FINAL DRAFT
International
Standard

ISO/IEC FDIS 24759

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

ISO/IEC JTC 1/SC 27

Secretariat: **DIN**

Voting begins on:
2024-11-26

Voting terminates on:
2025-01-21

RECIPIENTS OF THIS DRAFT ARE INVITED TO SUBMIT, WITH THEIR COMMENTS, NOTIFICATION OF ANY RELEVANT PATENT RIGHTS OF WHICH THEY ARE AWARE AND TO PROVIDE SUPPORTING DOCUMENTATION.

IN ADDITION TO THEIR EVALUATION AS BEING ACCEPTABLE FOR INDUSTRIAL, TECHNOLOGICAL, COMMERCIAL AND USER PURPOSES, DRAFT INTERNATIONAL STANDARDS MAY ON OCCASION HAVE TO BE CONSIDERED IN THE LIGHT OF THEIR POTENTIAL TO BECOME STANDARDS TO WHICH REFERENCE MAY BE MADE IN NATIONAL REGULATIONS.

Reference number
ISO/IEC FDIS 24759:2024(en)

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

Published in Switzerland

Contents

Page

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:—; 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.

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:—.

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:—.[1] 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:—.

Vendors can also use this document to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:— 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:—[1], *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

[1] Under preparation. Stage at the time of publication: ISO/IEC FDIS 19790:2024.

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:—. Clause 7 corresponds to ISO/IEC 19790:—, Annex A, and Clause 8 corresponds to ISO/IEC 19790:—, Annex B.

ISO/IEC 19790:—, 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:— 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:—, 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:— 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:— (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 "}".

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:—, 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:—, 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:—, 7.1	The cryptographic module level shall be independently determined in each area.
Required test procedures	
This assertion is not separately tested.	

Table 4 — VE and TE of AS01.04

General — levels 1, 2, 3 and 4	
AS01.04 ISO/IEC 19790:—, 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:—, 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:—, 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:—, 7.2.1	The documentation for cryptographic module specification specified in ISO/IEC 19790:—, 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:—, 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.

Table 8 — VE and TE of AS02.04

Types of cryptographic modules — levels 1, 2, 3 and 4	
AS02.04 ISO/IEC 19790:—, 7.2.2	For hardware, firmware or hybrid firmware modules, the applicable physical security and non-invasive security requirements specified in ISO/IEC 19790:—, 7.7 and ISO/IEC 19790:—, 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:—, 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:—, 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:—, 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:-, 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.

Table 12 — VE and TE of AS02.08

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.08 ISO/IEC 19790:—, 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:—, 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:—, 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.

Table 15 — VE and TE of AS02.11

Cryptographic boundary — levels 1, 2, 3 and 4	
AS02.11 ISO/IEC 19790:—, 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.