

Information technology — Security techniques — Test requirements for cryptographic modules

ICS 35.040

National foreword

This British Standard is the UK implementation of ISO/IEC 24759:2008. The UK participation in its preparation was entrusted to Technical Committee IST/33, IT - Security techniques.

A list of organizations represented on this committee can be obtained on request to its secretary.

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with a British Standard cannot confer immunity from legal obligations.

This British Standard was published under the authority of the Standards Policy and Strategy Committee on 31 July 2008

© BSI 2008

ISBN 978 0 580 56273 0

Amendments/corrigenda issued since publication

Date	Comments

INTERNATIONAL STANDARD

BS ISO/IEC 24759:2008

ISO/IEC 24759

First edition
2008-07-01

Information technology — Security techniques — Test requirements for cryptographic modules

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



Reference number
ISO/IEC 24759:2008(E)

AVA Documents
Document Sharing Hub
© ISO/IEC 2008

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.



COPYRIGHT PROTECTED DOCUMENT

© ISO/IEC 2008

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from either ISO at the address below or ISO's member body in the country of the requester.

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword.....	iv
1 Scope	1
2 Normative references	1
3 Terms and definitions.....	1
4 Abbreviated terms	4
5 Document Organization	5
5.1 General.....	5
5.2 Assertions and security requirements	5
5.3 Assertions with cross references	6
6 Security requirements	6
6.1 General test requirements	6
6.2 Cryptographic module specification	6
6.3 Cryptographic module ports and interfaces.....	14
6.4 Roles, services, and authentication.....	27
6.4.1 Roles	27
6.4.2 Services	28
6.4.3 Operator authentication	30
6.5 Finite state model	35
6.6 Physical security.....	39
6.6.1 General physical security requirements	39
6.6.2 Environmental failure protection/testing	55
6.7 Operational environment	57
6.8 Cryptographic key management.....	66
6.8.1 Random bit generators (RBGs)	67
6.8.2 Key generation	68
6.8.3 Key establishment	70
6.8.4 Key entry and output.....	71
6.8.5 Key storage	75
6.8.6 Key zeroisation	75
6.9 Self-tests.....	76
6.9.1 Power-up tests	79
6.9.2 Conditional tests.....	85
6.10 Design assurance	91
6.10.1 Configuration management.....	91
6.10.2 Delivery and operation	94
6.10.3 Development	95
6.10.4 Guidance documents	100
6.11 Mitigation of other attacks	101
6.12 Documentation requirements.....	102
6.13 Cryptographic module security policy	102
6.14 Approved protection profiles	103
6.15 Approved security functions	103
6.16 Approved key establishment methods.....	103
6.17 Recommended software development practices	103
6.18 Examples of mitigation of other attacks.....	103

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

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

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

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

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

Information technology — Security techniques — Test requirements for cryptographic modules

1 Scope

This International Standard specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2006. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This International Standard also specifies the requirements for information that vendors provide to testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformance to the requirements specified in ISO/IEC 19790:2006.

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

2 Normative references

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

ISO/IEC 15408 (all parts), *Information technology — Security techniques — Evaluation criteria for IT security*

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

ISO/IEC 19790:2006, *Information technology — Security techniques — Security requirements for cryptographic modules*

3 Terms and definitions

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

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

3.1

approval authority

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

[ISO/IEC 19790:2006, 3.1]

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

3.2 **ISO/IEC approved**

security function that is either

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

3.3 **asymmetric cryptographic technique**

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

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

3.4 **compromise**

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

3.5 **cryptographic module security policy** **security policy**

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

[ISO/IEC 19790:2006, 3.18]

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

3.6 **crypto officer**

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

[ISO/IEC 19790:2006, 3.19]

3.7 **firmware**

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

[ISO/IEC 19790:2006, 3.31]

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

3.8 **input data**

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

[ISO/IEC 19790:2006, 3.33]

3.9

maintenance role

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

[ISO/IEC 19790:2006, 3.41]

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

3.10

passivation

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

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

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

3.11

public key

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

[ISO/IEC 19790:2006, 3.56]

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

3.12

random bit generator

RBG

device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased

[ISO/IEC 19790:2006, 3.59]

NOTE See ISO/IEC 18031:2005.

3.13

role

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

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

3.14

security function

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

[ISO/IEC 19790:2006, 3.63]

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

3.15

seed key

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

3.16
simple power analysis
SPA

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

3.17
software

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

[ISO/IEC 19790:2006, 3.66]

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

3.18
split knowledge

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

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

3.19
system software

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

[ISO/IEC 19790:2006, 3.70]

EXAMPLES Operating system, compilers or utility programs.

3.20
tamper evidence

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

4 Abbreviated terms

API	Application Program Interface
CAPP	Controlled Access Protection Profile
CBC	Cipher Block Chaining
CC	Common Criteria, equivalent to ISO/IEC 15408
CSP	Critical Security Parameter
EAL	Evaluation Assurance Level
EDC	Error Detection Code
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
FSM	Finite State Model

HDL	Hardware Description Language
IC	Integrated Circuit
KEK	Key Encryption Key
PIN	Personal Identification Number
PROM	Programmable Read-Only Memory
PSP	Public Security Parameter
RAM	Random Access Memory
RBG	Random Bit Generator
ROM	Read-Only Memory

5 Document Organization

5.1 General

Clause 6 of this document specifies the methods that shall be used by testing laboratories and the requirements for information that vendors shall provide to testing laboratories. Clause 6 besides a general subclause 6.1 includes seventeen subclauses, corresponding to the ten areas of security requirements plus annexes A to G of ISO/IEC 19790:2006. Subclauses 6.14 to 6.18 are stating no requirements.

5.2 Assertions and security requirements

Within each subclause of clause 6, the corresponding security requirements from ISO/IEC 19790 are divided into a set of assertions (i.e., statements that have to be true for the module to satisfy the requirement of a given area at a given level). All of the assertions are direct quotations from ISO/IEC 19790:2006.

The assertions are denoted by the form

AS<requirement_number>.<assertion_sequence_number>

where “requirement_number” is the number of the corresponding area specified in ISO/IEC 19790 (i.e., one through ten) eleven corresponding Annex A of ISO/IEC 19790 and twelve corresponding Annex B of ISO/IEC 19790, and “sequence_number” is a sequential identifier for assertions within a subclause. After the statement of each assertion, the security levels to which the assertion applies (i.e., levels 1 through 4) are listed in parentheses.

Following each assertion is a set of requirements levied on the vendor. These requirements describe the types of documentation or explicit information that the vendor shall provide in order for the tester to verify conformance to the given assertion. These requirements are denoted by the form

VE<requirement_number>.<assertion_sequence_number>.<sequence_number>

where “requirement_number” and “assertion_sequence_number” are identical to the corresponding assertion requirement number and sequence number, and “sequence_number” is a sequential identifier for vendor requirements within the assertion requirement.

Also following each assertion and the requirements levied on the vendor is a set of requirements levied on the tester of the cryptographic module. These requirements instruct the tester as to what he or she shall do in order to test the cryptographic module with respect to the given assertion. These requirements are denoted by the form

TE<requirement_number>.<assertion_sequence_number>.<sequence_number>

where “requirement_number” and “assertion_sequence_number” are identical to the corresponding assertion requirement number and sequence number, and “sequence_number” is a sequential identifier for tester requirements within the assertion requirement.

5.3 Assertions with cross references

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

6 Security requirements

6.1 General test requirements

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

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

1. Tester performs tests at the tester’s facility
 2. Tester performs tests at vendor facility
 3. Tester supervises vendor performing tests at vendor facility
- Rationale is included that explains why tester could not perform the tests
 - Tester develops the required test plan and required tests
 - Tester directly observes the tests being performed

An assertion fails if any of its subsequent tests fails.

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

6.2 Cryptographic module specification

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

A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic functions or processes, and is contained within a defined cryptographic boundary.

NOTE This assertion is not separately tested.

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

A cryptographic module shall implement at least one approved security function used in an approved mode of operation.

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

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

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

The operator shall be able to determine when an approved mode of operation is selected.

Required Vendor Information

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

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

Required Test Procedure

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

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

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

For Security Levels 3 and 4, a cryptographic module shall indicate when an approved mode of operation is selected.

Required Vendor Information

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

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

Required Test Procedures

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

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

AS01.05: (Specification – Levels 1, 2, 3, and 4)

The cryptographic boundary shall consist of an explicitly defined perimeter that establishes the physical and/or logical bounds of a cryptographic module.

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

AS01.06: (Specification – Levels 1, 2, 3, and 4)

If a cryptographic module consists of software or firmware components, the cryptographic boundary shall contain the processor(s) and other hardware components that store and protect the software and firmware components.

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

Required Vendor Information

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

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

Required Test Procedures

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

TE01.06.02: The tester shall verify that, for each processor, the vendor has identified the software or firmware code modules executed by that processor, the services performed by that processor and associated code, and the memory devices containing the executable code and data.

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

AS01.07: (Specification – Levels 1, 2, 3, and 4)

The following documentation requirements {AS01.08 to AS01.17} shall apply to all security-specific hardware, software, and firmware contained within a cryptographic module.

NOTE This assertion is not separately tested.

AS01.08: (Specification – Levels 1, 2, 3, and 4)

Documentation shall specify the hardware, software, and firmware components of a cryptographic module, specify the cryptographic boundary surrounding these components, and describe the physical configuration of the module (see {sub}clause 7.5 {of ISO/IEC 19790:2006}).

Required Vendor Information

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

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

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

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

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

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

VE01.08.06: The vendor documentation shall indicate the internal layout and assembly methods (e.g., fasteners and fittings) of the module, including drawings that are at least approximately to scale. The interior of integrated circuits need not be shown.

VE01.08.07: The vendor documentation shall describe the primary physical parameters of the module, including descriptions of the enclosure, access points, circuit boards, location of power supply, interconnection wiring runs, cooling arrangements, and any other significant parameters.

Required Test Procedures

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

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

1. Processors, including microprocessors, digital signal processors, custom processors, microcontrollers, or any other types of processors.
2. Read-only memory (ROM) integrated circuits for program executable code and data (this may include mask-programmed ROM, programmable ROM (PROM) such as ultraviolet, erasable PROM (EPROM), electrically erasable PROM (EEPROM), or Flash-memory).
3. Random-access memory (RAM) or other integrated circuits for temporary data storage.
4. Semi-custom, application-specific integrated circuits, such as gate arrays, programmable logic arrays, field programmable gate arrays, or other programmable logic devices.
5. Fully custom, application-specific, integrated circuits, including any custom cryptographic integrated circuits.
6. Other active electronic circuit elements (the vendor does not have to list passive circuit elements such as pull up/pull down resistors or bypass capacitors if they do not provide security relevant function as part of the cryptographic module).
7. Power supply components, including power supply, voltage conversion modules (e.g., AC-to-DC or DC-to-DC modules), transformers, input power connectors, and output power connectors.
8. Circuit boards or other component mounting surfaces.
9. Enclosures, including any removable access doors or covers.
10. Physical connectors for devices outside the cryptographic module, or between any major independent submodules of the module.
11. Software/firmware modules that are modifiable.
12. Software/firmware modules that are unlikely to be modified.
13. Other component types not listed above.

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

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

2. The specification of the processors and software/firmware under assertion AS01.06. Verify that the list of processors, software modules, and hardware modules in the components list is the same as in the specifications under Assertion AS01.06.
3. The specification of the physical configuration under assertion AS01.08. Verify that the list of physical structures in the components list (such as circuit boards or other mounting surfaces, enclosures, and connectors) is the same as in the specifications under Assertion AS01.08.
4. The specification of the block diagram under assertion AS01.13. Verify that any individual components called out in the block diagram (e.g., processors, application-specific integrated circuits) are also listed in the components list.
5. Any components that are to be excluded from the requirements of ISO/IEC 19790 under the provisions of assertion AS01.09. Verify that components to be so excluded are still listed in the components list.

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

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

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

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

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

TE01.08.10: The tester shall verify that the vendor's documentation shows the internal layout of the module, including the placement and approximate dimensions of major identifiable components of the module. This has to include drawings that are at least approximately to scale.

TE01.08.11: The tester shall verify that the vendor's documentation indicates the major physical assemblies of the module and how they are assembled or inserted into the module.

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

1. Enclosure shape and approximate dimensions, including any access doors or covers
2. Circuit board(s) approximate dimensions, layout, and interconnections

3. Location of power supply, power converters, and power inputs and outputs
4. Interconnection wiring runs: routing and terminals
5. Cooling arrangements, such as conduction plates, cooling airflow, heat exchanger, cooling fins, fans, or other arrangements for removing heat from the module
6. Other component types not listed above

AS01.09: (Specification – Levels 1, 2, 3, and 4)

Documentation shall specify any hardware, software, or firmware components of a cryptographic module that are excluded from the security requirements of this International Standard {i.e., ISO/IEC 19790:2006} and explain the rationale for the exclusion.

Required Vendor Information

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

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

Required Test Procedures

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

TE01.09.02: If the vendor has indicated that certain components of the module are to be excluded from the requirements of ISO/IEC 19790, the tester shall verify that a rationale for each exclusion is provided. The rationale has to show that even if the component malfunctions, it cannot cause a potential release of CSPs, plaintext data, or other information that if misused could lead to a compromise. Rationale that may be acceptable, if adequately supported by documentation, include:

1. The component does not process CSPs, plaintext data, or other information that if misused could lead to a compromise
2. The component is not connected with security relevant components of the module that would allow inappropriate transfer of CSPs, plaintext data, or other information that if misused could lead to a compromise
3. All information processed by the component is strictly for internal use of the module, and does not in any way impact the equipment to which the module is connected

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

AS01.10: (Specification – Levels 1, 2, 3, and 4)

Documentation shall specify the physical ports and logical interfaces and all defined input and output data paths of a cryptographic module.

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

AS01.11: (Specification – Levels 1, 2, 3, and 4)

Documentation shall specify the manual or logical controls of a cryptographic module, physical or logical status indicators, and relevant physical, logical, and electrical characteristics.

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

AS01.12: (Specification – Levels 1, 2, 3, and 4)

Documentation shall list all security functions, both approved and non-approved, that are employed by the cryptographic module and shall specify all modes of operation, both approved and non-approved.

Required Vendor Information

VE01.12.01: The vendor shall provide a validation certificate for all approved security functions.

VE01.12.02: The vendor shall provide a list of all non-approved security functions.

Required Test Procedures

TE01.12.01: The tester shall verify that the vendor has provided validated certificate(s).

TE01.12.02: The tester shall verify that the vendor has provided the list of non-approved security functions.

AS01.13: (Specification – Levels 1, 2, 3, and 4)

Documentation shall specify a block diagram depicting all of the major hardware components of a cryptographic module and component interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory.

Required Vendor Information

VE01.13.01: The vendor documentation shall include a block diagram showing the hardware components and their interconnections. Components to be included in the block diagram shall include, as applicable:

1. Microprocessors
2. Input/output buffers
3. Plaintext/ciphertext buffers
4. Control buffers
5. Key storage
6. Working memory
7. Program memory
8. Other components types not listed above

VE01.13.02: The block diagram shall also include any (semi-) custom integrated circuits (e.g., gate arrays, field programmable gate arrays, or other programmable logic).

VE01.13.03: The block diagram shall show interconnections among major components of the module and between the module and equipment or components outside of the cryptographic boundary as required under assertion AS01.08 in this subclause.

VE01.13.04: The block diagram shall show the cryptographic boundary of the cryptographic module.

Required Test Procedures

TE01.13.01: The tester shall verify that the vendor has provided one or more block diagrams indicating major components of the cryptographic module. These shall include at least the following, as applicable to the vendor's design:

1. Microprocessors or any other processors listed in the components list under assertion AS01.08 in this subclause
2. Input/output buffer memory that stores or processes general input or output data other than plaintext/ciphertext message data or control information
3. Plaintext/ciphertext buffer memory that stores or processes message data to be encrypted or decrypted
4. Control buffer memory that stores or processes control and status information that is input into the module or output from the module
5. Key storage
6. Working memory for processing information
7. Program memory containing executable software or firmware code
8. (Semi-) custom integrated circuits, (e.g., application-specific integrated circuits, gate arrays, field programmable gate arrays, programmable logic arrays, or other programmable logic devices
9. Other components types not listed above

TE01.13.02: The tester shall verify that the block diagram indicates all significant interconnections and data flow among major components of the module, and between the module and outside equipment. In particular, each line on the block diagram indicating an interconnection has to be labelled with the type of information it transmits.

TE01.13.03: The tester shall verify that the block diagram indicates the cryptographic boundary for the cryptographic module, as required under assertion AS01.08 in this subclause.

AS01.14: (Specification – Levels 1, 2, 3, and 4)

Documentation shall specify the design of the hardware, software, and firmware components of a cryptographic module. High-level specification languages for software/firmware or schematics for hardware shall be used to document the design.

Required Vendor Information

VE01.14.01: The vendor shall provide a detailed specification of the design of the hardware, software, and/or firmware contained in the module. This documentation shall include, the finite state model and description referred to in subclause 7.4 of ISO/IEC 19790:2006. If the relationship between the finite state model and the design specification is not clear, the vendor shall provide additional documentation that sufficiently describes this relationship.

Required Test Procedures

TE01.14.01: The tester shall compare the design specification against the list of names of all hardware, software, and firmware components as documented in AS09.20 and AS09.21 to verify that the relationship between the finite state model and the design specification can be determined.

AS01.15: (Specification – Levels 1, 2, 3, and 4)

Documentation shall specify all security-related information, including CSPs, PSPs and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module.

Required Vendor Information

VE01.15.01: The vendor shall provide documentation specifying all security-related information, including secret and private cryptographic keys (both plaintext and encrypted), authentication data (e.g., passwords, PINs), CSPs, PSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module.

Required Test Procedures

TE01.15.01: The tester shall verify that the documentation specifies all security-related information, including CSPs, PSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module.

AS01.16: (Specification – Levels 1, 2, 3, and 4)

Documentation shall specify a cryptographic module security policy.

NOTE This assertion is tested as part of AS01.17

AS01.17: (Specification – Levels 1, 2, 3, and 4)

The security policy shall include the rules derived from the requirements of this {ISO/IEC 19790:2006} International Standard and the rules derived from any additional requirements imposed through product development (see Annex B {of ISO/IEC 19790:2006}).

NOTE This assertion is tested as part of AS12.01

6.3 Cryptographic module ports and interfaces

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

A cryptographic module shall restrict all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module.

Required Vendor Information

VE02.01.01: The vendor documentation shall specify each of the physical ports and logical interfaces of the cryptographic module, including the:

1. Physical ports and their pin assignments
2. Physical covers, doors or openings
3. Logical interfaces (e.g., APIs and all other data/control/status signals) and the signal names and functions
4. Manual controls (e.g., buttons or switches) for applicable physical control inputs
5. Physical status indicators (e.g., lights or displays) for applicable physical status outputs
6. Mapping of the logical interfaces to the physical ports, manual controls, and physical status indicators of the cryptographic module
7. Physical, logical, and electrical characteristics, as applicable, of the above ports and interfaces

VE02.01.02: 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 subclauses 6.2 and 6.10 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 AS01.08, AS01.10, and AS01.13 without inconsistencies in the description of components and physical layout for the input/output ports.

VE02.01.03: 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 subclauses 6.2 and 6.10 of this International Standard, and the specifications of the logical interfaces provided in assertions AS02.03 to AS02.09 of this subclause.

Required Test Procedures

TE02.01.01: 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:

1. 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
2. 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
3. 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
4. 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
5. 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
6. 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
7. 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

TE02.01.02: 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 subclauses 6.2 and 6.10 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 AS01.08, AS01.10, and AS01.13 and verify that there are no inconsistencies in the description of components and physical layout for the input/output ports.

TE02.01.03: 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 subclauses 6.2 and 6.10 of this International Standard, and the specifications of the logical interfaces provided in assertions AS02.03 to AS02.09 of this subclause.

TE02.01.04: 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.

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

The cryptographic module logical interfaces shall be distinctly defined 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).

Required Vendor Information

VE02.02.01: The vendor's design shall separate the cryptographic module interfaces into logically distinct and isolated categories, using the categories listed in assertion AS02.03, and, if applicable, AS02.09 in this subclause. This information shall be consistent with the specification of the logical interfaces and physical ports provided in AS02.01 in this subclause.

VE02.02.02: 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

TE02.02.01: 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 AS02.03 and, if applicable, AS02.09 of this subclause. This information shall be consistent with the specification and design of the logical interfaces and physical ports provided in AS02.01 in this subclause.

TE02.02.02: 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.

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

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

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

Required Vendor Information

VE02.03.01: The vendor documentation shall separate the cryptographic module interfaces into logically distinct and isolated categories by the following four distinctly defined logical interfaces within the cryptographic module ("input" and "output" are indicated from the perspective of the module):

- data input interface (for the input of data as specified in AS02.04),
- data output interface (for the output of data as specified in AS02.05 and AS02.06),
- control input interface (for the input of commands as specified in AS02.07), and
- status output interface (for the output of status information as specified in AS02.08).

Required Test Procedures

TE02.03.01: The tester shall verify that the vendor documentation specifies that the four logical interfaces as listed in VE02.03.01 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 AS02.04 to AS02.08 in this subclause.

Data input interface

AS02.04: (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, CSPs, PSPs, and status information from another module) shall enter via the "data input" interface.

Required Vendor Information

VE02.04.01: 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:

1. Plaintext data
2. Ciphertext or signed data
3. Cryptographic keys and other key management data (plaintext or encrypted)
4. Authentication data (plaintext or encrypted)
5. Status information from external sources
6. Any other input data

VE02.04.02: 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

TE02.04.01: 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:

1. Plaintext data that is to be encrypted or signed by the cryptographic module
2. Ciphertext or signed data that is to be decrypted or verified by the module
3. 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 subclause 7.7 of ISO/IEC 19790:2006)
4. Plaintext or encrypted authentication data that is input into the cryptographic module, including passwords, PINs, and/or biometric information
5. Status information from external sources (e.g., another cryptographic module or device)
6. Any other information that is input into the cryptographic module for processing or storage, except for control information that is covered separately in AS02.07

NOTE For Security Levels 1 and 2, the physical port or ports used for the entry of plaintext CSPs may be shared with other physical ports of the cryptographic module. (Corresponding requirements for Security Levels 3 and 4 are covered separately under assertion AS02.16 in this subclause.)

TE02.04.02: 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

AS02.05: (Data output interface – Levels 1, 2, 3, and 4)

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

Required Vendor Information

VE02.05.01: The cryptographic module shall have a data output interface. All data (except status data output via the status output interface) that has been processed and is to be output by the cryptographic module shall exit via the data output interface, including:

1. Plaintext data
2. Ciphertext data and digital signatures
3. Cryptographic keys and other key management data (plaintext or encrypted)
4. Control information to external targets
5. Any other output data

NOTE For Security Levels 1 and 2, the physical port or ports used for the output of plaintext cryptographic keys and other plaintext CSPs may be shared with other physical ports of the cryptographic module. (Corresponding requirements for Security Levels 3 and 4 are covered separately under assertion AS02.16 in this subclause.)

VE02.05.02: 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

TE02.05.01: 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) that has been processed and is to be output by the cryptographic module exits via the data output interface, including:

1. Plaintext data that has been decrypted by the cryptographic module
2. Ciphertext data that has been encrypted, and digital signatures that have been generated by the cryptographic module
3. 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 subclause 7.7 of ISO/IEC 19790:2006)
4. Control information sent outside the cryptographic module to external targets (e.g., another cryptographic module or device)
5. Any other information that is output from the cryptographic module after processing or storage except for status information that is covered separately in AS02.08 in this subclause.

NOTE For Security Levels 1 and 2, the physical port or ports used for the output of plaintext CSPs may be shared with other physical ports of the cryptographic module. For Security Levels 3 and 4 the tester shall verify separately that the corresponding requirements under assertion AS02.15 or AS02.16 in this subclause are covered.

TE02.05.02: 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.

AS02.06: (Data output interface – Levels 1, 2, 3, and 4)

All data output via the data output interface shall be inhibited when an error state exists and during self-tests (see {sub}clause 7.8 {of ISO/IEC 19790:2006}).

Required Vendor Information

VE02.06.01: The vendor documentation shall specify how the cryptographic module ensures that all data output via the data output interface is inhibited whenever the module is in an error state (error states are covered in subclause 7.4 of ISO/IEC 19790:2006). Status information may be allowed from the status output interface to identify the type of error, as long as no CSPs, plaintext data, or other information that if misused could lead to a compromised.

VE02.06.02: The vendor documentation shall specify how the design of the cryptographic module ensures that all data output via the data output interface is inhibited whenever the module is in a self-test condition (self-tests are covered in subclause 7.8 of ISO/IEC 19790:2006). Status information to display the results of the self-tests may be allowed from the status output interface, as long as no CSPs, plaintext data, or other information that if misused could lead to a compromise.

Required Test Procedures

TE02.06.01: 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 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 data output via the data output interface is inhibited, until error recovery occurs. Status information to identify the type of error may be allowed from the status output interface, as long as the tester can verify that no CSPs, plaintext data, or other information that if misused could lead to a compromise. The tester shall also verify

that the error states specified in response to this assertion are identical to the error states specified under AS04.03.

TE02.06.02: The tester shall cause the cryptographic module to enter each specified error state and verify that all data output via the data 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-detected cover or door, entering incorrectly-formatted commands, keys, or parameters, reducing input voltage, and/or any other error-causing actions.

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.

TE02.06.03: 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, as long as the tester can verify that no CSPs, plaintext data, or other information that if misused could lead to a compromise. The tester shall also verify that the self-test conditions specified in response to this assertion are identical to the self tests specified under AS08.07.

TE02.06.04: 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 display the results of the self-tests, the tester shall verify that no CSPs, plaintext data, or other information that if misused could lead to a compromise.

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.

TE02.06.05: 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

AS02.07: (Control input interface – Levels 1, 2, 3, and 4)

All input commands, signals, 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

VE02.07.01: 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:

1. Commands input logically via an API (e.g., for the software and firmware components of the cryptographic module)
2. Signals input logically or physically via one or more physical ports (e.g., for the hardware components of the cryptographic module)
3. Manual control inputs (e.g., using switches, buttons, or a keyboard)
4. Any other input control data

VE02.07.02: 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

TE02.07.01: 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:

1. Commands input logically via an API, such as function calls to a software library or to a smart card
2. 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
3. Manual control inputs (e.g., using switches, buttons, or a keyboard)
4. Any other input control data

TE02.07.02: 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.

Status output interface

AS02.08: (Status output interface – Levels 1, 2, 3, and 4)

All output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of a cryptographic module shall exit via the “status output” interface.

Required Vendor Information

VE02.08.01: 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:

1. Status information output logically via an API
2. Signals output logically or physically via one or more physical
3. Manual status outputs (e.g., using LEDs, buzzers, or a display)
4. Any other output status information

VE02.08.02: 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

TE02.08.01: 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:

1. Status information output logically via an API, such as return codes from a software library or a smart card
2. Signals output logically or physically via one or more physical ports, such as status information sent through a serial port or a PC Card connector
3. Manual status outputs (e.g., using LEDs, buzzers, or a display)
4. Any other output status information

TE02.08.02: 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, such as smart cards, tokens, displays, and/or other storage devices.

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

All external electrical power that is input to a cryptographic module (including power from an external power source or batteries) shall enter via a power port.

Required Vendor Information

VE02.09.01: If the cryptographic module requires or provides power to/from other devices external to the boundary (e.g., a power supply or a external battery), the vendor documentation shall specify a power interface and a corresponding physical port.

VE02.09.02: 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

TE02.09.01: 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.

TE02.09.02: 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.

NOTE A power interface may not be required if all power is provided or maintained internally to the module, and that replacement of an internal battery is considered a physical maintenance activity, and is subject to the requirements specified in subclause 7.5 of ISO/IEC 19790:2006.

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

The cryptographic module shall distinguish between data and control data for input and on the other hand data and status for output.

Required Vendor Information

VE02.10.01: The vendor documentation shall specify how the cryptographic module distinguishes between data and control for input and data 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 and status information exiting the module via the applicable output interfaces.

VE02.10.02: 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 and status information. If the physical and logical paths used by the input data and control information and the output data and status information are physically shared, the vendor documentation shall specify how logical separation is enforced by the cryptographic module.

VE02.10.03: The vendor documentation shall show consistency and shall show that the cryptographic module distinguishes between data and control for input and data 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 and status information exiting the module via the applicable output interfaces.

Required Test Procedures

TE02.10.01: The tester shall verify that the vendor documentation specifies how the cryptographic module distinguishes between data and control for input and data 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 and status information exiting to the status output interface.

TE02.10.02: 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 and status information. If the physical and logical paths used by the input data and control information and the output data and status information are physically shared, the tester shall verify that the vendor documentation specifies how logical separation is enforced by the cryptographic module.

TE02.10.03: 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 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 and status information exiting the module via the applicable output interfaces.

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

All input data entering the cryptographic module via the “data input” interface shall only pass through the input data path.

Required Vendor Information

VE02.11.01: 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 AS01.08, AS01.09, and AS01.13). 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.

VE02.11.02: 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.

Required Test Procedures

TE02.11.01: 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 AS01.08, AS01.09, and AS01.13). The input data paths shall be specified in sufficient detail for the tester to verify which type of data pass through each applicable physical port.

TE02.11.02: 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.

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

All output data exiting the cryptographic module via the “data output” interface shall only pass through the output data path.

Required Vendor Information

VE02.12.01: The vendor documentation shall specify the physical and logical paths used by all major categories of output data exiting the cryptographic module via the data output 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 AS01.08, AS01.09, and AS01.13).

VE02.12.02: All output data exiting the cryptographic module via the data output interface shall only use the specified paths.

Required Test Procedures

TE02.12.01: The tester shall verify that the vendor documentation specifies the physical and logical paths used by all major categories of output data exiting the cryptographic module via the data output 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 AS01.08, AS01.09, and AS01.13). The output data paths shall be specified in sufficient detail for the tester to verify which type of data passes through each applicable physical port.

TE02.12.02: The tester shall verify from the vendor documentation and by inspection of the cryptographic module, that all output data exiting the module via the data output 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 output 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.

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

The output data path shall be logically disconnected from the circuitry and processes while performing key generation, manual key entry, or key zeroisation.

Required Vendor Information

VE02.13.01: The vendor documentation shall specify how the physical and logical paths used by all major categories of output data exiting the cryptographic module are logically or physically disconnected from the processes performing key generation, manual key entry, and zeroisation of CSPs.

VE02.13.02: If the physical and logical paths followed by the output data and CSP information are physically shared, the cryptographic module shall enforce logical separation of the output data and CSP information.

VE02.13.03: The cryptographic module shall not allow the specified key processes to pass CSP information to the output data path, and shall not allow output data exiting the module to interfere with the key processes.

Required Test Procedures

TE02.13.01: The tester shall verify that the vendor documentation specifies how the physical and logical paths used by all major categories of output data exiting the cryptographic module are logically or physically disconnected from the processes performing key generation, manual key entry, and zeroisation of CSPs.

TE02.13.02: If the physical and logical paths followed by the output data and CSP information are physically shared, the tester shall verify that the vendor documentation specifies how the cryptographic module enforces logical separation of the output data and CSP information.

TE02.13.03: The tester shall verify that the output data path is logically or physically disconnected from the processes performing key generation, manual key entry, and zeroisation of CSPs by recording or observing the output data interface and the applicable physical ports and verifying that no CSP information is released.

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

To prevent the inadvertent output of sensitive information, two independent internal actions (e.g., two different software flags are set, one of which may be user initiated; or two hardware gates are set serially from two separate actions) shall be required to output plaintext CSPs or sensitive data via any output interface.

Required Vendor Information

VE02.14.01: If the cryptographic module allows plaintext CSPs or sensitive data to be output on one or more physical ports, two independent internal actions shall be performed by the module before the plaintext CSPs or sensitive data may be output. The vendor documentation shall specify the two independent internal actions performed and how the two independent internal actions protect against the inadvertent release of the plaintext CSPs or sensitive data.

VE02.14.02: If any software or firmware components are executed in the process of outputting plaintext CSPs or sensitive data, the cryptographic module shall ensure that the software or firmware components support the requirement for two independent internal actions before the output of any plaintext CSPs or sensitive data occurs.

Required Test Procedures

TE02.14.01: The tester shall verify whether the cryptographic module allows plaintext CSPs or sensitive data to be output on one or more physical ports. The tester shall verify that the vendor documentation specifies the two independent internal actions performed by the cryptographic module before the plaintext CSPs or sensitive data may be output. The tester shall also verify that the vendor documentation specifies how the two independent internal actions protect against the inadvertent release of the plaintext CSPs or sensitive data.

TE02.14.02: The tester shall cause the output of plaintext CSPs or sensitive data on one or more physical ports, and verify that the two independent internal actions function as specified. If any software or firmware components are executed in the process of outputting plaintext CSPs or sensitive data, the tester shall verify the applicable source code listings to ensure that the software or firmware components support the requirement for two independent internal actions before the output of any plaintext CSPs or sensitive data occurs.

AS02.15: (Ports and interfaces – Levels 3 and 4)

The physical port(s) used for the input and output of plaintext CSPs shall be physically separated from all other ports of the cryptographic module {or AS02.16 shall be satisfied}.

Required Vendor Information

VE02.15.01: 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.

VE02.15.02: 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

TE02.15.01: 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.

TE02.15.02: 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.

AS02.16: (Ports and interfaces – Levels 3 and 4)

The logical interfaces used for the input and output of plaintext CSPs shall be logically separated from all other interfaces using a trusted path {or AS02.15 shall be satisfied}.

Required Vendor Information

VE02.16.01: The vendor documentation shall specify if the cryptographic module inputs or outputs plaintext CSPs. The logical interfaces used for the input and output of plaintext CSPs shall be logically separated from all other interfaces using a trusted path.

VE02.16.02: 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 logical interface using the trusted path, and that no other data, plaintext or encrypted, enters or exits the module via the applicable logical interface using the trusted path.

Required Test Procedures

TE02.16.01: 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 cryptographic module that the applicable physical ports used for the input and output of plaintext CSPs are logically separated from all other logical interfaces of the module using a trusted path

TE02.16.02: 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 logical interface using the trusted path, and that no other data, plaintext or encrypted, enters or exits the module via the applicable logical interface using the trusted path.

AS02.17: (Ports and interfaces – Levels 3 and 4)

Plaintext CSPs shall be entered into the cryptographic module either via a trusted path or directly without travelling through any enclosing or intervening systems where the key components may inadvertently be stored, combined, or otherwise processed. (See {sub}clause 7.7.4 {of ISO/IEC 19790:2006})

Required Vendor Information

VE02.17.01: The vendor documentation shall specify if the cryptographic module inputs plaintext CSPs. The physical paths used for the input of these parameters shall be directly connected to the cryptographic boundary (e.g., via a trusted path or directly attached cable) of the cryptographic module without passing through any intervening systems, processors, circuitry, or other areas outside the cryptographic boundary.

Required Test Procedures

TE02.17.01: The tester shall verify if the vendor documentation specifies whether the cryptographic module inputs plaintext CSPs. The tester shall verify from the vendor documentation and also by inspection of the physical paths and the cryptographic boundary, that the physical ports used for the input of these parameters shall be directly connected to the cryptographic boundary (e.g., via a trusted path or directly attached cable) of the cryptographic module without passing through any intervening systems, processors, circuitry, or other areas outside the cryptographic boundary.

6.4 Roles, services, and authentication

AS03.01: (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 not separately tested.

AS03.02: (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

VE03.02.01: The vendor documentation shall specify whether multiple concurrent operators are allowed. The vendor shall describe 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 (e.g., one operator in a maintenance role and another in a user role simultaneously is not allowed).

Required Test Procedures

TE03.02.01: 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.

TE03.02.02: 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.

TE03.02.03: 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 by preventing the second operator from assuming the role.

6.4.1 Roles

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

A cryptographic module shall support the following authorised roles for operators:

User Role: The role assumed to perform general security services, including cryptographic operations and other approved security functions.

Crypto Officer Role: The role assumed to perform cryptographic initialisation or management functions (e.g., module initialisation, input/output of CSPs, PSPs, and audit functions).

Required Vendor Information

VE03.03.01: In the documentation required, the vendor shall include at least one user role and one crypto-officer role. These roles shall be specified by name and allowed services.

Required Test Procedures

TE03.03.01: The tester shall verify the vendor documentation that at least one user role and one crypto-officer role are defined. The tester shall verify that roles are specified by name and allowed services as specified above.

NOTE The assumption of roles shall be tested by TE03.02.02.

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

If the cryptographic module allows operators to perform maintenance services, then the module shall support the following authorised role:

Maintenance Role: The role assumed to perform physical maintenance and/or logical maintenance services (e.g., hardware/software diagnostics).

Required Vendor Information

VE03.04.01: If the cryptographic module has a maintenance interface, the vendor documentation shall explicitly state a maintenance role is supported. The documentation shall completely specify the role by name and allowed services.

Required Test Procedures

TE03.04.01: The tester shall verify the specifications of the module interfaces whether a maintenance interface is specified (see AS05.08). 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.

NOTE The assumption of roles is tested by TE03.02.02.

AS03.05: (Roles – Levels 1, 2, 3, and 4)

All CSPs shall be zeroised when entering or exiting the maintenance role.

Required Vendor Information

VE03.05.01: The vendor documentation shall specify how the module's CSPs, as defined in subclause 3.13 of ISO/IEC 19790, are actively zeroised when the maintenance role is entered or exited.

Required Test Procedures

TE03.05.01: If the vendor documentation states that a maintenance role is implemented in the module, the tester shall verify that the vendor documentation specifies the method by which all plaintext CSPs are zeroised when the maintenance role is entered or exited.

TE03.05.02: The tester shall, while in a non-maintenance role, enter known nonzero values for all plaintext CSPs. Upon assuming the maintenance role, the tester shall verify that zeroisation has taken place.

TE03.05.03: While in the maintenance role, the tester shall enter known nonzero values for all plaintext CSPs and, upon exit from the maintenance role, shall verify that zeroisation has taken place.

6.4.2 Services

AS03.06: (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.

AS03.07: (Services – Levels 1, 2, 3, and 4)

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.