester shall execute the service with both approved and non-approved key strengths and verify that the output indicator changes to indicate an approved or non-approved service.
TE02.22.05	If a single encryption service supports both approved and non-approved security functions or processes, the tester shall execute the service with both approved and non-approved security functions or processes, and verify that the output indicator changes to indicate an approved or non-approved service.

6.2.4.3 Degraded operation

Table 27 — VE and TE of AS02.23

Module operations — levels 1, 2, 3 and 4	
AS02.23 ISO/IEC 19790:2025, 7.2.4.3	For a cryptographic module to operate in degraded operation, the following shall apply:{AS02.24 to AS02.28}
Required test procedures	
This assertion is not separately tested.	

Table 28 — VE and TE of AS02.24

Module operations — levels 1, 2, 3 and 4	
AS02.24 ISO/IEC 19790:2025, 7.2.4.3	degraded operation shall be entered only after exiting an error state;
Required vendor information	
VE02.24.01	If the cryptographic module allows a degraded operation, the vendor shall provide a description of all degraded operation after exiting each error state.
VE02.24.02	The vendor shall provide specification of degraded operation. For each degraded operation, the specification shall include: a) conditions of entry into and exit from the degraded operation; b) operational security functions, services, or processes; c) non-functioning security functions, services, or processes; d) isolated mechanisms, functions, or components in the degraded operation; e) techniques to isolate mechanisms, functions, or components; f) status information provided in the degraded operation; g) status indicator if attempts are made to use a non-functioning security function, or process.
Required test procedures	
TE02.24.01	The tester shall verify that the documentation provided by the vendor clearly identifies the degraded operation and its conditions of entry and exit.
TE02.24.02	The tester shall use the documentation provided the vendor to check that the degraded operation can only be accessed after exiting an error state. The tester shall check that the error status indicator (see AS03.11) is correctly positioned.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 28 *(continued)*

TE02.24.03	The tester shall exercise the cryptographic module, causing it to operate in each degraded operation. For each degraded operation, the tester shall attempt to perform a service to verify that all conditional security function self-tests are performed prior to the first operational use of any security function.
TE02.24.04	The tester shall first exercise the cryptographic module, causing it to operate in each degraded operation. The tester shall next perform all pre-operational self-tests. If the cryptographic module passes all pre-operational self-tests without failure, the tester will verify that the cryptographic module exits degraded operation and returns to normal operation.
TE02.24.05	The tester shall first exercise the cryptographic module, causing it to operate in each degraded operation. The tester shall next perform all pre-operational self-tests causing an error condition in pre-operational self-tests to occur. The tester shall verify that the cryptographic module does not remain in degraded operation but enters an error state.

Table 29 — VE and TE of AS02.25

Module operations — levels 1, 2, 3 and 4	
AS02.25 ISO/IEC 19790:2025, 7.2.4.3	The module shall provide status information when re-configured and degraded operation entered;
Required test procedures	
This assertion is tested as part of AS02.24.	

Table 30 — VE and TE of AS02.26

Module operations — levels 1, 2, 3 and 4	
AS02.26 ISO/IEC 19790:2025, 7.2.4.3	the mechanism or process that failed shall be isolated;
Required vendor information	
VE02.26.01	The vendor-provided documentation requirement is specified under VE02.24.02. The vendor design shall ensure that any failure from the failed mechanisms, processes, and components cannot interfere or compromise the approved operation of the cryptographic module.
Required test procedures	
TE02.26.01	The tester shall inspect the module and review the vendor-provided documentation to verify that failed mechanisms, processes, and components are isolated before entering degraded operation.
TE02.26.02	The tester shall inspect the module and review the vendor-provided documentation to verify that failed mechanisms, processes, and components cannot interfere or compromise the approved operation of the cryptographic module.

Table 31 — VE and TE of AS02.27

Module operations — levels 1, 2, 3 and 4	
AS02.27 ISO/IEC 19790:2025, 7.2.4.3	all applicable conditional cryptographic algorithm self-tests shall be performed prior to the first operational use of the cryptographic algorithm after entering degraded operation;
Required test procedures	
This assertion is tested as part of AS02.24.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 32 — VE and TE of AS02.28

Module operations — levels 1, 2, 3 and 4	
AS02.28 ISO/IEC 19790:2025, 7.2.4.3	services shall provide an indicator if attempts are made to use the mechanism or process that failed.
Required vendor information	
VE02.28.01	The vendor-provided documentation requirement is specified under VE02.24.02. The vendor design shall ensure that service output includes an indicator if attempts are made to use the mechanism, or process that failed.
Required test procedures	
TE02.28.01	The tester shall verify from the vendor documentation that services provide documented indicators if attempts are made to use the mechanism, or process that failed.
TE02.28.02	The tester shall exercise the cryptographic module and verify that the documented indicator is provided if attempts are made to use the mechanism or process that failed.

Table 33 — VE and TE of AS02.29

Module operations — levels 1, 2, 3 and 4	
AS02.29 ISO/IEC 19790:2025, 7.2.4.3	Where a localized error is used, it shall be shown that the target error cannot impact other approved services running outside the isolated mechanism or process.
Required vendor information	
VE02.29.01	The vendor-provided documentation shall specify that the localized error does not impact other approved services running outside the isolated mechanism or process.
Required test procedures	
TE02.29.01	The tester shall verify from the vendor-provided documentation that the target error does not impact other approved services running outside the isolated mechanism or process.
TE02.29.02	The tester shall exercise the cryptographic module and verify that the module operates according to the documentation.
TE02.29.03	The tester shall trigger errors to the module. The tester shall determine if a triggered error is either localized or not (i.e. causes the entire module to enter the error state).
TE02.29.04	The tester shall inject errors to the module. If the tester determines that an injected error is localized, then the tester shall continue to operate the module to determine that the error does not propagate to other approved services running outside the isolated mechanism or process.

Table 34 — VE and TE of AS02.30

Module operations — levels 1, 2, 3 and 4	
AS02.30 ISO/IEC 19790:2025, 7.2.4.3	The cryptographic module shall remain in degraded operation until the cryptographic module has repeated pre-operational test self-tests covering either the entire module or the failed isolated mechanisms and processes.
Required vendor information	
VE02.30.01	The vendor-provided documentation shall specify that the cryptographic module remains in degraded operation until the cryptographic module has repeated pre-operational test self-tests.
VE02.30.02	The vendor-provided documentation shall specify what pre-operational self-tests are needed to exit the degraded state for every defined isolated mechanism or process.
Required test procedures	
TE02.30.01	The tester shall verify from the vendor-provided documentation that the cryptographic module remains in degraded operation until the cryptographic module has repeated pre-operational test self-tests.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 34 *(continued)*

TE02.30.02	The tester shall exercise the cryptographic module and verify that the module operates according to the documentation.
TE02.30.03	After the tester has injected an error and the module transitions to the degraded state, the tester shall cause the module to initiate the pre-operational self-tests for the entire module and determine that the module transitions from the degraded state to the non-degraded state.
TE02.30.04	After the tester has injected an error and the module transitions to the degraded state, the tester shall execute the pre-operational self-tests for only the failed isolated mechanisms and processes, and determine if the module transitions from the degraded state to the non-degraded state.

Table 35 — VE and TE of AS02.31

Module operations — levels 1, 2, 3 and 4	
AS02.31 ISO/IEC 19790:2025, 7.2.4.3	When only a subset of pre-operational self-tests are re-run ahead of exiting degraded operation, it shall be demonstrated why it was not necessary to re-run the excluded self-tests.
Required vendor information	
VE02.31.01	The vendor documentation shall demonstrate why it is not necessary to re-run excluded self-tests when only a subset of pre-operational self-tests are re-run ahead of exiting the degraded operation.
Required test procedures	
TE02.31.01	The tester shall review the vendor documentation to ensure that, when pre-operational self-tests re-run ahead of exiting the degraded operation only cover a sub-set of tests performed on power-on, it is not required to re-run the excluded self-test.
TE02.31.02	The tester shall exercise the cryptographic module and verify that the module operates according to the documentation.
TE02.31.03	After the tester has only run the sub-set of self-tests, the tester shall then run the module operationally for a sufficient period of time, utilizing all services of the module, to determine that the error in the isolated areas did not propagate to other areas of the module.

Table 36 — VE and TE of AS02.32

Module operations — levels 1, 2, 3 and 4	
AS02.32 ISO/IEC 19790:2025, 7.2.4.3	If the cryptographic module passes all the pre-operational self-tests while in degraded operation, the module shall exit degraded operation.
Required test procedures	
This assertion is tested as part of AS02.24.	

Table 37 — VE and TE of AS02.33

Module operations — levels 1, 2, 3 and 4	
AS02.33 ISO/IEC 19790:2025, 7.2.4.3	If the cryptographic module fails the pre-operational self-tests while in degraded operation, the module shall enter an error state.
Required test procedures	
This assertion is tested as part of AS02.24.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.3 Cryptographic module interfaces

6.3.1 Cryptographic module interfaces general requirements

Table 38 — VE and TE of AS03.01

Cryptographic module interfaces general requirements — levels 1, 2, 3 and 4	
AS03.01 ISO/IEC 19790:2025, 7.3.1	A cryptographic module shall restrict all logical information flow to only those physical access points and logical interfaces that are identified as entry and exit points to and from the cryptographic boundary of the module.
Required vendor information	
VE03.01.01	The vendor-provided documentation shall specify each of the physical ports and logical interfaces of the cryptographic module, including the following: a) physical ports and their pin assignments; b) physical covers, doors or openings; c) logical interfaces (e.g. APIs and all other data/control/status signals) and the signal names and functions; d) manual controls (e.g. buttons or switches) for applicable physical control inputs; e) physical status indicators (e.g. lights or displays) for applicable physical status outputs; f) mapping of the logical interfaces to the physical ports, manual controls, and physical status indicators of the cryptographic module; g) physical, logical, and electrical characteristics, as applicable, of the ports and interfaces specified in a) to f).
VE03.01.02	The vendor-provided documentation shall specify the information flows and physical access points of the cryptographic module by highlighting or annotating copies of the block diagrams, design specifications, and source code and schematics, as appropriate, provided in 6.2 and 6.11. The vendor shall also provide any other documentation necessary to clearly specify the relationship of the information flows and physical access points to the physical ports and logical interfaces. The vendor shall establish the above information in relation with the information provided under assertions AS02.05 and AS02.13 to AS02.16 without inconsistencies in the description of elements and physical layout for the input/output ports.
VE03.01.03	For each physical or logical input to the cryptographic module, or physical and logical output from the module, the vendor documentation shall specify the logical interface to which the physical input or output belongs, and the physical entry/exit port. The specifications provided shall be consistent with the specifications of the cryptographic module components provided under ISO/IEC 19790:2025, 7.2 and 7.11, and the specifications of the logical interfaces provided in assertions AS03.04 to AS03.13 of 6.3.2.
Required test procedures	
TE03.01.01	The tester shall verify that vendor-provided documentation specifies each of the physical ports and logical interfaces of the cryptographic module. The required specifications shall include: a) all physical input and output ports, including their pin assignments, physical locations within the module, a summary of the logical signals that flow through each port, and the timing sequence of signal flows if two or more signals share the same physical pin; b) all physical covers, doors, or openings, including their physical location within the cryptographic module, and the components or functions that can be accessed or modified via each cover/door/opening; c) all logical input and output interfaces (e.g. APIs and all other data/control/status signals), including a listing or annotated block diagram of all the logical data and control inputs and data and status outputs of the cryptographic module, and a listing and description of the signal names and functions;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 38 *(continued)*

	d) all manual controls used to physically enter control signals, such as switches or buttons, including their physical location within the cryptographic module, and a listing and description of the control signals that can be entered manually; e) all physical status indicators, including their physical location within the module and a listing and description of the status indication signals that are output physically; f) a mapping of the logical input and output interfaces to the physical input and output ports, manual controls, and physical status indicators of the cryptographic module; g) physical, logical, and electrical characteristics, as applicable, of the above physical ports and interfaces, including summaries of pin designations, logical signals carried on each port, voltage levels and their logical significance (e.g. what a low or high voltage signifies in terms of a logic "0", "1", or other meaning) and the timing of signals.
TE03.01.02	The tester shall verify that the vendor-provided documentation specifies all information flows and physical access points of the cryptographic module, by examining the block diagrams, design specifications, and source code and schematics, as appropriate, provided in 6.2 and 6.11, and any other documentation provided by the vendor. The documentation shall specify the relationship of the information flows and physical access points to the physical ports and logical interfaces of the cryptographic module. The tester shall compare the above information with the information provided under assertions AS02.05 and AS02.12 to AS02.16 and verify that there are no inconsistencies in the description of components and physical layout for the input/output ports.
TE03.01.03	The tester shall verify that for each physical or logical input to the cryptographic module, or physical and logical output from the module, the vendor-provided documentation specifies the logical interface to which the physical input or output belongs, and the physical entry/exit port. The specifications provided shall be consistent with the specifications of the cryptographic module components provided under 6.2 and 6.11, and the specifications of the logical interfaces provided in assertions AS03.04 to AS03.12 of 6.3.2.
TE03.01.04	The tester shall inspect the cryptographic module, to verify that all of the specifications for this assertion given by the vendor-provided documentation are consistent with the design and implementation of the cryptographic module.

Table 39 — VE and TE of AS03.02

Cryptographic module interfaces general requirements — levels 1, 2, 3 and 4	
AS03.02 ISO/IEC 19790:2025, 7.3.1	The cryptographic module logical interfaces shall be distinct from each other although they may share one physical port (e.g. input data may enter and output data may exit via the same port) or may be distributed over one or more physical ports (e.g. input data may enter via both a serial and a parallel port).
Required vendor information	
VE03.02.01	The vendor's design shall separate the cryptographic module interfaces into logically distinct and isolated categories, using the categories listed in assertion AS03.04, and, if applicable, AS03.12 and AS03.13 in 6.3.2. This information shall be consistent with the specification of the logical interfaces and physical ports provided in AS03.01 in 6.3.1.
VE03.02.02	The vendor-provided documentation shall provide a mapping of each category of logical interface to a physical port of the cryptographic module. A logical interface may be physically distributed across more than one physical port, or two or more logical interfaces may share one physical port as long as the information flows are kept logically separate. If two or more logical interfaces share the same physical port, the vendor-provided documentation shall specify how the information from the different interface categories is kept logically separate.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 39 *(continued)*

TE03.02.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the module interfaces are logically distinct and isolated for the categories of interfaces specified in assertions AS03.04 and, if applicable, AS03.12 and AS03.13 of 6.3.2. This information shall be consistent with the specification and design of the logical interfaces and physical ports provided in AS03.01 in 6.3.2.
TE03.02.02	The tester shall verify that the vendor documentation provides a mapping of each category of logical interface to a physical port of the cryptographic module. A logical interface may be physically distributed across more than one physical port, or two or more logical interfaces may share one physical port. If two or more interfaces share the same physical port, the tester shall verify that the vendor documentation specifies how the information flows for the input, output, control, and status interfaces are kept logically separate.
NOTE An API of a software component of a cryptographic module can be defined as one or more logical interface(s).	

Table 40 — VE and TE of AS03.03

Cryptographic module interfaces general requirements — levels 1, 2, 3 and 4	
AS03.03 ISO/IEC 19790:2025, 7.3.1	The documentation for cryptographic module interfaces specified in ISO/IEC 19790:2025, A.2.2 shall be provided.
Required vendor information	
VE03.03.01	The vendor shall provide documentation for cryptographic module interfaces as specified in ISO/IEC 19790:2025, A.2.2.
Required test procedures	
TE03.03.01	The tester shall verify the completeness of the documentation specified in ISO/IEC 19790:2025, A.2.2

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.3.2 Categories of interfaces

Table 41 — VE and TE of AS03.04

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.04 ISO/IEC 19790:2025, 7.3.3	A cryptographic module's interfaces shall be categorized into one or more of the following seven interface categories ("input" and "output" are indicated from the perspective of the module):
Required vendor information	
VE03.04.01	The vendor documentation shall separate the cryptographic module interfaces into logically distinct and isolated categories by the following seven distinctly defined interfaces within the cryptographic module ("input" and "output" are indicated from the perspective of the module): a) data input interface (for the input of data as specified in AS03.05); b) data output interface (for the output of data as specified in AS03.06 and AS03.07); c) control input interface (for the input of commands as specified in AS03.08); d) control output interface (for the output of commands as specified in AS03.09, and AS03.10); e) status output interface (for the output of status information as specified in AS03.11); f) maintenance interface (as specified in AS03.12); g) power interface (as specified in AS03.13).
Required test procedures	
TE03.04.01	The tester shall verify that the vendor-provided documentation specifies that the seven interfaces as listed in VE03.04.01 have been designed within the cryptographic module. If so, verification that the interfaces within the cryptographic module function as specified shall be performed under assertions AS03.05 to AS03.13 in 6.3.2.

Table 42 — VE and TE of AS03.05

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.05 ISO/IEC 19790:2025, 7.3.3	All input data shall enter via the data input interface.
Required vendor information	
VE03.05.01	The cryptographic module shall have a data input interface. All data (except control data entered via the control input interface) that shall be input to and processed by the cryptographic module shall enter via the data input interface, including: a) plaintext data; b) ciphertext or signed data; c) cryptographic keys and other key management data (plaintext or encrypted); d) authentication and verification data (plaintext or encrypted); e) status information from external sources; f) any other input data.
VE03.05.02	If applicable, the vendor documentation shall specify any external input devices to be used with the cryptographic module for the entry of data into the data input interface, such as smart cards, tokens, keypads, key loaders, and biometric devices.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 42 *(continued)*

TE03.05.01	The tester shall inspect the module to verify that the cryptographic module includes a data input interface, and that the data input interface functions as specified. The tester shall verify that all data (except control data entered via the control input interface) that shall be input to and processed by the cryptographic module enters via the data input interface, including: a) plaintext data that shall be encrypted or signed by the cryptographic module; b) ciphertext or signed data that shall be decrypted or verified by the module; c) plaintext or encrypted cryptographic keys and other key management data that are input into and used by the cryptographic module, including initialization data and vectors, split key information, and key accounting information. NOTE Other key management requirements are covered in ISO/IEC 19790:2025, 7.9.7. d) plaintext or encrypted authentication and verification data that is input into the cryptographic module, including passwords, PINs, and biometric information; e) status information from external sources (e.g. another cryptographic module or device); f) any other information that is input into the cryptographic module for processing or storage, except for control information that is covered separately in AS03.08.
TE03.05.02	The tester shall verify if the vendor-provided documentation specifies any external input devices to be used with the cryptographic module for the entry of data into the data input interface, such as smart cards, tokens, keypads, key loaders, and biometric devices. The tester shall enter data into the data input interface using the identified external input device(s), and verify that entry of data using the external input device functions as specified.

Table 43 — VE and TE of AS03.06

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.06 ISO/IEC 19790:2025, 7.3.1	All output data shall exit via the data output interface.
Required vendor information	
VE03.06.01	The cryptographic module shall have a data output interface. All data (except status data output via the status output interface and control data output via the control output interface) that has been processed and is output by the cryptographic module shall exit via the data output interface, including: a) plaintext data; b) ciphertext data and digital signatures; c) cryptographic keys and other key management data (plaintext or encrypted); d) any other information that is output from the cryptographic module after processing or storage except for status information that is covered separately in AS03.11 in 6.3.2 and control information that is covered separately in AS03.09 and AS03.10 in 6.3.2.
VE03.06.02	If applicable, the vendor-provided documentation shall specify any external output devices to be used with the cryptographic module for the output of data from the data output interface, such as smart cards, tokens, displays and other storage devices.
VE03.06.03	If the physical and logical paths followed by the output data and SSP information are physically shared, the vendor-provided documentation shall specify how the cryptographic module enforces logical separation of the output data and SSP information.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 43 *(continued)*

TE03.06.01	The tester shall inspect the module to verify that the cryptographic module includes a data output interface, and that the data output interface functions as specified. The tester shall verify that all data that has been processed and is output by the cryptographic module exits via the data output interface. This excludes status data which is output via the status output interface and control data which is output via the control output interface. These data include: a) plaintext data that has been decrypted by the cryptographic module; b) ciphertext data that has been encrypted, and digital signatures that have been generated by the cryptographic module; c) plaintext or encrypted cryptographic keys and other key management data that have been internally generated and output from the module, including initialization data and vectors, split key information, and key accounting information (other key management requirements are covered in ISO/IEC 19790:2025, 7.9.7); d) any other information that is output from the cryptographic module after processing or storage except for status information that is covered separately in AS03.11 in 6.3.2 and control information that is covered separately in AS03.09 and AS03.10 in 6.3.2.
TE03.06.02	The tester shall verify if vendor-provided documentation specifies any external output devices to be used with the cryptographic module for the output of data from the data output interface, such as smart cards, tokens, displays, and other storage devices. The tester shall output data from the data output interface using the identified external output device(s), and verify that output of data using the external output device functions as specified.
TE03.06.03	If the physical and logical paths followed by the output data and SSP information are physically shared, the tester shall verify that the vendor-provided documentation specifies how the cryptographic module enforces logical separation of the output data and SSP information.

Table 44 — VE and TE of AS03.07

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.07 ISO/IEC 19790:2025, 7.3.3	All output data shall be inhibited while the cryptographic module is in an error state, and also inhibited while performing pre-operational self-tests as specified in ISO/IEC 19790:2025, 7.10.3, and zeroization as specified in ISO/IEC 19790:2025, 7.9.7.
Required vendor information	
VE03.07.01	The vendor-provided documentation shall specify how the cryptographic module inhibits data output while the cryptographic module is in an error state, and also how it inhibits data output while performing pre-operational self-tests and zeroization.
VE03.07.02	The vendor-provided documentation shall specify how the design of the cryptographic module ensures that all output data is inhibited while the cryptographic module is in an error state, and also inhibited while performing pre-operational self-tests and zeroization.
Required test procedures	
TE03.07.01	The tester shall verify that the vendor documentation specifies that all data output via the data output interface is inhibited while: a) the cryptographic module is in an error state, and also b) performing: 1) pre-operational self-tests; 2) zeroization. This test procedure can be restated as follows.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 44 *(continued)*

	c) The tester shall verify from vendor-provided documentation that once an error condition is detected and the error state is entered, all data output via the data output interface is inhibited, until error recovery occurs. d) The tester shall verify from the vendor-provided documentation that once each of the following services is started, all data output via the data output interface is inhibited, until the service is completed successfully:
TE03.07.02	The tester shall cause the cryptographic module to enter each of following states: a) each self-test state performing pre-operational self-tests; b) each state performing zeroization; c) each error state and verify that all data output via the data output interface is inhibited. If it is not possible for the tester to cause an error then the vendor shall provide a rationale to the tester as to why this test cannot be performed. In such case, the tester shall follow alternative procedures allowed by the certification body to ensure that all data output via the data output interface is inhibited. EXAMPLE Examining the applicable source code. If status information is output from the status output interface to indicate the results of the self-tests, the tester shall verify that no CSPs, plaintext data, or other information are output that, if misused, can lead to a compromise.
TE03.07.03	The tester shall verify that the vendor-provided documentation specifies how the cryptographic module ensures that all data output via the data output interface is inhibited during the three states listed in TE03.07.02, i.e. a) to c). The tester shall also verify, by inspection of the design of the cryptographic module, that the data output interface is, in fact, logically or physically inhibited under these conditions.

Table 45 — VE and TE of AS03.08

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.08 ISO/IEC 19790:2025, 7.3.3	All control input shall enter via the control input interface.
Required vendor information	
VE03.08.01	The cryptographic module shall have a control input interface. All commands, signals, and control data (except data entered via the data input interface) used to control the operation of the cryptographic module shall enter via the control input interface, including: a) commands input logically via an API (e.g. for the software and firmware components of the cryptographic module); b) signals input logically or physically via one or more physical ports (e.g. for the hardware components of the cryptographic module); c) manual control inputs (e.g. using switches, buttons, or a keyboard); d) any other input control data.
VE03.08.02	If applicable, the vendor-provided documentation shall specify any external input devices to be used with the cryptographic module for the entry of commands, signals, and control data into the control input interface, such as smart cards, tokens, or keypads.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 45 *(continued)*

TE03.08.01	The tester shall inspect the module to verify that the cryptographic module includes a control input interface, and that the control input interface functions as specified. The tester shall verify that all commands, signals, and control data (except data entered via the data input interface) used to control the operation of the cryptographic module shall enter via the control input interface, including: a) commands input logically via an API, such as function calls to a software library or to a smart card; b) signals input logically or physically via one or more physical ports, such as commands and signals sent through a serial port or a PC Card; c) manual control inputs (e.g. using switches, buttons, or a keyboard); d) any other input control data.
TE03.08.02	The tester shall verify if the vendor-provided documentation specifies any external input devices to be used with the cryptographic module for the entry of commands, signals, and control data into the control input interface, such as smart cards, tokens, or keypads. The tester shall enter commands via the control input interface using the identified external input device(s), and verify that the input of commands using the external input device functions as specified.

Table 46 — VE and TE of AS03.09

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.09 ISO/IEC 19790:2025, 7.3.3	All control output shall exit via the control output interface.
Required vendor information	
VE03.09.01	The vendor-provided documentation shall specify that all output commands, signals, and control data (e.g. control commands to another module) used to control or indicate the state of operation of a cryptographic module exit via the control output interface.
Required test procedures	
TE03.09.01	The tester shall verify that the vendor-provided documentation specifies that all output commands, signals, and control data (e.g. control commands to another module) used to control or indicate the state of operation of a cryptographic module exit via the control output interface.
TE03.09.02	If the control output interface is specified, the tester shall inspect the module to verify that the control output interface functions as specified.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 47 — VE and TE of AS03.10

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.10 ISO/IEC 19790:2025, 7.3.3	All control output shall be inhibited when the cryptographic module is in an error state unless exceptions are specified and documented in the security policy.
Required vendor information	
VE03.10.01	The vendor-provided documentation shall specify how the cryptographic module ensures that all control output via the control output interface is inhibited whenever the module is in an error state. Status information may the type of error from the status output interface. NOTE Error states are covered in ISO/IEC 19790:2025, 7.11.
Required test procedures	
TE03.10.01	The tester shall verify that the vendor-provided documentation specifies that all control output via the control output interface is inhibited whenever the cryptographic module is in an error state. The tester shall verify from the vendor-provided documentation that once an error condition is detected and the error state is entered, all control output via the control output interface is inhibited, until error recovery occurs. The tester shall also verify that the error states specified in response to this assertion are identical to the error states specified under AS11.11.
TE03.10.02	The tester shall cause the cryptographic module to enter each specified error state and verify that all control output via the control output interface is inhibited. If status information is output from the status output interface to identify the type of error, the tester shall verify that the information output is not sensitive. The following actions may be used to cause the cryptographic module to enter an error state: opening a tamper-detecting cover or door; entering incorrectly-formatted commands, keys, or parameters; reducing input voltage, and any other error-causing actions. If it is not possible for the tester to cause an error, then the vendor shall provide a rationale to the tester as to why this test cannot be performed.

Table 48 — VE and TE of AS03.11

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.11 ISO/IEC 19790:2025, 7.3.3	All status output shall exit via the status output interface.
Required vendor information	
VE03.11.01	The cryptographic module shall have a status output interface. All status information, signals, logical indicators, and physical indicators used to indicate or display the status of the module shall exit via the status output interface, including: a) status information output logically via an API; b) signal outputs logically or physically via one or more physical ports; c) physical status indicator (e.g. using displays, lamps, buzzer, tone, or ring); d) any other output status information.
VE03.11.02	If applicable, the vendor-provided documentation shall specify any external output devices to be used with the cryptographic module for the output of status information, signals, logical indicators, and physical indicators via the status output interface, such as smart cards, tokens, displays, and other storage devices.
Required test procedures	
TE03.11.01	The tester shall inspect the module to verify that the cryptographic module includes a status output interface, and that the status output interface functions as specified. The tester shall verify that all status information, signals, logical indicators, and physical indicators used to indicate or display the status of the module shall exit via the status output interface, including:

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 48 *(continued)*

	a) status information output logically via an API, such as return codes from a software library or a smart card; b) signal outputs logically or physically via one or more physical ports, such as status information sent through a serial port or a PC Card connector; c) physical status indicator; d) any other output status information.
TE03.11.02	The tester shall verify that the vendor documentation specifies any external output devices (if applicable) to be used with the cryptographic module for the output of status information, signals, logical indicators, and physical indicators via the status output interface.
TE03.11.03	The tester shall verify that the status information output from the status output interface shall not output any information that can result in a compromise of CSPs.
NOTE The status output can be either implicit or explicit.	

Table 49 — VE and TE of AS03.12

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.12 ISO/IEC 19790:2025, 7.3.3	All physical and logical interfaces to the cryptographic module which are utilized when in the maintenance role shall be defined.
Required vendor information	
VE03.12.01	The vendor-provided documentation shall describe the physical and logical maintenance interfaces employed by the module when in the maintenance role.
Required test procedures	
TE03.12.01	The tester shall verify that the vendor-provided documentation describes all the physical and logical maintenance interfaces employed by the module when in the maintenance role.
TE03.12.02	The tester shall verify that the vendor-provided documentation and implementation are consistent.

Table 50 — VE and TE of AS03.13

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.13 ISO/IEC 19790:2025, 7.3.3	All external power shall enter or exit via a power interface.
Required vendor information	
VE03.13.01	If the cryptographic module requires or provides power to or from other devices external to the cryptographic boundary (e.g. a power supply, power cord, power inlet/outlet, wireless charging or an external battery), the vendor-provided documentation shall specify a power interface and a corresponding physical port.
VE03.13.02	All power entering or exiting the cryptographic module to or from other devices external to the cryptographic boundary shall pass through the specified power interface.
Required test procedures	
TE03.13.01	The tester shall verify if the vendor-provided documentation specifies whether the cryptographic module requires or provides power to or from other devices external to the cryptographic boundary. The tester shall also verify that the vendor-provided documentation specifies a power interface and a corresponding physical port.
TE03.13.02	The tester shall verify, by inspection of the cryptographic module, that all power entering or exiting the module to or from other devices external to the cryptographic boundary passes through the specified power interface.
NOTE This interface does not apply to software cryptographic modules or when all power is provided or maintained internally within the cryptographic boundary of the cryptographic module (e.g. an internal battery).	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 51 — VE and TE of AS03.14

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.14 ISO/IEC 19790:2025, 7.3.3	The cryptographic module shall distinguish between data, control information, and power for input to the module, and between data, control information, status information, and power for output from the module.
Required vendor information	
VE03.14.02	The vendor-provided documentation shall specify how the physical and logical paths used by the input data and control information are logically or physically disconnected from the physical and logical paths used by the output data, control and status information. If the physical and logical paths used by the input data and control information, as well as the output data, control and status information are physically shared, the vendor-provided documentation shall specify how logical separation is enforced by the cryptographic module.
VE03.14.03	The vendor-provided documentation shall show be consistent and shall show that the cryptographic module distinguishes data and control for input from data, control and status for output. The vendor documentation shall also show that the physical and logical paths followed by the input data and control information entering the module via the applicable input interfaces are logically or physically disconnected from the physical and logical paths followed by the output data, control and status information exiting the module via the applicable output interfaces.
Required test procedures	
TE03.14.01	The tester shall verify that the vendor-provided documentation specifies how the cryptographic module distinguishes between data and control for input and data, control and status for output. Input data entered from the data input interface, and control information entered from the control input interface shall be logically or physically distinguished from output data exiting to the output data interface, output control exiting to the output control interface, and status information exiting to the status output interface.
TE03.14.02	The tester shall verify that the vendor-provided documentation specifies how the physical and logical paths used by the input data and control information are logically or physically disconnected from the physical and logical paths used by the output data, control and status information. If the physical and logical paths used by the input data and control information, and the paths used by output data, control and status information are physically shared, the tester shall verify that the vendor-provided documentation specifies how logical separation is enforced by the cryptographic module.
TE03.14.03	The tester shall verify, by inspection of the module, the consistency of the vendor-provided documentation. The tester shall also verify that the cryptographic module distinguishes between data and control for input and data, control and status for output. The tester shall verify that path A is logically or physically disconnected from path B. Path A consists of the physical and logical paths followed by the input data and control information entering the module via the applicable input interfaces and path B consists of the physical and logical paths followed by the output data, control and status information exiting the module via the applicable output interfaces.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 52 — VE and TE of AS03.15

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.15 ISO/IEC 19790:2025, 7.3.3	The cryptographic module specification shall, unambiguously, specify format of input data and control information, including length restrictions for all variable length inputs.
Required vendor information	
VE03.15.01	The vendor-provided documentation shall specify the physical and logical paths used by all major categories of input data entering the cryptographic module via the data input interface and the applicable physical ports. The documentation shall include a specification of the applicable paths (e.g. by highlighted or annotated copies of the schematics, block diagrams, or other information provided under AS02.05 and AS02.13 to AS02.16). All input data entering the cryptographic module via the data input interface shall only use the specified paths while being processed or stored by each physical or logical sub-section of the module. The input data paths shall be specified in sufficient detail to ensure that the type of data pass through each applicable physical port can be verified. NOTE 1 The term “all major categories of input data” refer to items addressed in AS03.05 for data input and to items addressed in AS03.08 for control input.
VE03.15.02	The vendor-provided documentation shall specify that all input data entering the cryptographic module via the data input interface and applicable physical ports only use the specified paths. The documentation shall show that all logical and physical information flows used by the input data are consistent with the design and operation of the cryptographic module. The vendor documentation shall establish that there are no conflicts between the applicable paths that can lead to the compromise of CSPs, plaintext data, or other information of the cryptographic module.
VE03.15.03	The vendor-provided documentation shall unambiguously specify format of input data and control information including length restrictions for all variable length inputs.
VE03.15.04	The vendor-provided documentation shall identify which component within the cryptographic boundary is validating the format.
Required test procedures	
TE03.15.01	The tester shall verify that the vendor-provided documentation specifies the physical and logical paths used by all major categories of input data entering the cryptographic module via the data input interface. The tester shall also verify that the paths shall be documented in the specification (e.g. by highlighted or annotated copies of the schematics, block diagrams, or other information provided under AS02.05 and AS02.13 to AS02.16). The tester shall verify that the documentation specifies the type of data pass through each applicable physical port.
TE03.15.02	The tester shall review the documentation provided by the vendor and inspect the cryptographic module, to verify that all input data entering the module via the data input interface and applicable physical ports only use the specified paths. The tester shall examine all logical and physical information flows and shall verify that the specification of the paths used by the input data is consistent with the design and operation of the cryptographic module. The tester shall verify that there are no conflicts between the applicable paths that can lead to the compromise of CSPs, plaintext data, or other information.
TE03.15.03	The tester shall review the vendor-provided documentation and inspect the module to verify that the unambiguous specification is provided about the format of input data and control information, including length restrictions for all variable length inputs.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 52 *(continued)*

TE03.15.04	The tester shall verify that the identified component within the cryptographic boundary is located on the specified path under VE03.15.02.
TE03.15.05	The tester shall examine the applicable source code(s) to ensure that the identified component is actually validating the documented format.
TE03.15.06	The tester shall attempt to input data and control information which is not compliant with the format, and verify that such service inputs are rejected by the cryptographic module. NOTE 2 The test platform or configuration can impose a part of format/restrictions. EXAMPLE 1 A device driver to use the cryptographic module is enforcing a part of the format. EXAMPLE 2 A layer in a protocol stack supports fixed length packet only. If it is not possible for the tester to input certain data or control information which is not compliant with the format, then the tester shall ask the vendor to provide a rationale as to why this test cannot be performed. In such case, the tester shall follow alternative procedures allowed by the certification body to ensure that the cryptographic module is validating the format.

Table 53 — VE and TE of AS03.16

Categories of interfaces — levels 1, 2, 3 and 4	
AS03.16 ISO/IEC 19790:2025, 7.3.3	The cryptographic module shall confirm that all inputs conform to the specifications in AS03.15.
Required vendor information	
VE03.16.01	The vendor shall provide documentation that identifies the techniques used to confirm all inputs received on module interfaces.
Required test procedures	
TE03.16.01	The tester shall verify that provided documentation identifies the technique used to confirm all inputs received on module interfaces. NOTE 1 Additionally, this assertion is tested as part of AS03.15. NOTE 2 The tester can use the vendor-provided automated security diagnostic tools in AS11.30 in order to validate inputs.

6.3.3 Plaintext trusted path

6.3.3.1 Security level 3

Table 54 — VE and TE of AS03.17

Plaintext trusted path — levels 3 and 4	
AS03.17 ISO/IEC 19790:2025, 7.3.4.3	for the transmission of plaintext CSPs and key components between the cryptographic module and the sender or receiver's endpoint, the cryptographic module shall implement a plaintext trusted path;
Required vendor information	
VE03.17.01	The vendor shall describe the method of transmission of plaintext CSPs and the way they are protected via a plaintext trusted path.
Required test procedures	
TE03.17.01	The tester shall verify that the plaintext trusted path is able to protect plaintext CSPs between the cryptographic module's cryptographic boundary and the sender or receiver endpoint.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 55 — VE and TE of AS03.18

Plaintext trusted path — levels 3 and 4	
AS03.18 ISO/IEC 19790:2025, 7.3.4.3	the plaintext trusted path shall prevent unauthorized modification, substitution, and disclosure along the communication link;
Required test procedures	
This assertion is tested as part of AS03.19 and AS03.20.	

Table 56 — VE and TE of AS03.19

Plaintext trusted path — levels 3 and 4	
AS03.19 ISO/IEC 19790:2025, 7.3.4.3	the physical ports used for the plaintext trusted path shall be used only for the plaintext trusted path and be physically separated from all other ports, or {AS03.20 shall be satisfied}
Required vendor information	
VE03.19.01	The vendor-provided documentation shall specify if the cryptographic module inputs or outputs plaintext CSPs. The physical port(s) used for the input and output of plaintext CSPs shall be used only for the plaintext trusted path and shall be physically separated from all other physical ports of the cryptographic module.
VE03.19.02	If the cryptographic module inputs or outputs plaintext CSPs, the module shall ensure that only plaintext CSPs enter or exit the module through the applicable physical ports, and that no other data, unprotected or encrypted, enters or exits the module via the applicable physical ports.
VE03.19.03	The vendor-provided documentation shall provide rationale as to how the plaintext trusted path prevents unauthorized modification, substitution, and disclosure along the communication link.
Required test procedures	
TE03.19.01	The tester shall verify if the vendor-provided documentation specifies whether the cryptographic module inputs or outputs plaintext CSPs. The tester shall review the vendor-provided documentation and also inspect the physical ports on the cryptographic module that the applicable physical ports used for the input and output of plaintext CSPs are used only for the plaintext trusted path and they are physically separated from all other physical ports of the module.
TE03.19.02	If the cryptographic module inputs or outputs plaintext CSPs, the tester shall verify that only plaintext CSPs enter or exit the module through the applicable physical ports, and that no other data, unprotected or encrypted, enters or exits the module via the applicable physical ports.
TE03.19.03	The tester shall verify the correctness 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 ask the vendor to produce additional information as needed.
TE03.19.04	The tester shall, by attempting to access the communication link, verify that the plaintext trusted path prevents unauthorized modification, substitution, and disclosure along the communication link.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 57 — VE and TE of AS03.20

Plaintext trusted path — levels 3 and 4	
AS03.20 ISO/IEC 19790:2025, 7.3.4.3	the logical interfaces used for the plaintext trusted path shall be logically separated from all other interfaces; or {AS03.19 shall be satisfied}
Required vendor information	
VE03.20.01	The vendor-provided documentation shall describe how the logical interfaces used in the plaintext trusted path to input and output plaintext CSPs are logically separated from all other interfaces.
VE03.20.02	If the cryptographic module inputs or outputs plaintext CSPs, the module shall ensure that plaintext CSPs enter or exit the module through the applicable logical interface using the plaintext trusted path, and that no other data, unprotected or encrypted, enters or exits the module via the applicable logical interface using the plaintext trusted path.
VE03.20.03	The vendor-provided documentation shall provide rationale on how the plaintext trusted path prevents unauthorized modification, substitution, and disclosure along the communication link.
Required test procedures	
TE03.20.01	The tester shall review the vendor-provided documentation and inspect the cryptographic module to verify that the applicable logical interfaces used in the plaintext trusted path to input and output of plaintext CSPs are logically separated from all other logical interfaces of the module.
TE03.20.02	If the cryptographic module inputs or outputs plaintext CSPs, the tester shall verify that plaintext CSPs enter or exit the module through the applicable logical interface using the plaintext trusted path, and that no other data, unprotected or encrypted, enters or exits the module via the applicable logical interface using the plaintext trusted path.
TE03.20.03	The tester shall verify the correctness 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 ask the vendor to produce additional information as needed.
TE03.20.04	The tester shall, by attempting to access the communication link, verify that the plaintext trusted path prevents unauthorized modification, substitution, and disclosure along the communication link.

Table 58 — VE and TE of AS03.21

Plaintext trusted path — levels 3 and 4	
AS03.21 ISO/IEC 19790:2025, 7.3.4.3	identity-based authentication shall be employed for all services utilising the plaintext trusted path; and
Required vendor information	
VE03.21.01	The vendor shall provide a description of the authentication mechanism used by the plaintext trusted path.
Required test procedures	
TE03.21.01	The tester shall verify that an identity-based authentication mechanism is employed for all services utilizing the plaintext trusted path. The tester shall verify that services utilising the plaintext trusted path are not provided without successfully passing the operator authentication.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 59 — VE and TE of AS03.22

Plaintext trusted path — levels 3 and 4	
AS03.22 ISO/IEC 19790:2025, 7.3.4.3	a status indicator shall be provided when the plaintext trusted path is in use.
Required vendor information	
VE03.22.01	The vendor shall provide description of the indicator provided when plaintext trusted path is in use.
Required test procedures	
TE03.22.01	The tester shall verify, by exercising the module, that the status indicator is provided when the plaintext trusted path is in use.

6.3.3.2 Security level 4

Table 60 — VE and TE of AS03.23

Plaintext trusted path — level 4	
AS03.23 ISO/IEC 19790:2025, 7.3.4.4	In addition to the requirements of security level 3, multi-factor identity-based authentication or other authentication methods, as specified for security level 4 in ISO/IEC 19790:2025, Annex E, shall be employed for all services utilising the plaintext trusted path.
Required vendor information	
VE03.23.01	The vendor shall provide a description of the multi-factor identity-based authentication mechanism used by the plaintext trusted path.
Required test procedures	
TE03.23.01	The tester shall verify that a multi-factor identity-based authentication mechanism is employed for all services utilising the plaintext trusted path. The tester shall verify that services utilising the plaintext trusted path are not provided without successfully passing the operator authentication.

6.3.4 Protected internal paths

Table 61 — VE and TE of AS03.24

Protected internal paths — levels 2, 3 and 4	
AS03.24 ISO/IEC 19790:2025, 7.3.4.4	At security levels 2, 3, and 4, protected internal paths shall employ approved cryptographic algorithms to provide confidentiality and integrity of security relevant data and controls.
Required vendor information	
VE03.24.01	The vendor shall provide documentation that specifies protected internal paths for confidentiality and integrity of security relevant data and controls.
VE03.24.02	The vendor-provided documentation shall describe the cryptographic algorithms, the integrity mechanism and the key establishment methods used for all the internal protected paths for data and controls and provide a validation certificate if available or vendor affirmation as specified in VE02.18.01 and VE02.18.03.
Required test procedures	
TE03.24.01	The tester shall verify that the vendor-provided documentation specifies protected internal paths for confidentiality and integrity of security relevant data and controls.
TE03.24.02	The tester shall verify that the vendor-provided documentation describes the cryptographic algorithms, the integrity mechanism and the key establishment methods and provides a validation certificate if available or vendor affirmation as specified in TE02.18.01 and TE02.18.03.
TE03.24.03	For documented methods in VE03.24.01 and VE03.24.02, the tester shall verify by test and inspection of the module that the internal path of the module is using the methods described.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.4 Roles, services, and authentication

6.4.1 Roles, services, and authentication general requirements

Table 62 — VE and TE of AS04.01

Roles, services, and authentication general requirements — levels 1, 2, 3 and 4	
AS04.01 ISO/IEC 19790:2025, 7.4.1	A cryptographic module shall support authorized roles for operators and corresponding services within each role. A single operator may assume multiple roles.
Required test procedures	
This assertion is tested as part of AS04.11.	

Table 63 — VE and TE of AS04.02

Roles, services, and authentication general requirements — levels 1, 2, 3 and 4	
AS04.02 ISO/IEC 19790:2025, 7.4.1	If a cryptographic module supports concurrent operators, then the module shall internally maintain the separation of the roles assumed by each operator and the corresponding services.
Required vendor information	
VE04.02.01	The vendor-provided documentation shall specify whether multiple concurrent operators are allowed. The vendor-provided documentation shall specify the method by which separation of the authorized roles and services performed by each operator is achieved. The vendor-provided documentation shall also describe any restrictions on concurrent operators. EXAMPLE 1 One operator in a maintenance role and another in a user role simultaneously is not accepted. EXAMPLE 2 Multiple concurrent operators up to 16 operators in a user role are supported, but only one RSA key generation service can be run at a time in the cryptographic module. EXAMPLE 3 When multiple concurrent operators in a crypto officer role are logged in, but each crypto officer cannot change the authentication data of the other operators in a crypto officer role.
Required test procedures	
TE04.02.01	The tester shall verify that the vendor-provided documentation describes the method implemented by the module to enforce separation between the roles and services performed by concurrent operators.
TE04.02.02	If the module supports more than one role then the tester shall assume the identity of two independent operators: operator 1 and operator 2. The operators shall assume different roles. The tester shall verify that only the services allocated to each role can be performed in that role. The tester shall also attempt, for each operator, to access services that are unique to the role assumed by the other operator in order to verify that separation is maintained between the roles and services allowed in concurrent operators.
TE04.02.03	If the vendor-provided documentation specifies any restrictions on concurrent operators, the tester shall attempt to violate the restrictions by attempting to concurrently assume restricted roles as independent operators and verify that the module enforces the restrictions.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 64 — VE and TE of AS04.03

Roles, services, and authentication general requirements — levels 1, 2, 3 and 4	
AS04.03 ISO/IEC 19790:2025, 7.4.1	The documentation for roles, services, and authentication specified in ISO/IEC 19790:2025, A.2.3 shall be provided.
Required vendor information	
VE04.03.01	The vendor shall provide documentation for roles, services, and authentication as described ISO/IEC 19790:2025, A.2.3.
Required test procedures	
TE04.03.01	The tester shall check that vendor-provided documentation defines roles, services, and authentication in accordance with the specification in ISO/IEC 19790:2025, A.2.3.

6.4.2 Roles

Table 65 — VE and TE of AS04.04

Roles — levels 1, 2, 3 and 4	
AS04.04 ISO/IEC 19790:2025, 7.4.2	A cryptographic module shall, at a minimum, support a crypto officer role.
Required test procedures	
This assertion is tested as part of AS04.05.	

Table 66 — VE and TE of AS04.05

Roles — levels 1, 2, 3 and 4	
AS04.05 ISO/IEC 19790:2025, 7.4.2	The crypto officer role shall be assumed to perform cryptographic initialization or management functions, and general security services (e.g. module initialization, management of CSPs, PSPs, and auditing).
Required vendor information	
VE04.05.01	In the documentation required, the vendor shall include at least one crypto-officer role. These roles shall be specified by name and allowed services.
Required test procedures	
TE04.05.01	The tester shall verify that the vendor-provided documentation defines at least one crypto-officer role. The tester shall verify that roles are specified by name and allowed services as specified in AS04.05.

Table 67 — VE and TE of AS04.06

Roles — levels 1, 2, 3 and 4	
AS04.06 ISO/IEC 19790:2025, 7.4.2	If the cryptographic module supports a user role, then the user role shall be assumed to perform general security services, including cryptographic operations and other approved security functions.
Required vendor information	
VE04.06.01	If the cryptographic module supports a user role, the vendor-provided documentation shall (1) explicitly state that a user role is supported, and (2) completely specify the role by name and allowed services.
Required test procedures	
TE04.06.01	If the cryptographic module supports a user role, the tester shall verify that the vendor-provided documentation defines at least one user role. The tester shall verify that user role is specified by name and allowed services as specified in AS04.06.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 68 — VE and TE of AS04.07

Roles — levels 1, 2, 3 and 4	
AS04.07 ISO/IEC 19790:2025, 7.4.2	All plaintext CSPs, plaintext PSPs, and plaintext key components shall be zeroized when entering and when exiting the maintenance role.
Required vendor information	
VE04.07.01	If the cryptographic module has a maintenance interface, the vendor-provided documentation shall 1) explicitly state a maintenance role is supported, 2) completely specify the role by name, purpose, and allowed services, and 3) specify the maintenance access interface under VE03.12.01.
VE04.07.02	The vendor-provided documentation shall specify how the module's plaintext CSPs, plaintext PSPs, and plaintext key components are actively zeroized when the maintenance role is entered and exited.
Required test procedures	
TE04.07.01	The tester shall verify if the specifications of the module interfaces indicate a maintenance access interface (see AS03.12). If so, the tester shall verify the vendor-provided documentation pertaining to the authorized roles and verify that it specifies the maintenance role by name, purpose, and allowed services.
TE04.07.02	The tester shall verify if the specifications of the module interfaces define a maintenance role and check the zeroization of all plaintext CSPs, plaintext PSPs, and plaintext key components as described in the module specification.
TE04.07.03	While in the maintenance role, the tester shall enter, for all plaintext CSPs, plaintext PSPs, and plaintext key components, known values which are effective in demonstrating the zeroization and, upon exit from the maintenance role, the tester shall verify that zeroization has taken place.

6.4.3 Services

6.4.3.1 Services general requirements

Table 69 — VE and TE of AS04.08

Services — levels 1, 2, 3 and 4	
AS04.08 ISO/IEC 19790:2025, 7.4.3.1	Services shall refer to all operations or functions that can be performed by a module.
Required test procedures	
This assertion is not separately tested.	

Table 70 — VE and TE of AS04.09

Services — levels 1, 2, 3 and 4	
AS04.09 ISO/IEC 19790:2025, 7.4.3.1	Service inputs shall consist of all data or control inputs to the module that initiate or obtain specific services, operations, or functions.
Required test procedures	
This assertion is not separately tested.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 71 — VE and TE of AS04.10

Services — levels 1, 2, 3 and 4	
AS04.10 ISO/IEC 19790:2025, 7.4.3.1	Service outputs shall consist of all data outputs, control outputs, and status outputs that result from services, operations, or functions initiated or obtained by service inputs.
Required test procedures	
This assertion is not separately tested.	

Table 72 — VE and TE of AS04.11

Services — levels 1, 2, 3 and 4	
AS04.11 ISO/IEC 19790: 2025, 7.4.3.1	Each service input shall result in a service output.
Required vendor information	
VE04.11.01	The vendor-provided documentation shall describe the purpose and function of each service. The documentation shall include for each service: service inputs, corresponding service outputs, and the authorized role or roles in which the service can be performed.
Required test procedures	
TE04.11.01	The tester shall check the vendor-provided documentation and verify that the purpose and function of each service is described. The tester shall also check that the following information is specified for each service: service inputs, corresponding service outputs, and the authorized role or roles in which the service can be performed.
TE04.11.02	The tester shall perform the following for each service (i.e. security and non-security services, both approved and non-approved services). a) Enter each of the specified service inputs and observe that they result in the specified service outputs. b) For services that require the operator to assume a role, the role shall be assumed to enter each of the specified service inputs and observe that they result in the specified service outputs. c) For services that require the operator to assume a role, assume the role that is not specified for the service and enter each of the specified service inputs and observe that the service is not provided. d) For services that require the operator to assume an authenticated role, the role shall be assumed and authenticated to enter each of the specified service inputs and observe that they result in the specified service outputs. e) For services that require the operator to assume an authenticated role, the role shall be assumed but the authentication data shall be modified to fail authentication and enter each of the specified service inputs with the modified authenticate data and observe that the service is not provided. f) For services that provide data output over the data output interface, the tester shall verify the result against the expected result. EXAMPLE If the service provides data output which is a function of the services data input, the tester will verify the data output result as a function of the provided input data.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 73 — VE and TE of AS04.12

Services — levels 1, 2, 3 and 4	
AS04.12 ISO/IEC 19790:2025, 7.4.3.1	A cryptographic module shall provide the following services to operators:
Required test procedures	
This assertion is not separately tested.	

Table 74 — VE and TE of AS04.13

Services — levels 1, 2, 3 and 4	
AS04.13 ISO/IEC 19790:2025, 7.4.3.1	The cryptographic module shall output the name or module identifier, and the versioning information that can be correlated with a validation record (e.g. hardware and either software or firmware versioning information).
Required vendor information	
VE04.13.01	The vendor-provided documentation shall describe the output of the current name and versioning information of the cryptographic module.
VE04.13.02	The vendor-provided documentation shall identify the name or module identifier and the versioning information which will be posted as the validation record.
VE04.13.03	The vendor-provided documentation, either non-proprietary security policy or an administrator guidance, shall specify how to correlate the output of the current name and the versioning information with a validation record.
Required test procedures	
TE04.13.01	The tester shall verify that the service outputs (i.e. name or module identifier and versioning information) are consistent with specification and with information provided under assertions AS02.09, AS02.10, and AS11.04.
TE04.13.02	The tester shall verify that the documentation provided by the vendor (i.e. non-proprietary security policy or an Administrator guidance) provides sufficient information to unambiguously identify the module version.
TE04.13.03	The tester shall verify that the output of the current name or module identifier and the versioning information is sufficient for an operator to correlate the module with a validation record, with the help of non-proprietary security policy or an administrator guidance.

Table 75 — VE and TE of AS04.14

Services — levels 1, 2, 3 and 4	
AS04.14 ISO/IEC 19790:2025, 7.4.3.1	The cryptographic module shall output current status. This may include the output of status indicators in response to a service request.
Required vendor information	
VE04.14.01	The vendor-provided documentation shall describe the output of the current status of the module.
Required test procedures	
TE04.14.01	The tester shall verify the vendor-provided documentation to verify that the “show status” service is allocated to at least one authorized role. The tester shall verify that these services are described as specified in AS04.14.
TE04.14.02	The tester shall verify that the “show status” indicator matches the vendor-provided documentation.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 76 — VE and TE of AS04.15

Services — levels 1, 2, 3 and 4	
AS04.15 ISO/IEC 19790:2025, 7.4.3.1	The cryptographic module shall perform the pre-operational self-tests and conditional self-tests as specified in ISO/IEC 19790:2025, 7.10.
Required vendor information	
VE04.15.01	The vendor-provided documentation shall describe the initiation and running of user callable self-tests.
Required test procedures	
TE04.15.01	The tester shall verify that the module provides for the initiation of the running of pre-operational self-tests, as specified in ISO/IEC 19790:2025, 7.10 performed under documentation verification in TEA.01.01.
TE04.15.02	The tester shall initiate the service to perform self-tests. The tester shall verify that the pre-operational self-tests as specified in ISO/IEC 19790:2025, 7.10 have been performed.
TE04.15.03	The tester shall initiate the service to perform self-tests. The tester shall verify that once the module returns to the operational state, that all conditional cryptographic algorithm self-tests as specified in ISO/IEC 19790:2025, 7.10 are performed before the next operational use of the cryptographic algorithm.

Table 77 — VE and TE of AS04.16

Services — levels 1, 2, 3 and 4	
AS04.16 ISO/IEC 19790:2025, 7.4.3.1	The cryptographic module shall perform at least one approved security function as specified in ISO/IEC 19790:2025, 7.2.
Required test procedures	
This assertion is not separately tested.	

Table 78 — VE and TE of AS04.17

Services — levels 1, 2, 3 and 4	
AS04.17 ISO/IEC 19790:2025, 7.4.3.1	The cryptographic module shall perform zeroization of the parameters as specified in ISO/IEC 19790:2025, 7.9.7.
Required test procedures	
This assertion is not separately tested.	

6.4.3.2 Cryptographic bypass

Table 79 — VE and TE of AS04.18

Services — levels 1, 2, 3 and 4	
AS04.18 ISO/IEC 19790:2025, 7.4.3.2	If the module can output a particular data or status item in a cryptographically protected form, and (as a result of module configuration or operator intervention) can also output the item in a non-protected form, then a bypass capability shall be defined.
Required vendor information	
VE04.18.01	If the module implements a bypass capability, the vendor-provided documentation shall describe the bypass service.
Required test procedures	
TE04.18.01	The tester shall verify that the module implements a bypass capability as specified in the vendor-provided documentation.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 80 — VE and TE of AS04.19

Services — levels 1, 2, 3 and 4	
AS04.19 ISO/IEC 19790:2025, 7.4.3.2	the operator shall assume an authorized role before configuring the bypass capability;
Required vendor information	
VE04.19.01	If the module implements a bypass capability, the vendor-provided documentation shall describe how the operator assumes an authorized role before configuring the bypass capability.
Required test procedures	
TE04.19.01	The tester shall verify from the vendor documentation that the module requires an operator to assume an authorized role before configuring the bypass capability.
TE04.19.02	The tester shall assume the defined role that is documented to configure the bypass capability and perform the configuration.
TE04.19.03	The tester shall assume a defined role that is not documented to configure the bypass capability and attempt to perform the bypass configuration. The tester shall verify that the attempt fails.

Table 81 — VE and TE of AS04.20

Services — levels 1, 2, 3 and 4	
AS04.20 ISO/IEC 19790:2025, 7.4.3.2	two independent internal actions shall be required by the module to activate the capability to prevent the inadvertent bypass of plaintext data due to a single error.
Required vendor information	
VE04.20.01	If the module implements a bypass capability, the vendor-provided documentation shall describe the bypass service as specified in AS04.20.
VE04.20.02	The finite state model and other vendor-provided documentation shall indicate, for all transitions into an exclusive or alternating bypass state, two independent internal actions that are required to transition into each bypass state.
Required test procedures	
TE04.20.01	The tester shall verify whether the bypass capability is implemented by the module. The tester shall verify the vendor-provided documentation to verify that the bypass capability is allocated to at least one authorized role.
TE04.20.02	The tester shall verify the finite state model and other vendor-provided documentation to ensure that each transition into an exclusive or alternating bypass state shows two independent internal actions. This shall occur in order for the cryptographic module to transition into either exclusive or alternating bypass state.
TE04.20.03	The tester shall attempt to transition to each bypass state from each state that shows such a transition and verify that it takes two internal actions to accomplish each such transition.

Table 82 — VE and TE of AS04.21

Services — levels 1, 2, 3 and 4	
AS04.21 ISO/IEC 19790:2025, 7.4.3.2	The two independent internal actions shall modify firmware, software, or hardware behaviour (or a combination) that is dedicated to mediating the bypass capability (e.g. two different software or hardware flags are set, one of which may be user-initiated);
Required vendor information	
VE04.21.01	If the module implements a bypass capability, the vendor-provided documentation shall specify how the two independent internal actions modify firmware, software, or hardware behaviour (or a combination) that is dedicated to mediating the bypass capability.
VE04.21.02	The documentation provided by the vendor shall specify how the two independent internal actions protect against the inadvertent bypass of plain text data to a single error.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 82 *(continued)*

Required test procedures	
TE04.21.01	The tester shall verify that the vendor-provided documentation specifies how the two independent internal actions protect against the inadvertent bypass of plain text data due to a single error.
TE04.21.02	The tester shall verify that the two independent internal actions modify firmware, software, or hardware behaviour (or a combination) that is dedicated to mediating the bypass capability, by inspection of the module and by attempting to transition to each bypass state from each state that shows such a transition.

Table 83 — VE and TE of AS04.22

Services — levels 1, 2, 3 and 4	
AS04.22 ISO/IEC 19790:2025, 7.4.3.2	the module shall show its status to indicate whether the bypass capability: a) is not activated, and the module is exclusively providing services with cryptographic processing (e.g. plaintext data are encrypted); b) is activated and the module is exclusively providing services without cryptographic processing (e.g. plaintext data are not encrypted); or c) is alternately activated and deactivated and the module is providing some services with cryptographic processing and some services without cryptographic processing (e.g. for modules with multiple communication channels, plaintext data can be encrypted or not, depending on the configuration of each channel).
Required vendor information	
VE04.22.01	The vendor-provided documentation for the "show status" service shall indicate bypass status.
Required test procedures	
TE04.22.01	The tester shall review the vendor-provided documentation for the "show status" service and verify the bypass service indication.
TE04.22.02	The tester shall transition to each bypass state and verify that the "show status" indicates the applicable bypass status.

6.4.3.3 Re-authentication bypass

Table 84 — VE and TE of AS04.23

Services — levels 1, 2, 3 and 4	
AS04.23 ISO/IEC 19790:2025, 7.4.3.3	The re-authentication bypass shall only be enabled by the crypto officer. This configuration alongside any authentication state for operators may be preserved over resetting, rebooting, or power cycling of the module.
Required vendor information	
VE04.23.01	The vendor shall provide a description of the re-authentication bypass.
Required test procedures	
TE04.23.01	The tester shall verify that the re-authentication bypass can only be enabled and configured by the crypto officer.

Table 85 — VE and TE of AS04.24

Services — levels 1, 2, 3 and 4	
AS04.24 ISO/IEC 19790:2025, 7.4.3.3	two independent internal actions shall be required by the module to prevent inadvertent enabling of the re-authentication bypass due to a single error.
Required test procedures	
This assertion is tested as part of AS04.25.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 86 — VE and TE of AS04.25

Services — levels 1, 2, 3 and 4	
AS04.25 ISO/IEC 19790:2025, 7.4.3.3	The two independent internal actions shall modify firmware, software, or hardware behaviour (or a combination) that is dedicated to mediating the re-authentication bypass (e.g. two different software, firmware or hardware flags are set, one of which may be user-initiated); and
Required vendor information	
VE04.25.01	The vendor shall define a set of two internal actions to be independently done in order to activate the re-authentication bypass.
VE04.25.02	The documentation provided by vendor shall specify how the two independent internal actions modify software or hardware behaviour that is dedicated to mediating the re-authentication bypass.
VE04.25.03	The documentation provided by vendor shall specify how the two independent internal actions protect against the inadvertent output due to a single error.
Required test procedures	
TE04.25.01	The tester shall determine whether the cryptographic module implements a re-authentication bypass. The tester shall verify that the vendor-provided documentation specifies the two independent internal actions performed by the cryptographic module before activating the re-authentication bypass. The tester shall also verify that vendor-provided documentation specifies how the two independent internal actions protect against the inadvertent output due to a single error.
TE04.25.02	The tester shall activate the re-authentication bypass and verify that the two independent internal actions function as specified. If any software or firmware components are executed in the process of activation, the tester shall examine the applicable source code to ensure that the software or firmware components support the requirement for two independent internal actions before activating the re-authentication bypass.
TE04.25.03	The tester shall verify that the vendor-provided documentation specifies how the two independent internal actions protect against the inadvertent output due to a single error.

Table 87 — VE and TE of AS04.26

Services — levels 1, 2, 3 and 4	
AS04.26 ISO/IEC 19790:2025, 7.4.3.3	the module shall show its status to indicate whether the re-authentication bypass is activated.
Required vendor information	
VE04.26.01	The vendor shall document the status indicator used to confirm whether the re-authentication bypass is enabled.
Required test procedures	
TE04.26.01	The tester shall confirm that the vendor-provided documentation details the status indicator used to confirm whether the re-authentication bypass is enabled.
TE04.26.02	The tester shall enable the re-authentication bypass and confirm the documented status indicator lists the re-authentication bypass as enabled.
TE04.26.03	The tester shall disable the re-authentication bypass and confirm the documented status indicator lists the re-authentication bypass as disabled.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.4.3.4 Software/Firmware loading

Table 88 — VE and TE of AS04.27

Services — levels 1, 2, 3 and 4	
AS04.27 ISO/IEC 19790:2025, 7.4.3.4	If a cryptographic module has the capability of loading its software, firmware or bitstream components from an external source, then the following requirements shall apply: {AS04.28 to AS04.32}
Required test procedures	
This assertion is tested as part of AS04.28, AS04.29, AS04.30, AS04.31 and AS04.32.	

Table 89 — VE and TE of AS04.28

Services — levels 1, 2, 3 and 4	
AS04.28 ISO/IEC 19790:2025, 7.4.3.4	the security policy shall specify that, by policy, the operator may only load software, firmware or bitstream validated by a certification body prior to loading to maintain validation, except when loaded into a secure container meeting the requirements of ISO/IEC 19790:2025, 7.5;
Required test procedures	
This assertion is tested as part of ASB.01.	
NOTE 1 This assertion refers to ISO/IEC TS 20540.	

Table 90 — VE and TE of AS04.29

Services — levels 1, 2, 3 and 4	
AS04.29 ISO/IEC 19790:2025, 7.4.3.4	the software/firmware load test specified in ISO/IEC 19790:2025, 7.10.4.4 shall be performed before the loaded code can be executed;
Required test procedures	
This assertion is tested as part of AS10.37, AS10.38, AS10.39, AS10.40, AS10.41 and AS10.42.	

Table 91 — VE and TE of AS04.30

Services — levels 1, 2, 3 and 4	
AS04.30 ISO/IEC 19790:2025, 7.4.3.4	the cryptographic module shall withhold execution of any loaded or modified approved security functions until after the pre-operational self-tests specified in ISO/IEC 19790:2025, 7.10.3 have been successfully executed.
Required test procedures	
This assertion is tested as part of AS10.37, AS10.38, AS10.39, AS10.40, AS10.41 and AS10.42.	

Table 92 — VE and TE of AS04.31

Services — levels 1, 2, 3 and 4	
AS04.31 ISO/IEC 19790:2025, 7.4.3.4	Where pre-operational self-tests only cover the loaded or modified code, it shall be demonstrated why the excluded self-tests are not re-run; and
Required vendor information	
VE04.31.01	The vendor-provided documentation shall specify why it is not necessary to re-run the excluded self-tests when the pre-operational self-tests only cover a sub-set of the pre-operational self-tests supported by the module.
Required test procedures	
TE04.31.01	The tester shall verify that the vendor-provided documentation specifies why excluded self-tests are not required to be re-run, when pre-operational self-tests only cover a sub-set of the pre-operational self-tests supported by the module.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 92 *(continued)*

TE04.31.02	The tester shall exercise the cryptographic module and verify that the module operates according to the documentation.
TE04.31.03	The tester shall inject an error into the newly loaded or modified code. The tester shall initiate the pre-operational test self-tests for the newly loaded or modified code. The tester shall verify that the module fails and enters the error state.
TE04.31.04	The tester shall inject an error into the newly loaded or modified code. The tester shall initiate the pre-operational test self-tests for all the self-tests supported by the module except for the sub-set of self-tests supported or the newly loaded or modified code. The tester shall verify that the module does not fail or enter the error state.

Table 93 — VE and TE of AS04.32

Services — levels 1, 2, 3 and 4	
AS04.32 ISO/IEC 19790:2025, 7.4.3.4	the modules versioning information shall be modified to represent the addition or update of the newly loaded software or firmware.
Required vendor information	
VE04.32.01	The vendor shall provide the means to read the version of the newly loaded software or firmware.
Required test procedures	
TE04.32.01	The tester shall load new software/firmware in the module. The tester shall verify that the versioning information is modified to represent the addition or update of the newly loaded software or firmware.

6.4.4 Authentication

6.4.4.1 Authentication general requirements

Table 94 — VE and TE of AS04.33

Authentication — levels 2, 3 and 4	
AS04.33 ISO/IEC 19790:2025, 7.4.4.1	If role-based authentication mechanisms are supported by a cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator and {shall authenticate the assumption of the selected role (or set of roles).}
Required test procedures	
This assertion is tested as part of AS04.34.	

Table 95 — VE and TE of AS04.34

Authentication — levels 2, 3 and 4	
AS04.34 ISO/IEC 19790:2025, 7.4.4.1	{If role-based authentication mechanisms are supported by a cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator} and shall authenticate the assumption of the selected role (or set of roles).
Required vendor information	
VE04.34.01	The vendor shall document the type of authentication performed for the module. The vendor shall document the mechanisms used to perform the implicit or explicit selection of a role or set of roles and the authentication of the operator to assume the role(s).
Required test procedures	
TE04.34.01	The tester shall verify that the vendor-provided documentation specifies the mechanisms used to select a role or roles and to authenticate the operator to assume a role.
TE04.34.02	The tester shall verify that the module authenticates the operator to a selected role
TE04.34.03	The tester shall assume each role and initiate an error during the authentication procedure. The tester shall verify that the module denies access to each role.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 96 — VE and TE of AS04.35

Authentication — levels 2, 3 and 4	
AS04.35 ISO/IEC 19790:2025, 7.4.4.1	If a cryptographic module permits an operator to change roles, then the module shall authenticate the assumption of any role that was not previously authenticated for that operator.
Required vendor information	
VE04.35.01	The vendor-provided documentation shall describe the ability of an operator to change roles and shall state that an operator shall be authenticated in order to assume a new role.
Required test procedures	
TE04.35.01	The tester shall review the vendor-provided documentation to verify that the method by which an operator can change roles includes the authentication of the operator to assume a new role.
TE04.35.02	The tester shall verify that the module authenticates the operator to a new role.
TE04.35.03	The tester shall perform the following tests. a) Assume a role, attempt to change to another role that the operator is authorized to assume, and verify that the module allows the operator to request services assigned to the new role. b) Assume a role, attempt to change to another role that the operator is not authorized to assume, and verify that the module does not allow the operator to request the services assigned only to the new role.

Table 97 — VE and TE of AS04.36

Authentication — levels 3 and 4	
AS04.36 ISO/IEC 19790:2025, 7.4.4.1	If identity-based authentication mechanisms are supported by a cryptographic module, the module shall require that the operator be individually and uniquely identified, {shall require that one or more roles either be implicitly or explicitly selected by the operator,} {shall authenticate the identity of the operator and that the operator is authorised to assume the selected role or set of roles.}
Required vendor information	
VE04.36.01	The vendor-provided documentation shall specify the type of authentication implemented within the module. The vendor documentation shall specify: a) the mechanism(s) used to perform the identification of the operator, NOTE 1 This is associated with AS04.36. b) the mechanism(s) used to perform the authentication of the operator's identity, NOTE 2 This is associated with AS04.38. c) the mechanism(s) used to perform the implicit or explicit selection of a role or set of roles, NOTE 3 This is associated with AS04.37. d) the mechanism(s) used to perform the verification of the authorization of the operator to assume the role(s), and NOTE 4 This is associated with AS04.38. e) the mechanism(s) used to internally maintain the relationship between the identified and authenticated operator and the selected role or set of roles authorized to assume by the operator. NOTE 5 This is associated with AS04.37, AS04.38, and AS04.39.
Required test procedures	
TE04.36.01	The tester shall verify that the vendor-provided documentation specifies: a) how the operator is uniquely identified, NOTE 6 This is associated with AS04.36. b) how that identity is authenticated,

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 97 *(continued)*

	NOTE 7 This is associated with AS04.38. c) how the operator chooses a role, NOTE 8 This is associated with AS04.37. d) how the authorization of the operator to assume a role is performed based on the authenticated identity, and NOTE 9 This is associated with AS04.38. e) how the relationship is internally maintained between the identified and authenticated operator and the selected role or set of roles to which the operator is authorized to assume. NOTE 10 This is associated with AS04.37, AS04.38, and AS04.39.
TE04.36.02	The tester shall inspect the module and review the vendor-provided documentation to verify that it implements identification and authentication procedure as specified in the vendor-provided documentation, provided under VE04.36.01.
TE04.36.03	The tester shall initiate an error during the authentication procedure and shall verify that the module does not allow the tester to proceed beyond the authentication procedure.
TE04.36.04	The tester shall successfully authenticate his/her identity to the module. When required to select one or more roles, the tester shall select roles which are not compatible with the authenticated identity and shall verify that the authorization to assume these roles is denied. NOTE 11 This test procedure is associated with AS04.36 and AS04.38.

Table 98 — VE and TE of AS04.37

Authentication — levels 3 and 4	
AS04.37 ISO/IEC 19790:2025, 7.4.4.1	{If identity-based authentication mechanisms are supported by a cryptographic module, the module shall require that the operator be individually and uniquely identified,} shall require that one or more roles either be implicitly or explicitly selected by the operator, and {shall authenticate the identity of the operator and that the operator is authorised to assume the selected role or set of roles.}
Required test procedures	
This assertion is not separately tested.	

Table 99 — VE and TE of AS04.38

Authentication — levels 3 and 4	
AS04.38 ISO/IEC 19790:2025, 7.4.4.1	{If identity-based authentication mechanisms are supported by a cryptographic module, the module shall require that the operator be individually and uniquely identified,} {shall require that one or more roles either be implicitly or explicitly selected by the operator,} and shall authenticate the identity of the operator and that the operator is authorised to assume the selected role or set of roles.
Required test procedures	
This assertion is not separately tested.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 100 — VE and TE of AS04.39

Authentication — levels 3 and 4	
AS04.39 ISO/IEC 19790:2025, 7.4.4.1	If a cryptographic module permits an operator to change roles, then the module shall verify the authentication of the identified operator to assume any role that was not previously authenticated and the authorization of the identified operator to assume any role that was not previously authorized.
Required vendor information	
VE04.39.01	The vendor-provided documentation shall specify: a) whether the cryptographic module permits an operator to change roles; b) how an operator can change roles after the operator is identified and authenticated; c) how the relationship is internally maintained between the identified and authenticated operator and the selected role or set of roles that the operator is authorized to (see item e) of VE04.36.01); d) how the cryptographic module enforces the verification of authorization of the identified operator to assume a role that was not previously authorized; e) conditions under which the operator's identity shall be re-authenticated in changing roles.
Required test procedures	
TE04.39.01	The tester shall inspect the module and review the vendor documentation, to verify that the cryptographic module permits an operator to change roles.
TE04.39.02	The tester shall verify in the vendor-provided documentation that the method by which an operator can modify roles without re-authentication of the operator's identity includes the verification of the authorization of the operator for a role not previously authenticated.
TE04.39.03	The tester shall perform the following tests. a) Assume each role, attempt to change to another role that the tester is authorized to assume, verify that the tester's identity is not required to be re-authenticated, and verify that the tester can access the services associated with the new role. The tester shall perform services in the new role that were not associated with the previous role in order to verify that the tester has assumed a different role. b) Assume each role, attempt to change to another role that the operator is not authorized to assume, and verify that the module denies access to the role based on the identity of the operator.

Table 101 — VE and TE of AS04.40

Authentication — levels 1, 2, 3 and 4	
AS04.40 ISO/IEC 19790:2025, 7.4.4.1	When a cryptographic module is reset, rebooted, powered off and subsequently powered on, the module shall require the operator to be authenticated, unless the re-authentication bypass is enabled.
Required vendor information	
VE04.40.01	The vendor-provided documentation shall describe how the results of previous authentications are cleared when the module is powered off.
Required test procedures	
TE04.40.01	The tester shall verify that the vendor-provided documentation describes the clearing of previous authentications upon power off of the module.
TE04.40.02	The tester shall authenticate to the module and assume one or more roles, power off the module, power on the module, and attempt to perform services in those roles. To meet this assertion, the module shall deny access to the services after powering on and require that the tester be re-authenticated.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 102 — VE and TE of AS04.41

Authentication — levels 1, 2, 3 and 4	
AS04.41 ISO/IEC 19790:2025, 7.4.4.1	Authentication data within a cryptographic module shall be protected against unauthorized use, disclosure, modification, and substitution.
Required vendor information	
VE04.41.01	The vendor documentation shall describe the protection of all authentication data within the module. Protection shall include the implementation of mechanisms that protect against unauthorized use, disclosure, modification, and substitution.
Required test procedures	
TE04.41.01	The tester shall verify that the vendor-provided documentation describes the protection of authentication data. The tester shall verify that the documentation describes how the data will be protected against unauthorized use, disclosure, modification, and substitution.
TE04.41.02	The tester shall perform the attempt to access (by circumventing the documented protection mechanisms) authentication data which the tester is not authorized to access. If the module denies access or allows access only to encrypted or otherwise protected forms of data, the requirement is met.
NOTE Approved security functions can be used as part of the authentication mechanism.	

Table 103 — VE and TE of AS04.42

Authentication — levels 1, 2, 3 and 4	
AS04.42 ISO/IEC 19790:2025, 7.4.4.1	Verifier data within a cryptographic module shall be protected against unauthorized use, disclosure, modification, and substitution if it is considered a CSP, or {shall be protected against unauthorized modification and substitution if it is considered a PSP.}
Required vendor information	
VE04.42.01	The vendor documentation shall describe the protection of all verifier data within the module. Protection shall include the implementation of mechanisms that protect against unauthorized use, disclosure, modification, and substitution.
Required test procedures	
TE04.42.01	The tester shall verify that the vendor-provided documentation describes the method to protect verifier data. The tester shall verify that the documentation describes how the data will be protected against unauthorized use, disclosure, modification, and substitution.
TE04.42.02	The tester shall perform the following tests. a) Attempt to access (by circumventing the documented protection mechanisms) verifier data which the tester is not authorized to access. If the module denies access or allows access only to encrypted or otherwise protected forms of data, the requirement is met. b) Attempt to modify or substitute the verifier data using the modules interfaces and any method not specified by the vendor-provided documentation. The module shall prevent or detect the modification or substitution of verifier data such that the module does not allow the tester to authenticate using authentication data compatible with the modified or substituted verifier data or verifier data compatible with the modified or substituted authentication data.
NOTE Approved security functions can be used as part of the authentication mechanism.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 104 — VE and TE of AS04.43

Authentication — levels 1, 2, 3 and 4	
AS04.43 ISO/IEC 19790:2025, 7.4.4.1	{Verifier data within a cryptographic module shall be protected against unauthorized use, disclosure, modification, and substitution if it is considered a CSP}, or shall be protected against unauthorized modification and substitution if it is considered a PSP.
Required vendor information	
VE04.43.01	The vendor-provided documentation shall describe the protection of all verifier data within the module. Protection shall include the implementation of mechanisms that protect against unauthorized modification and substitution if it is considered a PSP.
Required test procedures	
TE04.43.01	The tester shall verify that the vendor-provided documentation describes the protection of verifier data. The tester shall verify that the documentation describes how the data will be protected against unauthorized modification and substitution if it is considered a PSP.
TE04.43.02	The tester shall perform the following tests. a) Attempt to modify or substitute the verifier data using the modules interfaces and any method not specified by the vendor-provided documentation. The module shall prevent or detect the modification or substitution of verifier data such that the module does not allow the tester to authenticate using authentication data compatible with the modified or substituted verifier data or verifier data compatible with the modified or substituted authentication data.

Table 105 — VE and TE of AS04.44

Authentication — levels 2, 3 and 4	
AS04.44 ISO/IEC 19790:2025, 7.4.4.1	If a cryptographic module does not contain the verifier data required to authenticate the operator for the first time the module is accessed, then other authentication methods (e.g. procedural controls) shall be used to control access to the module and initialize the authentication mechanisms.
Required vendor information	
VE04.44.01	The vendor-provided documentation shall specify means to control access to the module before it is initialized.
Required test procedures	
TE04.44.01	The tester shall verify that the vendor-provided documentation describes the procedure by which the operator is authenticated upon accessing the module for the first time.
TE04.44.02	If access to the module before initialization is procedurally controlled, the tester shall initiate a procedural error on an uninitialized module and shall verify that the module denies access. The tester shall assume the authorized 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 initialized and verify that the module denies access to the roles.

Table 106 — VE and TE of AS04.45

Authentication — levels 2, 3 and 4	
AS04.45 ISO/IEC 19790:2025, 7.4.4.1	If default verifier data is used to control access to the approved security functions and processes of the module, then on first-time authentication, new verifier data shall be configured for use in subsequent authentication attempts by each role or identity.
Required vendor information	
VE04.45.01	The vendor-provided documentation shall specify how, upon first-time authentication, the module enforces how the new verifier data shall be set for use in subsequent attempts by each role or identity.
VE04.45.02	The vendor-provided documentation shall specify how, upon subsequent authentication attempts, the module enforces that default verifier data cannot result in a successful authentication.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 106 *(continued)*

Required test procedures	
TE04.45.01	The tester shall verify that the vendor-provided documentation describes how, upon first-time authentication, the module enforces the configuration of the new verifier data for use in subsequent attempts by each role or identity.
TE04.45.02	If the module is designed to accept only new verifier data at first-time authentication, i.e. will not accept re-use of the default verifier data, the tester shall re-enter the default verifier data. If the module does not accept this verifier data, the test passes.

Table 107 — VE and TE of AS04.46

Authentication — levels 2, 3 and 4	
AS04.46 ISO/IEC 19790:2025, 7.4.4.1	This requirement shall be enforced by the module.
Required test procedures	
This assertion is tested as part of AS04.44 and AS04.45.	

Table 108 — VE and TE of AS04.47

Authentication — levels 2, 3 and 4	
AS04.47 ISO/IEC 19790:2025, 7.4.4.1	The module shall implement an approved authentication mechanism as referenced in ISO/IEC 19790:2025, Annex E
Required vendor information	
VE04.47.01	The vendor-provided documentation shall describe the approved authentication mechanism used to authenticate operators.
VE04.47.02	If the module implements an approved authentication mechanism, the vendor shall provide a validation certificate or vendor affirmation, if available, as specified in VE02.18.01 and VE02.18.03.
Required test procedures	
TE04.47.01	The tester shall verify that the authentication mechanism used to authenticate operators is an approved one.

Table 109 — VE and TE of AS04.48

Authentication — levels 2, 3 and 4	
AS04.48 ISO/IEC 19790:2025, 7.4.4.1	The strength of the approved authentication mechanism shall be specified in the security policy in accordance with ISO/IEC 19790:2025, Annex B
Required test procedures	
This assertion is tested as part of ASB.01.	

Table 110 — VE and TE of AS04.49

Authentication — levels 1, 2, 3 and 4	
AS04.49 ISO/IEC 19790:2025, 7.4.4.1	If the cryptographic module uses security functions to authenticate the operator, then those security functions shall be approved security functions.
Required vendor information	
VE04.49.01	The vendor-provided documentation shall specify the list of security functions used to authenticate operators.
VE04.49.02	The vendor shall provide a validation certificate if available for each approved security function as specified in VE02.18.01.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 110 *(continued)*

VE04.49.03	The vendor shall provide a list of all vendor affirmed security functions as specified in VE02.18.03.
Required test procedures	
TE04.49.01	The tester shall verify that the security functions used to authenticate operators are all approved security functions.

Table 111 — VE and TE of AS04.50

Authentication — levels 2, 3 and 4	
AS04.50 ISO/IEC 19790: 2025, 7.4.4.1	For each attempt to use the approved authentication mechanism, the module shall meet the strength of the authentication objective.
Required vendor information	
VE04.50.01	The vendor-provided documentation shall specify each authentication mechanism and the associated false acceptance rate or probability that a random access will succeed.
Required test procedures	
TE04.50.01	The tester shall verify that the vendor-provided documentation for each authentication mechanism specifies the associated false acceptance or random access rate.
TE04.50.02	The tester shall verify that the vendor-provided documentation specifies how to the objective for each authentication mechanism is met.

Table 112 — VE and TE of AS04.51

Authentication — levels 2, 3 and 4	
AS04.51 ISO/IEC 19790:2025, 7.4.4.1	For multiple attempts to use the approved authentication mechanism, the module shall use a rate limiting method to meet the strength of the authentication objective.
Required vendor information	
VE04.51.01	The vendor-provided documentation shall specify each authentication mechanism and the associated rate limiting method for multiple attempts that meets the strength of the authentication objective.
Required test procedures	
TE04.51.01	The tester shall verify the vendor-provided documentation for each authentication mechanism that the associated rate limiting method for multiple attempts is specified.
TE04.51.02	The tester shall verify that the associated rate limiting method is meeting the objective in the vendor-provided documentation for each authentication mechanism.

Table 113 — VE and TE of AS04.52

Authentication — levels 2, 3 and 4	
AS04.52 ISO/IEC 19790:2025, 7.4.4.1	The approved authentication mechanism shall be met by the module's implementation and not rely on documented procedural controls or security rules (e.g. password size restrictions).
Required vendor information	
VE04.52.01	The vendor shall provide complete description of the authentication mechanisms.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 113 *(continued)*

TE04.52.01	The tester shall inspect the module and review the vendor-provided documentation to verify that the approved authentication mechanism is met by the module's implementation and that it does not rely on documented procedural controls or security rules.
TE04.52.02	If the module allows configuration of the authentication mechanism, the tester shall follow the configuration instructions and then attempt to set authentication data to the module using verifier data that meets the strength of the authentication objective of the module, e.g. password of a sufficient length. If the module allows the tester to set the authentication mechanism, the test passes.
TE04.52.03	If the module allows configuration of the authentication mechanism, the tester shall follow the configuration instructions and then attempt to set authentication data to the module using verifier data that does not meet the strength of the authentication objective of the module, e.g. password of an insufficient length. If the module allows the tester to set the authentication mechanism to a weaker strength, the test fails.

Table 114 — VE and TE of AS04.53

Authentication — level 2	
AS04.53 ISO/IEC 19790:2025, 7.4.4.1	If the operating system implements the authentication mechanism, then the authentication mechanism shall meet the requirements in ISO/IEC 19790:2025, 7.4.4 that are applicable to the claimed security level of the authentication mechanism.
Required vendor information	
VE04.53.01	The vendor shall provide authentication mechanism specification of the operating system.
Required test procedures	
TE04.53.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the approved authentication mechanism implemented in the operating system meets the applicable requirements.

Table 115 — VE and TE of AS04.54

Authentication — levels 2, 3 and 4	
AS04.54 ISO/IEC 19790:2025, 7.4.4.1	Feedback of authentication data to an operator shall be obscured during the authentication process to anyone other than the operator (e.g. when entering a password, individual characters are not displayed long enough for anyone other than the operator to see them).
Required vendor information	
VE04.54.01	The vendor-provided documentation shall specify the method used to obscure feedback of the authentication data to anyone other than the operator during entry of the authentication data.
VE04.54.02	The vendor-provided 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 review the vendor-provided documentation to verify that the authentication data is obscured to anyone other than the operator 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 to anyone other than 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.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 116 — VE and TE of AS04.55

Authentication — levels 2, 3 and 4	
AS04.55 ISO/IEC 19790:2025, 7.4.4.1	Feedback provided to an operator during an attempted authentication shall prevent weakening of the authentication mechanism strength beyond the required authentication strength.
Required vendor information	
VE04.55.01	The vendor-provided documentation shall specify the feedback mechanism that is used when the operator is entering authentication data.
Required test procedures	
TE04.55.01	The tester shall verify from the vendor-provided documentation that the feedback mechanism does not provide information that can be used to guess or determine the authentication data.
TE04.55.02	The tester shall enter authentication data to assume each role to ensure that the feedback mechanism does not provide useful information.

6.4.4.2 Security level 1

Table 117 — VE and TE of AS04.56

Authentication — level 1	
AS04.56 ISO/IEC 19790:2025, 7.4.4.2	For security level 1, a cryptographic module is not required to employ authentication mechanisms to control access to the module. If a module does not support authentication mechanisms, the module shall require that the operator either implicitly or explicitly select one or more roles.
Required vendor information	
VE04.56.01	The vendor shall document the type of authentication performed for the module. The vendor shall document the mechanisms used to perform the implicit or explicit selection of a role or set of roles and the authentication of the operator to assume the role(s).
VE04.56.02	The non-proprietary security policy provided by the vendor shall provide a description of the roles, either implicit or explicit, that the operator can assume.
VE04.56.03	The non-proprietary security policy provided by the vendor shall provide instructions for the operator to assume either the implicit or explicit roles.
Required test procedures	
TE04.56.01	The tester shall verify that the vendor-provided non-proprietary security policy provides a description of the roles, either implicit or explicit, that the operator can assume and the means to assume each role.
TE04.56.02	The tester shall invoke the method described in the non-proprietary security policy and verify that each role can either be implicitly or explicitly assumed.

6.4.4.3 Security level 2

Table 118 — VE and TE of AS04.57

Authentication — level 2	
AS04.57 ISO/IEC 19790:2025, 7.4.4.3	For security level 2, a cryptographic module shall at a minimum employ role-based authentication to control access to the module.
Required test procedures	
This assertion is tested as part of AS04.33.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.4.4.4 Security level 3

Table 119 — VE and TE of AS04.58

Authentication — level 3	
AS04.58 ISO/IEC 19790:2025, 7.4.4.4	For security level 3, a cryptographic module shall employ identity-based authentication mechanisms to control access to the module.
Required test procedures	
This assertion is tested as part of AS04.37 and AS04.38.	

6.4.4.5 Security level 4

Table 120 — VE and TE of AS04.59

Authentication — level 4	
AS04.59 ISO/IEC 19790:2025, 7.4.4.5	In addition to the requirements at security level 3, a cryptographic module shall employ multi-factor identity-based authentication mechanisms or another authentication method that meets security level 4 requirements in ISO ISO/IEC 19790:2025, Annex E.
Required vendor information	
VE04.59.01	The vendor shall provide specification of a multi-factor identity-based authentication or another authentication method that meets security level 4 requirements in ISO/IEC 19790:2025, Annex E
Required test procedures	
TE04.59.01	The tester shall verify the vendor documentation and assess multi-factor identity-based authentication or another authentication method that meets security level 4 requirements in ISO/IEC 19790:2025, Annex E.
TE04.59.02	If the module supports multi-factor identity-based authentication, the tester shall verify that the authentication mechanisms require multiple authentication factors of at least two independent authentication factor categories, by categorizing each authentication factor into either something a person knows, something a person has, or something that a person is.

6.5 Software/firmware security

6.5.1 Software/firmware security general requirements

Table 121 — VE and TE of AS05.01

Software/firmware security general requirements — levels 1, 2, 3 and 4	
AS05.01 ISO/IEC 19790:2025, 7.5.1	The requirements of this clause shall apply to software, firmware, or bitstream components of a cryptographic module.
Required test procedures	
This assertion is tested as part of AS05.09, AS05.10, AS05.11, AS05.12, AS05.13, AS05.14, AS05.15, AS05.16, AS05.17, AS05.18, AS05.19, AS05.20, AS05.21, AS05.22, AS05.23, AS05.24, AS05.25, AS05.26, AS05.27, AS05.28 and AS05.29.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 122 — VE and TE of AS05.02

Software/firmware security general requirements — level 1	
AS05.02 ISO/IEC 19790:2025, 7.5.1	The secure container shall be controlled to prevent the non-validated executable firmware within the secure container from interfering or compromising the cryptographic module. In addition, {the following requirements shall apply:} {AS05.04 to AS05.08}
Required vendor information	
VE05.02.01	The vendor shall provide a description of how the secure container is controlled to prevent the non-validated executable firmware within the secure container from interfering or compromising the cryptographic module.
Required test procedures	
TE05.02.01	The tester shall review the vendor-provided documentation and by inspection of the implementation that the secure container is controlled to prevent the non-validated executable firmware within the secure container from interfering or compromising the cryptographic module.
NOTE This assertion is not applicable if the cryptographic module vendor does not claim the secure container.	

Table 123 — VE and TE of AS05.03

Software/firmware security general requirements — level 1	
AS05.03 ISO/IEC 19790:2025, 7.5.1	{The secure container shall be controlled to prevent the non-validated executable firmware within the secure container from interfering or compromising the cryptographic module.} In addition, the following requirements shall apply: {AS05.04 to AS05.08}.
Required test procedures	
This assertion is tested as part of AS05.04, AS05.05, AS05.06, AS05.07 and AS05.08.	

Table 124 — VE and TE of AS05.04

Software/firmware security general requirements — level 1	
AS05.04 ISO/IEC 19790:2025, 7.5.1	The software/firmware load test specified in ISO/IEC 19790:2025, 7.10.4.4 shall be performed by the module before the firmware that is loaded into the secure container can be executed.
Required test procedures	
This assertion is tested as part of AS10.37, AS10.38, AS10.39, AS10.40, AS10.41 and AS10.42.	

Table 125 — VE and TE of AS05.05

Software/firmware security general requirements — level 1	
AS05.05 ISO/IEC 19790:2025, 7.5.1	The boundary of the module with the secure container firmware shall be defined.
Required vendor information	
VE05.05.01	The vendor shall provide a description of the boundary of the cryptographic module with the secure container firmware.
Required test procedures	
TE05.05.01	The tester shall verify that the documentation provided by the vendor identifies the boundary of the cryptographic module with the secure container firmware.
TE05.05.02	The tester shall verify by identifying the boundary of the cryptographic module that the boundary of the cryptographic module in the documentation provided by the vendor is consistent with the boundary of the cryptographic module.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 126 — VE and TE of AS05.06

Software/firmware security general requirements — level 1	
AS05.06 ISO/IEC 19790:2025, 7.5.1	The interfaces provided by the module to the secure container firmware shall be defined (e.g. all interfaces that the module provides to the secure container to allow data and control input and output, status, etc. to the module's external interfaces from the executing firmware in the secure container).
Required vendor information	
VE05.06.01	The vendor shall provide a description of the interfaces provided by the cryptographic module to the secure container firmware.
Required test procedures	
TE05.06.01	The tester shall verify that the vendor-provided documentation identifies the interfaces provided by the cryptographic module to the secure container firmware.
TE05.06.02	The tester shall review the vendor-provided documentation and, identify the interfaces of the cryptographic module, to inspect that the cryptographic module is consistent with the interfaces of the cryptographic module.

Table 127 — VE and TE of AS05.07

Software/firmware security general requirements — levels 1, 2, 3 and 4	
AS05.07 ISO/IEC 19790:2025, 7.5.1	The services provided by the module to the secure container firmware shall be defined.
Required vendor information	
VE05.07.01	The vendor shall provide a description of the services provided by the cryptographic module to the secure container firmware, including the roles and authentication required to access each service.
Required test procedures	
TE05.07.01	The tester shall verify that the vendor-provided documentation identifies the services provided by the cryptographic module to the secure container firmware, including the roles and authentication required to access each service.
TE05.07.02	The tester shall verify from the vendor-provided documentation, by identifying the services of the cryptographic module that the cryptographic module is consistent with the services of the cryptographic module.
NOTE Authentication ahead of access to services requiring use of an authenticated role is tested as part of AS04.56 to AS04.59.	

Table 128 — VE and TE of AS05.08

Software/firmware security general requirements — level 1	
AS05.08 ISO/IEC 19790:2025, 7.5.1	All roles of the module that have access to the secure container firmware shall be defined.
Required vendor information	
VE05.08.01	The vendor shall provide a description of the roles of the cryptographic module that have access to the secure container firmware.
Required test procedures	
TE05.08.01	The tester shall verify that the vendor-provided documentation identifies the roles of the cryptographic module that have access to the secure container firmware.
TE05.08.02	The tester shall verify the vendor-provided documentation, by identifying the roles of the cryptographic module, to ensure that the cryptographic module is consistent with the roles of the cryptographic module that have access to the secure container firmware.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 129 — VE and TE of AS05.09

Software/firmware security general requirements — levels 1, 2, 3 and 4	
AS05.09 ISO/IEC 19790:2025, 7.5.1	The documentation for software/firmware security specified in ISO/IEC 19790:2025, A.2.4 shall be provided.
Required vendor information	
VE05.09.01	The vendor shall provide documentation as specified in ISO/IEC 19790:2025, A.2.4.
Required test procedures	
TE05.09.01	The tester shall verify completeness of the documentation specified in ISO/IEC 19790:2025, A.2.4.

6.5.2 Security level 1

Table 130 — VE and TE of AS05.10

Security level 1 — levels 1, 2, 3 and 4	
AS05.10 ISO/IEC 19790:2025, 7.5.2	The following requirements shall apply to software, firmware, or bitstream components of a cryptographic module for security level 1: {AS05.11 to AS05.19}.
Required test procedures	
This assertion is not separately tested.	

Table 131 — VE and TE of AS05.11

Security level 1 — levels 1, 2, 3 and 4	
AS05.11 ISO/IEC 19790:2025, 7.5.2	All software, firmware, or bitstream shall be in a form that satisfies the requirements of this document without modification prior to installation.
Required vendor information	
VE05.11.01	The vendor shall provide software, firmware, or bitstream specification.
Required test procedures	
TE05.11.01	The tester shall verify, by inspection of the cryptographic module, that specifications provided by vendor-provided documentation are consistent with the actual design of the cryptographic module.

Table 132 — VE and TE of AS05.12

Security level 1 — levels 1, 2, 3 and 4	
AS05.12 ISO/IEC 19790:2025, 7.5.2	A cryptographic mechanism using an approved integrity technique shall be applied to all software and firmware components within the module's defined cryptographic boundary in one of the following ways: a) by the cryptographic module itself; or b) by another validated cryptographic module utilising an approved service.
Required vendor information	
VE05.12.01	The vendor-provided documentation shall describe the approved integrity technique that is applied to software and firmware modules and the disjoint software or firmware components of a hybrid module.
VE05.12.02	The vendor-provided documentation shall specify how the integrity technique is applied to software and firmware modules and the disjoint software or firmware components of a hybrid module using either: a) a single encompassing message authentication code or signature, or

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 132 *(continued)*

	b) multiple disjoint codes or signatures.
VE05.12.03	The vendor-provided documentation shall describe whether the approved integrity technique is implemented either by the cryptographic module itself or by another validated cryptographic module utilising an approved service.
VE05.12.04	The vendor-provided documentation shall specify the location of the cryptographic key used in the integrity technique. If the approved digital signature is used as the integrity technique, the vendor-provided documentation shall also specify the location of the private signing key which is used to generate the reference signature.
VE05.12.05	The vendor shall provide a validation certificate if available or vendor affirmation for the approved integrity technique as specified in VE02.18.01 and VE02.18.03.
VE05.12.06	The vendor-provided documentation shall describe whether temporary value(s) generated during the integrity test of the module's software or firmware are zeroized upon completion of the integrity test.
Required test procedures	
TE05.12.01	The tester shall verify by inspection of the cryptographic module that an approved integrity technique is applied to software and firmware modules and the disjoint software or firmware components of a hybrid module.
TE05.12.02	The tester shall verify that the vendor has provided a validation certificate if available or vendor affirmation for the approved integrity technique implemented as specified in VE02.18.01 and VE02.18.03.
TE05.12.03	If the module implements a hash or MAC for the software/firmware integrity test, the tester shall verify that the vendor-provided documentation of the software/firmware integrity test fully describes the process by which the hash or MAC is calculated and verified.
TE05.12.04	If the module implements an approved digital signature for the software/firmware integrity test, the tester shall verify that the vendor-provided documentation of the software/firmware integrity test includes the following: a) specification of the approved digital signature algorithm implemented; b) identification of software and firmware that is protected using the approved digital signatures; c) verification that the pre-calculated value of the approved digital signature is included with the software or firmware; d) verification of the approved digital signature; e) failure of the self-test upon failure of the approved digital signature verification.
TE05.12.05	Even if the approved integrity technique is provided by another validated module, the tester shall verify that the determination of pass or fail of the software/firmware integrity test is made as specified in AS10.01.
TE05.12.06	By checking the code and design documentation, the tester shall verify that the implementation of the software/firmware test is consistent with the information provided under AS05.12 and AS05.15.
TE05.12.07	The tester shall modify the cryptographic software and firmware components. This test has failed if the integrity mechanisms do not detect the modifications.
TE05.12.08	The tester shall verify that the vendor-provided documentation describes whether temporary value(s) generated during the integrity test of the module's software or firmware are zeroized upon completion of the integrity test.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 133 — VE and TE of AS05.13

Security level 1 — levels 1, 2, 3 and 4	
AS05.13 ISO/IEC 19790:2025, 7.5.2	Acryptographic mechanism using an approved integrity technique or an error detection code (EDC) shall be applied to all firmware or bitstream components within the hardware module's defined cryptographic boundary or within disjoint hardware components of the hybrid module.
Required vendor information	
VE05.13.01	The vendor-provided documentation shall describe the approved integrity technique or error detection code that is applied to all firmware or bitstream components of a hardware cryptographic module and the firmware or bitstream components within a disjoint hardware component of a hybrid cryptographic module.
VE05.13.02	The vendor-provided documentation shall specify how the approved integrity technique or error detection code is applied to all firmware or bitstream components of a hardware cryptographic module and the firmware or bitstream components within a disjoint hardware component of a hybrid cryptographic module.
VE05.13.03	If the module implements an error detection code, the vendor shall provide the documentation required under VE05.14.01.
VE05.13.04	If the cryptographic module implements an approved integrity technique for the integrity test, the vendor-provided documentation shall provide information required under VE05.12.02, VE05.12.04, and VE05.12.05.
Required test procedures	
TE05.13.01	The tester shall verify by inspection of the cryptographic module that an approved integrity technique or error detection code is applied to all firmware or bitstream components of a hardware cryptographic module and all firmware or bitstream components within a disjoint hardware component of a hybrid cryptographic module.
TE05.13.02	If the module implements an error detection code, the tester shall follow procedures required under TE05.14.01.
TE05.13.03	If the module implements a hash or MAC for the integrity test, the tester shall follow procedures required under TE05.12.03.
TE05.13.04	If the module implements an approved digital signature for the integrity test, the tester shall follow procedures required under TE05.12.04.
TE05.13.05	By checking the code and design documentation, the tester shall verify that the implementation of the integrity test is consistent with the information provided under AS05.13 to AS05.15.
TE05.13.06	The tester shall modify the cryptographic firmware or bitstream components. This test has failed if the integrity mechanisms do not detect the modifications.

Table 134 — VE and TE of AS05.14

Security level 1 — levels 1, 2, 3 and 4	
AS05.14 ISO/IEC 19790:2025, 7.5.2	If an EDC is used, the EDC shall be at least 16 bits in length.
Required vendor information	
VE05.14.01	The vendor shall provide the specification of the error detection code used within the module. This mechanism shall be an error detection code of at least 16 bits in length. The vendor shall provide: a) description of EDC calculation algorithm; b) calculation of the EDCs when the firmware is installed; c) description of verification process: 1) recalculation of the EDCs when the self-test is initiated; 2) comparison of the stored EDC against the recalculated EDC; 3) expected outputs for success or failure of test.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 134 *(continued)*

Required test procedures	
TE05.14.01	The tester shall verify that the error detection code is at least 16 bits in length and verify by inspection that the following information is provided: a) the implementation of the EDC calculation algorithm; b) the verification process: 1) recalculation of the EDCs when the self-test is initiated; 2) comparison of the stored EDC against the recalculated EDC; 3) the expected outputs for success or failure of test.

Table 135 — VE and TE of AS05.15

Security level 1 — levels 1, 2, 3 and 4	
AS05.15 ISO/IEC 19790:2025, 7.5.2	If the integrity test fails (i.e. the calculated result is not successfully verified or the EDC cannot be verified depending on the module type), the module shall enter the error state.
Required vendor information	
VE05.15.01	The vendor shall provide the specification of the integrity test of software/firmware. This mechanism shall be an approved integrity technique or an error detection code depending on the module type (see AS05.12 and AS05.13).
Required test procedures	
TE05.15.01	The tester shall verify that if the integrity test fails, the module enters the error state.

Table 136 — VE and TE of AS05.16

Security level 1 — levels 1, 2, 3 and 4	
AS05.16 ISO/IEC 19790:2025, 7.5.2	The integrity test may consist of a single encompassing message authentication code; EDC; signature; or multiple disjoint authentication codes, EDCs or signatures of which failure of any disjoint authentication code, EDC or signature shall cause the module to enter the error state.
Required test procedures	
This assertion is tested as part of AS05.12, AS05.13 and AS05.15.	

Table 137 — VE and TE of AS05.17

Security level 1 — levels 1, 2, 3 and 4	
AS05.17 ISO/IEC 19790:2025, 7.5.2	An operator shall be able to perform the integrity test on demand.
Required vendor information	
VE05.17.01	The vendor-provided documentation shall describe the way to perform the integrity test on demand via a service, resetting, rebooting, or power cycling.
Required test procedures	
TE05.17.01	The tester shall verify that the integrity test can be performed on demand via a service, resetting, rebooting, or power cycling.
TE05.17.02	The tester shall verify by inspection of the module that the integrity of all software and firmware components within the module is tested during the integrity test callable on demand via a service, resetting, rebooting, or power cycling.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 138 — VE and TE of AS05.18

Security level 1 — levels 1, 2, 3 and 4	
AS05.18 ISO/IEC 19790:2025, 7.5.2	All data and control inputs, and data, control and status outputs of the cryptographic module and services shall be directed through a defined module interface.
Required vendor information	
VE05.18.01	The vendor-provided documentation requirement is specified under VE05.22.01 and 6.3.1, 6.3.2 and 6.4.3.
Required test procedures	
TE05.18.01	The tester shall verify that the vendor-provided documentation specifies the following: a) total set of commands used to request the services of the cryptographic module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.
TE05.18.02	The tester shall review the vendor-provided documentation and inspect the module to verify that all data and control inputs, and data, control and status outputs of the cryptographic module and services pass through only the defined module interface.

Table 139 — VE and TE of AS05.19

Security level 1 — levels 1, 2, 3 and 4	
AS05.19 ISO/IEC 19790:2025, 7.5.2	If software, firmware, or bitstream is loaded and is associated, bound to, modifies or is an executable requisite of the validated module, then the software/firmware load test is applicable and shall be performed by the validated module.
Required vendor information	
VE05.19.01	The vendor shall provide a specification of software/firmware loading processes, including: a) the type(s) of software or firmware loading processes: 1) adding software, firmware, or bitstream components; 2) updating existing software, firmware, or bitstream components; b) the location where newly loaded software, firmware, or bitstream components are stored; c) existing software, firmware, bitstream or hardware components to enforce the software, firmware or bitstream loading; d) existing software/firmware/bitstream components which will be affected, modified, or replaced as a result of software/firmware/bitstream loading; e) existing software/firmware/bitstream components which will be neither affected, modified, nor replaced as a result of software/firmware/bitstream loading.
VE05.19.02	The vendor shall provide the specification of the software/firmware load test performed by the validated module.
Required test procedures	
TE05.19.01	The tester shall review the vendor-provided documentation and inspect the module to determine whether the cryptographic module has a capability of loading software, firmware, or bitstream.
TE05.19.02	If the cryptographic module has a capability of loading any software, firmware, or bitstream components, the tester shall review the vendor documentation and inspect the module by the type(s) of software/firmware/bitstream loading to determine whether additional software, firmware and bitstream components are loaded, or existing software, firmware, and bitstream components are updated.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 139 *(continued)*

TE05.19.03	If additional software, firmware, and bitstream components are loaded, the tester shall verify that the software/firmware/bitstream load test is performed with the software/firmware/bitstream loading.
TE05.19.04	The tester shall review the vendor-provided documentation and inspect the module to verify that a crypto officer role is assumed to perform software/firmware/bitstream loading.
TE05.19.05	By checking the code and design documentation, the tester shall verify that the implementation of the software/firmware loading is consistent with the information provided under VE05.19.01.

6.5.3 Security level 2

Table 140 — VE and TE of AS05.20

Security level 2 — levels 2, 3 and 4	
AS05.20 ISO/IEC 19790:2025, 7.5.3	In addition to the requirements of security level 1, the following requirements shall apply to software and firmware modules or the disjoint software and firmware components of a hybrid module for security level 2: {AS05.21 to AS05.24}.
Required test procedures	
This assertion is tested as part of AS05.21, AS05.22, AS05.23 and AS05.24.	

Table 141 — VE and TE of AS05.21

Security level 2 — levels 2, 3 and 4	
AS05.21 ISO/IEC 19790:2025, 7.5.3	Code shall only be in executable form.
Required vendor information	
VE05.21.01	The vendor shall provide software and firmware description with the executable form used.
Required test procedures	
TE05.21.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the documented executable form does not require further compilation and that there is no dynamically modified code.
TE05.21.02	The tester shall inspect the cryptographic module and review the vendor-provided documentation to verify that the documented executable form is used for each software/firmware components.

Table 142 — VE and TE of AS05.22

Security level 2 — levels 2, 3 and 4	
AS05.22 ISO/IEC 19790:2025, 7.5.3	There shall be no services or control settings via the module interface to allow the operator to initiate or perform debugging techniques when operational.
Required vendor information	
VE05.22.01	The vendor shall provide specification of module interface services or control settings.
Required test procedures	
TE05.22.01	The tester shall verify the vendor documented specification of services or control settings.
TE05.22.02	The tester shall verify from the vendor-provided documentation that the services or control settings do not allow the operator to initiate or perform debugging techniques.
TE05.22.03	The tester shall test the services or control settings to verify that the operator cannot initiate or perform debugging techniques.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 143 — VE and TE of AS05.23

Security level 2 — levels 2, 3 and 4	
AS05.23 ISO/IEC 19790:2025, 7.5.3	An approved digital signature or keyed message authentication code shall be applied to all software and firmware within the module's defined cryptographic boundary.
Required vendor information	
VE05.23.01	The vendor shall provide documentation that identifies the technique used to maintain the integrity of the cryptographic software and firmware components.
Required test procedures	
TE05.23.01	The tester shall verify that the information specified in VE05.23.01 is included.
TE05.23.02	The tester shall attempt to corrupt the cryptographic software and firmware components. If the module determines that the integrity is maintained, this test has failed.

Table 144 — VE and TE of AS05.24

Security level 2 — levels 2, 3 and 4	
AS05.24 ISO/IEC 19790:2025, 7.5.3	If the calculated result is not successfully verified, the test fails, and the module shall enter the error state.
Required test procedures	
This assertion is tested as part of AS05.15 and AS05.23.	

6.5.4 Security levels 3 and 4

Table 145 — VE and TE of AS05.25

Security levels 3 and 4 — levels 3 and 4	
AS05.25 ISO/IEC 19790:2025, 7.5.4	In addition to the requirements of security levels 1 and 2, the following requirements shall apply to software and firmware modules or the disjoint software and firmware components of a hybrid module for security levels 3 and 4: {AS05.26 to AS05.29}
Required test procedures	
This assertion is tested as part of AS05.26, AS05.27, AS05.28 and AS05.29.	

Table 146 — VE and TE of AS05.26

Security levels 3 and 4 — levels 3 and 4	
AS05.26 ISO/IEC 19790:2025, 7.5.4	A cryptographic mechanism using an approved digital signature shall be applied to all software and firmware components within the module's defined cryptographic boundary.
Required vendor information	
VE05.26.01	The vendor shall provide documentation of the approved digital signature mechanism.
Required test procedures	
TE05.26.01	The tester shall verify by inspection of the cryptographic module that a cryptographic mechanism using an approved digital signature mechanism is applied to all software and firmware components within the module's defined cryptographic boundary.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 147 — VE and TE of AS05.27

Security levels 3 and 4 — levels 3 and 4	
AS05.27 ISO/IEC 19790:2025, 7.5.4	If the calculated result is not successfully verified, the test fails, and the module shall enter the error state.
Required test procedures	
This assertion is tested as part of AS05.23.	

Table 148 — VE and TE of AS05.28

Security levels 3 and 4 — levels 3 and 4	
AS05.28 ISO/IEC 19790:2025, 7.5.4	Failure of the verification of the single signature or any disjoint signature shall cause the module to enter the error state.
Required test procedures	
This assertion is tested as part of AS05.12.	

Table 149 — VE and TE of AS05.29

Security levels 3 and 4 — levels 3 and 4	
AS05.29 ISO/IEC 19790:2025, 7.5.4	The private signing key shall reside outside the module.
Required vendor information	
VE05.29.01	The vendor-provided documentation requirement is specified under VE05.12.04. The vendor design shall ensure that the private signing key for generating reference signature does not reside within the cryptographic module's cryptographic boundary.
Required test procedures	
TE05.29.01	The tester shall inspect the cryptographic module and review the vendor documentation to verify that the private signing key does not reside within the cryptographic boundary.

6.6 Operational environment

6.6.1 Operational environment general requirements

Table 150 — VE and TE of AS06.01

Operational environment general requirements — level 1	
AS06.01 ISO/IEC 19790:2025, 7.6.1	Hardware, firmware and hybrid firmware modules shall use a non-modifiable or limited operational environment.
Required test procedures	
This assertion is tested as part of AS06.03 and AS06.04.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 151 — VE and TE of AS06.02

Operational environment general requirements — levels 1 and 2	
AS06.02 ISO/IEC 19790:2025, 7.6.1	Software modules and hybrid software modules shall use a modifiable operational environment.
Required test procedures	
This assertion is tested as part of AS06.07, AS06.08, AS06.09, AS06.10, AS06.11, AS06.12, AS06.13, AS06.14, AS06.15, AS06.16, AS06.17, AS06.18, AS06.19, AS06.20, AS06.21, AS06.22, AS06.23, AS06.24, AS06.25, AS06.26, AS06.27, AS06.28, AS06.29, AS06.30, AS06.31, AS06.32 and AS06.33.	

6.6.2 Clause applicability

NOTE The requirements AS06.07 to AS06.33 apply to the operating system or operational environments as relevant.

Table 152 — VE and TE of AS06.03

Clause applicability — level 1	
AS06.03 ISO/IEC 19790:2025, 7.6.2	If the operational environment is non-modifiable and the module is security level 1 in ISO/IEC 19790:2025, 7.7, the operating system requirements in ISO/IEC 19790:2025, 7.6.3 security level 1 shall apply.
Required test procedures	
This assertion is tested as part of AS06.07, AS06.08, AS06.09, AS06.10 and AS06.11.	

Table 153 — VE and TE of AS06.04

Clause applicability — level 1	
AS06.04 ISO/IEC 19790:2025, 7.6.2	If the operational environment is a limited operational environment and the module is security level 1 in ISO/IEC 19790:2025, 7.7 the operating system requirements in ISO/IEC 19790:2025, 7.6.3 security level 1 shall apply.
Required test procedures	
This assertion is tested as part of AS06.07, AS06.08, AS06.09, AS06.10 and AS06.11.	

Table 154 — VE and TE of AS06.05

Clause applicability — levels 1 and 2	
AS06.05 ISO/IEC 19790:2025, 7.6.2	If the operational environment is a modifiable operational environment, the requirements in ISO/IEC 19790:2025, 7.6.3 shall apply.
Required test procedures	
This assertion is tested as part of AS06.07, AS06.08, AS06.09, AS06.10, AS06.11, AS06.12, AS06.13, AS06.14, AS06.15, AS06.16, AS06.17, AS06.18, AS06.19, AS06.20, AS06.21, AS06.22, AS06.23, AS06.24, AS06.25, AS06.26, AS06.27, AS06.28, AS06.29, AS06.30, AS06.31, AS06.32 and AS06.33.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 155 — VE and TE of AS06.06

Clause applicability — levels 1 and 2	
AS06.06 ISO/IEC 19790:2025, 7.6.2	The documentation requirements for the operational environment specified in ISO/IEC 19790:2025, A.2.5 shall be provided.
Required vendor information	
VE06.06.01	The vendor shall provide the documentation requirements as specified in ISO/IEC 19790:2025, A.2.5.
Required test procedures	
TE06.06.01	The tester shall verify that the vendor provides documentation as specified in ISO/IEC 19790:2025, A.2.5.

6.6.3 Operating system requirements for modifiable operational environments

6.6.3.1 Security level 1

Table 156 — VE and TE of AS06.07

Operating system requirements for modifiable operational environments — levels 1 and 2	
AS06.07 ISO/IEC 19790:2025, 7.6.3.1	Each instance of a cryptographic module shall have control over its own SSPs.
Required vendor information	
VE06.07.01	The vendor shall provide a description of the operating system mechanism used to ensure that each instance of a cryptographic module has control over its own SSPs while the cryptographic process is in use.
Required test procedures	
TE06.07.01	The tester shall review the vendor-provided documentation and inspect the operating system to verify that each instance of a cryptographic module has control over its own SSPs while the cryptographic module is in use.
TE06.07.02	The tester shall review the vendor-provided documentation and inspect the operating system to verify that the requirement is enforced by the cryptographic module itself.
TE06.07.03	The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to gain unauthorized access to secret and private keys, intermediate key generation values, and other SSPs which are under the control of the cryptographic module. If the tester can gain unauthorized access, the test fails.
NOTE 1 Each instance of a cryptographic module controls its own SSPs and are not owned or controlled by external processes/operators. NOTE 2 This requirement is not enforced by administrative documentation and procedures but by the cryptographic module itself.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 157 — VE and TE of AS06.08

Operating system requirements for modifiable operational environments — levels 1 and 2	
AS06.08 ISO/IEC 19790:2025, 7.6.3.1	The operating system shall provide the capability to separate individual application processes from each other in order to prevent uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless of whether these data are in the process memory or stored on persistent storage within the operational environment.
Required vendor information	
VE06.08.01	The vendor shall provide a description of the operating system mechanism used to provide the capability to separate individual application processes from each other in order to prevent uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless of whether this data is in the process memory or stored on persistent storage within the operational environment.
Required test procedures	
TE06.08.01	The tester shall review the vendor-provided documentation and inspect the operating system mechanism used to verify that it provides the capability to separate individual application processes from each other in order to prevent uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless of whether this data is in the process memory or stored on persistent storage within the operational environment.
TE06.08.02	The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to gain access to CSPs and perform modifications of SSPs regardless of whether this data is in the process memory or stored on persistent storage within the operational environment. If the tester can gain access, the test fails.

Table 158 — VE and TE of AS06.09

Operating system requirements for modifiable operational environments — levels 1 and 2	
AS06.09 ISO/IEC 19790:2025, 7.6.3.1	Restrictions to the configuration of the operating system shall be documented in the security policy of the cryptographic module.
Required vendor information	
VE06.09.01	The vendor shall provide documentation which provides a description of any restrictions to the configuration of the operating system.
Required test procedures	
TE06.09.01	The tester shall verify that any restrictions to the configuration of the operating system are documented in the security policy.

Table 159 — VE and TE of AS06.10

Operating system requirements for modifiable operational environments — levels 1 and 2	
AS06.10 ISO/IEC 19790:2025, 7.6.3.1	Processes that are spawned by the cryptographic module shall be owned by the module and are not owned by external processes/operators.
Required vendor information	
VE06.10.01	The vendor shall provide a description of the operating system mechanism used to ensure that processes which are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.
Required test procedures	
TE06.10.01	The tester shall verify the vendor-provided documentation and inspect the operating system to ensure that processes which are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 159 *(continued)*

TE06.10.02	The tester shall verify the vendor-provided documentation and inspect the operating system to ensure that the requirement shall be enforced by the cryptographic module itself.
TE06.10.03	The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to gain ownership of a spawned cryptographic process that is owned by a cryptographic module from either a separate external process or operator. If the tester can gain ownership of a spawned cryptographic process, the test fails.
NOTE This requirement cannot be enforced by administrative documentation and procedures but by the cryptographic module itself.	

Table 160 — VE and TE of AS06.11

Operating system requirements for modifiable operational environments — levels 1 and 2	
AS06.11 ISO/IEC 19790:2025, 7.6.3.1	These requirements cannot be enforced by administrative documentation and procedures and shall be enforced by the operating system itself. {AS06.07 to AS06.10}
Required vendor information	
VE06.11.01	The vendor shall provide documentation which provides a description of how the requirements from ISO/IEC 19790:2025, 7.6.3 are enforced by the operating system.
Required test procedures	
TE06.11.01	The tester shall verify that the vendor-provided documentation provides a description of how the requirements from ISO/IEC 19790:2025, 7.6.3 are enforced by the operating system.
TE06.11.02	The tester shall inspect the operating system and review the vendor-provided documentation to verify that requirements are enforced by the operating system.

6.6.3.2 Security level 2

Table 161 — VE and TE of AS06.12

Operating system requirements for modifiable operational environments — level 2	
AS06.12 ISO/IEC 19790:2025, 7.6.3.2	In addition to the requirements of security level 1, for security level 2 an operating system shall meet the following requirements or as allowed by the certification body: {AS06.13 to AS06.33}
Required vendor information	
VE06.12.01	The vendor shall provide documentation which provides a description of the operating system.
VE06.12.02	The vendor shall provide documentation comparing the operating system with the operating system allowed by the certification body.
Required test procedures	
TE06.12.01	The tester shall verify that the vendor-provided documentation provides a description of the operating system.
TE06.12.02	The tester shall inspect the operating system to verify that it matches the vendor-provided description of the operating system.
TE06.12.03	The tester shall inspect the operating system and review the vendor-provided description of the operating system to verify that the operating system is allowed by the certification body.
NOTE 1 If the operating system requirements are not specified by a certification body, the assertion is tested in AS06.12 to AS06.33. NOTE 2 If the operating system requirements are specified by a certification body the assertion is tested as specified in AS06.12.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 162 — VE and TE of AS06.13

Operating system requirements for modifiable operational environments — level 2	
AS06.13 ISO/IEC 19790:2025, 7.6.3.2	All cryptographic software, SSPs, control and status information shall be under the control of an operating system that implements either role-based access controls or, at the minimum, a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions, for example through access control lists (ACLs), and with the capability of assigning each user to more than one group.
Required vendor information	
VE06.13.01	The vendor shall provide operating system documentation which provides a description of the operating system control mechanisms which implements either role-based access controls or, at the minimum, a discretionary access control with a robust mechanism of defining new groups and assigning restrictive permissions. For example, this mechanism can include access control lists (ACLs) and with the capability of assigning each user to more than one group.
Required test procedures	
TE06.13.01	The tester shall verify, from the vendor-provided documentation and by inspection of operating system control mechanisms, that the operating system implements either role-based access controls or, at the minimum, a discretionary access control with a robust mechanism of defining new groups and assigning restrictive permissions, for example, through access control lists (ACLs) and with the capability of assigning each user to more than one group.
TE06.13.02	The tester shall configure the operating systems role-based access controls or discretionary access controls to give permissions to a specific user or group. The tester, assuming a permitted user or group role, shall attempt to execute, modify, or read SSPs, control or status data which the tester has authorized access.
TE06.13.03	The tester shall configure the operating systems role-based access controls or discretionary access controls to give permissions to a specific user or group. The tester, assuming a different user or group role, shall attempt to execute, modify, or read SSPs, control or status data, to which the tester has unauthorized access.

Table 163 — VE and TE of AS06.14

Operating system requirements for modifiable operational environments — level 2	
AS06.14 ISO/IEC 19790:2025, 7.6.3.2	The operating system shall be configured to protect against unauthorized execution, unauthorized modification, and unauthorized reading of SSPs, control and status data;
Required vendor information	
VE06.14.01	The vendor shall provide operating system documentation which provides a description of the operating system control mechanisms which can be configured to protect against unauthorized execution, unauthorized modification, and unauthorized reading of SSPs, control and status data.
Required test procedures	
TE06.14.01	The tester shall review the vendor-provided documentation and inspect operating system control mechanisms, to verify that the operating system can be configured to protect against unauthorized execution, unauthorized modification, and unauthorized reading of SSPs, control and status data.
TE06.14.02	The tester shall configure the operating system to protect against unauthorized execution, unauthorized modification, and unauthorized reading of SSPs, control and status data. While executing a cryptographic process, the tester shall attempt to execute, modify or read SSPs, control or status data, to which the tester has authorized access.
TE06.14.03	The tester shall configure the operating system to protect against unauthorized execution, unauthorized modification, and unauthorized 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, to which the tester has unauthorized access.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 164 — VE and TE of AS06.15

Operating system requirements for modifiable operational environments — level 2	
AS06.15 ISO/IEC 19790:2025, 7.6.3.2	{To protect plaintext data, cryptographic software and SSPs, the access control mechanisms of the operating system} shall be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to execute the stored cryptographic software;
Required vendor information	
VE06.15.01	The vendor shall provide operating system documentation which provides a description of how the access control mechanisms of the operating system are configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to execute the stored cryptographic software.
Required test procedures	
TE06.15.01	The tester shall review the vendor-provided documentation and inspect the operating system control mechanisms to verify that the operating system is configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to execute the stored cryptographic software.
TE06.15.02	The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to execute the stored cryptographic software. The tester shall verify that they have exclusive rights to execute the stored cryptographic software.
TE06.15.03	The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to not give rights to execute the stored cryptographic software. The tester shall verify that they do not have rights to execute the stored cryptographic software.

Table 165 — VE and TE of AS06.16

Operating system requirements for modifiable operational environments — level 2	
AS06.16 ISO/IEC 19790:2025, 7.6.3.2	{To protect plaintext data, cryptographic software and SSPs, the access control mechanisms of the operating system} shall be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to modify (i.e. write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data;
Required vendor information	
VE06.16.01	The vendor shall provide operating system documentation which provides a description of how the access control mechanisms of the operating system are configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to modify (i.e. write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 165 *(continued)*

TE06.16.01	The tester shall review the vendor-provided documentation and inspect operating system control mechanisms, to verify that the operating system is configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to modify (i.e. write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.
TE06.16.02	The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to modify (i.e. write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data. The tester shall verify that they have exclusive rights to modify (i.e. write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.
TE06.16.03	The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to not give rights to modify (i.e. write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data. The tester shall verify that they do not have rights to modify (i.e. write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.

Table 166 — VE and TE of AS06.17

Operating system requirements for modifiable operational environments — level 2	
AS06.17 ISO/IEC 19790:2025, 7.6.3.2	{To protect plaintext data, cryptographic software and SSPs, the access control mechanisms of the operating system} shall be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to read cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data;
Required vendor information	
VE06.17.01	The vendor shall provide operating system documentation which provides a description of how the access control mechanisms of the operating system are configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to read cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.
Required test procedures	
TE06.17.01	The tester shall review the vendor-provided documentation and inspect operating system control mechanisms, to verify that the operating system is configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to read cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.
TE06.17.02	The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to read cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data. The tester shall verify that they have exclusive rights to read cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.
TE06.17.03	The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to not give rights to read cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data. The tester shall verify that they do not have rights to read cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 167 — VE and TE of AS06.18

Operating system requirements for modifiable operational environments — level 2	
AS06.18 ISO/IEC 19790:2025, 7.6.3.2	{To protect plaintext data, cryptographic software and SSPs, the access control mechanisms of the operating system} shall be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to enter SSPs.
Required vendor information	
VE06.18.01	The vendor shall provide operating system documentation which provides a description of how the access control mechanisms of the operating system are configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to enter SSPs.
Required test procedures	
TE06.18.01	The tester shall review the vendor-provided documentation and inspect operating system control mechanisms, to verify that the operating system is configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to enter SSPs.
TE06.18.02	The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to enter SSPs. The tester shall verify that they have exclusive rights to enter SSPs.
TE06.18.03	The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to not give rights to enter SSPs. The tester shall verify that they do not have rights to enter SSPs.

Table 168 — VE and TE of AS06.19

Operating system requirements for modifiable operational environments — level 2	
AS06.19 ISO/IEC 19790:2025, 7.6.3.2	The following specifications shall be consistent with the roles or designated groups' rights and services as defined in the security policy:
Required test procedures	
This assertion is tested as part of AS06.20, AS06.21, AS06.22 and AS06.23.	

Table 169 — VE and TE of AS06.20

Operating system requirements for modifiable operational environments — level 2	
AS06.20 ISO/IEC 19790:2025, 7.6.3.2	When not supporting a maintenance role, the operating system shall prevent all operators and running processes from modifying running cryptographic processes (i.e. loaded and executing cryptographic program images). In this case, running processes refer to all processes, cryptographic or not, not owned or initiated by the operating system (i.e. operator-initiated);
Required vendor information	
VE06.20.01	The vendor shall provide operating system documentation which provides a description of how the operating system prevents all operators and running processes from modifying running cryptographic processes (i.e. loaded and executing cryptographic program images) when not in maintenance role.
VE06.20.02	The specifications of how the operating system prevents all operators and running processes from modifying running cryptographic processes (i.e. loaded and executing cryptographic program images) when not in maintenance role shall be consistent with the roles or designated groups' rights and services as defined in the security policy.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 169 *(continued)*

TE06.20.01	The tester shall verify, from the vendor-provided documentation and by inspection of operating system control mechanisms, that the operating system is configured to prevent all operators and running processes from modifying running cryptographic processes (i.e. loaded and executing cryptographic program images) when not in maintenance role.
TE06.20.02	The tester shall verify that the roles or designated groups' rights and services as defined in the security policy are consistent with how the operating system is configured to prevent all operators and running processes from modifying running cryptographic processes (i.e. loaded and executing cryptographic program images) when not in maintenance role.
TE06.20.03	The tester shall configure the operating system control mechanisms to prevent all operators and running processes from modifying running cryptographic processes (i.e. loaded and executing cryptographic program images) when not in maintenance role. The tester shall assume an operator role and verify that they are prevented from modifying running cryptographic processes (i.e. loaded and executing cryptographic program images) when not in maintenance role. The tester shall verify that running processes are prevented from modifying running cryptographic processes (i.e. loaded and executing cryptographic program images) when not in maintenance role.

Table 170 — VE and TE of AS06.21

Operating system requirements for modifiable operational environments — level 2	
AS06.21 ISO/IEC 19790:2025, 7.6.3.2	The operating system shall prevent user processes from gaining either read or write access to SSPs owned by other processes and to system SSPs;
Required vendor information	
VE06.21.01	The vendor shall provide operating system documentation which provides a description of how the operating system prevents processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs.
VE06.21.02	The specifications of how the operating system prevents processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs shall be consistent with the roles or designated groups' rights and services as defined in the security policy.
Required test procedures	
TE06.21.01	The tester shall verify, from the vendor-provided documentation and by inspection of operating system control mechanisms, that the operating system is configured to prevent processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs.
TE06.21.02	The tester shall verify that the roles or designated groups' rights and services as defined in the security policy are consistent with how the operating system is configured to prevent processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs.
TE06.21.03	The tester shall configure the operating system control mechanisms to prevent processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs. The tester shall verify that running processes in user roles or user groups are prevented from gaining either read or write access to SSPs owned by other processes and to system SSPs.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 171 — VE and TE of AS06.22

Operating system requirements for modifiable operational environments — level 2	
AS06.22 ISO/IEC 19790:2025, 7.6.3.2	The configuration of the operating system that meets AS06.20 and AS06.21 shall be specified in the administrator guidance.
Required vendor information	
VE06.22.01	The vendor shall provide the administrator guidance documents which provide a description of how the operating system is configured to meet the requirements in AS06.13 to AS06.18.
Required test procedures	
TE06.22.01	The tester shall verify that the vendor-provided administrator guidance documents provide a description of how the operating system is configured to meet the requirements in AS06.13 to AS06.18.

Table 172 — VE and TE of AS06.23

Operating system requirements for modifiable operational environments — level 2	
AS06.23 ISO/IEC 19790:2025, 7.6.3.2	The administrator guidance shall state that the operating system be configured as specified for the module contents to be considered protected.
Required vendor information	
VE06.23.01	The vendor shall provide the administrator guidance documents which state that the operating system shall be configured as specified AS06.13 to AS06.18 for the module contents to be considered protected.
Required test procedures	
TE06.23.01	The tester shall verify that the vendor-provided administrator guidance documents state that the operating system shall be configured as specified AS06.13 to AS06.18 for the module contents to be considered protected.

Table 173 — VE and TE of AS06.24

Operating system requirements for modifiable operational environments — level 2	
AS06.24 ISO/IEC 19790:2025, 7.6.3.2	The identification and authentication mechanism to the operating system shall meet the requirements of ISO/IEC 19790:2025, 7.4.4 at security level 2, 3 or 4, and be specified in the module's security policy.
Required test procedures	
This assertion is tested as part of AS06.27, AS06.28, AS06.29, AS06.30, AS06.31, AS06.32 and AS06.33.	

Table 174 — VE and TE of AS06.25

Operating system requirements for modifiable operational environments — level 2	
AS06.25 ISO/IEC 19790:2025, 7.6.3.2	All cryptographic software, SSPs, control and status information shall be under the control of an operating system.
Required test procedures	
This assertion is tested as part of AS06.27, AS06.28, AS06.29, AS06.30, AS06.31, AS06.32 and AS06.33.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 175 — VE and TE of AS06.26

Operating system requirements for modifiable operational environments — level 2	
AS06.26 ISO/IEC 19790:2025, 7.6.3.2	The operating system shall have, at a minimum, the following attributes:
Required test procedures	
This assertion is tested as part of AS06.27, AS06.28, AS06.29, AS06.30, AS06.31, AS06.32 and AS06.33.	

Table 176 — VE and TE of AS06.27

Operating system requirements for modifiable operational environments — level 2	
AS06.27 ISO/IEC 19790:2025, 7.6.3.2	The operating system shall provide an audit mechanism with the date and time of each audited event.
Required vendor information	
VE06.27.01	The vendor shall provide operating system documentation which provides a description of the audit mechanism provided by the operating system and how each event is marked with the date and time.
Required test procedures	
TE06.27.01	The tester shall review the vendor-provided documentation and inspect operating system to verify that an audit mechanism is provided and that each event is marked with the date and time.

Table 177 — VE and TE of AS06.28

Operating system requirements for modifiable operational environments — level 2	
AS06.28 ISO/IEC 19790:2025, 7.6.3.2	The cryptographic module shall not include SSPs as part of any audit record;
Required vendor information	
VE06.28.01	The vendor shall provide operating system documentation which provides a description of the cryptographic module's services that provide audit records to the audit mechanism of the operating system.
Required test procedures	
TE06.28.01	The tester shall verify, from the vendor-provided documentation and by inspection of the cryptographic module's services that provide audit records to the audit mechanism of the operating system, that no SSPs are provided in the audit records.
TE06.28.02	The tester shall execute the module's services that provide audit records and examine the operating system audit logs to verify that no SSPs were provided.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 178 — VE and TE of AS06.29

Operating system requirements for modifiable operational environments — level 2	
AS06.29 ISO/IEC 19790:2025, 7.6.3.2	The cryptographic module shall provide the following events to be recorded by the audit mechanism of the operating system: a) modifications, accesses, deletions, and additions of cryptographic data and SSPs; b) addition or deletion of an operator to and from a crypto officer role (if those roles are managed by the cryptographic module); c) the use of a security-relevant crypto officer function; d) requests to access verifier data associated with the cryptographic module; e) the use of an authentication mechanism (e.g. login) associated with the cryptographic module; and f) explicit requests to assume a crypto officer role.
Required vendor information	
VE06.29.01	The vendor shall provide operating system documentation which provides a description of the cryptographic module events that are provided and recorded by the audit mechanism of the operating system.
VE06.29.02	The vendor shall provide documentation identifying any events required to meet the requirements in AS06.29 that are recorded by the cryptographic module and where these events are not separately also recorded by the operating system.
Required test procedures	
TE06.29.01	The tester shall review the vendor-provided documentation and inspect the cryptographic module's services that provide audit event records to the audit mechanism of the operating system or of the cryptographic module to verify that the list of events specified in AS06.29 are provided by the cryptographic module for event recording.
TE06.29.02	The tester shall execute the module's services that provide audit event records and examine the operating system or cryptographic module audit logs to verify that the events in AS06.29 were recorded. NOTE 1 The tester is not expected to test the audit mechanism provided by the operating system and identified by the vendor. NOTE 2 Audit events can be recorded and stored in parallel by both the operating system and cryptographic module. The intent of this TE06.29.02 is to confirm that either the operating system or cryptographic module report a given event, but not both.

Table 179 — VE and TE of AS06.30

Operating system requirements for modifiable operational environments — level 2	
AS06.30 ISO/IEC 19790:2025, 7.6.3.2	The cryptographic module may record some or all of the events specified in ISO/IEC 19790:2025, 7.6.3.2 e) with its own audit mechanism; regardless, all audit requirements in AS06.29 shall be recorded, either by the operating system, module or a combination of both.
Required test procedures	
This assertion is tested as part of AS06.29.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 180 — VE and TE of AS06.31

Operating system requirements for modifiable operational environments — level 2	
AS06.31 ISO/IEC 19790:2025, 7.6.3.2	The audit mechanism of the operating system shall be capable of auditing the following operating system related events: a) all operator read or write accesses to audit data stored in the audit trail; b) access to files used by the cryptographic module to store cryptographic data or SSPs; c) addition or deletion of an operator to and from a crypto officer role (if those roles are managed by operating system); d) requests to use verifier data management mechanisms (if verifier data associated with the cryptographic module is managed by the operating system); e) attempts to use the plaintext trusted path function and whether the request was granted, when plaintext trusted path is supported at this security level; and f) identification of the initiator and target of a plaintext trusted path, when the plaintext trusted path is supported at this security level.
Required vendor information	
VE06.31.01	The vendor shall provide operating system documentation which provides a description of the operating system events that are provided and recorded by the audit mechanism of the operating system.
Required test procedures	
TE06.31.01	The tester shall verify, from the vendor documentation and by inspection of the operating system documentation, that the operating system provides the list of events specified in AS06.31 as audit event records to the audit mechanism of the operating system.
TE06.31.02	The tester shall execute the cryptographic module's services to verify that the operating system events in AS06.31 were recorded. NOTE The tester is not expected to test the audit mechanism provided by the operating system and identified by the vendor.

Table 181 — VE and TE of AS06.32

Operating system requirements for modifiable operational environments — level 2	
AS06.32 ISO/IEC 19790:2025, 7.6.3.2	The operating system shall be configured to prevent operators other than those with the privileges identified in the security policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.
Required vendor information	
VE06.32.01	The vendor shall provide operating system documentation that specifies how the operating system is configured to prevent operators other than those with the privileges identified in the security policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.
Required test procedures	
TE06.32.01	The tester shall verify, from the vendor-provided documentation and by inspection of operating system configuration controls, that the operating system is configured to prevent operators other than those with the privileges identified in the security policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 181 *(continued)*

TE06.32.02	The tester shall configure the operating system controls to prevent operators other than those with the privileges identified in the security policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.
TE06.32.03	The tester shall assume the privileges identified in the security policy to allow modification of the cryptographic module software and audit data stored within the operational environment of the cryptographic module. And then the tester shall verify that modification can be achieved.
TE06.32.04	The tester shall assume the privileges identified in the security policy that do not allow modification of the cryptographic module software and audit data stored within the operational environment of the cryptographic module. The tester shall then verify that modification cannot be achieved.

Table 182 — VE and TE of AS06.33

Operating system requirements for modifiable operational environments — level 2	
AS06.33 ISO/IEC 19790:2025, 7.6.3.2	Only operating systems that are configured to meet requirements specified in ISO/IEC 19790:2025, 7.6.3.2 shall be permitted at security level 2.
Required test procedures	
This assertion is tested as part of AS06.07, AS06.08, AS06.09, AS06.10, AS06.11, AS06.12, AS06.13, AS06.14, AS06.15, AS06.16, AS06.17, AS06.18, AS06.19, AS06.20, AS06.21, AS06.22, AS06.23, AS06.24, AS06.25, AS06.26, AS06.27, AS06.28, AS06.29, AS06.30, AS06.31 and AS06.32.	

6.7 Physical security

6.7.1 Physical security embodiments

Table 183 — VE and TE of AS07.01

Physical security embodiments — levels 1, 2, 3 and 4	
AS07.01 ISO/IEC 19790:2025, 7.7.1	A cryptographic module shall employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module when installed.
Required vendor information	
VE07.01.01	The vendor-provided documentation shall describe the applicable physical security mechanisms that are employed by the module. The contents of the module, including all hardware, firmware, and data (including unprotected CSPs) shall be protected.
Required test procedures	
TE07.01.01	The tester shall verify that the vendor-provided documentation describes the applicable physical security mechanisms that are employed by the module.
TE07.01.02	The tester shall verify that the physical security mechanisms documented are implemented.

Table 184 — VE and TE of AS07.02

Physical security embodiments — levels 1, 2, 3 and 4	
AS07.02 ISO/IEC 19790:2025, 7.7.1	All hardware, firmware, data elements and SSPs within the cryptographic boundary shall be physically protected as specified for the target physical security level.
Required test procedures	
This assertion is not separately tested.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 185 — VE and TE of AS07.03

Physical security embodiments — levels 1, 2, 3 and 4	
AS07.03 ISO/IEC 19790:2025, 7.7.1	The requirements of ISO/IEC 19790:2025, 7.7 shall be applicable to hardware and firmware modules, and hardware and firmware components of hybrid modules.
Required test procedures	
This assertion is not separately tested.	

Table 186 — VE and TE of AS07.04

Physical security embodiments — levels 1, 2, 3 and 4	
AS07.04 ISO/IEC 19790:2025, 7.7.1	The documentation for physical security specified in ISO/IEC 19790:2025, A.2.6 shall be provided.
Required test procedures	
This assertion is tested as part of ASA.01.	

6.7.2 Physical security general requirements

6.7.2.1 Physical security general requirements for all security levels

Table 187 — VE and TE of AS07.05

Physical security general requirements — levels 1, 2, 3 and 4	
AS07.05 ISO/IEC 19790:2025, 7.7.2.1	The following requirements shall apply to all physical embodiments: {AS07.06 to AS07.37}
Required test procedures	
This assertion is tested as part of AS07.06, AS07.07, AS07.08, AS07.09, AS07.10, AS07.11, AS07.12, AS07.13, AS07.14, AS07.15, AS07.16, AS07.17, AS07.18, AS07.19, AS07.20, AS07.21, AS07.22, AS07.23, AS07.24, AS07.25, AS07.26, AS07.27, AS07.28, AS07.29, AS07.30, AS07.31, AS07.32 and AS07.33.	

Table 188 — VE and TE of AS07.06

Physical security general requirements — levels 1, 2, 3 and 4	
AS07.06 ISO/IEC 19790:2025, 7.7.2.1	documentation shall specify the physical embodiment of the cryptographic module;
Required vendor information	
VE07.06.01	The vendor documentation shall specify the physical embodiment of the module: single-chip cryptographic module or multiple-chip cryptographic module as defined in ISO/IEC 19790:2025, 7.7.1. The specified physical embodiment shall be consistent with the module physical design. The vendor-provided documentation shall also state which security level (1 to 4) the module is intended to meet.
Required test procedures	
TE07.06.01	The tester shall verify that the vendor identified that the cryptographic module is either a single-chip module or a multiple-chip cryptographic module as defined in ISO/IEC 19790:2025, 7.7.1. The tester shall perform an independent determination that the physical embodiment satisfies one of the two criteria specified below. The fundamental determining characteristics of the two physical embodiments and some common examples are summarized below.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 188 *(continued)*

	a) Single-chip cryptographic module. Characteristics: A single integrated circuit (IC) chip, used as a standalone device or physically embedded within some other module or enclosure that possibly has no physical protection. The single-chip will consist of one die that may be covered with a uniform external material such as plastic or ceramic, and external input/output connectors. EXAMPLE Single IC chips, smart cards with a single IC chip, or other systems with a single IC chip to implement cryptographic and security relevant functions. b) Multiple-chip cryptographic module. Characteristics: Two or more IC chips interconnected and physically embedded within some other product or enclosure that possibly has no physical protection or physically embeds in an enclosure that is entirely physically protected.
TE07.06.02	The tester shall verify that the vendor-provided documentation states which security level the module is intended to meet. The tester shall perform an independent determination of the security level that the module actually meets.

Table 189 — VE and TE of AS07.07

Physical security general requirements — levels 1, 2, 3 and 4	
AS07.07 ISO/IEC 19790: 2025, 7.7.2.1	Whenever zeroization is performed for physical security purposes, the zeroization shall occur in a sufficiently small time period so as to prevent the recovery of the zeroized SSP between the time of detection and the actual zeroization.
Required vendor information	
VE07.07.01	The vendor-provided documentation shall specify the response time of the zeroization after tamper detection.
Required test procedures	
TE07.07.01	The tester shall verify that the vendor documentation describes the zeroization response time after the tamper detection.
TE07.07.02	The tester shall verify that the zeroization response mechanism is implemented as specified.
TE07.07.03	The tester shall attempt to prevent the module from performing zeroization after a tamper is detected by the module. If the tester succeeds, the test shall fail.

Table 190 — VE and TE of AS07.08

Physical security general requirements — levels 1, 2, 3 and 4	
AS07.08 ISO/IEC 19790:2025, 7.7.2.1	{If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g. by the module vendor or other authorized individual), then} a maintenance interface shall be defined.
Required test procedures	
This assertion is tested as part of AS03.12.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 191 — VE and TE of AS07.09

Physical security general requirements — levels 1, 2, 3 and 4	
AS07.09 ISO/IEC 19790:2025, 7.7.2.1	{If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g. by the module vendor or other authorized individual), then}: the maintenance interface shall include all physical access paths to the contents of the cryptographic module, including any removable covers or doors.
Required vendor information	
VE07.09.01	The vendor-provided documentation shall specify the maintenance interface, including any removable covers or doors.
Required test procedures	
TE07.09.01	The tester shall verify in the vendor documentation that a maintenance interface is provided, including any removable covers or doors.

Table 192 — VE and TE of AS07.10

Physical security general requirements — levels 1, 2, 3 and 4	
AS07.10 ISO/IEC 19790:2025, 7.7.2.1	{If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g. by the module vendor or other authorized individual), then}: any removable covers or doors included within the maintenance interface shall be safeguarded using the appropriate physical security mechanisms.
Required vendor information	
VE07.10.01	The vendor-provided documentation shall specify a physical protection such that any removable covers or doors included within the maintenance interface are safeguarded using the appropriate physical security mechanisms.
Required test procedures	
TE07.10.01	The tester shall verify that any removable covers or doors included within the maintenance interface are safeguarded using the appropriate physical security mechanisms.

6.7.2.2 Security level 1

Table 193 — VE and TE of AS07.11

Physical security general requirements — levels 1, 2, 3 and 4	
AS07.11 ISO/IEC 19790:2025, 7.7.2.2	The following requirements shall apply to all cryptographic modules for security level 1:{AS07.12 to AS07.13}
Required test procedures	
This assertion is tested as part of AS07.12 and AS07.13.	

Table 194 — VE and TE of AS07.12

Physical security general requirements — levels 1, 2, 3 and 4	
AS07.12 ISO/IEC 19790: 2025, 7.7.2.2	The cryptographic module shall consist of production-grade elements that include standard passivation techniques (e.g. a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or other physical damage).
Required vendor information	
VE07.12.01	The vendor-provided documentation shall provide evidence of the use of production-grade products or elements including evidence as to how these items have been tested to meet operational specifications .
VE07.12.02	The vendor-provided documentation shall cover the passivation techniques used during production of the module.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 194 *(continued)*

Required test procedures	
TE07.12.01	The tester shall review the vendor-provided documentation to verify that the module contains products or elements that have been designed to meet operational specifications.
TE07.12.02	The tester shall review the vendor-provided documentation to verify that a standard passivation has been applied to the module. The passivation shall be a sealing coat applied over the chip circuitry to protect it against environmental or other physical damage. If standard passivation is not used, then the documentation shall provide information to indicate why it is equivalent to a standard passivation approach.

Table 195 — VE and TE of AS07.13

Physical security general requirements — levels 1, 2, 3 and 4	
AS07.13 ISO/IEC 19790: 2025, 7.7.2.2	When performing physical maintenance, zeroization shall be performed either automatically by the cryptographic module or initiated by the operator.
Required vendor information	
VE07.13.01	If the module supports a maintenance role, the vendor-provided documentation shall identify whether zeroization is performed automatically by the module or is be initiated by the operator.
VE07.13.02	If CSPs, PSPs, and plaintext key components are zeroized procedurally while under the control of the operator (i.e. they are present to observe the method has completed successfully or controlled via a remote management session), vendor-provided documentation and the module security policy shall specify how the methods shall be performed.
VE07.13.03	If CSPs, PSPs, and plaintext key components are zeroized automatically upon assumption of the maintenance role, the vendor-provided documentation shall specify how the zeroization method(s) are employed such that plaintext CSPs, PSPs, and plaintext key components within the module cannot be obtained by an attacker.
Required test procedures	
TE07.13.01	The tester shall verify that the vendor-provided documentation identifies whether zeroization is performed automatically by the module or is initiated by the operator.
TE07.13.02	If procedural zeroization methods are used, the tester shall verify that the vendor-provided documentation, including the security policy, specifies that the procedure shall be performed under the control of the operator.
TE07.13.03	If the zeroization is initiated by the operator, the tester shall verify that vendor-provided documentation and the security policy specify the procedure for zeroization.
TE07.13.04	If zeroization is automatic, the tester shall verify which CSPs, PSPs, and plaintext key components are present in the module and assume the maintenance role. The tester shall then attempt to perform cryptographic operations using each of the plaintext CSPs, PSPs, and plaintext key components that were stored in the module. The tester shall verify that each unprotected SSP cannot be accessed.
TE07.13.05	The tester shall verify that all plaintext CSPs, PSPs, and plaintext key components that are not zeroized by the zeroize 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: 2025).

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.7.2.3 Security level 2

Table 196 — VE and TE of AS07.14

Physical security general requirements — levels 2, 3 and 4	
AS07.14 ISO/IEC 19790: 2025, 7.7.2.2	In addition to the general requirements for security level 1, the following requirements shall apply to all cryptographic modules for security level 2: {AS07.15 to AS07.20}
Required test procedures	
This assertion is tested as part of AS07.15, AS07.16, AS07.17, AS07.18, AS07.19 and AS07.20.	

Table 197 — VE and TE of AS07.15

Physical security general requirements — levels 2, 3 and 4	
AS07.15 ISO/IEC 19790: 2025, 7.7.2.3	The cryptographic module shall either be: a) entirely coated in a tamper evident material (excluding the protected internal paths); or b) include an enclosure that may include doors or removable covers (excluding the protected internal paths). EXAMPLE 1 Suitable coatings include epoxy resin and hard plastics. EXAMPLE 2 Suitable container materials include metals and hard plastics.
Required vendor information	
VE07.15.01	The vendor-provided documentation shall identify that the module is entirely coated in a tamper evident material (excluding the protected internal paths) or that the module is enclosed in a container that can include doors or removable covers (excluding the protected internal paths).
Required test procedures	
TE07.15.01	The tester shall inspect the module and review the vendor-provided documentation to verify that the module is either entirely coated in a tamper evident material (excluding the protected internal paths) or that the module is enclosed in a container that can include doors or removable covers (excluding the protected internal paths). The following requirements shall be met: a) The enclosure or coating shall completely surround the entire module (excluding the protected internal paths). b) The enclosure or coating material shall be of a composition defined in the vendor-provided documentation. c) The enclosure shall be production-grade. The vendor literature shall either show that an enclosure of the same material has been used commercially or provide data to show that it is equivalent to a commercial product.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 198 — VE and TE of AS07.16

Physical security general requirements — levels 2, 3 and 4	
AS07.16 ISO/IEC 19790: 2025, 7.7.2.3	If the module is in an enclosure containing doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys
Required vendor information	
VE07.16.01	The doors or covers included by the enclosure shall be locked with pick-resistant mechanical locks that employ physical or logical keys. The vendor-provided documentation shall describe the locks and the employed physical or logical keys.
Required test procedures	
TE07.16.01	The tester shall review the vendor-provided documentation and inspect the module to verify that doors or covers are locked with a pick-resistant lock that requires a physical key or a logical key.
TE07.16.02	The tester shall attempt to open the locked cover or door without use of the key and verify that the cover or door will not open without signs of damage.

Table 199 — VE and TE of AS07.17

Physical security general requirements — levels 2, 3 and 4	
AS07.17 ISO/IEC 19790: 2025, 7.7.2.3	{If the module is in an enclosure containing doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys} or shall be protected with tamper-evident seals (e.g. evidence tape or holographic seals).
Required vendor information	
VE07.17.01	The vendor-provided documentation shall describe the tamper-evident seals.
Required test procedures	
TE07.17.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the cover or door is protected with a tamper-evident seal such as evidence tape or a holographic seal.
TE07.17.02	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.

Table 200 — VE and TE of AS07.18

Physical security general requirements — levels 2, 3 and 4	
AS07.18 ISO/IEC 19790: 2025, 7.7.2.3	The cryptographic module shall provide tamper evidence (e.g. on the cover, enclosure, coating, package, or seal) to provide detectable evidence of attempts to modify or access the module.
Required vendor information	
VE07.18.01	The vendor-provided documentation shall identify the tamper-evident design of the module including all relevant characteristics required to ensure tamper evidence.
Required test procedures	
TE07.18.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the module includes tamper evidence. The inspection shall verify that the tamper-evident design will result in evidence being left from all attempts to modify, directly probe or manipulate the internals of the module.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 201 — VE and TE of AS07.19

Physical security general requirements — levels 2, 3 and 4	
AS07.19 ISO/IEC 19790: 2025, 7.7.2.3	The tamper-evident material, coating, enclosure or package shall either be opaque or translucent within the visible spectrum (i.e. light of wavelength range of 400 nm to 750 nm) to prevent the gathering of information about the internal operations of the critical areas of the module.
Required vendor information	
VE07.19.01	The vendor-provided documentation shall specify that the tamper evident material, coating, or enclosure is opaque or translucent within the visible spectrum.
Required test procedures	
TE07.19.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the tamper evident material, coating, or enclosure is opaque or translucent within the visible spectrum.
TE07.19.02	The tester shall illuminate the module within the entire range of the visible spectrum to verify that the tamper-evident material is opaque or translucent.

Table 202 — VE and TE of AS07.20

Physical security general requirements — levels 2, 3 and 4	
AS07.20 ISO/IEC 19790: 2025, 7.7.2.3	If the cryptographic module contains ventilation holes or slits, then the module shall be constructed in a manner to prevent the gathering of information of the module's internal construction or elements by direct visual observation using artificial light sources in the visual spectrum of the module's internal construction or elements.
Required vendor information	
VE07.20.01	If the module is contained within a cover or enclosure that contains any ventilation holes or slits, then they shall be constructed in a manner that prevents the gathering of information of the module's internal construction or elements by direct visual observation using artificial light sources in the visual spectrum of the module's internal construction or elements. The vendor-provided documentation shall describe the physical design approach that prevents such observation.
Required test procedures	
TE07.20.01	The tester shall review the vendor-provided documentation and inspect the module to verify whether the module has a cover or enclosure with ventilation holes, slits, or other openings, and if so, whether they are constructed to deter the gathering of information of the module's internal construction or elements by direct visual observation using artificial light sources in the visual spectrum of the module's internal construction or elements.

6.7.2.4 Security level 3

Table 203 — VE and TE of AS07.21

Physical security general requirements — levels 3 and 4	
AS07.21 ISO/IEC 19790: 2025, 7.7.2.4	In addition to the general requirements for security levels 1 and 2, the following requirements shall apply to all cryptographic modules for security level 3: {AS07.22 to AS07.30}.
Required test procedures	
This assertion is tested as part of AS07.22, AS07.23, AS07.24, AS07.25, AS07.26, AS07.27, AS07.28, AS07.29 and AS07.30.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 204 — VE and TE of AS07.22

Physical security general requirements — levels 3 and 4	
AS07.22 ISO/IEC 19790: 2025, 7.7.2.4	The module shall be covered (excluding the protected internal paths) with a hard, opaque tamper-evident coating, enclosure or package {to ensure that attempts at physical removal or penetration of the coating using non-chemical methods shall have a high probability of causing serious damage to the cryptographic module}
Required vendor information	
VE07.22.01	The vendor-provided documentation shall identify the hard, opaque tamper-evident coating, enclosure or package that is utilized
VE07.22.02	The vendor-provided documentation shall provide supporting design information for the module when covered with a hard, opaque tamper-evident coating, enclosure or package. The material shall be opaque within the visible spectrum.
Required test procedures	
TE07.22.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the module is covered with a hard, opaque tamper-evident coating enclosure or package.
TE07.22.02	The tester shall review the vendor-provided documentation and inspect the module to verify that the hard coating or potting material cannot be removed or penetrated without having a high probability of causing serious damage to the module. The tester shall verify the removal resistant properties of the module coating, enclosure or package. The tester shall attempt to peel or pry the material from the module and verify that this is not possible with a reasonable application of force so that the module ceased to function or that the module circuitry was obviously physically destroyed.

Table 205 — VE and TE of AS07.23

Physical security general requirements — levels 3 and 4	
AS07.23 ISO/IEC 19790: 2025, 7.7.2.4	{The module shall be covered (excluding the protected internal paths) with a hard, opaque tamper-evident coating, enclosure or package} to ensure that attempts at physical removal or penetration of the coating using non-chemical methods shall have a high probability of causing serious damage to the cryptographic module.
Required test procedures	
This assertion is tested as part of AS07.22.	

Table 206 — VE and TE of AS07.24

Physical security general requirements — levels 3 and 4	
AS07.24 ISO/IEC 19790: 2025, 7.7.2.4	If the cryptographic module contains any doors or removable covers or if a maintenance access interface is defined, then the module shall contain tamper response and zeroization capability.
Required test procedures	
This assertion is tested as part of AS07.25.	

Table 207 — VE and TE of AS07.25

Physical security general requirements — levels 3 and 4	
AS07.25 ISO/IEC 19790: 2025, 7.7.2.4	Any tamper response and zeroization capability shall immediately zeroize all plaintext CSPs, plaintext PSPs and plaintext key components when a tamper event is detected (e.g. a door is opened, a cover is removed, an internal tamper sensor is triggered such as a breach of a tamper detection envelope, or when the maintenance interface is accessed).
Required vendor information	
VE07.25.01	The vendor-provided documentation shall provide supporting design documentation for the module enclosure, tamper sensors or maintenance interface, if defined.
VE07.25.02	The vendor-provided documentation shall identify any doors or removable covers or maintenance interface and shall document the module's tamper response and zeroization circuitry.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 207 *(continued)*

VE07.25.03	The vendor-provided documentation shall identify any tamper detection sensors (e.g. tamper detection envelope) and shall document the module's tamper response and zeroization circuitry linked to these sensors.
Required test procedures	
TE07.25.01	The tester shall verify that the vendor-provided documentation specifies: a) all doors, removable covers and whether a maintenance interface is specified; b) the tamper response and zeroization circuitry linked to removable doors, removable covers and maintenance interface; c) all tamper sensors needed to meet the applicable requirements of ISO/IEC 19790: 2025, 7.7; and d) the tamper response and zeroization circuitry linked to all tamper sensors needed to meet applicable requirements of ISO/IEC 19790: 2025, 7.7.
TE07.25.02	If the module supports tamper detection and response, then the tester shall review the vendor-provided documentation to verify that the module zeroizes all plaintext CSPs, plaintext PSPs and plaintext key components.
TE07.25.03	The tester shall review the vendor-provided documentation and inspect the module to verify that the tamper response and zeroization circuitry, if supported, remains operational when plaintext CSPs, plaintext PSPs and plaintext key components are contained within the module.
TE07.25.04	If the module supports tamper detection and response, the tester shall test that the module zeroizes all plaintext CSPs, plaintext PSPs and plaintext key components when a cover or door is removed or if the maintenance interface is accessed.

Table 208 — VE and TE of AS07.26

Physical security general requirements — levels 3 and 4	
AS07.26 ISO/IEC 19790: 2025, 7.7.2.4	If a module supports a tamper response and zeroization capability, the tamper response and zeroization capability shall remain operational while plaintext CSPs, plaintext PSPs and plaintext key components are contained within the cryptographic module.
Required test procedures	
This assertion is tested as part of AS07.25.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 209 — VE and TE of AS07.27

Physical security general requirements — levels 3 and 4	
AS07.27 ISO/IEC 19790: 2025, 7.7.2.4	Zeroization triggered by the detection of a tamper event shall be performed by the module without external module power and before the internal module power is insufficient for the module's zeroization circuitry to function;
Required vendor information	
VE07.27.01	If the module contains a tamper response and zeroization capability, the vendor-provided documentation shall document how the zeroization can be completed following detection of a tamper event without external module power and before the internal module power is insufficient for the module's zeroization circuitry to function.
Required test procedures	
TE07.27.01	The tester shall verify that the vendor-provided documentation provides a justification for how the modules tamper response and zeroization design is able to satisfy AS07.27.
TE07.27.02	The tester shall disconnect all external power and breach the tamper detection envelope barrier and then verify that the module zeroizes all plaintext CSPs and plaintext operator PSPs. Based on the vendor presented justification, the tester shall perform tests in order to confirm AS07.27 is met. This shall be performed based on a combination of inspection of the module to confirm the modules design and subsequent test. NOTE In cases where the module does not store any plaintext CSP or plaintext operator PSPs in its power-off state, AS07.27 is implicitly met and no further testing is required.

Table 210 — VE and TE of AS07.28

Physical security general requirements — levels 3 and 4	
AS07.28 ISO/IEC 19790: 2025, 7.7.2.4	If the cryptographic module contains ventilation holes or slits, then the module shall be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g. prevent probing by a single articulated probe).
Required vendor information	
VE07.28.01	If the module is contained within a cover or enclosure that contains any ventilation holes or slits, then they shall be constructed in a manner that prevents undetected physical probing inside the enclosure. The vendor-provided documentation shall describe the ventilation physical design approach.
Required test procedures	
TE07.28.01	The tester shall review the vendor documentation and inspect the module to verify whether the module has a cover or enclosure with ventilation holes, slits, or other openings, and if so, whether they are constructed to deter undetected probing inside the cover or enclosure.

Table 211 — VE and TE of AS07.29

Physical security general requirements — levels 3 and 4	
AS07.29 ISO/IEC 19790: 2025, 7.7.2.4	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	
VE07.29.01	The vendor documentation shall describe the strength or hardness of the hard conformal or non-conformal enclosure, coatings or potting materials, and shall provide the rationale justifying that the strength or hardness is appropriate for the module design.
VE07.29.02	The vendor-provided security policy shall specify the highest and lowest temperatures within the temperature range.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 211 *(continued)*

TE07.29.01	The tester shall verify from the vendor-provided documentation and testing of the module that the strength or hardness of the hard conformal or non-conformal enclosure, coatings, or potting materials is implemented as specified. The tester shall verify the module hardness at the following temperatures: a) the lowest temperature of the module's intended temperature range of operation, storage and distribution; b) the highest temperature of the module's intended temperature range of operation, storage and distribution.
TE07.29.02	The tester shall verify that the vendor-provided security policy specifies the high and low temperature range.

Table 212 — VE and TE of AS07.30

Physical security general requirements — levels 3 and 4	
AS07.30 ISO/IEC 19790: 2025, 7.7.2.4	If tamper evident seals are employed, they shall be uniquely numbered or independently identifiable (e.g. uniquely numbered evidence tape or uniquely identifiable holographic seals).
Required vendor information	
VE07.30.01	The vendor shall provide the specification of the tamper evident seal.
Required test procedures	
TE07.30.01	The tester shall verify that tamper evident seals are uniquely numbered or independently identifiable as documented.

6.7.2.5 Security level 4

Table 213 — VE and TE of AS07.31

Physical security general requirements — level 4	
AS07.31 ISO/IEC 19790: 2025, 7.7.2.5	In addition to the general requirements for security levels 1, 2, and 3, the following requirement shall apply to all cryptographic modules for security level 4: {AS07.32 and AS07.33}.
Required test procedures	
This assertion is tested as part of AS07.32 and AS07.33.	

Table 214 — VE and TE of AS07.32

Physical security general requirements — level 4	
AS07.32 ISO/IEC 19790: 2025, 7.7.2.5	The cryptographic module shall provide protection from fault injection.
Required vendor information	
VE07.32.01	The vendor-provided documentation shall specify the protection mechanism from fault injection.
Required test procedures	
TE07.32.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the fault injection protection mechanisms are specified.
TE07.32.02	The tester shall inject faults at the module boundary including interfaces and determine that the module's security relevant functionality is not compromised.
NOTE Fault injection can be electrical, optical, or mechanical in nature.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 215 — VE and TE of AS07.33

Physical security general requirements — level 4	
AS07.33 ISO/IEC 19790: 2025, 7.7.2.5	The fault injection mitigation techniques and the mitigation metrics employed shall be documented as specified in ISO/IEC 19790: 2025, Annex B.
Required vendor information	
VE07.33.01	The vendor-provided documentation shall specify the fault injection mitigation techniques and the mitigation metrics employed by the module.
Required test procedures	
TE07.33.01	The tester shall verify that the fault injection mitigation techniques and the mitigation metrics employed by the module are documented as specified.

6.7.3 Physical security requirements for each physical security embodiment

6.7.3.1 Single-chip cryptographic modules

Table 216 — VE and TE of AS07.34

Physical security requirements for each physical security embodiment — level 4	
AS07.34 ISO/IEC 19790: 2025, 7.7.3.1	In addition to the general physical security requirements for security levels 1, 2, 3 and 4, the following requirements shall apply to single-chip cryptographic modules for security level 4.
Required vendor information	
VE07.34.01	The vendor-provided documentation shall specify that either (AS07.35) or (AS07.36 to AS07.37) are satisfied.
Required test procedures	
TE07.34.01	The tester shall verify that the vendor-provided documentation includes a statement as to what option has been taken to meet the level 4 requirements for single-chip cryptographic modules.

Table 217 — VE and TE of AS07.35

Physical security requirements for each physical security embodiment — level 4	
AS07.35 ISO/IEC 19790: 2025, 7.7.3.1	The removal-resistant coating or strong enclosure shall have solvency characteristics such that dissolving the coating or strong enclosure has a high probability of seriously damaging the module (i.e. the module will not function and be irreparably damaged); or {AS07.36 to AS07.37}.
Required vendor information	
VE07.35.01	The vendor-provided documentation shall describe the solvency characteristics of the removal-resistant coating. The solvency characteristics of the material shall be such that dissolving the material to remove it will have a high probability of dissolving or seriously damaging the module.
Required test procedures	
TE07.35.01	The tester shall verify the vendor-provided documentation to determine the solvency properties of the module's removal-resistant coating.
TE07.35.02	The tester shall test the solvency properties of the module's removal-resistant coating. The tester, based on documentation provided in VE07.35.01, shall verify what type of solvent would be required to compromise the removal-resistant coating.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 218 — VE and TE of AS07.36

Physical security requirements for each physical security embodiment — level 4	
AS07.36 ISO/IEC 19790: 2025, 7.7.3.1	{The removal-resistant coating or strong enclosure shall have solvency characteristics such that dissolving the coating or strong enclosure has a high probability of seriously damaging the module (i.e. the module will not function and be irreparably damaged);} or the module shall provide a tamper detection envelope with tamper detection circuitry that {shall detect tampering by means such as cutting, drilling, milling, grinding, burning, melting, or dissolving of the single-chip module coating or package to a sufficient extent that would allow access to or modification of SSPs, or would result in unauthorized use or modification of the module.}
Required vendor information	
VE07.36.01	The enclosure or potting material shall be encapsulated by a tamper detection envelope with tamper detection circuitry by the use of tamper detection mechanisms. The vendor-provided documentation shall describe the tamper detection envelope or tamper detection circuitry design.
Required test procedures	
TE07.36.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the module enclosure or potting material contains tamper detection mechanisms. This shall form a tamper detection envelope with tamper detection circuitry that protects the module elements. The mechanisms shall be designed such that any breach of the enclosure or potting material to access the module elements can be detected.

Table 219 — VE and TE of AS07.37

Physical security requirements for each physical security embodiment — level 4	
AS07.37 ISO/IEC 19790: 2025, 7.7.3.1	{The removal-resistant coating or strong enclosure shall have solvency characteristics such that dissolving the coating or strong enclosure has a high probability of seriously damaging the module (i.e. the module will not function and be irreparably damaged);} or {the module shall provide a tamper detection envelope with tamper detection circuitry} shall detect tampering by means such as cutting, drilling, milling, grinding, burning, melting, or dissolving of the single-chip module coating or package to a sufficient extent that would allow access to or modification of SSPs, or would result in unauthorized use or modification of the module.
Required vendor information	
VE07.37.01	The vendor-provided documentation shall describe the tamper detection design.
Required test procedures	
TE07.37.01	The tester shall verify from the vendor-provided documentation that the module contains tamper detection circuitry that continuously monitors the tamper detection envelope; detects any breach by means such as drilling, milling, grinding, or dissolving any portion of the envelope; and then zeroizes all plaintext CSPs, plaintext PSPs and plaintext key components.
TE07.37.02	The tester shall breach the tamper detection envelope using attacks relevant to its design and verify that the module detects the intrusion attempt and zeroizes all plaintext CSPs and plaintext operator PSPs.

6.7.3.2 Multiple-chip cryptographic modules

Table 220 — VE and TE of AS07.38

Physical security requirements for each physical security embodiment — level 4	
AS07.38 ISO/IEC 19790: 2025, 7.7.3.2	In addition to the general physical security requirements for security levels 1, 2, 3 and 4 specified in ISO/IEC 19790:2025, 7.7.2, the following requirements shall apply to multiple-chip cryptographic modules for security level 4:
Required test procedures	
This assertion is tested as part of AS07.39, AS07.40, AS07.41, AS07.42, AS07.43, AS07.44 and AS07.45.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 221 — VE and TE of AS07.39

Physical security requirements for each physical security embodiment — level 4	
AS07.39 ISO/IEC 19790: 2025, 7.7.3.2	All inter component interfaces carrying security relevant data and controls shall be either a protected internal path, or be fully enclosed in a tamper detection envelope with tamper detection circuitry.
Required vendor information	
VE07.39.01	The vendor documentation shall specify how all inter component interfaces carrying security relevant data and controls are either a protected internal path, or are fully enclosed in a tamper detection envelope with tamper detection circuitry.
Required test procedures	
TE07.39.01	The tester shall verify that the vendor documentation specifies how all inter component interfaces carrying security relevant data and controls are either a protected internal path, or are fully enclosed in a tamper detection envelope with tamper detection circuitry.
TE07.39.02	The tester shall verify by inspection of the module that all inter component interfaces are either a protected internal path, or are fully enclosed in a tamper detection envelope with tamper detection circuitry.

Table 222 — VE and TE of AS07.40

Physical security requirements for each physical security embodiment — level 4	
AS07.40 ISO/IEC 19790:2025, 7.7.3.1	All components shall either be covered with a hard, opaque removal-resistant coating, strong enclosure, or be fully enclosed in a tamper detection envelope.
Required vendor information	
VE07.40.01	The vendor-provided documentation shall describe how all components are either covered with a hard, opaque removal-resistant coating, strong enclosure, or are fully enclosed in a tamper detection envelope.
Required test procedures	
TE07.40.01	The tester shall review the vendor-provided documentation and verify that it describes how all components are either covered with a hard, opaque removal-resistant coating, strong enclosure, or are fully enclosed in a tamper detection envelope.
TE07.40.02	The tester shall inspect the module to verify that all components are either covered with a hard, opaque removal-resistant coating, strong enclosure, or are fully enclosed in a tamper detection envelope.

Table 223 — VE and TE of AS07.41

Physical security requirements for each physical security embodiment — level 4	
AS07.41 ISO/IEC 19790:2025, 7.7.3.2	Where a tamper detection envelope is used, it shall detect tampering by means such as cutting, drilling, milling, grinding, burning, melting, or dissolving of the module's enclosure to a sufficient extent that would allow access to or modification of SSPs, or would result in unauthorized use or modification of the module.
Required test procedures	
This assertion is tested as part of AS07.45.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 224 — VE and TE of AS07.42

Physical security requirements for each physical security embodiment — level 4	
AS07.42 ISO/IEC 19790:2025, 7.7.3.2	Where a hard opaque removal-resistant coating or strong enclosure is used, the material shall have hardness and adhesion characteristics such that attempting to peel or pry the coating or strong enclosure from the module will have a high probability of resulting in serious damage to the module (i.e. the module will not function and be irreparably damaged).
Required vendor information	
VE07.42.01	The vendor-provided documentation shall detail the hardness and adhesion characteristics such that attempting to peel or pry the coating or strong enclosure from the module will have a high probability of resulting in serious damage to the module.
Required test procedures	
TE07.42.01	The tester shall verify that the vendor-provided documentation detail the hardness and adhesion characteristics such that attempting to peel or pry the coating or strong enclosure from the module will have a high probability of resulting in serious damage to the module.
TE07.42.02	The tester shall verify the removal resistant properties of the module coating or strong enclosure. The tester shall attempt to peel or pry the material from the module and verify that this is not possible with a reasonable application of force so that the module ceased to function or that the module circuitry was obviously physically destroyed.

Table 225 — VE and TE of AS07.43

Physical security requirements for each physical security embodiment — level 4	
AS07.43 ISO/IEC 19790:2025, 7.7.3.2	Where a hard opaque removal-resistant coating or strong enclosure is used, the material shall have solvency characteristics such that dissolving the coating or strong enclosure will have a high probability of dissolving or seriously damaging the module (i.e. the module will not function and be irreparably damaged).
Required vendor information	
VE07.43.01	The vendor-provided documentation shall identify the hard, opaque removal-resistant coating or strong enclosure used. Documentation shall describe how the coating or strong enclosure has solvency characteristics such that dissolving the coating or strong enclosure will have a high probability of dissolving or seriously damaging the module (i.e. the module will not function and be irreparably damaged).
Required test procedures	
TE07.43.01	The tester shall verify by inspection and from the vendor-provided documentation that the module is covered with a hard, opaque removal-resistant coating or strong enclosure.
TE07.43.02	The tester shall verify by test that the removal-resistant coating or strong enclosure is either: a) resistant to common chemicals that would reasonably be expected to attack the structure of the coating or enclosure; or b) is seriously damaged by the chemical attack (i.e. the module will not function and be irreparably damaged).

Table 226 — VE and TE of AS07.44

Physical security requirements for each physical security embodiment — level 4	
AS07.44 ISO/IEC 19790:2025, 7.7.3.2	Where a tamper detection envelope is used, the cryptographic module shall contain tamper response and zeroization capability that continuously monitor the tamper detection envelope.
Required test procedures	
This assertion is tested as part of AS07.45.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 227 — VE and TE of AS07.45

Physical security requirements for each physical security embodiment — level 4	
AS07.45 ISO/IEC 19790:2025, 7.7.3.2	Where a tamper detection envelope is used, the cryptographic module on detection of tampering, shall immediately zeroize all plaintext CSPs, plaintext PSPs and plaintext key components.
Required vendor information	
VE07.45.01	The vendor documentation shall describe if any tamper detection envelope is used. If used, it shall then describe: a) how it detects tampering by means such as cutting, drilling, milling, grinding, burning, melting, or dissolving of the module's enclosure to a sufficient extent that would allow access to or modification of SSPs, or would result in unauthorized use or modification of the module; b) how the tamper response and zeroization capability continuously monitor the tamper detection envelope; and c) how the cryptographic module on detection of tampering, immediately zeroizes all plaintext CSPs, plaintext PSPs and plaintext key components.
Required test procedures	
TE07.45.01	The tester shall review the vendor-provided documentation and verify that it describes if any tamper detection envelope is used. If used, the tester shall review and confirm that the document describes: a) how it detects tampering by means such as cutting, drilling, milling, grinding, burning, melting, or dissolving of the module's enclosure to a sufficient extent that would allow access to or modification of SSPs, or would result in unauthorized use or modification of the module; b) how the tamper response and zeroization capability continuously monitor the tamper detection envelope; and c) how the cryptographic module on detection of tampering, immediately zeroizes all plaintext CSPs, plaintext PSPs and plaintext key components.
TE07.45.02	The tester shall review by inspection that the implementation of the module matches the tamper detection envelope design documented.
TE07.45.03	For each attack path (cutting, drilling, milling, grinding, burning, melting, or dissolving of the module's enclosure), the tester shall attempt to defeat the design of the modules tamper detection envelope and confirm that in each instance: a) the tamper detection envelope detects attempts to access or remove the tamper detection envelope; and b) following detection of tampering, the module immediately zeroizes all plaintext CSPs, plaintext PSPs and plaintext key components. NOTE It is possible to use a single test to verify protection against multiple attack paths where this can be justified based on the design of the tamper envelope. EXAMPLE In some designs, a single test focused on attacks using drilling can be sufficient to also test resistance to cutting and milling.
TE07.45.04	The tester shall review the implementation of the tamper detection mechanisms to confirm that they provide continuous monitor the tamper detection envelope sufficient to detect any access to or modification of SSPs, as would result in unauthorized use or modification of the module. In practice, a module can periodically poll sensors used to detect tampering. Where this is implemented, the test shall confirm that this is done on a frequency sufficient to avoid an attacker being able to breach the tamper detection envelope and disable the tamper response mechanisms ahead of plaintext CSPs, plaintext PSPs and plaintext key components being accessed.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.7.4 Environmental failure protection/testing

6.7.4.1 Security level 3

NOTE 1 A cryptographic module is not expected to employ environmental failure protection features or undergo environmental failure testing for security levels 1 and 2.

Table 228 — VE and TE of AS07.46

Environmental failure protection/testing — level 3	
AS07.46 ISO/IEC 19790:2025, 7.7.4.3	The module shall either employ EFP features or undergo EFT.
Required test procedures	
This assertion is tested as part of AS07.48, AS07.49, AS07.50, AS07.51, AS07.52, AS07.53, AS07.54, AS07.56, AS07.57, AS07.58, AS07.59 and AS07.60.	

6.7.4.2 Security level 4

Table 229 — VE and TE of AS07.47

Environmental failure protection/testing — level 4	
AS07.47 ISO/IEC 19790:2025, 7.7.4.4	The module shall employ EFP features.
Required test procedures	
This assertion is tested as part of AS07.48, AS07.49 and AS07.50.	

6.7.5 Environmental failure protection features

Table 230 — VE and TE of AS07.48

Environmental failure protection features — levels 3 and 4	
AS07.48 ISO/IEC 19790:2025, 7.7.5	EFP features shall protect a cryptographic module against unusual environmental conditions (accidental or induced) when outside of the module's normal operating range, that can compromise the security of the cryptographic module.
Required test procedures	
This assertion is tested as part of AS07.50.	

Table 231 — VE and TE of AS07.49

Environmental failure protection features — levels 3 and 4	
AS07.49 ISO/IEC 19790:2025, 7.7.5	The cryptographic module shall monitor and correctly respond when operating temperature and voltage are outside of the specified normal operating ranges.
Required test procedures	
This assertion is tested as part of AS07.50.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 232 — VE and TE of AS07.50

Environmental failure protection features — levels 3 and 4	
AS07.50 ISO/IEC 19790:2025, 7.7.5	If the temperature or voltage falls outside of the cryptographic module's normal operating range, the protection capability shall either: a) shutdown the module to prevent further operation; or b) immediately zeroize all plaintext CSPs, plaintext PSPs and plaintext key components.
Required vendor information	
VE07.50.01	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) zeroize all plaintext CSPs, plaintext PSPs and plaintext key components Documentation shall state which of these approaches was chosen and provide a specification description of the EFP features implemented within the module.
VE07.50.02	The security policy shall address whether the employed EFP feature forces module shutdown or zeroizes all plaintext CSPs, plaintext PSPs and plaintext key components and shall specify the temperature range met.
Required test procedures	
TE07.50.01	The tester shall configure the environmental condition (ambient temperature and voltage) close to the appropriate extreme of the normal operating range specified for the module and verify that the module continues to perform within normal operating parameters.
TE07.50.02	The tester shall extend the temperature and voltage outside of the specified normal range and verify that the module either shuts down to prevent further operations or zeroizes all plaintext CSPs, plaintext PSPs and plaintext key components.
TE07.50.03	If the module is designed to zeroize all plaintext CSPs, plaintext PSPs and plaintext key components, and the module was still operational after returning to the normal environmental range, the tester shall perform services that require CSPs, plaintext PSPs and plaintext key components and verify that the module does not perform these services.
TE07.50.04	The tester shall verify that the security policy specifies the normal operating temperature and voltage range. The tester shall also verify whether the module shuts down or zeroizes all plaintext CSPs, plaintext PSPs and plaintext key components if the operating temperature or voltage falls outside the normal operating range of the module.

6.7.6 Environmental failure testing procedures

Table 233 — VE and TE of AS07.51

Environmental failure testing procedures — level 3	
AS07.51 ISO/IEC 19790:2025, 7.7.6	EFT shall involve a combination of analysis, simulation, and testing of a cryptographic module to provide reasonable assurance that the environmental conditions (accidental or induced) when outside the module's normal operating ranges for temperature and voltage will not compromise the security of the cryptographic module.
Required test procedures	
This assertion is tested as part of AS07.54.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 234 — VE and TE of AS07.52

Environmental failure testing procedures — level 3	
AS07.52 ISO/IEC 19790:2025, 7.7.6	EFT shall demonstrate that, if the operating temperature or voltage falls outside the normal operating range of the module resulting in a failure, {at no time shall the security of the cryptographic module be compromised.}
Required test procedures	
This assertion is tested as part of AS07.54.	

Table 235 — VE and TE of AS07.53

Environmental failure testing procedures — level 3	
AS07.53 ISO/IEC 19790:2025, 7.7.6	{EFT shall demonstrate that, if the operating temperature or voltage falls outside the normal operating range of the module resulting in a failure,} at no time shall the security of the cryptographic module be compromised.
Required test procedures	
This assertion is tested as part of AS07.54.	

Table 236 — VE and TE of AS07.54

Environmental failure testing procedures — level 3	
AS07.54 ISO/IEC 19790:2025, 7.7.6	The temperature range to be tested shall be from a temperature within the normal operating temperature range to the lowest (i.e. coldest) temperature outside of the normal operating range that results in the module either failing or entering an error state.
Required vendor information	
VE07.54.01	If EFT is chosen for a particular condition, the module shall be tested within the temperature range specified in AS07.54 and voltage ranges specified in AS07.59 and AS07.60. The module shall either: a) continue to operate normally, or b) fail and shut down, or c) enter an error state. Documentation shall state which of these approaches was chosen and provide a specification description of the EFT.
VE07.54.02	The security policy shall address whether the employed EFT feature causes the module to continue to operate normally, fail, or enter an error state and shall specify the temperature range met.
Required test procedures	
TE07.54.01	The tester shall configure the environmental condition (i.e. ambient temperature and voltage) as specified in AS07.54, AS07.59, and AS07.60 and verify that the module either continues to operate normally, or shuts down to prevent further operations, or enter an error state.
TE07.54.02	If the module is designed to enter an error state, and the module was still operational after returning to the normal environmental range, the tester shall verify that the module is in an error state.
TE07.54.03	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 enters an error state if the operating temperature or voltage falls outside the normal operating range of the module.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 237 — VE and TE of AS07.55

Environmental failure testing procedures — level 3	
AS07.55 ISO/IEC 19790:2025, 7.7.6	The temperature range shall also be from a temperature within the normal operating temperature range to the highest (i.e. hottest) temperature outside of the normal operating range that results in the module either failing or entering an error state.
Required test procedures	
This assertion is tested as part of AS07.54.	

Table 238 — VE and TE of AS07.56

Environmental failure testing procedures — level 3	
AS07.56 ISO/IEC 19790:2025, 7.7.6	The temperature range to be tested shall be from 100 °C to 200 °C; however, {the test shall be interrupted as soon as either the module fails or the module enters an error state.}
Required test procedures	
This assertion is tested as part of AS07.54.	

Table 239 — VE and TE of AS07.57

Environmental failure testing procedures — level 3	
AS07.57 ISO/IEC 19790:2025, 7.7.6	{The temperature range to be tested shall be from 100 °C to 200 °C;} however, the test shall be interrupted as soon as either the module fails or the module enters an error state
Required test procedures	
This assertion is tested as part of AS07.54.	

Table 240 — VE and TE of AS07.58

Environmental failure testing procedures — level 3	
AS07.58 ISO/IEC 19790:2025, 7.7.6	Temperature shall be monitored internally at the sensitive elements and critical devices and not just at the module's cryptographic boundary.
Required vendor information	
VE07.58.01	The vendor shall document the sensitive elements and critical devices relevant to AS07.58.
Required test procedures	
TE07.58.01	The tester shall document how the temperature was monitored when performing the EFT testing in order to ensure that the temperature range documented in the test corresponds to the observed temperature internal to the sensitive elements and critical devices identified by the vendor and not just at the modules' s cryptographic boundary.

Table 241 — VE and TE of AS07.59

Environmental failure testing procedures — level 3	
AS07.59 ISO/IEC 19790:2025, 7.7.6	The voltage range tested shall be gradually decreasing from a voltage within the normal operating voltage range to a lower voltage outside of the normal voltage range that results in the module either failing or entering an error state.
Required test procedures	
This assertion is tested as part of AS07.54.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 242 — VE and TE of AS07.60

Environmental failure testing procedures — level 3	
AS07.60 ISO/IEC 19790:2025, 7.7.6	The voltage range tested shall also be gradually increasing from a voltage within the normal operating voltage range to a higher voltage outside of the normal voltage range that results in the module either failing or entering an error state.
Required test procedures	
This assertion is tested as part of AS07.54.	

6.8 Non-invasive security

6.8.1 Non-invasive security general requirements

Table 243 — VE and TE of AS08.01

Non-invasive security general requirements — levels 1, 2, 3 and 4	
AS08.01 ISO/IEC 19790:2025, 7.8.1	Non-invasive attack mitigation techniques implemented by the cryptographic module to protect the module's SSPs that are not referenced in ISO/IEC 19790:2025, Annex F shall meet the requirements in ISO/IEC 19790:2025, 7.12.
Required test procedures	
This assertion is tested as part of AS12.01, AS12.02, AS12.03 and AS12.04.	

Table 244 — VE and TE of AS08.02

Non-invasive security general requirements — levels 1, 2, 3 and 4	
AS08.02 ISO/IEC 19790:2025, 7.8.1	The documentation for non-invasive security specified in ISO/IEC 19790:2025, A.2.7 shall be provided.
Required vendor information	
VE08.02.01	The vendor shall provide the documentation requirements as specified in ISO/IEC 19790:2025, A.2.7.
Required test procedures	
TE08.02.01	The tester shall verify that the vendor provides documentation as specified in ISO/IEC 19790:2025, A.2.7.

6.8.2 Security levels 1 and 2

Table 245 — VE and TE of AS08.03

Security levels 1 and 2 — levels 1, 2, 3 and 4	
AS08.03 ISO/IEC 19790:2025, 7.8.2	For security levels 1 and 2, documentation shall specify all of the mitigation techniques employed to protect the module's SSPs from the non-invasive attacks referenced in ISO/IEC 19790:2025, Annex F.
Required vendor information	
VE08.03.01	The vendor shall provide supporting documentation which specifies all of the mitigation techniques employed to protect the module's SSPs from the non-invasive attacks specified in ISO/IEC 19790:2025, Annex F.
Required test procedures	
TE08.03.01	The tester shall verify that the vendor provides supporting documentation which specifies all of the mitigation techniques employed to protect the module's SSPs from the non-invasive attacks specified in ISO/IEC 19790:2025, Annex F.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 246 — VE and TE of AS08.04

Security levels 1 and 2 — levels 1, 2, 3 and 4	
AS08.04 ISO/IEC 19790:2025, 7.8.2	Documentation shall include evidence of the effectiveness of each of the attack mitigation techniques.
Required vendor information	
VE08.04.01	The vendor shall specify in the documentation the effectiveness of the mitigation techniques.
Required test procedures	
TE08.04.01	The tester shall verify that the vendor provides documentation that specifies the effectiveness of the mitigation techniques.

6.8.3 Security level 3

Table 247 — VE and TE of AS08.05

Security level 3 — level 3	
AS08.05 ISO/IEC 19790:2025, 7.8.3	In addition to the requirements for security levels 1 and 2, the cryptographic module shall be tested to meet the approved non-invasive attack mitigation test metrics for security level 3 as referenced in ISO/IEC 19790:2025, Annex F.
Required vendor information	
VE08.05.01	The vendor shall provide documentation that the module meets the approved non-invasive attack mitigation test metrics for security level 3.
Required test procedures	
TE08.05.01	The tester shall verify that the vendor provides documentation that the module meets the approved non-invasive attack mitigation test metrics for security level 3.
TE08.05.02	The module shall be tested in accordance with any of the test procedures specified in ISO/IEC 20085-1 and ISO/IEC 20085-2.

6.8.4 Security level 4

Table 248 — VE and TE of AS08.06

Security level 4 — level 4	
AS08.06 ISO/IEC 19790:2025, 7.8.4	In addition to the requirements for security levels 1 and 2, the cryptographic module shall be tested to meet the approved non-invasive attack mitigation test metrics for security level 4 as referenced in ISO/IEC 19790:2025, Annex F.
Required vendor information	
VE08.06.01	The vendor shall provide documentation that the module meets the approved non-invasive attack mitigation test metrics for security level 4.
Required test procedures	
TE08.06.01	The tester shall verify that the vendor provides documentation that the module meets the approved non-invasive attack mitigation test metrics for security level 4.
TE08.06.02	The module shall be tested in accordance with any of the text procedures specified in ISO/IEC 20085-1 and ISO/IEC 20085-2.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.9 Sensitive security parameter management

6.9.1 Sensitive security parameter management general requirements

Table 249 — VE and TE of AS09.01

Sensitive security parameter management general requirements — levels 1, 2, 3 and 4	
AS09.01 ISO/IEC 19790:2025, 7.9.1	CSPs shall be protected within the module from unauthorized access, use, disclosure, modification, and substitution.
Required vendor information	
VE09.01.01	The vendor-provided documentation shall describe the protection of all CSPs internal to the module. Protection shall include the implementation of mechanisms that protect against unauthorized access, use, disclosure, modification, and substitution.
Required test procedures	
TE09.01.01	The tester shall check the vendor-provided documentation that describes the protection of CSPs. The tester shall verify that the documentation describes how these CSPs are protected from unauthorized access, use, disclosure, modification, and substitution.
TE09.01.02	The tester shall attempt to access (by circumventing the documented protection mechanisms) CSPs which the tester is not authorized to access. To meet this assertion, the module is required to deny access.
TE09.01.03	The tester shall attempt to modify CSPs using any method not specified by the vendor-provided documentation. NOTE CSPs encrypted using a non-approved algorithm or proprietary algorithm or method are considered to be in unprotected form within the scope of this document.

Table 250 — VE and TE of AS09.02

Sensitive security parameter management general requirements — levels 1, 2, 3 and 4	
AS09.02 ISO/IEC 19790:2025, 7.9.1	PSPs shall be protected within the module against unauthorized modification and substitution.
Required vendor information	
VE09.02.01	The vendor-provided documentation shall describe the protection of all PSPs against unauthorized modification and substitution.
Required test procedures	
TE09.02.01	The tester shall verify that the vendor-provided documentation describes how the PSPs are protected from unauthorized modification and substitution.
TE09.02.02	The tester shall attempt to modify all PSPs using any method not specified by the vendor-provided documentation and shall attempt to enter them into the module.

Table 251 — VE and TE of AS09.03

Sensitive security parameter management general requirements — levels 1, 2, 3 and 4	
AS09.03 ISO/IEC 19790:2025, 7.9.1	A module shall associate an SSP which is generated, entered into, or output from the module with the entity (i.e. person, group, role, or process) to which the SSP is assigned.
Required vendor information	
VE09.03.01	The documented SSP procedures shall describe the mechanisms or procedures used to ensure that each SSP is associated with the correct entity.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 251 *(continued)*

TE09.03.01	The tester shall verify that the documented SSP entry/output procedures address how an entered or output SSP is associated with the correct entity.
TE09.03.02	For each SSP that can be entered, the tester shall first enter the SSP while assuming the correct entity. The tester shall then verify that entry is not possible when assuming an incorrect entity.
TE09.03.03	For each SSP that can be output, the tester shall first output the SSP while assuming the correct entity. The tester shall then verify that output is not possible when assuming an incorrect entity.

Table 252 — VE and TE of AS09.04

Sensitive security parameter management general requirements — levels 1, 2, 3 and 4	
AS09.04 ISO/IEC 19790:2025, 7.9.1	Authentication data, verifier data that are not PSPs, RBG state information, and intermediate key generation values shall be considered as CSPs.
Required vendor information	
VE09.04.01	The vendor shall provide documentation confirming that the authentication data and verifier data, which are not PSPs, RBG state information, and intermediate key generation values are defined as CSPs.
Required test procedures	
TE09.04.01	The tester shall verify that the vendor provides documentation that the authentication data and verifier data that are not PSPs, RBG state information, and intermediate key generation values are defined as CSPs.
TE09.04.02	The tester shall verify that the vendor-provided security policy defines any authentication data and verifier data that are not PSPs, RBG state information, and intermediate key generation values as CSPs.

Table 253 — VE and TE of AS09.05

Sensitive security parameter management general requirements — levels 1, 2, 3 and 4	
AS09.05 ISO/IEC 19790:2025, 7.9.1	Hash values of passwords shall be considered as CSPs unless they were generated using an approved password protection method (e.g. salt and hash) as specified in ISO/IEC 19790:2025, Annex E, in which case {the hash values of passwords shall be considered PSPs.}
Required vendor information	
VE09.05.01	The vendor shall provide documentation that hash values of passwords that were not generated using an approved password protection method (e.g. salt and hash) as specified in ISO/IEC 19790:2025, Annex E, are defined as CSPs.
Required test procedures	
TE09.05.01	The tester shall verify that the vendor provides documentation, to confirm that any hash values of passwords are defined as CSPs.
TE09.05.02	The tester shall verify that the security policy provided by the vendor defines any hash values of passwords as CSPs.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 254 — VE and TE of AS09.06

Sensitive security parameter management general requirements — levels 1, 2, 3 and 4	
AS09.06 ISO/IEC 19790:2025, 7.9.1	{Hash values of passwords shall be considered as CSPs unless they were generated using an approved password protection method (e.g. salt and hash) as specified in ISO/IEC 19790:2025, Annex E,} in which case the hash values of passwords shall be considered PSPs.
Required vendor information	
VE09.06.01	The vendor shall provide documentation that hash values of passwords which were generated using an approved password protection method (e.g. salt and hash) as specified in ISO/IEC 19790:2025, Annex E, are defined as PSPs.
Required test procedures	
TE09.06.01	The tester shall verify that the vendor provides documentation, to confirm that any hash values of passwords are defined as PSPs.
TE09.06.02	The tester shall verify that security policy provided by the vendor defines any hash values of passwords as PSPs.

Table 255 — VE and TE of AS09.07

Sensitive security parameter management general requirements — levels 1, 2, 3 and 4	
AS09.07 ISO/IEC 19790:2025, 7.9.1	When a hash function is used on passwords/PINs, whether it is on its own or as part of an approved password protection method in ISO/IEC 19790:2025, Annex E, then an approved hash algorithm as listed in ISO/IEC 19790:2025, Annex C shall be used.
Required vendor information	
VE09.07.01	The vendor-provided documentation shall describe the approved hash algorithm that is used to create the hash values of passwords/PINs.
VE09.07.02	The vendor shall provide a validation certificate if available as specified in VE02.18.01, or vendor affirmation as specified in VE02.18.03.
Required test procedures	
TE09.07.01	The tester shall verify by inspection of the cryptographic module that an approved hash algorithm is used to create the hash values of passwords/PINs.
TE09.07.02	The tester shall verify that the vendor has provided a validation certificate if available for the approved hash algorithm implemented as specified in VE02.18.01, or vendor affirmation as specified in VE02.18.03.

Table 256 — VE and TE of AS09.08

Sensitive security parameter management general requirements — levels 1, 2, 3 and 4	
AS09.08 ISO/IEC 19790:2025, 7.9.1	The documentation for sensitive security parameter management specified in ISO/IEC 19790:2025, A.2.8 shall be provided.
Required vendor information	
VE09.08.01	The vendor shall provide the documentation requirements as specified in ISO/IEC 19790:2025, A.2.8.
Required test procedures	
TE09.08.01	The tester shall verify that the vendor provides documentation as specified in ISO/IEC 19790:2025, A.2.8.

6.9.2 Random bit generators

NOTE A cryptographic module can contain random bit generators (RBGs), a chain of RBGs, or can be solely an RBG.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 257 — VE and TE of AS09.09

Random bit generators — levels 1, 2, 3 and 4	
AS09.09 ISO/IEC 19790:2025, 7.9.2	If an approved security function requires random values, then an approved RBG shall be used to provide these values.
Required vendor information	
VE09.09.01	The vendor shall provide the list of all RBGs used in approved security functions within the cryptographic module and their precise usage.
VE09.09.02	The vendor shall provide documentation that any random values used by approved security functions are provided from an approved RBG.
VE09.09.03	The vendor shall provide documentation that all RBGs used in approved security functions are tested in accordance with the method specified in ISO/IEC 20543.
Required test procedures	
TE09.09.01	The tester shall verify that all RBGs used by approved security functions are documented and their usage defined.
TE09.09.02	The tester shall verify from the vendor-provided documentation that the implemented RBGs used by approved security functions are compliant with the approved RBGs listed in ISO/IEC 19790:2025, Annex C.
TE09.09.03	The tester shall verify from the vendor-provided documentation that any random values used by approved security functions are provided from an approved RBG.
TE09.09.04	The tester shall verify from the vendor-provided documentation that all RBGs used in approved security functions are tested in accordance with the method specified in ISO/IEC 20543.
NOTE Approved RBGs are listed in ISO/IEC 19790:2025, Annex C.	

Table 258 — VE and TE of AS09.10

Random bit generators — levels 1, 2, 3 and 4	
AS09.10 ISO/IEC 19790:2025, 7.9.2	Entropy input used to seed an approved RBG shall be considered a CSP.
Required vendor information	
VE09.10.01	The vendor shall provide documentation that the entropy input used to seed an approved RBG is defined as a CSP.
Required test procedures	
TE09.10.01	The tester shall verify that the vendor provides documentation that the entropy input used to seed an approved RBG is defined as a CSP.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.9.3 Sensitive security parameter generation

Table 259 — VE and TE of AS09.11

Sensitive security parameter generation — levels 1, 2, 3 and 4	
AS09.11 ISO/IEC 19790:2025, 7.9.3	Compromising the security of the SSP generation method which uses the output of an approved RBG (e.g. guessing the seed value to initialize the deterministic RBG) shall require at least as many operations as determining the value of the generated SSP.
Required vendor information	
VE09.11.01	The vendor shall provide documentation that provides rationale stating how compromising the security of the SSP generation method (e.g. guessing the seed value to initialize the deterministic RBG) requires at least as many operations as determining the value of the generated SSP.
Required test procedures	
TE09.11.01	The tester shall verify that the vendor-provided documentation that provides rationale stating how compromising the security of the SSP generation method (e.g. guessing the seed value to initialize the deterministic RBG) requires at least as many operations as determining the value of the generated SSP.
TE09.11.02	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 ask the vendor to produce additional information.

Table 260 — VE and TE of AS09.12

Sensitive security parameter generation — levels 1, 2, 3 and 4	
AS09.12 ISO/IEC 19790:2025, 7.9.3	SSPs generated by the module from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function shall be generated using approved sensitive security parameter generation methods listed in ISO/IEC 19790:2025, Annex D.
Required vendor information	
VE09.12.01	The vendor shall provide the list of all SSPs generated by the module used in the cryptographic module and their precise usage. These SSPs are generated from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function.
VE09.12.02	The vendor shall provide documentation that SSPs generated by the module are generated using an approved SSP generation method. These SSPs are generated from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function.
Required test procedures	
TE09.12.01	The tester shall verify that all SSPs generated by the module are documented and their usage defined. These SSPs are generated from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function.
TE09.12.02	The tester shall verify from the vendor-provided documentation that the implemented SSPs generated by the module are compliant with the approved SSP generation methods listed in ISO/IEC 19790:2025, Annex D. These SSPs are generated from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

6.9.4 Automated sensitive security parameter establishment

NOTE Automated sensitive security parameter establishment can consist of automated SSP transport or SSP agreement methods.

© ISO/IEC 2025 – All rights reserved

Table 261 — VE and TE of AS09.13

Automated sensitive security parameter establishment — levels 1, 2, 3 and 4	
AS09.13 ISO/IEC 19790:2025, 7.9.4	Automated SSP establishment shall use an approved method listed in ISO/IEC 19790:2025, Annex D.
Required vendor information	
VE09.13.01	The vendor shall provide the list of all automated SSP establishment methods used in the cryptographic module and their precise usage.
Required test procedures	
TE09.13.01	The tester shall verify that all automated SSP establishment methods are documented and their usage defined.
TE09.13.02	The tester shall verify from the vendor-provided documentation that the implemented automated SSP establishment methods are compliant with the approved automated SSP establishment methods listed in ISO/IEC 19790:2025, Annex D.

6.9.5 Sensitive security parameter entry and output

6.9.5.1 Sensitive security parameter entry and output general requirements

NOTE Sensitive security parameters can be manually entered into or output from a module either directly (e.g. entered via a keyboard or number pad, or output via a visual display) or electronically (e.g. via a smart card/tokens, PC card, other electronic key loading device, or the module operational environment).

Table 262 — VE and TE of AS09.14

Sensitive security parameter entry and output — levels 1, 2, 3 and 4	
AS09.14 ISO/IEC 19790:2025, 7.9.5.1	If SSPs are manually entered or output from a module, the entry or output shall be through the defined module interfaces.
Required test procedures	
This assertion is tested as part of AS03.04, AS03.05, AS03.06, AS03.07, AS03.08, AS03.09, AS03.10, AS03.11, AS03.12, AS03.13 and AS03.14.	

Table 263 — VE and TE of AS09.15

Sensitive security parameter entry and output — levels 1, 2, 3 and 4	
AS09.15 ISO/IEC 19790:2025, 7.9.5.1	All cryptographically protected SSPs, entered or output from the module shall be protected using an approved security function, as specified in ISO/IEC 19790:2025, Annex C.
Required vendor information	
VE09.15.01	The vendor-provided documentation shall specify all cryptographically protected SSPs which are entered or output from the cryptographic module.
VE09.15.02	The vendor-provided documentation shall state the method used to cryptographically protect the SSPs which are entered or output from the cryptographic module.
Required test procedures	
TE09.15.01	The tester shall verify that the vendor has provided documentation specifying all the cryptographically protected SSPs which are entered and output from the cryptographic module.
TE09.15.02	The tester shall verify that the vendor has provided documentation specifying the method used to cryptographically protect the SSPs which are entered or output from the cryptographic module.
TE09.15.03	The tester shall verify that the method used to cryptographically protect the SSPs which are entered or output from the cryptographic module is performed using an approved security function.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 264 — VE and TE of AS09.16

Sensitive security parameter entry and output — levels 1, 2, 3 and 4	
AS09.16 ISO/IEC 19790:2025, 7.9.5.1	If encrypted SSPs are directly entered manually into the module, then the plaintext values of the SSPs shall not be displayed.
Required vendor information	
VE09.16.01	The documented SSP entry mechanisms for encrypted SSPs shall preclude the display of their plaintext values.
Required test procedures	
TE09.16.01	The tester shall verify that the documented SSP entry mechanisms for encrypted SSPs preclude the display of their plaintext values during the encrypted SSP entry process.
TE09.16.02	The tester shall enter all encrypted SSPs and monitor the output interfaces of the module to verify that any resulting plaintext SSP values are not displayed. NOTE For directly entered SSPs, the entered values can be temporarily displayed to allow visual verification and to improve accuracy.

Table 265 — VE and TE of AS09.17

Sensitive security parameter entry and output — levels 1, 2, 3 and 4	
AS09.17 ISO/IEC 19790:2025, 7.9.5.1	Except for authentication data, manually directly entered (plaintext or encrypted) SSPs shall be verified during entry into a module for accuracy using the conditional manual entry test specified in ISO/IEC 19790:2025, 7.10.4.5.
Required test procedures	
This assertion is tested as part of AS10.44, AS10.45, AS10.46 and AS10.47.	

Table 266 — VE and TE of AS09.18

Sensitive security parameter entry and output — levels 1, 2, 3 and 4	
AS09.18 ISO/IEC 19790:2025, 7.9.5.1	To prevent the inadvertent output of sensitive information, two independent internal actions shall be required by the module in order to output any plaintext CSP;
Required vendor information	
VE09.18.01	If the module outputs any plaintext CSPs, the vendor-provided documentation shall describe the output services.
VE09.18.02	The finite state model and other vendor-provided documentation shall indicate, for the output of plaintext CSPs, that two independent internal actions are required.
Required test procedures	
TE09.18.01	The tester shall verify from the vendor-provided documentation or finite state model that the module allows the output of plaintext CSPs.
TE09.18.02	The tester shall verify from the finite state model and other vendor-provided documentation that the output of plaintext CSPs requires two independent internal actions in order for the cryptographic module to output the plaintext CSPs.
TE09.18.03	The tester shall attempt to output plaintext CSPs without the module performing two independent internal actions. The module shall fail if the module allows the output of plaintext CSPs without two independent internal actions.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 267 — VE and TE of AS09.19

Sensitive security parameter entry and output — levels 1, 2, 3 and 4	
AS09.19 ISO/IEC 19790:2025, 7.9.5.1	For electronic entry or output via a wireless connection, CSPs and key components shall be encrypted.
Required vendor information	
VE09.19.01	If the module inputs or outputs CSPs, and key components via wireless interfaces, the vendor-provided documentation shall describe the wireless services.
VE09.19.02	If the module inputs or outputs CSPs, and key components via wireless interfaces, the vendor-provided documentation shall describe the encryption methods employed to encrypt the CSPs and key components.
Required test procedures	
TE09.19.01	The tester shall verify whether the module inputs or outputs CSPs and key components via wireless interfaces.
TE09.19.02	The tester shall verify that the encryption methods employed to encrypt the CSPs and key components are approved encryption methods. NOTE For security levels 1 and 2, plaintext CSPs and key components can be entered and output via physical port(s) and logical interface(s) shared with other physical ports and logical interfaces of the cryptographic module.

Table 268 — VE and TE of AS09.20

Sensitive security parameter entry and output — levels 1, 2, 3 and 4	
AS09.20 ISO/IEC 19790:2025, 7.9.5.1	Cryptographic keys established wirelessly using automated methods shall use an approved method listed in ISO/IEC 19790:2025, Annex D.
Required test procedures	
This assertion is tested as part of AS09.13.	

Table 269 — VE and TE of AS09.21

Sensitive security parameter entry and output — levels 1, 2, 3 and 4	
AS09.21 ISO/IEC 19790:2025, 7.9.5.1	If the cryptographic module employs split-knowledge procedures for cryptographic keys entry or output, at least two key components shall be required by the module to reconstruct the original cryptographic key.
Required vendor information	
VE09.21.01	The vendor-provided documentation shall specify the number of components that are required to construct the original CSP.
VE09.21.02	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 number less than the number of key components provides no information about the original key other than the length.
Required test procedures	
TE09.21.01	The tester shall verify that the vendor-provided documentation describes how the split-knowledge procedure requires at least two components to construct the original CSP.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 269 *(continued)*

TE09.21.02	The tester shall verify that the vendor-provided documentation describes how 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.
TE09.21.03	The tester shall verify that the vendor-provided documentation provides a rationale that no information is gained without knowing all the necessary key components, and 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.
TE09.21.04	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 ask the vendor to produce additional information.

6.9.5.2 Security levels 1 and 2

Table 270 — VE and TE of AS09.22

Sensitive security parameter entry and output — levels 1 and 2	
AS09.22 ISO/IEC 19790:2025, 7.9.5.2	For software modules or the software components of a hybrid software module, CSPs and key components may be entered or output from the module in plaintext form; in this case, the module shall not output the CSPs and key components from the operational environment.
Required vendor information	
VE09.22.01	For software modules or the software components of a hybrid software module, the vendor shall provide documentation showing that CSPs and key components that are entered or output from the module in plaintext form are maintained within the operational environment and that the plaintext form CSPs and key components is not output from the operational environment.
Required test procedures	
TE09.22.01	For software modules or the software components of a hybrid software module the tester shall verify that the vendor provides documentation showing that CSPs and key components that are entered or output from the module in plaintext form are maintained within the operational environment and that the plaintext form CSPs and key components are not output from the operational environment.

6.9.5.3 Security level 3

Table 271 — VE and TE of AS09.23

Sensitive security parameter entry and output — level 3	
AS09.23 ISO/IEC 19790:2025, 7.9.5.3	Cryptographic keys, key components from split-knowledge procedures, and non-key CSPs entered or output from the cryptographic module using direct entry or electronic methods shall either be encrypted or using a plaintext trusted path that meet security level 3 requirements in ISO/IEC 19790:2025, 7.3.4.
Required vendor information	
VE09.23.01	The vendor shall provide documentation that describes whether cryptographic keys, key components from split-knowledge procedures, and non-key CSPs are entered or output from the cryptographic module encrypted or using a plaintext trusted path.
VE09.23.02	For keys that are encrypted when entered or output from a module, the vendor-provided documentation shall describe the encryption method and provide a validation certificate if available or vendor affirmation as specified in VE02.18.01 and VE02.18.03.
VE09.23.03	For keys that are entered or output from a module using split-knowledge procedures, the vendor-provided documentation shall describe the split-knowledge methods used as specified in VE09.21.01 to VE09.21.02.
VE09.23.04	For keys that are entered or output from a module using a plaintext trusted path, the vendor-provided documentation shall describe the plaintext trusted path as specified in AS03.17 to AS03.22.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 271 *(continued)*

TE09.23.01	The tester shall verify that the vendor-provided documentation specifies that cryptographic keys, key components from split-knowledge procedures, and non-key CSPs are entered or output from the cryptographic module encrypted or using a plaintext trusted path.
TE09.23.02	For keys that are encrypted when entered or output from a module, the tester shall verify that the vendor-provided documentation describes the encryption method. The tester shall verify that the vendor provides a validation certificate if available or vendor affirmation as specified in TE02.18.01 and TE02.18.03.
TE09.23.03	For keys that are entered or output from a module using split-knowledge procedures, the tester shall verify that the vendor-provided documentation describes the split-knowledge methods used as specified in TE09.21.01 to TE09.21.04.
TE09.23.04	For keys that are entered or output from a module using a plaintext trusted path, the tester shall verify that the vendor-provided documentation describes the plaintext trusted path. used as specified in AS03.17 to AS03.22.
TE09.23.05	For documented methods in TE09.23.01 to TE09.23.04, the tester shall verify by test and inspection of the module that imported keys are using the methods described.

Table 272 — VE and TE of AS09.24

Sensitive security parameter entry and output — level 3	
AS09.24 ISO/IEC 19790:2025, 7.9.5.3	When entering or outputting key components from split-knowledge procedures, the module shall authenticate each operator (i.e. each distinct key component importer or exporter) separately with an authentication that meets security level 3 requirements in ISO/IEC 19790 :—, 7.4.4.
Required vendor information	
VE09.24.01	The vendor-provided documentation shall specify how that identity-based authentication is employed and checked ahead of entry of each separate key component.
Required test procedures	
TE09.24.01	The tester shall verify that that the vendor-provided documentation specifies how that identity-based authentication is employed and checked ahead of entry of each separate key component.
TE09.24.02	The test shall perform split-key entry to the module and confirm that separate identity-based authentication is required to enter each key component.

6.9.5.4 Security level 4

Table 273 — VE and TE of AS09.25

Sensitive security parameter entry and output — level 4	
AS09.25 ISO/IEC 19790:2025, 7.9.5.4	Cryptographic keys entered or output from the cryptographic module shall either be encrypted or entered using split-knowledge procedures.
Required vendor information	
VE09.25.01	The vendor-provided shall provide documentation that describes whether cryptographic keys are entered or output from the module encrypted or using split-knowledge procedures.
VE09.25.02	For keys that are encrypted when entered or output from a module, the vendor documentation shall describe the encryption method and provide a validation certificate if available or vendor affirmation as specified in VE02.18.01 and VE02.18.03.
VE09.25.03	For keys that are entered or output from a module using split-knowledge procedures, the vendor-provided documentation shall describe the split-knowledge methods used as specified in VE09.21.01 to VE09.21.02.
Required test procedures	
TE09.25.01	The tester shall verify that the vendor-provided documentation describes whether cryptographic keys are entered or output from the module encrypted or using split-knowledge procedures.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 273 *(continued)*

TE09.25.02	For keys that are encrypted when entered or output from a module, the tester shall verify that the vendor-provided documentation describes the encryption method and provide a validation certificate if available or vendor affirmation as specified in TE02.18.01 and VE02.18.03.
TE09.25.03	For keys that are entered or output from a module using split-knowledge procedures, the tester shall verify that the vendor-provided documentation describes the split-knowledge methods used as specified in TE09.21.01 to TE09.21.04.
TE09.25.04	For documented methods in TE09.25.01 to TE09.25.03, the tester shall verify by test and inspection of the module that imported keys are using the methods described.

Table 274 — VE and TE of AS09.26

Sensitive security parameter entry and output — level 4	
AS09.26 ISO/IEC 19790:2025, 7.9.5.4	Key components from split-knowledge procedures and non-key CSPs shall be entered or output from the module either encrypted or by a plaintext trusted path that meets security level 4 requirements in ISO/IEC 19790:2025, 7.3.4.
Required vendor information	
VE09.26.01	The vendor shall provide documentation that describes whether key components from split-knowledge procedures and non-key CSPs are entered or output from the module encrypted or using split-knowledge procedures.
VE09.26.02	For key components from split-knowledge procedures and non-key CSPs that are encrypted when entered or output from a module, the vendor-provided documentation shall describe the encryption method and provide a validation certificate if available or vendor affirmation as specified in VE02.18.01 and VE02.18.03.
VE09.26.03	For key components from split-knowledge procedures and non-key CSPs that are entered or output from a module using split-knowledge procedures, the vendor-provided documentation shall describe the split-knowledge methods used.
Required test procedures	
TE09.26.01	The tester shall verify that the vendor-provided documentation describes whether key components from split-knowledge procedures and non-key CSPs are entered or output from the module encrypted or using split-knowledge procedures.
TE09.26.02	For key components from split-knowledge procedures and non-key CSPs that are encrypted when entered or output from a module, the tester shall verify that the vendor documentation describes the encryption method. The tester shall verify that the vendor provides a validation certificate if available or vendor affirmation as specified in TE02.18.01 and VE02.18.03.
TE09.26.03	For key components from split-knowledge procedures and non-key CSPs that are entered or output from a module using split-knowledge procedures, the tester shall verify that the vendor documentation describes the split-knowledge methods used.
TE09.26.04	For documented methods in TE09.26.01 to TE09.26.03, the tester shall verify by test and inspection of the module that imported keys are using the methods described.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 275 — VE and TE of AS09.27

Sensitive security parameter entry and output — level 4	
AS09.27 ISO/IEC 19790:2025, 7.9.5.4	For key components entered or outputted as part of split-knowledge procedures, the module shall authenticate each operator (i.e. each distinct key component importer/exporter) separately with an authentication that meets security level 4 requirements in ISO/IEC 19790:2025, 7.4.4.
Required vendor information	
VE09.27.01	The vendor-provided documentation shall specify that multi-factor identity-based authentication or another that meets security level 4 requirements in ISO/IEC 19790:2025, 7.4.4 is employed for each separate key component.
Required test procedures	
TE09.27.01	The tester shall verify that multi-factor identity-based authentication or another that meets security level 4 requirements in ISO ISO/IEC 19790:2025, 7.4.4 is employed for each separate key component.
TE09.27.02	The tester shall verify the multi-factor authentication method or another under AS04.59.

6.9.6 Sensitive security parameter storage

Table 276 — VE and TE of AS09.28

Sensitive security parameter storage — levels 1, 2, 3 and 4	
AS09.28 ISO/IEC 19790:2025, 7.9.6	A module shall associate every SSP stored within the module with the entity (e.g. operator, role, or process) to which the SSP is assigned.
Required vendor information	
VE09.28.01	The vendor-provided documentation on key storage shall describe the mechanisms or procedures used to ensure that each key is associated with the correct entity.
Required test procedures	
TE09.28.01	The tester shall verify the documentation on key storage that the procedures address how a stored key is associated with the correct entity.
TE09.28.02	The tester shall modify the association of key and entity. The tester shall then attempt to perform cryptographic functions as one of the entities and shall verify that these functions fail.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.9.7 Sensitive security parameter zeroization

6.9.7.1 Sensitive security parameter zeroization general requirements

Table 277 — VE and TE of AS09.29

Sensitive security parameter zeroization — levels 1, 2, 3 and 4	
AS09.29 ISO/IEC 19790:2025, 7.9.7.1	A module shall provide methods to zeroize all plaintext CSPs, plaintext PSPs, and plaintext key components within the module.
Required vendor information	
VE09.29.01	The vendor-provided documentation shall specify the following zeroization information for operator CSPs and operator PSPs: a) zeroization techniques; b) restrictions when plaintext CSPs, plaintext PSPs, and plaintext key components can be zeroized; c) plaintext CSPs, plaintext PSPs, and plaintext key components that are zeroized; d) plaintext CSPs, plaintext PSPs, and plaintext key components that are not zeroized and rationale; e) rationale explaining how the zeroization technique is performed in a time that is not sufficient to compromise plaintext CSPs, plaintext PSPs and plaintext key components.
VE09.29.02	The vendor-provided documentation shall specify how the zeroization method(s) are employed such that plaintext CSPs, plaintext PSPs and plaintext key components within the module cannot be obtained by an attacker.
VE09.29.03	If plaintext CSPs, plaintext PSPs and plaintext key components 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-provided documentation and the module security policy shall specify how the methods shall be performed.
Required test procedures	
TE09.29.01	The tester shall verify the vendor documentation includes the information specified in VE09.29.01. 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 request the vendor to produce additional information as needed.
TE09.29.02	The tester shall verify which plaintext CSPs, plaintext PSPs and plaintext key components are present in the module and initiate the zeroize command. Following the completion of the zeroize command, the tester shall attempt to perform cryptographic operations using each of the plaintext CSPs, plaintext PSPs and plaintext key components that were stored in the module. The tester shall verify that each unprotected SSP cannot be accessed.
TE09.29.03	The tester shall initiate zeroization and verify the SSP destruction method is performed in a time that is not sufficient to compromise plaintext CSPs, plaintext PSPs, and plaintext key components.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 277 *(continued)*

TE09.29.04	The tester shall verify that all plaintext CSPs, plaintext PSPs, and plaintext key components to not be zeroized by the zeroize 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 19790:2025).
TE09.29.05	If procedural zeroization methods are used, the tester shall verify that the vendor-provided documentation, including the security policy, specifies that the procedure shall be performed under the control of the operator.
TE09.29.06	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 plaintext CSPs, plaintext PSPs and plaintext key components 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 ask the vendor to produce additional information. NOTE Temporarily stored plaintext CSPs, plaintext PSPs, plaintext key components, and other stored values owned by the module are zeroized when they are no longer required for future use.

Table 278 — VE and TE of AS09.30

Sensitive security parameter zeroization — levels 1, 2, 3 and 4	
AS09.30 ISO/IEC 19790:2025, 7.9.7.1	A zeroized SSP or key component shall not be retrievable or reusable, including in response to tamper.
Required vendor information	
VE09.30.01	The vendor-provided documentation shall specify how a zeroized SSP or key component cannot be retrievable or reusable.
Required test procedures	
TE09.30.01	The tester shall verify that the vendor-provided documentation specifies how a zeroized SSP or key component cannot be retrievable or reusable.
TE09.30.02	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 ask the vendor to produce additional information. Zeroization of protected PSPs, encrypted CSPs, or CSPs otherwise physically or logically protected within an additional embedded validated module (meeting the requirements of ISO/IEC 19790:2025) is not expected. SSPs are not expected to meet these zeroization requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialization key). NOTE 1 Zeroization of protected PSPs, encrypted CSPs or CSPs otherwise physically or logically protected within an additional embedded validated module (meeting the requirements of ISO/IEC 19790:2025) is not expected NOTE 2 SSPs are not expected to meet these zeroization requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialization key).

6.9.7.2 Security level 1

Table 279 — VE and TE of AS09.31

Sensitive security parameter zeroization — level 1	
AS09.31 ISO/IEC 19790:2025, 7.9.7.2	If zeroization is performed procedurally, the security policy shall provide instructions on how to perform the procedure, such that all plaintext CSPs, plaintext PSPs and plaintext key components are zeroized.
Required test procedures	
This assertion is tested as part of ASB.01.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.9.7.3 Security levels 2 and 3

Table 280 — VE and TE of AS09.32

Sensitive security parameter zeroization — levels 2, 3 and 4	
AS09.32 ISO/IEC 19790:2025, 7.9.7.3	The cryptographic module shall perform the zeroization of plaintext CSPs, plaintext PSPs and plaintext key components (e.g. overwriting with all zeros or all ones or with random data).
Required test procedures	
This assertion is tested as part of AS09.29.	

Table 281 — VE and TE of AS09.33

Sensitive security parameter zeroization — levels 2, 3 and 4	
AS09.33 ISO/IEC 19790:2025, 7.9.7.3	When zeroizing plaintext CSPs or plaintext PSPs, or both in response to a user request or tamper, the module shall not overwrite them with other plaintext CSPs or user PSPs, including in response to tamper.
Required vendor information	
VE09.33.01	The vendor-provided documentation shall specify that the zeroization excludes the overwriting of a plaintext SSP with another plaintext SSP.
Required test procedures	
TE09.33.01	The tester shall verify that the vendor-provided documentation specifies that the zeroization excludes the overwriting of a plaintext SSP with another plaintext SSP.

Table 282 — VE and TE of AS09.34

Sensitive security parameter zeroization — levels 2, 3 and 4	
AS09.34 ISO/IEC 19790:2025, 7.9.7.3	Temporary SSPs shall be zeroized when they are no longer required, however, in this case AS09.35 and AS03.07 are not applicable.
Required vendor information	
VE09.34.01	The vendor-provided documentation shall specify that temporary SSPs are zeroized when they are no longer required.
Required test procedures	
TE09.34.01	The tester shall verify that the vendor-provided documentation specifies that temporary SSPs are zeroized when they are no longer required.

Table 283 — VE and TE of AS09.35

Sensitive security parameter zeroization — levels 2, 3 and 4	
AS09.35 ISO/IEC 19790:2025, 7.9.7.3	The module shall provide an output status indication when the zeroization of plaintext CSPs, plaintext PSPs and plaintext key components is complete, including in response to tamper.
Required vendor information	
VE09.35.01	The vendor-provided documentation shall specify that the module provides an output status indication when the zeroization is complete (AS03.11).
Required test procedures	
TE09.35.01	The tester shall verify that the vendor provides documentation that specifies that the module provides an output status indication when the zeroization is complete.
TE09.35.02	The tester shall perform zeroization and verify the status output indicator.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.9.7.4 Security level 4

Table 284 — VE and TE of AS09.36

Sensitive security parameter zeroization — level 4	
AS09.36 ISO/IEC 19790:2025, 7.9.7.4	In addition to the requirements of security levels 2, and 3, the following requirements shall be met: {AS09.37 to AS09.39}
Required test procedures	
This assertion is tested as part of AS09.37, AS09.38 and AS09.39.	

Table 285 — VE and TE of AS09.37

Sensitive security parameter zeroization — level 4	
AS09.37 ISO/IEC 19790:2025, 7.9.7.4	The zeroization shall be immediate and non-interruptible; and {shall occur in a sufficiently small time period so as to prevent the recovery of the SSP being zeroized between the time zeroization is initiated and the actual zeroization completed, including in response to tamper}.
Required test procedures	
This assertion is tested as part of AS09.38.	

Table 286 — VE and TE of AS09.38

Sensitive security parameter zeroization — level 4	
AS09.38 ISO/IEC 19790:2025, 7.9.7.4	{The zeroization shall be immediate and non-interruptible;} and shall occur in a sufficiently small time period so as to prevent the recovery of the SSP being zeroized between the time zeroization is initiated and the actual zeroization completed, including in response to tamper.
Required vendor information	
VE09.38.01	The vendor shall provide documentation that the module zeroization is immediate, non-interruptible and occurs in a sufficiently short time period so as to prevent the recovery of the sensitive data after the time zeroization is initiated and before the actual zeroization has been completed.
Required test procedures	
TE09.38.01	The tester shall verify that the vendor provides documentation that the module zeroization is immediate, non-interruptible and occurs in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time when zeroization is initiated and the actual zeroization is completed.
TE09.38.02	The tester shall perform the module zeroization. The tester shall attempt to interrupt the zeroization process to prevent its completion in whole or part.

Table 287 — VE and TE of AS09.39

Sensitive security parameter zeroization — level 4	
AS09.39 ISO/IEC 19790:2025, 7.9.7.4	All SSPs shall be zeroized, including in response to tamper, such that the module is returned to the factory state.
Required vendor information	
VE09.39.01	The vendor shall provide documentation that all CSPs and PSPs are zeroized such that the module is returned to the factory state.
Required test procedures	
TE09.39.01	The tester shall verify that the vendor provides documentation that all CSPs and PSPs are zeroized such that the module is returned to the factory state.
TE09.39.02	The tester shall perform the module zeroization. The tester shall verify that the module has returned to the factory state.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.10 Self-tests

6.10.1 Self-test general requirements

Table 288 — VE and TE of AS10.01

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.01 ISO/IEC 19790:2025, 7.10.1	All self-tests shall be performed by the module, without external controls, externally provided input test vectors, expected output results, or operator intervention, and regardless of whether the module will operate an approved or non-approved service.
Required test procedures	
This assertion is not separately tested.	

Table 289 — VE and TE of AS10.02

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.02 ISO/IEC 19790:2025, 7.10.1	The determination of pass or fail shall be made by the module, without external controls, externally provided input test vectors, expected output results, or operator intervention, and regardless of whether the module will operate an approved or non-approved service.
Required test procedures	
This assertion is not separately tested.	
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.	

Table 290 — VE and TE of AS10.03

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.03 ISO/IEC 19790:2025, 7.10.1	The pre-operational self-tests shall be performed and passed successfully prior to the module providing any data output via the data output interface.
Required test procedures	
This assertion is tested as part of AS10.14.	

Table 291 — VE and TE of AS10.04

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.04 ISO/IEC 19790:2025, 7.10.1	Conditional self-tests shall be performed when an applicable cryptographic algorithm or process is invoked (i.e. cryptographic algorithms for which self-tests are required).
Required test procedures	
This assertion is tested as part of AS10.25.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 292 — VE and TE of AS10.05

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.05 ISO/IEC 19790:2025, 7.10.1	All self-tests identified in underlying standards in ISO/IEC 19790:2025, Annexes C, D and E shall be implemented as applicable.
Required vendor information	
VE10.05.01	The vendor-provided documentation shall provide the list of self-tests to include the following: a) pre-operational self-tests: 1) pre-operational software/firmware integrity test; 2) pre-operational bypass test; 3) pre-operational critical functions test; 4) conditional self-tests: b) conditional cryptographic algorithm test; 1) conditional pair-wise consistency test; 2) conditional software/firmware load test; 3) conditional manual entry test; 4) conditional bypass test; 5) conditional critical functions test.
VE10.05.02	The vendor-provided documentation shall specify that the tests identified in underlying standards (as specified in ISO/IEC 19790:2025, Annexes C, D and E) are implemented as applicable, or as defined by the certification body, in addition to those specified within in ISO/IEC 19790:2025.
Required test procedures	
TE10.05.01	The tester shall verify that the vendor provides documentation that the tests identified in the underlying standards specified in ISO/IEC 19790:2025, Annexes C, D and E are implemented as applicable, or as defined by the certification body, in addition to those specified within ISO/IEC 19790:2025.

Table 293 — VE and TE of AS10.06

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.06 ISO/IEC 19790:2025, 7.10.1	All self-tests identified in addition to or in lieu of those specified in the underlying standards in ISO/IEC 19790:2025, Annexes C, D and E shall be implemented as referenced in ISO/IEC 19790:2025, Annexes C, D and E for each approved security function.
Required test procedures	
This assertion is tested as part of AS10.01, AS10.02, AS10.03 and AS10.04.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 294 — VE and TE of AS10.07

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.07 ISO/IEC 19790:2025, 7.10.1	If a cryptographic module fails a self-test, the module: shall enter an error state; or {shall behave as specified by the certification body for that particular self-test failure, if that self-test is defined in underlying standards in ISO/IEC 19790:2025, Annexes C, D and E.}
Required vendor information	
VE10.07.01	For each error condition, the vendor-provided documentation shall provide the condition name, description of the condition, the events that can produce the condition, and the actions necessary to clear the condition and resume normal operation.
Required test procedures	
TE10.07.01	The tester shall verify the list of self-tests to test the module in ISO/IEC 19790:2025, Annexes C, D and E.
TE10.07.02	The tester shall check that the information provided above is specified for each error condition.
TE10.07.03	The tester shall cause each error condition to occur and shall attempt to clear the error condition. The tester shall verify that actions necessary to clear the error condition are consistent with the vendor-provided documentation. If the tester cannot cause each error condition to occur, the tester shall verify the code listing or design documentation to check whether the actions necessary to clear each error condition are consistent with the descriptions in the vendor-provided documentation.
TE10.07.04	The tester shall review the vendor-provided documentation and inspect the module to verify that determination of pass or fail of each self-test is made by the module, without external controls, externally provided input test vectors, expected output results, or operator intervention.

Table 295 — VE and TE of AS10.08

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.08 ISO/IEC 19790:2025, 7.10.1	{If a cryptographic module fails a self-test, the module: shall enter an error state; or} shall behave as specified by the certification body for that particular self-test failure, if that self-test is defined in underlying standards in ISO/IEC 19790:2025, Annexes C, D and E.
Required test procedures	
This assertion is not separately tested.	

Table 296 — VE and TE of AS10.09

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.09 ISO/IEC 19790:2025, 7.10.1	If a cryptographic module fails the conditional manual entry test or the conditional software/firmware load test, and in some cases the conditional critical function test, the module shall indicate the test failed, but the module is not required to enter an error state, inhibit data output, or cease cryptographic processing.
Required test procedures	
This assertion is tested as part of AS10.07.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 297 — VE and TE of AS10.10

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.10 ISO/IEC 19790:2025, 7.10.1	The operator of the module shall be able to determine if the module has entered an error state either by an error indicator output by the module or implicitly through an unambiguous procedure documented in the security policy.
Required vendor information	
VE10.10.01	The vendor shall document all error states associated with each self-test and shall indicate for each error state the expected error indicator.
VE10.10.02	If the module has entered an error state by an error indicator output implicitly, the vendor-provided non-proprietary security policy shall describe unambiguously the procedure to determine if the cryptographic module has entered an error state.
Required test procedures	
TE10.10.01	The tester shall verify the vendor-provided documentation, check that it lists every error state that the module enters upon failure of a self-test, and indicates the error indicator associated with each error state. The tester shall compare the list of error states to those defined in the finite state model (see AS11.11) to verify that they agree.
TE10.10.02	By inspecting the vendor-provided documentation specifying how each self-test handles errors, the tester shall verify that: a) the module enters an error state upon failing a self-test; b) the error state is consistent with the documentation and the finite state model; c) the module outputs an error indicator; d) the error indicator is consistent with the documented error indicator.
TE10.10.03	The tester shall run each self-test and cause the module to enter every error state. The tester shall compare the observed error indicator with the indicator specified in the vendor-provided documentation. If they are not the same, this test has failed.
TE10.10.04	If the module has entered an error state by an error indicator output implicitly, the tester shall verify that the module has entered the error state implicitly through the procedure documented in the non-proprietary security policy.

Table 298 — VE and TE of AS10.11

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.11 ISO/IEC 19790:2025, 7.10.1	The cryptographic module shall not perform any cryptographic operations or output control and data via the control and data output interface while in an error state.
Required vendor information	
VE10.11.01	The vendor-provided documentation requirements are specified under VE03.07.01, VE03.07.02, VE03.09.01, and VE03.10.01. The vendor design also shall ensure that cryptographic operations cannot be performed while the module is in the error state.
Required test procedures	
TE10.11.01	The tester shall verify that the inhibition of control and data output was performed under TE03.07.01, TE03.07.02, TE03.10.01 and TE03.10.02. The results of the verification shall indicate that: a) the vendor-provided documentation shows that all control and data output via the control and data output interface is inhibited whenever the module is in an error state; b) the module inhibits all control and data output when the module is in an error state.
TE10.11.02	The tester shall verify that the vendor-provided documentation specifies that cryptographic functions are inhibited while the module is in an error state.
TE10.11.03	The tester shall cause the module to enter the error state and verify that any cryptographic operations that the tester attempts to initiate are prevented.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 299 — VE and TE of AS10.12

Self-test general requirements — levels 1, 2, 3 and 4	
AS10.12 ISO/IEC 19790:2025, 7.10.1	The cryptographic module shall not utilize any functionality that relies upon a function or algorithm that failed a self-test until the relevant self-test has been repeated and successfully passed.
Required vendor information	
VE10.12.01	The vendor shall provide design documentation stating that the cryptographic module cannot utilize any functionality that relies upon a function or algorithm that failed a self-test until the relevant self-test has been repeated and successfully passed.
Required test procedures	
TE10.12.01	The tester shall cause an error in a function or algorithm to trigger a failed self-test and initiate a functionality that utilizes the function or algorithm. The tester shall verify that the module cannot utilize this functionality.
TE10.12.02	The tester shall run each self-test and cause the module to enter every error state or a degraded operation. The tester shall exercise the cryptographic module, and verify that the functionality cannot be utilized until the relevant self-test has been repeated and successfully passed.

6.10.2 Security levels 3 and 4

Table 300 — VE and TE of AS10.13

Security levels 3 and 4 — levels 3 and 4	
AS10.13 ISO/IEC 19790:2025, 7.10.2	At security levels 3 and 4, the module shall maintain an error log that contains at a minimum, the most recent error event (i.e. which self-test failed).
Required vendor information	
VE10.13.01	The vendor documentation shall specify the error logging functionality of the module including types of recorded information in the error log (e.g. which self-test has failed, when the error occurred).
Required test procedures	
TE10.13.01	The tester shall verify from the vendor-provided documentation that the error logging functionality provides information, at a minimum, of the most recent error event.
TE10.13.02	The tester shall cause the cryptographic module to enter an error state and verify that the module generates the error log, at a minimum, for the most recent error event.

Table 301 — VE and TE of AS10.14

Security levels 3 and 4 — levels 3 and 4	
AS10.14 ISO/IEC 19790:2025, 7.10.2	The error log shall be protected against unauthorized modification and substitution.
Required vendor information	
VE10.14.01	The vendor-provided documentation shall describe the mechanism that protects against unauthorized modification and substitution.
Required test procedures	
TE10.14.01	The tester shall verify from the vendor-provided documentation that the error log is protected against unauthorized modification and substitution.
TE10.14.02	The tester shall exercise the cryptographic module and verify that the error log is protected against unauthorized modification and substitution.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 302 — VE and TE of AS10.15

Security levels 3 and 4 — levels 1, 2, 3 and 4	
AS10.15 ISO/IEC 19790:2025, 7.10.2	The documentation for self-tests specified in ISO/IEC 19790:2025, A.2.9 shall be provided.
Required test procedures	
This assertion is tested as part of ASA.01.	

6.10.3 Pre-operational self-tests

6.10.3.1 Pre-operational self-test general requirements

Table 303 — VE and TE of AS10.16

Pre-operational self-tests — levels 1, 2, 3 and 4	
AS10.16 ISO/IEC 19790:2025, 7.10.3.1	The pre-operational self-tests shall be performed and passed successfully by a cryptographic module: a) after a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc); b) before the primary, secondary, or backup power is applied to the module; and c) before the module transitions to the operational state.
Required vendor information	
VE10.16.01	The vendor-provided documentation shall provide the information for each of the pre-operational self-tests.
VE10.16.02	The vendor shall provide the sequence of pre-operational self-tests after the module is powered on or instantiated and before the module transitions to the operational state.
Required test procedures	
TE10.16.01	The tester shall verify that the vendor-provided documentation specifies each pre-operational self-test. The tester shall verify that the pre-operational self-tests are performed as specified.
TE10.16.02	By checking the code and design documentation, the tester shall verify each pre-operational test is performed and passed successfully after a cryptographic module is powered on or instantiated and before the module transitions to the operational state.

Table 304 — VE and TE of AS10.17

Pre-operational self-tests — levels 1, 2, 3 and 4	
AS10.17 ISO/IEC 19790:2025, 7.10.3.1	A cryptographic module shall perform the following pre-operational self-tests, as applicable: a) pre-operational software/firmware integrity test; b) pre-operational bypass test; and c) pre-operational critical functions test.
Required test procedures	
This assertion is tested as part of AS10.18, AS10.19, AS10.20, AS10.21, AS10.22, AS10.23 and AS10.24.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.10.3.2 Pre-operational software/firmware integrity test

Table 305 — VE and TE of AS10.18

Pre-operational self-tests — levels 1, 2, 3 and 4	
AS10.18 ISO/IEC 19790:2025, 7.10.3.2	All software, firmware, and bitstream components within the cryptographic boundary shall be verified using an approved integrity technique or EDC satisfying the requirements defined in ISO/IEC 19790:2025, Clause 7.
Required test procedures	
This assertion is tested as part of AS05.12, AS05.13, AS05.14, AS05.15, AS05.16, AS05.17, AS05.18, AS05.19, AS05.20, AS05.21, AS05.22, AS05.23, AS05.24, AS05.25, AS05.26, AS05.27, AS05.28 and AS05.29.	

Table 306 — VE and TE of AS10.19

Pre-operational self-tests — levels 1, 2, 3 and 4	
AS10.19 ISO/IEC 19790:2025, 7.10.3.2	If the verification fails, the pre-operational software/firmware integrity test shall fail.
Required test procedures	
This assertion is not separately tested.	

Table 307 — VE and TE of AS10.20

Pre-operational self-tests — levels 1, 2, 3 and 4	
AS10.20 ISO/IEC 19790:2025, 7.10.3.2	If a hardware module does not contain firmware or bitstream, the module shall, at a minimum, implement one conditional cryptographic algorithm self-test as specified in ISO/IEC 19790:2025, 7.10.4.2 as a pre-operational self-test.
Required test procedures	
This assertion is not separately tested.	

6.10.3.3 Pre-operational bypass test

Table 308 — VE and TE of AS10.21

Pre-operational self-tests — levels 1, 2, 3 and 4	
AS10.21 ISO/IEC 19790:2025, 7.10.3.3	If a cryptographic module implements a bypass capability, then the module shall ensure the correct operation of the logic governing activation of the bypass capability by exercising that logic.
Required vendor information	
VE10.21.01	The vendor-provided documentation shall specify how the cryptographic module ensures the correct operation of the logic governing activation of the bypass capability.
Required test procedures	
TE10.21.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the logic governing activation of the bypass capability is implemented as specified.
TE10.21.02	The tester shall inspect the module and review the vendor-provided documentation to verify that the pre-operational bypass test is implemented to exercise the logic governing activation of the bypass capability.
TE10.21.03	The tester shall cause each error condition of the pre-operational bypass test to occur and shall verify that the inhibition of output is performed when in the resulting error state.
TE10.21.04	The tester shall run the pre-operational bypass test and shall verify that any functionality relies on the logic governing activation of the bypass capability cannot be utilized under TE10.12.01 and TE10.12.02.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 309 — VE and TE of AS10.22

Pre-operational self-tests — levels 1, 2, 3 and 4	
AS10.22 ISO/IEC 19790:2025, 7.10.3.3	The module shall also verify the data path by: a) setting the bypass switch to provide cryptographic processing and verify that data transferred through the bypass mechanism is cryptographically processed; and b) setting the bypass switch so as not to provide cryptographic processing and verify that data transferred through the bypass mechanism is not cryptographically processed.
Required vendor information	
VE10.22.01	The vendor-provided documentation shall specify how to set the bypass switch to provide cryptographic processing.
VE10.22.02	The vendor-provided documentation shall describe how the bypass mechanism is designed to enforce the data transfer of cryptographically processed data through the data path, by setting the bypass switch to provide cryptographic processing.
VE10.22.03	The vendor-provided documentation shall specify how to set the bypass switch so as to not provide cryptographic processing.
VE10.22.04	The vendor-provided documentation shall describe how the bypass mechanism is designed to enforce the data transfer of not cryptographically processed data through the data path by setting the bypass switch to not provide cryptographic processing.
Required test procedures	
TE10.22.01	The tester shall verify by inspection of the module that the module does not provide bypass capability by setting the bypass switch to provide cryptographic processing.
TE10.22.02	By checking either the code or design documentation, or both, the tester shall verify that the implementation of bypass mechanism is consistent with the vendor-provided documentation.
TE10.22.03	By checking either the code or design documentation, or both, the tester shall verify that the module performs the pre-operational bypass test which verifies that the data transferred through the data path is cryptographically processed by setting the bypass switch to provide cryptographic processing.
TE10.22.04	The tester shall verify by inspection of the module that the module provides bypass capability by setting the bypass switch to not provide cryptographic processing.
TE10.22.05	By checking either the code or design documentation, or both, the tester shall verify that the module performs the pre-operational bypass test which verifies that the data transferred through the data path is not cryptographically processed by setting the bypass switch to not provide cryptographic processing.

6.10.3.4 Pre-operational critical functions test

Table 310 — VE and TE of AS10.23

Pre-operational self-tests — levels 1, 2, 3 and 4	
AS10.23 ISO/IEC 19790:2025, 7.10.3.4	There may be other security functions critical to the secure operation of a cryptographic module that shall be tested as a pre-operational test.
Required test procedures	
This assertion is tested as part of AS10.24.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 311 — VE and TE of AS10.24

Pre-operational self-tests — levels 1, 2, 3 and 4	
AS10.24 ISO/IEC 19790:2025, 7.10.3.4	Documentation shall specify the pre-operational critical functions that are tested.
Required vendor information	
VE10.24.01	The vendor shall provide documentation of all critical functions. For each critical function that is tested, the vendor shall indicate: a) the purpose of the critical function; b) which critical functions are tested by which pre-operational self-tests; c) which critical functions are tested by which conditional self-tests.
Required test procedures	
TE10.24.01	The tester shall verify the vendor-provided documentation of the critical functions (pre-operational and conditional) that are tested and the self-tests that are designed to test them. This documentation shall include the following: a) identification and description of all critical functions; b) identification of at least one self-test for every critical function.
TE10.24.02	By checking the code and design documentation, the tester shall verify that the module performs the specified self-tests for each critical function.
NOTE Critical functions are defined as those functions that are not elsewhere defined in ISO/IEC 19790:2025, that, upon failure, can lead to the unauthorized access, use, disclosure, modification, and substitution of SSPs. Examples of critical functions include but not limited to random bit generation, operation of the security function, and cryptographic bypass.	

6.10.4 Conditional self-tests

6.10.4.1 Conditional self-test general requirements

Table 312 — VE and TE of AS10.25

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.25 ISO/IEC 19790:2025, 7.10.4.1	Conditional self-tests shall be performed by a cryptographic module when the conditions specified for the following tests occur: cryptographic algorithm self-test, pair-wise consistency test, software/firmware load test, manual entry test, conditional bypass test and conditional critical functions test.
Required vendor information	
VE10.25.01	The vendor-provided documentation shall provide the information on the conditional self-tests.
Required test procedures	
TE10.25.01	The tester shall verify that the vendor-provided documentation specifies conditional self-tests.
TE10.25.02	The tester shall verify that the conditional self-tests are performed as specified in the vendor-provided documentation.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.10.4.2 Conditional cryptographic algorithm self-test

Table 313 — VE and TE of AS10.26

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.26 ISO/IEC 19790:2025, 7.10.4.2	A cryptographic algorithm self-test shall be conducted for all approved cryptographic algorithms as referenced in ISO ISO/IEC 19790:2025, Annexes C, D and E.
Required vendor information	
VE10.26.01	The vendor-provided documentation shall provide the specification of the conditional cryptographic algorithm self-tests.
VE10.26.02	The vendor shall provide documentation that provides rationale stating how each conditional cryptographic algorithm self-test is performed prior to the first operational use of the cryptographic algorithm.
VE10.26.03	The vendor shall specify whether a known answer test, a comparison test or fault-detection test is used to test the module's cryptographic algorithm. If a comparison test or a fault-detection test, or both, are used, the vendor shall document this fact.
Required test procedures	
TE10.26.01	The tester shall review the vendor-provided documentation and inspect the module to verify that the module conducts a conditional cryptographic algorithm self-test prior to the first operational use of each cryptographic algorithm.

Table 314 — VE and TE of AS10.27

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.27 ISO/IEC 19790:2025, 7.10.4.2	The conditional cryptographic algorithm self-test shall be executed prior to the first operational use of the cryptographic algorithm after power-on, a new instantiation of the module or periodic self-test request.
Required vendor information	
VE10.27.01	The vendor-provided documentation shall specify when conditional cryptographic self-tests are performed by the module.
Required test procedures	
TE10.27.01	The tester shall review the vendor-provided documentation and inspect the module to verify that conditional cryptographic self-tests are performed by the module: a) prior to the first operational use of the cryptographic algorithm after power-on; b) on a new instantiation of the module; c) as triggered by periodic self-test request.

Table 315 — VE and TE of AS10.28

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.28 ISO/IEC 19790:2025, 7.10.4.2	If the calculated output does not equal the known answer, the cryptographic algorithm known-answer self-test shall fail.
Required vendor information	
VE10.28.01	The vendor-provided documentation shall specify the method used to compare the calculated output with the known answer.
VE10.28.02	The documentation shall show the transition into an error state and output of an error indicator when the two outputs are not equal.
Required test procedures	
TE10.28.01	The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.
TE10.28.02	This is tested under TE10.07.02, TE10.10.01, TE10.10.02, and TE10.10.03.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 316 — VE and TE of AS10.29

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.29 ISO/IEC 19790:2025, 7.10.4.2	A cryptographic algorithm self-test that is supported by the module shall, at a minimum, use any approved key length, modulus size, DSA prime, or curve that is supported by the module.
Required vendor information	
VE10.29.01	The vendor-provided documentation shall provide the specification of each conditional cryptographic algorithm self-test that is implemented by the module.
Required test procedures	
TE10.29.01	The tester shall review the vendor-provided documentation and inspect the module to verify that each conditional cryptographic algorithm test uses, at a minimum, at least one of the approved key lengths, modulus sizes, DSA primes, or curves that are supported by the module.

Table 317 — VE and TE of AS10.30

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.30 ISO/IEC 19790:2025, 7.10.4.2	If a cryptographic algorithm specifies multiple modes (e.g. ECB, CBC, etc), at a minimum, one mode shall be selected for the self-test that is supported by the module.
Required test procedures	
This assertion is tested as part of AS10.29.	

Table 318 — VE and TE of AS10.31

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.31 ISO/IEC 19790:2025, 7.10.4.2	One-way functions: Input test vector(s) generate output which shall be identical to expected output [e.g. hashing, keyed hashes, message authentication, RBG (fixed entropy input), SSP agreement].
Required test procedures	
This assertion is tested as part of AS10.28.	

Table 319 — VE and TE of AS10.32

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.32 ISO/IEC 19790:2025, 7.10.4.2	Reversible functions: The forward and reverse function shall be self-tested before each is separately used (e.g. symmetric key encryption and decryption, sensitive security parameter transport encryption and decryption, digital signature generation and verification).
Required test procedures	
This assertion is tested as part of AS10.28.	

Table 320 — VE and TE of AS10.33

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.33 ISO/IEC 19790:2025, 7.10.4.2	if the outputs are not equal, the cryptographic algorithm comparison self-test shall fail.
Required vendor information	
VE10.33.01	The vendor shall describe the implemented cryptographic algorithm comparison self-test.
VE10.33.02	Vendor-provided requirement is specified under VE10.28.01 for the vendor requirement.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 320 *(continued)*

TE10.33.01	The tester shall verify whether the documentation of the comparison test includes: a) use of two or more independent cryptographic algorithm implementations; b) continual comparison of the outputs of the cryptographic algorithm implementation; c) transition into an error state and output of an error indicator when the two outputs are not equal.
TE10.33.02	By checking the code and design documentation, the tester shall verify that the module implements the documented steps for performing the comparison test.

Table 321 — VE and TE of AS10.34

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.34 ISO/IEC 19790:2025, 7.10.4.2	if a fault is detected, the cryptographic algorithm self-test for fault detection shall fail. EXAMPLE The fault-detection test of the RBG will cover an error of the entropy source being correctly handled inside the implementation of the RBG.
Required vendor information	
VE10.34.01	The vendor shall specify whether a fault-detection test is used to test the module's cryptographic algorithm to complement either a known-answer test or a comparison test.
Required test procedures	
TE10.34.01	The tester shall verify the documentation of the fault-detection test includes: a) description of each error condition in the cryptographic algorithm specification/implementation; b) specification of the corresponding (internal) error indicator for each error condition; c) rationale stating each error condition is tested in the fault-detection test.
TE10.34.02	The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.
TE10.34.03	This is tested under TE10.07.02, TE10.07.03, TE10.11.02, TE10.11.03, TE10.12.01, and TE10.12.02.

6.10.4.3 Conditional pair-wise consistency test

Table 322 — VE and TE of AS10.35

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.35 ISO/IEC 19790:2025, 7.10.4.3	If a cryptographic module generates asymmetric key pairs, a pair-wise consistency test shall be performed for every generated asymmetric key pair as referenced in ISO/IEC 19790:2025, Annex C for the applicable cryptographic algorithm.
Required vendor information	
VE10.35.01	If public or private key pairs are used to perform an approved key transport, or an asymmetric cipher, the vendor-provided documentation shall describe the test for pair-wise consistency. This test consists of applying the public key to a plaintext value or to an encoded message. The resulting ciphertext shall be compared to the original plaintext to verify that they differ. a) If the two values are equal, then the cryptographic module shall enter an error state and output an error indicator via the status interface. b) If the two values differ, then the private key shall be applied to the ciphertext. If the result is not equal to the original plaintext, then pair-wise consistency test shall fail.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 322 *(continued)*

VE10.35.02	If public or private key pairs are to be used only for the calculation or verification of digital signatures, the vendor-provided documentation shall describe the test for pair-wise consistency by calculation and verification of a signature. If the signature cannot be verified, the pair-wise consistency test shall fail.
VE10.35.03	If public or private key pairs are used to perform a SSP agreement, the vendor-provided documentation shall describe the test for pair-wise consistency. The vendor-provided documentation shall identify the prerequisite algorithms of the SSP agreement. This test shall consist of applying the key pair to see if it passes the test for pair-wise consistency by exercising the prerequisite algorithms implemented. EXAMPLE The Diffie-Hellman key agreement uses the finite field cryptography primitive common to Digital Signature Algorithm.
Required test procedures	
TE10.35.01	If public or private key pairs are used to perform an approved key transport, or an asymmetric cipher, the tester shall verify that the implementation of the pair-wise consistency test, as defined in VE10.35.01, is consistent with the vendor-provided documentation by checking the code and design documentation.
TE10.35.02	If public or private key pairs are used for the calculation or verification of digital signatures, then the tester shall verify that the implementation of the pair-wise consistency test as defined in VE10.35.02 is consistent with the vendor-provided documentation by checking the code and design documentation.
TE10.35.03	If public or private key pairs are used to perform a SSP agreement, then the tester shall verify that the implementation of the pair-wise consistency test as defined in VE10.35.03 is consistent with the vendor-provided documentation by checking the code and design documentation.
TE10.35.04	If possible, the tester shall modify one of the keys of the key pairs before the pair-wise consistency test is performed. The test has failed if the pair-wise consistency test does not detect the modification.

6.10.4.4 Conditional software/firmware load test

Table 323 — VE and TE of AS10.36

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.36 ISO/IEC 19790:2025, 7.10.4.4	If a cryptographic module has the capability of loading software, firmware, or bitstream from an external source, then the following requirements in addition to those in ISO/IEC 19790:2025, 7.4.3.4 shall be performed:
Required test procedures	
This assertion is not separately tested.	

Table 324 — VE and TE of AS10.37

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.37 ISO/IEC 19790:2025, 7.10.4.4	The cryptographic module shall implement an approved data authentication technique to verify the authenticity of the software, firmware, or bitstream that is loaded;
Required vendor information	
VE10.37.01	The vendor-provided documentation shall describe the approved authentication technique used to protect the integrity of all externally loaded software, firmware and bitstream components.
VE10.37.02	If the module implements an approved authentication technique, the vendor shall provide a validation certificate if available or vendor affirmation as specified in VE02.18.01 and VE02.18.03.
VE10.37.03	The vendor shall provide documentation specifying how the reference authentication key is loaded independently in the module prior to the software, firmware, or bitstream loading.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 324 *(continued)*

VE10.37.04	The vendor-provided documentation shall describe the mechanisms to ensure that the loaded software, firmware, or bitstream cannot be used if the software/firmware load test fails.
Required test procedures	
TE10.37.01	The tester shall determine, from the vendor supplied documentation, which approved authentication technique is used for the software/firmware load test.
TE10.37.02	The tester shall verify that if an approved authentication technique is implemented, the vendor has provided a validation certificate if available or vendor affirmation as specified in VE02.18.01 and VE02.18.03.
TE10.37.03	If the module implements an approved authentication technique for the software/firmware load test, the tester shall verify that the vendor-provided documentation of the software/firmware load test includes: a) specification of the approved authentication technique implemented; b) identification of software and firmware that is protected using the approved authentication technique; c) calculation of the approved authentication technique when the software and firmware is loaded; d) verification of the approved authentication technique when the load test is initiated; e) failure of the self-test upon failure of the approved authentication technique verification.
TE10.37.04	By checking the code and design documentation, the tester shall verify that the implementation of the software/firmware load test is consistent with TE10.37.01, TE10.37.02, and TE10.37.03.
TE10.37.05	The tester shall test the module by modifying the software or firmware to be loaded, or by modifying the implemented authentication mechanism and initiating the self-test. Then the tester shall observe output from the status output interface or through the procedure documented in the non-proprietary security policy to determine if the module has entered an error state. If no indicator is output, explicitly or implicitly, that indicates that the software/firmware load test failed, thus the assertion fails. If it is not possible for the tester to modify the software or firmware to be loaded, or the implemented authentication mechanism, then the vendor shall provide a rationale to the tester as to why this test cannot be performed.
TE10.37.06	The tester shall exercise the cryptographic module, with modifying the software or firmware to be loaded, modifying the reference authentication key, or attempting to bypass the implemented authentication mechanism, and shall initiate the software/firmware load test. After the self-test fails, the tester shall verify that the loaded software or firmware cannot be used and that the module's versioning information is unchanged.
TE10.37.07	By checking the code and design documentation, the tester shall verify that the reference authentication key is loaded independently from the software or firmware loading.
TE10.37.08	By checking the code and design documentation, the tester shall verify that the software/firmware load test fails without loading the reference authentication key prior to the software or firmware loading.
TE10.37.09	If the module allows an operator to load the reference authentication key, the tester shall exercise the cryptographic module, without loading that reference authentication key in advance, and shall initiate the software/firmware load test. If the software/firmware load test passes, the assertion fails. If the factory loaded key cannot be replaced, the assertion passes.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 325 — VE and TE of AS10.38

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.38 ISO/IEC 19790:2025, 7.10.4.4	The reference authentication key shall be loaded independently in the module prior to the software, firmware, or bitstream loading;
Required test procedures	
This assertion is tested as part of AS10.37.	

Table 326 — VE and TE of AS10.39

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.39 ISO/IEC 19790:2025, 7.10.4.4	The applied approved data authentication technique shall be successfully verified or {the software/firmware load test shall fail.}
Required test procedures	
This assertion is tested as part of AS10.37.	

Table 327 — VE and TE of AS10.40

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.40 ISO/IEC 19790:2025, 7.10.4.4	{the software/firmware load test shall fail.} or the software/firmware load test shall fail.
Required test procedures	
This assertion is tested as part of AS10.37.	

Table 328 — VE and TE of AS10.41

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.41 ISO/IEC 19790:2025, 7.10.4.4	Loaded software, firmware, or bitstream shall not be used if the software/firmware load test fails.
Required test procedures	
This assertion is tested as part of AS10.37.	

Table 329 — VE and TE of AS10.42

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.42 ISO/IEC 19790:2025, 7.10.4.4	The software/firmware load test shall be performed and pass successfully prior to the first execution of any new software, firmware or bitstream components.
Required vendor information	
VE10.42.01	The vendor shall provide documentation specifying how the software/firmware load test is performed and passed successfully prior to the first execution of any new software, firmware or bitstream components.
Required test procedures	
TE10.42.01	The tester shall verify that the vendor-provided documentation specifies how the software/firmware load test is performed and passed successfully prior to the first execution of any new software, firmware or bitstream components.
TE10.42.02	The tester shall inspect the module to verify that the software/firmware load test is performed and passed successfully prior to the first execution of any new software, firmware or bitstream components.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.10.4.5 Conditional manual entry test

Table 330 — VE and TE of AS10.43

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.43 ISO/IEC 19790:2025, 7.10.4.5	If SSPs or key components are manually entered directly into a cryptographic module or if an error on the part of the human operator could result in the incorrect entry of the intended value, then the following manual entry tests shall be performed:
Required test procedures	
This assertion is not separately tested.	

Table 331 — VE and TE of AS10.44

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.44 ISO/IEC 19790:2025, 7.10.4.5	The SSP or key components shall have an EDC applied, or {shall be entered using duplicate entries.}
Required test procedures	
This assertion is tested as part of AS10.47.	

Table 332 — VE and TE of AS10.45

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.45 ISO/IEC 19790:2025, 7.10.4.5	{The SSP or key components shall have an EDC applied,} or shall be entered using duplicate entries.
Required test procedures	
This assertion is tested as part of AS10.47.	

Table 333 — VE and TE of AS10.46

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.46 ISO/IEC 19790:2025, 7.10.4.5	If an EDC is used, the EDC shall be at least 16 bits in length.
Required test procedures	
This assertion is tested as part of AS10.47.	

Table 334 — VE and TE of AS10.47

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.47 ISO/IEC 19790:2025, 7.10.4.5	If the EDC cannot be verified, or the duplicate entries do not match, the test shall fail.
Required vendor information	
VE10.47.01	The vendor shall document the manual entry test. Depending on whether error detection codes or duplicate entries of SSPs or key components are used, the manual entry test shall include the following: a) error detection code (EDC): 1) description of the EDC calculation algorithm; 2) description of the verification process; 3) expected outputs for success or failure of the test;

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 334 *(continued)*

	b) duplicate entries: 1) description of the verification process; 2) expected outputs for success or failure of the test.
VE10.47.02	If the EDC is associated with the SSP or key components, then the vendor-provided documentation that describes the format of the SSP or key components (see AS09.03) shall include fields for EDC.
Required test procedures	
TE10.47.01	The tester shall verify from the vendor documentation which method is used for the manual entry test (error detection codes or duplicate entries). Based on the method used, the tester shall check the vendor-provided documentation, code, or design documentation that specifies the implementation of the manual entry test to verify whether the following information is included: a) error detection codes: 1) SSP or key component format for all manually-entered SSPs or key components, including fields for EDC (see AS09.03); 2) description of EDC algorithm; 3) description of EDC verification process; 4) all expected outputs for success or failure of the test; b) duplicate entries of SSPs or key components: 1) duplicate entries for all manually-entered SSPs and key components; 2) description of duplicate entry verification process; 3) all expected outputs for success or failure of the test.
TE10.47.02	For manual entry tests using an EDC, the tester shall review the vendor-provided documentation and inspect the module to verify that the format of the SSP or key components include fields for EDC and that the EDC is at least 16 bits in length.
TE10.47.03	For manual entry tests using an EDC, the tester shall perform the following tests. a) The tester shall enter every manually entered SSP and verify that the procedure used to enter each SSP is in accordance with the documented procedure, including the form that the SSPs are in when they are entered. b) The tester shall enter each type of manually entered SSP without any errors and shall verify the status output interface. If no indicator is output, or if the indicator does not match the documented indicator for the success of the manual entry test, the test has failed. c) The tester shall attempt to perform cryptographic operations with each entered SSP to verify that it was entered correctly.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 334 *(continued)*

	d) The tester shall modify either the EDC associated with each manually entered SSP or the SSP itself and shall enter them into the module. The tester shall verify the indicator that is output from the status output interface; if no indicator is output, or the indicator does not match the documented indicator for the failure of the manual entry test, the test has failed. e) The tester shall attempt to perform cryptographic operations with each SSP that was not successfully entered. Each operation using each SSP is required to fail, verifying that the SSP was not entered.
TE10.47.04	For manual entry tests using duplicate entries of SSPs or key components, the tester shall perform the following tests. a) The tester shall enter each type of manually-entered SSP without any errors and shall verify the status output interface. If no indicator is output, or if the indicator does not match the documented indicator for the success of the manual entry test, the test has failed. b) The tester shall attempt to perform cryptographic operations with each entered SSP to verify that it was entered correctly. c) The tester shall modify one of the manually entered SSPs, either the first or second duplicate entry, and shall enter them into the module. The tester shall verify the indicator that is output from the status output interface; if no indicator is output, or the indicator does not match the documented indicator for the failure of the manual entry test, the test has failed. d) The tester shall attempt to perform cryptographic operations with each SSP that was not successfully entered. Each operation using each SSP is required to fail, verifying that the SSP was not entered.

6.10.4.6 Conditional bypass test

Table 335 — VE and TE of AS10.48

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.48 ISO/IEC 19790:2025, 7.10.4.6	If a cryptographic module implements a bypass capability where the services may be provided without cryptographic processing (e.g. transferring plaintext data through the module), then the following suite of bypass tests shall be performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext data:
Required test procedures	
This assertion is tested as part of AS10.49, AS10.50, AS10.51 and AS10.52.	

Table 336 — VE and TE of AS10.49

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.49 ISO/IEC 19790:2025, 7.10.4.6	A cryptographic module shall test for the correct operation of the services providing cryptographic processing when a switch takes place between an exclusive bypass service and an exclusive cryptographic service;
Required vendor information	
VE10.49.01	If the cryptographic module implements a bypass service, then the vendor shall implement a bypass test to verify the correct operation of the cryptographic service when a switch takes place between an exclusive bypass and an exclusive cryptographic service.
VE10.49.02	The vendor shall provide a description of the bypass test. The bypass test shall demonstrate that, when switched to an exclusive cryptographic service, the module does not output plaintext information.
Required test procedures	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 336 *(continued)*

TE10.49.01	The tester shall verify that the module implements a bypass test to verify the correct operation of the cryptographic service when a switch takes place between an exclusive bypass service and an exclusive cryptographic service.
TE10.49.02	The tester shall verify that the vendor-provided documentation is consistent with the bypass test implementation through a review of the source code and design documentation.
TE10.49.03	The tester shall switch the module from the exclusive bypass service to the exclusive cryptographic service and verify that plaintext information is not output.

Table 337 — VE and TE of AS10.50

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.50 ISO/IEC 19790:2025, 7.10.4.6	If a cryptographic module can automatically alternate between a bypass service and a cryptographic service, providing some services with cryptographic processing and some services without cryptographic processing, then the module shall test for the correct operation of the services providing cryptographic processing when the mechanism governing the switching procedure is modified (e.g. an IP address source/destination table);
Required vendor information	
VE10.50.01	If the cryptographic module is designed to automatically alternate between a bypass service and a cryptographic service, then the vendor shall implement a bypass test to verify the correct operation of the cryptographic service when the mechanism governing the switching procedure is modified.
VE10.50.02	The vendor shall provide a description of the test. The bypass test shall guarantee that when the mechanism governing the switching procedure is modified: a) the mechanism is verified not to have been altered since the last modification. If the mechanism has been altered, the cryptographic module shall enter an error state and output an error indicator to the status interface; b) the correct operation of the cryptographic service is verified by demonstrating that the module does not output plaintext information. The bypass test fails if the data that should be cryptographically processed is output in plaintext.
Required test procedures	
TE10.50.01	The tester shall verify that the module implements a bypass test to verify the correct operation of the cryptographic service when the mechanism governing the switching procedure is modified.
TE10.50.02	The tester shall verify that the description of the test is consistent with the bypass test implementation through the review of the source code and design documentation.
TE10.50.03	The tester shall verify the correct operation of the bypass test by: a) verifying that the mechanism governing the switching procedure checks to ensure that no alteration of the mechanism has taken place since the last modification. The tester will document the method used. If the design allows, the tester shall modify the mechanism to test the method used; b) modifying the mechanism governing the switching procedure in order to verify the correct operation of the mechanism and to verify the correct operation of the cryptographic service by verifying that the plaintext information is not output.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 338 — VE and TE of AS10.51

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.51 ISO/IEC 19790:2025, 7.10.4.6	If a cryptographic module maintains internal information that governs the bypass capability, then the module shall verify the integrity of the governing information through an approved integrity technique immediately preceding modification of the governing information, and {In addition to the requirements at security levels 1 and 2, the module shall repeatedly and automatically, upon a defined time period, without external input or control, perform the pre-operational or conditional cryptographic algorithm self-tests.}
Required test procedures	
This assertion is tested as part of AS10.52.	

Table 339 — VE and TE of AS10.52

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.52 ISO/IEC 19790:2025, 7.10.4.6	If a cryptographic module maintains internal information that governs the bypass capability, then {If the operational time period of a module between resetting, rebooting, or power cycling is sufficiently short, the periodic self-test requirements may be omitted; in this case, the security policy shall document the expected operational time period of the module, and that periodic self-tests are therefore not required.} and shall generate a new integrity value using the approved integrity technique immediately following the modification.
Required vendor information	
VE10.52.01	The vendor-provided documentation shall specify the method to modify the internal information that governs the bypass capability.
VE10.52.02	The vendor shall provide a detailed specification of the internal information that governs the bypass capability, the internal sequence to update the information, and the mechanism to maintain the integrity of the information using an approved integrity technique.
Required test procedures	
TE10.52.01	By checking the code and design documentation, the tester shall verify that the governing information maintained in the cryptographic module is consistent with the vendor-provided documentation.
TE10.52.02	By checking the code and design documentation, the tester shall verify that the internal sequence to update the governing information is consistent with the vendor-provided documentation.
TE10.52.03	By checking the code and design documentation, the tester shall verify that the mechanism to maintain the integrity of the governing information is consistent with the vendor-provided documentation.

6.10.4.7 Conditional critical functions test

Table 340 — VE and TE of AS10.53

Conditional self-tests — levels 1, 2, 3 and 4	
AS10.53 ISO/IEC 19790:2025, 7.10.4.7	There may be other security functions critical to the secure operation of a cryptographic module that shall be tested as a conditional self-test.
Required test procedures	
This assertion is tested as part of AS10.23.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

6.10.4.8 Periodic self-tests

6.10.4.8.1 Security levels 1 and 2

Table 341 — VE and TE of AS10.54

Conditional self-tests — levels 1 and 2	
AS10.54 ISO/IEC 19790:2025, 7.10.4.8.1	A cryptographic module shall permit operators to initiate the pre-operational or conditional cryptographic algorithm self-tests on demand for periodic testing of the module.
Required vendor information	
VE10.54.01	The vendor shall describe the procedure by which an operator can initiate the pre-operational self-tests on demand for periodic testing of the module. All of the pre-operational self-tests shall be included.
VE10.54.02	The vendor shall describe the procedure by which an operator can initiate the conditional cryptographic algorithm self-tests on demand for periodic testing of the module. At a minimum, conditional cryptographic algorithm tests shall be included.
Required test procedures	
TE10.54.01	The tester shall inspect the vendor-provided documentation to verify that initiation of pre-operational self-tests on demand is specified for all of the pre-operational self-tests.
TE10.54.02	The tester shall initiate the pre-operational self-tests on demand to verify that the initiation of the pre-operational self-tests on demand is consistent with the vendor-provided documentation.
TE10.54.03	The tester shall initiate the conditional cryptographic algorithm self-tests on demand to verify that the initiation of the conditional cryptographic algorithm self-tests on demand is consistent with the vendor-provided documentation.

6.10.4.8.2 Security levels 3 and 4

Table 342 — VE and TE of AS10.55

Conditional self-tests — levels 3 and 4	
AS10.55 ISO/IEC 19790:2025, 7.10.4.8.2	In addition to the requirements at security levels 1 and 2, the module shall repeatedly and automatically, upon a defined time period, without external input or control, perform the pre-operational or conditional cryptographic algorithm self-tests.
Required vendor information	
VE10.55.01	The vendor shall provide documentation that specifies how the pre-operational or conditional cryptographic algorithm self-tests are repeatedly performed upon a defined time, automatically, without external input or control.
VE10.55.02	The vendor-provided documentation shall include the specification on the status indicator used to indicate that the cryptographic module's operations are interrupted due to the pre-operational or conditional cryptographic algorithm self-tests.
VE10.55.03	The vendor-provided non-proprietary security policy shall provide the information on the defined time period and any conditions that result in the interruption of the module's operation during the time to repeat pre-operational or conditional cryptographic algorithm self-tests.
Required test procedures	
TE10.55.01	The tester shall verify, by inspection of the cryptographic module, that the pre-operational or conditional cryptographic algorithm self-tests are repeatedly performed as specified in VE10.55.01, VE10.55.02 and VE10.55.03.

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 343 — VE and TE of AS10.56

Conditional self-tests — levels 3 and 4	
AS10.56 ISO/IEC 19790:2025, 7.10.4.8.2	The time period and any conditions that can result in the interruption of the module's operations during the time to repeat the pre-operational or conditional cryptographic algorithm self-tests shall be specified in the security policy.
Required test procedures	
This assertion is tested as part of AS10.55.	

Table 344 — VE and TE of AS10.57

Conditional self-tests — levels 3 and 4	
AS10.57 ISO/IEC 19790:2025, 7.10.4.8.2	If the operational time period of a module between resetting, rebooting, or power cycling is sufficiently short, the periodic self-test requirements may be omitted; in this case, the security policy shall document the expected operational time period of the module, and that periodic self-tests are therefore not required.
Required test procedures	
This assertion is tested as part of ASB.01.	

6.11 Life-cycle assurance

6.11.1 Life-cycle assurance general requirements

Table 345 — VE and TE of AS11.01

Life-cycle assurance general requirements — levels 1, 2, 3 and 4	
AS11.01 ISO/IEC 19790:2025, 7.11.1	The documentation for life-cycle assurance specified in ISO/IEC 19790:2025, A.2.10 shall be provided.
Required vendor information	
VE11.01.01	The vendor shall provide the documentation requirements as specified in ISO/IEC 19790:2025, A.2.10.
Required test procedures	
TE11.01.01	The tester shall verify that the vendor provides documentation as specified in ISO/IEC 19790:2025, A.2.10.

6.11.2 Configuration management

6.11.2.1 Security levels 1 and 2

Table 346 — VE and TE of AS11.02

Configuration management — levels 1, 2, 3 and 4	
AS11.02 ISO/IEC 19790:2025, 7.11.2.2	The following requirements shall apply for security levels 1 and 2.
Required test procedures	
This assertion is tested as part of AS11.03, AS11.04, AS11.05 and AS11.06.	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 347 — VE and TE of AS11.03

Configuration management — levels 1 and 2	
AS11.03 ISO/IEC 19790:2025, 7.11.2.2	A configuration management system shall be used for the development of a cryptographic module and module components within the cryptographic boundary, and of associated module documentation.
Required vendor information	
VE11.03.01	The vendor-provided documentation shall describe the configuration management system for the cryptographic module, module components, and associated module documentation.
Required test procedures	
TE11.03.01	The tester shall verify that the documentation provided by the vendor state that a configuration management system has been implemented.

Table 348 — VE and TE of AS11.04

Configuration management — levels 1, 2, 3 and 4	
AS11.04 ISO/IEC 19790:2025, 7.11.2.2	Each version of each configuration item (e.g. hardware, software, and firmware components, module HDL, user guidance, security policy) that comprises the module and associated documentation shall be assigned and labelled with a unique identifier.
Required vendor information	
VE11.04.01	The vendor cryptographic module documentation shall include a configuration list of all configuration items. The vendor-provided documentation shall describe the method used to uniquely identify the configuration items.
VE11.04.02	The vendor-provided documentation shall describe the method used to uniquely identify the version of each configuration item being validated.
Required test procedures	
TE11.04.01	The tester shall verify that the vendor-provided configuration list includes configuration items.
TE11.04.02	The tester shall verify that the vendor-provided documentation specifies the method used to uniquely identify all configuration items.
TE11.04.03	The tester shall verify that vendor-provided documentation describes the method used to uniquely identify each version of a configuration item being validated.
TE11.04.04	The tester shall verify that vendor-provided documentation uniquely identifies the version of each configuration item being validated.

Table 349 — VE and TE of AS11.05

Configuration management — levels 1, 2, 3 and 4	
AS11.05 ISO/IEC 19790:2025, 7.11.2.2	The configuration management system shall track and maintain the changes to the identification and version or revision of each configuration item throughout the life-cycle of the validated cryptographic module.
Required vendor information	
VE11.05.01	The vendor-provided documentation shall describe how the configuration management system tracks and maintains the changes to the identification and version or revision of each configuration item throughout the life-cycle of the validated cryptographic module.
Required test procedures	
TE11.05.01	The tester shall verify that the vendor-provided documentation specifies the methods used to track and maintain the changes to the identification and version or the revision of each configuration item throughout the life-cycle of the validated cryptographic module.
TE11.05.02	The tester shall inspect the configuration management system to verify that it tracks and maintains the changes to the identification and version or revision of each configuration item throughout the life-cycle of the validated cryptographic module

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 350 — VE and TE of AS11.06

Configuration management — levels 1, 2, 3 and 4	
AS11.06 ISO/IEC 19790:2025, 7.11.2.2	The vendor shall protect confidential module documentation from unauthorized access.
Required vendor information	
VE11.06.01	The vendor-provided documentation shall specify the mechanism and procedure used to protect the confidential module documentation is protected from unauthorized access.
Required test procedures	
TE11.06.01	The tester shall verify the vendor-provided documentation that specifies the mechanism and procedure, such that the confidential module documentation is protected from unauthorized access.

6.11.2.2 Security levels 3 and 4

Table 351 — VE and TE of AS11.07

Configuration management — levels 3 and 4	
AS11.07 ISO/IEC 19790:2025, 7.11.2.3	In addition to the requirements for security levels 1 and 2, the configuration items shall be managed using an automated configuration management system.
Required vendor information	
VE11.07.01	The vendor-provided documentation shall specify how the configuration management system provides an automated means to support the generation of a cryptographic module.
Required test procedures	
TE11.07.01	The tester shall verify that the vendor-provided documentation specifies how the configuration management system provides an automated means to support the generation of a cryptographic module.

6.11.3 Design

Table 352 — VE and TE of AS11.08

Design — levels 1, 2, 3 and 4	
AS11.08 ISO/IEC 19790:2025, 7.11.3	Cryptographic modules shall be designed to allow the testing of all provided security related services.
Required test procedures	
This assertion is not separately tested.	
NOTE This assertion is tested in 6.4.3	

6.11.4 Finite state model

Table 353 — VE and TE of AS11.09

Finite state model — levels 1, 2, 3 and 4	
AS11.09 ISO/IEC 19790:2025, 7.11.4	The operation of a cryptographic module shall be specified using a finite state model (FSM), or equivalent, represented by a state transition diagram and a state transition table and state descriptions.
Required vendor information	

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved

Table 353 *(continued)*

VE11.09.01	The vendor shall provide a description of the finite state model. This description shall contain the identification and description of all states of the module and a description of all corresponding state transitions. The descriptions of the state transitions shall include internal module conditions, data inputs and control inputs that cause transitions from one state to another, data outputs and status outputs resulting from transitions from one state to another.
VE11.09.02	The vendor documentation shall establish a complete description of the following: a) normal operation; b) degraded operation; c) data input interface; d) data output interface; e) control input interface; f) control output interface; g) status output interface; h) plaintext trusted channel; i) crypto-officer and user role; j) other roles (if applicable); k) security services; l) SSP entry services (if applicable); m) show status service; n) operator authentication; o) self-tests; p) other authorized services, operations, and functions (if applicable); q) error states; r) bypass service (if applicable); s) maintenance access interface (if applicable); t) maintenance role (if a maintenance access interface is provided); u) SSP generation and establishment services (if applicable); v) SSP output services (if applicable); w) idle states (if applicable); x) uninitialized states (if applicable).
Required test procedures	
TE11.09.01	The tester shall verify that the vendor has provided a description of the finite state model. This description shall contain the identification and description of all states of the module and a description of all corresponding state transitions. The tester shall verify that the descriptions of the state transitions include the internal module conditions, data inputs and control inputs that cause transitions from one state to another, data outputs, control output and status outputs resulting from transitions from one state to another.
TE11.09.02	The tester shall verify that the finite state model (e.g. state transition diagram, state transition table and state descriptions) are consistent with the vendor-provided documentation that shall describe the following:

STANDARDSISO.COM : Click to view the full PDF of ISO/IEC 24759:2025

© ISO/IEC 2025 – All rights reserved