INTERNATIONAL STANDARD ISO/IEC 24759:2014
TECHNICAL CORRIGENDUM 1

Published 2015-10-01

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION • МЕЖДУНАРОДНАЯ ОРГАНИЗАЦИЯ ПО СТАНДАРТИЗАЦИИ • ORGANISATION INTERNATIONALE DE NORMALISATION
INTERNATIONAL ELECTROTECHNICAL COMMISSION • МЕЖДУНАРОДНАЯ ЭЛЕКТРОТЕХНИЧЕСКАЯ КОМИССИЯ • COMMISSION ÉLECTROTECHNIQUE INTERNATIONALE

Information technology — Security techniques — Test requirements for cryptographic modules —

TECHNICAL CORRIGENDUM 1

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

RECTIFICATIF TECHNIQUE 1

Technical Corrigendum 1 to ISO/IEC 24759:2014 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques*.

ICS 35.040 **Ref. No. ISO/IEC 24759:2014/Cor.1:2015(E)**

© ISO/IEC 2015 – All rights reserved

Published in Switzerland

Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

Contents

Page

Foreword v

1 Scope 1

2 Normative references 1

3 Terms and definitions 1

4 Symbols and abbreviated terms 1

5 Document organization 1
5.1 General 1
5.2 Assertions and security requirements 1

6 Security requirements 2
6.1 General 2
6.2 Cryptographic module specification 3
6.2.1 Cryptographic module specification general requirements 3
6.2.2 Types of cryptographic modules 3
6.2.3 Cryptographic boundary 5
6.2.4 Modes of operations 13
6.3 Cryptographic module interfaces 17
6.3.1 Cryptographic module interfaces general requirements 17
6.3.2 Types of interfaces 20
6.3.3 Definition of interfaces 20
6.3.4 Trusted channel 29
6.4 Roles, services, and authentication 31
6.4.1 Roles, services, and authentication general requirements 31
6.4.2 Roles 32
6.4.3 Services 33
6.4.4 Authentication 41
6.5 Software/Firmware security 49
6.6 Operational environment 56
6.6.1 Operational environment general requirements 56
6.6.2 Operating system requirements for limited or non-modifiable operational environments 57
6.6.3 Operating system requirements for modifiable operational environments 57
6.7 Physical security 67
6.7.1 Physical security embodiments 67
6.7.2 Physical security general requirements 68
6.7.3 Physical security requirements for each physical security embodiment 74
6.7.4 Environmental failure protection/testing 85
6.8 Non-invasive security 88
6.9 Sensitive security parameter management 90
6.9.1 Sensitive security parameter management general requirements 90
6.9.2 Random bit generators 92
6.9.3 Sensitive security parameter generation 92
6.9.4 Sensitive security parameter establishment 93
6.9.5 Sensitive security parameter entry and output 94
6.9.6 Sensitive security parameter storage 98
6.9.7 Sensitive security parameter zeroisation 98
6.10 Self-tests 101
6.10.1 Self-test general requirements 101
6.10.2 Pre-operational self-tests 105
6.10.3 Conditional self-tests 108
6.11 Life-cycle assurance 118
6.11.1 Life-cycle assurance general requirements 118
6.11.2 Configuration management 119
6.11.3 Design 120

Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

6.11.4 Finite state model 120
6.11.5 Development 124
6.11.6 Vendor testing 129
6.11.7 Delivery and operation 129
6.11.8 End of life 130
6.11.9 Guidance documents 131
6.12 Mitigation of other attacks 132
6.A Documentation requirements 133
6.B Cryptographic module security policy 133
6.C Approved security functions 134
6.D Approved sensitive security parameter generation and establishment methods 134
6.E Approved authentication mechanisms 134
6.F Approved non-invasive attack mitigation test metrics 135

© ISO/IEC 2015 – All rights reserved

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

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 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).

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. 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 meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, SC 27, *Security techniques*

This corrected version of ISO 24759:2014 incorporates the following corrections plus other minor editorial modifications.

— 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

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

— 6.8: AS08.04 modified

— 6.10.1: AS10.17 modified

© ISO/IEC 2015 – All rights reserved
Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

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/Cor.1:2015. 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/Cor.1:2015.

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/Cor.1:2015 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/Cor.1:2015, *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/Cor.1:2015 apply.

4 Symbols and abbreviated terms

For the purposes of this document, the symbols and abbreviated terms given in ISO/IEC 19790:2012/Cor.1:2015 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/Cor.1:2015.

5.2 Assertions and security requirements

Within each subclause, the corresponding security requirements from ISO/IEC 19790:2012/Cor.1:2015 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/Cor.1:2015.

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

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/Cor.1:2015 (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/Cor.1:2015 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 <u>shall</u> 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 clauses 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 <u>shall</u> 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

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

— 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 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/Cor.1:2015 subclause}* 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.**

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

— ***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 applicable physical security and non-invasive security requirements found in *{ISO/IEC 19790:2012/Cor.1:2015 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 software modules executing in a modifiable environment, the physical security requirements found in *{ISO/IEC 19790:2015 subclause}* 7.7 are optional and the applicable non-invasive security requirements in *{ISO/IEC 19790:2015 subclause}* 7.8 shall 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 19790:2015 subclause}* 7.5, 7.6, 7.7 and 7.8 shall apply.

NOTE This assertion is not tested separately.

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

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

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

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:

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.

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

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/Cor.1:2015}* (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/Cor.1:2015.

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.

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

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:

   2) Non-modifiable

      i) 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

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

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 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:

    2) Non-modifiable

        i) 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 that any

Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

components outside the cryptographic boundary are not listed as components of the cryptographic module.

b) The specification of the block diagram under assertion ASA.01. Verify that any individual components identified in the block diagram (e.g. processors, application specific integrated circuits) are also listed in the components list.

c) Any components that are to be excluded from the requirements of ISO/IEC 19790:2012/Cor.1:2015 under the provisions of assertions AS02.13 and AS02.14. Verify that components to be so excluded are still listed in the components list.

TE02.15.03: The tester shall verify that the cryptographic boundary is physically contiguous, such that there are no gaps that could allow uncontrolled input, output, or other access into the cryptographic module. (Physical protection and tamper protection are covered separately in requirements under 7.7 of ISO/IEC 19790:2012/Cor.1:2015.) The module design has to also ensure that there are no uncontrolled interfaces into or out of the cryptographic module.

TE02.15.04: The tester shall verify that the cryptographic boundary encompasses all components that are identified in the block diagram under assertion ASA.01 as inputting, outputting, or processing SSPs, plaintext data, or other information.

TE02.15.05: As a partial exception to the above requirements, the vendor is allowed to exclude certain components from the requirements of ISO/IEC 19790:2012/Cor.1:2015 after satisfying the requirements under assertions AS02.13 and AS02.14 in this subclause. The tester shall verify that any interfaces or physical connections between such excluded components and the rest of the module do not allow the following:

a) uncontrolled release of CSPs, plaintext data, or other information that if misused could lead to a compromise,

b) uncontrolled modifications of SSPs or other information that could lead to a compromise.

TE02.15.06: The tester shall verify that the vendor's documentation shows the internal layout of the module, including the placement and approximate dimensions of major identifiable components of the module. This has to include drawings that are at least approximately to scale.

TE02.15.07: The tester shall verify that the vendor's documentation indicates the major physical assemblies of the module and how they are assembled or inserted into the module.

TE02.15.08: 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:

a) Enclosure shape and approximate dimensions, including any access doors or covers

b) Circuit board(s) approximate dimensions, layout, and interconnections

c) Location of power supply, power converters, and power inputs and outputs

d) Interconnection wiring runs: routing and terminals

e) Cooling or heating arrangements, such as conduction plates, cooling airflow, heat exchanger, cooling fins, fans, heaters, or other arrangements for removing heat from or adding heat to the module

f) Other component types not listed above

TE02.15.09: The tester shall verify that the vendor provided block diagram represents the module's boundary and relationship of the hardware components.

AS02.16: (Specification – Levels 1, 2, 3, and 4)

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

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

— **The set of executable file or files that constitute the cryptographic module; and**

— **The instantiation of the cryptographic module saved in memory and executed by one or more processors.**

Required Vendor Information

VE02.16.01: All software components of the cryptographic module shall be identified in the vendor documentation. Components to be listed shall include all of the following:

a) The set of executable file or files that constitute the cryptographic module,

b) Other security relevant component types not listed above.

VE02.16.02: The vendor documentation shall indicate the internal software architecture, including how the software components interact.

VE02.16.03: The vendor documentation shall indicate the software environment (e.g. operating system, run-time library, etc.) on which the module executes.

Required Test Procedures

TE02.16.01: The tester shall verify that the documentation includes a components list that includes all software components of the cryptographic module.

TE02.16.02: 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:

a) The set of executable file or files that constitute the cryptographic module; and

b) Other component types not listed above.

TE02.16.03: 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 that any components outside the cryptographic boundary are not listed as components of the cryptographic module.

b) The specification of the software under assertion ASA.01. Verify that the list of software components is the same as in the specifications under assertion AS02.07.

c) The specification of the block diagram under assertion ASA.01. Verify that any individual components identified in the block diagram are also listed in the components list.

d) Any components that are to be excluded from the requirements of ISO/IEC 19790:2012/Cor.1:2015 under the provisions of assertions AS02.13 and AS02.14. Verify that components to be so excluded are still listed in the components list.

TE02.16.04: As a partial exception to the above requirements, the vendor is allowed to exclude certain components from the requirements of ISO/IEC 19790:2012/Cor.1:2015 after satisfying the requirements under assertions AS02.13 and AS02.14 in this subclause. The tester shall verify that any interfaces or physical connections between such excluded components and the rest of the module do not allow the following:

a) uncontrolled release of CSPs, plaintext data, or other information that if misused could lead to a compromise, nor

b) uncontrolled modifications of SSPs or other information that could lead to a compromise.

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

TE02.16.05: The tester shall verify that the vendor's documentation indicates the major software components of the module and how they are linked together forming the module.

AS02.17: (Specification – Levels 1, 2, 3, and 4)

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

- **The set of executable file or files that constitute the cryptographic module; and**
- **The instantiation of the cryptographic module saved in memory and executed by one or more processors.**

Required Vendor Information

VE02.17.01: All firmware components of the cryptographic module shall be identified in the vendor documentation. Components to be listed shall include all of the following:

a) The set of executable file or files that constitute the cryptographic module,

b) Other security relevant component types not listed above.

VE02.17.02: The vendor documentation shall indicate the internal firmware architecture, including how the firmware components interact.

VE02.17.03: The vendor documentation shall indicate the firmware environment (e.g. operating system, run-time library, etc.) on which the module executes.

Required Test Procedures

TE02.17.01: The tester shall verify that the documentation includes a components list that includes all firmware components of the cryptographic module.

TE02.17.02: 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:

a) The set of executable file or files that constitute the cryptographic module,

b) Other component types not listed above.

TE02.17.03: 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 that any components outside the cryptographic boundary are not listed as components of the cryptographic module.

b) The specification of the firmware under assertion ASA.01. Verify that the list of firmware components is the same as in the specifications under assertion AS02.07.

c) The specification of the block diagram under assertion ASA.01. Verify that any individual components identified in the block diagram are also listed in the components list.

d) Any components that are to be excluded from the requirements of ISO/IEC 19790:2012/Cor.1:2015 under the provisions of assertions AS02.13 and AS02.14. Verify that components to be so excluded are still listed in the components list.

TE02.17.04: As a partial exception to the above requirements, the vendor is allowed to exclude certain components from the requirements of ISO/IEC 19790:2012/Cor.1:2015 after satisfying the requirements under assertions AS02.13 and AS02.14 in this subclause. The tester shall verify that any interfaces or physical connections between such excluded components and the rest of the module do not allow the following

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

a) uncontrolled release of CSPs, plaintext data, or other information that if misused could lead to a compromise,

b) uncontrolled modifications of SSPs or other information that could lead to a compromise.

TE02.17.05: The tester shall verify that the vendor's documentation indicates the major firmware components of the module and how they are linked together forming the module.

AS02.18: (Specification – Levels 1, 2, 3, and 4)

The cryptographic boundary of a hybrid cryptographic module shall:

— **be the composite of the module's hardware component boundary and the disjoint software or firmware component(s) boundary; and**

— **include the collection of all ports and interfaces from each component.**

NOTE In addition to the disjoint software or firmware component(s), the hardware component can also include embedded software or firmware.

Required Vendor Information

VE02.18.01: The cryptographic module shall be identified in the vendor documentation as either a Hybrid Software Module or a Hybrid Firmware Module.

a) For Hybrid Software Module components, the vendor documentation shall provide information required under VE02.15.01 through VE02.15.04 and VE02.16.01 through VE02.16.03.

b) For Hybrid Firmware Module components, the vendor documentation shall provide information required under VE02.15.01 through VE02.15.04 and VE02.17.01 through VE02.17.03.

Required Test Procedures

TE02.18.01: The tester shall verify that the documentation identifies the module as either a Hybrid Software Module or a Hybrid Firmware Module.

a) For Hybrid Software Module components, the tester shall follow procedures required under TE02.15.01 through TE02.15.09 and TE02.16.01 through TE02.16.05.

b) For Hybrid Firmware Module components, the tester shall follow procedures required under TE02.15.01 through TE02.15.09 and TE02.17.01 through TE02.17.05.

6.2.4 Modes of operations

6.2.4.1 Modes of operation general requirements

AS02.19: (Specification – Levels 1, 2, 3, and 4)

The operator shall be able to operate the module in an approved mode of operation.

Required Vendor Information

VE02.19.01: The vendor provided non-proprietary security policy shall provide a description of the approved mode of operation.

VE02.19.02: The vendor provided non-proprietary security policy shall provide instructions for invoking the approved mode of operation.

Required Test Procedures

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

TE02.19.01: The tester shall verify that the vendor provided non-proprietary security policy contains a description of the approved mode of operation.

TE02.19.02: The tester shall invoke the approved mode of operation using the vendor provided instructions found in the non-proprietary security policy. The tester shall verify, by inspection and from the vendor documentation, that the cryptographic module is the approved mode of operation as a result of documented instructions.

AS02.20: (Specification – Levels 1, 2, 3, and 4)

An approved mode of operation shall be defined as the set of services which include at least one service that utilises an approved cryptographic algorithm, security function or process and those services or processes specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* 7.4.3.

Required Vendor Information

VE02.20.01: The vendor shall provide a validation certificate for each approved security function.

VE02.20.02: The vendor shall provide a list of all non-approved security functions.

Required Test Procedures

TE02.20.01: The tester shall verify that the vendor has provided a validation certificate for each approved security function issued by a validation authority.

TE02.20.02: The tester shall verify that the vendor has provided the list of non-approved security functions.

AS02.21: (Specification – Levels 1, 2, 3, and 4)

Non-approved cryptographic algorithms, security functions, and processes or other services not specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* 7.4.3 shall not be utilised by the operator in an approved mode of operation unless the non-approved cryptographic algorithm or security function is part of an approved process and is not security relevant to the approved processes operation (e.g. a non-approved cryptographic algorithm or non-approved generated key may be used to obfuscate data or CSPs but the result is considered unprotected plaintext and provides no security relevant functionality until protected with an approved cryptographic algorithm).

Required Vendor Information

VE02.21.01: The vendor provided documentation shall identify all of non-approved cryptographic algorithms, security functions or processes utilised for each service in each approved mode of operation.

VE02.21.02: The vendor documentation shall provide a rationale for why utilised non-approved cryptographic algorithms, security functions or processes are considered non-security relevant to the approved processes operation.

Required Test Procedures

TE02.21.01: The tester shall verify by inspection that the vendor provided documentation identifies all of non-approved cryptographic algorithms, security functions or processes utilised for each service in each approved mode of operation.

TE02.21.02: The tester shall verify the correctness of any rationale provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.

6.2.4.2 Normal operation

AS02.22: (Specification – Levels 1, 2, 3, and 4)

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

CSPs shall be exclusive between approved and non-approved services and modes of operation (e.g. not shared or accessed).

Required Vendor Information

VE02.22.01: The vendor shall provide a list of all CSPs within the module and identify their usage between approved and non-approved services and mode of operation.

VE02.22.02: The vendor shall provide a description of how each CSP becomes exclusive between approved and non-approved services and modes of operation.

Required Test Procedures

TE02.22.01: The tester shall verify that the vendor provided documentation contains a description of the usage of each CSP in an approved or non-approved mode of operation.

TE02.22.02: The tester shall verify by inspection and from the vendor documentation that the CSPs are exclusive between approved and non-approved services and modes of operation.

AS02.23: (Specification – Levels 1, 2, 3, and 4)

The module's security policy shall define the complete set of services that are provided for each defined mode of operation (both approved and non-approved).

NOTE This assertion is tested under ASB.01.

AS02.24: (Specification – Levels 1, 2, 3, and 4)

All services shall provide an indicator when the service utilises an approved cryptographic algorithm, security function or process in an approved manner and those services or processes specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* 7.4.3.

Required Vendor Information

VE02.24.01: The vendor provided documentation shall specify the indicator for each service.

Required Test Procedures

TE02.24.01: The tester shall verify that the vendor provided documentation contains a description of indicator when the service utilises an approved cryptographic algorithm, security function or process in an approved manner.

TE02.24.02: The tester shall execute all services and verify that the indicator provides an unambiguous indication of whether the service utilises an approved cryptographic algorithm, security function or process in an approved manner or not.

6.2.4.3 Degraded operation

AS02.25: (Specification – Levels 1, 2, 3, and 4)

For a cryptographic module to operate in degraded operation, the following *{ISO/IEC 19790:2012/Cor.1:2015 AS02.26 through AS02.30}* shall apply:

NOTE This assertion is not separately tested.

AS02.26: (Specification – Levels 1, 2, 3, and 4)

The degraded operation shall be entered only after exiting an error state;

Required Vendor Information

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

VE02.26.01: If the cryptographic module allows a degraded operation, the vendor shall provide a description of all degraded operation after exiting each error state.

VE02.26.02: The vendor shall provide specification of degraded operation. For each degraded operation, the specification shall include:

a) conditions of entry into and exit from the degraded operation

b) operational algorithms, security functions, services or processes

c) non-operational algorithms, security functions, services or processes

d) isolated mechanisms, functions, or components in the degraded operation

e) techniques to isolate mechanisms, functions or components

f) status information provided in the degraded operation

g) status indicator if attempts are made to use a non-operational algorithm, security function, or process

Required Test Procedures

TE02.26.01: The tester shall verify that the vendor provided documentation clearly identifies the degraded operation and its conditions of entry and exit.

TE02.26.02: The tester shall use the vendor documentation to check that the degraded operation can only be accessed after exiting in error state. The tester shall check that the error status indicator (see AS03.11) is correctly positioned.

TE02.26.03: The tester shall exercise the cryptographic module, causing it to operate in each degraded operation. For each degraded operation, tester shall attempt to perform a service to verify that all conditional algorithm self-tests are performed prior to the first operational use of any cryptographic algorithm.

TE02.26.04: The tester shall first exercise the cryptographic module, causing it to operate in each degraded operation. The tester shall next perform pre-operational self-tests to verify that the cryptographic module remains in degraded operation until such time the cryptographic module passes without failure all pre-operational self-tests successfully.

TE02.26.05: The tester shall first exercise the cryptographic module, causing it to operate in each degraded operation. The tester shall next perform pre-operational self-tests, causing an error condition in pre-operational self-tests to occur. The tester shall verify that the cryptographic module does not remain in degraded operation but enters an error state.

AS02.27: (Specification – Levels 1, 2, 3, and 4)

The module <u>shall</u> provide status information when re-configured and the degraded operation entered.

NOTE This assertion is not separately tested. Tested as part of AS02.26.

AS02.28: (Specification – Levels 1, 2, 3, and 4)

The mechanism or function that failed <u>shall</u> be isolated.

Required Vendor Information

VE02.28.01: The vendor documentation requirement is specified under VE02.26.02. The vendor design shall ensure that any failure from the failed mechanisms, functions, and components cannot interfere or compromise the approved operation of the cryptographic module.

Required Test Procedures

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

TE02.28.01: The tester shall verify by inspection and from the vendor documentation that failed mechanisms, functions, and components are isolated before entering degraded operation.

TE02.28.02: The tester shall verify by inspection and from the vendor documentation that failed mechanisms, functions, and components cannot interfere or compromise the approved operation of the cryptographic module.

AS02.29: (Specification – Levels 1, 2, 3, and 4)

All conditional algorithm self-tests shall be performed prior to the first operational use of the cryptographic algorithm after entering degraded operation.

NOTE This assertion is not separately tested. Tested as part of AS02.26.

AS02.30: (Specification – Levels 1, 2, 3, and 4)

Services shall provide an indicator if attempts are made to use a non-operational algorithm, security function, or process.

Required Vendor Information

VE02.30.01: The vendor documentation requirement is specified under VE02.26.02. The vendor design shall ensure that service output includes an indicator if attempts are made to use a non-operational algorithm, security function, or process.

Required Test Procedures

TE02.30.01: The tester shall verify from the vendor documentation that services provide documented indicators if attempts are made to use a non-operational algorithm, security function, or process.

TE02.30.02: The tester shall exercise the cryptographic module and verify that the documented indicator is provided if attempts are made to use a non-operational algorithm, security function, or process.

AS02.31: (Specification – Levels 1, 2, 3, and 4)

The cryptographic module shall remain in degraded operation until such time the cryptographic module passes without failure all pre-operational self-tests successfully.

NOTE This assertion is not separately tested. Tested as part of AS02.26.

AS02.32: (Specification – Levels 1, 2, 3, and 4)

If the cryptographic module fails the pre-operational self-tests, the module shall not enter a degraded operation.

NOTE This assertion is not separately tested. Tested as part of AS02.26.

6.3 Cryptographic module interfaces

6.3.1 Cryptographic module interfaces general requirements

AS03.01: (module interfaces – Levels 1, 2, 3, and 4)

A cryptographic module shall restrict all logical information flow to only those physical access points and logical interfaces that are identified as entry and exit points to and from the cryptographic boundary of the module.

Required Vendor Information

VE03.01.01: The vendor documentation shall specify each of the physical ports and logical interfaces of the cryptographic module, including the:

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

a) Physical ports and their pin assignments

b) Physical covers, doors or openings

c) Logical interfaces (e.g. APIs and all other data/control/status signals) and the signal names and functions

d) Manual controls (e.g. buttons or switches) for applicable physical control inputs

e) Physical status indicators (e.g. lights or displays) for applicable physical status outputs

f) Mapping of the logical interfaces to the physical ports, manual controls, and physical status indicators of the cryptographic module

g) Physical, logical, and electrical characteristics, as applicable, of the above ports and interfaces

VE03.01.02: The vendor documentation shall specify the information flows and physical access points of the cryptographic module by highlighting or annotating copies of the block diagrams, design specifications and/or source code and schematics provided in 6.2 and 6.11 of this International Standard. The vendor shall also provide any other documentation necessary to clearly specify the relationship of the information flows and physical access points to the physical ports and logical interfaces. The vendor shall establish the above information in relation with the information provided under assertions AS02.07 and AS02.15 through AS02.18 without inconsistencies in the description of components and physical layout for the input/output ports.

VE03.01.03: For each physical or logical input to the cryptographic module, or physical and logical output from the module, the vendor documentation shall specify the logical interface to which the physical input or output belongs, and the physical entry/exit port. The specifications provided shall be consistent with the specifications of the cryptographic module components provided under 6.2 and 6.11 of this International Standard, and the specifications of the logical interfaces provided in assertions AS03.04 to AS03.11 of this subclause.

Required Test Procedures

TE03.01.01: The tester shall verify that vendor documentation specifies each of the physical ports and logical interfaces of the cryptographic module. The required specifications shall include:

a) All physical input and output ports, including their pin assignments, physical locations within the module, a summary of the logical signals that flow through each port, and the timing sequence of signal flows if two or more signals share the same physical pin

b) All physical covers, doors, or openings, including their physical location within the cryptographic module, and the components or functions that can be accessed and/or modified via each cover/door/opening

c) All logical input and output interfaces (e.g. APIs and all other data/control/status signals), including a listing or annotated block diagram of all the logical data and control inputs and data and status outputs of the cryptographic module, and a listing and description of the signal names and functions

d) All manual controls used to physically enter control signals, such as switches or buttons, including their physical location within the cryptographic module, and a listing and description of the control signals that can be entered manually

e) All physical status indicators, including their physical location within the module and a listing and description of the status indication signals that are output physically

f) A mapping of the logical input and output interfaces to the physical input and output ports, manual controls, and physical status indicators of the cryptographic module

g) Physical, logical, and electrical characteristics, as applicable, of the above physical ports and interfaces, including summaries of pin designations, logical signals carried on each port, voltage levels and their logical significance (e.g. what a low or high voltage signifies in terms of a logic “0”, “1”, or other meaning) and the timing of signals

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

TE03.01.02: The tester shall verify that the vendor documentation specifies all information flows and physical access points of the cryptographic module, by examining the block diagrams, design specifications and/or source code and schematics provided in 6.2 and 6.11 of this International Standard, and any other documentation provided by the vendor. The documentation shall specify the relationship of the information flows and physical access points to the physical ports and logical interfaces of the cryptographic module. The tester shall compare the above information with the information provided under assertions AS02.07 and AS02.15 through AS02.18 and verify that there are no inconsistencies in the description of components and physical layout for the input/output ports.

TE03.01.03: The tester shall verify that for each physical or logical input to the cryptographic module, or physical and logical output from the module, the vendor documentation specifies the logical interface to which the physical input or output belongs, and the physical entry/exit port. The specifications provided shall be consistent with the specifications of the cryptographic module components provided under 6.2 and 6.11 of this International Standard, and the specifications of the logical interfaces provided in assertions AS03.04 to AS03.11 of this subclause.

TE03.01.04: The tester shall verify, by inspection of the cryptographic module, that all the above specifications provided by the vendor documentation are consistent with the actual design of the cryptographic module.

AS03.02: (Module interfaces – Levels 1, 2, 3, and 4)

The cryptographic module logical interfaces shall be distinct from each other although they may share one physical port (e.g. input data may enter and output data may exit via the same port) or may be distributed over one or more physical ports (e.g. input data may enter via both a serial and a parallel port).

NOTE An Application Program Interface (API) of a software component of a cryptographic module can be defined as one or more logical interface(s).

Required Vendor Information

VE03.02.01: The vendor's design shall separate the cryptographic module interfaces into logically distinct and isolated categories, using the categories listed in assertion AS03.04, and, if applicable, AS03.12 and AS03.13 in this subclause. This information shall be consistent with the specification of the logical interfaces and physical ports provided in AS03.01 in this subclause.

VE03.02.02: The vendor documentation shall provide a mapping of each category of logical interface to a physical port of the cryptographic module. A logical interface may be physically distributed across more than one physical port, or two or more logical interfaces may share one physical port as long as the information flows are kept logically separate. If two or more logical interfaces share the same physical port, the vendor documentation shall specify how the information from the different interface categories is kept logically separate.

Required Test Procedures

TE03.02.01: The tester shall verify, from the vendor documentation and by inspection of the cryptographic module, that the module interfaces are logically distinct and isolated for the categories of interfaces specified in assertions AS03.04 and, if applicable, AS03.12 and AS03.13 of this subclause. This information shall be consistent with the specification and design of the logical interfaces and physical ports provided in AS03.01 in this subclause.

TE03.02.02: The tester shall verify that the vendor documentation provides a mapping of each category of logical interface to a physical port of the cryptographic module. A logical interface may be physically distributed across more than one physical port, or two or more logical interfaces may share one physical port. If two or more interfaces share the same physical port, the tester shall verify that the vendor documentation specifies how the information flows for the input, output, control, and status interfaces are kept logically separate.

AS03.03: (Module interfaces – Levels 1, 2, 3, and 4)

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

The documentation requirements specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* A.2.3 shall be provided.

Required Vendor Information

VE03.03.01: The vendor shall provide documentation as specified in A.2.3 of ISO/IEC 19790:2012/Cor.1:2015.

Required Test Procedures

TE03.03.01: The tester shall verify completeness of the documentation specified in A.2.3 of ISO/IEC 19790:2012/Cor.1:2015.

6.3.2 Types of interfaces

6.3.3 Definition of interfaces

AS03.04: (Module interfaces – Levels 1, 2, 3, and 4)

A cryptographic module shall have the following five interfaces ("input" and "output" are indicated from the perspective of the module):

- **Data input interface**
- **Data output interface**
- **Control input interface**
- **Control output interface**
- **Status output interface**

Required Vendor Information

VE03.04.01: The vendor documentation shall separate the cryptographic module interfaces into logically distinct and isolated categories by the following five distinctly defined logical interfaces within the cryptographic module ("input" and "output" are indicated from the perspective of the module):

a) Data input interface (for the input of data as specified in AS03.05),

b) Data output interface (for the output of data as specified in AS03.06 and AS03.07),

c) Control input interface (for the input of commands as specified in AS03.08),

d) Control output interface (for the output of commands as specified in AS03.09, and AS03.10) and

e) Status output interface (for the output of status information as specified in AS03.11).

Required Test Procedures

TE03.04.01: The tester shall verify that the vendor documentation specifies that the five logical interfaces as listed in VE03.04.01 have been designed within the cryptographic module. If so, verification that the logical interfaces within the cryptographic module function as specified shall be performed under assertions AS03.05 to AS03.11 in this subclause.

Data input interface

AS03.05: (Data input interface – Levels 1, 2, 3, and 4)

All data (except control data entered via the control input interface) that is input to and processed by a cryptographic module (including plaintext data, ciphertext data, SSPs, and status information from another module) shall enter via the "data input" interface.

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

Required Vendor Information

VE03.05.01: The cryptographic module shall have a data input interface. All data (except control data entered via the control input interface) that is to be input to and processed by the cryptographic module shall enter via the data input interface, including:

a) Plaintext data

b) Ciphertext or signed data

c) Cryptographic keys and other key management data (plaintext or encrypted)

d) Authentication data (plaintext or encrypted)

e) Status information from external sources

f) Any other input data

VE03.05.02: If applicable, the vendor documentation shall specify any external input devices to be used with the cryptographic module for the entry of data into the data input interface, such as smart cards, tokens, keypads, key loaders, and/or biometric devices.

Required Test Procedures

TE03.05.01: The tester shall verify, by inspection, that the cryptographic module includes a data input interface, and that the data input interface functions as specified. The tester shall verify that all data (except control data entered via the control input interface) that is to be input to and processed by the cryptographic module enters via the data input interface, including:

a) Plaintext data that is to be encrypted or signed by the cryptographic module

b) Ciphertext or signed data that is to be decrypted or verified by the module

c) Plaintext or encrypted cryptographic keys and other key management data that are input into and used by the cryptographic module, including initialisation data and vectors, split key information, and/or key accounting information. (Other key management requirements are covered in 7.9 of ISO/IEC 19790:2012/Cor.1:2015.)

d) Plaintext or encrypted authentication data that is input into the cryptographic module, including passwords, PINs, and/or biometric information

e) Status information from external sources (e.g. another cryptographic module or device)

f) Any other information that is input into the cryptographic module for processing or storage, except for control information that is covered separately in AS03.08

TE03.05.02: The tester shall verify if the vendor documentation specifies any external input devices to be used with the cryptographic module for the entry of data into the data input interface, such as smart cards, tokens, keypads, key loaders, and/or biometric devices. The tester shall enter data into the data input interface using the identified external input device(s), and verify that entry of data using the external input device functions as specified.

Data output interface

AS03.06: (Data output interface – Levels 1, 2, 3, and 4)

All data (except status data output via the status output interface and control data output via the control output interface) that is output from a cryptographic module (including plaintext data, ciphertext data, and SSPs) shall exit via the "data output" interface.

Required Vendor Information

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

VE03.06.01: The cryptographic module shall have a data output interface. All data (except status data output via the status output interface and control data output via the control output interface) that has been processed and is to be output by the cryptographic module shall exit via the data output interface, including:

a) Plaintext data

b) Ciphertext data and digital signatures

c) Cryptographic keys and other key management data (plaintext or encrypted)

d) Any other information that is output from the cryptographic module after processing or storage except for status information that is covered separately in AS03.11 and control information that is covered separately in AS03.09 and AS03.10 in this subclause

VE03.06.02: If applicable, the vendor documentation shall specify any external output devices to be used with the cryptographic module for the output of data from the data output interface, such as smart cards, tokens, displays, and/or other storage devices.

Required Test Procedures

TE03.06.01: The tester shall verify, by inspection, that the cryptographic module includes a data output interface, and that the data output interface functions as specified. The tester shall verify that all data (except status data output via the status output interface and control data output via the control output interface) that has been processed and is to be output by the cryptographic module exits via the data output interface, including:

a) Plaintext data that has been decrypted by the cryptographic module

b) Ciphertext data that has been encrypted, and digital signatures that have been generated by the cryptographic module

c) Plaintext or encrypted cryptographic keys and other key management data that have been internally generated and output from the module, including initialisation data and vectors, split key information, and/or key accounting information (other key management requirements are covered in 7.9 of ISO/IEC 19790:2012/Cor.1:2015)

d) Any other information that is output from the cryptographic module after processing or storage except for status information that is covered separately in AS03.11 in this subclause and control information that is covered separately in AS03.09 and AS03.10 in this subclause.

TE03.06.02: The tester shall verify if vendor documentation specifies any external output devices to be used with the cryptographic module for the output of data from the data output interface, such as smart cards, tokens, displays, and/or other storage devices. The tester shall output data from the data output interface using the identified external output device(s), and verify that output of data using the external output device functions as specified.

AS03.07: (Data output interface – Levels 1, 2, 3, and 4)

All data output via the "data output" interface shall be inhibited while performing manual entry, pre-operational self-tests, software/firmware loading and zeroisation; or when the cryptographic module is in an error state.

Required Vendor Information

VE03.07.01: The vendor documentation shall specify how the cryptographic module inhibits data output while performing manual entry, pre-operational self-tests, software/firmware loading and zeroisation; or when the cryptographic module is in an error state.

VE03.07.02: The vendor documentation shall specify how the design of the cryptographic module ensures that all data output via the data output interface is inhibited while performing manual entry, pre-operational self-tests, software/firmware loading and zeroisation; or when the cryptographic module is in an error state.

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

Required Test Procedures

TE03.07.01: The tester shall verify that the vendor documentation specifies that all data output via the data output interface is inhibited

a) whenever the cryptographic module is performing

   1) manual entry,

   2) pre-operational self-tests,

   3) software/firmware loading,

   4) zeroisation;

b) or when the cryptographic module is in an error state.

This test procedure can be restated as follows:

a) The tester shall verify from the vendor documentation that once each of the following services is started, all data output via the data output interface is inhibited, until the service is completed successfully:

   1) manual entry,

   2) pre-operational self-tests,

   3) software/firmware loading,

   4) zeroisation.

b) The tester shall verify from vendor documentation that once an error condition is detected and the error state is entered, all data output via the data output interface is inhibited, until error recovery occurs.

TE03.07.02: The tester shall cause the cryptographic module to enter each of following states:

a) a state performing manual SSP entry,

b) a self-test state performing pre-operational self-tests,

c) a state performing software/firmware loading,

d) a state performing zeroisation,

e) an error state;

and verify that all data output via the data output interface is inhibited.

If it is not possible for the tester to cause an error then the vendor shall provide a rationale to the tester why this test cannot be performed. In such case, the tester shall follow alternative procedures allowed by the validation authority, to ensure that all data output via the data output interface is inhibited.

EXAMPLE Examining the applicable source code

TE03.07.03: The tester shall verify that the vendor documentation specifies that all data output via the data output interface is inhibited whenever the cryptographic module is in a self-test condition. The tester shall verify from the vendor documentation that once self-tests are being performed, all data output via the data output interface is inhibited, until the self-tests are completed. Status information to display the results of the self-tests may be allowed from the status output interface. The tester shall also verify that the self-test conditions specified in response to this assertion are identical to the self-tests specified under AS10.14.

Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

TE03.07.04: The tester shall command the module to perform the self-tests and verify that all data output via the data output interface is inhibited. If status information is output from the status output interface to indicate the results of the self-tests, the tester shall verify that no CSPs, plaintext data, or other information are output that if misused could lead to a compromise. If it is not possible for the tester to attempt data output during specific self-test state, then the vendor shall provide a rationale to the tester why this test cannot be performed. In such case, the tester shall follow alternative procedures allowed by the validation authority, to ensure that all data output via the data output interface is inhibited.

EXAMPLE 1 Examining the applicable source code

EXAMPLE 2 Using a simulator

EXAMPLE 3 Using a debugger

TE03.07.05: The tester shall verify that the vendor documentation specifies how the cryptographic module ensures that all data output via the data output interface is to be inhibited during error states or self-test conditions. The tester shall also verify, by inspection of the design of the cryptographic module, that the data output interface is, in fact, logically or physically inhibited under these conditions.

Control input interface

AS03.08: (Control input interface – Levels 1, 2, 3, and 4)

All input commands, signals (e.g. clock input), and control data (including function calls and manual controls such as switches, buttons, and keyboards) used to control the operation of a cryptographic module shall enter via the "control input" interface.

Required Vendor Information

VE03.08.01: The cryptographic module shall have a control input interface. All commands, signals, and control data (except data entered via the data input interface) used to control the operation of the cryptographic module shall enter via the control input interface, including:

a) Commands input logically via an API (e.g. for the software and firmware components of the cryptographic module)

b) Signals input logically or physically via one or more physical ports (e.g. for the hardware components of the cryptographic module)

c) Manual control inputs (e.g. using switches, buttons, or a keyboard)

d) Any other input control data

VE03.08.02: If applicable, the vendor documentation shall specify any external input devices to be used with the cryptographic module for the entry of commands, signals, and control data into the control input interface, such as smart cards, tokens, or keypads.

Required Test Procedures

TE03.08.01: The tester shall verify, by inspection, that the cryptographic module includes a control input interface, and that the control input interface functions as specified. The tester shall verify that all commands, signals, and control data (except data entered via the data input interface) used to control the operation of the cryptographic module shall enter via the control input interface, including:

a) Commands input logically via an API, such as function calls to a software library or to a smart card

b) Signals input logically or physically via one or more physical ports, such as commands and signals sent through a serial port or a PC Card

c) Manual control inputs (e.g. using switches, buttons, or a keyboard)

d) Any other input control data

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

TE03.08.02: The tester shall verify if the vendor documentation specifies any external input devices to be used with the cryptographic module for the entry of commands, signals, and control data into the control input interface, such as smart cards, tokens, or keypads. The tester shall enter commands via the control input interface using the identified external input device(s), and verify that input of commands using the external input device functions as specified.

Control output interface

AS03.09: (Control output interface – Levels 1, 2, 3, and 4)

All output commands, signals, and control data (e.g. control commands to another module) used to control or indicate the state of operation of a cryptographic module shall exit via the "control output" interface.

Required Vendor Information

VE03.09.01: The vendor documentation shall specify all output commands, signals, and control data (e.g. control commands to another module) used to control or indicate the state of operation of a cryptographic module shall exit via the control output interface

Required Test Procedures

TE03.09.01: The tester shall verify that the vendor documentation shall specify all output commands, signals, and control data (e.g. control commands to another module) used to control or indicate the state of operation of a cryptographic module shall exit via the control output interface

TE03.09.02: If the control output interface is specified, the tester shall verify, by inspection, that the control output interface functions as specified.

AS03.10: (Control output interface – Levels 1, 2, 3, and 4)

All control output via the "control output" interface shall be inhibited when the cryptographic module is in an error state unless exceptions are specified and documented in the security policy.

Required Vendor Information

VE03.10.01: The vendor documentation shall specify how the cryptographic module ensures that all control output via the control output interface is inhibited whenever the module is in an error state (error states are covered in 7.11 of ISO/IEC 19790:2012/Cor.1:2015). Status information may be allowed from the status output interface to identify the type of error.

VE03.10.02: The vendor documentation shall specify how the design of the cryptographic module ensures that all control output via the control output interface is inhibited whenever the module is in a self-test condition (self-tests are covered in 7.10 of ISO/IEC 19790:2012/Cor.1:2015). Status information to display the results of the self-tests may be allowed from the status output interface.

Required Test Procedures

TE03.10.01: The tester shall verify that the vendor documentation specifies that all control output via the control output interface is inhibited whenever the cryptographic module is in an error state. The tester shall verify from the vendor documentation that once an error condition is detected and the error state is entered, all control output via the control output interface is inhibited, until error recovery occurs. The tester shall also verify that the error states specified in response to this assertion are identical to the error states specified under AS11.08.

TE03.10.02: The tester shall cause the cryptographic module to enter each specified error state and verify that all control output via the control output interface is inhibited. If status information is output from the status output interface to identify the type of error, the tester shall verify that the information output is not sensitive. The following actions may be used to cause the cryptographic module to enter an error state - opening a tamper-detecting cover or door, entering incorrectly-formatted commands, keys, or parameters, reducing input voltage, and/or any other error-causing actions.

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

If it is not possible for the tester to cause an error then the vendor shall provide a rationale to the tester why this test cannot be performed.

TE03.10.03: The tester shall verify that the vendor documentation specifies that all control output via the control output interface is inhibited whenever the cryptographic module is in a self-test condition. The tester shall verify from the vendor documentation that once self-tests are being performed, all control output via the control output interface is inhibited, until the self-tests are completed. The tester shall also verify that the self-test conditions specified in response to this assertion are identical to the self-tests specified under AS10.14.

TE03.10.04: The tester shall cause the module to perform the self-tests and verify that all control output via the control output interface is inhibited.

TE03.10.05: The tester shall verify that the vendor documentation specifies how the cryptographic module ensures that all control output via the control output interface is to be inhibited during error states or self-test conditions. The tester shall also verify, by inspection of the implementation of the cryptographic module, that the control output interface is, in fact, logically or physically inhibited under these conditions.

Status output interface

AS03.11: (Status output interface – Levels 1, 2, 3, and 4)

All output signals, indicators (e.g. error indicator), and status data [including return codes and physical indicators such as visual (display, indicator lamps), audio (buzzer, tone, ring), and mechanical (vibration)] used to indicate the status of a cryptographic module shall exit via the "status output" interface.

NOTE Status output will be either implicit or explicit.

Required Vendor Information

VE03.11.01: The cryptographic module shall have a status output interface. All status information, signals, logical indicators, and physical indicators used to indicate or display the status of the module shall exit via the status output interface, including:

a) Status information output logically via an API

b) Signal outputs logically or physically via one or more physical ports

c) Manual status outputs (e.g. using displays, indicator, lamps, buzzer, tone, or ring)

d) Any other output status information

VE03.11.02: If applicable, the vendor documentation shall specify any external output devices to be used with the cryptographic module for the output of status information, signals, logical indicators, and physical indicators via the status output interface, such as smart cards, tokens, displays, and/or other storage devices.

Required Test Procedures

TE03.11.01: The tester shall verify, by inspection, that the cryptographic module includes a status output interface, and that the status output interface functions as specified. The tester shall verify that all status information, signals, logical indicators, and physical indicators used to indicate or display the status of the module shall exit via the status output interface, including:

a) Status information output logically via an API, such as return codes from a software library or a smart card

b) Signal outputs logically or physically via one or more physical ports, such as status information sent through a serial port or a PC Card connector

c) Manual status outputs (e.g. using LEDs, buzzers, or a display)

d) Any other output status information

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

TE03.11.02: The tester shall verify that the vendor documentation specifies any external output devices (if applicable) to be used with the cryptographic module for the output of status information, signals, logical indicators, and physical indicators via the status output interface.

TE03.11.03: The tester shall verify that the status information output from the status output interface shall not output any information that could result in a compromise of CSPs.

AS03.12: (Module interfaces – Levels 1, 2, 3, and 4)

Except for the software cryptographic modules, all modules shall also have the following interface.

NOTE This assertion is not tested separately.

AS03.13: (Module interfaces – Levels 1, 2, 3, and 4)

***Power interface:* All external electrical power that is input to a cryptographic module shall enter via a power interface.**

NOTE A power interface is not required if all power is provided or maintained internal to the module, and that replacement of an internal battery is considered a physical maintenance activity, and is subject to the requirements specified in 7.7 of ISO/IEC 19790:2012/Cor.1:2015.

Required Vendor Information

VE03.13.01: If the cryptographic module requires or provides power to/from other devices external to the boundary (e.g. a power supply or an external battery), the vendor documentation shall specify a power interface and a corresponding physical port.

VE03.13.02: All power entering or exiting the cryptographic module to/from other devices external to the cryptographic boundary shall pass through the specified power interface.

Required Test Procedures

TE03.13.01: The tester shall verify if the vendor documentation specifies whether the cryptographic module requires or provides power to/from other devices external to the cryptographic boundary (e.g. a power supply, power cord, power inlet/outlet, or an external battery). The tester shall also verify that the vendor documentation specifies a power interface and a corresponding physical port.

TE03.13.02: The tester shall verify, by inspection of the cryptographic module that all power entering or exiting the module to/from other devices external to the cryptographic boundary passes through the specified power interface.

AS03.14: (Module interfaces – Levels 1, 2, 3, and 4)

The cryptographic module shall distinguish between data, control information, and power for input, and data, control information, status information, and power for output.

Required Vendor Information

VE03.14.01: The vendor documentation shall specify how the cryptographic module distinguishes between data and control for input and data, control and status for output, and how the physical and logical paths followed by the input data and control information entering the module via the applicable input interfaces are logically or physically disconnected from the physical and logical paths followed by the output data, control and status information exiting the module via the applicable output interfaces.

VE03.14.02: The vendor documentation shall specify how the physical and logical paths used by the input data and control information are logically or physically disconnected from the physical and logical paths used by the output data, control and status information. If the physical and logical paths used by the input data and control information and the output data, control and status information are physically shared, the vendor documentation shall specify how logical separation is enforced by the cryptographic module.

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

VE03.14.03: The vendor documentation shall show consistency and shall show that the cryptographic module distinguishes between data and control for input and data, control and status for output, and that the physical and logical paths followed by the input data and control information entering the module via the applicable input interfaces are logically or physically disconnected from the physical and logical paths followed by the output data, control and status information exiting the module via the applicable output interfaces.

Required Test Procedures

TE03.14.01: The tester shall verify that the vendor documentation specifies how the cryptographic module distinguishes between data and control for input and data, control and status for output. Input data entered from the data input interface, and control information entered from the control input interface shall be logically or physically distinguished from output data exiting to the output data interface, output control exiting to the output control interface, and status information exiting to the status output interface.

TE03.14.02: The tester shall verify that the vendor documentation specifies how the physical and logical paths used by the input data and control information are logically or physically disconnected from the physical and logical paths used by the output data, control and status information. If the physical and logical paths used by the input data and control information and the output data, control and status information are physically shared, the tester shall verify that the vendor documentation specifies how logical separation is enforced by the cryptographic module.

TE03.14.03: The tester shall verify, by inspection, the consistency of the vendor documentation, and that the cryptographic module distinguishes between data and control for input and data, control and status for output, and that the physical and logical paths followed by the input data and control information entering the module via the applicable input interfaces are logically or physically disconnected from the physical and logical paths followed by the output data, control and status information exiting the module via the applicable output interfaces.

AS03.15: (Module interfaces – Levels 1, 2, 3, and 4)

The cryptographic module specification shall, unambiguously, specify format of input data and control information, including length restrictions for all variable length inputs.

Required Vendor Information

VE03.15.01: The vendor documentation shall specify the physical and logical paths used by all major categories of input data entering the cryptographic module via the data input interface and the applicable physical ports. The documentation shall include a specification of the applicable paths (e.g. by highlighted or annotated copies of the schematics, block diagrams, or other information provided under AS02.07 and AS02.15 through AS02.18). All input data entering the cryptographic module via the data input interface shall only use the specified paths while being processed or stored by each physical or logical sub-section of the module. The input data paths shall be specified in sufficient detail to verify which type of data pass through each applicable physical port.

NOTE The term “all major categories of input data” refer to items addressed in AS03.05 for data input, and to items addressed in AS03.08 for control input.

VE03.15.02: The vendor documentation shall specify that all input data entering the cryptographic module via the data input interface and applicable physical ports only use the specified paths. The documentation shall show that all logical and physical information flows used by the input data are consistent with the design and operation of the cryptographic module. The vendor documentation shall establish that there are no conflicts between the applicable paths that may lead to the compromise of CSPs, plaintext data, or other information of the cryptographic module.

VE03.15.03: The vendor provided documentation shall unambiguously specify format of input data and control information including length restrictions for all variable length inputs.

VE03.15.04: The vendor provided documentation shall identify which component within the cryptographic boundary is validating the format.

Required Test Procedures

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

TE03.15.01: The tester shall verify that the vendor documentation specifies the physical and logical paths used by all major categories of input data entering the cryptographic module via the data input interface. The tester shall also verify that the paths shall be documented in the specification (e.g. by highlighted or annotated copies of the schematics, block diagrams, or other information provided under AS02.07 and AS02.15 through AS02.18). The tester shall verify the documentation which type of data pass through each applicable physical port.

TE03.15.02: The tester shall verify from the vendor documentation and by inspection of the cryptographic module, that all input data entering the module via the data input interface and applicable physical ports only use the specified paths. The tester shall examine all logical and physical information flows and shall verify that the specification of the paths used by the input data is consistent with the design and operation of the cryptographic module. The tester shall verify that there are no conflicts between the applicable paths that may lead to the compromise of CSPs, plaintext data, or other information.

TE03.15.03: The tester shall verify, by inspection and from the vendor documentation, that the unambiguous specification is provided about the format of input data and control information, including length restrictions for all variable length inputs.

TE03.15.04: The tester shall verify that the identified component within the cryptographic boundary is located on the specified path under VE03.15.02.

TE03.15.05: The tester shall examine the applicable source code(s) to ensure that the identified component is actually validating the documented format.

TE03.15.06: The tester shall attempt to input data and/or control information which is not compliant with the format, and verify that such service inputs are rejected by the cryptographic module.

NOTE The test platform or configuration can impose a part of format/restrictions.

EXAMPLE 1 A device driver to use the cryptographic module is enforcing a part of the format.

EXAMPLE 2 A layer in a protocol stack supports fixed length packet only.

If it is not possible for the tester to input certain data or control information which is not compliant with the format, then the tester shall require the vendor to provide a rationale why this test cannot be performed. In such case, the tester shall follow alternative procedures allowed by the validation authority, to ensure that the cryptographic module is validating the format.

6.3.4 Trusted channel

AS03.16: (Trusted channel – Levels 3, and 4)

For the transmission of unprotected plaintext CSPs, key components and authentication data between the cryptographic module and the sender or receivers endpoint the cryptographic module <u>shall</u> implement a trusted channel.

Required Vendor Information

VE03.16.01: The vendor shall describe the method of transmission of unprotected CSPs and the way they are protected via a trusted channel.

Required Test Procedures

TE03.16.01: The tester shall verify that the trusted channel is able to protect unprotected CSPs between the cryptographic module boundary and the sender or receiver endpoint.

AS03.17: (Trusted channel – Levels 3 and 4)

The trusted channel <u>shall</u> prevent unauthorised modification, substitution, and disclosure along the communication link.

NOTE This assertion is not separately tested. Tested as part of AS03.18 or AS03.19.

Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

AS03.18: (Trusted channel – Levels 3 and 4)

The physical ports used for the trusted channel shall be physically separated from all other ports *{or AS03.19 shall be satisfied}*.

Required Vendor Information

VE03.18.01: The vendor documentation shall specify if the cryptographic module inputs or outputs plaintext CSPs. The physical port(s) used for the input and output of plaintext CSPs shall be physically separated from all other physical ports of the cryptographic module.

VE03.18.02: If the cryptographic module inputs or outputs plaintext CSPs, the module shall ensure that only plaintext CSPs enter or exit the module through the applicable physical ports, and that no other data, plaintext or encrypted, enters or exits the module via the applicable physical ports.

Required Test Procedures

TE03.18.01: The tester shall verify if the vendor documentation specifies whether the cryptographic module inputs or outputs plaintext CSPs. The tester shall verify, from the vendor documentation and also by inspection of the physical ports on the cryptographic module that the applicable physical ports used for the input and output of plaintext CSPs are physically separated from all other physical ports of the module.

TE03.18.02: If the cryptographic module inputs or outputs plaintext CSPs, the tester shall verify that only plaintext CSPs enter or exit the module through the applicable physical ports, and that no other data, plaintext or encrypted, enters or exits the module via the applicable physical ports.

AS03.19: (Trusted channels – Levels 3, and 4)

The logical interfaces used for the trusted channel shall be logically separated from all other interfaces *{or AS03.18 shall be satisfied}*.

Required Vendor Information

VE03.19.01: The vendor documentation shall describe how the logical interfaces used in the trusted channel to input and output plaintext CSPs are logically separated from all other interfaces.

VE03.19.02: If the cryptographic module inputs or outputs plaintext CSPs, the module shall ensure that plaintext CSPs enter or exit the module through the applicable logical interface using the trusted channel, and that no other data, plaintext or encrypted, enters or exits the module via the applicable logical interface using the trusted channel.

VE03.19.03: The vendor documentation shall provide rationale how the trusted channel prevents unauthorised modification, substitution, and disclosure along the communication link.

Required Test Procedures

TE03.19.01: The tester shall verify, from the vendor documentation and also by inspection of the cryptographic module that the applicable logical interfaces used in the trusted channel to input and output of plaintext CSPs are logically separated from all other logical interfaces of the module.

TE03.19.02: If the cryptographic module inputs or outputs plaintext CSPs, the tester shall verify that plaintext CSPs enter or exit the module through the applicable logical interface using the trusted channel, and that no other data, plaintext or encrypted, enters or exits the module via the applicable logical interface using the trusted channel.

TE03.19.03: The tester shall verify the correctness of any rationale provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.

TE03.19.04: The tester shall, by attempting to access the communication link, verify that the trusted channel prevents unauthorised modification, substitution, and disclosure along the communication link.

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

AS03.20: (Trusted channel – Levels 3, and 4)

Identity-based authentication shall be employed for all services utilising the trusted channel.

Required Vendor Information

VE03.20.01: The vendor shall provide description of the authentication mechanism used by the trusted channel.

Required Test Procedures

TE03.20.01: The tester shall verify that an identity-based authentication mechanism is employed for all services utilising the trusted channel. The tester shall verify that services utilising the trusted channel are not provided without successfully passing the operator authentication.

AS03.21: (Trusted channel – Levels 3, and 4)

A status indicator shall be provided when the trusted channel is in use.

Required Vendor Information

VE03.21.01: The vendor shall provide description of the indicator provided when trusted channel is in use.

Required Test Procedures

TE03.21.01: The tester shall verify, by exercising the module, that the status indicator is provided when the trusted channel is in use.

AS03.22: (Trusted channel – Level 4)

In addition to the requirements of Security Level 3, for Security Level 4 multi-factor identity-based authentication shall be employed for all services utilising the trusted channel.

Required Vendor Information

VE03.22.01: The vendor shall provide description of the multi-factor identity-based authentication mechanism used by the trusted channel.

Required Test Procedures

TE03.22.01: The tester shall verify that a multi-factor identity-based authentication mechanism is employed for all services utilising the trusted channel. The tester shall verify that services utilising the trusted channel are not provided without successfully passing the operator authentication.

6.4 Roles, services, and authentication

6.4.1 Roles, services, and authentication general requirements

AS04.01: (Roles, services, and authentication – Levels 1, 2, 3, and 4)

A cryptographic module shall support authorised roles for operators and corresponding services within each role.

NOTE This assertion is tested under AS04.11.

AS04.02: (Roles, services, and authentication – Levels 1, 2, 3, and 4)

If a cryptographic module supports concurrent operators, then the module shall internally maintain the separation of the roles assumed by each operator and the corresponding services.

Required Vendor Information

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

VE04.02.01: The vendor documentation shall specify whether multiple concurrent operators are allowed. The vendor documentation shall specify the method by which separation of the authorised roles and services performed by each operator is achieved. The vendor documentation shall also describe any restrictions on concurrent operators.

EXAMPLE 1 One operator in a maintenance role and another in a user role simultaneously is not allowed.

EXAMPLE 2 Multiple concurrent operators up to 16 operators in a user role are supported, but the only one RSA key generation service can be run at a time in the cryptographic module.

EXAMPLE 3 When multiple concurrent operators in a Crypto Officer role are logged in, but each Crypto Officer cannot change the authentication data of the other operators in a Crypto Officer role.

Required Test Procedures

TE04.02.01: The tester shall verify the vendor documentation that the method implemented by the module to enforce separation between the roles and services performed by concurrent operators is described.

TE04.02.02: The tester shall assume the identity of two independent operators: Operator1 and Operator2. The operators shall assume different roles. The tester shall verify that only the services allocated to the each role can be performed in that role. The tester shall also attempt, for each operator, to access services that are unique to the role assumed by the other operator in order to verify that separation is maintained between the roles and services allowed in concurrent operators.

TE04.02.03: If the vendor documentation specifies any restrictions on concurrent operators, the tester shall attempt to violate the restrictions by attempting to concurrently assume restricted roles as independent operators and verify that the module enforces the restrictions.

AS04.03: (Roles – Levels 1, 2, 3, and 4)

The documentation requirements specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* A.2.4 shall be provided.

Required Vendor Information

VE04.03.01: The vendor shall provide documentation as described in *{ISO/IEC 19790:2012/Cor.1:2015}* A.2.4.

Required Test Procedures

TE04.03.01: The tester shall check vendor documentation against *{ISO/IEC 19790:2012/Cor.1:2015}* A.2.4 specification.

6.4.2 Roles

AS04.04: (Roles – Levels 1, 2, 3, and 4)

A cryptographic module shall, at a minimum, support a *Crypto Officer Role*.

NOTE This assertion is not separately tested. Tested as part of AS04.05.

AS04.05: (Roles – Levels 1, 2, 3, and 4)

The *Crypto Officer Role* shall be assumed to perform cryptographic initialisation or management functions, and general security services (e.g. module initialisation, management of CSPs, PSPs, and audit functions).

Required Vendor Information

VE04.05.01: In the documentation required, the vendor shall include at least one crypto-officer role. These roles shall be specified by name and allowed services.

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

Required Test Procedures

TE04.05.01: The tester shall verify the vendor documentation that at least one crypto-officer role is defined. The tester shall verify that roles are specified by name and allowed services as specified in AS04.05.

AS04.06: (Roles – Levels 1, 2, 3, and 4)

If the cryptographic module supports a *User Role*, then the *User Role* shall be assumed to perform general security services, including cryptographic operations and other approved security functions.

Required Vendor Information

VE04.06.01: If the cryptographic module supports a User Role, the vendor provided documentation shall (1) explicitly state that a User Role is supported, and (2) completely specify the role by name and allowed services.

Required Test Procedures

TE04.06.01: The tester shall determine, from the vendor documentation, whether the cryptographic module supports a User Role. If the cryptographic module supports a User Role, the tester shall verify the vendor documentation that at least one user role is defined. The tester shall verify that user role is specified by name and allowed services as specified in AS04.06.

AS04.07: (Roles – Levels 1, 2, 3, and 4)

All unprotected SSPs shall be zeroised when entering or exiting the Maintenance Role.

Required Vendor Information

VE04.07.01: If the cryptographic module has a maintenance access interface, the vendor provided documentation shall 1) explicitly state a maintenance role is supported, 2) completely specify the role by name, purpose, and allowed services, and 3) specify the maintenance access interface under VE07.11.01.

VE04.07.02: The vendor documentation shall specify how the module's unprotected SSPs, as defined in 3.110 of ISO/IEC 19790:2012/Cor.1:2015, are actively zeroised when the maintenance role is entered or exited.

Required Test Procedures

TE04.07.01: The tester shall verify the specifications of the module interfaces whether a maintenance access interface is specified (see AS07.11). If so, the tester shall verify the vendor documentation pertaining to the authorised roles and verify that the maintenance role is specified by name, purpose, and allowed services.

TE04.07.02: The tester shall verify the specifications of the module interfaces whether a maintenance role is defined and check the zeroisation of all unprotected SSPs as described in the module specification.

TE04.07.03: While in the maintenance role, the tester shall enter, for all unprotected SSPs, known values which are effective in demonstrating the zeroisation and, upon exit from the maintenance role, shall verify that zeroisation has taken place.

6.4.3 Services

6.4.3.1 Services general requirements

AS04.08: (Services – Levels 1, 2, 3, and 4)

***Services* shall refer to all of the services, operations, or functions that can be performed by a module.**

NOTE This assertion is not separately tested.

AS04.09: (Services – Levels 1, 2, 3, and 4)

Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

Service inputs **shall consist of all data or control inputs to the module that initiate or obtain specific services, operations, or functions.**

NOTE This assertion is not separately tested.

AS04.10: (Services – Levels 1, 2, 3, and 4)

Service outputs **shall consist of all data outputs, control outputs, and status outputs that result from services, operations, or functions initiated or obtained by service inputs.**

NOTE This assertion is not separately tested.

AS04.11: (Services – Levels 1, 2, 3, and 4)

Each service input shall result in a service output.

Required Vendor Information

VE04.11.01: The vendor documentation shall describe the purpose and function of each service. The documentation shall include for each service: service inputs, corresponding service outputs, and the authorised role or roles in which the service can be performed.

Required Test Procedures

TE04.11.01: The tester shall check the vendor documentation and verify that the purpose and function of each service is described. The tester shall also check that the following information is specified for each service: service inputs, corresponding service outputs, and the authorised role or roles in which the service can be performed.

TE04.11.02: The tester shall perform the following for each service (i.e. security and non-security services, both approved and non-approved services):

— Enter each of the specified service inputs and observe that they result in the specified service outputs.

— For services that require the operator to assume a role, the role shall be assumed to enter each of the specified service inputs and observe that they result in the specified service outputs.

— For services that require the operator to assume a role, assume the role that is not specified for the service and enter each of the specified service inputs and observe that the service is not provided.

— For services that require the operator to assume an authenticated role, the role shall be assumed and authenticated to enter each of the specified service inputs and observe that they result in the specified service outputs.

— For services that require the operator to assume an authenticated role, the role shall be assumed but the authentication data shall be modified to fail authentication and enter each of the specified service inputs and observe that the service is not provided.

— For services that provide data output over the Data output interface, the tester shall verify the result against the expected result.

EXAMPLE If the service provides data output which is a function of the services data input, the tester will verify the data output result as a function of the provided input data.

AS04.12: (services – Levels 1, 2, 3, and 4)

A cryptographic module shall provide the following services to operators.

NOTE This assertion is not separately tested.

Show module's versioning information

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

AS04.13: (Services – Levels 1, 2, 3, and 4)

The cryptographic module shall output the name or module identifier and the versioning information that can be correlated with a validation record (e.g. hardware, software and/or firmware versioning information).

Required Vendor Information

VE04.13.01: The vendor documentation shall describe the output of the current name and versioning information of the cryptographic module;

VE04.13.02: The vendor provided documentation shall identify the name or module identifier and the versioning information which will be posted as the validation record.

VE04.13.03: The vendor provided documentation, either non-proprietary security policy or an Administrator guidance, shall specify how to correlate the output of the current name and the versioning information with a validation record.

Required Test Procedures

TE04.13.01: The tester shall verify that the service outputs (i.e. name, or module identifier and versioning information) are consistent with specification and with information provided under assertions AS02.11, AS02.12, and AS11.04.

TE04.13.02: The tester shall verify that the vendor provided documentation (i.e. non-proprietary security policy or an Administrator guidance) provides sufficient information to unambiguously identify the module version.

TE04.13.03: The tester shall verify that the output of the current name or module identifier and the versioning information is sufficient for an operator to correlate the module with a validation record, with the help of non-proprietary security policy or an administrator guidance.

Show Status

AS04.14: (Services – Levels 1, 2, 3, and 4)

The cryptographic module shall output current status.

Required Vendor Information

VE04.14.01: The vendor documentation shall describe the output of the current status of the module.

Required Test Procedures

TE04.14.01: The tester shall verify the vendor documentation to verify that the “Show Status” service is allocated to at least one authorised role. The tester shall verify that these services are described as specified in AS04.14.

TE04.14.02: The tester shall verify that the “Show Status” indicator matches the vendor documentation.

Perform self-tests

AS04.15: (Services – Levels 1, 2, 3, and 4)

The cryptographic module shall initiate and run the pre-operational self-tests as specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* 7.10.2.

Required Vendor Information

VE04.15.01: The vendor documentation shall describe the initiation and running of user callable self-tests.

Required Test Procedures

AVA Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015

TE04.15.01: The tester shall verify that the module provides for the initiation of the running of pre-operational self-tests, as specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* 7.10 this is performed under documentation verification in TEA.01.01.

Perform approved security functions

AS04.16: (Services – Levels 1, 2, 3, and 4)

The cryptographic module shall perform at least one approved security function used in an approved mode of operation as specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* 7.2.4.

NOTE This assertion is not separately tested.

Perform zeroisation

AS04.17: (Services – Levels 1, 2, 3, and 4)

The cryptographic module shall perform zeroisation of the parameters as specified in *{ISO/IEC 19790:2012/Cor.1:2015 subclause}* 7.9.7.

NOTE This assertion is not separately tested.

6.4.3.2 Bypass capability

AS04.18: (Bypass capability – Levels 1, 2, 3, and 4)

If the module can output a particular data or status item in a cryptographically protected form, or (as a result of module configuration or operator intervention) can also output the item in a non-protected form, then a bypass capability shall be defined.

Required Vendor Information

VE04.18.01: If the module implements a bypass capability, the vendor documentation shall describe the bypass service.

Required Test Procedures

TE04.18.01: The tester shall verify that the module implements a bypass capability as specified in the vendor documentation.

AS04.19: (Bypass capability – Levels 1, 2, 3, and 4)

***If a cryptographic module implements a bypass capability, then* the operator shall assume an authorised role before configuring the bypass capability.**

Required Vendor Information

VE04.19.01: If the module implements a bypass capability, the vendor documentation shall describe how the operator assumes an authorised role before configuring the bypass capability.

Required Test Procedures

TE04.19.01: The tester shall verify from the vendor documentation that the module requires an operator to assume an authorised role before configuring the bypass capability.

TE04.19.02: The tester shall assume the defined role that is documented to configure the bypass capability and perform the configuration.

TE04.19.03: The tester shall assume a defined role that is not documented to configure the bypass capability and attempt to perform the bypass configuration. The tester shall verify the attempt fails.

AS04.20: (Bypass capability – Levels 1, 2, 3, and 4)

Documents
Document Sharing Hub
Full document details: ISO_IEC 24759_2014_Cor 1_2015

***If a cryptographic module implements a bypass capability, then* two independent internal actions shall be required to activate the capability to prevent the inadvertent bypass of plaintext data due to a single error.**

Required Vendor Information

VE04.20.01: If the module implements a bypass capability, the vendor documentation shall describe the bypass service as specified in AS04.20.

VE04.20.02: The finite state model and other the vendor documentation shall indicate, for all transitions into an exclusive or alternating bypass state, two independent internal actions that are required to transition into each bypass state.

Required Test Procedures

TE04.20.01: The tester shall verify whether the bypass capability is implemented by the module. The tester shall verify the vendor documentation to verify that the bypass capability is allocated to at least one authorised role.

TE04.20.02: The tester shall verify the finite state model and other the vendor documentation whether each transition into an exclusive or alternating bypass state shows two independent internal actions that have to occur in order for the cryptographic module to transition into either exclusive or alternating bypass state.

TE04.20.03: The tester shall attempt to transition to each bypass state from each state that shows such a transition, and verify that it takes two internal actions to accomplish each such transition.

AS04.21: (Bypass capability – Levels 1, 2, 3, and 4)

***If a cryptographic module implements a bypass capability, then* the two independent internal actions shall modify software and/or hardware behaviour that is dedicated to mediate the bypass capability.**

Required Vendor Information

VE04.21.01: If the module implements a bypass capability, the vendor provided documentation shall specify how the two independent internal actions modify software and/or hardware behaviour that is dedicated to mediate the bypass capability.

VE04.21.02: The vendor provided documentation shall specify how the two independent internal actions protect against the inadvertent bypass of plain text data to a single error.

Required Test Procedures

TE04.21.01: The tester shall verify that vendor documentation specifies how the two independent internal actions protect against the inadvertent bypass of plain text data due to a single error.

TE04.21.02: The tester shall verify that the two independent internal actions modify software and/or hardware behaviour that is dedicated to mediate the bypass capability, by inspection and by attempting to transition to each bypass state from each state that shows such a transition.

AS04.22: (Bypass capability – Levels 1, 2, 3, and 4)

***If a cryptographic module implements a bypass capability, then* the module shall show status to indicate whether the bypass capability:**

a) *is not* activated, and the module is exclusively providing services *with* cryptographic processing (e.g. plaintext data *is* encrypted); or

b) *is* activated and the module is exclusively providing services *without* cryptographic processing (e.g. plaintext data *is not* encrypted); or

Documents
Document Sharing Hub

Full document details: ISO_IEC 24759_2014_Cor 1_2015