INTERNATIONAL STANDARD

ISO/IEC 24759

Third edition
2017-03

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 24759:2017(E)

© ISO/IEC 2017

COPYRIGHT PROTECTED DOCUMENT

Contents

iTeh Standards
(https://standards.iteh.ai)
Document Preview

ISO/IEC 24759:2017
https://standards.iteh.ai/catalog/standards/iso/27725936-c104-45ea-b242-feb94c990e9c/iso-iec-24759-2017

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.

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 ISO documents 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).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

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

For an explanation on 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 the following URL: www.iso.org/iso/foreword.html.

This document was prepared by ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

This third edition cancels and replaces the second edition (ISO/IEC 24759:2014), of which it constitutes a minor revision. It also incorporates the Technical Corrigendum ISO/IEC 24759:2014/Cor.1:2015.

The main changes compared to the previous edition (plus other minor editorial modifications) are as follows:

— References to ISO/IEC 19790:2012 have been corrected throughout:

— 6.2.3.2: AS02.15, AS02.16, AS02.17 and AS02.18 modified;

— 6.3.3: AS03.04, AS03.07, AS03.10 and AS03.15 modified;

— 6.3.4: AS03.19 modified;

— 6.4.1: AS04.02 modified;

— 6.4.2; AS04.05, AS04.06 and AS04.07 modified;

— 6.4.3.1: AS04.11, AS04.13 and AS04.14;

— 6.4.3.2 and AS04.20;

— 6.4.4: AS04.39, AS04.40 and AS04.42 modified;

— 6.5: AS05.05, AS05.06, AS05.07, AS05.08, AS05.13, AS05.17 and AS05.18 modified;

— 6.8: AS08.04 modified;

— 6.10.1: AS10.17 modified.

iTeh Standards
(https://standards.iteh.ai)
Document Preview

Information technology — Security techniques — 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 19790:2012. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This document 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 document 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 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 19790:2012, *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.

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

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

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

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 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, Annex A to Annex 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 to twelve and A to 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 to 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 document.

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

NOTE   6.1 states general requirements to meet the assertions of the other subclauses in Clause 6, and ISO/IEC 19790:2012, Annex A to Annex F. 6.1 sets no assertion of itself and is not separately tested.

AS01.01: (General — Levels 1, 2, 3, and 4)

This clause specifies the security requirements that <u>shall</u> be satisfied by the cryptographic module's compliance to {ISO/IEC 19790:2012}.

AS01.02: (General — Levels 1, 2, 3, and 4)

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

NOTE   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.

— 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.

AS01.03: (General — Levels 1, 2, 3, and 4)

The cryptographic module <u>shall</u> be independently rated in each area.

AS01.04: (General — Levels 1, 2, 3, and 4)

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

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 <u>shall</u> 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}* A.2.2 <u>shall</u> 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 <u>shall</u> 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 to 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 applicable physical security and non-invasive security requirements found in *{ISO/IEC 19790:2012}* 7.7 and 7.8 <u>shall</u> apply.

NOTE   This assertion is not tested separately.

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

For software modules executing in a modifiable environment, the physical security requirements found in *{ISO/IEC 19790:2012}* 7.7 are optional and the applicable non-invasive security requirements in *{ISO/IEC 19790:2012}* 7.8 <u>shall</u> apply.

NOTE   This assertion is not tested separately.

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

For hybrid modules, all applicable requirements of *{ISO/IEC 19790:2012}* 7.5, 7.6, 7.7 and 7.8 <u>shall</u> apply.

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 <u>shall</u> 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 to 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 to AS02.18 within the cryptographic boundary.

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

The requirements of {ISO/IEC 19790:2012} <u>shall</u> 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 <u>shall</u>, 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 document).

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 <u>shall</u> 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 composition 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 and justify that these components will not interfere with the approved secure operation of the module.

VE02.13.02: The vendor 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, cannot interfere with the approved secure operation of the module. Rationale that may 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

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

TE02.13.02: 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 require the vendor to produce additional information as needed.

TE02.13.03: 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.

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.

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.

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 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 components, 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 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.