INTERNATIONAL STANDARD

ISO/IEC 24759

First edition
2008-07-01

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 24759:2008(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*.

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 19790:2006. 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' conformance to the requirements specified in ISO/IEC 19790:2006.

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

2 Normative references

The following referenced documents are indispensable for the application 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 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

ISO/IEC 18031:2005, *Information technology — Security techniques — Random bit generation*

ISO/IEC 19790:2006, *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 and the following apply.

NOTE Definitions followed by a reference in square brackets are taken verbatim from ISO/IEC 19790:2006. All other terms and definitions are adapted from those in ISO/IEC 19790:2006.

3.1
approval authority
any national or international organization/authority mandated to approve and/or evaluate security functions

[ISO/IEC 19790:2006, 3.1]

NOTE An approval authority in the context of this definition evaluates and approves security functions based on their cryptographic or mathematical merits but is not the testing entity which would test for conformance to this International Standard and ISO/IEC 19790:2006.

3.2
ISO/IEC approved
security function that is either

— specified in an ISO/IEC standard, or

— adopted/recommended in an ISO/IEC standard and specified either in an annex of the ISO/IEC standard or in a document normatively referenced by the ISO/IEC standard

3.3
asymmetric cryptographic technique
cryptographic technique that uses two related transformations; public transformation (defined by the public key) and private transformation (defined by the private key)

NOTE The two transformations have the property that, given the public transformation, it is computationally infeasible to derive the private transformation in a given limited timeframe and with given computational resources.

3.4
compromise
unauthorized disclosure, modification, substitution, or use of critical security parameters (ISO/IEC 19790:2006, 3.13) or the unauthorized modification or substitution of public security parameters (ISO/IEC 19790:2006, 3.58)

3.5
cryptographic module security policy
security policy
precise specification of the security rules under which a cryptographic module shall operate, including the rules derived from the requirements of this International Standard and additional rules imposed by the module

[ISO/IEC 19790:2006, 3.18]

NOTE See ISO/IEC 19790:2006, Annex B.

3.6
crypto officer
role taken by an individual or a process (i.e. subject) acting on behalf of an individual, allowing to perform cryptographic initialization or management functions of a cryptographic module

[ISO/IEC 19790:2006, 3.19]

3.7
firmware
programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution

[ISO/IEC 19790:2006, 3.31]

EXAMPLE Storage hardware may include but is not limited to ROM, PROM, EEPROM, or FLASH.

3.8
input data
information that is entered into a cryptographic module and may be used for the purposes of transformation or computation using an approved security function

[ISO/IEC 19790:2006, 3.33]

3.9
maintenance role
role assumed to perform physical maintenance and/or logical maintenance services

[ISO/IEC 19790:2006, 3.41]

EXAMPLE Maintenance services may include but are not limited to hardware and/or software diagnostics.

3.10
passivation
effect of a reactive process in semiconductor junctions, surfaces or components and integrated circuits constructed to include means of detection and protection

NOTE 1 Silicon dioxide and phosphorus glass are examples of passivation material.

NOTE 2 Passivation can modify the behaviour of the circuit. Passivation material is technology dependent.

3.11
public key
that key of an entity's asymmetric key pair which can be made public

[ISO/IEC 19790:2006, 3.56]

NOTE In the case of an asymmetric signature system, the public key defines the verification transformation. In the case of an asymmetric encipherment system, the public key defines the encipherment transformation. A key that is "publicly known" is not necessarily globally available. The key may only be available to members of a pre-specified group.

3.12
random bit generator
RBG
device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased

[ISO/IEC 19790:2006, 3.59]

NOTE See ISO/IEC 18031:2005.

3.13
role
security attribute associated to a user defining the user access rights or limitations to services of a cryptographic module

NOTE One or more services may be associated to a role. A role may be associated to one or more users and a user may assume one or more roles.

3.14
security function
cryptographic algorithms together with modes of operation, such as block ciphers, stream ciphers, asymmetric key, message authentication codes, hash functions, or other security functions, random bit generators, entity authentication and key establishment all approved either by ISO/IEC or an approval authority

[ISO/IEC 19790:2006, 3.63]

NOTE See ISO/IEC 19790:2006, Annex D.

3.15
seed key
secret value which can be used to initialize a random bit generator

3.16
simple power analysis
SPA
direct analysis (primarily visual) of patterns of instruction execution (or execution of individual instructions), in relation to the electrical power consumption of a cryptographic module, for the purpose of extracting information correlated to a cryptographic operation

3.17
software
programs and data components within the cryptographic boundary and usually stored on erasable media which can be dynamically written and modified during execution

[ISO/IEC 19790:2006, 3.66]

EXAMPLE Erasable media may include but are not limited to hard drives.

3.18
split knowledge
process by which a cryptographic key is split into multiple key components, individually sharing no knowledge of the complete key, that can be subsequently input into, or output from, a cryptographic module by separate entities and combined to recreate the original cryptographic key

NOTE All or a subset of the components may be required to perform the combination.

3.19
system software
general purpose software within the cryptographic boundary designed to facilitate the operation of the cryptographic module

[ISO/IEC 19790:2006, 3.70]

EXAMPLES Operating system, compilers or utility programs.

3.20
tamper evidence
observable indication that an attempt has been made to compromise the security of a cryptographic module

4 Abbreviated terms

API Application Program Interface

CAPP Controlled Access Protection Profile

CBC Cipher Block Chaining

CC Common Criteria, equivalent to ISO/IEC 15408

CSP Critical Security Parameter

EAL Evaluation Assurance Level

EDC Error Detection Code

EFP Environmental Failure Protection

EFT Environmental Failure Testing

FSM Finite State Model

HDL Hardware Description Language

IC Integrated Circuit

KEK Key Encryption Key

PIN Personal Identification Number

PROM Programmable Read-Only Memory

PSP Public Security Parameter

RAM Random Access Memory

RBG Random Bit Generator

ROM Read-Only Memory

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 seventeen subclauses, corresponding to the ten areas of security requirements plus annexes A to G of ISO/IEC 19790:2006. Subclauses 6.14 to 6.18 are stating no requirements.

5.2 Assertions and security requirements

Within each subclause of clause 6, the corresponding security requirements from ISO/IEC 19790 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 19790:2006.

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 (i.e., one through ten) eleven corresponding Annex A of ISO/IEC 19790 and twelve corresponding Annex B of ISO/IEC 19790, 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 conformance 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.

5.3 Assertions with cross references

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

6 Security requirements

6.1 General test requirements

A module is to be tested against the requirements of each area addressed in this clause. The cryptographic module is to be independently rated in each area.

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

1. Tester performs tests at the tester’s facility
2. Tester performs tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility

- Rationale is included that explains why tester could not perform the tests
- Tester develops the required test plan and required tests
- Tester directly observes the tests being performed

An assertion fails if any of its subsequent tests fails.

NOTE 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.

6.2 Cryptographic module specification

AS01.01: (Specification – Levels 1, 2, 3, and 4)
A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, and is contained within a defined cryptographic boundary.

NOTE This assertion is not separately tested.

AS01.02: (Specification – Levels 1, 2, 3, and 4)
A cryptographic module shall implement at least one approved security function used in an approved mode of operation.

NOTE 1 This assertion is tested as part of AS01.12.

NOTE 2 Approved security functions are listed at Annex D (informative) of ISO/IEC 19790:2006.

AS01.03: (Specification – Levels 1, 2, 3, and 4)
The operator shall be able to determine when an approved mode of operation is selected.

Required Vendor Information

VE01.03.01: The vendor provided non-proprietary security policy shall provide a description of the approved mode of operation.

VE01.03.02: The vendor provided non-proprietary security policy shall provide instructions for invoking the approved mode of operation.

Required Test Procedure

TE01.03.01: The tester shall verify that the vendor provided non-proprietary security policy contains a description of the approved mode of operation.

TE01.03.02: The tester shall invoke the approved mode of operation using the vendor provided instructions found in the non-proprietary security policy.

AS01.04: (Specification – Levels 3 and 4)
For Security Levels 3 and 4, a cryptographic module shall indicate when an approved mode of operation is selected.

Required Vendor Information

VE01.04.01: The vendor provided non-proprietary security policy shall provide a description of the method used to indicate when a cryptographic module is in an approved mode of operation.

VE01.04.02: The vendor provided non-proprietary security policy shall provide instructions for obtaining the approved mode of operation indicator.

Required Test Procedures

TE01.04.01: The tester shall verify that the vendor provided non-proprietary security policy contains a description of the method used to indicate when a cryptographic module is in an approved mode of operation.

TE01.04.02: The tester shall use the vendor provided instructions described in the non-proprietary security policy to obtain the approved mode of operation indicator.

AS01.05: (Specification – Levels 1, 2, 3, and 4)
The cryptographic boundary shall consist of an explicitly defined perimeter that establishes the physical and/or logical bounds of a cryptographic module.

NOTE This assertion is tested as part of AS01.08.

AS01.06: (Specification – Levels 1, 2, 3, and 4)
If a cryptographic module consists of software or firmware components, the cryptographic boundary shall contain the processor(s) and other hardware components that store and protect the software and firmware components.

NOTE Hardware, software, and firmware components of a cryptographic module can be excluded from the requirements of ISO/IEC 19790 if shown that these components do not affect the security of the module.

Required Vendor Information

VE01.06.01: For each processor in the module, the vendor shall identify, by major services, the software or firmware that are executed by the processor, and the memory devices that contain the executable code and data.

VE01.06.02: For each processor, the vendor shall identify any hardware with which the processor interfaces.

Required Test Procedures

TE01.06.01: The tester shall verify that each processor identified under this assertion is both contained in the components list under assertion AS01.08 and in the cryptographic boundary defined under assertion AS01.08.

TE01.06.02: 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.

TE01.06.03: The tester shall verify that, for each processor, the vendor has identified any hardware with which the processor interfaces. This includes, as applicable, any hardware components that provide input, control, or status data to the processor and associated software/firmware, and any hardware components that receive output, control, or status data from the processor and associated software/firmware. Such hardware components may be within the cryptographic module, or may be user equipment outside the module such as input/output devices.

AS01.07: (Specification – Levels 1, 2, 3, and 4)
The following documentation requirements *{AS01.08 to AS01.17}* shall apply to all security-specific hardware, software, and firmware contained within a cryptographic module.

NOTE This assertion is not separately tested.

AS01.08: (Specification – Levels 1, 2, 3, and 4)
Documentation shall specify the hardware, software, and firmware components of a cryptographic module, specify the cryptographic boundary surrounding these components, and describe the physical configuration of the module (see *{sub}*clause 7.5 *{of ISO/IEC 19790:2006}*).

Required Vendor Information

VE01.08.01: All hardware, software, and firmware components of the cryptographic module shall be identified in the vendor documentation. Components to be listed shall include all of the following:

1. Integrated circuits, including processors, memory, and (semi-) custom integrated circuits
2. Other active electronic circuit elements
3. Power inputs and outputs, and internal power supplies or converters
4. Physical structures, including circuit boards or other mounting surfaces, enclosures, and connectors
5. Software and firmware modules
6. Other security relevant component types not listed above

VE01.08.02: The above list of components shall be consistent with the information provided for all other assertions in subclause 6.2 of this International Standard.

VE01.08.03: The vendor documentation shall specify the module's cryptographic boundary. The cryptographic boundary shall be an explicitly defined, contiguous perimeter that establishes the physical bounds of the cryptographic module. The boundary definition shall specify module components and connections (ports), and also module information flows, processing, and input/output data.

VE01.08.04: The cryptographic boundary shall include any hardware or software that inputs, processes, or outputs important security parameters that could lead to the compromise of sensitive information if not properly controlled.

VE01.08.05: The vendor documentation shall specify the physical embodiments of the module – single-chip cryptographic module, multiple-chip embedded cryptographic module, or multiple-chip standalone cryptographic module, as defined in subclause 7.5 of ISO/IEC 19790:2006.

VE01.08.06: 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. The interior of integrated circuits need not be shown.

VE01.08.07: 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.

Required Test Procedures

TE01.08.01: The tester shall verify that the documentation includes a components list that includes all hardware, software, and firmware components of the cryptographic module.

TE01.08.02: The tester shall verify that the components list includes all occurrences of the following types of components, excluding only component types that are not used in the module:

1. Processors, including microprocessors, digital signal processors, custom processors, microcontrollers, or any other types of processors.

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. Other active electronic circuit elements (the vendor does not have to list passive circuit elements such as pull up/pull down resistors or bypass capacitors if they are do not provide security relevant function as part of the cryptographic module).

7. 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.

8. Circuit boards or other component mounting surfaces.

9. Enclosures, including any removable access doors or covers.

10. Physical connectors for devices outside the cryptographic module, or between any major independent submodules of the module.

11. Software/firmware modules that are modifiable.

12. Software/firmware modules that are unlikely to be modified.

13. Other component types not listed above.

TE01.08.03: The tester shall verify that the components list is consistent with information provided for other assertions of this subclause, as defined below:

1. The specification of the cryptographic boundary under assertion AS01.08. Verify that all components inside the cryptographic boundary are included in the components list, and that any components outside the cryptographic boundary are not listed as components of the cryptographic module.

2. The specification of the processors and software/firmware under assertion AS01.06. Verify that the list of processors, software modules, and hardware modules in the components list is the same as in the specifications under Assertion AS01.06.

3. The specification of the physical configuration under assertion AS01.08. Verify that the list of physical structures in the components list (such as circuit boards or other mounting surfaces, enclosures, and connectors) is the same as in the specifications under Assertion AS01.08.

4. The specification of the block diagram under assertion AS01.13. Verify that any individual components called out in the block diagram (e.g., processors, application-specific integrated circuits) are also listed in the components list.

5. Any components that are to be excluded from the requirements of ISO/IEC 19790 under the provisions of assertion AS01.09. Verify that components to be so excluded are still listed in the components list.

TE01.08.04: The tester shall verify that the documentation explicitly shows where the cryptographic boundary physical perimeter lies. This can be supplied via a listing of all significant components inside the cryptographic boundary plus all ports connected to equipment outside the cryptographic boundary. The documentation has to also supply a listing of all significant information flows and processing to be performed inside the cryptographic boundary plus all information that is input and output to the exterior of the cryptographic boundary. TE01.08.05: The tester shall verify that the vendor provided documentation includes sufficient detail for components at the cryptographic boundary to precisely define the cryptographic boundary.

TE01.08.06: 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. (Physical protection and tamper protection are covered separately in requirements under subclause 7.5 of ISO/IEC 19790:2006.) The module design has to also ensure that there are no uncontrolled interfaces into or out of the cryptographic module that could pass critical security parameters (CSPs), plaintext data, or other information that if misused could lead to a compromise.

TE01.08.07: The tester shall verify that the cryptographic boundary encompasses all components that are identified in the block diagram under assertion AS01.13 in this subclause as inputting, outputting, or processing CSPs, plaintext data, or other information that if misused could lead to a compromise.

TE01.08.08: As a partial exception to the above requirements, the vendor is allowed to exclude certain components from the requirements of ISO/IEC 19790 after satisfying the requirements under assertion AS01.09 in this subclause. The vendor may then treat such excluded components as effectively outside the cryptographic boundary of the module. In this case, the tester shall verify that any interfaces or physical connections between such excluded components and the rest of the module do not allow uncontrolled release of CSPs, plaintext data, or other information that if misused could lead to a compromise.

TE01.08.09: The tester shall verify that the vendor identified that the cryptographic module is either a single-chip module, a multi-chip embedded module, or a multi-chip standalone module as defined in subclause 7.5 of ISO/IEC 19790:2006.

TE01.08.10: 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 components of the module. This has to include drawings that are at least approximately to scale.

TE01.08.11: 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.

TE01.08.12: The tester shall verify that the vendor's documentation describes the primary physical parameters of the module. This description has to include at least the following:

1. Enclosure shape and approximate dimensions, including any access doors or covers

2. Circuit board(s) approximate dimensions, layout, and interconnections

3. Location of power supply, power converters, and power inputs and outputs

4. Interconnection wiring runs: routing and terminals

5. Cooling arrangements, such as conduction plates, cooling airflow, heat exchanger, cooling fins, fans, or other arrangements for removing heat from the module

6. Other component types not listed above

AS01.09: (Specification – Levels 1, 2, 3, and 4)
Documentation shall specify any hardware, software, or firmware components of a cryptographic module that are excluded from the security requirements of this International Standard *{i.e., ISO/IEC 19790:2006}* and explain the rationale for the exclusion.

Required Vendor Information

VE01.09.01: All components that are to be excluded from the security requirements shall be explicitly listed in the vendor documentation.

VE01.09.02: The vendor documentation shall provide the rationale for excluding each of the components listed in response to requirement VE01.09.01. The vendor shall show that each component, even if malfunctioning or misused, cannot cause a compromise under any reasonable condition.

Required Test Procedures

TE01.09.01: The tester shall verify whether the vendor indicates that any components of the module are to be excluded from the requirements of ISO/IEC 19790:2006. If none are so listed, all components have to meet the other requirements of this and all other subclauses.

TE01.09.02: If the vendor has indicated that certain components of the module are to be excluded from the requirements of ISO/IEC 19790, 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 CSPs, plaintext data, or other information that if misused could lead to a compromise. Rationale that may be acceptable, if adequately supported by documentation, include:

1. The component does not process CSPs, plaintext data, or other information that if misused could lead to a compromise

2. The component is not connected with security relevant components of the module that would allow inappropriate transfer of CSPs, plaintext data, or other information that if misused could lead to a compromise

3. 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

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.

AS01.10: (Specification – Levels 1, 2, 3, and 4)
Documentation shall specify the physical ports and logical interfaces and all defined input and output data paths of a cryptographic module.

NOTE This assertion is tested as part of AS02.01.

AS01.11: (Specification – Levels 1, 2, 3, and 4)
Documentation shall specify the manual or logical controls of a cryptographic module, physical or logical status indicators, and relevant physical, logical, and electrical characteristics.