INTERNATIONAL STANDARD

ISO/IEC 24759

Second edition
2014-02-01

Information technology — Security techniques — Test requirements for cryptographic modules

Technologies de l'information — Techniques de sécurité — Exigences d'essai pour modules cryptographiques

Reference number
ISO/IEC 24759:2014(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web 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. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of the joint technical committee is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights.

ISO/IEC 24759 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This second edition cancels and replaces the first edition (ISO/IEC 24759:2008), which has been technically revised.

Information technology — Security techniques — Test requirements for cryptographic modules

1 Scope

This International Standard specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This International Standard also specifies the requirements for information that vendors provide to testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2012.

Vendors can use this International Standard as guidance in trying to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2012 before they apply to the testing laboratory for testing.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19790:2012 apply.

4 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 19790:2012 apply.

5 Document organization

5.1 General

Clause 6 of this document specifies the methods that shall be used by testing laboratories and the requirements for information that vendors shall provide to testing laboratories. Clause 6, besides a general subclause 6.1, includes eleven subclauses corresponding to the eleven areas of security requirements and six subclauses corresponding to the six Annexes A to F of ISO/IEC 19790:2012.

5.2 Assertions and security requirements

Within each subclause, the corresponding security requirements from ISO/IEC 19790:2012 are divided into a set of assertions (i.e., statements that have to 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 19790:2012.

The assertions are denoted by the form

AS<requirement_number>.<assertion_sequence_number>

where "requirement_number" is the number of the corresponding area specified in ISO/IEC 19790:2012 (i.e., one through twelve and A through F), 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 through 4) are listed in parentheses.

Following each assertion 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.

Also following each assertion and the requirements levied on the vendor is 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.

A validation authority may modify, add or delete VEs and/or TEs in this international standard.

5.3 Assertions with cross references

For clarity in some assertions, cross references to ISO/IEC 19790:2012 or other assertions numbers have been put between curly brackets "*{*" and "*}*". Those cross references are written in italics.

6 Security requirements

6.1 General

AS01.01: (Specification – Levels 1, 2, 3, and 4)

This clause specifies the security requirements that shall be satisfied by the cryptographic module's compliance to this International Standard.

NOTE This subclause states general requirements to meet the assertions of the other subclauses in clause 6, and A through F. This subclause sets no assertion of itself and is not separately tested.

AS01.02: (Specification – Levels 1, 2, 3, and 4)

A cryptographic module shall be tested against the requirements of each area addressed in this clause.

NOTE 1 The tests can be performed in one or more of the following manners:

a) Tester performs tests at the tester's facility

b) Tester performs tests at the vendor's facility

c) Tester supervises vendor performing tests at the vendor's facility

1) Rationale is included that explains why tester could not perform the tests

2) Tester develops the required test plan and required tests

3) Tester directly observes the tests being performed

An assertion fails if any of its subsequent tests fails.

NOTE 2 This subclause states general requirements to meet the assertions of the other subclauses in clause 6. This subclause sets no assertion of itself and is not separately tested.

AS01.03: (Specification – Levels 1, 2, 3, and 4)

The cryptographic module shall be independently rated in each area.

NOTE This subclause states general requirements to meet the assertions of the other subclauses in clauses 6 and A through F. This subclause sets no assertion of itself and is not separately tested.

AS01.04: (Specification – Levels 1, 2, 3, and 4)

All documentation, including copies of the user and installation manuals, design specifications, life-cycle documentation shall be provided for a cryptographic module that is to undergo an independent verification or evaluation scheme.

NOTE This subclause states general requirements to meet the assertions of the other subclauses in clauses 6 and A through F. This subclause sets no assertion of itself and is not separately tested.

6.2 Cryptographic module specification

6.2.1 Cryptographic module specification general requirements

AS02.01: (Specification – Levels 1, 2, 3, and 4)

A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof, that at a minimum, implements a defined cryptographic service employing an approved cryptographic algorithm, security function or process and contained within a defined cryptographic boundary.

NOTE This assertion is not separately tested.

AS02.02: (Specification – Levels 1, 2, 3, and 4)

The documentation requirements specified in *{ISO/IEC 19790:2012 Annex}* A.2.2 shall be provided.

NOTE This assertion is tested as part of ASA.01.

6.2.2 Types of cryptographic modules

AS02.03: (Specification – Levels 1, 2, 3, and 4)

A cryptographic module shall be defined as one of the following module types:

— ***Hardware module* is a module whose cryptographic boundary is specified at a hardware perimeter. Firmware and/or software, which may also include an operating system, may be included within this hardware cryptographic boundary.**

— ***Software module* is a module whose cryptographic boundary delimits the software exclusive component(s) (may be one or multiple software components) that execute(s) in a modifiable operational environment. The computing platform and operating system of the operational environment which the software executes in are external to the defined software module boundary.**

— ***Firmware module*** **is a module whose cryptographic boundary delimits the firmware exclusive component(s) that execute(s) in a limited or non-modifiable operational environment. The computing platform and operating system of the operational environment which the firmware executes in are external to the defined firmware module boundary but explicitly bound to the firmware module.**

— ***Hybrid Software module*** **is a module whose cryptographic boundary delimits the composite of a software component and a disjoint hardware component (i.e. the software component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment which the software executes in are external to the defined hybrid software module boundary.**

— ***Hybrid Firmware module*** **is a module whose cryptographic boundary delimits the composite of a firmware component and a disjoint hardware component (i.e. the firmware component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment which the firmware executes in are external to the defined hybrid firmware module boundary but explicitly bound to the hybrid firmware 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, software and/or firmware components of the cryptographic module.

Required Test Procedures

TE02.03.01: The tester shall verify that the vendor provided documentation identifies one of the module types listed in AS02.03.

TE02.03.02: The tester shall verify from the vendor provided specification documentation, by identifying all hardware, software and/or firmware components (AS02.15 through AS02.18), that the cryptographic module is consistent with the type of the cryptographic module.

AS02.04: (Specification – Levels 1, 2, 3, and 4)

For hardware and firmware modules, the physical security and non-invasive security requirements found in *{ISO/IEC 19790:2012 subclause}* 7.7 and 7.8 shall apply.

NOTE This assertion is not tested separately.

AS02.05: (Specification – Levels 1, 2, 3, and 4)

For hybrid modules, the software and firmware component(s) shall meet all applicable requirements of *{ISO/IEC 19790:2012 subclause}* 7.5 and 7.6.

NOTE This assertion is not tested separately.

AS02.06: (Specification – Levels 1, 2, 3, and 4)

{For hybrid modules} **The hardware component(s) shall meet all applicable requirements of *{ISO/IEC 19790:2012 subclause}* 7.7 and 7.8.**

NOTE This assertion is not tested separately.

6.2.3 Cryptographic boundary

6.2.3.1 Cryptographic boundary general requirements

AS02.07: (Specification – Levels 1, 2, 3, and 4)

The 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

VE02.07.01: The vendor documentation shall specify all components within the cryptographic boundary.

Required Test Procedures

TE02.07.01: The tester shall verify by inspection and from the vendor documentation that all the components specified in AS02.15 through AS02.18 are within the cryptographic boundary.

TE02.07.02: The tester shall verify by inspection and from the vendor documentation that there are no unidentified components which are not specified in AS02.15 through AS02.18 within the cryptographic boundary.

AS02.08: (Specification – Levels 1, 2, 3, and 4)

The requirements of this International Standard shall apply to all algorithms, security functions, processes and components within the module's cryptographic boundary.

NOTE This assertion is not tested separately.

AS02.09: (Specification – Levels 1, 2, 3, and 4)

The cryptographic boundary shall, at a minimum, encompass all security relevant algorithms, security functions, processes and components of a cryptographic module (i.e., security relevant within the scope of this International Standard).

Required Vendor Information

VE02.09.01: The vendor shall provide a list of all the security relevant algorithms, security functions, processes and components within the cryptographic boundary.

Required Test Procedures

TE02.09.01: The tester shall verify that the vendor provided documentation clearly identifies and lists all the security relevant algorithms, security functions, processes and components of the module within the cryptographic boundary.

AS02.10: (Specification – Levels 1, 2, 3, and 4)

Non-security relevant algorithms, security functions, processes or components which are used in an approved mode of operation shall be implemented in a manner to not interfere or compromise the approved operation of the cryptographic module.

Required Vendor Information

VE02.10.01: The vendor provided documentation shall list the non-security relevant functions used in an approved mode of operation and justify that they are not interfering with the approved mode of operation of the module.

Required Test Procedures

TE02.10.01: The tester shall verify through documentation review and inspection of the module that the non-security relevant functions are not interfering or compromising the approved mode of operation of the module.

TE02.10.02: The tester shall verify the correctness of any rationale for not interfering nor compromising provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.

AS02.11: (Specification – Levels 1, 2, 3, and 4)

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

VE02.11.01: The vendor shall provide the defined name of the module.

Required Test Procedures

TE02.11.01: The tester shall verify that the vendor provided module name is consistent with the composition of the components within the cryptographic boundary.

TE02.11.02: The tester shall verify that the module name does not represent a compostion of components or functions that are not consistent with the composition of the components within the cryptographic boundary.

AS02.12: (Specification – Levels 1, 2, 3, and 4)

The cryptographic module shall have, at minimum, specific versioning information representing the distinct individual hardware, software and/or firmware components.

Required Vendor Information

VE02.12.01: The vendor shall provide the versioning information of the modules distinct individual hardware, software and/or firmware components.

Required Test Procedures

TE02.12.01: The tester shall verify the versioning information represents the modules distinct individual hardware, software and/or firmware components.

AS02.13: (Specification – Levels 1, 2, 3, and 4)

The excluded hardware, software or firmware components shall be implemented in a manner to not interfere or compromise the approved secure operation of the cryptographic module.

Required Vendor Information

VE02.13.01: The vendor shall describe the excluded components of the module which are not within the cryptographic module and justify that these components will not interfere with the approved mode of operation of the module.

Required Test Procedures

TE02.13.01: The tester shall verify from the vendor provided documentation that the excluded components of the cryptographic boundary will not interfere with the approved mode of operation of the module.

AS02.14: (Specification – Levels 1, 2, 3, and 4)

The excluded hardware, software or firmware shall be specified *{ ISO/IEC 19790:2012}* (Annex A).

Required Vendor Information

VE02.14.01: All components that are to be excluded from the security requirements shall be explicitly listed in the vendor documentation.

VE02.14.02: The vendor documentation shall provide the rationale for excluding each of the components listed in response to requirement VE02.13.01. The vendor shall show that each component, even if malfunctioning or misused, cannot cause a compromise.

Required Test Procedures

TE02.14.01: The tester shall verify whether the vendor indicates that any components of the module are to be excluded from the requirements of ISO/IEC 19790:2012.

TE02.14.02: If the vendor has indicated that certain components of the module are to be excluded from the requirements of ISO/IEC 19790:2012, the tester shall verify that a rationale for each exclusion is provided. The rationale has to show that even if the component malfunctions, it cannot cause a potential release of , plaintext data, or other information that if misused could lead to a compromise. Rationale that may be acceptable, if adequately supported by documentation, includes:

a) The component does not process SSPs, plaintext data, or other information that if misused could lead to a compromise

b) 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 if misused could lead to a compromise

c) All information processed by the component is strictly for internal use of the module, and does not in any way impact the equipment to which the module is connected

TE02.14.03: 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 require the vendor to produce additional information as needed.

6.2.3.2 Definitions of cryptographic boundary

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

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

— **The set of hardware components which may include:**

  — **physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between components,**

  — **active electrical components such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc.**

  — **physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces,**

  — **firmware, which may include an operating system,**

  — **other components types not listed above.**

Required Vendor Information

VE02.15.01: All hardware components of the cryptographic module shall be identified in the vendor documentation. Components 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 components.

   1) circuit boards, substrates and mounting surfaces.

b) Active electrical components 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 manufactuer 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 components, including power supply, voltage conversion modules (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 do not need 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 may include an operating system,

1) Executable code:

i) Non-modifiable

ii) Modifiable

e) Other components 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.

VE02.15.02: The vendor 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.

VE02.15.03: The vendor documentation shall describe the primary physical parameters of the module, including descriptions of the enclosure, access points, circuit boards, location of power supply, interconnection wiring runs, cooling arrangements, and any other significant parameters.

VE02.15.04: The vendor documentation shall include a block diagram which represents the module's boundary and relationship of the hardware components.

Required Test Procedures

TE02.15.01: The tester shall identify all hardware components of the cryptographic module. Components 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 components.

   1) circuit boards, substrates and mounting surfaces.

b) Active electrical components 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 manufactuer 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 components, including power supply, voltage conversion modules (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 do not need 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 may include an operating system,

   1) Executable code:

      i) Non-modifiable

      ii) Modifiable

e) Other components 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.

TE02.15.02: The tester shall verify that the components list is consistent with information provided for other assertions of this subclause, as defined below:

a) The specification of the cryptographic boundary under assertion AS02.07. Verify that all components inside the cryptographic boundary are included in the components list and vice versa. Also verify