BS ISO/IEC 24759:2025

BSI Standards Publication

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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24759:2025

National foreword

This British Standard is the UK implementation of ISO/IEC 24759:2025. It supersedes BS ISO/IEC 24759:2017, which is withdrawn.

The UK participation in its preparation was entrusted to Technical Committee IST/33/3, Security Evaluation, Testing and Specification.

A list of organizations represented on this committee can be obtained on request to its committee manager.

Contractual and legal considerations

This publication has been prepared in good faith, however no representation, warranty, assurance or undertaking (express or implied) is or will be made, and no responsibility or liability is or will be accepted by BSI in relation to the adequacy, accuracy, completeness or reasonableness of this publication. All and any such responsibility and liability is expressly disclaimed to the full extent permitted by the law.

This publication is provided as is, and is to be used at the recipient's own risk.

The recipient is advised to consider seeking professional guidance with respect to its use of this publication.

This publication is not intended to constitute a contract. Users are responsible for its correct application.

© The British Standards Institution 2025
Published by BSI Standards Limited 2025

ISBN 978 0 539 16820 4

ICS 35.030

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 March 2025.

Amendments/corrigenda issued since publication

Date	Text affected

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24759:2025

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

Reference number
ISO/IEC 24759:2025(en)

© ISO/IEC 2025

Documents
Document Sharing Hub

Full document details: BS 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

Documents
Document Sharing Hub

Full document details: BS ISO/IEC 24759:2025

Contents

Page

Foreword ... **v**
Introduction ... **vi**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Symbols and abbreviated terms ... **2**
5 Document organization ... **2**
5.1 General ... 2
5.2 Assertions and security requirements ... 3
5.3 Assertions with cross references ... 3
6 Security requirements ... **4**
6.1 General ... 4
6.2 Cryptographic module specification ... 5
6.2.1 Cryptographic module specification general requirements ... 5
6.2.2 Types of cryptographic modules ... 5
6.2.3 Cryptographic boundary ... 6
6.2.4 Module operations ... 16
6.3 Cryptographic module interfaces ... 23
6.3.1 Cryptographic module interfaces general requirements ... 23
6.3.2 Categories of interfaces ... 26
6.3.3 Plaintext trusted path ... 35
6.3.4 Protected internal paths ... 38
6.4 Roles, services, and authentication ... 39
6.4.1 Roles, services, and authentication general requirements ... 39
6.4.2 Roles ... 40
6.4.3 Services ... 41
6.4.4 Authentication ... 49
6.5 Software/firmware security ... 59
6.5.1 Software/firmware security general requirements ... 59
6.5.2 Security level 1 ... 62
6.5.3 Security level 2 ... 67
6.5.4 Security levels 3 and 4 ... 68
6.6 Operational environment ... 69
6.6.1 Operational environment general requirements ... 69
6.6.2 Clause applicability ... 70
6.6.3 Operating system requirements for modifiable operational environments ... 71
6.7 Physical security ... 83
6.7.1 Physical security embodiments ... 83
6.7.2 Physical security general requirements ... 84
6.7.3 Physical security requirements for each physical security embodiment ... 95
6.7.4 Environmental failure protection/testing ... 100
6.7.5 Environmental failure protection features ... 100
6.7.6 Environmental failure testing procedures ... 101
6.8 Non-invasive security ... 104
6.8.1 Non-invasive security general requirements ... 104
6.8.2 Security levels 1 and 2 ... 104
6.8.3 Security level 3 ... 105
6.8.4 Security level 4 ... 105
6.9 Sensitive security parameter management ... 106
6.9.1 Sensitive security parameter management general requirements ... 106
6.9.2 Random bit generators ... 108
6.9.3 Sensitive security parameter generation ... 110
6.9.4 Automated sensitive security parameter establishment ... 110

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

6.9.5 Sensitive security parameter entry and output 111
6.9.6 Sensitive security parameter storage 117
6.9.7 Sensitive security parameter zeroization 118
6.10 Self-tests 122
6.10.1 Self-test general requirements 122
6.10.2 Security levels 3 and 4 126
6.10.3 Pre-operational self-tests 127
6.10.4 Conditional self-tests 130
6.11 Life-cycle assurance 143
6.11.1 Life-cycle assurance general requirements 143
6.11.2 Configuration management 143
6.11.3 Design 145
6.11.4 Finite state model 145
6.11.5 Development 149
6.11.6 Vendor testing 155
6.11.7 Delivery and operation 157
6.11.8 Guidance documents 160
6.12 Mitigation of other attacks 161
6.12.1 Mitigation of other attacks general requirements 161
6.12.2 Security levels 1, 2 and 3 161
6.12.3 Security level 4 161

7 Documentation requirements 162
7.1 Purpose 162
7.2 Items 163
7.2.1 Cryptographic module specification 163
7.2.2 Cryptographic module interfaces 164
7.2.3 Roles, services, and authentication 164
7.2.4 Software/Firmware security 165
7.2.5 Operational environment 165
7.2.6 Physical security 166
7.2.7 Non-invasive security 167
7.2.8 Sensitive security parameter management 167
7.2.9 Self-tests 169
7.2.10 Life-cycle assurance 169
7.2.11 Mitigation of other attacks 171

8 Cryptographic module security policy 172
8.1 General 172
8.2 Items 173
8.2.1 General 173
8.2.2 Cryptographic module specification 174
8.2.3 Cryptographic module interfaces 175
8.2.4 Roles, services, and authentication 175
8.2.5 Software/Firmware security 176
8.2.6 Operational environment 177
8.2.7 Physical security 178
8.2.8 Non-invasive security 179
8.2.9 Sensitive security parameters management 179
8.2.10 Self-tests 180
8.2.11 Life-cycle assurance 180
8.2.12 Mitigation of other attacks 181

Bibliography 182

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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

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

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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 "}".

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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;

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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;

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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:

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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).	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.	

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025

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.

© ISO/IEC 2025 – All rights reserved

Documents
Document Sharing Hub
Full document details: BS ISO/IEC 24759:2025