INTERNATIONAL STANDARD

ISO/IEC 24759

First edition
2008-07-01

Information technology — Security techniques — Test requirements for cryptographic modules

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

Reference number
ISO/IEC 24759:2008(E)

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

Published in Switzerland

Contents

Page

Foreword

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

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

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

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

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

Information technology — Security techniques — Test requirements for cryptographic modules

1 Scope

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

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

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

2 Normative references

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

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

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

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

3 Terms and definitions

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

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

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

[ISO/IEC 19790:2006, 3.1]

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

3.2
ISO/IEC approved
security function that is either

— specified in an ISO/IEC standard, or

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

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

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

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

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

[ISO/IEC 19790:2006, 3.18]

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

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

[ISO/IEC 19790:2006, 3.19]

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

[ISO/IEC 19790:2006, 3.31]

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

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

[ISO/IEC 19790:2006, 3.33]

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

[ISO/IEC 19790:2006, 3.41]

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

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

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

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

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

[ISO/IEC 19790:2006, 3.56]

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

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

[ISO/IEC 19790:2006, 3.59]

NOTE See ISO/IEC 18031:2005.

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

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

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

[ISO/IEC 19790:2006, 3.63]

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

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

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

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

[ISO/IEC 19790:2006, 3.66]

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

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

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

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

[ISO/IEC 19790:2006, 3.70]

EXAMPLES Operating system, compilers or utility programs.

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

4 Abbreviated terms

API Application Program Interface

CAPP Controlled Access Protection Profile

CBC Cipher Block Chaining

CC Common Criteria, equivalent to ISO/IEC 15408

CSP Critical Security Parameter

EAL Evaluation Assurance Level

EDC Error Detection Code

EFP Environmental Failure Protection

EFT Environmental Failure Testing

FSM Finite State Model

HDL Hardware Description Language

IC Integrated Circuit

KEK Key Encryption Key

PIN Personal Identification Number

PROM Programmable Read-Only Memory

PSP Public Security Parameter

RAM Random Access Memory

RBG Random Bit Generator

ROM Read-Only Memory

5 Document Organization

5.1 General

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

5.2 Assertions and security requirements

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

The assertions are denoted by the form

AS<requirement_number>.<assertion_sequence_number>

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

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

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

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

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

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

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

5.3 Assertions with cross references

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

6 Security requirements

6.1 General test requirements

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

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

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

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

An assertion fails if any of its subsequent tests fails.

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

6.2 Cryptographic module specification

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

NOTE This assertion is not separately tested.

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

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

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

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

Required Vendor Information

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

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

Required Test Procedure

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

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

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

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

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

NOTE This assertion is not separately tested.

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

Required Vendor Information

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

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

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

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

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

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

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

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

Required Test Procedures

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

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

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

2. Read-only memory (ROM) integrated circuits for program executable code and data (this may include mask-programmed ROM, programmable ROM (PROM) such as ultraviolet, erasable PROM (EPROM), electrically erasable PROM (EEPROM), or Flash-memory.

3. Random-access memory (RAM) or other integrated circuits for temporary data storage.

4. Semi-custom, application-specific integrated circuits, such as gate arrays, programmable logic arrays, field programmable gate arrays, or other programmable logic devices.

5. Fully custom, application-specific, integrated circuits, including any custom cryptographic integrated circuits.

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

7. Power supply components, including power supply, voltage conversion modules (e.g., AC-to-DC or DC-to-DC modules), transformers, input power connectors, and output power connectors.

8. Circuit boards or other component mounting surfaces.

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

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

11. Software/firmware modules that are modifiable.

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

13. Other component types not listed above.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4. Interconnection wiring runs: routing and terminals

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

6. Other component types not listed above

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

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

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

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

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

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

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 andCSP 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 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 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 senstive 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.

AS03.08: (Services – Levels 1, 2, 3, and 4)
Service outputs shall consist of all data and status outputs that result from services, operations, or functions initiated or obtained by service inputs.

NOTE This assertion is not separately tested.

AS03.09: (Services – Levels 1, 2, 3, and 4)

Each service input shall result in a service output.

NOTE This assertion is not separately tested.

AS03.10: (Services – Levels 1, 2, 3, and 4)

A cryptographic module shall provide the following services to operators:

1. ***Show Status.*** **Output the current status of the cryptographic module.**

2. ***Perform Self-Tests.*** **Initiate and run the self-tests as specified in *{sub}*clause 7.8 *{of ISO/IEC 19790:2006}*.**

3. ***Perform Approved Security Function.*** **Perform at least one approved security function used in an approved mode of operation, as specified in *{sub}*clause 7.1 *{of ISO/IEC 19790:2006}*.**

Required Vendor Information

VE03.10.01: The vendor documentation shall describe the output of the current status of the module and the initiation and running of user callable self-tests, along with other services as specified by VE11.01.01.

Required Test Procedures

TE03.10.01: The tester shall verify the vendor documentation to verify that the “Show Status” service and the user callable self-test initiation service are each allocated to at least one authorised role. The tester shall verify that these services are described as specified in AS11.01.

TE03.10.02: The tester shall verify that the “Show Status” indicator matches the vendor documentation.

TE03.10.03: The tester shall verify that the module provides for the initiation of the running of power-up self-tests, as specified in subclause 7.9 of ISO/IEC 19790: this is performed under documentation verification in TE11.01.01.

AS03.11: (Services – Levels 1, 2, 3, and 4)
If a cryptographic module implements a bypass capability, where services are provided without cryptographic processing (e.g., transferring plaintext through the module without encryption), 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 (e.g., two different software or hardware flags are set, one of which may be user-initiated), and
- the module shall show status to indicate whether the bypass capability:
    - ***is*** **not activated, and the module is exclusively providing services with cryptographic processing (e.g., plaintext data is encrypted);**
    - ***is*** **activated and the module is exclusively providing services without cryptographic processing (e.g., plaintext data is not encrypted); or**
    - ***is*** **alternately activated and deactivated and the module is providing some services with cryptographic processing and some services without cryptographic processing (e.g., for modules with multiple communication channels, plaintext data is or is not encrypted depending on each channel configuration).**

Required Vendor Information

VE03.11.01: If the module implements a bypass capability, the vendor documentation shall describe the bypass service as specified in AS03.11.

VE03.11.02: 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

TE03.11.01: 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.

TE03.11.02: 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.

TE03.11.03: 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.

6.4.3 Operator authentication

NOTE A cryptographic module is not required to employ authentication mechanisms for Security Level 1 to control access to the module.

AS03.12: (Operator authentication – Levels 2, 3, and 4)

Depending on the security level, the module shall support at least one of the following mechanisms to control access to the module. It shall support either:

- **Role-Based Authentication *{AS03.13 to AS03.15}* or**
- **Identity-Based Authentication *{AS03.16 and AS03.17}*.**

NOTE This assertion is not separately tested.

Role-Based Authentication

AS03.13: (Role-based authentication – Level 2)

If role-based authentication mechanisms are supported by a cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator.

NOTE This assertion is not separately tested.

AS03.14: (Role-based authentication – Level 2)

***{If role-based authentication mechanisms are supported by the cryptographic module, the module}* shall authenticate the assumption of the selected role (or set of roles).**

Required Vendor Information

VE03.14.01: The vendor shall document the type of authentication performed for the module. The vendor shall document the mechanisms used to perform the implicit or explicit selection of a role or set of roles and the authentication of the operator to assume the role(s).

Required Test Procedures

TE03.14.01: The tester shall verify that the vendor documentation specifies the mechanisms used for the selection of a role or roles and the authentication of the operator to assume a role.

TE03.14.02: The tester shall assume each role and initiate an error during the authentication procedure. The tester shall verify that the module denies access to each role.

AS03.15: (Role-based authentication – Level 2)
***{If role-based authentication mechanisms are supported by the cryptographic module, the following shall apply:}* If a cryptographic module permits an operator to change roles, then the module shall authenticate the assumption of any role that was not previously authenticated.**

Required Vendor Information

VE03.15.01: The vendor documentation shall describe the ability of an operator to modify roles and shall state that authentication of an operator to assume a new role is required.

Required Test Procedures

TE03.15.01: The tester shall verify the vendor documentation to verify that the method by which an operator can modify roles includes the authentication of the operator to assume a new role.

TE03.15.02: The tester shall perform the following tests:

1. Assume a role, attempt to modify to another role that the operator *is* authorised to assume, and verify that the module allows the operator to request services assigned to the new role.

2. Assume a role, attempt to modify to another role that the operator *is not* authorised to assume, and verify that the module does not allow the operator to request the services assigned only to the new role.

Identity-Based Authentication

AS03.16: (Identity-based authentication – Level 3 and 4)

If identity-based authentication mechanisms are supported by a cryptographic module, the module shall require that the operator be individually identified, shall require that one or more roles either be implicitly or explicitly selected by the operator, and shall authenticate the identity of the operator and the authorisation of the operator to assume the selected role (or set of roles).

Required Vendor Information

VE03.16.01: The vendor shall document the type of authentication implemented within the module. The vendor shall document the mechanism(s) used to perform the identification of the operator, the authentication of the operator's identity, the implicit or explicit selection of a role or set of roles, and the verification of the operator to assume the role(s).

Required Test Procedures

TE03.16.01: The tester shall verify that the vendor documentation specifies how the operator is uniquely identified, how that identity is authenticated, how the operator chooses a role, and how the authorisation of the operator to assume a role is performed based on the authenticated identity.

TE03.16.02: The tester shall initiate an error during the authentication procedure and shall verify that the module does not allow the tester to proceed beyond the authentication procedure.

TE03.16.03: The tester shall successfully authenticate his/her identity to the module. When required to select one or more roles, the tester shall select roles not compatible with the authenticated identity and shall verify that authorisation to assume the roles is denied.

AS03.17: (Identity-based authentication – Levels 3 and 4)

{If identity-based authentication mechanisms are supported by a cryptographic module, the following shall apply:} **If a cryptographic module permits an operator to change roles, then that module shall verify the authorisation of the identified operator to assume any role that was not previously authorised.**

Required Vendor Information

VE03.17.01: The vendor documentation shall describe the ability of an operator to modify roles and shall state that verification of the authentication of the operator for a new role is required.

Required Test Procedures

TE03.17.01: The tester shall verify the vendor documentation that the method by which an operator can modify roles without re-authentication of the operator's identity includes the verification of the authorisation of the operator for a role not previously authenticated.

TE03.17.02: The tester shall perform the following tests:

1. Assume each role, attempt to modify to another role that the tester *is* authorised to assume, verify that the tester's identity does not have to be reauthenticated, and verify that the tester can access the services associated with the new role. The tester shall perform services in the new role that were not associated with the previous role in order to verify that the tester has assumed a different role.

2. Assume each role, attempt to modify to another role that the operator *is not* authorised to assume, and verify that the module denies access to the role based on the identity of the operator.

AS03.18: (Operator authentication – Levels 2, 3, and 4)
When a module is powered off and subsequently powered on, the results of previous authentications shall not be retained and the module shall require the operator to be re-authenticated.

Required Vendor Information

VE03.18.01: The vendor documentation shall describe how the results of previous authentications are cleared when the module is powered off.

Required Test Procedures

TE03.18.01: The tester shall verify the vendor documentation that the clearing of previous authentications upon power off of the module is described.

TE03.18.02: The tester shall authenticate to the module and assume one or more roles, power off the module, power on the module, and attempt to perform services in those roles. To meet this assertion, the module shall deny access to the services and require that the tester be reauthenticated.

AS03.19: (Operator authentication – Levels 2, 3, and 4)
Authentication data within the module shall be protected against unauthorised disclosure, modification, and substitution.

Required Vendor Information

VE03.19.01: The vendor documentation shall describe the protection of all authentication data to the module. Protection shall include the implementation of mechanisms that protect against unauthorised disclosure, modification, and substitution.

Required Test Procedures

TE03.19.01: The tester shall verify the vendor documentation that describes the protection of authentication data. The tester shall verify that the documentation describes how the data will be protected against unauthorised disclosure, modification, and substitution.

TE03.19.02: The tester shall perform the following tests:

1. Attempt to access (by circumventing the documented protection mechanisms) authentication data for which the tester is not authorised to have access. If the module denies access or allows access only to encrypted or otherwise protected forms of data, the requirement is met.

2. Modify authentication data using any method not specified by the vendor documentation and attempt to enter the modified data. The module shall not allow the tester to be authenticated using the modified data.

AS03.20: (Operator authentication – Levels 2, 3, and 4)
If a cryptographic module does not contain the authentication data required to authenticate the operator for the first time the module is accessed, then other authorised methods (e.g., procedural controls or use of factory-set or default authentication data) shall be used to control access to the module and initialise the authentication mechanisms.

Required Vendor Information

VE03.20.01: The vendor documentation shall specify means to control access to the module before it is initialised.

Required Test Procedures

TE03.20.01: The tester shall verify the vendor documentation describes the procedure by which the operator is authenticated upon accessing the module for the first time.

TE03.20.02: If access to the module before initialisation is controlled, the tester shall initiate an error on an uninitialised module and shall verify that the module denies access. The tester shall assume the authorised role and verify that the required authentication complies with the documented procedures. The tester shall attempt to assume other roles before the module has been initialised and verify that the module denies access to the roles.

AS03.21: (Operator authentication – Levels 2, 3, and 4)
The strength of the authentication mechanism shall conform to the following specifications *{AS03.22 to AS03.25}*.

NOTE This assertion is not separately tested.

AS03.22: (Operator authentication – Levels 2, 3, and 4)

For each attempt to use the authentication mechanism, the probability shall meet the strength of the authentication objective.

NOTE For example, less than one in 1,000,000 that a random attempt may succeed (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination thereof).

Required Vendor Information

VE03.22.01: The vendor documentation shall specify each authentication mechanism and the associated false acceptance rate or probability that a random access will succeed.

Required Test Procedures

TE03.22.01: The tester shall verify the vendor documentation for each authentication mechanism that the associated false acceptance or random access rate is specified.

TE03.22.02: The tester shall verify the vendor documentation for each authentication mechanism that the objective is met.

AS03.23: (Operator authentication – Levels 2, 3, and 4)

For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall meet the strength of the authentication objective.

NOTE For example be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur

Required Vendor Information

VE03.23.01: The vendor documentation shall specify each authentication mechanism and the associated probability of a successful random attempt during a one-minute period.

Required Test Procedures

TE03.23.01: The tester shall verify the vendor documentation for each authentication mechanism that the associated probability of a successful random is specified.

TE03.23.02: The tester shall verify the vendor documentation for each authentication mechanism that the associated probability of a successful random is meeting the objective.

AS03.24: (Operator authentication – Levels 2, 3, and 4)

Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password).

Required Vendor Information

VE03.24.01: The vendor documentation shall specify the method used to obscure feedback of the authentication data to an operator during entry of the authentication data.

Required Test Procedures

TE03.24.01: The tester shall verify the vendor documentation that the authentication data is obscured during data entry.

TE03.24.02: The tester shall enter authentication data and verify that there is no visible display of authentication data during data entry.

AS03.25: (Operator authentication – Levels 2, 3, and 4)

Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism by providing more information than the fact that the authentication passed or failed.

Required Vendor Information

VE03.25.01: The vendor documentation shall specify the feedback mechanism that is used when the operator is entering authentication data.

Required Test Procedures

TE03.25.01: The tester shall verify the vendor documentation that the feedback mechanism does not provide information that could be used to guess or determine the authentication data.

TE03.25.02: The tester shall enter authentication data to assume each role to ensure that the feedback mechanism does not provide useful information.

AS03.26: (Operator authentication – Level 1)

If a module does not support authentication mechanisms, the module shall require that the operator either implicitly or explicitly select one or more roles.

Required Vendor Information

VE03.26.01: The vendor shall document the type of authentication performed for the module. The vendor shall document the mechanisms used to perform the implicit or explicit selection of a role or set of roles and the authentication of the operator to assume the role(s).

VE03.26.02: The vendor provided non-proprietary security policy shall provide a description of the roles, either implicit or explicit, that the operator can assume.

VE03.26.03: The vendor provided non-proprietary security policy shall provide instructions for the operator to assume either the implicit or explicit roles.

Required Test Procedures

TE03.26.01: The tester shall verify that the vendor provided non-proprietary security policy provides a description of the roles, either implicit or explicit, that the operator can assume and the means to assume each role.

TE03.26.02: The tester shall invoke the method described in the non-proprietary security policy and verify that each role can either be implicitly or explicitly assumed.

AS03.27: (Operator authentication – Level 2)
A cryptographic module shall employ role-based authentication to control access to the module.

NOTE This assertion is tested as part of AS03.13.

AS03.28: (Operator authentication – Levels 3 and 4)
A cryptographic module shall employ identity-based authentication mechanisms to control access to the module.

NOTE This assertion is tested as part of AS03.16 and AS03.17.

6.5 Finite state model

AS04.01: (Finite state model – Levels 1, 2, 3, and 4)
The operation of a cryptographic module shall be specified using a finite state model (or equivalent) represented by a state transition diagram and/or a state transition table.

The state transition diagram and/or state transition table includes:

- **all operational and error states of a cryptographic module;**
- **the corresponding transitions from one state to another;**
- **the input events that cause transitions from one state to another; and**
- **the output events resulting from transitions from one state to another.**

Required Vendor Information

VE04.01.01: The vendor shall provide a description of the finite state model. This description shall contain the identification and description of all states of the module, and a description of all corresponding state transitions. The descriptions of the state transitions shall include internal module conditions, data inputs and control inputs that cause transitions from one state to another, data outputs and status outputs resulting from transitions from one state to another.

VE04.01.02: The vendor documentation shall establish a complete description of the following:

1. Data input interface
2. Data output interface
3. Control input interface
4. Status output interface
5. Crypto officer role
6. User role
7. Other roles (if applicable)
8. Key entry services (if applicable)
9. Show status service
10. Self-tests
11. Other authorised services, operations, and functions (if applicable)
12. Error states
13. Bypass service (if applicable)
14. Maintenance interface (if applicable)
15. Maintenance role (if a maintenance interface is provided)
16. Key generation services (if applicable)
17. Key output services (if applicable)
18. Idle states (if applicable)
19. Uninitialised states (if applicable)

Required Test Procedures

TE04.01.01: The tester shall verify that the vendor has provided a description of the finite state model. This description shall contain the identification and description of all states of the module, and a description of all corresponding state transitions. The tester shall verify that the descriptions of the state transitions include the internal module conditions, data inputs and control inputs that cause transitions from one state to another, data outputs and status outputs resulting from transitions from one state to another.

TE04.01.02: The tester shall verify that the finite state diagrams and the descriptions are consistent with the vendor documentation that shall describe the following:

1. Data input interface
2. Data output interface
3. Control input interface
4. Status output interface
5. Crypto officer role
6. User role
7. Other roles (if applicable)
8. Key entry services (if applicable)
9. Show status service
10. Self-tests
11. Other authorised services, operations, and functions (if applicable)
12. Error states
13. Bypass service (if applicable)
14. Maintenance interface (if applicable)
15. Maintenance role (if a maintenance interface is provided)
16. Key generation services (if applicable)
17. Key output services (if applicable)
18. Idle states (if applicable)
19. Uninitialised states (if applicable)

TE04.01.03: The tester shall verify that every state that is identified in the finite state diagram(s) is also identified and described in the description.

TE04.01.04: The tester shall verify that every state that is identified and described in the description is also identified in the finite state diagram(s).

TE04.01.05: The tester shall verify that the operation of the module is consistent with the finite state diagrams and descriptions.

TE04.01.06: If the module includes a maintenance interface, then the tester shall verify that the finite state model has at least one maintenance state define. All maintenance states have to be contained in the finite state diagram(s) and described in the description of the finite state model.

TE04.01.07: The tester shall verify the descriptions of the states of the cryptographic module if the descriptions clearly define disjoint states. The tester shall verify that all possible combinations of data and control inputs can be partitioned into disjoint sets.

TE04.01.08: The tester shall exercise the cryptographic module, causing it to enter each of its major states. For each state that has a distinct indicator, the tester shall attempt to verify the indicator while the module is in the state. If the expected indicator is not observed, or two or more such indicators are observed at the same time (indicating that the module is in more than one state at one time), this test fails.

TE04.01.09: The tester shall verify that there exists a chain of transitions from an initial power on state to each other state in the model that is not an initial power on state.

TE04.01.10: The tester shall verify that there exists a chain of transitions from each non-power off state to a power off state of the model.

TE04.01.11: The tester shall verify that the actions of the finite state model, as the result of all possible data and control inputs, are defined. An example of an acceptable inclusive statement is:

"The action of the finite state model as a result of all other combinations of data and control inputs is to place the finite state model into the ERROR-3 state."

AS04.02: (Finite state model – Levels 1, 2, 3, and 4)
A cryptographic module shall include the following operational and error states:

1. ***Power on/off states*. States for primary, secondary, or backup power. These states may distinguish between power sources being applied to the cryptographic module.**
2. ***Crypto officer states*. States in which the crypto officer services are performed (e.g., cryptographic initialisation and key management).**
3. ***CSP/PSP entry states*. States for entering CSPs and PSPs into the cryptographic module.**
4. ***User states*. States in which authorised users obtain security services, perform cryptographic operations, or perform other approved or non-approved functions.**
5. ***Self-test states*. States in which the cryptographic module is performing self-tests.**
6. ***Error states*. States when the cryptographic module has encountered an error. Error states may include "hard" errors that indicate an equipment malfunction and that may require maintenance, service or repair of the cryptographic module, or recoverable "soft" errors that may require initialisation or resetting of the module.**

NOTE This assertion is tested as part of AS04.01.

AS04.03: (Finite state model – Levels 1, 2, 3, and 4)

Recovery from error states shall be possible except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.

Required Vendor Information

VE04.03.01: The vendor documentation shall describe the applicable recovery for each error state that does not require maintenance, service, or repair of the cryptographic module.

Required Test Procedures

TE04.03.01: From each error state that does not require maintenance, service, or repair, the tester shall verify that the cryptographic module can be caused to transition to an acceptable operational or initialisation state. This effort consists of two parts: first, the tester shall verify that the cryptographic module indicates when it is an error state, and second, that the module operates correctly in this target state. The tester shall report how the requirement was verified (i.e., by code examination or by exercising the module).

AS04.04: (Finite state model – Levels 1, 2, 3, and 4)
If a cryptographic module contains a maintenance role, then a maintenance state shall be included.

NOTE 1 This assertion is tested as part of AS04.01.

NOTE 2 For definition of maintenance states see subclause 7.4 of ISO/IEC 19790:2006.

6.6 Physical security

AS05.01: (Physical security – Levels 1, 2, 3, and 4)
A cryptographic module shall employ physical security mechanisms in order to restrict unauthorised physical access to the contents of the module and to deter unauthorised use or modification of the module (including substitution of the entire module) when installed.

Required Vendor Information

VE05.01.01: The vendor documentation shall describe the applicable physical security mechanisms that are employed by the module. The contents of the module, including all hardware, firmware, software, and data (including plaintext cryptographic keys and plaintext CSPs) shall be protected.

Required Test Procedures

TE05.01.01: The tester shall verify that the vendor documentation describes the applicable physical security mechanisms that are employed by the module.

TE05.01.02: The tester shall verify that the physical security mechanisms documented are implemented.

AS05.02: (Physical security – Levels 1, 2, 3, and 4)

All hardware, software, firmware, and data components within the cryptographic boundary shall be protected.

NOTE This assertion is not separately tested.

AS05.03: (Physical security – Levels 1, 2, 3, and 4)

Depending on the physical security mechanisms of a cryptographic module, unauthorised attempts at physical access, use, or modification shall have a high probability of being detected subsequent to an attempt by leaving visible signs (i.e., tamper evidence) *{and/or AS05.04 shall apply}*.

NOTE This assertion is not separately tested.

AS05.04: (Physical security – Levels 1, 2, 3, and 4)

***{Depending on the physical security mechanisms of a cryptographic module, unauthorised attempts at physical access, use, or modification shall have a high probability of being detected}* during an access attempt so that appropriate immediate actions can be taken by the cryptographic module to protect CSPs and PSPs (i.e., tamper response).**

NOTE This assertion is not separately tested.

AS05.05: (Physical security – Levels 1, 2, 3, and 4)

***{In conjunction with AS05.04:} Immediate actions* shall be taken to mean that retrieval of CSPs and PSPs are not possible.**

NOTE This assertion is not separately tested.

6.6.1 General physical security requirements

AS05.06: (Physical security – Levels 1, 2, 3, and 4)
The following requirements *{AS05.07 to AS05.23}* shall apply to all physical embodiments.

NOTE This assertion is not separately tested.

AS05.07: (Physical security – Levels 1, 2, 3, and 4)
Documentation shall specify the physical embodiment and the security level for which the physical security mechanisms of a cryptographic module are implemented.

Required Vendor Information

VE05.07.01: The vendor documentation shall specify the physical embodiment 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. (See also VE01.08.05.)

The specified physical embodiment shall be consistent with the module physical design. The vendor documentation shall also state which security level (1 through 4) the module is intended to meet.

Required Test Procedures

TE05.07.01: 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. (See also TE01.08.09.)

The tester shall perform an independent determination that the physical embodiment satisfies one of the three criteria specified below. The fundamental determining characteristics of the three physical embodiments and some common examples are summarised below.

1. *Single-chip cryptographic module.* Characteristics: A single integrated circuit (IC) chip, used as a standalone device or physically embedded within some other module or enclosure that may not be physically protected. The single-chip will consist of one die that is may be covered with a uniform external material such as plastic or ceramic, and external input/output connectors. Examples: Single IC chips, smart cards with a single IC chip, or other systems with a single IC chip to implement cryptographic functions.

2. *Multiple-chip embedded cryptographic module.* Characteristics: Two or more IC chips interconnected and physically embedded within some other product or enclosure that may not be physically protected.

3. *Multiple-chip standalone cryptographic module.* Characteristics: Two or more IC chips interconnected and physically embedded in an enclosure that is entirely physically protected.

TE05.07.02: The tester shall verify that the vendor documentation states which security level the module is intended to meet. The tester shall perform an independent determination of the security level that the module actually meets.

AS05.08: (Physical security – Levels 1, 2, 3, and 4)
If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g., by the module vendor or other authorised individual), then a maintenance access interface shall be defined.

Required Vendor Information

VE05.08.01: The vendor documentation shall describe the maintenance access interface employed by the module.

Required Test Procedures

TE05.08.01: The tester shall verify that the vendor documentation describes the maintenance access interface.

TE05.08.02: The tester shall verify that the vendor documentation and implementation are consistent.

AS05.09: (Physical security – Levels 1, 2, 3, and 4)

If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g., by the module vendor or other authorised individual), then the maintenance access interface shall include all physical access paths to the contents of the cryptographic module, including any removable covers or doors.

Required Vendor Information

VE05.09.01: The vendor documentation shall specify the maintenance access interface, including any removable covers or doors.

Required Test Procedures

TE05.09.01: The tester shall verify the vendor documentation that a maintenance access interface is provided, including any removable covers or doors.

AS05.10: (Physical security – Levels 1, 2, 3, and 4)

If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g., by the module vendor or other authorised individual), then any removable covers or doors included within the maintenance access interface shall be safeguarded using the appropriate physical security mechanisms.

Required Vendor Information

VE05.10.01: The vendor documentation shall specify a physical protection such that any removable covers or doors included within the maintenance access interface are safeguarded using the appropriate physical security mechanisms.

Required Test Procedures

TE05.10.01: The tester shall very that any removable covers or doors included within the maintenance access interface are safeguarded using the appropriate physical security mechanisms.

AS05.11: (Physical security – Levels 1, 2, 3, and 4)

If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g., by the module vendor or other authorised individual), then all CSPs shall be zeroised when the maintenance access interface is accessed.

Required Vendor Information

VE05.11.01: The vendor documentation shall specify how the module's plaintext CSPs are zeroised when the maintenance access interface is accessed.

Required Test Procedures

TE05.11.01: If the vendor documentation states that a maintenance access interface is provided, the tester shall verify that the vendor documentation specifies how plaintext CSPs contained in the module are zeroised when accessing the maintenance access interface.

TE05.11.02: The tester shall assume the maintenance role and access the maintenance interface while the unit is powered on, and verify that all operational keys are zeroised.

NOTE Removing power to memory and allowing charge to slowly dissipate is not sufficient.

AS05.12: (Physical security – Level 1)
The following requirements *{AS05.13 to AS05.15}* shall apply to all cryptographic modules for Security Level 1.

NOTE This assertion is not separately tested.

AS05.13: (Physical security – Levels 1, 2, 3, and 4)
The cryptographic module shall consist of production-grade components that shall include standard passivation techniques (e.g., a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or other physical damage).

Required Vendor Information

VE05.13.01: The module shall be a standard, production-quality IC, designed to meet commercial-grade specifications for power, temperature, reliability, shock and vibration, etc. The module shall use standard passivation techniques for the entire chip. The vendor documentation shall describe the IC quality. If an IC is used that is not a standard device, its passivation design shall also be described.

Required Test Procedures

TE05.13.01: The tester shall verify by inspection, or from the vendor documentation, that the module contains standard integrated circuits with a uniform exterior material and standard connectors. The tester shall verify from the vendor documentation that the chips in the module are commercial grade in regards to power and voltage ranges, temperature, reliability, and shock and vibration.

TE05.13.02: The tester shall verify from the vendor documentation that the module has a standard passivation applied to it. The passivation has to be a sealing coat applied over the chip circuitry to protect it against environmental or other physical damage. If standard passivation is not used, then the documentation shall provide information to indicate why it is equivalent to a standard passivation approach.

AS05.14: (Physical security – Levels 1, 2, 3, and 4)

When performing physical maintenance, all CSPs contained in the cryptographic module shall be zeroised.

NOTE This assertion is tested as part of AS05.11.

AS05.15: (Physical security – Levels 1, 2, 3, and 4)
Zeroisation shall either be performed procedurally by the operator or automatically by the cryptographic module.

NOTE This assertion is not separately tested.

AS05.16: (Physical security – Levels 2, 3, and 4)
In addition to the general requirements for Security Level 1, the following requirement *{AS05.17}* shall apply to all cryptographic modules for Security Level 2.

NOTE This assertion is not separately tested.

AS05.17: (Physical security – Levels 2, 3, and 4)
The cryptographic module shall provide evidence of tampering (e.g., on the cover, enclosure, and seal) when physical access to the module is attempted.

NOTE This assertion is tested as part of AS05.25 and AS05.26 for single-chip embodiments, AS05.35 and AS05.36 for multiple-chip embedded embodiments, and AS05.51 for multiple-chip standalone embodiments.

AS05.18: (Physical security – Levels 3 and 4)
In addition to the general requirements for Security Levels 1 and 2, the following requirements *{AS05.19 to AS05.22}* shall apply to all cryptographic modules for Security Level 3.

NOTE This assertion is not separately tested.

AS05.19: (Physical security – Levels 3 and 4)

If the cryptographic module contains any doors or removable covers or if a maintenance access interface is defined, then the module shall contain tamper response and zeroisation capability.

NOTE This assertion is tested as part of AS05.11 for general requirements, AS05.29 for single-chip embodiments, AS05.41 for multiple-chip embodiments and AS05.55 for multiple-chip standalone embodiments.

AS05.20: (Physical security – Levels 3 and 4)
The tamper response and zeroisation capability shall immediately zeroise all CSPs when a door is opened, a cover is removed, or when the maintenance access interface is accessed.

NOTE This assertion is tested as part of AS05.11 for general requirements, AS05.29 for single-chip embodiments, AS05.41 for multiple-chip embedded embodiments, and AS05.55 for multiple-chip standalone embodiments.

AS05.21: (Physical security – Levels 3 and 4)
The tamper response and zeroisation capability shall remain operational when CSPs are contained within the cryptographic module.

NOTE This assertion is tested as part of AS05.29 for single-chip embodiments, AS05.41 for multiple-chip embedded embodiments, and AS05.55 for multiple-chip standalone embodiments.

AS05.22: (Physical security – Levels 3 and 4)
If the cryptographic module contains ventilation holes or slits, then the holes or slits shall be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., require at least one 90 degree bend or obstruction with a substantial blocking material).

Required Vendor Information

VE05.22.01: If the module is contained within a cover or enclosure that contains any ventilation holes or slits; then they shall be constructed in a manner that prevents undetected physical probing inside the enclosure. The vendor documentation shall describe the ventilation physical design approach.

Required Test Procedures

TE05.22.01: The tester shall verify by inspection and from the vendor documentation whether the module has a cover or enclosure with ventilation holes, slits, or other openings, and if so, whether they are constructed to deter undetected probing inside the cover or enclosure.

AS05.23: (Physical security – Level 4)
In addition to the general requirements for Security Levels 1, 2 and 3, the module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in *{sub}*clause 7.5.2 *{of ISO/IEC 19790:2006}* for Security Level 4.

NOTE This assertion is tested as part of AS05.60 – AS05.69.

6.6.1.1 Single-Chip Cryptographic Modules

NOTE 1 In addition to the general security requirements specified in subclause 7.5.1 of ISO/IEC 19790, the requirements specified in AS05.24 to AS05.32 are specific to single-chip cryptographic modules.

NOTE 2 There are no additional Security Level 1 requirements for single-chip cryptographic modules.

AS05.24: (Single-Chip – Levels 2, 3, and 4)
In addition to the requirements for Security Level 1, the following requirements *{AS05.25 and AS05.26}* shall apply to single-chip cryptographic modules for Security Level 2.

NOTE This assertion is not separately tested.

AS05.25: (Single-Chip – Levels 2, 3, and 4)
The cryptographic module shall be covered with a tamper-evident coating (e.g., a tamper-evident passivation material or a tamper-evident material covering the passivation) or contained in a tamper-evident enclosure to deter direct observation, probing, or manipulation of the module and to provide evidence of attempts to tamper with or remove the module.

NOTE This requirement is associated with AS05.17.

Required Vendor Information

VE05.25.01: The vendor documentation shall identify the tamper-evident coating and its characteristics.

Required Test Procedures

TE05.25.01: The tester shall verify by inspection and from the vendor documentation that the module is covered with a tamper-evident coating. The inspection shall verify that the tamper-evident coating completely covers the module and deters direct observation, probing, or manipulation of the single-chip.

AS05.26: (Single-Chip – Levels 2, 3, and 4)
The tamper-evident coating or tamper-evident enclosure shall be opaque within the visible spectrum (i.e., light of wavelength range of 400nm to 750nm).

Required Vendor Information

VE05.26.01: The vendor documentation shall specify that the material shall be opaque within the visible spectrum.

Required Test Procedures

TE05.26.01: The tester shall verify by inspection and from the vendor documentation that the single-chip module is covered an opaque coating within the visible spectrum.

AS05.27: (Single-Chip – Levels 3 and 4)
In addition to the requirements for Security Levels 1 and 2, the following requirements *{AS05.28 or AS05.29}* shall apply to single-chip cryptographic modules for Security Level 3.

Required Vendor Information

VE05.27.01: The vendor documentation shall state which of the two approaches specified in AS05.28 and AS05.29 is used to meet the requirement.

Required Test Procedures

TE05.27.01: The tester shall verify by inspection and from the vendor documentation which of the two approaches specified in AS05.28 and AS05.29 is used to meet the requirement.

TE05.27.02: The tester shall follow procedures in TE05.28 but not TE05.29, if approach AS05.28 is found. If instead approach AS05.29 is found, the tester shall follow procedures specified in TE05.29 but not TE05.28.

AS05.28: (Single-Chip – Levels 3 and 4)
***{Either}* the module shall be covered with a hard opaque tamper-evident coating (e.g., a hard opaque epoxy covering the passivation) {*or AS05.29 shall be satisfied*}.**

Required Vendor Information

VE05.28.01: The vendor documentation shall state clearly that the approach specified in AS05.28 is used to meet the requirement.

VE05.28.02: The vendor documentation shall provide supporting detailed design information, especially the type of coating that is used and its characteristics.

Required Test Procedures

TE05.28.01: The tester shall verify by inspection and from the vendor documentation that the module is covered with a hard opaque tamper evident coating.

TE05.28.02 The tester shall verify that the vendor documentation does sufficiently provide supporting detailed design information, especially specifying the type of coating that is used and its characteristics.

TE05.28.03: The tester shall verify that the coating cannot be easily penetrated to the depth of the underlying circuitry, and that it leaves tamper evidence. The inspection has to verify that the coating completely covers the module, is visibly opaque, and deters direct observation, probing, or manipulation.

AS05.29: (Single-Chip – Levels 3 and 4)
***{If AS05.28 is not satisfied, then the}* enclosure shall be implemented so that attempts at removal or penetration of the enclosure shall have a high probability of causing serious damage to the cryptographic module (i.e., the module will not function).**

Required Vendor Information

VE05.29.01: The vendor documentation shall provide supporting detailed design information, especially whether the enclosure contains any doors or removable covers and whether a maintenance access interface is specified. The enclosure shall be designed such that attempts to remove it will have a high probability of causing serious damage to the circuitry within the module.

VE05.29.02: If the enclosure contains any doors or removable covers, or if a maintenance access interface is specified, then the module shall contain tamper response and zeroisation circuitry. The circuitry shall continuously monitor the covers and doors, and upon the removal of a cover or the opening of a door, shall zeroise all plaintext CSPs. The circuitry shall be operational whenever plaintext CSPs are contained within the module.

Required Test Procedures

TE05.29.01: The tester shall verify that the documentation specifies that the enclosure cannot be removed easily and whether the module contains doors or removable covers or has a maintenance access interface. If the enclosure contains any doors or removable covers, or if a maintenance access interface is specified, then the tester shall verify that the documentation specifies that the module contains tamper response and zeroisation circuitry.

TE05.29.02: If the enclosure has removable covers or doors, or if a maintenance access interface is specified, the tester shall verify from the vendor documentation that the module zeroises all plaintext CSPs when a cover or door is removed or if the maintenance access interface is accessed.

TE05.29.03: The tester shall verify by inspection and from the vendor documentation that the tamper response and zeroisation circuitry remains operational when plaintext CSPs are contained within the module.

TE05.29.04: The tester shall verify by inspection and from the vendor documentation that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

TE05.29.05: If the enclosure has doors or removable covers , or if a maintenance access interface is specified, the tester shall test that the module zeroises all plaintext CSPs when a cover or door is removed or if the maintenance access interface is accessed.

TE05.29.06: The tester shall test that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

AS05.30: (Single-Chip – Level 4)
In addition to the requirements for Security Levels 1, 2, and 3, the following requirements *{AS05.31 and AS05.32}* shall apply to single-chip cryptographic modules for Security Level 4.

NOTE This assertion is not separately tested.

AS05.31: (Single-Chip – Level 4)
The cryptographic module shall be covered with a hard, opaque removal-resistant coating with hardness and adhesion characteristics such that attempting to peel or pry the coating from the module will have a high probability of resulting in serious damage to the module (i.e., the module will not function).

Required Vendor Information

VE05.31.01: The vendor documentation shall clearly identify the kind of coating used and shall provide details of its characteristics, especially hardness and removal resistance.

VE05.31.02: The module shall be covered with a hard, opaque removal-resistant coating. The hardness and adhesion characteristics of the material shall be such that attempting to peel or pry the material from the module will have a high probability of resulting in serious damage to the module (i.e., the module does not function). The material shall be opaque within the visible spectrum.

Required Test Procedures

TE05.31.01: The tester shall verify by inspection and from the vendor documentation that the module is covered with a hard, opaque removal-resistant coating.

TE05.31.02: The tester shall verify the removal-resistant properties of the module coating. The tester shall attempt to peel or pry the material from the module, and verify that this is not possible with a reasonable application of force, that the module ceased to function, or that the module circuitry was obviously physically destroyed.

AS05.32: (Single-Chip – Level 4)
The removal-resistant coating shall have solvency characteristics such that dissolving the coating will have a high probability of dissolving or seriously damaging the module (i.e., the module will not function).

Required Vendor Information

VE05.32.01: The vendor documentation shall describe the solvency characteristics of the removal-resistant coating. The solvency characteristics of the material shall be such that dissolving the material to remove it will have a high probability of dissolving or seriously damaging the module.

Required Test Procedures

TE05.32.01: The tester shall verify the vendor documentation to determine the solvency properties of the modules removal-resistant coating.

TE05.32.02: The tester shall test the solvency properties of the modules removal-resistant coating. The tester, based on documentation provided in VE05.32.01, shall verify what type of solvent would be required to compromise the removal-resistant coating.

6.6.1.2 Multiple-Chip Embedded Cryptographic Modules

NOTE In addition to the general security requirements specified in subclause 7.5.1 of ISO/IEC 19790, the following requirements AS05.33 to AS05.49 are specific to multiple-chip embedded cryptographic modules.

AS05.33: (Multiple Chip Embedded – Levels 1, 2, 3, and 4)
If the cryptographic module is contained within an enclosure or removable cover, a production-grade enclosure or removable cover shall be used.

Required Vendor Information

VE05.33.01: The module shall be entirely contained within a production-grade enclosure or removable cover. The vendor documentation shall describe the cover or enclosure.

Required Test Procedures

TE05.33.01: The tester shall verify by inspection and from the vendor documentation that the module is contained within an enclosure or removable cover that is of production-grade.

AS05.34: (Multiple Chip Embedded – Levels 2, 3, and 4)
In addition to the requirement for Security Level 1, the following requirements *{AS05.35 through AS 05.40}* shall apply to multiple-chip embedded cryptographic modules for Security Level 2 *{and the assertions AS05.35 through AS 05.40 shall be satisfied in the following groups: (AS05.35 and AS05.36) or (AS05.37, AS05.38 and AS05.39) or (AS05.37, AS05.38 and AS05.40)}*.

Required Vendor Information

VE05.34.01: The vendor documentation shall specify that either (AS05.35 and AS05.36) or (AS05.37, AS05.38 and (AS05.39 or AS05.40)) are satisfied.

Required Test Procedures

TE05.34.01: The tester shall verify by inspection and from the vendor documentation that either (AS05.35 and AS05.36) or (AS05.37, AS05.38 and (AS05.39 or AS05.40)) are satisfied.

AS05.35: (Multiple Chip Embedded – Levels 2, 3, and 4)
The module components shall be covered with a tamper-evident coating or potting material (e.g., etch-resistant coating or bleeding paint) to deter direct observation, probing, or manipulation of module components and to provide evidence of attempts to tamper with or remove module components *{or the groups (AS05.37, AS05.38 and AS05.39) or (AS05.37, AS05.38 and AS05.40) shall be satisfied}*.

Required Vendor Information

VE05.35.01: The vendor documentation shall specify that the module is encapsulated with an opaque, tamper-evident coating such as etch-resistant coating or bleeding paint.

Required Test Procedures

TE05.35.01: The tester shall verify by inspection and from the vendor documentation that the module is encapsulated with an opaque, tamper-evident material.

TE05.35.02: The tester shall verify by testing that the module provides evidence of attempts to tamper with or remove module components.

AS05.36: (Multiple Chip Embedded – Levels 2, 3, and 4)
***{In conjunction with AS05.35 the}* tamper-evident coating or tamper-evident enclosure shall be opaque within the visible spectrum *{or the groups (AS05.37, AS05.38 and AS05.39) or (AS05.37, AS05.38 and AS05.40) shall be satisfied}*.**

Required Vendor Information

VE05.36.01: The material shall be opaque within the visible spectrum. The vendor documentation shall identify the kind of opaque tamper-evident coating and its characteristics.

Required Test Procedures

TE05.36.01: The inspection shall verify that the tamper-evident material completely covers the module and is visibly opaque.

AS05.37: (Multiple Chip Embedded – Levels 2, 3, and 4)
***{If the group (AS05.35 and AS05.36) is not satisfied, then the}* module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers*{and the groups (AS05.37, AS05.38 and AS05.39) or (AS05.37, AS05.38 and AS05.40) shall be satisfied}*.**

Required Vendor Information

VE05.37.01: The module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include removable covers or doors. The vendor documentation shall describe the enclosure and its hardness characteristics.

Required Test Procedures

TE05.37.01: The tester shall verify by inspection and from the vendor documentation that the module is contained within an enclosure that meets the following requirements:

1. The enclosure has to completely surround the entire module.
2. The enclosure material has to be of a composition defined in the vendor documentation.
3. The enclosure has to be production-grade. The vendor literature has to either show that an enclosure of the same material has been used commercially, or provide data to show that it is equivalent to a commercial product.

AS05.38: (Multiple Chip Embedded – Levels 2, 3, and 4)
***{In conjunction with AS05.37}* the enclosure shall be opaque within the visible spectrum *{and the groups (AS05.37, AS05.38 and AS05.39) or (AS05.37, AS05.38 and AS05.40) shall be satisfied}*.**

Required Vendor Information

VE05.38.01: The enclosure shall be opaque within the visible spectrum. The vendor documentation shall describe the enclosure's opacity characteristics.

Required Test Procedures

TE05.38.01: The tester shall verify by inspection and from the vendor documentation that the enclosure is opaque within the visible spectrum.

AS05.39: (Multiple Chip Embedded – Levels 2, 3, and 4)
***{If the group (AS05.35 and AS05.36) is not satisfied, then}* if the enclosure includes any doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys *{and the groups (AS05.37, AS05.38 and AS05.39) or (AS05.37, AS05.38 and AS05.40) shall be satisfied}*.**

Required Vendor Information

VE05.39.01: The doors or covers included by the enclosure shall be locked with pick-resistant mechanical locks that employ physical or logical keys. The vendor documentation shall describe the locks and the employed physical or logical keys.

Required Test Procedures

TE05.39.01: The tester shall verify by inspection and from the vendor documentation that the doors or covers are locked with a pick-resistant lock that requires a physical key or a logical key.

TE05.39.02: The tester shall attempt to open the locked cover or door without use of the key and verify that the cover or door will not open without signs of damage.

AS05.40: (Multiple Chip Embedded – Levels 2, 3, and 4)
{If the group (AS05.35 and AS05.36) is not satisfied and the enclosure includes any doors or removable covers without matching AS05.39, then} **they** ***{i.e., the doors or covers}*** **shall be protected with tamper-evident seals (e.g., evidence tape or holographic seals)** ***{and the group (AS05.37, AS05.38 and AS05.40) shall be satisfied}*****.**

Required Vendor Information

VE05.40.01: The vendor documentation shall describe the tamper-evident seals.

Required Test Procedures

TE05.40.01: The tester shall verify by inspection and from the vendor documentation that the cover or door is protected with a tamper-evident seal such as evidence tape or a holographic seal.

TE05.40.02: The tester shall verify that the cover or door cannot be opened without breaking or removing the seal, and that the seal cannot be removed and later replaced.

AS05.41: (Multiple-Chip Embedded – Levels 3 and 4)
In addition to the requirements for Security Levels 1 and 2, the following requirements ***{AS05.42 or AS05.43}*** **shall apply to multiple-chip embedded cryptographic modules for Security Level 3.**

NOTE This assertion is not separately tested.

AS05.42: (Multiple-Chip Embedded – Levels 3 and 4)
{Either the} **multiple-chip embodiment of the circuitry within the cryptographic module shall be covered with a hard coating or potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum** ***{or AS05.43 shall be satisfied}*****.**

Required Vendor Information

VE05.42.01: The vendor documentation shall provide design documentation for the hard coating or potting material.

VE05.42.02: The vendor documentation shall provide documentation regarding the opacity characteristics of the hard coating or potting material.

Required Test Procedures

TE05.42.01: The tester shall verify that the vendor documentation specifies the hard coating or potting material.

TE05.42.02 The tester shall verify by inspection and from the vendor documentation the opacity characteristics of the hard coating or potting material.

TE05.42.03: The tester shall verify by inspection and from the vendor documentation that the hard coating or potting material cannot be removed or penetrated without having a high probability of causing serious damage to the module.

AS05.43: (Multiple-Chip Embedded – Levels 3 and 4)
***{If AS05.42 does not apply, the}* applicable Security Level 3 requirements for multiple-chip standalone cryptographic modules shall apply*{i.e., according to AS05.57 the module shall be contained within a strong enclosure such that attempts at removal or penetration of the enclosure will have a high probability of causing serious damage to the module (i.e., the module will not function)}*. (*{Sub}*Clause 7.5.1.3 *{of ISO/IEC 19790:2006}*)**

Required Vendor Information

VE05.43.01: The vendor documentation shall provide supporting design documentation for the strong enclosure. The module shall be entirely contained within a strong enclosure. The enclosure shall be designed such that attempts to remove it will have a high probability of causing serious damage to the circuitry within the module (i.e., the module does not function).

VE 05.43.02: If the enclosure contains any doors or removable covers, then the module shall contain tamper response and zeroisation circuitry. The circuitry shall continuously monitor the covers and doors, and upon the removal of a cover or the opening of a door, shall zeroise all plaintext CSPs. The circuitry shall be operational whenever plaintext CSPs are contained within the module.

Required Test Procedures

TE05.43.01: The tester shall verify that the vendor documentation specifies whether the enclosure contains any doors or removable covers and whether a maintenance access interface is specified, then the module shall contain tamper response and zeroisation circuitry.

TE05.43.02: If the enclosure contains any doors or removable covers, or if a maintenance access interface is specified, then the tester shall verify that the vendor documentation specifies that the module zeroises all plaintext CSPs when a door or cover is removed or if the maintenance access interface is accessed.

TE05.43.03: The tester shall verify that the vendor documentation specifies which requirement option in VE05.43.01 and VE05.43.02 is implemented and provides design documentation.

TE05.43.04: The tester shall verify by inspection and from the vendor documentation that the tamper response and zeroisation circuitry remains operational when plaintext CSPs are contained within the module.

TE05.43.05: The tester shall verify by inspection and from the vendor documentation that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

TE05.43.06: The tester shall verify the strength of the enclosure by attempting to access the underlying circuitry and verifying that the enclosure is not easily breached. The tester shall verify by inspection and from the vendor documentation that the enclosure cannot be removed.

TE05.43.07: If the strong enclosure has doors or removable covers, or if a maintenance access interface is specified, the tester shall verify from the vendor documentation that the module zeroises all plaintext CSPs when a cover or door is removed.

TE05.43.08: If the enclosure has doors or removable covers, or if a maintenance access interface is specified, the tester shall test that the module zeroises all plaintext CSPs when a cover or door is removed or if the maintenance access interface is accessed.

TE05.43.09: The tester shall test that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

AS05.44: (Multiple-Chip Embedded – Level 4)
In addition to the requirements for Security Levels 1, 2 and 3, the following requirements *{AS05.45 through AS05.49}* shall apply to multiple-chip embedded cryptographic modules for Security Level 4.

NOTE This assertion is not separately tested.

AS05.45: (Multiple-Chip Embedded – Level 4)
The module components shall be covered by potting material or contained within an enclosure encapsulated by a tamper detection envelope (e.g., a flexible printed circuit with a serpentine geometric pattern of conductors or a wire-wound package or a non-flexible, brittle circuit or a strong enclosure) that shall detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure to an extent sufficient for accessing CSPs and/or PSPs.

Required Vendor Information

VE05.45.01: The module shall be contained within a tamper detection envelope that will detect tampering attacks against the potting material or enclosure. The vendor documentation shall describe the tamper detection envelope design.

Required Test Procedures

TE05.45.01: The tester shall verify from the vendor documentation and by inspection that the module contains a tamper detection envelope that surrounds the module components. This barrier shall be designed such that any breach by means such as drilling, milling, grinding, or dissolving to access the module components can be detected by monitoring components in the module.

AS05.46: (Multiple Chip Embedded – Level 4)
The module shall contain tamper response and zeroisation circuitry that shall continuously monitor the tamper detection envelope.

Required Vendor Information

VE05.46.01: The module shall contain tamper response and zeroisation circuitry that continuously monitors the tamper detection envelope for tampering, and upon the detection of tampering, shall zeroise all plaintext CSPs. The circuitry shall be operational whenever plaintext CSPs are contained within the module. The vendor documentation shall describe the tamper response and zeroisation design.

Required Test Procedures

TE05.46.01: The tester shall verify from the vendor documentation that the module contains tamper response and zeroisation circuitry that continuously monitors the tamper detection envelope; detects any breach by means such as drilling, milling, grinding or dissolving any portion of the envelope; and then zeroises all plaintext CSPs.

AS05.47: (Multiple Chip Embedded – Level 4)
***{In conjunction with AS05.46 the module shall contain tamper response and zeroisation circuitry}* and upon the detection of tampering, shall immediately zeroise all CSPs.**

Required Vendor Information

VE05.47.01: The module shall contain tamper response and zeroisation circuitry that continuously monitors the tamper detection envelope for tampering, and upon the detection of tampering, shall zeroise all plaintext CSPs. The vendor documentation shall describe the tamper response and zeroisation design.

Required Test Procedures

TE05.47.01: The tester shall breach the tamper detection envelope barrier and then verify that the module zeroises all plaintext CSPs.

AS05.48: (Multiple Chip Embedded – Level 4)

The tamper response circuitry shall remain operational when CSPs and/or PSPs are contained within the cryptographic module.

NOTE This assertion is not separately tested.

AS05.49: (Multiple Chip Embedded – Level 4)

The zeroisation capability shall remain operational when CSPs are contained within the cryptographic module.

NOTE This assertion is not separately tested.

6.6.1.3 Multiple-Chip Standalone Cryptographic Modules

NOTE In addition to the general security requirements specified in subclause 7.5.1 of ISO/IEC 19790, the following requirements AS05.50 to AS05.63 are specific to multiple-chip standalone cryptographic modules.

AS05.50: (Multiple-Chip Standalone – Levels 1, 2, 3, and 4)
For Security Level 1, the cryptographic module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers.

Required Vendor Information

VE05.50.01: The module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include removable covers or doors. The vendor documentation shall describe the enclosure and its hardness characteristics.

Required Test Procedures

TE05.50.01: The tester shall verify by inspection and from the vendor documentation that the module is contained within an enclosure that meets the following requirements:

1. The enclosure has to completely surround the entire module.
2. The enclosure material has to be of a composition defined in the vendor documentation.
3. The enclosure has to be production-grade. The vendor literature has to either show that an enclosure of the same material has been used commercially, or provide data to show that it is equivalent to a commercial product.

AS05.51: (Multiple-Chip Standalone – Levels 2, 3, and 4)
In addition to the requirements for Security Level 1, the following requirements *{AS05.52 through AS05.54}* shall apply to multiple-chip standalone cryptographic modules for Security Level 2.

NOTE This assertion is not separately tested.

AS05.52: (Multiple-Chip Standalone – Levels 2, 3, and 4)
The enclosure of the cryptographic module shall be opaque within the visible spectrum.

Required Vendor Information

VE05.52.01: The enclosure shall be opaque within the visible spectrum. The vendor documentation shall describe the enclosure's opacity characteristics.

Required Test Procedures

TE05.52.01: The tester shall verify by inspection that the enclosure is opaque within the visible spectrum.

AS05.53: (Multiple-Chip Standalone – Levels 2, 3, and 4)
If the enclosure of the cryptographic module includes any doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys *{or AS05.54 shall apply}*.

Required Vendor Information

VE05.53.01: If the enclosure includes any removable covers or doors, then either they shall be locked with pick-resistant mechanical locks that employ physical or logical keys. The vendor documentation shall describe pick-resistant mechanical locks that employ physical or logical keys.

Required Test Procedures

TE05.53.01: The tester shall verify whether the enclosure contains any removable covers or doors. The tester shall verify that each cover or door is locked with a pick-resistant lock that requires a physical key or a logical key. The tester shall attempt to open the locked cover or door without use of the key and verify that the cover or door will not open without signs of damage.

AS05.54: (Multiple-Chip Standalone – Levels 2, 3, and 4)
***{If AS05.53 is not satisified, then the doors or covers}* shall be protected with tamper-evident seals (e.g., evidence tape or holographic seals).**

Required Vendor Information

VE05.54.01: If the enclosure is protected via tamper-evident seals such as evidence tape or holographic seals, the vendor documentation shall describe the tamper-evident seals.

Required Test Procedures

TE05.54.01: The cover or door is protected with a seal such as evidence tape or a holographic seal. The tester shall verify that the cover or door cannot be opened without breaking or removing the seal, and that the seal cannot be removed and later replaced.

AS05.55: (Multiple-Chip Standalone – Levels 3 and 4)
In addition to the requirements for Security Levels 1 and 2, the following requirements *{AS05.56 or AS05.57}* shall apply to multiple-chip standalone cryptographic modules for Security Level 3.

NOTE This assertion is not separately tested.

AS05.56: (Multiple-Chip Standalone – Levels 3 and 4)
{Either} the multiple-chip embodiment of the circuitry within the module shall be covered with a hard potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum {or AS05.57 shall be satisfied}.

NOTE This assertion is tested in AS05.42.

AS05.57: (Multiple-Chip Standalone – Levels 3 and 4)
{If AS05.56 does not apply, the} module shall be contained within a strong enclosure such that attempts at removal or penetration of the enclosure will have a high probability of causing serious damage to the module (i.e., the module will not function).

NOTE This assertion is tested in AS05.43.

AS05.58: (Multiple-Chip Standalone – Level 4)
In addition to the requirements for Security Levels 1, 2 and 3, the following requirements *{AS05.59 through AS05.63}* shall apply to multiple-chip standalone cryptographic modules for Security Level 4.

NOTE This assertion is not separately tested.

AS05.59: (Multiple-Chip Standalone – Level 4)
The module shall be encapsulated by a tamper detection envelope, by the use of tamper detection mechanisms such as cover switches (e.g., micro switches, magnetic Hall effect switches, permanent magnetic actuators, etc.), motion detectors (e.g., ultrasonic, infrared, or microwave), or other tamper detection mechanisms as described above for multiple-chip embedded cryptographic modules.

Required Vendor Information

VE05.59.01: The enclosure or potting material shall be encapsulated by a tamper detection envelope by the use of tamper detection mechanisms. The vendor documentation shall describe the tamper detection envelope design.

Required Test Procedures

TE05.59.01: The tester shall verify from the vendor documentation and by inspection that the module enclosure or potting material contains tamper detection mechanisms, which shall form a tamper detection envelope that protects the module components. The mechanisms shall be designed such that any breach of the enclosure or potting material to access the module components can be detected.

AS05.60: (Multiple-Chip Standalone – Level 4)
The tamper detection mechanisms shall detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure, to an extent sufficient for accessing CSPs and/or PSPs.

NOTE This assertion is not separately tested.

AS05.61: (Multiple-Chip Standalone – Level 4)
The cryptographic module shall contain tamper response and zeroisation capability that shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroise all CSPs.

Required Vendor Information

VE05.61.01: The module shall contain tamper response and zeroisation circuitry that continuously monitors the tamper detection envelope for tampering, and upon the detection of tampering, shall zeroise all plaintext CSPs. The circuitry shall be operational whenever plaintext CSPs are contained within the module. The vendor documentation shall describe the tamper response and zeroisation design.

Required Test Procedures

TE05.61.01: The tester shall verify from the vendor documentation that the module contains tamper response and zeroisation circuitry that continuously monitors the tamper detection envelope; detects any breach by means such as drilling, milling, grinding or dissolving any portion of the envelope; and then zeroises all plaintext CSPs.

TE05.61.02: The tester shall breach the tamper detection envelope barrier and then verify that the module zeroises all plaintext CSPs.

AS05.62: (Multiple-Chip Standalone – Level 4)
The tamper response capability shall remain operational when CSPs and/or PSPs are contained within the cryptographic module.

NOTE This assertion is not separately tested.

AS05.63: (Multiple-Chip Standalone – Level 4)
The zeroisation capability shall remain operational when CSPs are contained within the cryptographic module.

NOTE This assertion is not separately tested.

6.6.2 Environmental failure protection/testing

AS05.64: (Environmental failure protection/testing – Level 4)
A module shall either employ environmental failure protection (EFP) features *{AS05.65 to AS05.69}* or undergo environmental failure testing (EFT) *{AS05.70 to AS05.74}*.

Required Vendor Information

VE05.64.01: The vendor shall use either of the following:

1. EFP features; or
2. EFT

as specified in subclause 7.5.2 of ISO/IEC 19790, to ensure that the following four unusual environmental conditions or fluctuations (accidental or induced) outside of the module's normal operation range will not compromise the security of the module:

A. Low temperature

B. High temperature

C. Large negative voltage

D. Large positive voltage

The vendor shall choose to use EFP or EFT for each condition, but each choice is independent of the choices for the other conditions. The vendor shall provide corresponding supporting EFP/EFT documentation for each condition, specifying how the selected approach is used.

Required Test Procedures

TE05.64.01 The tester shall verify that the documentation states EFP/EFT selection for each condition and how the specified approach is used.

6.6.2.1 Environmental Failure Protection Features (Alternative 1)

AS05.65: (Environmental failure protection features – Level 4)
Environmental failure protection (EFP) features *{AS05.66 to AS05.69}* shall protect a cryptographic module against unusual environmental conditions or fluctuations (accidental or induced) outside of the module's normal operating range that can compromise the security of the module.

NOTE This assertion is tested as part of AS05.68.

AS05.66: (Environmental failure protection features – Level 4)
The module shall monitor and correctly respond to fluctuations in the operating temperature and voltage outside of the specified normal operating ranges.

NOTE This assertion is tested as part of AS05.68.

AS05.67: (Environmental failure protection features – Level 4)
The EFP features shall involve electronic capability or devices that continuously measure the operating temperature and voltage of a cryptographic module.

NOTE This assertion is tested as part of AS05.68.

AS05.68: (Environmental failure protection features – Level 4)
If the temperature or voltage falls outside of the cryptographic module's normal operating range, the protection capability shall either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs.

Required Vendor Information

VE05.68.01: If EFP is chosen for a particular condition, the module shall monitor and correctly respond to fluctuations in the operating temperature or voltage, outside of the module's normal operating range for that condition. The protection features shall continuously measure these environmental conditions. If a condition is determined to be outside of the module's normal operating range, the protection circuitry shall either:

1. Shut down the module; or

2. Zeroise all plaintext CSPs

Documentation shall state which of these approaches was chosen and provide a specification description of the EFP features implemented within the module.

Required Test Procedures

TE05.68.01: The tester shall configure the environmental condition (ambient temperature and voltage) close to the appropriate extreme of the normal operating range specified for the module, and verify that the module continues to perform within normal operating parameters.

TE05.68.02: The tester shall extend the temperature and voltage outside of the specified normal range and verify that the module either shuts down to prevent further operations or zeroises all plaintext CSPs.

TE05.68.03: If the module is designed to zeroise all plaintext CSPs, and the module was still operational after returning to the normal environmental range, the tester shall perform services that require keys and verify that the module does not perform these services.

AS05.69: (Environmental failure protection features – Level 4)
Documentation shall specify the normal operating ranges of a cryptographic module and the environmental failure protection features employed by the module.

NOTE This assertion is tested as part of AS05.68.

6.6.2.2 Environmental Failure Testing Procedures (Alternative 2)

AS05.70: (Environmental failure testing procedures – Level 4)
Environmental failure testing (EFT) shall involve a combination of analysis, simulation, and testing of a cryptographic module to provide reasonable assurance that environmental conditions or fluctuations (accidental or induced) outside the module's normal operating ranges for temperature and voltage will not compromise the security of the module.

NOTE This assertion is tested as part of AS05.72.

AS05.71: (Environmental failure testing procedures – Level 4)
EFT shall demonstrate that, if the operating temperature or voltage falls outside the normal operating range of the module resulting in a failure, at no time shall the security of the cryptographic module be compromised.

NOTE This assertion is tested as part of AS05.72.

AS05.72: (Environmental failure testing procedures – Level 4)

The temperature range to be tested shall be from a temperature within the normal operating temperature range up to the largest negative temperature that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs; and from a temperature within the normal operating temperature range up to the largest positive temperature that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs. The temperature range to be tested shall be from - 100° to + 200° Celsius (- 150° to + 400° Fahrenheit), however, the test shall be interrupted as soon as either (1) the module is shutdown to prevent further operation, (2) all CSPs are immediately zeroised or (3) put the module in failure.

Required Vendor Information

VE05.72.01: If EFT is chosen for a particular condition, the module shall be tested within the temperature and voltage ranges specified in AS05.68. The module shall either:

1. Continue to operate normally; or
2. Shut down; or
3. Zeroise all plaintext CSPs

Documentation shall state which of these approaches was chosen and provide a specification description of the EFT.

Required Test Procedures

TE05.72.01: The tester shall configure the environmental condition (ambient temperature and voltage) as specified in AS05.68, and verify that the module either continues to operate normally, or shuts down to prevent further operations, or zeroises all plaintext CSPs.

TE05.72.02: If the module is designed to zeroise all plaintext CSPs, and the module was still operational after returning to the normal environmental range, the tester shall perform services that require keys and verify that the module does not perform these services.

AS05.73: (Environmental failure testing procedures – Level 4)

The voltage range to be tested shall be from the smallest negative voltage (with respect to ground) that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs to the smallest positive voltage (with respect to ground) that that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all CSPs, including reversing the polarity of the voltages.

NOTE This assertion is tested as part of AS05.72.

AS05.74: (Environmental failure testing procedures – Level 4)
Documentation shall specify the normal operating ranges of the cryptographic module and the environmental failure tests performed.

NOTE This assertion is tested as part of AS05.72.

6.7 Operational environment

AS06.01: (Operational environment – Levels 1, 2, 3, and 4)
If the operational environment is a modifiable operational environment the operating system requirements in *{sub}*clause 7.6.1 *{of ISO/IEC 19790:2006}* shall apply.

NOTE This assertion is not separately tested.

NOTE If the operational environment is non-modifiable or a limited operational environment, the operating system requirements in subclause 7.6.1 of ISO/IEC 19790 do not apply.

AS06.02: (Operational environment – Levels 1, 2, 3, and 4)
Documentation shall specify the operational environment for a cryptographic module, including, if applicable, the operating system employed by the module, and for Security Levels 2, 3, and 4, the approved Protection Profile as listed in Annex C *{of ISO/IEC 19790:2006}*.

Required Vendor Information

VE06.02.01: The vendor documentation shall describe the operational environment in which the module operates.

Required Test Procedures

TE06.02.01: The tester shall verify that the information specified in VE06.02.01 is included.

AS06.03: (Operational environment – Levels 1, 2, 3, and 4)

The following requirements *{AS06.04 through AS06.08}* shall apply to operating systems for Security Level 1.

NOTE This assertion is not separately tested.

AS06.04: (Operational environment – Level 1 Only)
For Security Level 1 only, the operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded).

Required Vendor Information

VE06.04.01: The vendor shall provide a description of the mechanism used to ensure that only one user at a time can use the cryptographic module.

Required Test Procedures

TE06.04.01: The tester shall verify, from the vendor documentation and by inspection of the cryptographic module, that only one operator at a time can access the cryptographic module.

TE06.04.02: The tester shall operate the cryptographic module as described in the crypto officer and user guidance documentation. While the cryptographic module is operating as specified, the same or another tester shall attempt to circumvent the single-user enforcement mechanism.

AS06.05: (Operational environment – Level 1 Only)
For Security Level 1 only, the cryptographic module shall prevent access by other processes to CSPs, and/or PSPs, during the time the cryptographic module is executing/operational.

NOTE Processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.

Required Vendor Information

VE06.05.01: The vendor shall provide a description of the mechanism used to ensure that no other process can access CSPs, and/or PSPs while the cryptographic process is in use.

Required Test Procedures

TE06.05.01: The tester shall verify, from the vendor documentation and by inspection of the cryptographic module, that no other process can access CSPs, and/or PSPs while the cryptographic module is in use.

TE06.05.02: The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to access secret and private keys, intermediate key generation values, and other CSPs.

AS06.06: (Operational environment – Level 1 Only)
Non-cryptographic processes shall not interrupt a cryptographic module during execution.

Required Vendor Information

VE06.06.01: The vendor shall provide a description of the mechanism used to ensure that no other process can interrupt the cryptographic module during execution.

Required Test Procedures

TE06.06.01: The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are operating, the same or another tester shall attempt to execute another process.

AS06.07: (Operational environment – Levels 1, 2, 3, and 4)
All cryptographic software and firmware shall be installed in a form that protects the software and firmware source and executable code from unauthorised disclosure and modification.

Required Vendor Information

VE06.07.01: The vendor shall provide a list of the cryptographic software and firmware that are stored on the cryptographic module and shall provide a description of the protection mechanisms used to prevent unauthorised disclosure and modification.

Required Test Procedures

TE06.07.01: The tester shall attempt to perform unauthorised accesses and unauthorised modifications to software and firmware source and executable code.

AS06.08: (Operational environment – Levels 1, 2, 3, and 4)
A cryptographic mechanism using an approved integrity technique (e.g., an approved message authentication code or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the cryptographic module.

NOTE This cryptographic mechanism requirement may be incorporated as part of the Software/Firmware Integrity Test (subclause 7.8.1 of ISO/IEC 19790:2006) if an approved authentication technique is employed for that test.

Required Vendor Information

VE06.08.01: The vendor shall provide documentation that identifies the technique used to maintain the integrity of the cryptographic software and firmware components.

Required Test Procedures

TE06.08.01: The tester shall verify that the information specified in VE06.08.01 is included.

TE06.08.02: The tester shall modify the cryptographic software and firmware components.

This test fails if the integrity techniques does not detect the modifications.

AS06.09: (Operational environment – Level 2)
In addition to the applicable requirements for Security Level 1, the following requirements *{AS06.10 through AS06.20}* shall also apply for Security Level 2.

NOTE This assertion is not separately tested.

AS06.10: (Operational environment – Level 2)
All cryptographic software and firmware, CSPs, PSPs and control and status information shall be under the control of an operating system that meets the functional requirements specified in the Protection Profiles specified in Annex C *{*of ISO/IEC 19790:2006*}* and shall be evaluated at the ISO/IEC 15408 evaluation assurance level EAL2.

Required Vendor Information

VE06.10.01: The vendor shall provide documentation that the operating system controlling the cryptographic module has successfully passed evaluation at EAL2 for the functional requirements specified in the protection profiles listed in Annex C of ISO/IEC 19790

Required Test Procedures

TE06.10.01: The tester shall verify that the operating system has received a certificate mutually recognised in accordance with the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.

AS06.11: (Operational environment – Levels 2, 3, and 4)
To protect plaintext data, cryptographic software and firmware, CSPs, PSPs, the discretionary access control mechanisms of the operating system shall be configured to specify the set of roles that can *execute* stored cryptographic software and firmware.

Required Vendor Information

VE06.11.01: The vendor documentation requirement is specified under VE06.14.01.

Required Test Procedures

TE06.11.01: This TE is tested as part of TE06.14.01.

TE06.11.02: The tester shall assume a role with privileges to execute the stored cryptographic software and firmware components. The tester shall execute the stored cryptographic software and firmware components to verify the correct configuration of the operating system access control mechanisms.

TE06.11.03: The tester shall assume a role that does not have privileges to execute the stored cryptographic software and firmware components. The tester shall attempt to execute the stored cryptographic software and firmware components to verify the correct configuration of the operating system access control mechanisms. If the tester can execute the stored cryptographic software and firmware components, this test fails.

AS06.12: (Operational environment – Levels 2, 3, and 4)
***{To protect plaintext data, cryptographic software and firmware, CSPs, PSPs, the discretionary access control mechanisms of the operating system shall be configured to specify the set of roles that can} modify* (i.e., write, replace, and delete) the following cryptographic module software or firmware components stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., audit data), CSPs, PSPs, and plaintext data.**

Required Vendor Information

VE06.12.01: The vendor documentation requirement is specified under VE06.14.01.

Required Test Procedures

TE06.12.01: This TE is tested as part of TE06.14.01.

TE06.12.02: The tester shall assume a role with privileges to modify the following cryptographic module software and firmware components stored within the cryptographic boundary:

1. Cryptographic programs

2. Cryptographic data (e.g., audit data)
3. CSPs
4. PSPs
5. Plaintext data

The tester shall modify the cryptographic module software and firmware components stored within the cryptographic boundary.

TE06.12.03: The tester shall assume a role that does not have privileges to modify the stored cryptographic software and firmware components. The tester shall attempt to modify the stored cryptographic software and firmware components.

AS06.13: (Operational environment – Levels 2, 3, and 4)
***{To protect plaintext data, cryptographic software and firmware, CSPs, PSPs, the discretionary access control mechanisms of the operating system shall be configured to specify the set of roles that can} read* the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., audit data), CSPs, and plaintext data.**

Required Vendor Information

VE06.13.01: The vendor documentation requirement is specified underVE06.14.01.

Required Test Procedures

TE06.13.01: This TE is tested as part of TE06.14.01.

TE06.13.02: The tester shall assume a role with privileges to read the following cryptographic module software components stored within the cryptographic boundary:

1. Cryptographic data (e.g. audit data)
2. CSPs
3. Plaintext data

The tester shall read the cryptographic module software components stored within the cryptographic boundary.

TE06.13.03: The tester shall assume a role that does not have privileges to read the stored cryptographic software components. The tester shall attempt to read the stored cryptographic software components.

AS06.14: (Operational environment – Levels 2, 3, and 4)
***{To protect plaintext data, cryptographic software and firmware, CSPs, PSPs, the discretionary access control mechanisms of the operating system shall be configured to specify the set of roles that can} enter* CSPs and/or PSPs.**

Required Vendor Information

VE06.14.01: The vendor shall provide documentation that specifies how the discretionary access control (DAC) mechanism is configured to meet the requirements of AS06.11, AS06.12, AS06.13, and AS06.14.

Required Test Procedures

TE06.14.01: The tester shall verify that the vendor has supplied the information required under VE06.14.01.

TE06.14.02: The tester shall assume a role with privileges to enter CSPs and/or PSPs. The tester shall enter CSPs and/or PSPs.

TE06.14.03: The tester shall assume a role that does not have privileges to enter CSPs and/or PSPs. The tester shall attempt to enter CSPs and/or PSPs.

AS06.15: (Operational environment – Levels 2, 3, and 4)
The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images).

Required Vendor Information

VE06.15.01: The vendor shall provide documentation that specifies how the operating system prevents all operators and executing processes from modifying executing cryptographic processes.

Required Test Procedures

TE06.15.01: The tester shall verify that the vendor has supplied the information required under VE06.15.01.

TE06.15.02: The tester shall attempt to modify executing cryptographic processes. This test fails if an operator or executing process can modify an executing cryptographic process.

AS06.16: (Operational environment – Levels 2, 3, and 4)
The operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary.

Required Vendor Information

VE06.16.01: The vendor shall provide documentation that specifies how the operating system prevents operators and executing processes from reading cryptographic software stored within the cryptographic boundary.

Required Test Procedures

TE06.16.01: The tester shall verify that the vendor has supplied the information required under VE06.16.01.

TE06.16.02: The tester shall attempt to read cryptographic software stored within the cryptographic boundary. The tester shall verify that no operator or executing process can read the cryptographic software stored within the cryptographic boundary.

AS06.17: (Operational environment – Levels 2, 3, and 4)
The operating system shall provide an audit mechanism to record modifications, accesses, deletions, and additions of cryptographic data, CSPs and PSPs.

NOTE An assumption of this assertion is that the cryptographic module is using the audit mechanism provided by the operating system to audit the identified events. It is insufficient for the cryptographic module software to use another file as its audit log, no matter how well protected.

Required Vendor Information

VE06.17.01: The vendor shall identify all the events that are auditable by the cryptographic module software. The list shall include the events specified in AS06.18 and AS06.19.

Required Test Procedures

TE06.17.01: The tester shall verify that the vendor has supplied the information required under VE06.17.01

TE06.17.02: The tester shall verify, from the vendor documentation and by inspection of the cryptographic module, that the cryptographic module is using the audit mechanism provided by the operating system to audit the identified events.

TE06.17.03: The tester shall exercise the cryptographic module, with the auditing capability turned on, and perform the actions that generate auditable events. The tester shall verify the system's audit log if all the events were audited.

NOTE The tester DOES NOT have to test the audit mechanism provided by the operating system and identified by the vendor.

AS06.18: (Operational environment – Levels 2, 3, and 4)
The following events shall be recorded by the audit mechanism:

- **attempts to provide invalid input for crypto officer functions, and**
- **the addition or deletion of an operator to/from a crypto officer role.**

NOTE This assertion is tested as part of AS06.17.

AS06.19: (Operational environment – Levels 2, 3, and 4)
The audit mechanism shall be capable of auditing the following events:

- **operations to process audit data stored in the audit trail,**
- **requests to use authentication data management mechanisms,**
- **use of a security-relevant crypto officer function,**
- **requests to access user authentication data associated with the cryptographic module,**
- **use of an authentication mechanism (e.g., login) associated with the cryptographic module,**
- **explicit requests to assume a crypto officer role; and**
- **the allocation of a function to a crypto officer role.**

NOTE This assertion is tested as part of AS06.17.

AS06.20: (Operational environment – Levels 2, 3, and 4)
The stored audit data shall be protected from unauthorised access.

Required Vendor Information

VE06.20.01: The vendor shall provide documentation that specifies how the stored audit date is protected from unauthorised access.

Required Test Procedures

TE06.20.01: The tester shall verify that the vendor has supplied the information required under VE06.20.01.

TE06.20.02: The tester shall attempt to read audit data stored within the cryptographic boundary. The tester shall verify that a user without authorisation cannot access the store audit data that is stored within the cryptographic boundary.

AS06.21: (Operational environment – Level 3)
In addition to the applicable requirements for Security Levels 1 and 2, the following requirements *{AS06.22 to AS06.27}* shall apply for Security Level 3.

NOTE This assertion is not separately tested.

AS06.22: (Operational environment – Level 3)

All cryptographic software and firmware, CSPs, PSPs and control and status information shall be under the control of an operating system that meets the functional requirements specified in the Protection Profiles specified in Annex C *{ of ISO/IEC 19790:2006}*.

Required Vendor Information

VE06.22.01: The vendor shall provide documentation that the operating system is controlling all cryptographic software and firmware, CSPs, PSPs and control and status information.

Required Test Procedures

TE06.22.01: The tester shall verify that the operating system all cryptographic software and firmware, CSPs, PSPs and control and status information and is meeting functional requirements specified in the protection profiles specified in Annex C of ISO/IEC 19790:2006 is controlling.

AS06.23: (Operational environment – Level 3)

The operating system shall be evaluated at the ISO/IEC 15408 evaluation assurance level EAL3 and include the following additional requirements: Trusted Path (FTP_TRP.1) and Informal TOE Security Policy Model (ADV_SPM.1).

Required Vendor Information

VE06.23.01: The vendor shall provide documentation that the operating system controlling the cryptographic module has successfully passed evaluation at EAL3 (plus Informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1)) for the functional requirements (plus Trusted Path (FTP_TRP.1)) specified in the protection profiles listed in Annex C of ISO/IEC 19790:2006.

Required Test Procedures

TE06.23.01: The tester shall verify that the operating system has received a certificate mutually recognised in accordance with the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.

AS06.24: (Operational environment – Levels 3 and 4)

All CSPs, control inputs, and status outputs shall be communicated via a trusted mechanism (e.g., a dedicated I/O physical port or a trusted path).

Required Vendor Information

VE06.24.01: The vendor shall document the trusted path mechanism used by the cryptographic module to communicate CSPs, control inputs, and status outputs.

Required Test Procedures

TE06.24.01: The tester shall verify that the vendor has supplied the information required under VE06.24.01.

TE06.24.02: The tester shall use the trusted mechanism to communicate all CSPs, control inputs, and status outputs

NOTE If the trusted mechanism is a trusted path, and the trusted path was an evaluated feature of the operating system, the tester need not independently test the trusted path. If the trusted mechanism is not a trusted path, or if a trusted path is not an evaluated feature of the operating system, then the tester shall test for correct operation and non-circumventability of the trusted mechanism.

TE06.24.03: The tester shall attempt, for each input and output identified in AS06.24, to enter or output the information via an untrusted mechanism.

AS06.25: (Operational environment – Levels 3 and 4)
If a trusted path is used, the TOE Security Functions (TSF) shall support the trusted path between the TSF and the operator when a positive TSF-to-operator connection is required.

Required Vendor Information

VE06.25.01: The vendor documentation shall specify the trusted path used between the TSF and the operator when a positive TSF-to-operator connection is required.

Required Test Procedures

TE06.25.01: The tester shall verify that the vendor documentation specifies the trusted path used between the TSF and the operator when a positive TSF-to-operator connection is required.

AS06.26: (Operational environment – Levels 3 and 4)
Communications via this trusted path shall be activated exclusively by an operator or the TSF and shall be logically isolated from other paths.

Required Vendor Information

VE06.26.01: The vendor shall document how the trusted path is activated exclusively by an operator or the TSF and is logically isolated from other paths.

Required Test Procedures

TE06.26.01: The tester shall verify that the vendor has supplied the information required under VE06.26.01.

TE06.26.02: The tester shall invoke the trusted path. If the capability exists for the TSF to invoke the trusted path, the tester shall exercise the cryptographic module to cause the TSF to invoke the trusted path.

TE06.26.03: The tester shall attempt to cause the trusted path to be invoked by non-TSF software.

AS06.27: (Operational environment – Levels 3 and 4)
In addition to the audit requirements of Security Level 2, the following events shall be recorded by the audit mechanism:

- **attempts to use the trusted path function;**
- **identification of the initiator and target of a trusted path;**
- **unsuccessful self test operations; and**
- **notification of tamper detection.**

Required Vendor Information

VE06.27.01: The vendor list of audited events shall include attempts to use the trusted path function, and identification of the initiator and target of a trusted path.

Required Test Procedures

TE06.27.01: The tester shall verify that the vendor has supplied the information required under VE06.27.01

NOTE The tester DOES NOT have to test the audit mechanism provided by the operating system and identified by the vendor.

TE06.27.02: The tester shall exercise the cryptographic module, with the auditing capability turned on, and perform the actions that generate the audited events. The tester shall verify the system's audit log if all the events were audited.

AS06.28: (Operational environment – Level 4)
In addition to the applicable requirements *{AS06.03 to AS06.27}* for Security Levels 1, 2, and 3, the following requirements *{AS06.29 and AS06.30}* shall also apply to operating systems for Security Level 4.

NOTE This assertion is tested as part of AS06.29.

AS06.29: (Operational environment – Level 4)
All cryptographic software, CSPs, PSPs and control and status information shall be under the control of an operating system that meets the functional requirements specified in the Protection Profiles specified in Annex C {of ISO/IEC 19790:2006}.

Required Vendor Information

VE06.29.01: The vendor shall provide documentation that the operating system is controlling all cryptographic software, CSPs, PSPs and control and status information.

Required Test Procedures

TE06.29.01: The tester shall verify that the documentation that the operating system demonstrate controlling of all cryptographic software, CSPs, PSPs and control and status information.

AS06.30: (Operational environment – Level 4)
The operating system shall be evaluated at the ISO/IEC 15408 evaluation assurance level EAL4.

Required Vendor Information

VE06.30.01: The vendor shall provide documentation that the operating system controlling the cryptographic module has successfully passed evaluation at EAL4 for the functional requirements specified in the protection profiles listed in Annex C of ISO/IEC 19790:2006.

Required Test Procedures

TE06.30.01: The tester shall verify that the operating system has received a certificate mutually recognised in accordance with the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.

6.8 Cryptographic key management

NOTE CSPs encrypted using a non-approved algorithm or proprietary algorithm or method are considered in plaintext form, within the scope of this International Standard.

General

AS07.01: (Key management – Levels 1, 2, 3, and 4)
CSPs shall be protected within the cryptographic module from unauthorised disclosure, modification, and substitution.

Required Vendor Information

VE07.01.01: The vendor documentation shall describe the protection of all CSPs internal to the module. Protection shall include the implementation of mechanisms that protect against unauthorised disclosure, unauthorised modification, and unauthorised substitution.

Required Test Procedures

TE07.01.01: The tester shall check the vendor documentation that describes the protection of CSPs. The tester shall verify that the documentation describes how these CSPs are protected from unauthorised disclosure, unauthorised modification, and unauthorised substitution.

TE07.01.02: The tester shall perform the following tests:

1. Attempt to access (by circumventing the documented protection mechanisms) CSPs for which the tester is not authorised to access. To meet this assertion the module is required to deny access or to allow access only to encrypted or otherwise protected forms of the CSPs.

2. Modify all CSPs using any method not specified by the vendor documentation and attempt to enter them into the module. The module is required to not allow any of the CSPs to be successfully loaded to meet this assertion. The tester shall attempt to perform cryptographic operations using secret keys and private keys. The module is required to not perform the operations to meet this assertion. The tester shall attempt to perform a cryptographic service using the CSPs. The module is required to not perform the operations to meet this assertion.

AS07.02: (Key management – Levels 1, 2, 3, and 4)
PSPs shall be protected within the cryptographic module against unauthorised modification and substitution.

Required Vendor Information

VE07.02.01: The vendor documentation shall describe the protection of all PSPs against unauthorised modification and substitution.

Required Test Procedures

TE07.02.01: The tester shall verify that the vendor documentation describe how the PSPs are protected from unauthorised modification and unauthorised substitution.

TE07.02.02: The tester shall modify all PSPs using any method not specified by the vendor documentation and shall attempt to enter them into the module. The module is required to not allow any of the PSPs to be successfully loaded to meet this assertion. The tester shall attempt to perform cryptographic operations using these PSPs; the module is required to not perform the operations, indicating that the PSPs were not loaded, to meet this assertion.

AS07.03: (Key management – Levels 1, 2, 3, and 4)
Documentation shall specify all CSPs and PSPs employed by a cryptographic module.

Required Vendor Information

VE07.03.01: The vendor documentation shall provide a list all CSPs and PSPs used by the module.

Required Test Procedures

TE07.03.01: The tester shall verify the vendor documentation that the information specified in VE07.03.01 is included.

6.8.1 Random bit generators (RBGs)

NOTE A cryptographic module may employ random bit generators (RBGs), a chain of RBGs, or may be solely an RBG.

AS07.04: (Random bit generators – Levels 1, 2, 3, and 4)
All RBGs and their usage shall be defined.

Required Vendor Information

VE 07.04.01 The vendor shall provide the list of all RBGs used in the cryptographic module and their precise usage.

Required Test Procedures

TE07.04.01 The tester shall verify that all RBGs are listed and their usage defined.

AS07.05: (Random bit generators – Levels 1, 2, 3, and 4)
If a cryptographic module employs an approved RBG, or chain of RBGs, in an approved mode of operation, the RBG entropy source shall be subject to the RBG entropy test as specified in *{sub}*clause 7.8.1 *{of ISO/IEC 19790:2006}*.

NOTE This assertion is tested in AS08.20.

AS07.06: (Random bit generators – Levels 1, 2, 3, and 4)
If a cryptographic module employs an approved RBG, or chain of RBGs, in an approved mode of operation, the deterministic components of an RBG shall be subject to the cryptographic algorithm test in {sub}clause 7.8.1 {of ISO/IEC 19790:2006}.

NOTE This assertion is tested in AS08.14.

AS07.07: (Random bit generators – Levels 1, 2, 3, and 4)
If a cryptographic module employs an approved RBG, or chain of RBGs, in an approved mode of operation, the data output from the RBG shall pass the continuous random bit generator test as specified in *{sub}*clause 7.8.2 *{of ISO/IEC 19790:2006}*.

NOTE This assertion is tested in AS08.33, AS08.34 and AS08.35.

AS07.08: (Random bit generators – Levels 1, 2, 3, and 4)

The RBG and its mode of operation shall be compliant with ISO/IEC 18031.

Required Vendor Information

VE07.08.01: The vendor shall provide documentation stating that the RBG is compliant with ISO/IEC 18031.

Required Test Procedures

TE07.08.01: The tester shall verify that the vendor has provided documentation asserting that the RBG is compliant with ISO/IEC 18031.

TE07.08.02: The tester shall verify the vendor provided documentation that the implemented RBG matches the specified compliant RBG.

6.8.2 Key generation

AS07.09: (Key generation – Levels 1, 2, 3, and 4)
Cryptographic keys generated by the cryptographic module for use by an approved algorithm or security function shall be generated using an approved RBG.

Required Vendor Information

VE07.09.01: The vendor shall provide documentation stating that an approved RBG is used to generate keys.

Required Test Procedures

TE07.09.01: The tester shall verify that the vendor has provided documentation asserting that an approved RBG is used to generate keys.

TE07.09.02: The tester shall verify that the implemented RBG is an approved RBG.

AS07.10: (Key generation – Levels 1, 2, 3, and 4)
Compromising the security of the key generation method (e.g., guessing the seed value to initialise the deterministic RBG) shall require at least as many operations as determining the value of the generated key.

Required Vendor Information

VE07.10.01: The vendor shall provide documentation that provides rationale stating how compromising the security of the key generation method (e.g., guessing the seed value to initialise the deterministic RBG) shall require at least as many operations as determining the value of the generated key.

Required Test Procedures

TE07.10.01: The tester shall verify that the vendor provided documentation that provides rationale stating how compromising the security of the key generation method (e.g., guessing the seed value to initialise the deterministic RBG) shall require at least as many operations as determining the value of the generated key.

TE07.10.02: The tester shall verify the accuracy 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.

AS07.11: (Key generation – Levels 1, 2, 3, and 4)
If a seed key is entered during the key generation process, entry of the key shall meet the key entry requirements specified in *{sub}*clause 7.7.4 *{of ISO/IEC 19790:2006}*.

NOTE This assertion is not separately tested.

AS07.12: (Key generation – Levels 1, 2, 3, and 4)
If intermediate key generation values are output from the cryptographic module, the values shall be output either:

1. **in encrypted form; or**
2. **under split knowledge techniques.**

Required Vendor Information

VE07.12.01: The vendor documentation shall indicate whether any intermediate key generation values are output from the module upon completion of the key generation process.

VE07.12.02: If intermediate key generation values are output from the cryptographic module upon the completion of the key generation process, then the documentation shall specify that the values are output either (1) in encrypted form or (2) under split knowledge procedures.

Required Test Procedures

TE07.12.01: The tester shall verify that the vendor documentation indicates whether any intermediate key generation values are output from the module upon completion of the key generation process.

TE07.12.02: The tester shall verify that no intermediate key generation values are output from the cryptographic module during the key generation process.

TE07.12.03: The tester shall verify the output interface that all output matches the documented output and that no plaintext intermediate key generation values are output.

TE07.12.04: The tester shall verify that upon completion, the intermediate key generation values are output in either (1) in encrypted form, or (2) under split knowledge procedures.

6.8.3 Key establishment

NOTE Key establishment may be performed by approved methods (e.g., use of a public key algorithm), manual transport methods (use of a manually-transported key loading device), or a combination of electronic and manual transport methods.

AS07.13: (Key establishment – Levels 1, 2, 3, and 4)
If a cryptographic module employs key establishment methods, only approved key establishment methods shall be used and defined.

NOTE Examples of approved key establishment methods can be found in Annex E of ISO/IEC 19790:2006.

Required Vendor Information

VE07.13.01: The vendor shall provide documentation specifying that an approved key establishment method is used.

Required Test Procedures

TE07.13.01: The tester shall verify that the vendor has provided documentation asserting that the approved key establishment methods used are found in Annex E of ISO/IEC 19790:2006.

TE07.13.02: The tester shall verify the vendor provided documentation that the implemented key establishment methods match the specified approved key establishment methods.

AS07.14: (Key establishment – Levels 1, 2, 3, and 4)
Compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require at least as many operations as determining the key value being transported or agreed upon.

Required Vendor Information

VE07.14.01: The vendor shall provide documentation that provides rationale stating how compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require as many operations as determining the value of the cryptographic key being transported or agreed upon.

Required Test Procedures

TE07.14.01: The tester shall verify that the vendor provided documentation provides rationale stating how compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require as many operations as determining the value of the cryptographic key being transported or agreed upon.

TE07.14.02: The tester shall verify the accuracy 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.

AS07.15: (Key establishment – Levels 1, 2, 3, and 4)
If a key transport method is used, the cryptographic key being transported shall meet the key entry/output requirements of *{sub}*clause 7.7.4 *{of ISO/IEC 19790:2006}*.

NOTE 1 This assertion is tested as part of AS07.17 to AS07.23.

NOTE 2 If a key agreement method is used (e.g., a cryptographic key is derived from shared intermediate values), the shared values are not required to meet the key entry/output requirements of subclause 7.7.4 of ISO/IEC 19790:2006.

6.8.4 Key entry and output

NOTE Cryptographic keys may be entered into or output from a cryptographic module.

AS07.16: (Key entry and output – Levels 1, 2, 3, and 4)
The entry or output of keys shall be performed and defined using either manual (e.g., via a keyboard) or electronic methods (e.g., smart cards/tokens, PC cards, or other electronic key loading devices or connections).

NOTE This assertion is tested as part of AS07.18 to AS07.29.

AS07.17: (Key entry and output – Levels 1, 2, 3, and 4)
A seed key, if entered during key generation, shall be entered in the same manner as cryptographic keys.

Required Vendor Information

VE07.17.01: The key management documentation shall describe the entry of the seed key.

Required Test Procedures

TE07.17.01: The tester shall verify the vendor provided documentation whether a seed key is used for key generation. If so, the tester shall verify the key management documentation that entry of the seed key is identical to the entry of a cryptographic key.

TE07.17.02: The tester shall enter a seed key and shall verify that the method used to enter it is consistent with the documented method.

AS07.18: (Key entry and output – Levels 1, 2, 3, and 4)
All encrypted secret and private keys, entered into or output from a cryptographic module and used in an approved mode of operation, shall be encrypted using an approved algorithm (listed at Annex D *{of ISO/IEC 19790:2006}*) and may be integrity protected.

NOTE Public keys may be entered into or output from a cryptographic module in plaintext form and may be integrity protected.

Required Vendor Information

VE07.18.01: The vendor shall supply documentation specifying the approved algorithms used to encrypt secret and private keys entered into or output from the cryptographic module.

Required Test Procedures

TE07.18.01: The tester shall verify that the vendor supplied documentation specifies the approved algorithms used to encrypt secret and private keys entered into or output from the cryptographic module.

TE07.18.02: The tester shall verify the vendor provided documentation that the implemented approved algorithms used to encrypt secret and private keys entered into or output from the cryptographic module matches the specified encryption methods.

AS07.19: (Key entry and output – Levels 1, 2, 3, and 4)
A cryptographic module shall associate a key (secret, private, or public) entered into or output from the module with the name of the correct entity (i.e., person, group, or process) to which the key is assigned.

Required Vendor Information

VE07.19.01: The documented key entry/output procedures shall describe the mechanisms or procedures used to ensure that each key is associated with the correct entity.

Required Test Procedures

TE07.19.01: The tester shall verify the documented key entry/output procedures that the procedures address how an entered or output key is associated with the correct entity.

TE07.19.02: For each key that can be entered, the tester shall first enter the key while assuming the correct entity. The tester shall then verify that entry is not possible when assuming an incorrect entity.

TE07.19.03: For each key that can be output, the tester shall first output the key while assuming the correct entity. The tester shall then verify that output is not possible when assuming an incorrect entity.

AS07.20: (Key entry and output – Levels 1, 2, 3 and 4)
Manually-entered cryptographic keys shall be verified during entry into a cryptographic module for accuracy using the manual key entry test specified in *{sub}*clause 7.8.2 *{of ISO/IEC 19790:2006}*.

NOTE 1 This assertion is not separately tested.

NOTE 2 During key entry, the manually entered values may be temporarily displayed to allow visual verification and to improve accuracy.

AS07.21: (Key entry and output – Levels 1, 2, 3, and 4)
If encrypted cryptographic keys or key components are manually entered into the cryptographic module, then the plaintext values of the cryptographic keys or key components shall not be displayed.

Required Vendor Information

VE07.21.01: The documented key entry procedures shall preclude the display of plaintext secret or private keys that result from the entry of encrypted keys or key components.

Required Test Procedures

TE07.21.01: The tester shall verify the documented key entry procedures that the display of plaintext keys resulting from the entry of encrypted keys or key components is not allowed during the key entry process.

TE07.21.02: The tester shall enter all encrypted cryptographic keys and key components and shall monitor the output interface of the module to verify that any resulting plaintext key material is not displayed.

AS07.22: (Key entry and output – Levels 1 and 2)
Secret and private keys transported using electronic methods shall be entered into and output from a cryptographic module in encrypted form.

NOTE Secret and private keys transported using *manual transport methods* may be entered into or output from a cryptographic module in plaintext form.

Required Vendor Information

VE07.22.01: The vendor documentation shall specify keys that are transported using electronic methods. The vendor documentation shall state whether these keys are entered into and output in encrypted form.

Required Test Procedures

TE07.22.01: The tester shall verify that the vendor has provided documentation asserting that secret and private keys transported using electronic methods are entered into and output from the cryptographic module in encrypted form.

TE07.22.02: If automated means are used to transport secret and private keys, the tester shall verify that these keys are entered into and output from the cryptographic module in encrypted form.

AS07.23: (Key entry and output – Levels 3 and 4)
Secret and private keys transported using electronic methods shall be entered into and output from a cryptographic module in encrypted form.

NOTE This assertion is tested as part of AS07.22.

AS07.24: (Key entry and output – Levels 3 and 4)
Secret and private keys transported using *manual transport methods* shall be entered into or output from a cryptographic module either (1) in encrypted form or (2) using split knowledge techniques (i.e., as two or more plaintext cryptographic key components).

Required Vendor Information

VE07.24.01: The vendor documentation requirement is specified under VE11.01.01.

Required Test Procedures

TE07.24.01: Verification of the vendor documentation is performed under TE11.01.01.

TE07.24.02: The tester shall verify that the vendor has provided documentation asserting that secret and private keys transported using manual methods are entered into or output from the cryptographic module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext cryptographic key components).

TE07.24.03: If manual methods are used to transport secret and private keys, the tester shall verify that these keys are entered into the cryptographic module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext cryptographic key components).

TE07.24.04: If manual methods are used to transport secret and private keys, the tester shall verify that these keys are output from the cryptographic module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext cryptographic key components).

AS07.25: (Key entry and output – Levels 3 and 4)
If split knowledge procedures are used, the cryptographic module shall separately authenticate the operator entering or outputting each key component.

Required Vendor Information

VE07.25.01: The vendor documentation shall specify the method the cryptographic module uses to separately authenticate the operator entering or outputting each key component.

Required Test Procedures

TE07.25.01: The tester shall check that authentication is performed for each key component and that the authentication is in accordance with the documented key entry and output procedures.

TE07.25.02: The tester shall enter each key component using split knowledge procedures and verify that each operator entering a key component is authenticated.

TE07.25.03: The tester shall output each key component using split knowledge procedures and verify that each operator outputting a key component is authenticated.

AS07.26: (Key entry and output – Levels 3 and 4)
***{If split knowledge procedures are used,}* plaintext cryptographic key components shall be entered into or output from 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 7.2 *{of ISO/IEC 19790:2006}*).**

NOTE This assertion is not separately tested.

AS07.27: (Key entry and output – Levels 3 and 4)
***{If split knowledge procedures are used,}* at least two key components shall be required to reconstruct the original cryptographic key.**

Required Vendor Information

VE07.27.01: If manually transported secret or private keys are entered or output under split knowledge procedures, the vendor documentation shall specify the number of key components that are required to construct the original key.

Required Test Procedures

TE07.27.01: The tester shall verify the vendor documentation that the entry of manually transported secret or private keys entered under split knowledge procedures requires at least two components to construct the original key.

TE07.27.02: The tester shall verify the vendor documentation that the output of manually transport secret or private keys output under split knowledge procedures does not result in the output of a single key component that can be used to construct the original key.

AS07.28: (Key entry and output – Levels 3 and 4)

***{If split knowledge procedures are used,}* documentation shall verify that if knowledge of *n* key components is required to reconstruct the original key, then knowledge of any *n*-1 key components provides no information about the original key other than the length.**

Required Vendor Information

VE07.28.01: The vendor shall provide documentation that provides rationale stating how knowledge of any *n* –1 key components provides no information about the original key other than the length.

Required Test Procedures

TE07.28.01: The tester shall verify that the vendor provided documentation provides rationale stating if *n* key components are required to construct the original key, then knowledge of any *n* –1 key components provides no information about the original key other than the length.

TE07.28.02: The tester shall verify the accuracy 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.

AS07.29: (Key entry and output – Levels 3 and 4)
***{If split knowledge procedures are used,}* the documentation shall specify the procedures employed by a cryptographic module.**

Required Vendor Information

VE07.29.01: The vendor shall supply documentation specifying the split knowledge procedures employed by the cryptographic module.

Required Test Procedures

TE07.29.01: The tester shall verify that the documentation matches the implementation.

6.8.5 Key storage

AS07.30: (Key storage – Levels 1, 2, 3, and 4)
Cryptographic keys stored within a cryptographic module shall be stored either in plaintext form or encrypted form.

Required Vendor Information

VE07.30.01: The vendor shall supply documentation specifying the storage methods for the keys specified VE11.01.01.

Required Test Procedures

TE07.30.01: The tester shall verify that the documentation describes key storage mechanisms within the cryptographic module.

TE07.30.02: The tester shall verify that the key storage mechanisms are correctly implemented within the cryptographic module.

AS07.31: (Key storage – Levels 1, 2, 3, and 4)
Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorised operators.

NOTE This assertion is tested under AS07.01.

AS07.32: (Key storage – Levels 1, 2, 3, and 4)
A cryptographic module shall associate a cryptographic key (secret, private, or public) stored within the module with the correct entity (e.g., person, group, or process) to which the key is assigned.

Required Vendor Information

VE07.32.01: The vendor documentation on key storage shall describe the mechanisms or procedures used to ensure that each key is associated with the correct entity.

Required Test Procedures

TE07.32.01: The tester shall verify the documentation on key storage that the procedures address how a stored key is associated with the correct entity.

TE07.32.02: The tester shall modify the association of key and entity. The tester shall then attempt to perform cryptographic functions as one of the entities and shall verify that these functions fail.

6.8.6 Key zeroisation

AS07.33: (Key zeroisation – Levels 1, 2, 3, and 4)

A cryptographic module shall provide methods to zeroise all CSPs.

NOTE Zeroisation of encrypted CSPs or CSPs otherwise physically or logically protected within an additional embedded validated module (meeting the requirements of ISO/IEC 19790:2006) is not required.

Required Vendor Information

VE07.33.01: The vendor documentation shall specify the following CSPs zeroisation information:

a. Zeroisation techniques

b. Restrictions when plaintext CSPs can be zeroised

c. Plaintext CSPs that are zeroised

d. Plaintext CSPs that are not zeroised and rationale

e. Rationale explaining how the zeroisation technique is performed in a time that is not sufficient to compromise plaintext CSPs

Required Test Procedures

TE07.33.01: The tester shall verify the vendor documentation that the information specified in VE07.33.01 is included. The tester shall verify the accuracy 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.

TE07.33.02: The tester shall verify which keys are present in the module and initiate the zeroise command. Following the completion of the zeroise command; the tester shall attempt to perform cryptographic operations using each of the plaintext CSPs that were stored in the module. The tester shall verify that each plaintext CSPs cannot be accessed.

TE07.33.03: The tester shall initiate zeroisation and verify the key destruction method is performed in a time that is not sufficient to compromise plaintext CSPs.

TE07.33.04: The tester shall verify that all plaintext CSPs that are not zeroised by the zeroise command are either 1) encrypted using an approved algorithm, or 2) physically or logically protected within an embedded validated cryptographic module (validated as conforming to ISO/IEC 19790:2006). Self-tests

6.9 Self-tests

AS08.01: (Self-tests – Levels 1, 2, 3, and 4)
A cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly.

NOTE This assertion is tested as part of AS08.07.

AS08.02: (Self-tests – Levels 1, 2, 3, and 4)
***Power-up self-tests* shall be performed when the cryptographic module is powered up.**

NOTE This assertion is tested as part of AS08.07.

AS08.03: (Self-tests – Levels 1, 2, 3, and 4)
***Conditional self-tests* shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required).**

NOTE 1 This assertion is tested as part of AS08.07.

NOTE 2 A cryptographic module may perform other power-up or conditional self-tests in addition to the tests specified in ISO/IEC 19790:2006.

AS08.04: (Self-tests – Levels 1, 2, 3, and 4)
If a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator.

Required Vendor Information

VE08.04.01: The vendor shall document all error states associated with each self-test and shall indicate for each error state the expected error indicator.

Required Test Procedures

TE08.04.01: The tester shall verify the vendor documentation, check that it lists every error state that the module enters upon failure of a self-test, and indicates the error indicator associated with each error state. The tester shall compare the list of error states to those defined in the finite state model (see AS04.05) to verify that they agree.

TE08.04.02: By inspecting the vendor documentation that specifies how each self-test handles errors, the tester shall verify that:

1. The module enters an error state upon failing a self-test.
2. The error state is consistent with the documentation and the finite state model.
3. The module outputs an error indicator.
4. The error indicator is consistent with the documented error indicator.

TE08.04.03: The tester shall run self-tests and cause the module to enter every error state. The tester shall compare the observed error indicator with the indicator specified in the vendor documentation. If they are not the same, this test fails.

AS08.05: (Self-tests – Levels 1, 2, 3, and 4)
The cryptographic module shall not perform any cryptographic operations while in an error state.

Required Vendor Information

VE08.05.01: The Vendor documentation requirement is specified under VE02.06.01 for the vendor design requirement. The vendor design shall ensure that cryptographic operations cannot be performed while the module is in the error state.

Required Test Procedures

TE08.05.01: The tester shall verify that the inhibition of output was performed under TE02.06.01 and TE02.06.02. The results of the verification shall indicate that the module inhibits all data output when the module is in an error state.

TE08.05.02: The tester shall verify that the vendor documentation specifies that cryptographic functions are inhibited while the module is in an error state. Cryptographic functions include the following:

1. Encryption
2. Decryption
3. Secure message hashing
4. Digital signature creation and verification
5. Other operations that require the use of cryptography

TE08.05.03: The tester shall enter the module in the error state and verify that any cryptographic operations that the tester attempts to initiate are prevented.

AS08.06: (Self-tests – Levels 1, 2, 3, and 4)
All data output via the data output interface shall be inhibited when an error state exists.

Required Vendor Information

VE08.06.01: The Vendor documentation requirement is specified under VE02.06.01 for the vendor design requirement. The vendor design shall ensure that cryptographic operations cannot be performed while the module is in an error state.

Required Test Procedures

TE08.06.01: The tester shall verify that the inhibition of output was performed under TE02.06.01 and TE02.06.02. The results of the verification shall indicate that the vendor documentation shows that all data output via the data output interface is inhibited whenever the module is in an error state.

TE08.06.02: The tester shall enter the module in an error state and verify that all data output via the data output interface is inhibited when an error state exists.

AS08.07: (Self-tests – Levels 1, 2, 3, and 4)
Documentation shall specify:

- **the self-tests performed by the cryptographic module, including power-up and conditional tests,**
- **the error states that a cryptographic module can enter when a self-test fails, and**
- **the conditions and actions necessary to exit the error states and resume normal operation of a cryptographic module (i.e., this may include maintenance or repair of the module.)**

Required Vendor Information

VE08.07.01: The vendor shall provide a list of all self-tests that the module can perform. This list shall include both power-up tests and conditional tests.

VE08.07.02: For each error condition, the vendor documentation shall provide the condition name, the events that can produce the condition, and the actions necessary to clear the condition and resume normal operation.

Required Test Procedures

TE08.07.01: The tester shall verify the list of self-tests to include the following:

1. Power-up tests
   - Cryptographic algorithm test
   - RBG entropy test
   - Software/firmware integrity test
   - Critical functions test
   - Other self-tests that are performed at power-up and on demand
2. Conditional tests
   - Pair-wise consistency test (if the module generates public and private keys)
   - Manual key entry test

- Continuous RBG test
- Bypass test
- Software/firmware load test
- Other conditional tests

TE08.07.02: The tester shall check that the information provided above is specified for each error condition.

TE08.07.03: The tester shall cause each error condition to occur and shall attempt to clear the error condition. The tester shall verify that actions necessary to clear the error condition are consistent with the vendor documentation. If the tester cannot cause each error condition to occur, the tester shall verify the code listing and or design documentation whether the actions necessary to clear each error condition are consistent with the descriptions in the vendor documentation.

6.9.1 Power-up tests

AS08.08: (Power-up tests – Levels 1, 2, 3, and 4)
Power-up tests shall be performed by a cryptographic module when it is powered up (after being powered off, reset, rebooted, etc.).

NOTE This assertion is tested as part of AS08.09.

AS08.09: (Power-up tests – Levels 1, 2, 3, and 4)
The power-up tests shall be initiated automatically and shall not require operator intervention.

Required Vendor Information

VE08.09.01: The vendor documentation shall require that the running of power-up self-tests not involve any inputs from or actions by the operator.

Required Test Procedures

TE08.09.01: The tester shall verify that the vendor documentation includes the information required under VE08.09.01.

TE08.09.02: The tester shall power-up the module and verify that the module performs the power-up self-tests without requiring any operator intervention.

AS08.10: (Power-up tests – Levels 1, 2, 3, and 4)
When the power-up tests are completed, the results shall be output via the "status output" interface or implicitly.

Required Vendor Information

VE08.10.01: The vendor shall document the indicator that the module outputs upon successful completion of the power-up self-tests.

Required Test Procedures

TE08.10.01: The tester shall verify that the vendor documentation specifies an indicator that is output from the status output interface upon successful completion of the power-up self-tests.

TE08.10.02: The tester shall power-up the module and shall monitor the status output interface. The expected indicator from the status output interface is required to be consistent with the documented indicator.

AS08.11: (Power-up tests – Levels 1, 2, 3, and 4)
All data output via the output interface shall be inhibited when the tests are performed.

NOTE This assertion is tested as part of AS02.06.

AS08.12: (Power-up tests – Levels 1, 2, 3, and 4)

In addition to performing the power-up tests *{AS08.08 to AS08.11}* when powered up, the module shall permit operators to initiate the tests on demand for periodic testing of the module.

Required Vendor Information

VE08.12.01: The vendor shall describe the procedure by which an operator can initiate the power-up self-tests on demand. All of the power-up self-tests have to be included.

Required Test Procedures

TE08.12.01: The tester shall verify in the vendor documentation that initiation of power-up self-tests on demand is specified for all of the power-up self-tests.

TE08.12.02: The tester shall initiate the power-up on demand self-tests to verify that the initiation of the power-up self-tests on demand is consistent with the vendor documentation.

AS08.13: (Power-up tests – Levels 1, 2, 3, and 4)
The module shall perform the following power-up tests *{AS08.14 to AS08.25}*.

Required Vendor Information

VE08.13.01: Vendor documentation requirement is specified under VE08.07.01 for the vendor requirement.

Required Test Procedures

TE08.13.01: Verification of the documented list of power-up self-tests was performed under TE08.07.01.

TE08.13.02: Verification that the module performs the self-tests as documented is done under requirements for AS08.14 through AS08.26.

Cryptographic algorithm test

AS08.14: (Algorithm test – Levels 1, 2, 3, and 4)
A cryptographic algorithm test using a known answer shall be conducted for all cryptographic functions (e.g., encryption, decryption, authentication) of each approved cryptographic algorithm implemented by a cryptographic module.

NOTE A known-answer test involves operating the cryptographic algorithm on data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer).

Required Vendor Information

VE08.14.01: Vendor documentation requirement is specified under VE08.07.01 for the vendor requirement.

Required Test Procedures

TE08.14.01: By inspecting the vendor documentation, the tester shall verify that a known answer test is associated with all cryptographic functions of each approved cryptographic algorithm implemented by the cryptographic module as indicated in AS01.12.

TE08.14.02: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

AS08.15: (Algorithm test – Levels 1, 2, 3, and 4)
If the calculated output *{of AS08.14}* does not equal the known answer, the known-answer test shall fail.

Required Vendor Information

VE08.15.01: The vendor documentation shall specify the method used to compare the calculated output with the known answer.

VE08.15.02: The documentation shall show the transition into an error state and output of an error indicator when the two outputs are not equal.

Required Test Procedures

TE08.15.01: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

TE08.15.02: This is tested under TE08.04.01, TE08.04.02, and TE08.04.03.

AS08.16: (Algorithm test – Levels 1, 2, 3, and 4)
Cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the Digital Signature Algorithm) shall be tested using a known-answer test or shall be tested using a pair-wise consistency test (specified below *{see AS08.28 and subclause 7.8.2.1 of ISO/IEC 19790:2006}*).

Required Vendor Information

VE08.16.01: Vendor documentation requirement is specified under VE08.07.01 for the vendor requirement.

VE08.16.02: The vendor documentation shall specify the test(s) that is implemented.

Required Test Procedures

TE08.16.01: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

TE08.16.02: By inspecting the vendor documentation, the tester shall verify if either a known-answer test or a pair-wise consistency test is associated with the cryptographic function.

TE08.16.03: Pair-wise consistency is tested in AS08.28.

AS08.17: (Algorithm test – Levels 1, 2, 3, and 4)

Message digest algorithms shall have an independent known-answer test or the known-answer test shall be included with the associated cryptographic algorithm test (e.g., the Digital Signature Standard).

Required Vendor Information

VE08.17.01: Vendor documentation requirement is specified under VE08.07.01 for the vendor requirement.

VE08.17.02: The vendor documentation shall specify the test(s) which is implemented.

Required Test Procedures

TE08.17.01: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

TE08.17.02: The tester shall verify whether the module implements a message digest algorithm. If so, the tester shall verify that the vendor documentation specifies whether the message digest algorithm has its own known answer test or whether it is included in the known answer test of another algorithm.

TE08.17.03: By checking the code listing and/or design documentation, the tester shall verify that the module uses either a separate known answer test or the known answer test of an algorithm in order to test a message digest algorithm.

AS08.18: (Algorithm test – Levels 1, 2, 3, and 4)
If a cryptographic module includes two independent implementations of the same cryptographic algorithm, then the known-answer test may be omitted but, shall be replaced having the outputs of two implementations shall be continuously compared.

Required Vendor Information

VE08.18.01: Vendor documentation requirement is specified under VE08.07.01 for the vendor requirement.

VE08.18.02: The vendor shall specify whether a known answer test or the comparison of the output of two independent cryptographic algorithm implementations (compared answer test) is used to test the module's cryptographic algorithm. If the compared answer test is used, the vendor shall document this fact.

Required Test Procedures

TE08.18.01: The tester shall verify from the vendor documentation whether a known answer test or a compared answer test is used to test the module's cryptographic algorithm. If the compared answer test is used, the tester shall verify whether the documentation of the compared answer test includes:

1. Use of two independent cryptographic algorithm implementations
2. Continual comparison of the outputs of the algorithm implementation
3. Transition into an error state and output of an error indicator when the two outputs are not equal

TE08.18.02: By checking the code and/or design documentation, the tester shall verify that the module implements the documented steps for performing a compared answer test.

AS08.19: (Algorithm test – Levels 1, 2, 3, and 4)
If the outputs of two implementations are not equal, the cryptographic algorithm test shall fail.

NOTE This assertion is tested as part of AS08.18.

RBG entropy test

AS08.20: (RGB entropy test – Levels 1, 2, 3, and 4)
If a cryptographic module employs approved RBGs in an approved mode of operation, the module shall perform the cryptographic health tests on the RBG entropy sources found in ISO/IEC 18031.

Required Vendor Information

VE08.20.01: The vendor shall provide documentation that states the module performs the cryptographic health tests on the RBG entropy sources are as specified in ISO/IEC 18031.

Required Vendor Information

TE08.20.01: By checking the code and/or design documentation, the tester shall verify that the module implements the cryptographic health tests on the RBG entropy sources.

TE08.20.02: The tester shall force an error such that the entropy test shall fail. Validation of whether the module enters the error state and outputs an error indicator upon failure of the entropy test shall be verified. If the validation is not verified, this test fails. If it is not possible for the tester to force an error then the vendor shall provide a rationale to the tester why this test cannot be performed.