INTERNATIONAL STANDARD

ISO/IEC 24759

Second edition
2014-02-01

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 24759:2014(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*.

This second edition cancels and replaces the first edition (ISO/IEC 24759:2008), which has been technically revised.

Information technology — Security techniques — Test requirements for cryptographic modules

1 Scope

This International Standard specifies the methods to be used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790:2012. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories.

This International Standard also specifies the requirements for information that vendors provide to testing laboratories as supporting evidence to demonstrate their cryptographic modules' conformity to the requirements specified in ISO/IEC 19790:2012.

Vendors can use this International Standard as guidance in trying to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2012 before they apply to the testing laboratory for testing.

2 Normative references

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

ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19790:2012 apply.

4 Symbols and abbreviated terms

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

5 Document organization

5.1 General

Clause 6 of this document specifies the methods that shall be used by testing laboratories and the requirements for information that vendors shall provide to testing laboratories. Clause 6, besides a general subclause 6.1, includes eleven subclauses corresponding to the eleven areas of security requirements and six subclauses corresponding to the six Annexes A to F of ISO/IEC 19790:2012.

5.2 Assertions and security requirements

Within each subclause, the corresponding security requirements from ISO/IEC 19790:2012 are divided into a set of assertions (i.e., statements that have to be true for the module to satisfy the requirement of a given area at a given level). All of the assertions are direct quotations from ISO/IEC 19790:2012.

The assertions are denoted by the form

AS<requirement_number>.<assertion_sequence_number>

where "requirement_number" is the number of the corresponding area specified in ISO/IEC 19790:2012 (i.e., one through twelve and A through F), and "sequence_number" is a sequential identifier for assertions within a subclause. After the statement of each assertion, the security levels to which the assertion applies (i.e., levels 1 through 4) are listed in parentheses.

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

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

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

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

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

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

A validation authority may modify, add or delete VEs and/or TEs in this international standard.

5.3 Assertions with cross references

For clarity in some assertions, cross references to ISO/IEC 19790:2012 or other assertions numbers have been put between curly brackets "***{***" and "***}***". Those cross references are written in italics.

6 Security requirements

6.1 General

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

This clause specifies the security requirements that shall be satisfied by the cryptographic module's compliance to this International Standard.

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

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

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

NOTE 1 The tests can be performed in one or more of the following manners:

a) Tester performs tests at the tester's facility

b) Tester performs tests at the vendor's facility

c) Tester supervises vendor performing tests at the vendor's facility

1) Rationale is included that explains why tester could not perform the tests

2) Tester develops the required test plan and required tests

3) Tester directly observes the tests being performed

An assertion fails if any of its subsequent tests fails.

NOTE 2 This subclause states general requirements to meet the assertions of the other subclauses in clause 6. This subclause sets no assertion of itself and is not separately tested.

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

The cryptographic module shall be independently rated in each area.

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

AS01.04: (Specification – Levels 1, 2, 3, and 4)

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

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

6.2 Cryptographic module specification

6.2.1 Cryptographic module specification general requirements

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

A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof, that at a minimum, implements a defined cryptographic service employing an approved cryptographic algorithm, security function or process and contained within a defined cryptographic boundary.

NOTE This assertion is not separately tested.

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

The documentation requirements specified in *{ISO/IEC 19790:2012 Annex}* A.2.2 shall be provided.

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

6.2.2 Types of cryptographic modules

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

A cryptographic module shall be defined as one of the following module types:

— ***Hardware module* is a module whose cryptographic boundary is specified at a hardware perimeter. Firmware and/or software, which may also include an operating system, may be included within this hardware cryptographic boundary.**

— ***Software module* is a module whose cryptographic boundary delimits the software exclusive component(s) (may be one or multiple software components) that execute(s) in a modifiable operational environment. The computing platform and operating system of the operational environment which the software executes in are external to the defined software module boundary.**

— ***Firmware module*** **is a module whose cryptographic boundary delimits the firmware exclusive component(s) that execute(s) in a limited or non-modifiable operational environment. The computing platform and operating system of the operational environment which the firmware executes in are external to the defined firmware module boundary but explicitly bound to the firmware module.**

— ***Hybrid Software module*** **is a module whose cryptographic boundary delimits the composite of a software component and a disjoint hardware component (i.e. the software component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment which the software executes in are external to the defined hybrid software module boundary.**

— ***Hybrid Firmware module*** **is a module whose cryptographic boundary delimits the composite of a firmware component and a disjoint hardware component (i.e. the firmware component is not contained within the hardware module boundary). The computing platform and operating system of the operational environment which the firmware executes in are external to the defined hybrid firmware module boundary but explicitly bound to the hybrid firmware module.**

Required Vendor Information

VE02.03.01: The vendor shall provide a description of the cryptographic module describing the type of cryptographic module. It will explain the rationale of the module type selection.

VE02.03.02: The vendor shall provide a specification of the cryptographic module identifying all hardware, software and/or firmware components of the cryptographic module.

Required Test Procedures

TE02.03.01: The tester shall verify that the vendor provided documentation identifies one of the module types listed in AS02.03.

TE02.03.02: The tester shall verify from the vendor provided specification documentation, by identifying all hardware, software and/or firmware components (AS02.15 through AS02.18), that the cryptographic module is consistent with the type of the cryptographic module.

AS02.04: (Specification – Levels 1, 2, 3, and 4)

For hardware and firmware modules, the physical security and non-invasive security requirements found in *{ISO/IEC 19790:2012 subclause}* 7.7 and 7.8 shall apply.

NOTE This assertion is not tested separately.

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

For hybrid modules, the software and firmware component(s) shall meet all applicable requirements of *{ISO/IEC 19790:2012 subclause}* 7.5 and 7.6.

NOTE This assertion is not tested separately.

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

{For hybrid modules} **The hardware component(s) shall meet all applicable requirements of *{ISO/IEC 19790:2012 subclause}* 7.7 and 7.8.**

NOTE This assertion is not tested separately.

6.2.3 Cryptographic boundary

6.2.3.1 Cryptographic boundary general requirements

AS02.07: (Specification – Levels 1, 2, 3, and 4)

The cryptographic boundary shall consist of an explicitly defined perimeter (i.e. set of hardware, software or firmware components) that establishes the boundary of all components of the cryptographic module.

Required Vendor Information

VE02.07.01: The vendor documentation shall specify all components within the cryptographic boundary.

Required Test Procedures

TE02.07.01: The tester shall verify by inspection and from the vendor documentation that all the components specified in AS02.15 through AS02.18 are within the cryptographic boundary.

TE02.07.02: The tester shall verify by inspection and from the vendor documentation that there are no unidentified components which are not specified in AS02.15 through AS02.18 within the cryptographic boundary.

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

The requirements of this International Standard shall apply to all algorithms, security functions, processes and components within the module's cryptographic boundary.

NOTE This assertion is not tested separately.

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

The cryptographic boundary shall, at a minimum, encompass all security relevant algorithms, security functions, processes and components of a cryptographic module (i.e., security relevant within the scope of this International Standard).

Required Vendor Information

VE02.09.01: The vendor shall provide a list of all the security relevant algorithms, security functions, processes and components within the cryptographic boundary.

Required Test Procedures

TE02.09.01: The tester shall verify that the vendor provided documentation clearly identifies and lists all the security relevant algorithms, security functions, processes and components of the module within the cryptographic boundary.

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

Non-security relevant algorithms, security functions, processes or components which are used in an approved mode of operation shall be implemented in a manner to not interfere or compromise the approved operation of the cryptographic module.

Required Vendor Information

VE02.10.01: The vendor provided documentation shall list the non-security relevant functions used in an approved mode of operation and justify that they are not interfering with the approved mode of operation of the module.

Required Test Procedures

TE02.10.01: The tester shall verify through documentation review and inspection of the module that the non-security relevant functions are not interfering or compromising the approved mode of operation of the module.

TE02.10.02: The tester shall verify the correctness of any rationale for not interfering nor compromising provided by the vendor. The burden of proof is on the vendor; if there is any uncertainty or ambiguity, the tester shall require the vendor to produce additional information as needed.

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

The defined name of a cryptographic module shall be representative of the composition of the components within the cryptographic boundary and not representative of a larger composition or product.

Required Vendor Information

VE02.11.01: The vendor shall provide the defined name of the module.

Required Test Procedures

TE02.11.01: The tester shall verify that the vendor provided module name is consistent with the composition of the components within the cryptographic boundary.

TE02.11.02: The tester shall verify that the module name does not represent a compostion of components or functions that are not consistent with the composition of the components within the cryptographic boundary.

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

The cryptographic module shall have, at minimum, specific versioning information representing the distinct individual hardware, software and/or firmware components.

Required Vendor Information

VE02.12.01: The vendor shall provide the versioning information of the modules distinct individual hardware, software and/or firmware components.

Required Test Procedures

TE02.12.01: The tester shall verify the versionig information represents the modules distinct individual hardware, software and/or firmware components.

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

The excluded hardware, software or firmware components shall be implemented in a manner to not interfere or compromise the approved secure operation of the cryptographic module.

Required Vendor Information

VE02.13.01: The vendor shall describe the excluded components of the module which are not within the cryptographic module and justify that these components will not interfere with the approved mode of operation of the module.

Required Test Procedures

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

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

The excluded hardware, software or firmware shall be specified *{ ISO/IEC 19790:2012}* (Annex A).

Required Vendor Information

VE02.14.01: All components that are to be excluded from the security requirements shall be explicitly listed in the vendor documentation.

VE02.14.02: The vendor documentation shall provide the rationale for excluding each of the components listed in response to requirement VE02.13.01. The vendor shall show that each component, even if malfunctioning or misused, cannot cause a compromise.

Required Test Procedures

TE02.14.01: The tester shall verify whether the vendor indicates that any components of the module are to be excluded from the requirements of ISO/IEC 19790:2012.

TE02.14.02: If the vendor has indicated that certain components of the module are to be excluded from the requirements of ISO/IEC 19790:2012, 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 , plaintext data, or other information that if misused could lead to a compromise. Rationale that may be acceptable, if adequately supported by documentation, includes:

a) The component does not process SSPs, plaintext data, or other information that if misused could lead to a compromise

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

c) 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

TE02.14.03: 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.

6.2.3.2 Definitions of cryptographic boundary

AS02.15: (Specification – Levels 1, 2, 3, and 4)

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

- **The set of hardware components which may include:**
  - **physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between components,**
  - **active electrical components such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc.**
  - **physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces,**
  - **firmware, which may include an operating system,**
  - **other components types not listed above.**

Required Vendor Information

VE02.15.01: All hardware components of the cryptographic module shall be identified in the vendor documentation. Components to be listed shall include all of the following:

a) Physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between components.

   1) circuit boards, substrates and mounting surfaces.

b) Active electrical components such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc.

   1) processors, including microprocessors, digital signal processors, custom processors, microcontrollers, or any other types of processors (identify manufactuer and type),

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

3) random-access memory (RAM) or other integrated circuits for temporary data storage,

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

5) fully custom, application-specific, integrated circuits, including any custom cryptographic integrated circuits,

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

7) other active electronic circuit elements (passive circuit elements such as pull up/pull down resistors or bypass capacitors do not need to be included if they do not provide security relevant function as part of the cryptographic module).

c) Physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces,

1) physical structures and enclosures, including any removable access doors or covers,

2) potting or encapsulation materials,

3) boundary connectors,

4) connectors between major independent sub assemblies within the module.

d) Firmware, which may include an operating system,

1) Executable code:

i) Non-modifiable

ii) Modifiable

e) Other components types not listed above

1) cooling or heating arrangements, such as conduction plates, cooling airflow, heat exchanger, cooling fins, fans, heaters, or other arrangements for removing or adding heat.

VE02.15.02: The vendor documentation shall indicate the internal layout and assembly methods (e.g. fasteners and fittings) of the module, including drawings that are at least approximately to scale.

VE02.15.03: The vendor documentation shall describe the primary physical parameters of the module, including descriptions of the enclosure, access points, circuit boards, location of power supply, interconnection wiring runs, cooling arrangements, and any other significant parameters.

VE02.15.04: The vendor documentation shall include a block diagram which represents the module's boundary and relationship of the hardware components.

Required Test Procedures

TE02.15.01: The tester shall identify all hardware components of the cryptographic module. Components to be listed shall include all of the following:

a) Physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between components.

    1) circuit boards, substrates and mounting surfaces.

b) Active electrical components such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc.

    1) processors, including microprocessors, digital signal processors, custom processors, microcontrollers, or any other types of processors (identify manufactuer and type),

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

    3) random-access memory (RAM) or other integrated circuits for temporary data storage,

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

    5) fully custom, application-specific, integrated circuits, including any custom cryptographic integrated circuits,

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

    7) other active electronic circuit elements (passive circuit elements such as pull up/pull down resistors or bypass capacitors do not need to be included if they do not provide security relevant function as part of the cryptographic module).

c) Physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces,

    1) physical structures and enclosures, including any removable access doors or covers,

    2) potting or encapsulation materials,

    3) boundary connectors,

    4) connectors between major independent sub assemblies within the module.

d) Firmware, which may include an operating system,

    1) Executable code:

        i) Non-modifiable

        ii) Modifiable

e) Other components types not listed above

    1) cooling or heating arrangements, such as conduction plates, cooling airflow, heat exchanger, cooling fins, fans, heaters, or other arrangements for removing or adding heat.

TE02.15.02: The tester shall verify that the components list is consistent with information provided for other assertions of this subclause, as defined below:

a) The specification of the cryptographic boundary under assertion AS02.07. Verify that all components inside the cryptographic boundary are included in the components list and vice versa. Also verify

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

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

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

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

TE02.15.04: The tester shall verify that the cryptographic boundary encompasses all components that are identified in the block diagram under assertion ASA.01 in this subclause as inputting, outputting, or processing SSPs, plaintext data, or other information that if misused could lead to a compromise.

TE02.15.05: As a partial exception to the above requirements, the vendor is allowed to exclude certain components from the requirements of ISO/IEC 19790:2012 after satisfying the requirements under assertion AS02.14 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.

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

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

TE02.15.08: The tester shall verify that the vendor's documentation describes the primary physical parameters of the module. This description has to include at least the following:

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

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

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

d) Interconnection wiring runs: routing and terminals

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

f) Other component types not listed above

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

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

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

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

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

Required Vendor Information

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

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

b) Other security relevant component types not listed above.

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

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

Required Test Procedures

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

TE02.16.02: The tester shall verify that the components list includes all occurrences of the following types of components, excluding only component types that are not used in the module:

a) Software components.

b) Other component types not listed above.

TE02.16.03: The tester shall verify that the components list is consistent with information provided for other assertions of this subclause, as defined below:

a) The specification of the cryptographic boundary under assertion AS02.07. Verify that all components inside the cryptographic boundary are included in the components list and vice versa. Also verify that any components outside the cryptographic boundary are not listed as components of the cryptographic module.

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

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

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

TE02.16.04: As a partial exception to the above requirements, the vendor is allowed to exclude certain components from the requirements of ISO/IEC 19790:2012 after satisfying the requirements under assertions AS02.13 and AS02.14 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.

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

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

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

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

— **The instantiation of the cryptographic module saved in memory and executed by the processor.**

Required Vendor Information

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

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

b) Other security relevant component types not listed above.

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

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

Required Test Procedures

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

TE02.17.02: The tester shall verify that the components list includes all occurrences of the following types of components, excluding only component types that are not used in the module:

a) Firmware components.

b) Other component types not listed above.

TE02.17.03: The tester shall verify that the components list is consistent with information provided for other assertions of this subclause, as defined below:

a) The specification of the cryptographic boundary under assertion AS02.07. Verify that all components inside the cryptographic boundary are included in the components list and vice versa. Also verify that any components outside the cryptographic boundary are not listed as components of the cryptographic module.

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

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

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

TE02.17.04: As a partial exception to the above requirements, the vendor is allowed to exclude certain components from the requirements of ISO/IEC 19790:2012 after satisfying the requirements under assertions AS02.13 and AS02.14 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.

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

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

The cryptographic boundary of a hybrid cryptographic module shall:

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

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

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

Required Vendor Information

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

— Hybrid Software Module components listed shall include the requirements in VE02.15.01 through VE02.15.04 and VE02.16.01 through VE02.16.03.

— Hybrid Firmware Module components listed shall include the requirements in VE02.15.01 through VE02.15.04 and VE02.17.01 through VE02.17.03.

Required Test Procedures

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

— Hybrid Software Module components listed shall include the requirements in TE02.15.01 through TE02.15.09 and TE02.16.01 through TE02.16.05.

— Hybrid Firmware Module components listed shall include the requirements in TE02.15.01 through TE02.15.09 and TE02.17.01 through TE02.17.05.

6.2.4 Modes of operations

6.2.4.1 Modes of operation general requirements

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

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

Required Vendor Information

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

VE02.21.02: The vendor documentation shall provide a rationale for why utilised non-approved cryptographic algorithms, security functions or processes are considered not security relevant to the approved processes operation.

Required Test Procedures

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

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

6.2.4.2 Normal operation

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

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

NOTE This assertion is tested under ASB.01.

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

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

Required Vendor Information

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

Required Test Procedures

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

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

6.2.4.3 Degraded operation

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

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

NOTE This assertion is not separately tested.

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

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

Required Vendor Information

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

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

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

b) available algorithms, security functions, services or processes

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

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

e) techniques to isolate mechanisms, functions or components

f) status information provided in the degraded operation

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

Required Test Procedures

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

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

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

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

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

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

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

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

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

The mechanism or function that failed shall be isolated.

Required Vendor Information

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

Required Test Procedures

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

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

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

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

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

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

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

Required Vendor Information

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

Required Test Procedures

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

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

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

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

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

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

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

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

6.3 Cryptographic module interfaces

6.3.1 Cryptographic module interfaces general requirements

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

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

Required Vendor Information

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

a) Physical ports and their pin assignments

b) Physical covers, doors or openings

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

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

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

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

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

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

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

Required Test Procedures

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

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

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

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

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

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

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

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

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

TE03.01.03: The tester shall verify that for each physical or logical input to the cryptographic module, or physical and logical output from the module, the vendor documentation specifies the logical interface to which the physical input or output belongs, and the physical entry/exit port. The specifications provided shall be consistent with the specifications of the cryptographic module components provided under

6.2 and 6.11 of this International Standard, and the specifications of the logical interfaces provided in assertions AS03.04 to AS03.11 of this subclause.

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

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

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

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

Required Vendor Information

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

Required Test Procedures

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

6.3.2 Types of interfaces

6.3.3 Definition of interfaces

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

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

— ***Data input interface***

— ***Data output interface***

— ***Control input interface***

— ***Control output interface***

— ***Status output interface***

Required Vendor Information

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

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

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

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

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

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

Required Test Procedures

TE03.04.01: The tester shall verify that the vendor documentation specifies that the five logical interfaces as listed in VE03.04.01 have been designed within the cryptographic module. If so, verification that the logical interfaces within the cryptographic module function as specified shall be performed under assertions AS03.04 to AS03.11 in this subclause.

Data input interface

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

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

Required Vendor Information

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

a) Plaintext data

b) Ciphertext or signed data

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

d) Authentication data (plaintext or encrypted)

e) Status information from external sources

f) Any other input data

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

Required Test Procedures

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

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

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

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

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

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

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

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

Data output interface

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

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

Required Vendor Information

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

a) Plaintext data

b) Ciphertext data and digital signatures

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

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

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

Required Test Procedures

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

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

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

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

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

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

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

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

Required Vendor Information

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

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

Required Test Procedures

TE03.07.01: The tester shall verify that the vendor documentation specifies that all data output via the data output interface is inhibited whenever the cryptographic module is performing manual key entry, pre-operational self-tests, software/firmware loading and zeroisation; or when the cryptographic module is in an error state. The tester shall verify from the vendor documentation that when performing manual key entry, pre-operational self-tests, software/firmware loading and zeroisation; or when the cryptographic module is in an error state, all data output via the data output interface is inhibited, until error recovery occurs.

TE03.07.02: The tester shall cause the cryptographic module to enter each specified state while performing manual key entry, pre-operational self-tests, software/firmware loading and zeroisation;

or when the cryptographic module is in an error state and verify that all data output via the data output interface is inhibited.

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

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

TE03.07.04: The tester shall cause 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 are output 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.

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

Control input interface

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

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

Required Vendor Information

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

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

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

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

d) Any other input control data

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

Required Test Procedures

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

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

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

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

d) Any other input control data

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

Control output interface

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

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

Required Vendor Information

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

Required Test Procedures

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

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

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

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

Required Vendor Information

VE03.10.01: The vendor documentation shall specify how the cryptographic module ensures that all control output via the control output interface is inhibited whenever the module is in an error state (error states are covered in 7.11 of ISO/IEC 19790:2012. 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.

VE03.10.02: The vendor documentation shall specify how the design of the cryptographic module ensures that all control output via the control output interface is inhibited whenever the module is in a self-test condition (self-tests are covered in 7.10 of ISO/IEC 19790:2012). 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

TE03.10.01: The tester shall verify that the vendor documentation specifies that all control output via the control output interface is inhibited whenever the cryptographic module is in an error state. The tester shall verify from the vendor documentation that once an error condition is detected and the error state is entered, all control output via the control output interface is inhibited, until error recovery occurs. 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 AS11.08.

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

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

TE03.10.03: The tester shall verify that the vendor documentation specifies that all control output via the control output interface is inhibited whenever the cryptographic module is in a self-test condition. The tester shall verify from the vendor documentation that once self-tests are being performed, all control output via the control output interface is inhibited, until the self-tests are completed. 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 AS10.07.

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

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

Status output interface

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

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

NOTE Status output will be either implicit or explicit.

Required Vendor Information

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

a) Status information output logically via an API

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

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

d) Any other output status information

VE03.11.02: If applicable, the vendor documentation shall specify any external output devices to be used with the cryptographic module for the output of status information, signals, logical indicators, and

physical indicators via the status output interface, such as smart cards, tokens, displays, and/or other storage devices.

Required Test Procedures

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

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

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

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

d) Any other output status information

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

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

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

NOTE This assertion is not tested separately.

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

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

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

Required Vendor Information

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

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

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

Required Test Procedures

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

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

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

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

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

Required Vendor Information

VE03.15.01: The vendor documentation shall specify the physical and logical paths used by all major categories of input data entering the cryptographic module via the data input interface and the applicable physical ports. The documentation shall include a specification of the applicable paths (e.g. by highlighted or annotated copies of the schematics, block diagrams, or other information provided under AS02.07 and AS02.15 through AS02.18). All input data entering the cryptographic module via the

data input interface shall only use the specified paths while being processed or stored by each physical or logical sub-section of the module.

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

Required Test Procedures

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

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

6.3.4 Trusted channel

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

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

Required Vendor Information

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

Required Test Procedures

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

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

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

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

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

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

Required Vendor Information

VE03.19.01: The vendor documentation shall 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 channel.

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

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

Required Test Procedures

TE03.19.01: The tester shall verify 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 channel.

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

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

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

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

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

Required Vendor Information

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

Required Test Procedures

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

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

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

Required Vendor Information

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

Required Test Procedures

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

AS03.22: (Trusted channel – Level 4)

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

Required Vendor Information

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

Required Test Procedures

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

6.4 Roles, services, and authentication

6.4.1 Roles, services, and authentication general requirements

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

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

NOTE This assertion is tested under AS04.11.

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

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

Required Vendor Information

VE04.02.01: 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

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

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

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

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

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

Required Vendor Information

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

Required Test Procedures

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

6.4.2 Roles

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

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

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

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

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

Required Vendor Information

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

Required Test Procedures

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

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

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

Required Vendor Information

VE04.06.01: If in the documentation required, the vendor includes one user role, this role shall be specified by name and allowed services.

Required Test Procedures

TE04.06.01: The tester shall verify the vendor documentation that at least one user role is defined. The tester shall verify that user role is specified by name and allowed services as specified above.

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

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

Required Vendor Information

VE04.07.01: The vendor documentation shall specify how the module's unprotected SSPs, as defined in 3.110 of ISO/IEC 19790:2012, are actively zeroised when the maintenance role is entered or exited.

Required Test Procedures

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

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

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

6.4.3 Services

6.4.3.1 Services general requirements

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

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

NOTE This assertion is not separately tested.

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

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

NOTE This assertion is not separately tested.

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

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

NOTE This assertion is not separately tested.

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

Each service input shall result in a service output.

Required Test Procedures

TE04.11.01: The tester shall check the vendor documentation and verify that the purpose and function of each service is described. The tester shall also check that the following information is specified for

each service: service inputs, corresponding service outputs, and the authorized role or roles in which the service can be performed.

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

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

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

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

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

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

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

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

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

A cryptographic module shall provide the following services to operators.

NOTE This assertion is not separately tested.

Show module's versioning information

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

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

Required Vendor Information

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

VE04.13.02: The vendor shall supply a validation record of the cryptographic module with name and versioning data.

Required Test Procedures

TE04.13.01: The tester shall verify that the name and versioning information are consistent with specification and that the vendor is providing delivery information of the cryptographic module including sufficient data to unambiguously identify the module version.

TE04.13.02: The tester shall verify the validation record of the module.

Show Status

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

The cryptographic module shall output current status.

Required Vendor Information

VE04.14.01: The vendor documentation shall describe the output of the current status of the module and the initiation and running of user callable self-tests.

Required Test Procedures

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

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

Perform self-tests

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

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

Required Vendor Information

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

Required Test Procedures

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

Perform approved security functions

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

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

NOTE This assertion is not separately tested.

Perform zeroisation

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

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

NOTE This assertion is not separately tested.

6.4.3.2 Bypass capability

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

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

NOTE This assertion is not separately tested.

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

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

Required Vendor Information

VE04.19.01: If the module implements a bypass capability, the vendor documentation shall describe the bypass service as specified in AS04.19.

VE04.19.02: The finite state model and other the vendor documentation shall indicate, for all transitions into an exclusive or alternating bypass state, two independent internal actions that are required to transition into each bypass state.

Required Test Procedures

TE04.19.01: The tester shall verify whether the bypass capability is implemented by the module. The tester shall verify the vendor documentation to verify that the bypass capability is allocated to at least one authorised role.

TE04.19.02: The tester shall verify the finite state model and other the vendor documentation whether each transition into an exclusive or alternating bypass state shows two independent internal actions that have to occur in order for the cryptographic module to transition into either exclusive or alternating bypass state.

TE04.19.03: The tester shall attempt to transition to each bypass state from each state that shows such a transition, and verify that it takes two internal actions to accomplish each such transition.

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

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

Required Vendor Information

VE04.20.01: If the module implements a bypass capability, the vendor documentation shall describe the bypass service as specified in AS04.19.

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

Required Test Procedures

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

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

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

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

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

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

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

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

c) ***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

VE04.22.01: The vendor documentation for the “Show Status” service shall indicate bypass status.

Required Test Procedures

TE04.22.01: The tester shall review the vendor documentation for the “Show Status” service and verify the bypass service indication.

TE04.22.02: The tester shall transition to each bypass state and verify that the “Show Status” indicates the applicable bypass status.

6.4.3.3 Self-Initiated cryptographic output cabability

AS04.23: (Self-initiated cryptographic output capability – Levels 1, 2, 3, and 4)

The self-initiated cryptographic output capability shall be configured by the Crypto Officer and this configuration may be preserved over resetting, rebooting, or power cycling of the module.

Required Vendor Information

VE04.23.01: The vendor shall provide description of the self-initiated cryptographic output capability.

Required Test Procedures

TE04.23.01: The tester shall verify that the self-initiated cryptographic output capability must be configured by the Crypto Officer.

AS04.24: (Self-initiated cryptographic output capability – Levels 1, 2, 3, and 4)

If a cryptographic module implements a self-initiated cryptographic output capability, then **two independent internal actions shall be required to activate the capability to prevent the inadvertent output due to a single error.**

NOTE This assertion is not separately tested. Tested as part of AS04.25.

AS04.25: (Self-initiated cryptographic output capability – Levels 1, 2, 3, and 4)

If a cryptographic module implements a self-initiated cryptographic output capability, then **the two independent internal actions shall modify software and/or hardware behaviour that is dedicated to mediate the capability (e.g. two different software or hardware flags are set, one of which may be user-initiated).**

Required Vendor Information

VE04.25.01: The vendor shall define a set of two internal actions to be independently done in order to activate the self-initiated cryptographic output capability.

VE04.25.02: The vendor provided documentation shall specify how the two independent internal actions modify software and/or hardware behaviour that is dedicated to mediate the self-initiated cryptographic output capability.

VE04.25.03: The vendor provided documentation shall specify how the two independent internal actions protect against the inadvertent output due to a single error.

Required Test Procedures

TE04.25.01: The tester shall determine whether the cryptographic module implements a self-initiated cryptographic output capability. The tester shall verify that vendor documentation specifies the two independent internal actions performed by the cryptographic module before activating the self-initiated cryptographic output capability. The tester shall also verify that vendor documentation specifies how the two independent internal actions protect against the inadvertent output due to a single error.

TE04.25.02: The tester shall activate the self-initiated cryptographic output capability, and verify that the two independent internal actions function as specified. If any software or firmware components are executed in the process of activation, the tester shall examine the applicable source code to ensure that the software or firmware components support the requirement for two independent internal actions before activating the self-initiated cryptographic output capability.

TE04.25.03: The tester shall verify that an status indicator is provided to indicate when the self-initiated cryptographic output capability is activated.

AS04.26: (Self-initiated cryptographic output capability– Levels 1, 2, 3, and 4)

If a cryptographic module implements a self-initiated cryptographic output capability, then **the module shall show status to indicate whether the self-initiated cryptographic output capability is activated.**

NOTE This assertion is not separately tested. Tested as part of AS04.25.

6.4.3.4 Software/Firmware loading

AS04.27: (Software/Firmware loading – Levels 1, 2, 3, and 4)

If a cryptographic module has the capability of loading software or firmware from an external source, then the following requirements shall apply.

NOTE This assertion is not separately tested. Tested as part of AS04.28.

AS04.28: (Software/Firmware loading – Levels 1, 2, 3, and 4)

The loaded software or firmware shall be validated by a validation authority prior to loading to maintain validation.

Required Vendor Information

VE04.28.01: The vendor shall provide a certificate of validation by a validation authority. This certificate shall unambiguously identity the software or firmware loaded in the cryptographic module.

Required Test Procedures

TE04.28.01: The tester shall check that the software or firmware version is the one who claims to be. This identification shall be consistent with the one verified in 7.2.3.1 of ISO/IEC 19790:2012.

AS04.29: (Software/Firmware loading – Levels 1, 2, 3, and 4)

All data output via the data output interface shall be inhibited until the software/firmware loading and load test has completed successfully.

Required Vendor Information

VE04.29.01: The vendor shall describe the process used to inhibit data output during loading processes and load test.

Required Test Procedures

TE04.29.01: The tester shall verify that the data output is inhibited during software or firmware loading.

AS04.30: (Software/Firmware loading – Levels 1, 2, 3, and 4)

The *Software/Firmware Load Test* specified in *{ISO/IEC 19790:2012 subclause}* 7.10.3.4 shall be performed before the loaded code can be executed.

NOTE This assertion is not separately tested. Tested as part of AS10.37 through AS10.41.

AS04.31: (Software/Firmware loading – Levels 1, 2, 3, and 4)

The cryptographic module shall withhold execution of any loaded or modified approved security functions until after the pre-operational self-tests specified in *{ISO/IEC 19790:2012 subclause}* 7.10.2 have been successfully executed.

NOTE This assertion is not separately tested. Tested as part of AS10.37 through AS10.41.

AS04.32: (Software/Firmware loading – Levels 1, 2, 3, and 4)

The modules versioning information shall be modified to represent the addition and/or update of the newly loaded software or firmware (*{ISO/IEC 19790:2012 subclause}* 7.4.3).

Required Vendor Information

VE04.32.01: The vendor shall provide the means to read the version of the newly loaded software or firmware.

Required Test Procedures

TE04.32.01: The tester shall initiate the software/firmware load test. After the pre-operational self-tests have been successfully executed subsequent to software/firmware load test, the tester shall verify that the versioning information is modified to represent the the addition and/or update of the newly loaded software or firmware.

AS04.33: (Software/Firmware loading – Levels 1, 2, 3, and 4)

If the loading of new software or firmware is a complete image replacement, this shall constitute an entirely new module which would require validation by a validation authority to maintain validation.

Required Vendor Information

VE04.33.01: The vendor provided documentation shall specify whether the module supports a complete image replacement as a result of software/firmware load test.

VE04.33.02: The vendor shall provide a certificate of validation by a validation authority. This certificate shall unambiguously identity the software or firmware loaded in the cryptographic module

Required Test Procedures

TE04.33.01: The tester shall ensure that the new complete image replacement is validated by a validation authority by inspection of the name and version as indicated in AS04.13.

AS04.34: (Software/Firmware loading – Levels 1, 2, 3, and 4)

The new software or firmware image shall only be executed after the module transitions through a power-on reset.

Required Vendor Information

VE04.34.01: If a complete image replacement is supported, the vendor provided documentation shall specify how the new image is executed only after the module transitions through a power-on reset.

Required Test Procedures

TE04.34.01: The tester shall initiate the software/firmware load test. After the software/firmware load test passed, the tester shall verify that the loaded software or firmware cannot be used until after the pre-operational self-tests have been successfully executed through power-on reset.

AS04.35: (Software/Firmware loading – Levels 1, 2, 3, and 4)

All SSPs shall be zeroised prior to execution of the new image.

Required Vendor Information

VE04.35.01: If a complete image replacement is supported, the vendor provided documentation shall specify that SSP zeroisation takes place prior to execution of the new image.

VE04.35.02: If a complete image replacement is supported, the vendor documentation shall specify the following SSPs zeroisation information:

a) Zeroisation techniques

b) Rationale explaining how the zeroisation technique is performed in a time that is not sufficient to compromise SSPs

Required Test Procedures

TE04.35.01: The tester shall review the vendor documentation to verify that the information specified in VE04.35.01 is included. The tester shall determine 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.

TE04.35.02: The tester shall note which keys are present in the module and initiate the power-on reset subsequent to software/firmware load test. Following the completion of the pre-operational self-test, the tester shall attempt to perform cryptographic operations using each of the SSPs that were stored in the module. The tester shall verify that each SSP cannot be accessed.

6.4.4 Authentication

Role-Based Authentication

AS04.36: (Role-Based Authentication – Levels 2, 3, and 4)

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 and shall authenticate the assumption of the selected role (or set of roles).

NOTE This assertion is not separately tested. Tested as part of AS04.37.

AS04.37: (Role-Based Authentication – Levels 2, 3, and 4)

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 and shall authenticate the assumption of the selected role (or set of roles).

Required Vendor Information

VE04.37.01: 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

TE04.37.01: 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.

TE04.37.02: 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.

AS04.38: (Role-Based Authentication – Levels 2, 3 and 4)

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 for that operator.

Required Vendor Information

VE04.38.01: 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

TE04.38.01: 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.

TE04.38.02: The tester shall perform the following tests:

a) 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.

b) 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

AS04.39: (Identity-Based Authentication – Levels 3 and 4)

If identity-based authentication mechanisms are supported by a cryptographic module, the module shall require that the operator be individually and uniquely 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 authorization of the operator to assume the selected role or set of roles}*.

Required Vendor Information

VE04.39.01: 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

TE04.39.01: 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.

TE04.39.02: 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.

TE04.39.03: 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.

AS04.40: (Identity-Based Authentication – Levels 3 and 4)

{If identity-based authentication mechanisms are supported by a cryptographic module, the module shall require that the operator be individually and uniquely 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 authorization of the operator to assume the selected role or set of roles}.***

Required Vendor Information

VE04.40.01: 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

TE04.40.01: The tester shall verify in 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.

TE04.40.02: The tester shall perform the following tests:

a) 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.

b) 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.

AS04.41: (Identity-Based Authentication – Levels 3 and 4)

{If identity-based authentication mechanisms are supported by a cryptographic module, the module shall require that the operator be individually and uniquely 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 authorization of the operator to assume the selected role or set of roles.**

NOTE This assertion is not separately tested.

AS04.42: (Identity-Based Authentication – Levels 3 and 4)

If a cryptographic module permits an operator to change roles, then the module shall verify the authorisation of the identified operator to assume any role that was not previously authorised.

NOTE This assertion is not separately tested.

AS04.43: (Operator authentication – Levels 1, 2, 3, and 4)

When a cryptographic module is reset, rebooted, powered off and subsequently powered on, the module shall require the operator to be authenticated.

Required Vendor Information

VE04.43.01: The vendor documentation shall describe how the results of previous authentications are cleared when the module is powered off.

Required Test Procedures

TE04.43.01: The tester shall verify the vendor documentation that the clearing of previous authentications upon power off of the module is described.

TE04.43.02: 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.

AS04.44: (Operator authentication – Levels 1, 2, 3, and 4)

Authentication data within a cryptographic module shall be protected against unauthorised use, disclosure, modification, and substitution.

NOTE Approved security functions may be used as part of the authentication mechanism.

Required Vendor Information

VE04.44.01: 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

TE04.44.01: 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.

TE04.44.02: The tester shall perform the following tests:

a) 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.

b) 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.

AS04.45: (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

VE04.45.01: The vendor documentation shall specify means to control access to the module before it is initialised.

Required Test Procedures

TE04.45.01: The tester shall verify the vendor documentation describes the procedure by which the operator is authenticated upon accessing the module for the first time.

TE04.45.02: 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.

TE04.45.03: If default authentication data is used to access to the module and to initialise the authentication mechansim, the tester shall assume the authenticated role, and verify that the default authenticatiaon data is replaced upon the first-time authentication. The tester shall also enter the default authentication data after the first-time authentication and verify that the cryptographic module does not allow the tester to be authenticated.

AS04.46: (Operator authentication – Levels 2, 3, and 4)

If default authentication data is used to control access to the module, then default authentication data shall be replaced upon first-time authentication (*{ISO/IEC 19790:2012 subclause}* 7.9.7).

NOTE This assertion is not separately tested. Tested as part of AS04.45.

AS04.47: (Operator authentication – Levels 2, 3, and 4)

If the cryptographic module uses security functions to authenticate the operator, then those security functions shall be approved security functions.

Required Vendor Information

VE04.47.01: The vendor provided documentation shall specify the list of security functions used to authenticate operators.

VE04.47.02: The vendor shall provide a validation certificate for each approved security functions as specified in VE02.20.01.

Required Test Procedures

TE04.47.01: The tester shall verify that the security functions used to authenticate operators are all approved security functions.

AS04.48: (Operator authentication – Levels 2, 3, and 4)

The module shall implement an approved authentication mechanism as specified in *{ISO/IEC 19790:2012}* Annex E.

Required Vendor Information

VE04.48.01: The vendor documentation shall describe the approved authentication mechanism used to authenticate operators.

VE04.48.02: If the module implements an approved authentication mechanism, the vendor shall provide a validation certificate as specified in VE02.20.01.

Required Test Procedures

TE04.48.01: The tester shall verify that the authentication mechanism used to authenticate operators is an approved one.

AS04.49: (Operator authentication – Levels 2, 3, and 4)

The strength of the approved authentication mechanism shall be specified in the security policy (*{ISO/IEC 19790:2012}* Annex B).

NOTE This assertion is not separately tested. Tested as part of ASB.01.

AS04.50: (Operator authentication – Levels 2, 3, and 4)

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

Required Vendor Information

VE04.50.01: 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

TE04.50.01: The tester shall verify the vendor documentation for each authentication mechanism that the associated false acceptance or random access rate is specified.

TE04.50.02: The tester shall verify the vendor documentation for each authentication mechanism that the objective is met.

AS04.51: (Operator authentication – Levels 2, 3, and 4)

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

Required Vendor Information

VE04.51.01: 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

TE04.51.01: The tester shall verify the vendor documentation for each authentication mechanism that the associated probability of a successful random is specified.

TE04.51.02: The tester shall verify the vendor documentation for each authentication mechanism that the associated probability of a successful random is meeting the objective.

AS04.52: (Operator authentication – Levels 2, 3, and 4)

The approved authentication mechanism shall be met by the module's implementation and not rely on documented procedural controls or security rules (e.g. password size restrictions).

Required Vendor Information

VE04.52.01: The vendor shall provide complete description of the authentication mechanisms.

Required Test Procedures

TE04.52.01: The tester shall verify by inspection and from the vendor documentation.that the approved authentication mechanism is met by the module's implementation and does not rely on documented procedural controls or security rules.

AS04.53: (Operator authentication – Level 2)

If the operating system implements the authentication mechanism, then the authentication mechanism shall meet the requirements of this clause.

Required Vendor Information

VE04.53.01: The vendor shall provide authentication mechanism specification of the operating system.

Required Test Procedures

TE04.53.01: The tester shall verify the vendor documentation and by inspection that the approved authentication mechanism implemented in the operating system meets the applicable requirements.

AS04.54: (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

VE04.54.01: 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

TE04.54.01: The tester shall verify the vendor documentation that the authentication data is obscured during data entry.

TE04.54.02: The tester shall enter authentication data and verify that there is no visible display of authentication data during data entry.

AS04.55: (Operator authentication – Levels 2, 3, and 4)

Feedback provided to an operator during an attempted authentication shall prevent weakening of the authentication mechanism strength beyond the required authentication strength.

Required Vendor Information

VE04.55.01: The vendor documentation shall specify the feedback mechanism that is used when the operator is entering authentication data.

Required Test Procedures

TE04.55.01: 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.

TE04.55.02: The tester shall enter authentication data to assume each role to ensure that the feedback mechanism does not provide useful information.

AS04.56: (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

VE04.56.01: 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).

VE04.56.02: The vendor provided non-proprietary security policy shall provide a description of the roles, either implicit or explicit, that the operator can assume.

VE04.56.03: The vendor provided non-proprietary security policy shall provide instructions for the operator to assume either the implicit or explicit roles.

Required Test Procedures

TE04.56.01: 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.

TE04.56.02: 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.

AS04.57: (Operator authentication – Level 2)

A cryptographic module shall at a minimum employ *role-based* authentication to control access to the module.

NOTE This assertion is not separately tested. Tested as part of AS04.13.

AS04.58: (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 not separately tested. Tested as part of AS04.16 and AS04.17.

AS04.59: (Operator authentication – Level 4)

A cryptographic module shall employ *multi-factor identity-based* authentication mechanisms to control access to the module.

VE04.59.01: The vendor shall provide specification of a multi factor identity-based authentication and provide testing features of the mechanism.

Required Test Procedures

TE04.59.01: The tester shall verify the vendor documentation and assess multi-factor identity-based authentication.

6.5 Software/Firmware security

AS05.01: (Software/Firmware security – Levels 1, 2, 3, and 4)

The requirements of this clause shall apply to software and firmware components of a cryptographic module.

NOTE This assertion is not separately tested. Tested as part of AS05.02 through AS05.21.

AS05.02: (Software/Firmware security – Levels 1, 2, 3 and 4)

The documentation requirements specified in *{ISO/IEC 19790:2012 Annex}* A.2.5 shall be provided.

Required Vendor Information

VE05.02.01: The vendor shall provide documentation as specified in A.2.5 of ISO/IEC 19790:2012.

Required Test Procedures

TE05.02.01: The tester shall verify completeness of the documentation specified in A.2.5 of ISO/IEC 19790:2012.

AS05.03: (Software/Firmware security – Levels 1, 2, 3 and 4)

The following requirements shall apply to software and firmware components of a cryptographic module for Security Level 1.

NOTE This assertion is not separately tested.

AS05.04: (Software/Firmware security – Levels 1, 2, 3 and 4)

All software and firmware shall be in a form that satisfies the requirements of this International Standard without modification prior to installation *{ISO/IEC 19790:2012 subclause}* (7.11.7).

Required Vendor Information

VE05.04.01: The vendor shall provide software and firmware specification.

Required Test Procedures

TE05.04.01: The tester shall verify, by inspection of the cryptographic module, that specifications provided by vendor documentation are consistent with the actual design of the cryptographic module.

AS05.05: (Software/Firmware security – Levels 1, 2, 3 and 4)

A cryptographic mechanism using an approved integrity technique shall be applied to all software and firmware components within the module's defined cryptographic boundary in one of the following ways:

— **by the cryptographic module itself; or**

— **by another validated cryptographic module operating in an approved mode of operation.**

Required Vendor Information

VE05.05.01: The vendor provided documentation shall specify that the integrity technique is applied to all software and firmware components either 1) by the cryptographic module itself; or 2) by another validated cryptographic module operating in an approved mode of operation.

VE05.05.02: The vendor provided documentation shall specify how the integrity technique is applied to all software and firmware components using either 1) a single encompassing message authentication code or signature; or 2) multiple disjoint codes or signatures.

VE05.05.03: The vendor provided documentation shall specify the location of the cryptographic key used in the integrity technique. If the approved digital signature is used as the integrity technique, the vendor documentation shall also specify the location of the private signing key which is used to generate reference signature.

Required Test Procedures

TE05.05.01: The tester shall verify by inspection of the cryptographic module that an approved integrity technique is applied to all software and firmware components within the module.

AS05.06: (Software/Firmware security – Levels 1, 2, 3 and 4)

If the integrity test fails, the module shall enter the error state.

Required Vendor Information

VE05.06.01: The vendor shall provide the specification of the integrity test of Software/firmware. This mechanism shall be an approved security function.

Required Test Procedures

TE05.06.01: The tester shall verify that if the integrity test fails, the module enters the error state.

TE05.06.02: The tester shall verify that the intermediate value generated during integrity test are zeroised after execution of the integrity test.

AS05.07: (Software/Firmware security – Levels 1, 2, 3 and 4)

The approved integrity technique may consist of a single encompassing message authentication code or signature, or multiple disjoint authentication codes or signatures of which failure of any disjoint authentication code or signature shall cause the module to enter the error state.

NOTE This assertion is not separately tested. Tested as part of AS05.05 and AS05.06.

AS05.08: (Software/Firmware security – Levels 1, 2, 3 and 4)

The temporary value(s) generated during the integrity test of the module's software or firmware shall be zeroised from the module upon completion of the integrity test.

NOTE This assertion is not separately tested. Tested as part of AS05.06.

AS05.09: (Software/Firmware security – Levels 1, 2, 3 and 4)

An operator shall be able to perform the approved integrity technique on demand via an HMI, SFMI, HSMI or HFMI service *{ISO/IEC 19790:2012 subclause}* (7.3.2).

Required Vendor Information

VE05.09.01: The vendor documentation shall describe the way to perform the approved integrity technique on demand via an HMI, SFMI, HSMI or HFMI service.

Required Test Procedures

TE05.09.01: The tester shall verify that the integrity test can be performed via an HMI, SFMI, HSMI or HFMI service.

TE05.09.02: The tester shall verify that during the execution of the integrity test all data and control inputs, and data and status outputs (specified in 7.3.2) of the cryptographic module and services (specified in 7.4.3) can be transmitted via an HMI, SFMI, HSMI or HFMI service.

AS05.10: (Software/Firmware security – Levels 1, 2, 3 and 4)

All data and control inputs, and data, control and status outputs (specified in *{ISO/IEC 19790:2012 subclause}* 7.3.3) of the cryptographic module and services (*{ISO/IEC 19790:2012 subclause}*7.4.3) shall be directed through a defined HMI, SFMI, HFMI or HSMI.

NOTE This assertion is not separately tested. Tested as part of AS05.09.

AS05.11: (Software/Firmware security – Levels 1, 2, 3 and 4)

If the software or firmware that is loaded is associated, bound, modifies or is an executable requisite of the validated module but is not a complete replacement or overlay of the validated module, then the software/firmware load test is applicable and shall be performed by the validated module.

Required Vendor Information

VE05.11.01: The vendor shall provide the specification of the software/firmware load test performed by the validated module.

Required Test Procedures

TE05.11.01: The tester shall verify the vendor documentation and vendor implementation.

AS05.12: (Software/Firmware security – Levels 2, 3 and 4)

The following requirements shall apply to software and firmware components of a cryptographic module for Security Level 2.

NOTE This assertion is not separately tested. Tested as part of AS05.13 through AS05.16.

AS05.13: (Software/Firmware security – Levels 2, 3 and 4)

The software and firmware components of a cryptographic module shall only include code that is in executable form (e.g. no source code, object code or just-in-time compiled code).

Required Vendor Information

VE05.13.01: The vendor shall provide software and firmware description with the executable form used.

Required Test Procedures

TE05.13.01: The tester shall verify the vendor documentation software and vendor implementation in order to avoid dynamically modified code.

AS05.14: (Software/Firmware security – Levels 2, 3 and 4)

There shall be no services via the HMI, SFMI, HFMI or HSMI interface to allow the operator to examine the executable code.

Required Vendor Information

VE05.14.01: The vendor shall provide specification of HMI, SFMI, HFMI, or HSMI services.

Required Test Procedures

TE05.14.01: The tester shall verify the vendor documented specification of services.

VE05.14.02: The tester shall verify from the vendor documentation that the services do not allow the operator to examine the executable code.

VE05.14.03: The tester shall test the services to verify that the operator cannot examine the executable code.

AS05.15: (Software/Firmware security – Levels 2, 3 and 4)

An approved digital signature or keyed message authentication code shall be applied to all software and firmware within the module's defined cryptographic boundary.

Required Vendor Information

VE05.15.01: The vendor shall provide documentation that identifies the technique used to maintain the integrity of the cryptographic software and firmware components.

Required Test Procedures

TE05.15.01: The tester shall verify that the information specified in VE05.15.01 is included. If this information is not included, then this assertion fails.

TE05.15.02: The tester shall attempt to corrupt the cryptographic software and firmware components. If the integrity is maintained, this TE fails.

AS05.16: (Software/Firmware security – Levels 2, 3 and 4)

If the calculated result does not equal the previously generated result, the test fails and the module shall enter the error state.

NOTE This assertion is not separately tested. Tested as part of AS05.15.

AS05.17 : (Software/Firmware security – Levels 3 and 4)

The following requirements shall apply to software and firmware components of a cryptographic module for Security Level 3 and 4.

NOTE This assertion is not separately tested.

AS05.18: (Software/Firmware security – Levels 3 and 4)

A cryptographic mechanism using an approved digital signature shall be applied to all software and firmware components within the module's defined cryptographic boundary.

Required Vendor Information

VE05.18.01: The vendor shall provide documentation of the approved digital signature mechanism.

Required Test Procedures

TE05.18.01: The tester shall verify by inspection of the cryptographic module that a cryptographic mechanism using an approved digitial signature mechism is applied to all software and firmware components within the modules defined cryptographic boundary.

AS05.19: (Software/Firmware security – Levels 3 and 4)

If the calculated result does not equal the previously generated result, the test fails and the module shall enter the error state.

NOTE This assertion is not separately tested. Tested as part of AS05.15.

AS05.20: (Software/Firmware security – Levels 3 and 4)

The digital signature technique may consist of a single encompassing signature or multiple disjoint signatures of which failure of any disjoint signature shall cause the module to enter the error state.

NOTE This assertion is not separately tested. Tested as part of AS05.05.

AS05.21: (Software/Firmware security – Levels 3 and 4)

The private signing key shall reside outside the module.

Required Vendor Information

VE05.21.01: The vendor documentation requirement is specified under VE05.05.03. The vendor design shall ensure that the private signing key for generating reference signature does not reside within the cryptographic module boundary.

Required Test Procedures

TE05.21.01: The tester shall verify, by inspection and from the vendor documentation, that the private signing key does not reside within the cryptographic boundary.

6.6 Operational environment

6.6.1 Operational environment general requirements

AS06.01: (Operational environment – Levels 1 and 2)

If the operational environment is *non-modifiable* or a *limited* operational environment, only the operating system requirements in *{ISO/IEC 19790:2012 subclause}* 7.6.2 shall apply.

NOTE This assertion is not separately tested. It is tested as part of AS06.04.

AS06.02: (Operational environment – Levels 1 and 2)

If the operational environment is a *modifiable* operational environment, the operating system requirements in *{ISO/IEC 19790:2012 subclause}* 7.6.3 shall apply.

NOTE This assertion is not separately tested. It is tested as part of AS06.05 through AS06.29 as applicable.

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

The documentation requirements specified in *{ISO/IEC 19790:2012 Annex}* A.2.6 shall be provided.

Required Vendor Information

VE06.03.01: The vendor shall provide the documentation requirements as specified in A.2.6 of ISO/IEC 19790:2012.

Required Test Procedures

TE06.03.01: The tester shall verify that the vendor provides documentation as specified in A.2.6 of ISO/IEC 19790:2012.

6.6.2 Operating system requirements for limited or non-modifiable operational environments

AS06.04: (Operational environment – Level 1)

The requirements in *{ISO/IEC 19790:2012 subclause}* 7.6.3 *Security Level 1* shall be applicable if the module is Security Level 1 in *{ISO/IEC 19790:2012 subclause}* 7.7.

NOTE This assertion is not separately tested. It is tested as part of AS06.05 through AS06.08.

{The requirements AS06.05 through AS06.29 apply to the operating system or operating environment as applicable}

6.6.3 Operating system requirements for modifiable operational environments

AS06.05: (Operational environment – Levels 1 and 2)

Each instance of a cryptographic module shall have control over its own SSPs.

NOTE 1 Each instance of a cryptographic module controls its own SSPs and are not owned or controlled by external processes/operators.

NOTE 2 This requirement cannot be enforced by administrative documentation and procedures, but must be enforced by the cryptographic module itself.

Required Vendor Information

VE06.05.01: The vendor shall provide a description of the operating system mechanism used to ensure that each instance of a cryptographic module has control over its own SSPs 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 operating system, that each instance of a cryptographic module has control over its own SSPs while the cryptographic module is in use.

TE06.05.02: The tester shall verify, from the vendor documentation and by inspection of the operating system, that the requirement shall be enforced by the cryptographic module itself.

TE06.05.03: 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 gain unauthorized access to secret and private keys, intermediate key generation values, and other SSPs which are under the control of the cryptographic module.

AS06.06: (Operational environment – Levels 1 and 2)

The operational environment shall provide the capability to separate individual application processes from each other by preventing uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless if this data is in the process memory or stored on persistent storage within the operational environment.

Required Vendor Information

VE06.06.01: The vendor shall provide a description of the operational environment mechanism used to provide the capability to separate individual application processes from each other by preventing uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless if this data is in the process memory or stored on persistent storage within the operational environment.

Required Test Procedures

TE06.06.01: The tester shall verify, from the vendor documentation and by inspection of the operational environment mechanism used that it provides the capability to separate individual application processes from each other by preventing uncontrolled access to CSPs and uncontrolled modifications of SSPs regardless if this data is in the process memory or stored on persistent storage within the operational environment.

TE06.06.02: 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 gain access to CSPs and perform modifications of SSPs regardless if this data is in the process memory or stored on persistent storage within the operational environment.

AS06.07: (Operational environment – Levels 1 and 2)

Restrictions to the configuration of the operational environment shall be documented in the security policy of the cryptographic module.

Required Vendor Information

VE06.07.01: The vendor shall provide documentation which provides a description of any restrictions to the operational environment.

Required Test Procedures

TE06.07.01: The tester shall verify from the vendor documentation any restrictions to the operational environment.

TE06.07.02: The tester shall verify that any restrictions to the operational environment are documented in the Security Policy.

AS06.08: (Operational environment – Levels 1 and 2)

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

NOTE This requirement cannot be enforced by administrative documentation and procedures, but must be enforced by the cryptographic module itself.

Required Vendor Information

VE06.08.01: The vendor shall provide a description of the operating system mechanism used to ensure that processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.

Required Test Procedures

TE06.08.01: The tester shall verify, from the vendor documentation and by inspection of the operating system, that processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.

TE06.08.02: The tester shall verify, from the vendor documentation and by inspection of the operating system, that the requirement shall be enforced by the cryptographic module itself.

TE06.08.03: 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 gain ownership of a spawned cryptographic process that is owned by a cryptographic module from either a separate external process or operator.

AS06.09: (Operational environment – Level 2)

For Security Level 2 an operating environment shall meet the following requirements or as allowed by the validation authority.

NOTE 1 If the operating environment requirements are not specified by a validation authority, the assertion is tested in AS06.10 through AS06.29.

NOTE 2 If the operating environment requirements are specified by a validation authority, the assertion is tested as follows.

Required Vendor Information

VE06.09.01: The vendor shall provide documentation which provides a description of the operating envrionment.

VE06.09.02: The vendor shall provide documentation comparing the operating environment with the operating environment allowed by the validation authority.

Required Test Procedures

TE06.09.01: The tester shall verify that the vendor documentation provides a description of the operating system.

TE06.09.02: The tester shall verify by inspection of the operating system that it matches the vendor provided description of the operating system.

TE06.09.03: The tester shall verify by inspection of the operating system and the vendor provided description of the operating system that it is allowed by the validation authority.

AS06.10: (Operational environment – Level 2)

All cryptographic software, SSPs, and control and status information shall be under the control of an operating system that implements either role-based access controls or, at the minimum, a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions for example through access control lists (ACLs), and with the capability of assigning each user to more than one group.

Required Vendor Information

VE06.10.01: The vendor shall provide operating system documentation which provides a description of the operating system control mechansims which implements either role-based access controls or, at the minimum, a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions for example through access control lists (ACLs), and with the capability of assigning each user to more than one group.

Required Test Procedures

TE06.10.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechansims, that the operating system implements either role-based access controls or, at the minimum, a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions for example through access control lists (ACLs), and with the capability of assigning each user to more than one group.

TE06.10.02: The tester shall configure the operating systems role-based access controls or discretionary access controls to give permissions to a specifc user or group. The tester, assuming a permitted user or group role, shall attempt to execute, modify, or read SSPs, control or status data which the tester has authorized access.

TE06.10.03: The tester shall configure the operating systems role-based access controls or discretionary access controls to give permissions to a specifc user or group. The tester, assuming a different user or group role, shall attempt to execute, modify, or read SSPs, control or status data which the tester has unauthorized access.

AS06.11: (Operational environment – Level 2)

The operating system shall be configured to protect against unauthorised execution, modification, and reading of SSPs, control and status data.

Required Vendor Information

VE06.11.01: The vendor shall provide operating system documentation which provides a description of the operating system control mechansims which can be configured to protect against unauthorised execution, modification, and reading of SSPs, control and status data.

Required Test Procedures

TE06.11.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechansims, that the operating system can be configured to protect against unauthorised execution, modification, and reading of SSPs, control and status data.

TE06.11.02: The tester shall configure the operating system to protect against unauthorised execution, modification, and reading of SSPs, control and status data. During execution of a cryptographic process, the tester shall attempt to execute, modify or read SSPs, control or status data which the tester has authorized access.

TE06.11.03: The tester shall configure the operating system to protect against unauthorised execution, modification, and reading of SSPs, control and status data. During execution of a cryptographic process, the tester shall attempt to execute, modify or read SSPs, control or status data which the tester has unauthorized access.

AS06.12: (Operational environment – Level 2)

{To protect plaintext data, cryptographic software, SSPs, and authentication data, the access control mechanisms of the operating system} **shall be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *execute* the stored cryptographic software.**

Required Vendor Information

VE06.12.01: The vendor shall provide operating system documentation which provides a description of how the access control mechanisms of the operating system are configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *execute* the stored cryptographic software.

Required Test Procedures

TE06.12.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechanisms, that the operating system is configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *execute* the stored cryptographic software.

TE06.12.02: The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to *execute* the stored cryptographic software. The tester shall verify that they have exclusive rights to *execute* the stored cryptographic software.

TE06.12.03: The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to not give exclusive rights to *execute* the stored cryptographic software. The tester shall verify that they do not have exclusive rights to *execute* the stored cryptographic software.

AS06.13: (Operational environment – Level 2)

{To protect plaintext data, cryptographic software, SSPs, and authentication data, the access control mechanisms of the operating system} **shall be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *modify* (i.e., write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.**

Required Vendor Information

VE06.13.01: The vendor shall provide operating system documentation which provides a description of how the access control mechanisms of the operating system are configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *modify* (i.e., write, replace, and delete) the following cryptographic module software stored within the

cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.

Required Test Procedures

TE06.13.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechanisms, that the operating system is configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *modify* (i.e., write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.

TE06.13.02: The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to *execute* the stored cryptographic software. The tester shall verify that they have exclusive rights to *modify* (i.e., write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.

TE06.13.03: The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to not give exclusive rights to *modify* (i.e., write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data. The tester shall verify that they do not have exclusive rights to *modify* (i.e., write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g. cryptographic audit data), SSPs, and plaintext data.

AS06.14: (Operational environment – Level 2)

***{To protect plaintext data, cryptographic software, SSPs, and authentication data, the access control mechanisms of the operating system}* shall be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *read* cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.**

Required Vendor Information

VE06.14.01: The vendor shall provide operating system documentation which provides a description of how the access control mechanisms of the operating system are configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *read* cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.

Required Test Procedures

TE06.14.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechanisms, that the operating system is configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *read* cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.

TE06.14.02: The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to *read* cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.

TE06.14.03: The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to not give exclusive rights to *read* cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data. The tester shall verify that they do not have exclusive rights to *read* cryptographic data (e.g. cryptographic audit data), CSPs, and plaintext data.

AS06.15: (Operational environment – Level 2)

{To protect plaintext data, cryptographic software, SSPs, and authentication data, the access control mechanisms of the operating system} **shall be configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *enter* SSPs.**

Required Vendor Information

VE06.15.01: The vendor shall provide operating system documentation which provides a description of how the access control mechanisms of the operating system are configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *enter* SSPs.

Required Test Procedures

TE06.15.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechanisms, that the operating system is configured to define and enforce the set of roles or the groups and their associated restrictive permissions that have exclusive rights to *enter* SSPs.

TE06.15.02: The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to give exclusive rights to *enter* SSPs.

TE06.15.03: The tester shall configure the operating system control mechanisms to define and enforce the set of roles or the groups and their associated restrictive permissions to not give exclusive rights to *enter* SSPs. The tester shall verify that they do not have exclusive rights to *enter* SSPs.

AS06.16: (Operational environment – Level 2)

The following specifications shall be consistent with the roles or designated groups' rights and services as defined in the security policy.

NOTE This assertion is not separately tested. It is tested as part of AS06.17 through AS06.20.

AS06.17: (Operational environment – Level 2)

When not supporting a maintenance role, the operating system shall prevent all operators and running processes from modifying running cryptographic processes (i.e., loaded and executing cryptographi program images).

Required Vendor Information

VE06.17.01: The vendor shall provide operating system documentation which provides a description of how the operating system prevents all operators and running processes from modifying running cryptographic processes (i.e., loaded and executing cryptographic program images) when not in maintenance mode.

VE06.17.02: The specifications of how the operating system prevents all operators and running processes from modifying running cryptographic processes (i.e., loaded and executing cryptographic program images) when not in maintenance mode shall be consistent with the roles or designated groups' rights and services as defined in the Security Policy.

Required Test Procedures

TE06.17.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechanisms, that the operating system is configured to prevent all operators and running processes from modifying running cryptographic processes (i.e., loaded and executing cryptographic program images) when not in maintenance mode.

TE06.17.02: The tester shall verify that the roles or designated groups' rights and services as defined in the Security Policy is consistent with how the operating system is configured to prevent all operators and running processes from modifying running cryptographic processes (i.e., loaded and executing cryptographic program images) when not in maintenance mode.

TE06.17.03: The tester shall configure the operating system control mechanisms to prevent all operators and running processes from modifying running cryptographic processes (i.e., loaded and executing cryptographic program images) when not in maintenance mode. The tester shall assume an operator role and verify that they are prevented from modifying running cryptographic processes (i.e., loaded and executing cryptographic program images) when not in maintenance mode. The tester shall verify that running processs are prevented from modifying running cryptographic processes (i.e., loaded and executing cryptographic program images) when not in maintenance mode.

AS06.18: (Operational environment – Level 2)

The operating system shall prevent processes in user role or user groups from gaining either *read* or *write* access to SSPs owned by other processes and to system SSPs.

Required Vendor Information

VE06.18.01: The vendor shall provide operating system documentation which provides a description of how the operating system prevents processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs.

VE06.18.02: The specifications of how the operating system prevents processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs shall be consistent with the roles or designated groups' rights and services as defined in the Security Policy.

Required Test Procedures

TE06.18.01: The tester shall verify that the vendor documentation, and by inspection of operating system control mechanisms, that the operating system is configured to prevent processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs.

TE06.18.02: The tester shall verify that the roles or designated groups' rights and services as defined in the Security Policy is consistent with how the operating system is configured to prevent processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs.

TE06.18.03: The tester shall configure the operating system control mechanisms to prevent processes in user roles or user groups from gaining either read or write access to SSPs owned by other processes and to system SSPs. The tester shall verify that running processes in user roles or user groups are prevented from gaining either read or write access to SSPs owned by other processes and to system SSPs.

AS06.19: (Operational environment – Level 2)

The configuration of the operating system that meets the above requirements *{AS06.16 through AS06.18}* shall be specified in the Administrator Guidance.

Required Vendor Information

VE06.19.01: The vendor shall provide the Administrator Guidance documents which provides a description of how the operating system is configured to meet the requirements in AS06.16 through AS06.18.

Required Test Procedures

TE06.19.01: The tester shall verify that the vendor provided Administrator Guidance documents provide a description of how the operating system is configured to meet the requirements in AS06.16 through AS06.18.

AS06.20: (Operational environment – Level 2)

The Administrator Guidance shall state that the operating system must be configured as specified *{AS06.16 through AS06.18}* for the module contents to be considered protected.

Required Vendor Information

VE06.20.01: The vendor shall provide the Administrator Guidance documents which state that the operating system shall be configured as specified AS06.16 through AS06.18 for the module contents to be considered protected.

Required Test Procedures

TE06.20.01: The tester shall verify that the vendor provided Administrator Guidance documents state that the operating system shall be configured as specified AS06.16 through AS06.18 for the module contents to be considered protected.

AS06.21: (Operational environment – Level 2)

The identification and authentication mechanism to the operating system shall meet the requirements of *{ISO/IEC 19790:2012 subclause}* 7.4.3 and be specified in the modules security policy.

NOTE This assertion is not separately tested. Tested as part of AS06.24 through AS06.28.

AS06.22: (Operational environment – Level 2)

All cryptographic software, SSPs, control and status information shall be under the control of *{an operating system which shall have, at a minimum, the following attributes.}*

NOTE This assertion is not separately tested. Tested as part of AS06.24 through AS06.28.

AS06.23: (Operational environment – Level 2)

***{All cryptographic software, SSPs, control and status information shall be under the control of}* an operating system which shall have, at a minimum, the following attributes.**

NOTE This assertion is not separately tested. Tested as part of AS06.24 through AS06.28.

AS06.24: (Operational environment – Level 2)

The operating system shall provide an audit mechanism with the date and time of each audited event.

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

VE06.24.01: The vendor shall provide operating system documentation which provides a description of the audit mechanism provided by the operating system and how each event is marked with the date and time.

Required Test Procedures

TE06.24.01: The tester shall verify that the vendor documentation, and by inspection of operating system, that an audit mechansim is provided and that each event is marked with the date and time.

AS06.25: (Operational environment – Level 2)

The cryptographic module shall not include SSPs as part of any audit record.

Required Vendor Information

VE06.25.01: The vendor shall provide operating system documentation which provides a description of the cryptographic modules services that provide audit records to the audit mechanism of the operating system.

Required Test Procedures

TE06.25.01: The tester shall verify that the vendor documentation, and by inspection of the cryptographic modules services that provide audit records to the audit mechanism of the operating system that no SSPs are provided in the audit records.

TE06.25.02: The tester shall execute the modules services that provide audit records and examine the operating system audit logs to verify that no SSPs were provided.

AS06.26: (Operational environment – Level 2)

The cryptographic module shall provide the following events to be recorded by the audit mechanism of the operating system:

- **modifications, accesses, deletions, and additions of cryptographic data and SSPs;**
- **attempts to provide invalid input for Crypto Officer functions;**
- **addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by the cryptographic module);**
- **the use of a security-relevant Crypto Officer function;**
- **requests to access authentication data associated with the cryptographic module;**
- **the use of an authentication mechanism (e.g. login) associated with the cryptographic module; and**
- **explicit requests to assume a Crypto Officer role.**

Required Vendor Information

VE06.26.01: The vendor shall provide operating system documentation which provides a description of the cryptographic module events that are provided and recorded by the audit mechanism of the operating system.

Required Test Procedures

TE06.26.01: The tester shall verify that the vendor documentation, and by inspection of the cryptographic modules services that provide audit event records to the audit mechanism of the operating system, that the list of events specified in AS06.26 *{modifications, accesses, deletions, and additions of cryptographic data and SSPs; attempts to provide invalid input for Crypto Officer functions; addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by the cryptographic module); the use of a security-relevant Crypto Officer function; requests to access authentication data associated with the cryptographic module; the use of an authentication mechanism (e.g. login) associated with the cryptographic module; and explicit requests to assume a Crypto Officer role}* are provided by the cryptographic module for event recording.

TE06.26.02: The tester shall execute the modules services that provide audit event records and examine the operating system audit logs to verify that the events in AS06.26 *{modifications, accesses, deletions, and additions of cryptographic data and SSPs; attempts to provide invalid input for Crypto Officer functions; addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by the cryptographic module); the use of a security-relevant Crypto Officer function; requests to access authentication data associated with the cryptographic module; the use of an authentication mechanism (e.g. login) associated with the cryptographic module; and explicit requests to assume a Crypto Officer role}* were recorded.

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

AS06.27: (Operational environment – Level 2)

The audit mechanism of the operating system shall be capable of auditing the following operating system related events:

- **all operator read or write accesses to audit data stored in the audit trail;**
- **access to files used by the cryptographic module to store cryptographic data or SSPs;**
- **addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by operational environment);**
- **requests to use authentication data management mechanisms;**
- **attempts to use the trusted channel function and whether the request was granted, when trusted channel is supported at this security level; and**
- **identification of the initiator and target of a trusted channel, when trusted channel is supported at this security level.**

Required Vendor Information

VE06.27.01: The vendor shall provide operating system documentation which provides a description of the operating system events that are provided and recorded by the audit mechanism of the operating system.

Required Test Procedures

TE06.27.01: The tester shall verify that the vendor documentation, and by inspection of the operating system documentation, that the operating system provides the list of events specified in AS06.27 *{all operator read or write accesses to audit data stored in the audit trail; access to files used by the cryptographic module to store cryptographic data or SSPs; addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by operational environment); requests to use authentication data management mechanisms; attempts to use the trusted channel function and whether the request was granted, when trusted channel is supported at this security level; and identification of the initiator and target of a trusted channel, when trusted channel is supported at this security level}* as audit event records to the audit mechanism of the operating system.

TE06.27.02: The tester shall execute the cryptogrpahic modules services to verify that the operating system events in AS06.27 *{all operator read or write accesses to audit data stored in the audit trail; access to files used by the cryptographic module to store cryptographic data or SSPs; addition or deletion of an operator to and from a Crypto Officer role (if those roles are managed by operational environment); requests to use authentication data management mechanisms; attempts to use the trusted channel function and whether the request was granted, when trusted channel is supported at this security level; and identification of the initiator and target of a trusted channel, when trusted channel is supported at this security level}* were recorded.

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

AS06.28: (Operational environment – Level 2)

The operating system shall be configured to prevent operators other than those with the privileges identified in the Security Policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.

Required Vendor Information

VE06.28.01: The vendor shall provide operating system documentation that specifies how the operating system is configured to prevent operators other than those with the privileges identified in the Security Policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.

Required Test Procedures

TE06.28.01: The tester shall verify that the vendor documentation, and by inspection of operating system configuration controls, that the operating system is configured to prevent operators other than those with the privileges identified in the Security Policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.

TE06.28.02: The tester shall configure the operating system controls to prevent operators other than those with the privileges identified in the Security Policy from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.

TE06.28.03: The tester shall assume the privileges identified in the Security Policy to allow modification of the cryptographic module software and audit data stored within the operational environment of the cryptographic module and verify that modification can be achieved.

TE06.28.04: The tester shall assume the privileges identified in the Security Policy that do not allow modification of the cryptographic module software and audit data stored within the operational environment of the cryptographic module and verify that modification can not be achieved.

AS06.29: (Operational environment – Level 2)

Only operating systems that are configured to meet the above security requirements *{AS06.05 through AS06.28}* shall be permitted at this security level, whether or not the cryptographic module operates in an approved mode of operation.

NOTE This assertion is not separately tested. Tested as part of AS06.05 through AS06.28.

6.7 Physical security

6.7.1 Physical security embodiments

AS07.01: (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

VE07.01.01: 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 CSPs) shall be protected.

Required Test Procedures

TE07.01.01: The tester shall verify that the vendor documentation describes the applicable physical security mechanisms that are employed by the module.

TE07.01.02: The tester shall verify that the physical security mechanisms documented are implemented.

AS07.02: (Physical security – Levels 1, 2, 3, and 4)

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

NOTE This assertion is not separately tested.

AS07.03: (Physical security – Levels 1, 2, 3, and 4)

The requirements of this clause shall be applicable to hardware and firmware modules, and hardware and firmware components of hybrid modules.

NOTE This assertion is not separately tested.

AS07.04: (Physical security – Levels 1, 2, 3, and 4)

The requirements of this clause shall be applicable at the defined physical boundary of the module.

NOTE This assertion is not separately tested.

AS07.05: (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

— **during an access attempt**

{and appropriate immediate actions shall be taken by the cryptographic module to protect CSPs}.

NOTE This assertion is not separately tested.

AS07.06: (Physical security – Levels 1, 2, 3, and 4)

{In conjunction with AS07.05:} **Appropiate immediate actions shall be taken by the cryptographic module to protect CSPs.**

NOTE This assertion is not separately tested.

AS07.07: (Physical security – Levels 1, 2, 3, and 4)

The documentation requirements specified in *{ISO/IEC 19790:2012 subclause}* A.2.7 shall be provided.

NOTE This assertion is not separately tested.

6.7.2 Physical security general requirements

AS07.08: (Physical security – Levels 1, 2, 3, and 4)

The following requirements shall apply to all physical embodiments.

NOTE Tested as part of AS07.09 through AS07.33.

AS07.09: (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

VE07.09.01: 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 7.7.1 of ISO/IEC 19790:2012.

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

TE07.09.01: 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 7.7.1 of ISO/IEC 19790:2012.

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.

a) 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 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.

b) 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.

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

TE07.09.02: 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.

AS07.10: (Physical security – Levels 1, 2, 3, and 4)

Whenever zeroisation is performed for physical security purposes, the zeroisation shall occur in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time of detection and the actual zeroisation.

Required Vendor Information

VE07.10.01: The vendor documentation shall specify the response time of the zeroisation after tamper detection.

Required Test Procedures

TE07.10.01: The tester shall verify that the vendor documentation describes the zeroisation response time after the tamper detection.

TE07.10.02: The tester shall verify that the zeroisation response mechanism is implemented as specified.

AS07.11: (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} **a maintenance access interface shall be defined.**

Required Vendor Information

VE07.11.01: The vendor documentation shall describe the maintenance access interface employed by the module.

Required Test Procedures

TE07.11.01: The tester shall verify that the vendor documentation describes the maintenance access interface.

TE07.11.02: The tester shall verify that the vendor documentation and implementation are consistent.

AS07.12: (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

VE07.12.01: The vendor documentation shall specify the maintenance access interface, including any removable covers or doors.

Required Test Procedures

TE07.12.01: The tester shall verify in the vendor documentation that a maintenance access interface is provided, including any removable covers or doors.

AS07.13: (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

VE07.13.01: 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

TE07.13.01: The tester shall very that any removable covers or doors included within the maintenance access interface are safeguarded using the appropriate physical security mechanisms.

AS07.14: (Physical security – Levels 1, 2, 3, and 4)

The following requirements shall apply to all cryptographic modules for Security Level 1.

NOTE Tested as part of AS07.15 through AS07.16.

AS07.15: (Physical security – Levels 1, 2, 3, and 4)

The cryptographic module shall consist of production-grade components that 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

VE07.15.01: The module shall consist of standard, production-quality ICs, 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

TE07.15.01: 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.

TE07.15.02: 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.

AS07.16: (Physical security – Levels 1, 2, 3, and 4)

When performing physical maintenance, zeroisation shall either be performed procedurally by the operator or automatically by the cryptographic module.

NOTE This assertion is tested as part of AS07.10.

AS07.17: (Physical security – Levels 2, 3, and 4)

The following requirement shall apply to all cryptographic modules for Security Level 2.

NOTE Tested as part of AS07.18 through AS07.20.

AS07.18: (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 AS07.34 and AS07.35 for single-chip embodiments, AS07.44 and AS07.45 for multiple-chip embedded embodiments, and AS07.62 and AS07.63 for multiple-chip standalone embodiments.

AS07.19: (Physical security – Levels 2, 3, and 4)

The tamper-evident material, coating or enclosure shall either be opaque or translucent within the visible spectrum (i.e., light of wavelength range of 400nm to 750nm) to prevent the gathering of information about the internal operations of the critical areas of the module.

Required Vendor Information

VE07.19.01: The vendor documentation shall specify that the tamper evident material, coating or enclosure shall be opaque or translucent within the visible spectrum.

Required Test Procedures

TE07.19.01: The tester shall verify by inspection and from the vendor documentation that the tamper evident material, coating or enclosure is opaque or translucent within the visible spectrum.

AS07.20: (Physical security – Levels 2, 3, and 4)

If the cryptographic module contains ventilation holes or slits, then the module shall be constructed in a manner to prevent the gathering of information of the module's internal construction or components by direct visual observation using artificial light sources in the visual spectrum of the module's internal construction or components.

Required Vendor Information

VE07.20.01: 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

TE07.20.01: 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.

AS07.21: (Physical security – Levels 3 and 4)

The following requirements shall apply to all cryptographic modules for Security Level 3.

NOTE Tested as part of AS07.22 through AS07.28.

AS07.22: (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 AS07.13 for general requirements, AS07.38 for single-chip embodiments, AS07.50 for multiple-chip embodiments and AS07.62 for multiple-chip standalone embodiments.

AS07.23: (Physical security – Levels 3 and 4)

The tamper response and zeroisation capability shall immediately zeroise all unprotected SSPs 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 AS07.13 for general requirements, AS07.38 for single-chip embodiments, AS07.50 for multiple-chip embedded embodiments, and AS07.62 for multiple-chip standalone embodiments.

AS07.24: (Physical security – Levels 3 and 4)

The tamper response and zeroisation capability shall remain operational when unprotected SSPs are contained within the cryptographic module.

NOTE This assertion is tested as part of AS07.38 for single-chip embodiments, AS07.50 for multiple-chip embedded embodiments, and AS07.65 for multiple-chip standalone embodiments.

AS07.25: (Physical security – Levels 3 and 4)

If the cryptographic module contains ventilation holes or slits, then the module shall be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g. prevent probing by a single articulated probe).

Required Vendor Information

VE07.25.01: 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

TE07.25.01: 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.

AS07.26: (Physical security – Levels 3 and 4)

Strong or hard conformal or non-conformal enclosures, coatings or potting materials shall maintain strength and hardness characteristics over the modules intended temperature range of operation, storage and distribution.

Required Vendor Information

VE07.26.01: The vendor documentation shall describe the strength of the enclosure and the rational that the strength is appropriate for the module design.

Required Test Procedures

TE07.26.01: The tester shall verify from the vendor documentation and inspection of the module that enclosure is the one designed as specified.

AS07.27: (Physical security – Levels 3 and 4)

If tamper evident seals are employed, they shall be uniquely numbered or independently identifiable (e.g. uniquely numbered evidence tape or uniquely identifiable holographic seals).

Required Vendor Information

VE07.27.01: The vendor shall provide the specification of the tamper evident seal.

Required Test Procedures

TE07.27.01: The tester shall verify that tamper evident seals are uniquely numbered or independently identifiable as documented.

AS07.28: (Physical security – Levels 3 and 4)

The module shall either include EFP features or undergo EFT.

NOTE This assertion is tested as part of AS07.68.

AS07.29: (Physical security – Level 4)

The following requirement shall apply to all cryptographic modules for Security Level 4.

NOTE Tested as part of AS07.30 through AS07.33.

AS07.30: (Physical security – Level 4)

The cryptographic module shall be protected either by a hard opaque removal-resistant coating, or by a tamper detection envelope with tamper response and zeroisation capability.

NOTE This assertion is tested as part of AS07.40 for single-chip embodiments, AS07.52 for multiple-chip embedded embodiments, and AS07.64 for multiple-chip standalone embodiments.

AS07.31: (Physical security – Level 4)

The module shall include EFP features.

NOTE This assertion is tested as part of AS07.72.

AS07.32: (Physical security – Level 4)

The cryptographic module shall provide protection from fault induction.

Required Vendor Information

VE07.32.01: The vendor documentation shall specify the protection mechanism from fault induction.

Required Test Procedures

TE07.32.01: The tester shall verify from the vendor documentation and by inspection of the module that each protection mechanism functions as specified.

AS07.33: (Physical security – Level 4)

The fault induction mitigation techniques and the mitigation metrics employed shall be documented as specified in *{ISO/IEC 19790:2012}* Annex B.

Required Vendor Information

VE07.33.01: The vendor documentation shall specify the fault induction mitigation techniques and the mitigation metrics employed by the module.

Required Test Procedures

TE07.33.01: The tester shall verify that the fault induction mitigation techniques and the mitigation metrics employed by the module are documented as specified.

6.7.3 Physical security requirements for each physical security embodiment

6.7.3.1 Single-chip cryptographic modules

NOTE 1 In addition to the general security requirements specified in 7.7.2 of ISO/IEC 19790:2012, the requirements specified in AS07.34 to AS07.42 are specific to single-chip cryptographic modules.

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

AS07.34: (Single-chip cryptographic modules – Levels 2, 3, and 4)

The following requirements shall apply to single-chip cryptographic modules for Security Level 2.

NOTE This assertion is tested as part of AS07.35.

AS07.35: (Single-chip cryptographic modules – 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 AS07.18.

Required Vendor Information

VE07.35.01: The vendor documentation shall identify the tamper-evident coating and its characteristics.

Required Test Procedures

TE07.35.01: 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.

AS07.36: (Single-chip cryptographic modules – Levels 3 and 4)

The following requirements shall apply to single-chip cryptographic modules for Security Level 3.

NOTE This requirement is tested in AS07.37 or AS07.38.

Required Vendor Information

VE07.36.01: The vendor documentation shall state which of the two approaches specified in AS07.37 and AS07.38 is used to meet the requirement.

Required Test Procedures

TE07.36.01: The tester shall verify by inspection and from the vendor documentation which of the two approaches specified in AS07.37 and AS07.38 is used to meet the requirement.

TE07.36.02: The tester shall follow procedures in TE07.37 but not TE07.38, if approach AS07.37 is found. If instead approach AS07.38 is found, the tester shall follow procedures specified in TE07.38 but not TE07.37.

AS07.37: (Single-chip cryptographic modules – 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) over the manufacturers specified temperature range {*or AS07.38 shall be satisfied}*.**

Required Vendor Information

VE07.37.01: The vendor documentation shall state clearly that the approach specified in AS07.37 is used to meet the requirement.

VE07.37.02: The vendor documentation shall provide supporting detailed design information, especially the type of coating that is used and its characteristics.

Required Test Procedures

TE07.37.01: The tester shall verify by inspection and from the vendor documentation that the module is covered with a hard opaque tamper evident coating.

TE07.37.02: 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.

TE07.37.03: 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.

AS07.38: (Single-chip cryptographic modules – Levels 3 and 4)

***{If AS07.37 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)}*.**

NOTE This assertion is not separately tested. Tested in AS07.39.

AS07.39: (Single-chip cryptographic modules – Levels 3 and 4)

***{If AS07.37 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

VE07.39.01: 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.

VE07.39.02: 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

TE07.39.01: 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.

TE07.39.02: 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.

TE07.39.03: 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.

TE07.39.04: 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.

TE07.39.05: 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.

TE07.39.06: The tester shall test that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

AS07.40: (Single-chip cryptographic modules – Level 4)

The following requirements shall apply to single-chip cryptographic modules for Security Level 4.

NOTE This assertion is tested in AS07.41 and AS07.42.

AS07.41: (Single-chip cryptographic modules – 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

VE07.41.01: The vendor documentation shall clearly identify the kind of coating used and shall provide details of its characteristics, especially hardness and removal resistance.

VE07.41.02: 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

TE07.41.01: The tester shall verify by inspection and from the vendor documentation that the module is covered with a hard, opaque removal-resistant coating.

TE07.41.02: 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.

AS07.42: (Single-chip cryptographic modules – 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

VE07.42.01: 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

TE07.42.01: The tester shall verify the vendor documentation to determine the solvency properties of the modules removal-resistant coating.

TE07.42.02: The tester shall test the solvency properties of the modules removal-resistant coating. The tester, based on documentation provided in VE07.32.01, shall verify what type of solvent would be required to compromise the removal-resistant coating.

6.7.3.2 Multiple-chip embedded cryptographic modules

NOTE In addition to the general security requirements specified in 7.7.2 of ISO/IEC 19790:2012, the following requirements AS07.43 to AS07.58 are specific to multiple-chip embedded cryptographic modules.

AS07.43: (Multiple chip embedded cryptographic modules – 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

VE07.43.01: 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

TE07.43.01: 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.

AS07.44: (Multiple chip embedded cryptographic modules – Levels 2, 3, and 4)

The following requirements *{AS07.45 through AS 07.46}* shall apply to multiple-chip embedded cryptographic modules for Security Level 2 *{and the assertions AS07.45 through AS 07.46 shall be satisfied in the following groups: (AS07.45) or (AS07.46 and AS07.47) or (AS07.46 and AS07.48)}*.

Required Vendor Information

VE07.44.01: The vendor documentation shall specify that either (AS07.45) or (AS07.46 and (AS07.47 or AS07.48)) are satisfied.

Required Test Procedures

TE07.44.01: The tester shall verify by inspection and from the vendor documentation that either (AS07.45) or (AS07.46 and (AS07.47 or AS07.48)) are satisfied.

AS07.45: (Multiple chip embedded cryptographic modules – 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 and to provide evidence of attempts to tamper with or remove module components *{or the groups (AS07.46 and AS07.47) or (AS07.46 and AS07.48) shall be satisfied}*.

Required Vendor Information

VE07.45.01: 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

TE07.45.01: The tester shall verify by inspection and from the vendor documentation that the module is encapsulated with an opaque, tamper-evident material.

TE07.45.02: The tester shall verify by testing that the module provides evidence of attempts to tamper with or remove module components.

AS07.46: (Multiple chip embedded cryptographic modules – Levels 2, 3, and 4)

***{If AS07.45 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 (AS07.47 and AS07.48) or (AS07.47 and AS07.49) shall be satisfied}*.**

Required Vendor Information

VE07.46.01: 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

TE07.46.01: The tester shall verify by inspection and from the vendor documentation that the module is contained within an enclosure that meets the following requirements:

a) The enclosure has to completely surround the entire module.

b) The enclosure material has to be of a composition defined in the vendor documentation.

c) 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.

AS07.47: (Multiple chip embedded cryptographic modules – Levels 2, 3, and 4)

{If AS07.45 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 *{or AS07.48 shall be satisfied}*.**

Required Vendor Information

VE07.47.01: 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

TE07.47.01: 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.

TE07.47.02: 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.

AS07.48: (Multiple chip embedded cryptographic modules – Levels 2, 3, and 4)

{If AS07.45 is not satisfied and the enclosure includes any doors or removable covers without matching AS07.47, then they(i.e. the doors or removable covers)} **shall be protected with tamper-evident seals (e.g. evidence tape or holographic seals) *{and the group (AS07.47 and AS07.49) shall be satisfied}*.**

Required Vendor Information

VE07.48.01: The vendor documentation shall describe the tamper-evident seals.

Required Test Procedures

TE07.48.01: 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.

TE07.48.02: 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.

AS07.49: (Multiple chip embedded cryptographic modules – Levels 3 and 4)

The following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 3.

NOTE This assertion is tested in AS07.50 or AS07.51.

AS07.50: (Multiple chip embedded cryptographic modules – 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) *{or AS07.51 shall be satisfied}* 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).**

Required Vendor Information

VE07.50.01: The vendor documentation shall provide design documentation for the hard coating or potting material.

VE07.50.02: The vendor documentation shall provide documentation regarding the opacity characteristics of the hard coating or potting material.

Required Test Procedures

TE07.50.01: The tester shall verify that the vendor documentation specifies the hard coating or potting material.

TE07.50.02: The tester shall verify by inspection and from the vendor documentation the opacity characteristics of the hard coating or potting material.

TE07.50.03: 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.

AS07.51: (Multiple chip embedded cryptographic modules – Levels 3 and 4)

***{If AS07.50 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).**

Required Vendor Information

VE07.51.01: 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).

VE07.51.02: 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

TE07.51.01: 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.

TE07.51.02: 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.

TE07.51.03: The tester shall verify that the vendor documentation specifies which requirement option in VE07.51.01 and VE07.51.02 is implemented and provides design documentation.

TE07.51.04: 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.

TE07.51.05: 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.

TE07.51.06: 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.

TE07.51.07: 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.

TE07.51.08: 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.

TE07.51.09: The tester shall test that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

AS07.52: (Multiple chip embedded cryptographic modules – Level 4)

The following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 4.

NOTE This assertion is tested in AS07.53 through AS07.59.

AS07.53: (Multiple chip embedded cryptographic modules – Level 4)

The module components shall be within a strong or hard conformal or non-conformal enclosure.

Required Vendor Information

VE07.53.01: 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

TE07.53.01: 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.

AS07.54: (Multiple chip embedded cryptographic modules – Level 4)

The enclosure shall be encapsulated by a tamper detection envelope (e.g. a flexible mylar 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, burning, melting, or dissolving of the potting material or enclosure to an extent sufficient for accessing SSPs}*****.**

NOTE This assertion is not separately tested. Tested in AS07.55.

AS07.55: (Multiple chip embedded cryptographic modules – Level 4)

{The enclosure shall be encapsulated by a tamper detection envelope (e.g. a flexible mylar 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, burning, melting, or dissolving of the potting material or enclosure to an extent sufficient for accessing SSPs.**

Required Vendor Information

VE07.55.01: 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

TE07.55.01: The tester shall verify from 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.

AS07.56: (Multiple chip embedded cryptographic modules – Level 4)

The module shall contain tamper response and zeroisation circuitry *{that shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroise all unprotected SSPs}.*

NOTE This assertion is not separately tested. Tested in AS07.57 and AS07.58.

AS07.57: (Multiple chip embedded cryptographic modules – Level 4)

***{The module shall contain tamper response and zeroisation circuitry}* that shall continuously monitor the tamper detection envelope *{and, upon the detection of tampering, shall immediately zeroise all unprotected SSPs}*.**

Required Vendor Information

VE07.57.01: 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

TE07.57.01: 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.

AS07.58: (Multiple chip embedded cryptographic modules – Level 4)

***{The module shall contain tamper response and zeroisation circuitry that shall continuously monitor the tamper detection envelope }* and upon the detection of tampering, shall immediately zeroise all unprotected SSPs.**

Required Vendor Information

VE07.58.01: 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

TE07.58.01: The tester shall breach the tamper detection envelope barrier and then verify that the module zeroises all plaintext CSPs.

AS07.59: (Multiple chip embedded cryptographic modules – Level 4)

The tamper response circuitry shall remain operational when unprotected SSPs are contained within the cryptographic module.

NOTE This assertion is not separately tested.

6.7.3.3 Multiple-chip standalone cryptographic modules

NOTE In addition to the general security requirements specified in 7.7.2 of ISO/IEC 19790:2012, the following requirements AS07.60 to AS07.71 are specific to multiple-chip standalone cryptographic modules.

AS07.60: (Multiple-chip standalone cryptographic modules – Levels 1, 2, 3, and 4)

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

VE07.60.01: 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

TE07.60.01: The tester shall verify by inspection and from the vendor documentation that the module is contained within an enclosure that meets the following requirements:

a) The enclosure has to completely surround the entire module.

b) The enclosure material has to be of a composition defined in the vendor documentation.

c) 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.

AS07.61: (Multiple-chip standalone cryptographic modules – Levels 2, 3, and 4)

The following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 2.

NOTE This assertion is tested in AS07.62 or AS07.63.

AS07.62: (Multiple-chip standalone cryptographic modules – 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 AS07.63 shall apply}*.

Required Vendor Information

VE07.62.01: 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

TE07.62.01: 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.

AS07.63: (Multiple-chip standalone cryptographic modules – Levels 2, 3, and 4)

{If AS07.62 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

VE07.63.01: 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

TE07.63.01: 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.

AS07.64: (Multiple-chip standalone cryptographic modules – Levels 3 and 4)

The following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 3.

NOTE This assertion is tested in AS07.65.

AS07.65: (Multiple-chip standalone cryptographic modules – Levels 3 and 4)

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).

Required Vendor Information

VE07.65.01: 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).

VE07.65.02: 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

TE07.65.01: 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.

TE07.65.02: 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.

TE07.65.03: The tester shall verify that the vendor documentation specifies which requirement option in VE07.51.01 and VE07.51.02 is implemented and provides design documentation.

TE07.65.04: 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.

TE07.65.05: 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.

TE07.65.06: 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.

TE07.65.07: 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.

TE07.65.08: 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.

TE07.65.09: The tester shall test that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

AS07.66: (Multiple-chip standalone cryptographic modules – Level 4)

The following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 4.

NOTE This assertion is tested in AS07.67 through AS07.72.

AS07.67: (Multiple-chip standalone cryptographic modules – Level 4)

The enclosure of the cryptographic module shall contain a tamper detection envelope that use 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 in *{ISO/IEC 19790:2012 subclause}* 7.7.3.2 Security Level 4.

Required Vendor Information

VE07.67.01: 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

TE07.67.01: 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.

AS07.68: (Multiple-chip standalone cryptographic modules – Level 4)

The tamper detection mechanisms shall respond to attacks such as cutting, drilling, milling, grinding, burning, melting, or dissolving to an extent sufficient for accessing SSPs.

NOTE This assertion is tested as part of AS07.71.

AS07.69: (Multiple-chip standalone cryptographic modules – 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 unprotected SSPs}*.

NOTE This assertion is tested as part of AS07.71.

AS07.70: (Multiple-chip standalone cryptographic modules – 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 unprotected SSPs}*.**

NOTE This assertion is tested as part of AS07.71.

AS07.71: (Multiple-chip standalone cryptographic modules – 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 unprotected SSPs.**

Required Vendor Information

VE07.71.01: 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 SSPs. The circuitry shall be operational whenever plaintext SSPs are contained within the module. The vendor documentation shall describe the tamper response and zeroisation design.

Required Test Procedures

TE07.71.01: 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 SSPs.

TE07.71.02: The tester shall breach the tamper detection envelope barrier and then verify that the module zeroises all t plaintext SSPs.

AS07.72: (Multiple-chip standalone cryptographic modules – Level 4)

The tamper response and zeroisation capability shall remain operational when unprotected SSPs are contained within the cryptographic module.

NOTE This assertion is tested as part of AS07.71.

6.7.4 Environmental failure protection/testing

6.7.4.1 Environmental failure protection/testing general requirements

NOTE A cryptographic module is not required to employ environmental failure protection features or undergo environmental failure testing for Security Levels 1 and 2.

AS07.73: (Environmental failure protection/testing – Levels 3 and 4)

A module shall either employ environmental failure protection (EFP) features ***{AS07.75 to AS07.77}*** **or undergo environmental failure testing (EFT)** ***{AS07.78 to AS07.84}*****.**

Required Vendor Information

VE07.73.01: The vendor shall use either of the following:

a) EFP features; or

b) EFT

as specified in 7.7.4 of ISO/IEC 19790:2012, 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

TE07.73.01 The tester shall verify that the documentation states EFP/EFT selection for each condition and how the specified approach is used.

AS07.74: (Environmental failure protection/testing – Level 4)

A module shall employ environmental failure protection (EFP) features.

NOTE This assertion is tested in AS07.75 through AS07.77.

6.7.4.2 Environmental failure protection features

AS07.75: (Environmental failure protection features – Levels 3 and 4)

Environmental failure protection (EFP) features shall protect a cryptographic module against unusual environmental conditions (accidental or induced) when outside of the module's normal operating range that can compromise the security of the module.

NOTE This assertion is tested as part of AS07.77.

AS07.76: (Environmental failure protection features – Levels 3 and 4)

The cryptographic module shall monitor and correctly respond when operating temperature and voltage are outside of the specified normal operating ranges.

NOTE This assertion is tested as part of AS07.77.

AS07.77: (Environmental failure protection features – Levels 3 and 4)

If the temperature or voltage falls outside of the cryptographic module's normal operating range, the protection capability shall either:

— **shutdown the module to prevent further operation,**

or

— **immediately zeroise all unprotected SSPs.**

Required Vendor Information

VE07.77.01: 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:

a) Shut down the module; or

b) Zeroise all plaintext SSPs

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

TE07.77.01: 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.

TE07.77.02: 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 SSPs.

TE07.77.03: If the module is designed to zeroise all plaintext SSPs, 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.

6.7.4.3 Environmental failure testing procedures

AS07.78: (Environmental failure testing procedures – Levels 3 and 4)

Environmental failure testing (EFT) shall involve a combination of analysis, simulation, and testing of a cryptographic module to provide reasonable assurance that the environmental conditions (accidental or induced) when 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 AS07.81.

AS07.79: (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 AS07.81.

AS07.80: (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 AS07.81.

AS07.81: (Environmental failure testing procedures – Level 4)

The temperature range to be tested shall be from a temperature within the normal operating temperature range to the lowest (i.e. coldest) temperature that either (1) shutdown the module to prevent further operation or (2) immediately zeroise all unprotected SSPs; and from a temperature within the normal operating temperature range to the highest (i.e. hottest) temperature that either (1) shuts down or goes into an error state or (2) zeroises all unprotected SSPs.

Required Vendor Information

VE07.81.01: If EFT is chosen for a particular condition, the module shall be tested within the temperature and voltage ranges specified in AS07.82. The module shall either:

a) Continue to operate normally; or

b) Shut down; or

c) Zeroise all plaintext SSPs

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

Required Test Procedures

TE07.81.01: The tester shall configure the environmental condition (ambient temperature and voltage) as specified in AS07.82, and verify that the module either continues to operate normally, or shuts down to prevent further operations, or zeroises all plaintext SSPs.

TE07.81.02: If the module is designed to zeroise all plaintext SSPs, 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.

AS07.82: (Environmental failure testing procedures – Level 4)

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 unprotected SSPs are immediately zeroised or (3) the module enters a failure state}*.

NOTE This assertion is tested as part of AS07.81.

AS07.83: (Environmental failure testing procedures – Level 4)

***{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 unprotected SSPs are immediately zeroised or (3) the module enters a failure state.**

NOTE This assertion is tested as part of AS07.81.

AS07.84: (Environmental failure testing procedures – Level 4)

Temperature shall be monitored internally at the sensitive components and critical devices and not just at the physical boundary of the module.

NOTE This assertion is tested as part of AS07.81.

AS07.85: (Environmental failure testing procedures – Level 4)

The voltage range tested shall be gradually decreasing from a voltage within the normal operating voltage range to a lower voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroises all unprotected SSPs; *{and shall be gradually increasing from a voltage within the normal operating voltage range to a higher voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroises all unprotected SSPs}*.

NOTE This assertion is tested as part of AS07.81.

AS07.86: (Environmental failure testing procedures – Level 4)

***{The voltage range tested shall be gradually decreasing from a voltage within the normal operating voltage range to a lower voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroises all unprotected SSPs;}* and shall be gradually increasing from a voltage within the normal operating voltage range to a higher voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroises all unprotected SSPs.**

NOTE This assertion is tested as part of AS07.81.

6.8 Non-invasive security

AS08.01: (Non-invasive security – Levels 1, 2, 3, and 4)

Non-invasive attack mitigation techniques implemented by the cryptographic module to protect the module's SSPs that are not referenced in *{ISO/IEC 19790:2012}* Annex F shall meet the requirements in *{ISO/IEC 19790:2012 subclause}* 7.12.

NOTE This assertion is not separately tested. It is tested as part of AS12.01 through AS12.04.

AS08.02: (Non-invasive security – Levels 1, 2, 3, and 4)

Non-invasive attack mitigation techniques implemented by the cryptographic module to protect the module's SSPs that are referenced in *{ISO/IEC 19790:2012}* Annex F shall meet the following requirements.

NOTE This assertion is not separately tested.

AS08.03: (Non-invasive security – Levels 1, 2, 3, and 4)

The documentation requirements specified in *{ISO/IEC 19790:2012 Annex}* A.2.8 shall be provided.

Required Vendor Information

VE08.03.01: The vendor shall provide the documentation requirements as specified in A.2.8 of ISO/IEC 19790:2012.

Required Test Procedures

TE08.03.01: The tester shall verify that the vendor provides documentation as specified in A.2.8 of ISO/IEC 19790:2012.

AS08.04: (Non-invasive security – Levels 1, 2, 3, and 4)

Documentation shall specify all of the mitigation techniques employed to protect the module's CSPs from the non-invasive attack mitigation techniques referenced in *{ISO/IEC 19790:2012}* Annex F.

Required Vendor Information

VE08.04.01: The vendor shall provide supporting documentation which specifies all of the mitigation techniques employed to protect the module's CSPs from the non-invasive attacks specified in *{ISO/IEC 19790:2012}* Annex F.

Required Test Procedures

TE08.04.01: The tester shall verify that the vendor provides supporting documentation which specifies all of the mitigation techniques employed to protect the module's CSPs from the non-invasive attacks specified in *{ISO/IEC 19790:2012}* Annex F.

AS08.05: (Non-invasive security – Levels 1, 2, 3, and 4)

Documentation shall include evidence of the effectiveness of each of the attack mitigation techniques.

Required Vendor Information

VE08.05.01: The vendor shall specify in the documentation the effectiveness of the mitigation techniques.

Required Test Procedures

TE08.05.01: The tester shall verify that the vendor provides documentation that specifies the effectiveness of the mitigation techniques.

AS08.06: (Non-invasive security – Level 3)

The cryptographic module shall be tested to meet the approved non-invasive attack mitigation test metrics for Security Level 3 as specified in *{ISO/IEC 19790:2012}* Annex F.

Required Vendor Information

VE08.06.01: The vendor shall provide documentation that the module meets the approved non-invasive mitigation methods for Security Level 3.

Required Test Procedures

TE08.06.01: The tester shall verify that the vendor provides documentation that the module meets the approved non-invasive mitigation methods for Security Level 3.

AS08.07: (Non-invasive security – Level 4)

The cryptographic module shall be tested to meet the approved non-invasive attack mitigation test metrics for Security Level 4 as specified in *{ISO/IEC 19790:2012}* Annex F.

Required Vendor Information

VE08.07.01: The vendor shall provide documentation that the module meets the approved non-invasive mitigation methods for Security Level 4.

Required Test Procedures

TE08.07.01: The tester shall verify that the vendor provides documentation that the module meets the approved non-invasive mitigation methods for Security Level 4.

6.9 Sensitive security parameter management

6.9.1 Sensitive security parameter management general requirements

AS09.01: (Sensitive security parameter management – Levels 1, 2, 3, and 4)

CSPs shall be protected within the module from unauthorised access, use, disclosure, modification, and substitution.

Required Vendor Information

VE09.01.01: 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 access, use, disclosure, modification, and substitution.

Required Test Procedures

TE09.01.01: 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 access, use, disclosure, modification, and substitution.

TE09.01.02: The tester shall 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.

TE09.01.03: The tester shall attempt to modify CSPs using any method not specified by the vendor documentation.

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.

AS09.02: (Sensitive security parameter management – Levels 1, 2, 3, and 4)

PSPs shall be protected within the module against unauthorised modification and substitution.

Required Vendor Information

VE09.02.01: The vendor documentation shall describe the protection of all PSPs against unauthorised modification and substitution.

Required Test Procedures

TE09.02.01: The tester shall verify that the vendor documentation describe how the PSPs are protected from unauthorised modification, and substitution.

TE09.02.02: The tester shall attempt to modify all PSPs using any method not specified by the vendor documentation and shall attempt to enter them into the module.

AS09.03: (Sensitive security parameter management – Levels 1, 2, 3, and 4)

A module shall associate an SSP which is generated, entered into or output from the module with the entity (i.e. person, group, role, or process) to which the SSP is assigned.

Required Vendor Information

VE09.03.01: The documented SSP procedures shall describe the mechanisms or procedures used to ensure that each SSP is associated with the correct entity.

Required Test Procedures

TE09.03.01: The tester shall verify the documented SSP entry/output procedures that the procedures address how an entered or output SSP is associated with the correct entity.

TE09.03.02: For each SSP that can be entered, the tester shall first enter the SSP while assuming the correct entity. The tester shall then verify that entry is not possible when assuming an incorrect entity.

TE09.03.03: For each SSP that can be output, the tester shall first output the SSP while assuming the correct entity. The tester shall then verify that output is not possible when assuming an incorrect entity.

AS09.04: (Sensitive security parameter management – Levels 1, 2, 3, and 4)

Hash values of passwords, RBG state information and intermediate key generation values shall be considered CSPs.

Required Vendor Information

VE09.04.01: The vendor shall provide documentation that hash values of passwords, RBG state information and intermediate key generation values are defined as CSPs.

Required Test Procedures

TE09.04.01: The tester shall verify that the vendor provides documentation that hash values of passwords, RBG state information and intermediate key generation values are defined as CSPs.

TE09.04.02: The tester shall verify that the vendor provided Security Policy defines any hash values of passwords, RBG state information and intermediate key generation values are defined as CSPs.

AS09.05: (Sensitive security parameter management – Levels 1, 2, 3, and 4)

The documentation requirements specified in *{ISO/IEC 19790:2012 Annex}* A.2.9 shall be provided.

Required Vendor Information

VE09.05.01: The vendor shall provide the documentation requirements as specified in A.2.9 of ISO/IEC 19790:2012.

Required Test Procedures

TE09.05.01: The tester shall verify that the vendor provides documentation as specified in A.2.9 of ISO/IEC 19790:2012.

6.9.2 Random bit generators

NOTE A cryptographic module may contain RBGs, a chain of RBGs, or may be solely an RBG.

AS09.06: (Random bit generators – Levels 1, 2, 3, and 4)

If an approved security function, SSP generation or SSP establishment method requires random values, then an approved RBG shall be used to provide these values.

NOTE Approved RBGs are listed in ISO/IEC 19790:2012, Annex C.

Required Vendor Information

VE09.06.01: The vendor shall provide the list of all RBGs used in approved security functions, SSP generation or SSP establishment methods within the cryptographic module and their precise usage.

VE09.06.02: The vendor shall provide documentation that any random values used by approved security functions, SSP generation or SSP establishment method are provided from an approved RBG.

Required Test Procedures

TE09.06.01: The tester shall verify that all RBGs used by approved security functions, SSP generation or SSP establishment methods are documented and their usage defined.

TE09.06.02: The tester shall verify from the vendor provided documentation that the implemented RBGs used by approved security functions, SSP generation or SSP establishment methods are compliant with the approved RBGs listed in ISO/IEC 19790:2012, Annex C.

TE09.06.03: The tester shall verify from the vendor provided documentation that any random values used by approved security functions, SSP generation or SSP establishment method are provided from an approved RBG.

AS09.07: (Random bit generators – Levels 1, 2, 3, and 4)

If entropy is collected from outside the cryptographic boundary of the module, the data stream generated using this entropy input shall be considered a CSP.

Required Vendor Information

VE09.07.01: The vendor shall provide documentation that the input datastream generated from entropy collected from outside the cryptographic module's boundary is defined as a CSP.

Required Test Procedures

TE09.07.01: The tester shall verify that the vendor provides documentation that the input datastream generated from entropy collected from outside the cryptographic module's boundary is defined as a CSP.

6.9.3 Sensitive security parameter generation

AS09.08: (Sensitive security parameter generation – Levels 1, 2, 3, and 4)

Compromising the security of the SSP generation method which uses the output of an approved RBG (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 SSP.

Required Vendor Information

VE09.08.01: The vendor shall provide documentation that provides rationale stating how compromising the security of the SSP 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 SSP.

Required Test Procedures

TE09.08.01: The tester shall verify that the vendor provided documentation that provides rationale stating how compromising the security of the SSP 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 SSP.

TE09.08.02: 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.

AS09.09: (Sensitive security parameter generation – Levels 1, 2, 3, and 4)

SSPs generated by the module from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function or SSP establishment method shall be generated using an approved SSP generation method listed in *{ISO/IEC 19790:2012}* Annex D.

NOTE Approved sensitive security parameter generation methods are listed in ISO/IEC 19790:2012, Annex D.

Required Vendor Information

VE09.09.01: The vendor shall provide the list of all SSPs generated by the module from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function or SSP establishment methods used in the cryptographic module and their precise usage.

VE09.09.02: The vendor shall provide documentation that SSPs generated by the module from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function or SSP establishment method are generated using an approved SSP generation method.

Required Test Procedures

TE09.09.01: The tester shall verify that all SSPs generated by the module from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function or SSP establishment methods are documented and their usage defined.

TE09.09.02: The tester shall verify from the vendor provided documentation that the implemented SSPs generated by the module from either the output of an approved RBG or derived from an SSP entered into the module and used by an approved security function or SSP establishment methods are compliant with the approved SSP generation methods listed in ISO/IEC 19790:2012, Annex D.

6.9.4 Sensitive security parameter establishment

NOTE Sensitive establishment may consist of automated SSP transport or SSP agreement methods or manual SSP entry or output or output via direct or electronic methods.

AS09.10: (Sensitive security parameter establishment – Levels 1, 2, 3, and 4)

Automated SSP establishment shall use an approved method listed in *{ISO/IEC 19790:2012 }* Annex D.

NOTE Approved sensitive security parameter establishment methods are listed in ISO/IEC 19790:2012, Annex D.

Required Vendor Information

VE09.10.01: The vendor shall provide the list of all automated SSP establishment methods used in the cryptographic module and their precise usage.

Required Test Procedures

TE09.10.01: The tester shall verify that all automated SSP establishment methods are documented and their usage defined.

TE09.10.02: The tester shall verify from the vendor provided documentation that the implemented automated SSP establishment methods are compliant with the approved automated SSP establishment methods listed in ISO/IEC 19790:2012, Annex D.

AS09.11: (Sensitive security parameter establishment – Levels 1, 2, 3, and 4)

Manual SSP establishment shall meet the requirements of *{ISO/IEC 19790:2012 subclause}* 7.9.5.

NOTE This assertion is tested as part of AS09.12 through AS09.24.

6.9.5 Sensitive security parameter entry and output

NOTE Sensitive security parameters may be manually entered into or output from a module either *directly* (e.g. entered via a keyboard or number pad, or output via a visual display) or *electronically* (e.g. via a smart card/tokens, PC card, other electronic key loading device, or the module operating system).

AS09.12: (Sensitive security parameter entry and output – Levels 1, 2, 3, and 4)

If SSPs are manually entered into or output from a module, the entry or output shall be through the defined HMI, SFMI, HFMI or HSMI (*{ISO/IEC 19790:2012 subclause}* 7.3.2) interfaces.

NOTE This assertion is tested as part of AS03.04 through AS03.14.

AS09.13: (Sensitive security parameter entry and output – Levels 1, 2, 3, and 4)

All cryptographically protected SSPs, entered into or output from the module shall be encrypted using an approved security function.

Required Vendor Information

VE09.13.01: The vendor documentation shall specify all cryptographically protected SSPs which are entered into or output from the cryptographic module.

VE09.13.02: The vendor documentation shall state the encryption method used to cryptographically protect the SSPs which are entered into or output from the cryptographic module.

Required Test Procedures

TE09.13.01: The tester shall verify that the vendor has provided documentation specifying all the cryptographically protected SSPs which are entered into and output from the cryptographic module.

TE09.13.02: The tester shall verify that the vendor has provided documentation specifies the encryption method used to cryptographically protect the SSPs which are entered into or output from the cryptographic module.

TE09.13.03: The tester shall verify that the encryption method used to cryptographically protect the SSPs which are entered into or output from the cryptographic module is performed using an approved security funciton.

NOTE For directly entered SSPs, the entered values may be temporarily displayed to allow visual verification and to improve accuracy.

AS09.14: (Sensitive security parameter entry and output – Levels 1, 2, 3, and 4)

If encrypted SSPs are directly entered into the module, then the plaintext values of the SSPs shall not be displayed.

Required Vendor Information

VE09.14.01: The documented SSP entry mechanisms for encrypted SSPs shall preclude the display of their plaintext values.

Required Test Procedures

TE09.14.01: The tester shall verify the documented SSP entry mechanisms for encrypted SSPs precludes the display of their plaintext values during the encrypted SSP entry process.

TE09.14.02: The tester shall enter all encrypted SSPs and shall monitor the output interfaces of the module to verify that any resulting plaintext SSP values are not displayed.

AS09.15: (Sensitive security parameter entry and output – Levels 1, 2, 3, and 4)

Directly entered (plaintext or encrypted) SSPs shall be verified during entry into a module for accuracy using the conditional manual entry test specified in *{ISO/IEC 19790:2012 subclause }* 7.10.3.5.

NOTE This assertion is tested as part of AS10.42 through AS10.46.

AS09.16: (Sensitive security parameter entry and output – Levels 1, 2, 3, and 4)

To prevent the inadvertent output of sensitive information, two independent internal actions shall be required in order to output any plaintext CSP.

Required Vendor Information

VE09.16.01: If the module outputs any plaintext CSPs, the vendor documentation shall describe the output services.

VE09.16.02: The finite state model and other vendor documentation shall indicate, for the output of plaintext CSPs, that two independent internal actions that are required.

Required Test Procedures

TE09.16.01: The tester shall verify from the vendor documentation or finite state model that the module allows the output of plaintext CSPs.

TE09.16.02: The tester shall verify the finite state model and other vendor documentation that the output of plaintext CSPs requires two independent internal actions in order for the cryptographic module to output the plaintext CSPs.

TE09.16.03: The tester shall attempt to output plaintext CSPs without the module performing two independent internal actions. The module shall fail if the module allows the output of plaintext CSPs without two independent internal actions.

AS09.17: (Sensitive security parameter entry and output – Levels 1, 2, 3, and 4)

These two independent internal actions shall be dedicated to mediating the output of the CSPs.

NOTE This assertion is not separately tested. Tested as part of AS09.16.

AS09.18: (Sensitive security parameter entry and output – Levels 1, 2, 3, and 4)

For electronic entry or output via a wireless connection; CSPs, key components and authentication data shall be encrypted.

Required Vendor Information

VE09.18.01: If the module inputs or outputs CSPs, key components and authentication data via wireless interfaces, the vendor documentation shall describe the wireless services.

VE09.18.02: If the module inputs or outputs CSPs, key components and authentication data via wireless interfaces, the vendor documentation shall describe the encryption methods employed to encrypt the CSPs, key components and authentication data.

Required Test Procedures

TE09.18.01: The tester shall verify whether the module inputs or outputs CSPs, key components and authentication data via wireless interfaces.

TE09.18.02: The tester shall verify that the encryption methods employed to encrypt the CSPs, key components and authentication data are approved encryption methods.

NOTE For Security Levels 1 and 2, plaintext CSPs, key components and authentication data may be entered and output via physical port(s) and logical interface(s) shared with other physical ports and logical interfaces of the cryptographic module.

AS09.19: (Sensitive security parameter entry and output – Levels 1, and 2)

For software modules or the software components of a hybrid software module, CSPs, key components and authentication data may be entered into or output in either encrypted or plaintext form provided that the CSPs, key components and authentication data shall be maintained within the operational environment and meet the requirements of *{ISO/IEC 19790:2012 subclause}* 7.6.3.

Required Vendor Information

VE09.19.01: For software modules or the software components of a hybrid software module the vendor shall provide documentation that CSPs, key components and authentication data may be entered into or output in either encrypted or plaintext form provided that the CSPs, key components and authentication data are maintained within the operational environment and meet the requirements in 7.6.3 of ISO/IEC 19790:2012 *{AS06.05 through AS06.29 as applicable}*.

Required Test Procedures

TE09.19.01: For software modules or the software components of a hybrid software module the tester shall verify that the vendor provides documentation that CSPs, key components and authentication data may be entered into or output in either encrypted or plaintext form provided that the CSPs, key components and authentication data are maintained within the operational environment and meet the requirements in 7.6.3 of ISO/IEC 19790:2012 *{AS06.05 through AS06.29 as applicable}*.

AS09.20: (Sensitive security parameter entry and output – Levels 3, and 4)

CSPs, key components and authentication data shall be entered into or output from the module either encrypted or by a trusted channel.

NOTE This assertion is tested as part of AS09.13 or AS03.16 through AS03.22.

AS09.21: (Sensitive security parameter entry and output – Levels 3, and 4)

CSPs which are plaintext secret and private cryptographic keys shall be entered into or output from the module using split knowledge procedures using a trusted channel.

Required Vendor Information

VE09.21.01: The vendor shall supply documentation specifying the split knowledge procedures employed by the cryptographic module using a trusted channel for the input or output of plaintext secret and private cryptographic keys.

Required Test Procedures

TE09.21.01: The tester shall verify that the documentation specifying the split knowledge procedures employed by the cryptographic module using a trusted channel for the input or output of plaintext secret and private cryptographic keys matches the implementation.

TE09.21.02: The tester shall verify the split knowledge procedure splits the key into multiple key components, with each key component individually sharing no knowledge of the original key.

TE09.21.03: The tester shall verify that a subset of the split knowledge components or all components are required to be entered or output for each key.

TE09.21.04: The tester shall verify the trusted channel under AS03.16 through AS03.21 for Level 3 and AS03.22 for Level 4.

AS09.22: (Sensitive security parameter entry and output – Level 3)

If the module employs split knowledge procedures, the module shall employ separate identity-based operator authentication for entering or outputting each key component, *{and at least two key components shall be required to reconstruct the original cryptographic key}*.

Required Vendor Information

VE09.22.01: The vendor documentation shall specify that identity-based authentication is employed for each separate key component.

Required Test Procedures

TE09.22.01: The tester shall verify that identity-based authentication is employed for each separate key component.

AS09.23: (Sensitive security parameter entry and output – Level 3)

{If the module employs split knowledge procedures, the module shall employ separate identity-based operator authentication for entering or outputting each key component,} **and at least two key components shall be required to reconstruct the original cryptographic key.**

Required Vendor Information

VE09.23.01: The vendor documentation shall specify the number of components that are required to construct the original CSP.

Required Test Procedures

TE09.23.01: The tester shall verify in the vendor documentation that the split knowledge procedure requires at least two components to construct the original CSP.

TE09.23.02: The tester shall verify the vendor documentation that the output of CSPs under split knowledge procedures does not result in the output of a single component that can be used to construct the original CSP.

AS09.24: (Sensitive security parameter entry and output – Level 4)

The module shall employ multi-factor separate identity-based operator authentication for entering or outputting each key component.

Required Vendor Information

VE09.24.01: The vendor documentation shall specify that multi-factor identity-based authentication is employed for each separate key component.

Required Test Procedures

TE09.24.01: The tester shall verify that multi-factor identity-based authentication is employed for each separate key component.

TE09.24.02: The tester shall verify the mulit-factor authentication method under AS04.59.

6.9.6 Sensitive security parameter storage

AS09.25: (Sensitive security parameter storage – Levels 1, 2, 3, and 4)

A module shall associate every SSP stored within the module with the entity (e.g. operator, role, or process) to which the SSP is assigned.

Required Vendor Information

VE09.25.01: 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

TE09.25.01: The tester shall verify the documentation on key storage that the procedures address how a stored key is associated with the correct entity.

TE09.25.02: 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.

AS09.26: (Sensitive security parameter storage – Levels 1, 2, 3, and 4)

Access to plaintext CSPs by unauthorised operators shall be prohibited.

NOTE This assertion is tested under AS09.01.

AS09.27: (Sensitive security parameter storage – Levels 1, 2, 3, and 4)

Modification of PSPs by unauthorized operators shall be prohibited.

Required Vendor Information

VE09.27.01: The vendor shall provide documentation that modification of PSPs by unauthorized operators shall be prohibited.

Required Test Procedures

TE09.27.01: The tester shall verify that the vendor provides documentation that modification of PSPs by unauthorized operators shall be prohibited.

TE09.27.02: The tester shall assume an unauthorized role and attempt to modify PSPs stored within the module and verify that this attempt fails.

6.9.7 Sensitive security parameter zeroisation

AS09.28: (Sensitive security parameter zeroisation – Levels 1, 2, 3, and 4)

A module shall provide methods to zeroise all unprotected SSPs and key components within the module.

NOTE 1 This assertion is tested AS09.30.

NOTE 2 Temporarily stored SSPs and other stored values owned by the module should be zeroised when they are no longer needed for future use.

AS09.29: (Sensitive security parameter zeroisation – Levels 1, 2, 3, and 4)

A zeroised SSP shall not be retrievable or reusable.

Required Vendor Information

VE09.29.01: The vendor documentation shall specify how a zeroised SSP can not be retrievable or reusable.

Required Test Procedures

TE09.29.01: The tester shall verify that the vendor provides documentation specifies how a zeroised SSP can not be retrievable or reusable.

TE09.29.02: 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.

NOTE 1 Zeroisation of protected PSPs, encrypted CSPs, or CSPs otherwise physically or logically protected within an additional embedded validated module (meeting the requirements of this International Standard) is not required.

NOTE 2 SSPs need not meet these zeroisation requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialisation key).

AS09.30: (Sensitive security parameter zeroisation – Levels 2, 3, and 4)

The cryptographic module shall perform the zeroisation of unprotected SSPs (e.g. overwriting with all zeros or all ones or with random data).

Required Vendor Information

VE09.30.01: The vendor documentation shall specify the following SSPs zeroisation information:

a) Zeroisation techniques

b) Restrictions when plaintext SSPs can be zeroised

c) Plaintext SSPs that are zeroised

d) Plaintext SSPs 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 SSPs

Required Test Procedures

TE09.30.01: The tester shall verify the vendor documentation that the information specified in VE09.30.01 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.

TE09.30.02: 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 SSPs that were stored in the module. The tester shall verify that each plaintext SSPs cannot be accessed.

TE09.30.03: The tester shall initiate zeroisation and verify the key destruction method is performed in a time that is not sufficient to compromise plaintext SSPs.

TE09.30.04: The tester shall verify that all plaintext SSPs 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 19790:2012).

AS09.31: (Sensitive security parameter zeroisation – Levels 2, 3, and 4)

Zeroisation shall exclude the overwriting of an unprotected SSP with another unprotected SSP.

Required Vendor Information

VE09.31.01: The vendor documentation shall specify that the zeroisation excludes the overwriting of an unprotected SSP with another unprotected SSP.

Required Test Procedures

TE09.31.01: The tester shall verify that the vendor provided documentation specifies that the zeroisation excludes the overwriting of an unprotected SSP with another unprotected SSP.

AS09.32: (Sensitive security parameter zeroisation – Levels 2, 3, and 4)

Temporary SSPs shall be zeroised when they are no longer needed.

Required Vendor Information

VE09.32.01: The vendor documentation shall specify that temporary SSPs are zeroised when they are no longer needed.

Required Test Procedures

TE09.32.01: The tester shall verify that the vendor provides documentation specifies that temporary SSPs are zeroised when they are no longer needed.

AS09.33: (Sensitive security parameter zeroisation – Levels 2, 3, and 4)

The module shall provide an output status indication when the zeroisation is complete.

Required Vendor Information

VE09.33.01: The vendor documentation shall specify that the module provides an output status indication when the zeroisation is complete *{AS03.11}*.

Required Test Procedures

TE09.33.01: The tester shall verify that the vendor provides documentation that specifies that the module provides an output status indication when the zeroisation is complete.

TE09.33.02: The tester shall perform zeroisation and verify the status output indicator.

AS09.34: (Sensitive security parameter zeroisation – Level 4)

The following requirements *{ISO/IEC 19790:2012 AS09.35 through AS09.37}* shall be met:

NOTE This assertion is tested under AS09.35 through AS09.37.

AS09.35: (Sensitive security parameter zeroisation – Level 4)

Zeroisation shall be immediate and non-interruptible *{and shall occur in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time zeroisation is initiated and the actual zeroisation completed and {AS09.37 shall be met}}*.

NOTE This assertion is tested in AS09.36.

AS09.36: (Sensitive security parameter zeroisation – Level 4)

***{Zeroisation shall be immediate and non-interruptible}* and shall occur in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time zeroisation is initiated and the actual zeroisation completed and *{AS09.37 shall be met}*.**

Required Vendor Information

VE09.36.01: The vendor shall provide documentation that the module zeroisation is immediate and non-interruptible and occurs in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time zeroisation is initiated and the actual zeroisation completed.

Required Test Procedures

TE09.36.01: The tester shall verify that the vendor provides documentation that the module zeroisation is immediate and non-interruptible and occurs in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time zeroisation is initiated and the actual zeroisation completed.

TE09.36.02: The tester shall perform the module zeroisation. The test shall attempt to interrupt the zeroisation process to prevent its completion in whole or part.

AS09.37: (Sensitive security parameter zeroisation – Level 4)

All unprotected SSPs shall be zeroised whether plaintext or cryptographically protected, such that the module is returned to the factory state.

Required Vendor Information

VE09.37.01: The vendor shall provide documentation that all unprotected SSPs are zeroised whether plaintext or cryptographically protected, such that the module is returned to the factory state.

Required Test Procedures

TE09.37.01: The tester shall verify that the vendor provides documentation that all unprotected SSPs are zeroised whether plaintext or cryptographically protected, such that the module is returned to the factory state.

TE09.37.02: The tester shall perform the module zeroisation. The tester shall verify that the module has returned to the factory state.

6.10 Self-tests

6.10.1 Self-test general requirements

AS10.01: (Self-tests – Levels 1, 2, 3, and 4)

All self-tests shall be performed, *{and determination of pass or fail shall be made by the module, without external controls, externally provided input text vectors, expected output results, or operator intervention or whether the module will operate in an approved or non-approved mode}*.

NOTE This assertion is not separately tested.

AS10.02: (Self-tests – Levels 1, 2, 3, and 4)

***{All self-tests shall be performed,}* and determination of pass or fail shall be made by the module, without external controls, externally provided input text vectors, expected output results, or operator intervention or whether the module will operate in an approved or non-approved mode.**

NOTE This assertion is not separately tested.

AS10.03: (Self-tests – Levels 1, 2, 3, and 4)

The pre-operational self-tests shall be performed and passed successfully prior to the module providing any data output via the data output interface.

NOTE This assertion is tested as part of AS10.15.

AS10.04: (Self-tests – Levels 1, 2, 3, and 4)

Conditional self-tests shall be performed when an applicable security function or process is invoked (i.e. security functions for which self-tests are required).

NOTE 1 This assertion is tested as part of AS10.25.

NOTE 2 A cryptographic module may perform other power-up or conditional self-tests in addition to the tests specified in ISO/IEC 19790:2012.

AS10.05: (Self-tests – Levels 1, 2, 3, and 4)

All self-tests identified in underlying algorithmic standards (*{ISO/IEC 19790:2012}* Annexes C through E) shall be implemented as applicable within the cryptographic module.

NOTE This assertion is tested as part of AS10.26.

AS10.06: (Self-tests – Levels 1, 2, 3, and 4)

All self-tests identified in addition or in lieu of those specified in the underlying algorithmic standards (*{ISO/IEC 19790:2012}* Annexes C through E) shall be implemented as specified in *{ISO/IEC 19790:2012}* Annexes C through E for each approved security function, SSP establishment method and authentication mechanism.

NOTE This assertion is tested as part of AS10.26.

AS10.07: (Self-tests – Levels 1, 2, 3, and 4)

If a cryptographic module fails a self-test, the module shall enter an error state *{and shall output an error indicator as specified in {ISO/IEC 19790:2012 subclause} 7.3.3}*.

Required Vendor Information

VE10.07.01: For each error condition, the vendor documentation shall provide the condition name, description of the condition, the events that can produce the condition, and the actions necessary to clear the condition and resume normal operation.

Required Test Procedures

TE10.07.01: The tester shall verify the list of self-tests to include the following:

a) Pre-operational self-tests
    1) Pre-operational software/firmware integrity test
    2) Pre-operational bypass test
    3) Pre-operational critical functions test
b) Conditional self-tests
    1) Conditional cryptographic algorithm test
    2) Conditional pair-wise consistency test
    3) Conditional software/firmware load test
    4) Conditional manual entry test
    5) Conditional bypass test
    6) Conditional critical functions test

TE10.07.02: The tester shall check that the information provided above is specified for each error condition.

TE10.07.03: 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.

TE10.07.04: The tester shall verify that all self-tests are performed regardless if the cryptographic module operates in an approved mode or non-approved mode.

TE10.07.05: The tester shall verify by inspection and from the vendor documentation that determination of pass or fail of each self-test is made by the module, without external controls, externally provided input text vectors, expected output results, or operator intervention.

AS10.08: (Self-tests – Levels 1, 2, 3, and 4)

***{If a cryptographic module fails a self-test, the module shall enter an error state}* and shall output an error indicator as specified in *{ISO/IEC 19790:2012 subclause }* 7.3.3.**

Required Vendor Information

VE10.08.01: 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

TE10.08.01: 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 AS11.10) to verify that they agree.

TE10.08.02: By inspecting the vendor documentation that specifies how each self-test handles errors, the tester shall verify that:

a) The module enters an error state upon failing a self-test.

b) The error state is consistent with the documentation and the finite state model.

c) The module outputs an error indicator.

d) The error indicator is consistent with the documented error indicator.

TE10.08.03: The tester shall run each self-test 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.

AS10.09: (Self-tests – Levels 1, 2, 3, and 4)

The cryptographic module shall not perform any cryptographic operations or output control and data via the control and data output interface while in an error state.

Required Vendor Information

VE10.09.01: The vendor documentation requirements are specified under VE03.07.01, VE03.07.02, VE03.10.01 and VE03.10.02. The vendor design also shall ensure that cryptographic operations cannot be performed while the module is in the error state.

Required Test Procedures

TE10.09.01: The tester shall verify that the inhibition of control and data output was performed under TE03.07.01, TE03.07.02, TE03.10.01 and TE03.10.02. The results of the verification shall indicate that:

a) The vendor documentation shows that all control and data output via the control and data output interface is inhibited whenever the module is in an error state.

b) The module inhibits all control and data output when the module is in an error state.

TE10.09.02: The tester shall verify that the vendor documentation specifies that cryptographic functions are inhibited while the module is in an error state.

TE10.09.03: The tester shall cause the module to enter the error state and verify that any cryptographic operations that the tester attempts to initiate are prevented.

AS10.10: (Self-tests – Levels 1, 2, 3, and 4)

The cryptographic module shall not utilise any functionality that relies upon a function or algorithm that failed a self-test until the relevant self-test has been repeated and successfully passed.

Required Vendor Information

VE10.10.01: The vendor shall provide design documentation that the cryptographic module cannot utilise any functionality that relies upon a function or algorithm that failed a self-test until the relevant self-test has been repeated and successfully passed.

Required Test Procedures

TE10.10.01: The tester shall cause an error in a function or algorithm that failed a self-test and initiate a functionality that utilise the function or algorithm and verify that the module cannot utilise this functionality.

TE10.10.02: The tester shall run each self-test and cause the module to enter every error state or a degraded operation. The tester shall exercise the cryptographic module, and verify that the functionality cannot be utilised until the relevant self-test has been repeated and successfully passed.

AS10.11: (Self-tests – Levels 1, 2, 3, and 4)

If a module does not output an error status upon failure of a module self-test, the operator of the module shall be able to determine if the module has entered an error state implicitly through an unambiguous procedure documented in the security policy (*{ISO/IEC 19790:2012}* Annex B).

Required Vendor Information

VE10.11.01: If the module does not output an error status upon failure of the module self-test, the vendor provided non-proprietary security policy shall describe unambiguously the procedure to determine if the cryptographic module has entered an error state.

Required Test Procedures

TE10.11.01: The tester shall run each self-test and cause the module to enter every error state. The tester shall verify that the module has entered the error state implicitly through the procedure documented in the non-proprietary security policy.

AS10.12: (Self-tests – Levels 3, and 4)

The module shall maintain an error log that is accessible by an authorised operator of the module.

Required Vendor Information

VE10.12.01: The vendor documentation shall specify the error logging functionality of the module including types of recorded information in the error log (e.g. which self-test has failed, when the error occurred).

VE10.12.02: The vendor documentation shall describe the mechanism to maintain the integrity of the error log.

Required Test Procedures

TE10.12.01: The tester shall verify, from the vendor documentation, that an unauthorised operator cannot access to the error log.

TE10.12.02: The tester shall verify, from the vendor documentation, that the error logging functionality provides information, at a minimum, the most recent error event.

NOTE This TE is to cover assertion AS10.13.

TE10.12.03: The tester shall cause the cryptographic module to enter an error state and verify that the module generates the error log, at a minimum, for the most recent error event.

TE10.12.04: The tester shall access the error log without assuming any authenticated role supported by the cryptographic module. If the error log can be accessed, this assertion fails.

TE10.12.05: The tester shall exercise the cryptographic module, and verify that the error log is protected against unauthorised modification and substitution.

AS10.13: (Self-tests – Levels 3, and 4)

The error log shall provide information, at a minimum, the most recent error event (i.e. which self-test failed).

NOTE This assertion is tested as part of AS10.12.

AS10.14: (Self-tests – Levels 1, 2, 3, and 4)

The documentation requirements specified in *{ISO/IEC 19790:2012 Annex}* A.2.10 shall be provided.

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

6.10.2 Pre-operational self-tests

6.10.2.1 Pre-operational self-test general requirements

AS10.15: (Pre-operational self-tests – Levels 1, 2, 3, and 4)

The pre-operational tests shall be performed and passed successfully by a cryptographic module between the time a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.) and before the module transitions to the operational state.

Required Vendor Information

VE10.15.01: The vendor documentation shall provide the information for each of the pre-operational self-tests.

VE10.15.02: The vendor shall provide the sequence of pre-operational self-tests between the time the module is powered on or instantiated and before the module transitions to the operational state.

Required Test Procedures

TE10.15.01: The tester shall verify that the vendor documentation specifies each pre-operational self-test. The tester shall verify that the pre-operational self-tests are performed as specified.

TE10.15.02: By checking the code and/or design documentation, the tester shall verify each pre-operational test is performed and passed successfully between the time a cryptographic module is powered on or instantiated and before the module transitions to the operational state.

AS10.16: (Pre-operational self-tests – Levels 1, 2, 3, and 4)

A cryptographic module shall perform the following pre-operational tests, as applicable:

- **pre-operational software/firmware integrity test;**
- **pre-operational bypass test; and**
- **pre-operational critical functions test.**

NOTE This assertion is tested as part of AS10.17 to AS10.24.

6.10.2.2 Pre-operational software/firmware integrity test

AS10.17: (Pre-operational software/firmware integrity test – Levels 1, 2, 3, and 4)

All software and firmware components within the cryptographic boundary shall be verified using an approved *integrity technique* satisfying the requirements defined in *{ISO/IEC 19790:2012 subclause}* 7.5.

Required Vendor Information

VE10.17.01: The vendor documentation shall describe the approved integrity technique employed by the cryptographic module to verify the integrity of all software and firmware components within the cryptographic boundary.

VE10.17.02: The vendor documentation shall describe whether the approved integrity technique is implemented either by the cryptographic module itself or by another validated cryptographic module operating in an approved mode of operation.

VE10.17.03: The vendor documentation shall describe the implemented integrity mechanism.

VE10.17.04: The vendor shall provide a validation certificate for the approved integrity technique as specified in VE02.20.01.

Required Test Procedures

TE10.17.01: The tester shall verify that the vendor has provided a validation certificate for the approved integrity technique implemented as specified in VE02.20.01.

TE10.17.02: If the module implements a hash or MAC for the software/firmware integrity test, the tester shall verify that the vendor documentation of the software/firmware integrity test fully describes the process by which the hash or MAC is calculated and verified.

TE10.17.03: If the module implements an approved digital signature for the software/firmware integrity test, the tester shall verify that the vendor documentation of the software/firmware integrity test includes the following:

a) Specification of the approved digital signature algorithm implemented.

b) Identification of software and firmware that is protected using the approved digital signatures.

c) Verification that the pre-calculated value of the approved digital signature is included with the software or firmware.

d) Verification of the approved digital signature.

e) Failure of the self-test upon failure of the approved digital signature verification.

TE10.17.04: If the module implements the approved integrity technique, by checking the code and/or design documentation, the tester shall verify that the implementation of the software/firmware integrity test is consistent with TE10.17.01, TE10.17.02, and TE10.17.03.

TE10.17.05: Even if the approved integrity technique is provided by another validated module, the tester shall verify that the determination of pass or fail of the software/firmware integrity test is made as specified in AS10.01.

TE10.17.06: The tester shall modify the cryptographic software and firmware components. This test fails if the integrity mechanisms do not detect the modifications.

AS10.18: (Pre-operational software/firmware integrity test – Levels 1, 2, 3, and 4)

If the verification fails, the pre-operational software/firmware integrity test shall fail.

NOTE This assertion is not tested separately.

AS10.19: (Pre-operational software/firmware integrity test – Levels 1, 2, 3, and 4)

If a hardware module does not contain either software or firmware, the module shall, at a minimum, implement one cryptographic algorithm self-test as specified in *{ISO/IEC 19790:2012 subclause }* 7.10.3.2 as a pre-operational self-test.

NOTE This assertion is not tested separately.

AS10.20: (Pre-operational software/firmware integrity test – Levels 1, 2, 3, and 4)

A cryptographic algorithm that is used to perform the approved integrity technique for the pre-operational software/firmware test shall first pass the cryptographic algorithm self-test specified in *{ISO/IEC 19790:2012 subclause }* 7.10.3.2.

Required Vendor Information

VE10.20.01: The vendor documentation requirement is specified under VE10.15.02.

Required Test Procedures

TE10.20.01: By checking the codes and/or design documentation, the tester shall verify that the cryptographic algorithm test used to perform the approved integrity technique is passed before the pre-operational software/firmware integrity test starts.

6.10.2.3 Pre-operational bypass test

AS10.21: (Pre-operational bypass test – Levels 1, 2, 3, and 4)

If a cryptographic module implements a *bypass* capability, then the module shall ensure the correct operation of the logic governing activation of the bypass capability by exercising that logic.

Required Vendor Information

VE10.21.01: The vendor documentation shall specify how the cryptographic module ensures the correct operation of the logic governing activation of the bypass capability.

Required Test Procedures

TE10.21.01: The tester shall verify from the vendor documentation and by inspection of the module that the logic governing activation of the bypass capability is implemented as specified.

TE10.21.02: The tester shall verify by inspection and from the vendor documentation that the pre-operational bypass test is implemented which exercises the logic governing activation of the bypass capability.

TE10.21.03: The tester shall cause each error condition of the pre-operational bypass test to occur, and shall verify that the inhibition of output was performed under TE03.07.01 through TE03.07.05 and TE03.10.01 through TE03.10.05.

TE10.21.04: The tester shall run the pre-operational bypass test, and shall verify that any functionality relies on the logic governing activation of the bypass capability cannot be utilised under TE10.10.01, TE10.10.02.

AS10.22: (Pre-operational bypass test – Levels 1, 2, 3, and 4)

The module shall also verify the data path by:

- **setting the bypass switch to provide cryptographic processing and verify that data transferred through the bypass mechanism is cryptographically processed, and**
- **setting the bypass switch to not provide cryptographic processing and verify that data transferred through the bypass mechanism is not cryptographically processed.**

Required Vendor Information

VE10.22.01: The vendor documentation shall specify how to set the bypass switch to provide cryptographic processing.

VE10.22.02: The vendor documentation shall describe how the bypass mechanism is designed to enforce the data transfer of cryptographically processed data through the data path, by setting the bypass switch to provide cryptographic processing.

VE10.22.03: The vendor documentation shall specify how to set the bypass switch to not provide cryptographic processing.

VE10.22.04: The vendor documentation shall describe how the bypass mechanism is designed to enforce the data transfer of not cryptographically processed data through the data path, by setting the bypass switch to not provide cryptographic processing.

Required Test Procedures

TE10.22.01: The tester shall verify by inspection that the module does not provide bypass capability by setting the bypass switch to provide cryptographic processing.

TE10.22.02: By checking the code and/or design documentation, the tester shall verify that the implementation of bypass mechanism is consistent with the vendor documentation.

TE10.22.03: By checking the code and/or design documentation, the tester shall verify that the module performs the pre-operational bypass test which verifies that the data transferred through the data path is cryptographically processed by setting the bypass switch to provide cryptographic processing.

TE10.22.04: The tester shall verify by inspection that the module provides bypass capability by setting the bypass switch to provide cryptographic processing by setting the bypass switch not to provide cryptographic processing.

TE10.22.05: By checking the code and/or design documentation, the tester shall verify that the module performs the pre-operational bypass test which verifies that the data transferred through the data path is not cryptographically processed by setting the bypass switch to not provide cryptographic processing.

6.10.2.4 Pre-operational critical functions test

AS10.23: (Pre-operational critical functions test – Levels 1, 2, 3, and 4)

There may be other security functions critical to the secure operation of a cryptographic module that shall be tested as a pre-operational test.

NOTE This assertion is tested as part of AS10.24.

AS10.24: (Pre-operational critical functions test – Levels 1, 2, 3, and 4)

Documentation shall specify the pre-operational critical functions that are tested.

NOTE Critical functions are defined as those functions that, upon failure, could lead to the disclosure of CSPs. Examples of critical functions include but not limited to random bit generation, operation of the cryptographic algorithm, and cryptographic bypass.

Required Vendor Information

VE10.24.01: The vendor shall provide documentation of all critical functions. For each critical function, the vendor shall indicate:

a) The purpose of the critical function

b) Which critical functions are tested by which pre-operational self-tests

c) Which critical functions are tested by which conditional self-tests

Required Test Procedures

TE10.24.01: The tester shall verify the vendor provided documentation of the critical functions and the self-tests that are designed to test them. This documentation shall include the following:

a) Identification and description of all critical functions

b) Identification of at least one self-test for every critical function

TE10.24.02: By checking the code and/or design documentation, the tester shall verify that the module performs the specified self-tests for each critical function.

6.10.3 Conditional self-tests

6.10.3.1 Conditional self-test general requirements

AS10.25: (Conditional self-tests – Levels 1, 2, 3, and 4)

Conditional self-tests **shall be performed by a cryptographic module when the conditions specified for the following tests occur: Cryptographic Algorithm Self-Test, Pair-Wise Consistency Test, Software/Firmware Load Test, Manual Entry Test, Conditional Bypass Test and Conditional Critical Functions Test.**

Required Vendor Information

VE10.25.01: The vendor documentation shall provide the information on the conditional self-tests.

Required Test Procedures

TE10.25.01: The tester shall verify that the vendor documentation specifies conditional self-tests.

TE10.25.02: The tester shall verify that the conditional self-tests are performed as specified.

6.10.3.2 Conditional cryptographic algorithm self-test

AS10.26: (Conditional cryptographic algorithm self-test – Levels 1, 2, 3, and 4)

A cryptographic algorithm test shall be conducted for all cryptographic functions (e.g. security functions, SSP establishment methods and authentication) of each approved cryptographic algorithm implemented in the cryptographic module as specified in *{ISO/IEC 19790:2012}* Annexes C through E.

NOTE This assertion is tested as part of AS10.27.

AS10.27: (Conditional cryptographic algorithm self-test – Levels 1, 2, 3, and 4)

The conditional test shall be performed prior to the first operational use of the cryptographic algorithm.

Required Vendor Information

VE10.27.01: The vendor documentation shall provide the specification of the conditional cryptographic algorithm self-tests.

VE10.27.02: The vendor shall provide documentation that provides rationale stating how each conditional cryptographic algorithm self-test is performed prior to the first operational use of the cryptographic algorithm.

VE10.27.03: The vendor shall specify whether a known answer test, a comparison test and/or fault-detection test is used to test the module' cryptographic algorithm. If a comparison test and/or a fault-detection test are used, the vendor shall document this fact.

Required Test Procedures

TE10.27.01: The tester shall verify by inspection of the module or from the vendor documentation that the module conducts conditional cryptographic algorithm self-test prior to the first operational use of each cryptographic algorithm.

AS10.28: (Conditional cryptographic algorithm self-test – Levels 1, 2, 3, and 4)

If the calculated output does not equal the known answer, the cryptographic algorithm known-answer self-test shall fail.

Required Vendor Information

VE10.28.01: The vendor documentation shall specify the method used to compare the calculated output with the known answer.

VE10.28.02: 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

TE10.28.01: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

TE10.28.02: This is tested under TE10.07.02, TE10.08.01, TE10.08.02, and TE10.08.03.

AS10.29: (Conditional cryptographic algorithm self-test – Levels 1, 2, 3, and 4)

An algorithm self-test shall at a minimum use the smallest approved key length, modulus size, DSA prime, or curves as appropriate that is supported by the module.

Required Vendor Information

VE10.29.01: The vendor documentation shall provide the specification of each conditional cryptographic algorithm self-test that is implemented by the module.

Required Test Procedures

TE10.29.01: The tester shall verify by inspection and from the vendor documentation that each conditional cryptographic algorithm test implements, at a minimum, the smallest approved key length, modulus size, DSA prime, or curves as appropriate that are supported by the module.

AS10.30: (Conditional cryptographic algorithm self-test – Levels 1, 2, 3, and 4)

If an algorithm specifies multiple modes (e.g. ECB, CBC, etc), at a minimum, one mode shall be selected for the self-test that is supported by the module or as specified by the validation authority.

NOTE This assertion is tested as part of AS10.29.

AS10.31: (Conditional cryptographic algorithm self-test – Levels 1, 2, 3, and 4)

Examples of known-answer tests: **One-way functions: Input test vector(s) generate output which shall be identical to expected output (e.g. hashing, keyed hashes, message authentication, RBG (fixed entropy vector), SSP agreement).**

NOTE This assertion is tested as part of AS10.28.

AS10.32: (Conditional cryptographic algorithm self-test – Levels 1, 2, 3, and 4)

Examples of known-answer tests**: Reversible functions: Both the forward and reverse function shall be self-tested (e.g. symmetric key encryption and decryption, SSP transport encryption and decryption, digital signature generation and verification)**

NOTE This assertion is tested as part of AS10.28.

AS10.33: (Conditional cryptographic algorithm self-test – Levels 1, 2, 3, and 4)

A *comparison test* compares the output of two or more independent cryptographic algorithm implementations, if the outputs are not equal, the cryptographic algorithm comparison self-test shall fail.

Required Vendor Information

VE10.33.01: The vendor shall describe the implemented cryptographic algorithm comparison self-test.

VE10.33.02: Vendor documentation requirement is specified under VE10.27.03 for the vendor requirement.

Required Test Procedures

TE10.33.01: The tester shall verify whether the documentation of the comparison test includes:

a) Use of two or more independent cryptographic algorithm implementations

b) Continual comparison of the outputs of the algorithm implementation

c) Transition into an error state and output of an error indicator when the two outputs are not equal

TE10.33.02: By checking the code and/or design documentation, the tester shall verify that the module implements the documented steps for performing the comparison test.

AS10.34: (Conditional cryptographic algorithm self-test – Levels 1, 2, 3, and 4)

A *fault-detection test* involves the implementation of fault detection mechanisms integrated within the cryptographic algorithm implementation, if a fault is detected, the cryptographic algorithm fault-detection self-test shall fail.

EXAMPLE The fault-detection test of the RBG will cover an error of the entropy source being correctly handled inside the implementation of the RBG.

Required Vendor Information

VE10.34.01: The vendor shall specify whether a fault-detection test is used to test the module's cryptographic algorithm to complement either a known-answer test or a comparison test.

Required Test Procedures

TE10.34.01: The tester shall verify the documentation of the fault-detection test includes:

a) Description of each error condition in the cryptographic algorithm specification/implementation

b) Specification of the corresponding (internal) error indicator for each error condition

c) Rationale stating the each error condition is tested in the fault-detection test

TE10.34.02: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

TE10.34.03: This is tested under TE10.07.02, TE10.07.03, TE10.09.02, TE10.09.03, TE10.10.01, and TE10.10.02.

6.10.3.3 Conditional pair-wise consistency test

AS10.35: (Conditional pair-wise consistency test – Levels 1, 2, 3, and 4)

If a cryptographic module generates public or private key pairs, a pair-wise consistency test shall be performed for every generated public and private key pair as specified in *{ISO/IEC 19790:2012}* Annexes C through E for the applicable cryptographic algorithm.

Required Vendor Information

VE10.35.01: If public or private key pairs are used to perform an approved key transport, or an asymmetric cipher, the vendor documentation shall describe the test for pair-wise consistency. This

test consists of applying the public key to a plaintext value or to an encoded message. The resulting ciphertext shall be compared to the original plaintext to verify that they differ.

— If the two values are equal, then the cryptographic module shall enter an error state and output an error indicator via the status interface.

— If the two values differ, then the private key shall be applied to the ciphertext if the result is not equal to the original plaintext then pair-wise consistency test shall fail.

VE10.35.02: If public or private key pairs are to be used only for the calculation and/or verification of digital signatures, the vendor documentation shall describe the test for pair-wise consistency by calculation and verification of a signature. If the signature cannot be verified, the pair-wise consistency test shall fail.

VE10.35.03: If public or private key pairs are used to perform a SSP agreement, the vendor documentation shall describe the test for pair-wise consistency. The vendor documentation shall identify the prerequisite algorithms of the SSP agreement. This test shall consists of applying the key pair to see if it passes the test for pair-wise consistency by exercising the prerequisite algorithms implemented.

EXAMPLE The Diffie-Hellman key agreement uses the finite field cryptography primitive common to Digital Signature Algorithm.

Required Test Procedures

TE10.35.01: If public or private key pairs are to be used to perform an approved key transport, or an asymmetric cipher, the tester shall verify that the implementation of the pair-wise consistency test, as defined in VE10.35.01, is consistent with the vendor documentation by checking the code and/or design documentation.

TE10.35.02: If public or private key pairs are used for the calculation and/or verification of digital signatures, then the tester shall verify that the implementation of the pair-wise consistency test as defined in VE10.35.02 is consistent with the vendor documentation by checking the code and/or design documentation.

TE10.35.03: If public or private key pairs are used to perform a SSP agreement, then the tester shall verify that the implementation of the pair-wise consistency test as defined in VE10.35.03 is consistent with the vendor documentation by checking the code and/or design documentation.

6.10.3.4 Conditional software/firmware load test

AS10.36: (Conditional software/firmware load test – Levels 1, 2, 3, and 4)

If a cryptographic module has the capability of loading software or firmware from an external source, then the following requirements in addition to those in *{ISO/IEC 19790:2012 subclause}* 7.4.3.4 shall be performed.

NOTE This assertion is not tested separately.

AS10.37: (Conditional software/firmware load test – Levels 1, 2, 3, and 4)

The cryptographic module shall implement an approved authentication technique to verify the validity of the software or firmware that is loaded.

Required Vendor Information

VE10.37.01: The vendor documentation shall describe the approved authentication technique used to protect the integrity of all externally loaded software and firmware components.

VE10.37.02: If the module implements an approved authentication technique the vendor shall provide a validation certificate as specified in VE02.20.01.

VE10.37.03: The vendor shall provide documentation specifying how the referenced authentication key is loaded independently in the module prior to the software or firmware loading.

VE10.37.04: The vendor documentation shall describe the mechanisms to ensure that the loaded software or firmware cannot be used if the software/firmware load test fails.

Required Test Procedures

TE10.37.01: The tester shall determine from the vendor supplied documentation which approved authentication technique is used for the software/firmware load test.

TE10.37.02: The tester shall verify that if an approved authentication technique is implemented, the vendor has provided a validation certificate as specified in VE02.20.01.

TE10.37.03: If the module implements an approved authentication technique for the software/firmware load test, the tester shall verify that the vendor documentation of the software/firmware load test includes:

a) Specification of the approved authentication technique implemented.

b) Identification of software and firmware that is protected using the approved authentication technique.

c) Calculation of the approved authentication technique when the software and firmware is loaded.

d) Verification of the approved authentication technique when the load test is initiated.

e) Failure of the self-test upon failure of the approved authentication technique verification.

TE10.37.04: By checking the code and/or design documentation, the tester shall verify that the implementation of the software/firmware load test is consistent with TE10.37.01, TE10.37.02 and TE10.37.03.

TE10.37.05: The tester shall test the module by modifying the software or firmware to be loaded, or the implemented authentication mechanism and initiating the self-test, and observing the output from the status output interface. If no indicator is output that indicates that the software/firmware load test failed, the assertion fails. If it is not possible for the tester to modify the software or firmware to be loaded, or the implemented authentication mechanism, then the vendor shall provide a rationale to the tester why this test cannot be performed.

TE10.37.06: The tester shall exercise the cryptographic module, with modifying the software or firmware to be loaded, modifying the referenced authentication signature, or the implemented authentication mechanism, and shall initiate the software/firmware load test. After the self-test fails, the tester shall verify that the loaded software or firmware cannot be used and that the module's versioning information is unchanged.

TE10.37.07: By checking the code and/or design documentation, the tester shall verify that the reference authentication signature is loaded independently from the software or firmware loading.

TE10.37.08: By checking the code and/or design documentation, the tester shall verify that the software/firmware load test fails without loading the reference authentication signature prior to the software or firmware loading.

TE10.37.09: The tester shall exercise the cryptographic module, without loading the reference authentication signature in advance, and shall initiate the software/firmware load test. If the software/firmware load test passes, the assertion fails.

AS10.38: (Conditional software/firmware load test – Levels 1, 2, 3, and 4)

The reference authentication key shall be loaded independently in the module prior to the software or firmware loading.

NOTE This assertion is tested as part of AS10.37.

AS10.39: (Conditional software/firmware load test – Levels 1, 2, 3, and 4)

The applied approved authentication technique shall be successfully verified *{or the software/firmware load test shall fail}*.

NOTE This assertion is tested as part of AS10.37.

AS10.40: (Conditional software/firmware load test – Levels 1, 2, 3, and 4)

***{The applied approved authentication technique shall be successfully verified}* or the software/firmware load test shall fail.**

NOTE This assertion is tested as part of AS10.37.

AS10.41: (Conditional software/firmware load test – Levels 1, 2, 3, and 4)

Loaded software or firmware shall not be used if the software/firmware load test fails.

NOTE This assertion is tested as part of AS10.37.

6.10.3.5 Conditional manual entry test

AS10.42: (Conditional manual entry test – Levels 1, 2, 3, and 4)

If SSPs or key components are manually entered directly into a cryptographic module or if error on the part of the human operator could result in the incorrect entry of the intended value, then the following manual entry tests shall be performed.

NOTE This assertion is not separately tested.

AS10.43: (Conditional manual entry test – Levels 1, 2, 3, and 4)

The SSP or key components shall have an error detection code (EDC) applied, *{or shall be entered using duplicate entries}*.

NOTE This assertion is not separately tested.

AS10.44: (Conditional manual entry test – Levels 1, 2, 3, and 4)

***{The SSP or key components shall have an error detection code (EDC) applied,}* or shall be entered using duplicate entries.**

NOTE This assertion is not separately tested.

AS10.45: (Conditional manual entry test – Levels 1, 2, 3, and 4)

If an EDC is used, the EDC shall be at least 16 bits in length.

NOTE This assertion is not separately tested.

AS10.46: (Conditional manual entry test – Levels 1, 2, 3, and 4)

If the EDC cannot be verified, or the duplicate entries do not match, the test shall fail.

Required Vendor Information

VE10.46.01: The vendor shall document the manual entry test. Depending on whether error detection codes or duplicate entries of SSPs or key components are used, the manual entry test shall include the following:

a) Error detection code (EDC):

    1) Description of EDC calculation algorithm

2) Description of verification process

3) Expected outputs for success or failure of test

b) Duplicate key entries:

1) Description of verification process

2) Expected outputs for success or failure of test

VE10.46.02: If the EDC is associated with the SSP or key components, then the vendor documentation that describes the format of the SSP or key components (see AS09.03) shall include fields for EDC.

Required Test Procedures

TE10.46.01: The tester shall verify from the vendor documentation which method is used for the manual key entry test (error detection codes or duplicate key entries). Based on the method used, the tester shall check the vendor documentation, code, and/or design documentation that specifies the implementation of the manual key entry test to verify whether the following information is included:

a) Error detection codes:

1) SSP or key component format for all manually-entered SSPs or key components, including fields for EDC (see AS09.03)

2) Description of EDC algorithm

3) Description of EDC verification process

4) All expected outputs for success or failure of the test

b) Duplicate entries of SSPs or key components:

1) Duplicate entries for all manually-entered SSPs and key components

2) Description of duplicate entry verification process

3) All expected outputs for success or failure of the test

TE10.46.02: For manual entry tests using an EDC, the tester shall verify by inspection and from the vendor documentation that the format of the SSP or key components include fields for EDC, and that the EDC is at least 16 bits in length.

TE10.46.03: For manual entry tests using an EDC, the tester shall perform the following tests:

a) The tester shall enter every manually entered SSP and verify that the procedure used to enter each SSP is in accordance with the documented procedure, including the form that the SSP are in when they are entered.

b) The tester shall enter each type of manually entered SSP without any errors and shall verify the status output interface. If no indicator is output, or if the indicator does not match the documented indicator for the success of the manual entry test, the test is failed.

c) The tester shall attempt to perform cryptographic operations with each entered SSP to verify that it was entered correctly.

d) The tester shall modify either the EDC associated with each manually entered SSP or the SSP itself and shall enter them into the module. The tester shall verify the indicator that is output from the status output interface; if no indicator is output, or the indicator does not match the documented indicator for the failure of the manual entry test, the test is failed.

e) The tester shall attempt to perform cryptographic operations with each SSP that was not successfully entered. Each operation using each SSP is required to fail, verifying that the SSP was not entered.

TE10.46.04: For manual entry tests using duplicate entries of SSPs or key components, the tester shall perform the following tests:

a) The tester shall enter each type of manually-entered SSP without any errors and shall verify the status output interface. If no indicator is output, or if the indicator does not match the documented indicator for the success of the manual entry test, the test is failed.

b) The tester shall attempt to perform cryptographic operations with each entered SSP to verify that it was entered correctly.

c) The tester shall modify one of the manually entered SSPs, either the first or second duplicate entry, and shall enter them into the module. The tester shall verify the indicator that is output from the status output interface; if no indicator is output, or the indicator does not match the documented indicator for the failure of the manual entry test, the test is failed.

d) The tester shall attempt to perform cryptographic operations with each SSP that was not successfully entered. Each operation using each SSP is required to fail, verifying that the SSP was not entered.

6.10.3.6 Conditional bypass test

AS10.47: (Conditional bypass test – Levels 1, 2, 3, and 4)

If a cryptographic module implements a bypass capability where the services may be provided without cryptographic processing (e.g. transferring plaintext through the module), then the following suite of bypass tests shall be performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext.

NOTE This assertion is tested as part of AS10.48 through AS10.51.

AS10.48: (Conditional bypass test – Levels 1, 2, 3, and 4)

A cryptographic module shall test for the correct operation of the services providing cryptographic processing when a switch takes place between an exclusive bypass service and an exclusive cryptographic service.

Required Vendor Information

VE10.48.01: If the cryptographic module implements a bypass service, then the vendor shall implement a bypass test to verify the correct operation of the cryptographic service when a switch takes place between an exclusive bypass and an exclusive cryptographic service.

VE10.48.02: The vendor shall provide a description of the bypass test. The bypass test shall demonstrate that, when switched to an exclusive cryptographic service, the module does not output plaintext information.

Required Test Procedures

TE10.48.01: The tester shall verify that the module implements a bypass test to verify the correct operation of the cryptographic service when a switch takes place between an exclusive bypass service and an exclusive cryptographic service.

TE10.48.02: The tester shall verify that the vendor documentation is consistent with the bypass test implementation through a review of the source code and/or design documentation.

TE10.48.03: The tester shall switch the module from the exclusive bypass service to the exclusive cryptographic service and verify that plaintext information is not output.

AS10.49: (Conditional bypass test – Levels 1, 2, 3, and 4)

If a cryptographic module can automatically alternate between a bypass service and a cryptographic service, providing some services with cryptographic processing and some services without cryptographic processing, then the module shall test for the correct operation of the

services providing cryptographic processing when the mechanism governing the switching procedure is modified (e.g. an IP address source/destination table).

Required Vendor Information

VE10.49.01: If the cryptographic module is designed to automatically alternate between a bypass service and a cryptographic service, then the vendor shall implement a bypass test to verify the correct operation of the cryptographic service when the mechanism governing the switching procedure is modified.

VE10.49.02: The vendor shall provide a description of the test. The bypass test shall guarantee that when the mechanism governing the switching procedure is modified:

a) The mechanism is verified not to have been altered since the last modification. If the mechanism has been altered, the cryptographic module shall enter an error state and output an error indicator to the status interface.

b) The correct operation of the cryptographic service is verified by demonstrating that the module does not output plaintext information. The bypass test fails if the module outputs plaintext information.

Required Test Procedures

TE10.49.01: The tester shall verify that the module implements a bypass test to verify the correct operation of the cryptographic service when the mechanism governing the switching procedure is modified.

TE10.49.02: The tester shall verify that the description of the test is consistent with the bypass test implementation through the review of the source code and/or design documentation.

TE10.49.03: The tester shall verify the correct operation of the bypass test by:

a) Verifying that the mechanism governing the switching procedure checks to ensure that no alteration of the mechanism has taken place since the last modification. The tester will document the method used. If the design allows, the tester shall modify the mechanism to test the method used.

b) Modifying the mechanism governing the switching procedure in order to verify the correct operation of the mechanism and to verify the correct operation of the cryptographic service by verifying that the plaintext information is not output.

AS10.50: (Conditional bypass test – Levels 1, 2, 3, and 4)

If a cryptographic module maintains internal information that governs the bypass capability, then the module shall verify the integrity of the governing information through an approved integrity technique immediately preceding modification of the governing information, *{and shall generate a new integrity value using the approved integrity technique immediately following the modification}*.

NOTE This assertion is not separately tested. Tested as part of AS10.51.

AS10.51: (Conditional bypass test – Levels 1, 2, 3, and 4)

***{If a cryptographic module maintains internal information that governs the bypass capability, then the module shall verify the integrity of the governing information through an approved integrity technique immediately preceding modification of the governing information,}* and shall generate a new integrity value using the approved integrity technique immediately following the modification.**

Required Vendor Information

VE10.51.01: The vendor documentation shall specify the method to modify the internal information that governs the bypass capability.

VE10.51.02: The vendor shall provide a detailed specification of the internal information that governs the bypass capability, the internal sequence to update the information, and the mechanism to maintain the integrity of the information using an approved integrity technique.

Required Test Procedures

TE10.51.01: By checking the code and/or design documentation, the tester shall verify that the governing information maintained in the cryptographic module is consistent with the vendor documentation.

TE10.51.02: By checking the code and/or design documentation, the tester shall verify that the internal sequence to update the governing information is consistent with the vendor documentation.

TE10.51.03: By checking the code and/or design documentation, the tester shall verify that the mechanism to maintain the governing information is consistent with the vendor documentation.

6.10.3.7 Conditional critical functions test

AS10.52: (Conditional critical functions test – Levels 1, 2, 3, and 4)

There may be other security functions critical to the secure operation of a cryptographic module that shall be tested as a conditional self-test.

NOTE This assertion is tested as part of AS10.24.

6.10.3.8 Periodic self-tests

AS10.53: (Periodic self-test – Levels 1, 2, 3, and 4)

A cryptographic module shall permit operators to initiate the pre-operational or conditional self-tests on demand for periodic testing of the module. Acceptable means for the on-demand initiation of periodic self-tests are: provided service, resetting, rebooting, or power cycling.

Required Vendor Information

VE10.53.01: The vendor shall describe the procedure by which an operator can initiate the pre-operational self-tests on demand for periodic testing of the module. All of the pre-operational self-tests have to be included.

VE10.53.02: The vendor shall describe the procedure by which an operator can initiate the conditional self-tests on demand for periodic testing of the module. At a minimum, conditional cryptographic algorithm tests have to be included.

Required Test Procedures

TE10.53.01: The tester shall inspect the vendor documentation to verify that initiation of pre-operational self-tests on demand is specified for all of the pre-operational self-tests.

TE10.53.02: The tester shall initiate the pre-operational self-tests on demand to verify that the initiation of the pre-operational self-tests on demand is consistent with the vendor documentation.

TE10.53.03: The tester shall initiate the conditional self-tests on demand to verify that the initiation of the conditional self-tests on demand is consistent with the vendor documentation.

AS10.54: (Periodic self-test – Levels 3 and 4)

The module shall repeatedly upon a defined time period automatically, without external input or control, perform the pre-operational or conditional self-tests.

Required Vendor Information

VE10.54.01: The vendor shall provide documentation that specifies how the pre-operational and conditional self-tests are repeatedly performed upon a defined time, automatically, without external input or control.

VE10.54.02: The vendor documentation shall include the specification on the status indicator used to indicate that the cryptographic module's operations are interrupted due to the pre-operational or conditional self-tests.

VE10.54.03: The vendor provided non-proprietary security policy shall provide the information on the defined time period and any conditions that result in the interruption of the module's operation during the time to repeat pre-operational or conditional self-tests.

Required Test Procedures

TE10.54.01: The tester shall verify, by inspection of the cryptographic module, that the pre-operational and conditional self-tests are repeatedly performed as specified in VE10.54.01, and VE10.54.02.

AS10.55: (Periodic self-test – Levels 3 and 4)

The time period and any conditions that may result in the interruption of the module's operations during the time to repeat the pre-operational or conditional self-tests shall be specified in the security policy (*{ISO/IEC 19790:2012}* Annex B) (e.g. If the module is performing mission critical services that can't be interrupted and the time period is passed for the initiation of the pre-conditional self-tests; the self-tests may be deferred after the time period is passed again.).

NOTE This assertion is tested as part of AS10.54.

6.11 Life-cycle assurance

6.11.1 Life-cycle assurance general requirements

AS11.01: (Life-Cycle assurance – Levels 1, 2, 3, and 4)

The documentation requirements specified in *{ISO/IEC 19790:2012 Annex}* A.2.11 shall be provided.

Required Vendor Information

VE11.01.01: The vendor shall provide the documentation requirements as specified in A.2.11 of ISO/IEC 19790:2012.

Required Test Procedures

TE11.01.01: The tester shall verify that the vendor provides documentation as specified in A.2.11 of ISO/IEC 19790:2012.

6.11.2 Configuration management

AS11.02: (Configuration management – Levels 1, 2, 3, and 4)

The following security requirements *{ISO/IEC 19790:2012 AS11.03 through AS11.05}* shall apply to cryptographic modules for Security Levels 1 and 2.

NOTE This assertion is tested as part of AS11.03 through AS11.05.

AS11.03: (Configuration management – Levels 1, 2, 3, and 4)

A configuration management system shall be used for the development of a cryptographic module and module components within the cryptographic boundary, and of associated module documentation.

Required Vendor Information

VE11.03.01: The vendor documentation shall describe the configuration management system for the cryptographic module, module components, and associated module documentation.

Required Test Procedures

TE11.03.01: The tester shall verify the vendor provided documents that a configuration management system has been implemented.

AS11.04: (Configuration management – Levels 1, 2, 3, and 4)

Each version of each configuration item (e.g. cryptographic module, module hardware parts, module software components, module HDL, user guidance, security policy, etc.) that comprises the module and associated documentation shall be assigned and labeled with a unique identifier.

Required Vendor Information

VE11.04.01: The vendor cryptographic module documentation shall include a configuration list of all configuration items. The vendor documentation shall describe the method used to uniquely identify the configuration items.

VE11.04.02: The vendor documentation shall describe the method used to uniquely identify the version of each configuration item being validated.

Required Test Procedures

TE11.04.01: The tester shall verify the vendor provided configuration list inclusion of configuration items.

TE11.04.02: The tester shall verify that the vendor documentation specifies the method used to uniquely identify all configuration items.

TE11.04.03: The tester shall verify that vendor documentation describes the method used to uniquely identify each version of a configuration item being validated.

TE11.04.04: The tester shall verify that vendor documentation uniquely identifies the version of each configuration item being validated.

AS11.05: (Configuration management – Levels 1, 2, 3, and 4)

The configuration management system shall track and maintain the changes to the identification and version or revision of each configuration item throughout the life-cycle of the validated cryptographic module.

Required Vendor Information

VE11.05.01: The vendor documentation shall specify the measures such that only authorised changes are made to the configuration items.

Required Test Procedures

TE11.05.01: The tester shall verify the vendor documentation that specifies the measures such that only authorised changes are made to the configuration items.

AS11.06: (Configuration management – Levels 3, and 4)

The configuration items shall be managed using an automated configuration management system.

Required Vendor Information

VE11.06.01: The vendor documentation shall specify how the configuration management system provides an automated means to support the generation of a cryptographic module.

Required Test Procedures

TE11.06.01: The tester shall verify the vendor documentation that specifies how the configuration management system provides an automated means to support the generation of a cryptographic module.

6.11.3 Design

AS11.07: (Design – Levels 1, 2, 3, and 4)

Cryptographic modules shall be designed to allow the testing of all provided security related services.

NOTE This assertion is tested in 6.4.3 of this International Standard.

6.11.4 Finite state model

AS11.08: (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 a state transition table and state descriptions.

Required Vendor Information

VE11.08.01: 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.

VE11.08.02: The vendor documentation shall establish a complete description of the following:

a) Normal operation

b) Degraded operation

c) Data input interface

d) Data output interface

e) Control input interface

f) Control output interface

g) Status output interface

h) Trusted Channel

i) Crypto officer role

j). User role

k) Other roles (if applicable)

l). Security Services

m) SSP entry services (if applicable)

n) Show status service

o) Operator authentication

p) Self-tests

q) Other authorised services, operations, and functions (if applicable)

r) Error states

s) Bypass service (if applicable)

t) Maintenance access interface (if applicable)

u) Maintenance role (if a maintenance access interface is provided)

v) SSP generation and establishment services (if applicable)

w) SSP output services (if applicable)

x) Idle states (if applicable)

y) Uninitialised states (if applicable)

Required Test Procedures

TE11.08.01: 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.

TE11.08.02: The tester shall verify that the finite state diagrams and the descriptions are consistent with the vendor documentation that shall describe the following:

a) Normal operation

b) Degraded operation

c) Data input interface

d) Data output interface

e) Control input interface

f) Control output interface

g) Status output interface

h) Trusted Channel

i) Crypto officer role

j) User role

k) Other roles (if applicable)

l) Security Services

m) SSP entry services (if applicable)

n) Show status service

o) Operator authentication

p) Self-tests

q) Other authorised services, operations, and functions (if applicable)

r) Error states

s) Bypass service (if applicable)

t) Maintenance access interface (if applicable)

u) Maintenance role (if a maintenance access interface is provided)

v) SSP generation and establishment services (if applicable)

w) SSP output services (if applicable)

x) Idle states (if applicable)

y) Uninitialised states (if applicable)

TE11.08.03: The tester shall verify that each distinct cryptographic module service, security function use, error state, self-test, or operator authentication is depicted as a separate state in the finite state model.

TE11.08.04: The tester shall verify that every state that is identified in the finite state diagram(s) is also identified and described in the description.

TE11.08.05: The tester shall verify that every state that is identified and described in the description is also identified in the finite state diagram(s).

TE11.08.06: The tester shall verify that the operation of the module is consistent with the finite state diagrams and descriptions.

TE11.08.07: If the module includes a maintenance access 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.

TE11.08.08: 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.

TE11.08.09: 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.

TE11.08.10: 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.

TE11.08.11: 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.

TE11.08.12: 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."

AS11.09: (Finite state model – Levels 1, 2, 3, and 4)

The FSM shall be sufficiently detailed to demonstrate that the cryptographic module complies with all of the requirements of this International Standard.

NOTE This assertion is not separately tested. Tested as part of AS11.10 through AS11.13.

AS11.10: (Finite state model – Levels 1, 2, 3, and 4)

The FSM of a cryptographic module shall include, as a minimum, the following operational and error states:

- ***Power on/off state*. A state in which the module is powered off, placed in standby mode (volatile memory maintained), or the operational state preserved in non-volatile memory (e.g. hibernation mode) and in which primary, secondary, or backup power is applied to the module. This state may distinguish between power sources being applied to a cryptographic module. For a software module, power on is the action of spawning an executable image of the cryptographic module.**
- ***General initialisation state*: A state in which the cryptographic module is undergoing initialising before the module transitions to the approved state.**
- ***Crypto Officer State*: a state in which the Crypto Officer services are performed (e.g. cryptographic initialisation, secure administration, and key management).**
- ***CSP entry state:* a state for entering the CSPs into the cryptographic module.**
- ***User state:* (if a User role is implemented): a state in which authorised users obtain security services, perform cryptographic operations, or perform other approved functions.**
- ***Approved state*: a state in which approved security functions are performed.**
- ***Self-test state*: a state in which the cryptographic module is performing self-tests.**
- ***Error state*: a state when the cryptographic module has encountered an error condition (e.g. failed a self-test). There may be one or more error conditions that result in a single module error state. 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 AS11.08.

AS11.11: (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

VE11.11.01: 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

TE11.11.01: 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).

AS11.12: (Finite state model – Levels 1, 2, 3, and 4)

Each distinct cryptographic module service, security function use, error state, self-test, or operator authentication shall be depicted as a separate state.

NOTE This assertion is tested as part of AS11.08.

AS11.13: (Finite state model – Levels 1, 2, 3, and 4)

Changing to the Crypto Officer state from any other role other than the Crypto Officer shall be prohibited.

Required Vendor Information

VE11.13.01: The vendor shall provide documentation that changing to the Crypto Officer state from any other role other than the Crypto Officer is prohibited.

Required Test Procedures

TE11.13.01: The tester shall verify that the vendor provides documentation that changing to the Crypto Officer state from any other role other than the Crypto Officer is prohibited.

6.11.5 Development

AS11.14: (Development – Levels 1, 2, 3, and 4)

The following requirements shall apply to cryptographic modules for Security Level 1.

NOTE This assertion is tested as part of AS11.15 through AS11.21.

AS11.15: (Development – Levels 1, 2, 3, and 4)

If a cryptographic module contains software or firmware, the source code, language reference, the compilers, compiler versions and compiler options, the linker and linker options, the runtime libraries and runtime library settings, configuration settings, build processes and methods, the build options, environmental variables and all other resources used to compile and link the source code into an executable form shall be tracked using the configuration management system.

Required Vendor Information

VE11.15.01: For cryptographic modules which contain software or firmware, the vendor shall provide documentation of the source code, language reference, the compilers, compiler versions and compiler options, the linker and linker options, the runtime libraries and runtime library settings, configuration settings, build processes and methods, the build options, environmental variables and all other resources used to compile and link the source code into an executable form.

VE11.15.02: For each of the documented items in VE11.15.01, the vendor shall provide documentation that these items are tracked using the configuration management system.

Required Test Procedures

TE11.15.01: For cryptographic modules which contain software or firmware, the tester shall verify that the vendor provides documentation of the source code, language reference, the compilers, compiler versions and compiler options, the linker and linker options, the runtime libraries and runtime library settings, configuration settings, build processes and methods, the build options, environmental variables and all other resources used to compile and link the source code into an executable form.

TE11.15.02: For each of the documented items in TE11.15.01, the tester shall verify that the vendor provides documentation that these items are tracked using the configuration management system.

AS11.16: (Development – Levels 1, 2, 3, and 4)

If a cryptographic module contains software or firmware, the source codes shall be annotated with comments that depict the correspondence of the software or firmware to the design of the module.

Required Vendor Information

VE11.16.01: The vendor shall supply a list of the names of all the software and firmware components contained in the cryptographic module.

VE11.16.02: The vendor shall supply an annotated source listing of each software and firmware component contained in the cryptographic module.

Required Test Procedures

TE11.16.01: The tester shall use the list supplied by the vendor to verify that a source listing for each software or firmware component is contained in the module.

AS11.17: (Development – Levels 1, 2, 3, and 4)

If a cryptographic module contains hardware, documentation shall specify the schematics and/or Hardware Description Language (HDL), as applicable.

Required Vendor Information

VE11.17.01: The vendor shall supply a list of the hardware components contained in the cryptographic module.

Required Test Procedures

TE11.17.01: The tester shall use the list supplied by the vendor to verify that the documentation includes schematics and/or Hardware Description Language (HDL) listings for the hardware components.

AS11.18: (Development – Levels 1, 2, 3, and 4)

If a cryptographic module contains hardware, the HDL shall be annotated with comments that depict the correspondence of the hardware to the design of the module.

Required Vendor Information

VE11.18.01: The vendor shall supply an annotated HDL listing of each hardware component contained in the cryptographic module

Required Test Procedures

TE11.18.01: The tester shall use the list supplied by the vendor to verify that a HDL listing for each hardware component is contained in the module.

AS11.19: (Development – Levels 1, 2, 3, and 4)

***{For software and firmware cryptographic modules and the software or firmware component of a hybrid module}* the result of the integrity and authentication technique mechanisms specified in *{ISO/IEC 19790:2012 subclause}* 7.5 and *{ISO/IEC 19790:2012 subclause}* 7.10 shall be calculated and integrated into the software or firmware module by the vendor during the module development.**

Required Vendor Information

VE11.19.01: For software and firmware cryptographic modules and the software or firmware component of a hybrid module the vendor shall provide documentation that the result of the integrity and authentication technique mechanisms specified in *{ISO/IEC 19790:2012}* 7.5 and *{ISO/IEC 19790:2012}* 7.10 shall be calculated and integrated into the software or firmware module by the vendor during the module development.

Required Test Procedures

TE11.19.01: For software and firmware cryptographic modules and the software or firmware component of a hybrid module the tester shall verify that the vendor provides documentation that the result of the integrity and authentication technique mechanisms specified in *{ISO/IEC 19790:2012}* 7.5 and *{ISO/IEC 19790:2012}* 7.10 shall be calculated and integrated into the software or firmware module by the vendor during the module development.

AS11.20: (Development – Levels 1, 2, 3, and 4)

***{For software and firmware cryptographic modules and the software or firmware component of a hybrid module}* the cryptographic module documentation shall specify the compiler, configuration settings and methods to compile the source code into an executable form.**

NOTE This assertion is tested as part of AS11.15.

AS11.21: (Development – Levels 1, 2, 3, and 4)

{For software and firmware cryptographic modules and the software or firmware component of a hybrid module} **the cryptographic module shall be developed using production-grade development tools (e.g. compilers).**

Required Vendor Information

VE11.21.01: The vendor shall provide documentation that the cryptographic module shall be developed using production-grade development tools (e.g. compilers).

Required Test Procedures

TE11.21.01: The tester shall verify that the vendor provides documentation that the module meets the cryptographic module shall be developed using production-grade development tools (e.g. compilers).

AS11.22: (Development – Levels 2, 3, and 4)

The following requirements *{ISO/IEC 19790:2012 AS11.23 through AS11.26}* shall apply to cryptographic modules for Security Levels 2 and 3.

NOTE This assertion is tested as part of AS11.23 through AS11.26.

AS11.23: (Development – Levels 2, 3, and 4)

All software or firmware shall be implemented using a high-level, non-proprietary language *{or rationale shall be provided for the use of a low-level language (e.g. assembly language or microcode) if essential to the performance of the module or when a high-level language is not available}*.

Required Vendor Information

VE11.23.01: The vendor shall provide documentation that all software or firmware within a cryptographic module is implemented using a high-level, non-proprietary language.

Required Test Procedures

TE11.23.01: The tester shall verify that the vendor provides documentation that all software or firmware within a cryptographic module is implemented using a high-level, non-proprietary language.

AS11.24: (Development – Levels 2, 3, and 4)

{All software or firmware shall be implemented using a high-level, non-proprietary language} **or rationale shall be provided for the use of a low-level language (e.g. assembly language or microcode) if essential to the performance of the module or when a high-level language is not available.**

Required Vendor Information

VE11.24.01: The vendor shall identify each of the software and firmware components that is not written in a high-level language and provide a rationale or justification for why the component are written in a low-level language. The rationale shall cite either the unavailability of a high-level language or the need for enhanced performance for the software or firmware.

Required Test Procedures

TE11.24.01: The tester shall examine the source code for each of the software and/or firmware components to verify which ones are written in a low-level language. The tester shall verify that there are no software and/or firmware components written in a low-level language that were not identified by the vendor in VE11.24.01.

AS11.25: (Development – Levels 2, 3, and 4)

Custom integrated circuits within a cryptographic module shall be implemented using a high-level Hardware Description Language (HDL) (e.g. VHDL or Verilog).

Required Vendor Information

VE11.25.01: The vendor shall supply documentation on the hardware components that are implemented using a high-level specification language.

Required Test Procedures

TE11.25.01: The tester shall verify the vendor documentation that the information specified in VE11.25.01 is included.

AS11.26: (Development – Levels 2, 3, and 4)

Software or firmware cryptographic modules shall be designed and implemented in a manner that avoids the use of code, parameters or symbols not necessary for the module's functionality and execution.

Required Vendor Information

VE11.26.01: For software and software components of a hybrid module and firmware and firmware components of a hybrid module the vendor shall supply documentation that the software or firmware is designed and implemented in a manner that avoids the use of code, parameters or symbols not necessary for the module's functionality and execution.

Required Test Procedures

TE11.26.01: For software and software components of a hybrid module and firmware and firmware components of a hybrid module the tester shall verify that the vendor provides documentation that the software or firmware is designed and implemented in a manner that avoids the use of code, parameters or symbols not necessary for the module's functionality and execution.

AS11.27: (Development – Level 4)

The following requirement shall apply to cryptographic modules for Security Level 4.

NOTE This assertion is tested as part of AS11.28.

AS11.28: (Development – Level 4)

For each cryptographic module hardware and software component, the documentation shall be annotated with comments that specify (1) the pre-conditions required upon entry into the module component, function, or procedure in order to execute correctly and (2) the post-conditions expected to be true when the execution of the module component, function, or procedure is complete.

NOTE The preconditions and post conditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behaviour of the cryptographic module component, function, or procedure.

Required Vendor Information

VE11.28.01: The source code listings for all hardware, software, and firmware components, shall include as comments, pre- and post-conditions as required in AS11.28.

Required Test Procedures

TE11.28.01: The tester shall verify the source code listings that the information specified in VE11.28.01 is included.

6.11.6 Vendor testing

AS11.29: (Vendor testing – Levels 1, 2, 3, and 4)

Documentation shall specify the functional testing performed on the cryptographic module.

Required Vendor Information

VE11.29.01: The vendor shall provide documentation that specifies the functional testing performed on the cryptographic module.

Required Test Procedures

TE11.29.01: The tester shall verify that the vendor provides documentation that specifies the functional testing performed on the cryptographic module.

AS11.30: (Vendor testing – Levels 1, 2, 3, and 4)

For software or firmware cryptographic modules and the software or firmware component of a hybrid module, the vendor shall use current automated security diagnostic tools (e.g. detect buffer overflow).

Required Vendor Information

VE11.30.01: For software or firmware cryptographic modules and the software or firmware component of a hybrid module the vendor shall provide documentation that current automated security diagnostic tools (e.g. detect buffer overflow, etc) were used.

Required Test Procedures

TE11.30.01: For software or firmware cryptographic modules and the software or firmware component of a hybrid module the tester shall verify that the vendor provides documentation that current automated security diagnostic tools (e.g. detect buffer overflow, etc) were used.

AS11.31: (Vendor testing – Levels 3, and 4)

Documentation shall specify the procedures for and the results of low-level testing performed on the cryptographic module.

Required Vendor Information

VE11.31.01: The vendor shall provide documentation that specifies the procedures for and the results of low-level testing performed on the cryptographic module.

Required Test Procedures

TE11.31.01: The tester shall verify that the vendor provides documentation that specifies the procedures for and the results of low-level testing performed on the cryptographic module.

6.11.7 Delivery and operation

AS11.32: (Delivery and operation – Levels 1, 2, 3, and 4)

Documentation shall specify the procedures for secure installation, initialisation, and startup of the cryptographic module.

Required Vendor Information

VE11.32.01: The vendor documentation shall describe the steps necessary for the secure installation, initialisation, and start-up of the cryptographic module.

Required Test Procedures

TE11.32.01: The tester shall verify the vendor provided documentation that it includes installation, initialisation, and start-up procedures that result in a secure configuration.

TE11.32.02: The tester shall perform the procedures for the secure installation, initialisation, and startup of the cryptographic module and verify their correctness.

AS11.33: (Delivery and operation – Levels 2, 3, and 4)

Documentation shall specify the procedures required for maintaining security while distributing, installation and the initialisation of versions of a cryptographic module to authorised operators.

Required Vendor Information

VE11.33.01: The delivery documentation shall describe the procedures necessary to maintain security when distributing the cryptographic module to authorised operators.

Required Test Procedures

TE11.33.01: The tester shall verify the vendor provided documentation that procedures required for maintaining security while distributing and delivering versions of the cryptographic module to authorised operators are correct.

AS11.34: (Delivery and operation – Levels 2, 3, and 4)

The procedures shall specify how to detect tamper during the delivery, installation and initialisation of the module to the authorised operators.

Required Vendor Information

VE11.34.01: The vendor shall provide documentation that specifies the procedures how to detect tamper during the delivery, installation and initialisation of the module to the authorised operators.

Required Test Procedures

TE11.34.01: The tester shall verify that the vendor provides documentation that specifies the procedures how to detect tamper during the delivery, installation and initialisation of the module to the authorised operators.

AS11.35: (Delivery and operation – Level 4)

The procedures shall require the authorised operator to authenticate to the module using authentication data provided by the vendor.

Required Vendor Information

VE11.35.01: The vendor shall provide documentation for the procedures required by the authorised operator to authenticate to the module using authentication data provided by the vendor.

Required Test Procedures

TE11.35.01: The tester shall verify that the vendor provides documentation for the procedures required by the authorised operator to authenticate to the module using authentication data provided by the vendor.

6.11.8 End of life

AS11.36: (End of life – Levels 1, 2, 3, and 4)

Documentation shall specify the procedures for secure sanitization of the cryptographic module.

Required Vendor Information

VE11.36.01: The vendor shall provide documentation that specifies the procedures for secure sanitization of the cryptographic module.

Required Test Procedures

TE11.36.01: The tester shall verify that the vendor provides documentation that specifies the procedures for secure sanitization of the cryptographic module.

AS11.37: (End of life – Levels 3, and 4)

Documentation shall specify the procedures required for the secure destruction of the module.

Required Vendor Information

VE11.37.01: The vendor shall provide documentation that specifies the procedures required for the secure destruction of the module.

Required Test Procedures

TE11.37.01: The tester shall verify that the vendor provides documentation that specifies the procedures required for the secure destruction of the module.

6.11.9 Guidance documents

AS11.38: (Guidance documents – Levels 1, 2, 3, and 4)

***Administrator guidance* shall specify:**

- **the administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the Crypto Officer and/or other administrative roles;**
- **procedures required to keep independent operator authentication mechanisms functionally independent;**
- **procedures on how to administer the cryptographic module in an approved mode of operation; and**
- **assumptions regarding User behavior that are relevant to the secure operation of the cryptographic module.**

Required Vendor Information

VE11.38.01: The vendor shall provide documentation that includes the information list in AS11.38.

VE11.38.02: The non-proprietary guidance shall be available to the appropiate administrators of the module.

Required Test Procedures

TE11.38.01: The tester shall verify that the vendor provides documentation that includes the information list in AS11.38.

AS11.39: (Guidance documents – Levels 1, 2, 3, and 4)

***Non-administrator guidance* shall specify:**

- **the approved and non-approved security functions, physical ports, and logical interfaces available to the users of a cryptographic module; and**
- **all User responsibilities necessary for the approved mode of operation of a cryptographic module.**

Required Vendor Information

VE11.39.01: The vendor shall provide documentation that includes the information list in AS11.39.

VE11.39.02: The non-proprietary guidance shall be available to the appropiate non-administrators of the module.

Required Test Procedures

TE11.39.01: The tester shall verify that the vendor provides documentation that includes the information list in AS11.39.

6.12 Mitigation of other attacks

NOTE 1 The existence and proper functioning of the security mechanisms will be validated when requirements and associated tests are developed.

NOTE 2 The non-proprietary security policy shall include the requirements specified in B.2.12 *{of ISO/IEC 19790:2012}*.

AS12.01: (Mitigation of other attacks – Levels 1, 2, 3, and 4)

The documentation requirements specified in *{ISO/IEC 19790:2012 Annex}* A.2.12 shall be provided.

Required Vendor Information

VE12.01.01: The vendor shall provide the documentation requirements as specified in A.2.12 of ISO/IEC 19790:2012.

Required Test Procedures

TE12.01.01: The tester shall verify that the vendor provides documentation as specified in A.2.12 of ISO/IEC 19790:2012.

AS12.02: (Mitigation of other attacks – Levels 1, 2, 3, and 4)

If a cryptographic module is designed to mitigate one or more specific attack(s) not defined elsewhere in this International Standard *{ISO/IEC 19790:2012}*, then the module's supporting documents shall enumerate the attack(s) the module is designed to mitigate.

Required Vendor Information

VE12.02.01: The vendor shall provide supporting documentation which enumerates the attack(s) the module is designed to mitigate.

Required Test Procedures

TE12.02.01: The tester shall verify that the vendor provides supporting documentation which enumerates the attack(s) the module is designed to mitigate.

AS12.03: (Mitigation of other attacks – Level 4)

The following requirement shall apply to cryptographic modules for Security Level 4.

NOTE This assertion is tested as part of AS12.04.

AS12.04: (Mitigation of other attacks – Level 4)

If the mitigation of specific attacks not defined elsewhere in this International Standard *{ISO/IEC 19790:2012}* is claimed, documentation shall specify the methods used to mitigate the attacks and the methods to test the effectiveness of mitigation techniques.

Required Vendor Information

VE12.04.01: The vendor shall specify in the documentation the methods used to mitigate the attack(s).

VE12.04.02: The vendor shall specify in the documentation the test methods used to test the effectiveness of the mitigation techniques.

VE12.04.03: The vendor shall specify in the documentation the effectiveness of the mitigation techniques.

Required Test Procedures

TE12.04.01: The tester shall verify that the vendor provides documentation that specifies the methods used to mitigate the attack(s).

TE12.04.02: The tester shall verify that the vendor provides documentation that specifies the test methods used to test the effectiveness of the mitigation techniques.

TE12.04.03: The tester shall verify that the vendor provides documentation that specifies the effectiveness of the mitigation techniques.

6.13 A - Documentation requirements

NOTE ISO/IEC 19790:2012, Annex A specifies the minimum documentation requirements of a cryptographic module.

ASA.01: (Documentation – Levels 1, 2, 3, and 4)

This annex *{ ISO/IEC 19790:2012 Annex A}* specifies the minimum documentation which shall be required for a cryptographic module that is to undergo an independent verification scheme *{and the documentation shall meet those requirements}*.

Required Vendor Information

VEA.01.01: The vendor shall provide documentation for a cryptographic module that fulfills but is not limited to the minimum documentation requirements as specified in A.2.1 to A.2.12 of ISO/IEC 19790:2012.

Required Test Procedures

TEA.01.01: The tester shall verify that the vendor provides documentation for a cryptographic module that fulfills but is not limited to the minimum documentation requirements as specified in A.2.1 to A.2.12 of ISO/IEC 19790:2012.

6.14 B - Cryptographic module security policy

NOTE ISO/IEC 19790:2012, Annex B specifies the minimum requirements of a cryptographic module security policy.

ASB.01: (Security policy – Levels 1, 2, 3, and 4)

The following list summarises requirements that shall be provided in the non-proprietary Security Policy.

Required Vendor Information

VEB.01.01: The vendor shall provide a non-proprietary cryptographic module security policy that fulfills but is not limited to the minimum security policy requirements as specified in B.2.1 to B.2.12 of ISO/IEC 19790:2012.

Required Test Procedures

TEB.01.01: The tester shall verify that the vendor provides a non-proprietary cryptographic module security policy that fulfills but is not limited to the minimum security policy requirements as specified in B.2.1 to B.2.12 of ISO/IEC 19790:2012.

ASB.02: (Security policy – Levels 1, 2, 3, and 4)

The format of the security policy shall be presented in the order indicated in this Appendix *{ISO/IEC 19790:2012 Annex B}* or as specified by a validation authority.

Required Vendor Information

VEB.02.01: The vendor shall provide a non-proprietary cryptographic module security policy that is presented in the order specified in B.2.1 to B.2.12 of ISO/IEC 19790:2012 or as specified by a validation authority.

Required Test Procedures

TEB.02.01: The tester shall verify that the vendor provides a non-proprietary cryptographic module security policy that is presented in the order specified in B.2.1 to B.2.12 of ISO/IEC 19790:2012 or as specified by a validation authority.

ASB.03: (Security policy – Levels 1, 2, 3, and 4)

The security policy shall not be marked as proprietary or copyrighted without a statement allowing copying or distribution.

Required Vendor Information

VEB.03.01: The vendor shall provide a security policy that is not marked as proprietary or copyrighted.

VEB.03.02: If the vendor provided security policy is marked copyrighted then it shall include a statement allowing copying or distribution.

Required Test Procedures

TEB.03.01: The tester shall verify that the vendor provided security policy is not marked as proprietary or copyrighted.

TEB.03.02: If the vendor provided security policy is marked copyrighted then the tester shall verify that it includes a statement allowing copying or distribution.

6.15 C - Approved security functions

NOTE 1 ISO/IEC 19790:2012, Annex C specifies the approved security functions for a cryptographic module.

NOTE 2 There are no requirements for this subclause.

6.16 D - Approved sensitive security parameter generation and establishment methods

NOTE 1 ISO/IEC 19790:2012, Annex D specifies the approved sensitive security parameter generation and establishment methods for a cryptographic module.

NOTE 2 There are no requirements for this subclause.

6.17 E - Approved authentication mechanisms

NOTE 1 ISO/IEC 19790:2012, Annex E specifies the approved authentication mechansims for a cryptographic module.

NOTE 2 There are no requirements for this subclause.

6.18 F - Approved non-invasive attack mitigation test metrics

NOTE 1 ISO/IEC 19790:2012, Annex F specifies the approved non-invasive mitigation test metrics for a cryptographic module.

NOTE 2 There are no requirements for this subclause.

ICS 35.040

Price based on 129 pages