Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

January 04, 2011
Draft

CMVP Program Staff
(NIST, CSEC and CMVP Laboratories)

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick Gallagher, Under Secretary for Standards
and Technology Director

Derived Test Requirements for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

1. Introduction

Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of the cryptographic module. These areas include the following:

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
9. Self Tests
10. Design Assurance
11. Mitigation of Other Attacks

The Cryptographic Module Validation Program (CMVP - www.nist.gov/cmvp) validates cryptographic modules to FIPS PUB 140-2 and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC - www.cse-cst.gc.ca). Modules validated as conforming to FIPS PUB 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated information (Canada).

In the CMVP, vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested. Organizations wishing to have validations performed would contract with the laboratories for the required services.

2. Purpose

The purpose of this document is to describe the methods that will be used by accredited laboratories to test whether the cryptographic module conforms to the requirements of FIPS PUB 140-2. It includes detailed procedures, inspections, and tests that the tester must follow, and the expected results that must be achieved for the cryptographic module to satisfy the FIPS PUB 140-2 requirements. These detailed methods are intended to provide a high degree of objectivity during the testing process and to ensure consistency across the accredited testing laboratories.

This document also details the requirements for vendor information that must be provided as supplementary evidence to demonstrate conformance to FIPS PUB 140-2 requirements. Vendors may use this document as a guide in trying to determine if their cryptographic modules meet the security requirements of FIPS PUB 140-2 before they apply to the laboratory for testing.

3. Document Organization

This document includes eleven sections, corresponding to the eleven areas of security requirements of FIPS PUB 140-2.

Within each section, the corresponding security requirements from FIPS PUB 140-2 are divided into a set of assertions (i.e., statements that must 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 FIPS PUB 140-2.

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 FIPS PUB 140-2 (i.e., one through eleven), and "sequence_number" is a sequential identifier for assertions within a section. 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 must provide in order for the tester to determine conformance to the given assertion. These requirements are denoted by the form

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

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

Also following each assertion and the requirements levied on the vendor is a set of requirements levied on the tester of the cryptographic module. These requirements instruct the tester as to what he or she must 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.

4. Disclaimer

Every attempt has been made to maintain complete consistency with FIPS PUB 140-2. However, if an inconsistency is found within this *draft* of the Derived Test Requirements for FIPS PUB 140-2, the requirements of FIPS PUB 140-2 take precedence.

Table of Contents

1. CRYPTOGRAPHIC MODULE SPECIFICATION

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

Note: This assertion is not separately tested.

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

Note: This assertion is tested as part of AS01.12.

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

Required Vendor Information

VE01.03.01: The vendor provided nonproprietary security policy shall provide a description of the Approved mode of operation.

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

Required Test Procedure

TE01.03.01: The tester shall verify that the vendor provided nonproprietary security policy contains a description of the Approved mode of operation.

TE01.03.02: The tester shall invoke the Approved mode of operation using the vendor provided instructions found in the nonproprietary security policy.

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

Note: This assertion is tested as part of AS01.08.

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

Required Vendor Information

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

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

Required Test Procedures

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

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

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

AS01.07: (Levels 1, 2, 3, and 4) The following documentation requirements shall apply to all security-specific hardware, software, and firmware contained within the cryptographic module.

Note: This assertion is not separately tested.

AS01.08: (Levels 1, 2, 3, and 4) Documentation shall specify the hardware, software, and firmware components of the cryptographic module, specify the cryptographic boundary surrounding these components, and describe the physical configuration of the module.

Required Vendor Information

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

1. Integrated circuits, including processors, memory, and (semi-) custom integrated circuits
2. Other active electronic circuit elements
3. Power inputs and outputs, and internal power supplies or converters

4. Physical structures, including circuit boards or other mounting surfaces, enclosures, and connectors

5. Software and firmware modules

6. Other component types not listed above

VE01.08.02: The above list of components shall be consistent with the information provided for all other assertions of this section.

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

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

VE01.08.05: The vendor documentation shall specify the physical embodiments of the module – single-chip cryptographic module, multiple-chip embedded cryptographic module, or multiple-chip standalone cryptographic module, as defined in Section 4.5 of FIPS PUB 140-2.

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

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

Required Test Procedures

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

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

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

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

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

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

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

6. Other active electronic circuit elements (the vendor does not have to list passive circuit elements such as pull up/pull down resistors or bypass capacitors if they do not play a significant role in the security of the cryptographic module and are not at the cryptographic boundary)

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

8. Circuit boards or other component mounting surfaces

9. Enclosures, including any removable access doors or covers

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

11. Software/firmware modules that are modifiable.

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

13. Other component types not listed above

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

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

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

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

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

5. Any components that are to be excluded from the requirements of FIPS PUB 140-2 under the provisions of assertion AS01.09. Verify that components to be so excluded are still listed in the master components list.

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

TE01.08.05: The tester shall verify that the vendor provided documentation includes sufficient detail for components at the cryptographic boundary to precisely define the cryptographic boundary.

TE01.08.06: The tester shall verify that the cryptographic boundary is physically contiguous, such that there are no gaps that could allow uncontrolled input, output, or other access into the cryptographic module. (Physical protection and tamper protection are covered separately in requirements under Section 4.5 of FIPS PUB 140-2.) The module design must also ensure that there are no uncontrolled interfaces into or out of the cryptographic module that could pass critical security parameters (CSPs), plaintext data, or other information that if misused could lead to a compromise.

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

TE01.08.08: As a partial exception to the above requirements, the vendor is allowed to exclude certain components from the requirements of FIPS PUB 140-2 after satisfying the requirements under assertion AS01.09 in this section. The vendor may then treat such excluded components as effectively outside the cryptographic boundary of the module. In this case, the tester shall verify that any interfaces or physical connections between such excluded components and the rest of the module do not allow uncontrolled release of CSPs, plaintext data, or other information that if misused could lead to a compromise.

TE01.08.09: The tester shall verify that the vendor identified that the cryptographic module is either a single-chip module, a multi-chip embedded module, or a multi-chip standalone module as defined in Section 4.5 of FIPS PUB 140-2.

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

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

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

1. Enclosure shape and approximate dimensions, including any access doors or covers
2. Circuit board(s) approximate dimensions, layout, and interconnections
3. Location of power supply, power converters, and power inputs and outputs
4. Interconnection wiring runs: routing and terminals
5. Cooling arrangements, such as conduction plates, cooling airflow, heat exchanger, cooling fins, fans, or other arrangements for removing heat from the module
6. Other component types not listed above

AS01.09: (Levels 1, 2, 3, and 4) Documentation shall specify any hardware, software, or firmware components of the cryptographic module that are excluded from the security requirements of this standard and explain the rationale for the exclusion.

Required Vendor Information

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

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

Required Test Procedures

TE01.09.01: The tester shall determine whether the vendor indicates that any components of the module are to be excluded from the requirements of FIPS PUB 140-2. If none are so listed, all components must meet the other requirements of this and all other sections.

TE01.09.02: If the vendor has indicated that certain components of the module are to be excluded from the requirements of FIPS PUB 140-2, the tester shall determine that a rationale for the exclusion is provided. The rationale must show that even if the component malfunctions, it cannot cause a potential release of CSPs, plaintext data, or other information that if misused could lead to a compromise. Rationale that may be acceptable, if adequately supported by documentation, include:

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

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

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

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

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

Note: This assertion is tested as part of AS02.01.

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

Note: This assertion is tested as part of AS02.01.

AS01.12: (Levels 1, 2, 3, and 4) Documentation shall list all security functions, both Approved and non-Approved, that are employed by the cryptographic module and shall specify all modes of operation, both Approved and non-Approved.

Required Vendor Information

VE01.12.01: The vendor shall provide a validation certificate for all Approved cryptographic algorithms.

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

VE01.12.03: The vendor shall provide a list of all vendor affirmed security methods.

VE01.12.04: The vendor provided nonproprietary security policy shall include reference to all vendor affirmed security methods.

Required Test Procedures

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

TE01.12.02: The tester shall verify that the vendor has provided the list of non-Approved security functions as described above.

TE01.12.03: The tester shall verify that the vendor has provided the list of vendor affirmed security methods as described above.

TE01.12.04: The tester shall verify that the vendor provided documentation specifies how the implemented vendor affirmed security methods conform to the relevant standards.

AS01.13: (Levels 1, 2, 3, and 4) Documentation shall specify a block diagram depicting all of the major hardware components of the cryptographic module and their interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory.

Required Vendor Information

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

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

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

VE01.13.03: The block diagram shall show interconnections among major components of the module and between the module and equipment or components outside of the cryptographic boundary.

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

Required Test Procedures

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

1. Microprocessors or any other processors listed in the master components list under assertion AS01.08 in this section

2. Input/output buffer memory that stores or processes general input or output data other than plaintext/ciphertext message data or control information

3. Plaintext/ciphertext buffer memory that stores or processes message data to be encrypted or decrypted

4. Control buffer memory that stores or processes control and status information that is input into the module or output from the module

5. Key storage

6. Working memory for processing information

7. Program memory containing executable software or firmware code

8. (Semi-) custom integrated circuits, (e.g., application-specific integrated circuits, gate arrays, field programmable gate arrays, programmable logic arrays, or other programmable logic devices

9. Other components types not listed above

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

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

AS01.14: (Levels 1, 2, 3, and 4) Documentation shall specify the design of the hardware, software, and firmware components of the cryptographic module. High-level specification languages for software/firmware or schematics for hardware shall be used to document the design.

Required Vendor Information

VE01.14.01: The vendor shall provide a detailed specification of the design of the hardware, software, and/or firmware contained in the module. This documentation shall include, the finite state model and description referred to in Section 4.4 of FIPS PUB 140-2. If the relationship between the finite state model and the design specification is not clear, the vendor shall provide additional documentation that describes this relationship.

Required Test Procedures

TE01.14.01: The tester shall compare the design specification against the list of names of all hardware, software, and firmware components as documented in VE10.07.01 to verify that the relationship between the finite state model and the design specification can be determined.

AS01.15: (Levels 1, 2, 3, and 4) Documentation shall specify all security-related information, including secret and private cryptographic keys (both plaintext and encrypted), authentication data (e.g., passwords, PINs), CSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module.

Required Vendor Information

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

Required Test Procedures

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

AS01.16: (Levels 1, 2, 3, and 4) Documentation shall specify the cryptographic module security policy. The security policy shall include the rules derived from the requirements of this standard and the rules derived from any additional requirements imposed by the vendor.

Required Vendor Information

VE01.16.01: The vendor shall provide a separate nonproprietary security policy. The security policy is defined in Appendix C of FIPS PUB 140-2.

Required Test Procedures

TE01.16.01: The tester shall review the nonproprietary security policy provided by the vendor. The tester must determine that the nonproprietary security policy meets the requirements specified in Appendix C of FIPS PUB 140-2.

2. CRYPTOGRAPHIC MODULE PORTS AND INTERFACES

AS02.01: (Levels 1, 2, 3, and 4) The cryptographic module shall restrict all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module.

Required Vendor Information

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

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

VE02.01.02: 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 Sections 1 and 10. 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.

VE02.01.03: For each physical or logical input to the cryptographic module, or physical and logical output from the module, 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 sections 1 and 10, and the specifications of the logical interfaces provided in assertions AS02.03 to AS02.09 of this section.

Required Test Procedures

TE02.01.01: The tester shall verify that vendor documentation specifies each of the physical ports and logical interfaces of the cryptographic module. The required specifications shall include:

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

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

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

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

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

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

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

TE02.01.02: The tester shall verify that 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 Sections 1 and 10, and any other documentation provided by the vendor. The documentation shall specify the relationship of the information flows and physical access points to the physical ports and logical interfaces of the cryptographic module. The tester shall compare the above information with the information provided under assertions AS01.08, AS01.10, and AS01.13 and verify that there are no inconsistencies in the description of components and physical layout for the input/output ports.

TE02.01.03: The tester shall verify that for each physical or logical input to the cryptographic module, or physical and logical output from the module, 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 sections 1 and 10, and the specifications of the logical interfaces provided in assertions AS02.03 to AS02.09 of this section.

TE02.01.04: The tester shall verify, by inspection of the cryptographic module, that all the above specifications provided by vendor documentation are consistent with the actual design of the cryptographic module.

AS02.02: (Levels 1, 2, 3, and 4) The cryptographic module interfaces shall be logically 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).

Required Vendor Information

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

VE02.02.02: 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, vendor documentation shall specify how the information from the different interface categories is kept logically separate.

Required Test Procedures

TE02.02.01: The tester shall verify, from vendor documentation and by inspection of the cryptographic module, that the module interfaces are logically distinct and isolated for the categories of interfaces specified in assertions AS02.03 and, if applicable, AS02.09 of this section. This information shall be

consistent with the specification and design of the logical interfaces and physical ports provided in AS02.01 in this section.

TE02.02.02: The tester shall verify that 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 vendor documentation specifies how the information flows for the input, output, control, and status interfaces are kept logically separate.

AS02.03: (Levels 1, 2, 3, and 4) The cryptographic module shall have the following four logical interfaces ("input" and "output" are indicated from the perspective of the module):

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

Required Vendor Information

VE02.03.01: Vendor documentation shall specify that the following four logical interfaces have been designed within the cryptographic module ("input" and "output" are indicated from the perspective of the module):

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

Required Test Procedures

TE02.03.01: The tester shall verify that vendor documentation specifies that the four logical interfaces as listed in VE02.03.01 have been designed within the cryptographic module. If so, verification that the logical interfaces within the cryptographic module function as specified shall be performed under assertions AS02.04, AS02.05, AS02.07, and AS02.08.

AS02.04: (Levels 1, 2, 3, and 4) All data (except control data entered via the control input interface) that is input to and processed by the cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and status information from another module) shall enter via the "data input" interface.

Required Vendor Information

VE02.04.01: The cryptographic module shall have a data input interface. All data (except control data entered via the control input interface) that is to be input to and processed by the cryptographic module shall enter via the data input interface, including:

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

VE02.04.02: If applicable, vendor documentation shall specify any external input devices to be used with the cryptographic module for the entry of data into the data input interface, such as smart cards, tokens, keypads, key loaders, and/or biometric devices.

Required Test Procedures

TE02.04.01: The tester shall verify, by inspection, that the cryptographic module includes a data input interface, and that the data input interface functions as specified. The tester shall verify that all data (except control data entered via the control input interface) that is to be input to and processed by the cryptographic module enters via the data input interface, including:

1. Plaintext data that is to be encrypted or signed by the cryptographic module
2. Ciphertext or signed data that is to be decrypted or verified by the module
3. Plaintext or encrypted cryptographic keys and other key management data that are input into and used by the cryptographic module, including initialization data and vectors, split key information, and/or key accounting information. (Other key management requirements are covered in section 7)
4. Plaintext or encrypted authentication data that is input into the cryptographic module, including passwords, PINs, and/or biometric information
5. Status information from external sources (e.g., another cryptographic module or device)
6. Any other information that is input into the cryptographic module for processing or storage, except for control information that is covered separately in AS02.07

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

TE02.04.02: The tester shall verify if 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.

AS02.05: (Levels 1, 2, 3, and 4) All data (except status data output via the status output interface) that is output from the cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and control information for another module) shall exit via the "data output" interface.

Required Vendor Information

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

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

VE02.05.02: If applicable, vendor documentation shall specify any external output devices to be used with the cryptographic module for the output of data from the data output interface, such as smart cards, tokens, displays, and/or other storage devices.

Required Test Procedures

TE02.05.01: The tester shall verify, by inspection, that the cryptographic module includes a data output interface, and that the data output interface functions as specified. The tester shall verify that all data (except status data output via the status output interface) that has been processed and is to be output by the cryptographic module exits via the data output interface, including:

1. Plaintext data that has been decrypted by the cryptographic module
2. Ciphertext data that has been encrypted, and digital signatures that have been generated by the cryptographic module
3. Plaintext or encrypted cryptographic keys and other key management data that have been internally generated and output from the module, including initialization data and vectors, split key information, and/or key accounting information (other key management requirements are covered in Section 7)
4. Control information sent outside the cryptographic module to external targets (e.g., another cryptographic module or device)
5. Any other information that is output from the cryptographic module after processing or storage except for status information that is covered separately in AS02.08

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

TE02.05.02: The tester shall verify if vendor documentation specifies any external output devices to be used with the cryptographic module for the output of data from the data input interface, such as smart cards, tokens, displays, and/or other storage devices. The tester shall output data from the data output interface using the identified external output device(s), and verify that output of data using the external output device functions as specified.

AS02.06: (Levels 1, 2, 3, and 4) All data output via the data output interface shall be inhibited when an error state exists and during self-tests.

Required Vendor Information

VE02.06.01: Vendor documentation shall specify how the cryptographic module ensures that all data output via the data output interface is inhibited whenever the module is in an error state (error states are covered in Section 4). Status information may be allowed from the status output interface to identify the type of error, as long as no CSPs, plaintext data, or other information that if misused could lead to a compromised.

VE02.06.02: Vendor documentation shall specify how the design of the cryptographic module ensures that all data output via the data output interface is inhibited whenever the module is in a self-test condition (self-tests are covered in Section 9). Status information to display the results of the self-tests may be allowed from the status output interface, as long as no CSPs, plaintext data, or other information that if misused could lead to a compromise.

Required Test Procedures

TE02.06.01: The tester shall verify that vendor documentation specifies that all data output via the data output interface is inhibited whenever the cryptographic module is in an error state. The tester shall verify from vendor documentation that once an error condition is detected and the error state is entered, all data output via the data output interface is inhibited, until error recovery occurs. Status information to identify the type of error may be allowed from the status output interface, as long as the tester can verify that no CSPs, plaintext data, or other information that if misused could lead to a compromise. The tester shall also verify that the error states specified in response to this assertion are identical to the error states specified under AS04.06.

TE02.06.02: To the extent that the cryptographic module design and operating procedures allow, the tester shall cause the cryptographic module to enter each specified error state and verify that all data output via the data output interface is inhibited. If status information is output from the status output interface to identify the type of error, the tester shall verify that the information output is not sensitive. The following actions may be used to cause the cryptographic module to enter an error state - opening a tamper-detected cover or door, entering incorrectly-formatted commands, keys, or parameters, reducing input voltage, and/or any other error-causing actions.

TE02.06.03: The tester shall verify that 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 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 AS09.08.

TE02.06.04: To the extent that the cryptographic module design and operating procedures allow, the tester shall command the module to perform the self-tests and verify that all data output via the data output interface is inhibited. If status information is output from the status output interface to display the results of the self-tests, the tester shall verify that no CSPs, plaintext data, or other information that if misused could lead to a compromise.

TE02.06.05: The tester shall verify that 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.

AS02.07: (Levels 1, 2, 3, and 4) All input commands, signals, and control data (including calls and manual controls such as switches, buttons, and keyboards) used to control the operation of the cryptographic module shall enter via the "control input" interface.

Required Vendor Information

VE02.07.01: The cryptographic module shall have a control input interface. All commands, signals, and control data (except data entered via the data input interface) used to control the operation of the cryptographic module shall enter via the control input interface, including:

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

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

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

4. Any other input control data

VE02.07.02: If applicable, vendor documentation shall specify any external input devices to be used with the cryptographic module for the entry of commands, signals, and control data into the control input interface, such as smart cards, tokens, or keypads.

Required Test Procedures

TE02.07.01: The tester shall verify, by inspection, that the cryptographic module includes a control input interface, and that the control input interface functions as specified. The tester shall verify that all commands, signals, and control data (except data entered via the data input interface) used to control the operation of the cryptographic module shall enter via the control input interface, including:

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

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

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

4. Any other input control data

TE02.07.02: The tester shall verify if 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 output device(s), and verify that input of commands using the external output device functions as specified.

AS02.08: (Levels 1, 2, 3, and 4) All output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of the cryptographic module shall exit via the "status output" interface.

Required Vendor Information

VE02.08.01: The cryptographic module shall have a status output interface. All status information, signals, logical indicators, and physical indicators used to indicate or display the status of the module shall exit via the status output interface, including:

1. Status information output logically via an API

2. Signals output logically or physically via one or more physical

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

4. Any other output status information

VE02.08.02: If applicable, vendor documentation shall specify any external output devices to be used with the cryptographic module for the output of status information, signals, logical indicators, and physical indicators via the status output interface, such as smart cards, tokens, displays, and/or other storage devices.

Required Test Procedures

TE02.08.01: The tester shall verify, by inspection, that the cryptographic module includes a status output interface, and that the status output interface functions as specified. The tester shall verify that all status

information, signals, logical indicators, and physical indicators used to indicate or display the status of the module shall exit via the status output interface, including:

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

2. Signals output logically or physically via one or more physical ports, such as status information sent through a serial port or a PC Card connector

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

4. Any other output status information

AS02.09: (Levels 1, 2, 3, and 4) All external electrical power that is input to the cryptographic module (including power from an external power source or batteries) shall enter via a power port.

Required Vendor Information

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

Required Test Procedures

TE02.09.01: The tester shall verify if 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 vendor documentation specifies a power interface and a corresponding physical port.

TE02.09.02: The tester shall verify, by inspection of the cryptographic module, that all power entering or exiting the module to/from other devices external to the cryptographic boundary passes through the specified power interface. Note that a power interface may not be required if all power is provided or maintained internally to the module, and that replacement of an internal battery is considered a physical maintenance activity, and is subject to the requirements provided under the assertions in Section 5.

AS02.10: (Levels 1, 2, 3, and 4) The cryptographic module shall distinguish between data and control for input and data and status for output.

Required Vendor Information

VE02.10.01: Vendor documentation shall specify how the cryptographic module distinguishes between data and control for input and data and status for output, and how the physical and logical paths followed by the input data and control information entering the module via the applicable input interfaces are logically or physically disconnected from the physical and logical paths followed by the output data and status information exiting the module via the applicable output interfaces.

Required Test Procedures

TE02.10.01: The tester shall verify that vendor documentation specifies how the cryptographic module distinguishes between data and control for input and data and status for output. Input data entered from the data input interface, and control information entered from the control input interface shall be logically or physically distinguished from output data exiting to the output data interface and status information exiting to the status output interface.

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

TE02.10.03: The tester shall verify, by inspection, the consistency of the vendor documentation, and that the cryptographic module distinguishes between data and control for input and data and status for output, and that the physical and logical paths followed by the input data and control information entering the module via the applicable input interfaces are logically or physically disconnected from the physical and logical paths followed by the output data and status information exiting the module via the applicable output interfaces.

AS02.11: (Levels 1, 2, 3, and 4) All input data entering the cryptographic module via the "data input" interface shall only pass through the input data path.

Required Vendor Information

VE02.11.01: Vendor documentation shall specify the physical and logical paths used by all major categories of input data entering the cryptographic module via the data input interface and the applicable physical ports. The documentation shall include a specification of the applicable paths (e.g., by highlighted or annotated copies of the schematics, block diagrams, or other information provided under AS01.08, AS01.09, and AS01.13). All input data entering the cryptographic module via the data input interface shall only use the specified paths while being processed or stored by each physical or logical sub-section of the module.

Required Test Procedures

TE02.11.01: The tester shall verify that vendor documentation specifies the physical and logical paths used by all major categories of input data entering the cryptographic module via the data input interface. The tester shall also verify that the paths shall be documented in the specification (e.g., by highlighted or annotated copies of the schematics, block diagrams, or other information provided under AS01.08, AS01.09, and AS01.13). The input data paths shall be specified in sufficient detail for the tester to determine which type of data pass through each applicable physical port.

TE02.11.02: The tester shall verify from vendor documentation and by inspection of the cryptographic module, that all input data entering the module via the data input interface and applicable physical ports only use the specified paths. The tester shall examine all logical and physical information flows and shall verify that the specification of the paths used by the input data is consistent with the design and operation of the cryptographic module. The tester shall verify that there are no conflicts between the applicable paths that may lead to the compromise of CSPs, plaintext data, or other information.

AS02.12: (Levels 1, 2, 3, and 4) All output data exiting the cryptographic module via the "data output" interface shall only pass through the output data path.

Required Vendor Information

VE02.12.01: Vendor documentation shall specify the physical and logical paths used by all major categories of output data exiting the cryptographic module via the data output interface and the applicable physical ports. The documentation shall include a specification of the applicable paths (e.g., by highlighted or annotated copies of the schematics, block diagrams, or other information provided under AS01.08, AS01.09, and AS01.13). All output data exiting the cryptographic module via the data output interface shall only use the specified paths.

Required Test Procedures

TE02.12.01: The tester shall verify that vendor documentation specifies the physical and logical paths used by all major categories of output data exiting the cryptographic module via the data output interface. The tester shall also verify that the paths shall be documented in the specification (e.g., by highlighted or annotated copies of the schematics, block diagrams, or other information provided under AS01.08, AS01.09, and AS01.13). The output data paths shall be specified in sufficient detail for the tester to determine which type of data passes through each applicable physical port.

TE02.12.02: The tester shall verify from vendor documentation and by inspection of the cryptographic module, that all output data exiting the module via the data output interface and applicable physical ports only use the specified paths. The tester shall examine all logical and physical information flows and shall verify that the specification of the paths used by the output data is consistent with the design and operation of the cryptographic module. The tester shall verify that there are no conflicts between the applicable paths that may lead to the comproise of CSPs, plaintext data, or other information.

AS02.13: (Levels 1, 2, 3, and 4) The output data path shall be logically disconnected from the circuitry and processes while performing key generation, manual key entry, or key zeroization.

Required Vendor Information

VE02.13.01: Vendor documentation shall specify how the physical and logical paths used by all major categories of output data exiting the cryptographic module are logically or physically disconnected from the processes performing key generation, manual key entry, and zeroization of cryptographic keys and CSPs. The cryptographic module shall not allow the specified key processes to pass key/CSP information to the output data path, and shall not allow output data exiting the module to interfere with the key processes.

Required Test Procedures

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

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

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

AS02.14: (Levels 1, 2, 3, and 4) To prevent the inadvertent output of sensitive information, two independent internal actions shall be required to output data via any output interface through which plaintext cryptographic keys or CSPs or sensitive data are output (e.g., two different software flags are set, one of which may be user initiated; or two hardware gates are set serially from two separate actions).

Required Vendor Information

VE02.14.01: If the cryptographic module allows plaintext cryptographic key components or other unprotected CSPs to be output on one or more physical ports, two independent internal actions shall be performed by the module before the plaintext cryptographic key components or other unprotected CSPs may be output. Vendor documentation shall specify the two independent internal actions performed and

how the two independent internal actions protect against the inadvertent release of the plaintext cryptographic key components or other unprotected CSPs.

Required Test Procedures

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

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

AS02.15: (Levels 1, 2, 3, and 4) Documentation shall specify the physical ports and logical interfaces and all defined input and output data paths.

Note: This assertion is not separately tested. Verification of vendor documentation is performed under assertions AS02.01 to AS02.14 and AS02.16 to AS02.18.

AS02.16: (Levels 3 and 4) The physical port(s) used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be physically separated from all other ports of the cryptographic module or AS02.17 must be satisfied.

Required Vendor Information

VE02.16.01: Vendor documentation shall specify if the cryptographic module inputs or outputs plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs. The physical port(s) used for the input and output of plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs shall be physically separated from all other physical ports of the cryptographic module.

Required Test Procedures

TE02.16.01: The tester shall verify if vendor documentation specifies whether the cryptographic module inputs or outputs plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs. The tester shall verify, from 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 cryptographic key components, plaintext authentication data, or other unprotected CSPs are physically separated from all other physical ports of the module.

TE02.16.02: If the cryptographic module inputs or outputs plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs, the tester shall verify that only plaintext cryptographic keys, plaintext authentication data, or other unprotected CSPs enter or exit the module through the applicable physical ports, and that no other data, plaintext or encrypted, enters or exits the module via the applicable physical ports.

AS02.17: (Levels 3 and 4) The logical interfaces used for the input and output of plaintext cryptographic key components, authentication data, and CSPs shall be logically separated from all other interfaces using a trusted path or AS02.16 must be satisfied.

Required Vendor Information

VE02.17.01: Vendor documentation shall specify if the cryptographic module inputs or outputs plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs. The logical interfaces used for the input and output of plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs shall be logically separated from all other interfaces using a trusted path.

Required Test Procedures

TE02.17.01: The tester shall verify if vendor documentation specifies whether the cryptographic module inputs or outputs plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs. The tester shall verify, from vendor documentation and also by inspection of the cryptographic module, that the applicable logical ports used for the input and output of plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs are logically separated from all other logical interfaces of the module using a trusted path

TE02.17.02: If the cryptographic module inputs or outputs plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs, the tester shall verify that only plaintext cryptographic keys, plaintext authentication data, or other unprotected CSPs enter or exit the module through the applicable logical interface using the trusted path, and that no other data, plaintext or encrypted, enters or exits the module via the applicable logical interface using the trusted path.

AS02.18: (Levels 3 and 4) Plaintext cryptographic key components, authentication data, and other CSPs shall be directly entered into the cryptographic module (e.g., via a trusted path or directly attached cable).

Required Vendor Information

VE02.18.01: Vendor documentation shall specify if the cryptographic module inputs plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs. The physical ports used for the input of these parameters shall be directly connected to the cryptographic boundary (e.g., via a trusted path or directly attached cable) of the cryptographic module without passing through any intervening systems, processors, circuitry, or other areas outside the cryptographic boundary.

Required Test Procedures

TE02.18.01: The tester shall verify if vendor documentation specifies whether the cryptographic module inputs plaintext cryptographic key components, plaintext authentication data, or other unprotected CSPs. The tester shall verify from vendor documentation and also by inspection of the physical ports and the cryptographic boundary, that the physical ports used for the input of these parameters shall be directly connected to the cryptographic boundary (e.g., via a trusted path or directly attached cable) of the cryptographic module without passing through any intervening systems, processors, circuitry, or other areas outside the cryptographic boundary.

3. ROLES, SERVICES, AND AUTHENTICATION

AS03.01: (Levels 1, 2, 3, and 4) The cryptographic module shall support authorized roles for operators and corresponding services within each role.

Note: This assertion is not separately tested.

AS03.02: (Levels 1, 2, 3, and 4) If the cryptographic module supports concurrent operators, then the module shall internally maintain the separation of the roles assumed by each operator and the corresponding services.

Required Vendor Information

VE03.02.01: The vendor documentation shall specify whether multiple concurrent operators are allowed. The vendor shall describe the method by which separation of the authorized roles and services performed by each operator is achieved. The vendor documentation shall also describe any restrictions on concurrent operators (e.g., one operator in a maintenance role and another in a user role simultaneously is not allowed).

Required Test Procedures

TE03.02.01: The tester shall review the vendor documentation and verify that the method implemented by the module to enforce separation between the roles and services performed by concurrent operators is described.

TE03.02.02: The tester shall assume the identity of two independent operators: Operator1 and Operator2. The operators shall assume different roles. The tester shall verify that only the services allocated to the each role can be performed in that role. The tester shall also attempt, for each operator, to access services that are unique to the role assumed by the other operator in order to verify that separation is maintained between the roles and services allowed in concurrent operators.

TE03.02.03: If the vendor documentation specifies any restrictions on concurrent operators, the tester shall attempt to violate the restrictions by attempting to concurrently assume restricted roles as independent operators and verify that the module enforces the restrictions by preventing the second operator from assuming the role.

3.1 Roles

AS03.03: (Levels 1, 2, 3, and 4) The cryptographic module shall support the following authorized roles for operators:

> ***User Role.*** **The role assumed to perform general security services, including cryptographic operations and other Approved security functions.**
>
> ***Crypto Officer Role*****: The role assumed to perform a set of cryptographic initialization or management functions (e.g., module initialization, input/output of cryptographic keys and CSPs, and audit functions).**

Required Vendor Information

VE03.03.01: In the documentation required to satisfy VE03.06.01, the vendor shall include at least one user role and one crypto-officer role.

Required Test Procedures

TE03.03.01: The tester shall review the vendor documentation and verify that at least one user role and one crypto-officer role are defined. These roles shall be specified by name and allowed services. These roles shall be described as specified in AS03.03. (The assumption of roles is tested by TE03.06.02.)

AS03.04: (Levels 1, 2, 3, and 4) If the cryptographic module allows operators to perform maintenance services, then the module shall support the following authorized role:

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

Required Vendor Information

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

Required Test Procedures

TE03.04.01: The tester shall review the specifications of the module interfaces to determine whether a maintenance interface is specified (see AS05.07). If so, the tester shall check the vendor documentation pertaining to the authorized roles and verify that the maintenance role is specified by name, purpose, and allowed services. (The assumption of roles is tested by TE03.06.02.)

AS03.05: (Levels 1, 2, 3, and 4) All plaintext secret and private keys and unprotected CSPs shall be zeroized when entering or exiting the maintenance role.

Required Vendor Information

VE03.05.01: The vendor documentation shall specify how the module's plaintext secret and private keys and other unprotected critical security parameters, as defined in Section 2.1 of FIPS PUB 140-2, are actively zeroized when the maintenance role is entered or exited.

Required Test Procedures

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

TE03.05.02: The tester shall, while in a non-maintenance role, load nonzero values for all private and secret keys and other unprotected CSPs. Upon assuming the maintenance role, the tester shall verify that zeroization has taken place.

TE03.05.03: While in the maintenance role, the tester shall load nonzero values for all private and secret keys and other unprotected CSPs and, upon exit from the maintenance role, shall verify that zeroization has taken place.

AS03.06: (Levels 1, 2, 3, and 4) Documentation shall specify all authorized roles supported by the cryptographic module.

Required Vendor Information

VE03.06.01: Vendor documentation shall specify each distinct authorized role, including its name and the services that are performed in the role.

Required Test Procedures

TE03.06.01: The tester shall review the vendor documentation and verify that, for each defined role, the name and available services for this role are specified. The roles that should be described are as follows:

1. Crypto-officer role (one or more)
2. User role (required) (one or more)
3. Maintenance role (only if the module includes a maintenance interface)
4. Other roles

TE03.06.02: The tester shall assume each of the authorized roles described in the vendor documentation and verify that each of them can be assumed. Verification of the services that are designated for each role will be performed under AS03.14.

3.2 Services

AS03.07: (Levels 1, 2, 3, and 4) *Services* shall refer to all of the services, operations, or functions that can be performed by the cryptographic module.

Note: This assertion is not separately tested.

AS03.08: (Levels 1, 2, 3, and 4) Service inputs shall consist of all data or control inputs to the cryptographic module that initiate or obtain specific services, operations, or functions.

Note: This assertion is not separately tested.

AS03.09: (Levels 1, 2, 3, and 4) *Service outputs* shall consist of all data and status outputs that result from services, operations, or functions initiated or obtained by service inputs.

Note: This assertion is not separately tested.

AS03.10: (Levels 1, 2, 3, and 4) Each service input shall result in a service output.

Note: This assertion is not separately tested.

AS03.11: (Levels 1, 2, 3, and 4) The cryptographic module shall provide the following services to operators:

> ***Show Status.*** **Output the current status of the cryptographic module.**
>
> ***Perform Self-Tests.*** **Initiate and run the self-tests as specified in Section 4.9.**
>
> ***Perform Approved Security Function.*** **Perform at least one Approved security function used in an Approved mode of operation, as specified in Section 4.1**

Required Vendor Information

VE03.11.01: The vendor documentation shall describe the output of the current status of the module and the initiation and running of user callable self-tests, along with other services as specified by VE03.14.01 and VE03.15.01.

Required Test Procedures

TE03.11.01: The tester shall check the vendor documentation to verify that the “Show Status” service and the user callable self-test initiation service are each allocated to at least one authorized role. The tester shall verify that these services are described as specified in AS.03.14.

TE03.11.02: The tester shall verify that the “Show Status” indicator matches the vendor documentation.

TE03.11.03: Verification that the module provides for the initiation of the running of power-up self-tests, as specified in Section 4.9, is performed under TE03.14.02.

AS03.12: (Levels 1, 2, 3, and 4) If a cryptographic module implements a bypass capability, where services are provided without cryptographic processing (e.g., transferring plaintext through the module without encryption), then two independent internal actions shall be required to activate the capability to prevent the inadvertent bypass of plaintext data due to a single error (e.g., two different software or hardware flags are set, one of which may be user-initiated).

Required Vendor Information

VE03.12.01: If the module implements a bypass capability, the vendor documentation shall describe the bypass service as specified in AS03.12.

VE03.12.02: The finite state model and other vendor documentation shall indicate, for all transitions into an exclusive or alternating bypass state, two independent internal actions that are required to transition into each bypass state.

Required Test Procedures

TE03.12.01: The tester shall determine whether the bypass capability is implemented by the module. The tester shall check the vendor documentation to verify that the bypass capability is allocated to at least one authorized role.

TE03.12.02: The tester shall review the finite state model and other vendor documentation to determine whether each transition into an exclusive or alternating bypass state shows two independent internal actions that must occur in order for the cryptographic module to transition into either exclusive or alternating bypass state.

TE03.12.03: The tester shall attempt to transition to each bypass state from each state that shows such a transition, and determine that it takes two internal actions to accomplish each such transition.

AS03.13: (Levels 1, 2, 3, and 4) If the cryptographic module implements a bypass capability, where services are provided without cryptographic processing (e.g., transferring plaintext through the module without encryption), then the module shall show status to indicate whether

1) **the bypass capability *is not* activated, and the module is exclusively providing services *with* cryptographic processing (e.g., the plaintext *is* encrypted),**

2) **the bypass capability *is* activated and the module is exclusively providing services *without* cryptographic processing (e.g., plaintext data *is not* encrypted), or**

3) **the bypass capability *is alternately* activated and deactivated and the module is providing some services *with* cryptographic processing and some services *without* cryptographic processing (e.g., for modules with multiple communication channels, plaintext data *is* or *is not* encrypted depending on each channel configuration).**

Required Vendor Information

VE03.13.01: The vendor documentation for the “Show Status” service shall indicate bypass status.

Required Test Procedures

TE03.13.01: The tester shall review the vendor documentation for the “Show Status” service and verify the bypass service indication.

TE03.13.02: The tester shall transition to each bypass state and verify that the "Show Status" indicates the applicable bypass status.

AS03.14: (Levels 1, 2, 3, and 4) Documentation shall specify:

- **the services, operations, or functions provided by the cryptographic module, both Approved and non-Approved, and**
- **for each service provided by the module, the service inputs, corresponding service outputs, and the authorized role(s) in which the service can be performed.**

Required Vendor Information

VE03.14.01: The vendor documentation shall describe each service including purpose and function.

VE03.14.02: The vendor documentation shall specify for each service, the service inputs, corresponding service outputs, and the authorized role or roles in which the service can be performed. Service inputs shall consist of all data or control inputs to the module that initiate or obtain specific services, operations, or functions. Service outputs shall consist of all data and status outputs that result from services, operations or functions initiated or obtained by service inputs.

Required Test Procedures

TE03.14.01: 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.

TE03.14.02: The tester shall perform the following for each role:

1. Perform each of the specified services for the role to verify that they have been implemented for that role.
2. Enter each of the specified service inputs and observe that they result in the specified service outputs.
3. Attempt to perform services that are not specified for the role to verify that they have not been implemented for that role.

AS03.15: (Levels 1, 2, 3, and 4) Documentation shall specify any services provided by the cryptographic module for which the operator is not required to assume an authorized role, and how these services do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the module.

Required Vendor Information

VE03.15.01: The vendor documentation shall describe each service, including its purpose and function.

VE03.15.02: The vendor documentation shall specify, for each service, the service inputs and corresponding service outputs. Service inputs shall consist of all data or control inputs to the module that initiate or obtain specific services, operations, or functions. Service outputs shall consist of all data and status outputs that result from the services, operations, or functions initiated or obtained by service inputs.

Required Test Procedures

TE03.15.01: The tester shall check the vendor documentation and verify that the purpose and function of each service is described, and the service inputs and corresponding service outputs are described.

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

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

2. Attempt to perform services that require a role to verify that they have not been implemented.

3.3 Operator Authentication

AS03.16: (Levels 2, 3, and 4) Depending on the security level, the cryptographic module shall perform at least one of the following mechanisms to control access to the module: *role-based authentication* or *identity-based authentication*.

Note: This assertion is not separately tested.

Role-Based Authentication

AS03.17: (Level 2) If role-based authentication mechanisms are supported by the 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

VE03.17.01: The vendor shall document the type of authentication performed for the module. The vendor shall document the mechanisms used to perform the implicit or explicit selection of a role or set of roles and the authentication of the operator to assume the role(s).

Required Test Procedures

TE03.17.01: The tester shall verify that the vendor documentation specifies the mechanisms used for the selection of a role or roles and the authentication of the operator to assume a role.

TE03.17.02: The tester shall assume each role and initiate an error during the authentication procedure. The tester shall observe that the module denies access to each role.

AS03.18: (Level 2) If the cryptographic module permits an operator to change roles, then the module shall authenticate the assumption of any role that was not previously authenticated.

Required Vendor Information

VE03.18.01: The vendor documentation shall describe the ability of an operator to change roles and shall state that verification of an operator to assume a new role is required.

Required Test Procedures

TE03.18.01: The tester shall check the vendor documentation to verify that the method by which an operator can change roles includes the verification of the operator to assume a new role.

TE03.18.02: The tester shall perform the following tests:

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

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

Identity-Based Authentication

AS03.19: (Level 3 and 4) If identity-based authentication mechanisms are supported by the cryptographic module, the module shall require that the operator be individually identified, shall require that one or more roles either be implicitly or explicitly selected by the operator, and shall authenticate the identity of the operator and the authorization of the operator to assume the selected role (or set of roles).

Required Vendor Information

VE03.19.01: The vendor shall document the type of authentication implemented within the module. The vendor shall document the mechanism(s) used to perform the identification of the operator, the authentication of the operator's identity, the implicit or explicit selection of a role or set of roles, and the verification of the operator to assume the role(s).

Required Test Procedures

TE03.19.01: 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 authorization of the operator to assume a role is performed based on the authenticated identity.

TE03.19.02: The tester shall initiate an error during the authentication procedure and shall observe that the module does not allow the tester to proceed beyond the authentication procedure.

TE03.19.03: 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 observe that authorization to assume the roles is denied.

AS03.20: (Levels 3 and 4) If the cryptographic module permits an operator to change roles, then the module shall verify the authorization of the identified operator to assume any role that was not previously authorized.

Required Vendor Information

VE03.20.01: The vendor documentation shall describe the ability of an operator to change roles and shall state that verification of the authentication of the operator for a new role is required.

Required Test Procedures

TE03.20.01: The tester shall review the vendor documentation to verify that the method by which an operator can change roles without re-authentication of the operator's identity includes the verification of the authorization of the operator for a role not previously authenticated.

TE03.20.02: The tester shall perform the following tests:

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

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

AS03.21: (Levels 1, 2, 3, and 4) When the cryptographic module is powered off and subsequently powered on, the results of previous authentications shall not be retained and the module shall require the operator to be re-authenticated.

Required Vendor Information

VE03.21.01: The vendor documentation shall describe how the results of previous authentications are cleared when the module is powered off.

Required Test Procedures

TE03.21.01: The tester shall review the vendor documentation and verify that the clearing of previous authentications upon power off of the module is described.

TE03.21.02: The tester shall authenticate himself/herself 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. The module should deny access to the services and require that the tester be reauthenticated.

AS03.22: (Levels 2, 3, and 4) Authentication data within the cryptographic module shall be protected against unauthorized disclosure, modification, and substitution.

Required Vendor Information

VE03.22.01: The vendor documentation shall describe the protection of all authentication data to the module. Protection shall include the implementation of mechanisms that protect against unauthorized disclosure, modification, and substitution.

Required Test Procedures

TE03.22.01: The tester shall review 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 unauthorized disclosure, modification, and substitution.

TE03.22.02: The tester shall perform the following tests:

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

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

AS03.23: (Levels 1,2, 3, and 4) If the cryptographic module does not contain the authentication data required to authenticate the operator for the first time the module is accessed, then other authorized methods (e.g., procedural controls or use of factory-set or default authentication data) shall be used to control access to the module and initialize the authentication mechanisms.

Required Vendor Information

VE03.23.01: The vendor documentation shall specify means to control access to the module before it is initialized.

Required Test Procedures

TE03.23.01: The tester shall verify the vendor documentation describes the procedure by which the operator is authenticated upon accessing the module for the first time.

TE03.23.02: If access to the module before initialization is controlled, the tester shall initiate an error on an uninitialized module and shall verify that the module denies access. The tester shall assume the authorized 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 initialized and verify that the module denies access to the roles.

AS03.24: (Levels 2, 3, and 4) The strength of the authentication mechanism shall conform to the following specifications:

Note: This assertion is not separately tested.

AS03.25: (Levels 2, 3, and 4) For each attempt to use the authentication mechanism, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur (e.g., guessing a password or PIN, false acceptance error rate of a biometric device, or some combination of authentication methods).

Required Vendor Information

VE03.25.01: The vendor documentation shall specify each authentication method and the associated false acceptance rate or probability that a random access will succeed.

Required Test Procedures

TE03.25.01: The tester shall review the vendor documentation and verify for each authentication method that the associated false acceptance or random access rate is less than one in 1,000,000.

AS03.26: (Levels 2, 3, and 4) For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.

Required Vendor Information

VE03.26.01: The vendor documentation shall specify each authentication method and the associated probability of a successful random attempt during a one-minute period.

Required Test Procedures

TE03.26.01: The tester shall review the vendor documentation and verify for each authentication method that the associated probability of a successful random attempt during a one-minute period is less than one in 100,000.

AS03.27: (Levels 2, 3, and 4) Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password).

Required Vendor Information

VE03.27.01: The vendor documentation shall specify the method used to obscure feedback of the authentication data to an operator during entry of the authentication data.

Required Test Procedures

TE03.27.01: The tester shall review the vendor documentation and verify that the authentication data is obscured during data entry.

TE03.27.02: The tester shall enter authentication data and verify that there is no visible display of authentication data during data entry.

AS03.28: (Levels 2, 3, and 4) Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism.

Required Vendor Information

VE03.28.01: The vendor documentation shall specify the feedback mechanism that is used when the operator is entering authentication data.

Required Test Procedures

TE03.28.01: The tester shall review the vendor documentation and verify that the feedback mechanism does not provide information that could be used to guess or determine the authentication data.

TE03.28.02: The tester shall enter authentication data to assume each role to ensure that the feedback mechanism does not provide useful information.

AS03.29: (Levels 1, 2, 3, and 4) Documentation shall specify:

- **the authentication mechanisms supported by the cryptographic module,**
- **the types of authentication data required by the module to implement the supported authentication mechanisms,**
- **the authorized methods used to control access to the module for the first time and initialize the authentication mechanisms, and**
- **the strength of the authentication mechanisms supported by the module.**

Note: This assertion is not separately tested.

AS03.30: (Level 1) If authentication mechanisms are not supported by the cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator.

Required Vendor Information

VE03.30.01: The vendor shall document the type of authentication performed for the module. The vendor shall document the mechanisms used to perform the implicit or explicit selection of a role or set of roles and the authentication of the operator to assume the role(s).

VE03.30.02: The vendor provided nonproprietary security policy shall provide a description of the roles, either implicit or explicit, that the operator can assume.

VE03.30.03: The vendor provided non-proprietary security policy shall provide instructions for the operator to assume either the implicit or explicit roles.

Required Test Procedures

TE03.30.01: The tester shall verify that the vendor provided nonproprietary security policy provides a description of the roles, either implicit or explicit, that the operator can assume and the means to assume each role.

TE03.30.02: The tester shall invoke the method described in the non-proprietary security policy and verify that each role can either be implicitly or explicitly assumed.

AS03.31: (Level 2) A cryptographic module shall employ role-based authentication to control access to the module.

Note: This assertion is tested as part of AS03.17.

AS03.32: (Levels 3 and 4) The cryptographic module shall employ *identity-based* authentication mechanisms to control access to the module.

Note: This assertion is tested as part of AS03.19.

4. FINITE STATE MODEL

AS04.01: (Levels 1, 2, 3, and 4) The operation of the cryptographic module shall be specified using a finite state (or equivalent) represented by a state transition diagram and/or a state transition table. (The state transition diagram and/or state transition table includes all operational and error states of the cryptographic module, the corresponding transitions from one state to another, the input events that cause transitions from one state to another, and the output events resulting from transitions from one state to another.)

Note: This assertion is tested as part of AS04.05.

AS04.02: (Levels 1, 2, 3, and 4) The cryptographic module shall include the following operational and error states:

> ***Power on/off states*. States for primary, secondary, or backup power. These states may distinguish between power sources being applied to the cryptographic module.**
>
> ***Crypto officer states*. States in which the crypto officer services are performed (e.g., cryptographic initialization and key management).**
>
> ***Key/CSP entry states*. States for entering cryptographic keys and CSPs into the cryptographic module.**
>
> ***User states*. States in which authorized users obtain security services, perform cryptographic operations, or perform other Approved or non-Approved functions.**
>
> ***Self-test states*. States in which the cryptographic module is performing self-tests.**
>
> ***Error states*. States when the cryptographic module has encountered an error (e.g., failed a self-test or attempted to encrypt when missing operational keys or CSPs). 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 initialization or resetting of the module.**

Note: This assertion is tested as part of AS04.05.

AS04.03: (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 Test Procedures

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

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

Note: This assertion is tested as part of AS04.05.

AS04.05: (Levels 1, 2, 3, and 4) Documentation shall include a representation of the finite state (or equivalent) using a state transition diagram and/or state transition table that shall specify:

- **all operational and error states of the cryptographic module,**
- **the corresponding transitions from one state to another,**
- **the input events, including data inputs and control outputs, that cause transitions from one state to another, and**
- **the output events, including internal module conditions, data outputs, and status outputs resulting from transitions from one state to another.**

Required Vendor Information

VE04.05.01: 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.

Required Test Procedures

TE04.05.01: The tester shall verify that the vendor has provided a description of the finite state model. This description shall contain the identification and description of all states of the module, and a description of all corresponding state transitions. The tester shall verify that the descriptions of the state transitions include the internal module conditions, data inputs and control inputs that cause transitions from one state to another, data outputs and status outputs resulting from transitions from one state to another.

TE04.05.02: The tester shall verify that the finite state diagrams and the descriptions are consistent with the vendor documentation that describes the following:

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

TE04.05.03: The tester shall verify that every state that is identified in the finite state diagram(s) is also identified and described in the description.

TE04.05.04: The tester shall verify that every state that is identified and described in the description is also identified in the finite state diagram(s).

TE04.05.05: The tester shall verify that the operation of the module is consistent with the finite state diagrams and descriptions.

TE04.05.06: If the module includes a maintenance interface, then the tester shall verify that the finite state model has at least one maintenance state define. All maintenance states must be contained in the finite state diagram(s) and described in the description of the finite state model.

TE04.05.07: The tester shall review the descriptions of the states of the cryptographic module to determine if the descriptions clearly define disjoint states. The tester shall verify that all possible combinations of data and control inputs can be partitioned into disjoint sets.

TE04.05.08: The tester shall exercise the cryptographic module, causing it to enter each of its major states. For each state that has a distinct indicator, the tester shall attempt to observe the indicator while the module is in the state. If the expected indicator is not observed, or two or more such indicators are observed at the same time (indicating that the module is in more than one state at one time), this test fails.

TE04.05.09: The tester shall verify that there exists a chain of transitions from an initial power on state to each other state in the model that is not an initial power on state.

TE04.05.10: The tester shall verify that there exists a chain of transitions from each non-power off state to a power off state of the model.

TE04.05.11: The tester shall verify that the actions of the finite state model, as the result of all possible data and control inputs, are defined. An example of an acceptable inclusive statement is:

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

5. PHYSICAL SECURITY

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

Required Vendor Information - Firmware Module (Level 1 only)

VE05.01.01: The vendor shall provide a description of the mechanism used to ensure that no other process can access private and secret keys, intermediate key generation values, and other CSPs, while the cryptographic process is in use.

VE05.01.02: The vendor shall provide a description of the mechanism used to ensure that no other process can interrupt the cryptographic module during execution.

VE05.01.03: The vendor shall provide a list of the cryptographic firmware that are stored on the cryptographic module and shall provide a description of the protection mechanisms used to prevent unauthorized disclosure and modification.

Required Test Procedures – Firmware Module (Level 1 only)

TE05.01.01: The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to access secret and private keys, intermediate key generation values, and other CSPs.

TE05.01.02: The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are operating, the same or another tester shall attempt to execute another process.

TE05.01.03: The tester shall attempt to perform unauthorized accesses and unauthorized modifications to software and firmware source and executable code.

AS05.02: (Levels 1, 2, 3, and 4) All hardware, software, firmware, and data components within the cryptographic boundary shall be protected.

Note: This assertion is not separately tested.

5.1 General Physical Security Requirements

AS05.03: (Levels 1, 2, 3, and 4) The following requirements shall apply to all physical embodiments.

Note: This assertion is not separately tested.

AS05.04: (Levels 1, 2, 3, and 4) Documentation shall specify the physical embodiment and the security level for which the physical security mechanisms of the cryptographic module are implemented.

Required Vendor Information

VE05.04.01: 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 Section 4.5 of FIPS PUB 140-2. (See also VE01.08.05.) The specified physical embodiment shall be consistent with the module physical design. The vendor documentation shall also state which security level (1 through 4) the module is intended to meet.

Required Test Procedures

TE05.04.01: 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 Section 4.5 of FIPS PUB 140-2. (See also TE01.08.09.) The tester shall make 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 summarized below.

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

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

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

TE05.04.02: The tester shall verify that the vendor documentation states which security level the module is intended to meet. The tester shall make an independent determination of the security level that the module actually meets.

AS05.05: (Levels 1, 2, 3, and 4) Documentation shall specify the physical security mechanisms of the cryptographic module.

Required Vendor Information

VE05.05.01: The vendor documentation shall describe the applicable physical security mechanisms that are employed by the module. The contents of the module, including all hardware, firmware, software, and data (including plaintext cryptographic keys and unprotected CSPs) shall be protected.

Required Test Procedures

TE05.05.01: The tester shall verify that the vendor documentation describes the applicable physical security mechanisms that are employed by the module.

AS05.06: (Levels 1, 2, 3, and 4) If the cryptographic 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 authorized individual), then a maintenance access interface shall be defined.

Required Vendor Information

VE05.06.01: The vendor documentation shall describe the maintenance access interface employed by the module.

Required Test Procedures

TE05.06.01: The tester shall verify that the vendor documentation describes the maintenance access interface.

TE05.06.02: The tester shall verify that the vendor documentation and implementation are consistent.

AS05.07: (Levels 1, 2, 3, and 4) If the cryptographic 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 authorized individual), then the maintenance access interface shall include all physical access paths to the contents of the cryptographic module, including any removable covers or doors.

Required Vendor Information

VE05.07.01: The vendor documentation shall specify the maintenance access interface, including any removable covers or doors.

Required Test Procedures

TE05.07.01: The tester shall review the vendor documentation to verify that a maintenance access interface is provided, including any removable covers or doors.

AS05.08: (Levels 1, 2, 3, and 4) If the cryptographic 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 authorized individual), then any removable covers or doors included within the maintenance access interface shall be safeguarded using the appropriate physical security mechanisms.

Note: This assertion is tested as part of AS05.07.

AS05.09: (Levels 1, 2, 3, and 4) If the cryptographic 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 authorized individual), then all plaintext secret and private keys and CSPs shall be zeroized when the maintenance access interface is accessed.

Required Vendor Information

VE05.09.01: The vendor documentation shall specify how the module's plaintext keys and other CSPs are zeroized when the maintenance access interface is accessed.

Required Test Procedures

TE05.09.01: If vendor documentation states that a maintenance access interface is provided, the tester shall verify that the vendor documentation specifies how plaintext keys and other unprotected CSPs contained in the module are zeroized when accessing the maintenance access interface.

TE05.09.02: If the module design and operating procedures allow it, the tester shall access the maintenance access interface while the unit is powered on, and verify that all operational keys are zeroized. Removing power to memory and allowing charge to slowly dissipate is not sufficient

AS05.10: (Levels 1, 2, 3, and 4) If the cryptographic 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 authorized individual), then documentation shall specify the maintenance access interface and how plaintext secret and private keys and CSPs are to be zeroized when the maintenance access interface is accessed.

Required Vendor Information

VE05.10.01: Vendor documentation shall define the procedures by which authorized maintenance actions for the module are performed.

Required Test Procedures

TE05.10.01: If vendor documentation states that a maintenance access interface is provided, the tester shall verify that the vendor documentation specifies maintenance actions that are authorized for the module.

AS05.11: (Level 1) The following requirements shall apply to all cryptographic modules for Security Level 1.

Note: This assertion is not separately tested.

AS05.12: (Levels 1, 2, 3, and 4) The cryptographic module shall consist of production-grade components that shall include standard passivation techniques (e.g., a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or other physical damage).

Required Vendor Information

VE05.12.01: The module shall be a standard, production-quality IC, designed to meet commercial-grade specifications for power, temperature, reliability, shock and vibration, etc. The module shall use standard passivation techniques for the entire chip. The vendor documentation shall describe the IC quality. If an IC is used that is not a standard device, its passivation design shall also be described.

Required Test Procedures

TE05.12.01: The tester shall verify by inspection, or from vendor documentation, that the module contains standard integrated circuits with a uniform exterior material and standard connectors. The tester shall verify from vendor documentation that the chips in the module are commercial grade in regards to power and voltage ranges, temperature, reliability, and shock and vibration.

TE05.12.02: The tester shall verify from vendor documentation that the module has a standard passivation applied to it. The passivation must be a sealing coat applied over the chip circuitry to protect it against environmental or other physical damage. If standard passivation is not used, then the documentation shall provide information to indicate why it is equivalent to a standard passivation approach.

AS05.13: (Levels 1, 2, 3, and 4) When performing physical maintenance, all plaintext secret and private keys and other unprotected CSPs contained in the cryptographic module shall be zeroized.

Note: This assertion is tested as part of AS05.09.

AS05.14: (Levels 1, 2, 3, and 4) Zeroization shall either be performed procedurally by the operator or automatically by the cryptographic module.

Note: This assertion is not separately tested.

AS05.15: (Levels 2, 3, and 4) In addition to the general requirements for Security Level 1, the following requirement shall apply to all cryptographic modules for Security Level 2.

Note: This assertion is not separately tested.

AS05.16: (Levels 2, 3, and 4) The cryptographic module shall provide evidence of tampering (e.g., on the cover, enclosure, and seal) when physical access to the module is attempted.

Note: This assertion is tested as part of AS05.25 for single-chip embodiments, AS05.36 and AS05.37 for multiple-chip embedded embodiments, and AS05.50 for multiple-chip standalone embodiments.

AS05.17: (Levels 3 and 4) In addition to the general requirements for Security Levels 1 and 2, the following requirements shall apply to all cryptographic modules for Security Level 3.

Note: This assertion is not separately tested.

AS05.18: (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 zeroization circuitry.

Note: This assertion is tested as part of AS05.29 for single-chip embodiments, AS05.53 for multiple-chip embedded and multiple-chip standalone embodiments.

AS05.19: (Levels 3 and 4) The tamper response and zeroization circuitry shall immediately zeroize all plaintext secret and private keys and CSPs when a door is opened, a cover is removed, or when the maintenance access interface is accessed.

Note: This assertion is tested as part of AS05.29 for single-chip embodiments, AS05.39 for multiple-chip embedded embodiments, and AS05.53 for multiple-chip standalone embodiments.

AS05.20: (Levels 3 and 4) The tamper response and zeroization circuitry shall remain operational when plaintext secret and private cryptographic keys or CSPs are contained within the cryptographic module.

Note: This assertion is tested as part of AS05.29 for single-chip embodiments, AS05.39 for multiple-chip embedded embodiments, and AS05.53 for multiple-chip standalone embodiments.

AS05.21: (Levels 3 and 4) If the cryptographic module contains ventilation holes or slits, then the holes or slits shall be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., require at least one 90 degree bend or obstruction with a substantial blocking material).

Required Vendor Information

VE05.21.01: If the module is contained within a cover or enclosure that contains any ventilation holes or slits; then they shall be constructed in a manner that prevents undetected physical probing inside the enclosure. The vendor documentation shall describe the ventilation physical design approach.

Required Test Procedures

TE05.21.01: The tester shall verify by inspection and from vendor documentation whether the module has a cover or enclosure with ventilation holes, slits, or other openings, and if so, whether they are constructed to deter undetected probing inside the cover or enclosure.

AS05.22: (Level 4) In addition to the general requirements for Security Levels 1, 2 and 3, the following requirement shall apply to all cryptographic modules for Security Level 4.

Note: This assertion is not separately tested.

AS05.23: (Level 4) The cryptographic module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in Section 4.5.5.

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

5.2 Single-Chip Cryptographic Modules

Note: There are no additional Security Level 1 requirements for single-chip cryptographic modules.

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

Note: This assertion is not separately tested.

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

Note: This requirement is associated with AS05.16.

Required Vendor Information

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

Required Test Procedures

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

AS05.26: (Single-Chip - Levels 2, 3, and 4) The tamper-evident coating or tamper-evident enclosure shall be opaque within the visible spectrum.

Required Vendor Information

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

Required Test Procedures

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

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

Note: This assertion is not separately tested.

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

Required Vendor Information

VE05.28.01: The vendor documentation shall state which of the two approaches specified in AS05.28 is used to meet the requirement, and provide supporting detailed design information. Under Option 1, the tester shall follow procedures in TE05.28.01. Under Option 2, the tester shall follow procedures specified in TE05.29.01.

Required Test Procedures

TE05.28.01: The tester shall verify by inspection and from vendor documentation that the module is covered with a hard opaque tamper evident coating. The documentation should specify the type of coating that is used and its characteristics.

TE05.28.02: 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 must verify that the coating completely covers the module, is visibly opaque, and deters direct observation, probing, or manipulation. (Portions of this verification may already have been performed at Security Level 2 in TE05.25.01.)

AS05.29: (Single-Chip – Levels 3 and 4) Either the enclosure shall be designed 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) or AS05.28 shall be satisfied.

Note: These requirements are associated with AS05.18, AS05.19 and AS05.20.

Required Vendor Information

VE05.29.01: If the cryptographic module is contained in an enclosure, the vendor documentation shall provide design information. The enclosure shall be designed such that attempts to remove it will have a high probability of causing serious damage to the circuitry within the module.

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

Required Test Procedures

TE05.29.01: The vendor documentation shall specify if the module contains doors or removable covers or has a maintenance access interface, then the module shall contain tamper response and zeroization circuitry.

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

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

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

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

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility

- Rationale must be included that explains why tester could not perform the tests
- Tester must develop the required test plan and required tests
- Tester must directly observe the tests being performed

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

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

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

Note: This assertion is not separately tested.

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

Required Vendor Information

VE05.31.01: The 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. The vendor documentation shall identify the kind of coating used and its characteristics.

Required Test Procedures

TE05.31.01: The tester shall verify by inspection and from vendor documentation that the module is covered with a hard, opaque removal-resistant coating. The documentation shall specify the coating used and provide data on its hardness and removal resistance.

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

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

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

Required Vendor Information

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

Required Test Procedures

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

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

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

5.3 Multiple-Chip Embedded Cryptographic Modules

AS05.33: (Multiple Chip Embedded - Levels 1, 2, 3, and 4) The following requirement shall apply to multiple-chip embedded cryptographic modules for Security Level 1.

Note: This assertion is not separately tested.

AS05.34: (Multiple Chip Embedded - Levels 1, 2, 3, and 4) If the cryptographic module is contained within an enclosure or removable cover, a production-grade enclosure or removable cover shall be used.

Required Vendor Information

VE05.34.01: The module shall be entirely contained within a production-grade enclosure or removable cover. The vendor documentation shall describe the cover or enclosure.

Required Test Procedures

TE05.34.01: The tester shall verify by inspection and from vendor documentation that the module is contained within an enclosure or removable cover that is of production grade.

AS05.35: (Multiple Chip Embedded - Levels 2, 3, and 4) In addition to the requirement for Security Level 1, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 2.

Note: This assertion is not separately tested.

AS05.36: (Multiple Chip Embedded - Levels 2, 3, and 4) Either

- **the cryptographic module components shall be covered with a tamper-evident coating or potting material (e.g., etch-resistant coating or bleeding paint) or contained in a tamper-evident enclosure to deter direct observation, probing, or manipulation of module components and to provide evidence of attempts to tamper with or remove module components, and**

- **the tamper-evident coating or tamper-evident enclosure shall be opaque within the visible spectrum,**

or

- **AS05.37 shall be satisfied.**

Note: This requirement is associated with AS05.16.

Required Vendor Information

VE05.36.01: The module shall be encapsulated with an opaque, tamper-evident coating such as etch-resistant coating or bleeding paint. The material shall be opaque within the visible spectrum. The vendor documentation shall identify the kind of opaque tamper-evident coating and its characteristics.

Required Test Procedures

TE05.36.01: The tester shall verify by inspection and from vendor documentation that the module is encapsulated with an opaque, tamper-evident material. The inspection shall verify that the tamper-evident material completely covers the module and is visibly opaque.

TE05.36.02: The tester shall verify by testing that the module provides evidence of attempts to tamper with or remove module components.

AS05.37: (Multiple Chip Embedded - Levels 2, 3, and 4) Either

- **the cryptographic module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers,**

- **the enclosure shall be opaque within the visible spectrum, and**

- **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 they shall be protected with tamper-evident seals (e.g., evidence tape or holographic seals).**

or

- **AS05.36 shall be satisfied.**

Note: This requirement is associated with AS05.16.

Required Vendor Information

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

VE05.37.02: The enclosure shall be opaque within the visible spectrum. The vendor documentation shall describe the enclosure's opacity characteristics.

VE05.37.03: 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; or they shall be protected via tamper-evident seals. The vendor documentation shall describe the tamper-evident seals.

Required Test Procedures

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

1. The enclosure must completely surround the entire module.

2. The enclosure material must of a composition defined in the vendor documentation.

3. The enclosure must be production grade. The vendor literature must 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.

TE05.37.02: The tester shall verify by inspection that the enclosure is opaque within the visible spectrum.

TE05.37.03: The tester shall determine whether the enclosure contains any removable covers or doors. The tester shall verify that each cover and door meets one of the two requirements below:

1. The 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 determine that the cover or door will not open without signs of damage; or

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

AS05.38: (Multiple-Chip Embedded - Levels 3 and 4) In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 3.

Note: This assertion is not separately tested.

AS05.39: (Multiple-Chip Embedded - Levels 3 and 4) Either

- **the multiple-chip embodiment of the circuitry within the cryptographic module shall be covered with a hard coating or potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum**

or

- **the applicable Security Level 3 requirements for multiple-chip standalone cryptographic modules shall apply. (Section 4.5.4)**

Note: The following requirements (TE05.39.01, TE05.39.02, TE05.39.04, TE05.39.05, TE05.39.09 and TE05.39.10) are associated with AS05.18, AS05.19 and AS05.20.

Required Vendor Information

VE05.39.01: The vendor documentation shall state which of the approaches specified in AS05.39 are implemented in the module and provide supporting design documentation. Depending on this choice, the corresponding vendor requirement (one of the following, respectively) must be met:

1. The multiple-chip circuitry of the module shall be completely covered with a hard, opaque potting material. The material shall be opaque within the visible spectrum.

2. 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). If the enclosure contains any removable covers or doors, then the module shall contain tamper response and zeroization circuitry. The circuitry shall continuously monitor the covers and doors, and upon the removal of a cover or the opening of a door, shall zeroize all plaintext secret and private keys and unprotected CSPs. The circuitry shall be operational whenever plaintext secret and private keys and unprotected CSPs, are contained within the module.

Required Test Procedures

TE05.39.01: The vendor documentation shall specify if the module contains doors or removable covers or has a maintenance access interface, then the module shall contain tamper response and zeroization circuitry.

TE05.39.02: If the enclosure has removable covers or doors, or if a maintenance access interface is specified, the tester shall verify from vendor documentation that the module zeroizes all plaintext secret and private keys, and CSPs when a cover or door is removed or if the maintenance access interface is accessed.

TE05.39.03: The tester shall verify that the vendor documentation specifies which requirement option in VE05.39.01 is implemented and provides design documentation.

TE05.39.04: The tester shall verify by inspection and from vendor documentation that the tamper response and zeroization circuitry remains operational when plaintext secret and private keys and CSPs are contained within the module.

TE05.39.05: The tester shall verify by inspection and from vendor documentation that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

TE05.39.06: (Option 1 - *Utilize a hard opaque material*) The tester shall verify by inspection and from vendor documentation that the module is covered with a hard opaque material. The documentation shall specify the material that is used. The tester shall verify that it cannot be easily penetrated to the depth of the underlying circuitry. The tester shall verify that the material completely covers the module and is visibly opaque within the visible spectrum.

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

TE05.39.07: (Option 2 - *Utilize a strong enclosure*) The tester shall determine 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 vendor documentation that the enclosure cannot be removed.

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

TE05.39.08: (Option 2 - *Utilize a strong enclosure*) If the strong enclosure has removable covers or doors, the tester shall verify from vendor documentation that the module zeroizes all plaintext secret and private keys and CSPs when a cover or door is removed.

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

TE05.39.09: If the enclosure has removable covers or doors, or if a maintenance access interface is specified, the tester shall test that the module zeroizes all plaintext secret and private keys and CSPs when a cover or door is removed or if the maintenance access interface is accessed.

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

TE05.39.10: The tester shall test that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

AS05.40: (Multiple-Chip Embedded – Level 4) In addition to the requirements for Security Levels 1, 2 and 3, the following requirements shall apply to multiple-chip embedded cryptographic modules for Security Level 4.

Note: This assertion is not separately tested.

AS05.41: (Multiple-Chip Embedded – Level 4) The cryptographic module components shall be covered by potting material or contained within an enclosure 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, or dissolving of the potting material or enclosure to an extent sufficient for accessing plaintext secret and private keys cryptographic keys or CSPs.

Required Vendor Information

VE05.41.01: The module shall be contained within a tamper detection envelope that will detect tampering attacks against the potting material or enclosure. The vendor documentation shall describe the tamper detection envelope design.

Required Test Procedures

TE05.41.01: 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.

AS05.42: (Multiple Chip Embedded – Level 4) The cryptographic module shall contain tamper response and zeroization circuitry.

Note: This assertion is tested as part of AS05.43 and AS05.44.

AS05.43: (Multiple Chip Embedded – Level 4) The tamper response and zeroization circuitry shall continuously monitor the tamper detection envelope.

Note: This assertion is tested in AS05.44.

AS05.44: (Multiple Chip Embedded – Level 4) Upon the detection of tampering, the tamper response and zeroization circuitry shall immediately zeroize all plaintext secret and private cryptographic keys and CSPs.

Required Vendor Information

VE05.44.01: The module shall contain tamper response and zeroization circuitry that continuously monitors the tamper detection envelope for tampering, and upon the detection of tampering, shall zeroize all plaintext secret and private keys and other unprotected CSPs. The circuitry shall be operational whenever plaintext secret and private keys and other unprotected CSPs are contained within the module. The vendor documentation shall describe the tamper response and zeroization design.

Required Test Procedures

TE05.44.01: The tester shall verify from vendor documentation that the module contains tamper response and zeroization 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 zeroizes all plaintext secret and private keys and other unprotected CSPs.

TE05.44.02: The tester shall breach the tamper detection envelope barrier and then verify that the module zeroizes all plaintext secret and private keys and other unprotected CSPs.

Note: This test can be verified in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
    - Rationale must be included that explains why tester could not perform the tests

- Tester must develop the required test plan and required tests
- Tester must directly observe the tests being performed

AS05.45: (Multiple Chip Embedded – Level 4) The tamper response and zeroization circuitry shall remain operational when plaintext secret and private cryptographic keys or CSPs are contained within the cryptographic module.

Note: This assertion is tested as part of AS05.44.

5.4 Multiple-Chip Standalone Cryptographic Modules

AS05.46: (Multiple-Chip Standalone – Levels 1, 2, 3, and 4) The following requirement shall apply to multiple-chip standalone cryptographic modules for Security Level 1.

Note: This assertion is not separately tested.

AS05.47: (Multiple-Chip Standalone – 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

VE05.47.01: The module shall be entirely contained within a metal or hard plastic production-grade enclosure that may include removable covers or doors. The vendor documentation shall describe the enclosure and its hardness characteristics.

Required Test Procedures

TE05.47.01: The tester shall verify by inspection and from vendor documentation that the module is contained within an enclosure that meets the following requirements:

1. The enclosure must completely surround the entire module.

2. The enclosure material must of a composition defined in the vendor documentation.

3. The enclosure must be production grade. The vendor literature must either show that an enclosure of the same material has been used commercially, or provide data to show that it is equivalent to a commercial product.

AS05.48: (Multiple-Chip Standalone – Levels 2, 3, and 4) In addition to the requirements for Security Level 1, the following requirements shall apply to multiple-chip standalone cryptographic modules for Security Level 2.

Note: This assertion is not separately tested.

AS05.49: (Multiple-Chip Standalone – Levels 2, 3, and 4) The enclosure of the cryptographic module shall be opaque within the visible spectrum.

Required Vendor Information

VE05.49.01: The enclosure shall be opaque within the visible spectrum. The vendor documentation shall describe the enclosure's opacity characteristics.

Required Test Procedures

TE05.49.01: The tester shall verify by inspection that the enclosure is opaque within the visible spectrum.

AS05.50: (Multiple-Chip Standalone – Levels 2, 3, and 4) If the enclosure of the cryptographic module includes any doors or removable covers, then the doors or covers shall be locked with pick-resistant mechanical locks employing physical or logical keys or they shall be protected with tamper-evident seals (e.g., evidence tape or holographic seals).

Required Vendor Information

VE05.50.01: 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; or they shall be protected via tamper-evident seals such as evidence tape or holographic seals. The vendor documentation shall describe the implemented tamper-protection approach.

Required Test Procedures

TE05.50.01: The tester shall determine whether the enclosure contains any removable covers or doors. The tester shall verify that each cover and door meets one of the two requirements below:

1. The 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 determine that the cover or door will not open without signs of damage; or

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

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

Note: This assertion is not separately tested.

AS05.52: (Multiple-Chip Standalone – Levels 3 and 4) Either

- **the multiple-chip embodiment of the circuitry within the cryptographic module shall be covered with a hard potting material (e.g., a hard epoxy material) that is opaque within the visible spectrum**

or

- **AS05.53 must be satisfied.**

Required Vendor Information

VE05.52.01: The vendor documentation shall state which of the two approaches specified in AS05.52 is implemented and provide design information.

VE05.52.02: (Option 1) The multiple-chip embodiment of the circuitry shall be covered with a hard opaque potting material. The material shall be opaque within the visible spectrum.

Required Test Procedures

TE05.52.01: The tester shall verify that the vendor documentation specifies which requirement option in VE05.52.01 is implemented and provide design documentation.

TE05.52.02: (Option 1 – *Covered with a hard opaque potting material*) Encapsulate within a hard, opaque potting material. The tester shall verify from vendor documentation and by inspection, if internal access is possible, that the circuitry within the module is covered with a hard opaque potting material. The documentation shall specify which potting material is used and its hardness characteristics.

TE05.52.03: (Option 1 – *Covered with a hard opaque potting material*) If access is possible, the tester shall verify that the cover cannot be easily penetrated to the depth of the underlying circuitry. If access is possible, the tester shall verify that the potting material covers the circuitry within the module and is opaque in the visible spectrum.

AS05.53: (Multiple-Chip Standalone – Levels 3 and 4) Either

- **the cryptographic 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)**

or

- **AS05.52 must be satisfied.**

Required Vendor Information

Note: The following requirements (TE05.53.01, TE05.53.02, TE05.53.04, TE05.53.05, TE05.53.08 and TE05.53.09) are associated with AS05.18, AS05.19 and AS05.20.

VE05.53.01: The vendor documentation shall state which of the approaches specified in AS05.53 are implemented in the module and provide supporting design documentation.

VE05.53.02: (Option 1) 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. If the enclosure contains any removable covers or doors, then the module shall contain tamper response and zeroization circuitry. The circuitry shall continuously monitor the covers and doors, and upon the removal of a cover or the opening of a door, shall zeroize all plaintext secret and private keys and unprotected CSPs. The circuitry shall be operational whenever plaintext secret and private keys and unprotected CSPs, are contained within the module.

Required Test Procedures

TE05.53.01: The vendor documentation shall specify if the module contains doors or removable covers or has a maintenance access interface, then the module shall contain tamper response and zeroization circuitry.

TE05.53.02: If the enclosure has removable covers or doors, or if a maintenance access interface is specified, the tester shall verify from vendor documentation that the module zeroizes all plaintext secret and private keys and CSPs when a cover or door is removed or if the maintenance access interface is accessed.

TE05.53.03: The tester shall verify that the vendor documentation specifies which requirement option in VE05.53.01 is implemented and provides design documentation.

TE05.53.04: The tester shall verify by inspection and from vendor documentation that the tamper response and zeroization circuitry remains operational when plaintext secret and private keys and CSPs are contained within the module.

TE05.53.05: The tester shall verify by inspection and from vendor documentation that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

TE05.53.06: (Option 1 - *Utilize a strong enclosure*) The tester shall determine 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 vendor documentation that the enclosure cannot be removed.

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

TE05.53.07: (Option 1 - *Utilize a strong enclosure*) If the strong enclosure has removable covers or doors, the tester shall verify from vendor documentation that the module zeroizes all plaintext secret and private keys and CSPs when a cover or door is removed.

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

TE05.53.08: If the enclosure has removable covers or doors, or if a maintenance access interface is specified, the tester shall test that the module zeroizes all plaintext secret and private keys and CSPs when a cover or door is removed or if the maintenance access interface is accessed.

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

TE05.53.09: The tester shall test that the enclosure cannot be removed or penetrated without having a high probability of causing serious damage to the module.

Note: This test can be performed in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

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

Note: This assertion is not separately tested.

AS05.55: (Multiple-Chip Standalone – Level 4) The potting material or enclosure of the cryptographic module shall be encapsulated by a tamper detection envelope, by the use of tamper detection mechanisms such as cover switches (e.g., microswitches, magnetic Hall effect switches, permanent magnetic actuators, etc.), motion detectors (e.g., ultrasonic, infrared, or microwave), or other tamper detection mechanisms as described above for multiple-chip embedded cryptographic modules.

Required Vendor Information

VE05.55.01: The enclosure or potting material shall be encapsulated by a tamper detection envelope by the use of tamper detection mechanisms. The vendor documentation shall describe the tamper detection envelope design.

Required Test Procedures

TE05.55.01: The tester shall verify from vendor documentation and by inspection that the module enclosure or potting material contains tamper detection mechanisms, which shall form a tamper detection envelope that protects the module components. The mechanisms shall be designed such that any breach of the enclosure or potting material to access the module components can be detected.

AS05.56: (Multiple-Chip Standalone – Level 4) The tamper detection mechanisms shall detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure, to an extent sufficient for accessing plaintext secret and private cryptographic keys and CSPs.

Note: This assertion is tested as part of AS05.58.

AS05.57: (Multiple-Chip Standalone – Level 4) The cryptographic module shall contain tamper response and zeroization circuitry.

Note: This assertion is tested as part of AS05.58.

AS05.58: (Multiple-Chip Standalone – Level 4) The tamper response and zeroization circuitry shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroize all plaintext secret and private cryptographic keys and CSPs.

Required Vendor Information

VE05.58.01: The module shall contain tamper response and zeroization circuitry that continuously monitors the tamper detection envelope for tampering, and upon the detection of tampering, shall zeroize all plaintext secret and private keys and other unprotected CSPs. The circuitry shall be operational whenever plaintext secret and private keys and other unprotected CSPs are contained within the module. The vendor documentation shall describe the tamper response and zeroization design.

Required Test Procedures

TE05.58.01: The tester shall verify from vendor documentation that the module contains tamper response and zeroization 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 zeroizes all plaintext secret and private keys and other unprotected CSPs.

TE05.58.02: The tester shall breach the tamper detection envelope barrier and then verify that the module zeroizes all plaintext secret and private keys and other unprotected CSPs.

Note: This test can be verified in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

AS05.59: (Multiple-Chip Standalone – Level 4) The tamper response and zeroization circuitry shall remain operational when plaintext cryptographic keys and CSPs are contained within the cryptographic module.

Note: This assertion is tested as part of AS05.58.

5.5 Environmental Failure Protection/Testing

AS05.60: (Level 4) The cryptographic module shall either employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT).

Required Vendor Information

VE05.60.01: The vendor shall use either of the following:

1. EFP features; or
2. EFT

as specified in Section 4.5.5, 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 must 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.

5.5.1 Environmental Failure Protection Features (Alternative 1)

AS05.61: (Level 4) Environmental failure protection (EFP) features shall protect the cryptographic module against unusual environmental conditions or fluctuations (accidental or induced) outside of the module's normal operating range that can compromise the security of the module.

Note: This assertion is tested as part of AS05.64.

AS05.62: (Level 4) In particular, the cryptographic module shall monitor and correctly respond to fluctuations in the operating temperature and voltage outside of the specified normal operating ranges.

Note: This assertion is tested as part of AS05.64.

AS05.63: (Level 4) The EFP features shall involve electronic circuitry or devices that continuously measure the operating temperature and voltage of the cryptographic module.

Note: This assertion is tested as part of AS05.64.

AS05.64: (Level 4) If the temperature or voltage fall outside of the cryptographic module's normal operating range, the protection circuitry shall either (1) shutdown the module to prevent further operation or (2) immediately zeroize all plaintext secret and private cryptographic keys and CSPs.

Required Vendor Information

VE05.64.01: If EFP is chosen for a particular condition, the module shall monitor and correctly respond to fluctuations in the operating temperature or voltage, outside of the module's normal operating range for that condition. The protection features shall continuously measure these environmental conditions. If a condition is determined to be outside of the module's normal operating range, the protection circuitry shall either:

1. Shut down the module; or

2. Zeroize all plaintext secret and private keys and other unprotected CSPs

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

Required Test Procedures

TE05.64.01: 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.

Note: This test can be verified in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

TE05.64.02: The tester shall extend the temperature and voltage outside of the specified normal range and determine that the module either shuts down to prevent further operations or zeroizes all plaintext secret and private keys and other unprotected CSPs.

Note: This test can be verified in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

TE05.64.03: If the module is designed to zeroize all plaintext secret and private keys and other unprotected CSPs, and the module was still operational after returning to the normal environmental range, the tester shall perform services that require keys and verify that the module does not perform these services.

Note: This test can be verified in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

AS05.65: (Level 4) Documentation shall specify the normal operating ranges of the cryptographic module and the environmental failure protection features employed by the module.

Note: This assertion is tested as part of AS05.60 and AS05.64.

5.5.2 Environmental Failure Testing Procedures (Alternative 2)

AS05.66: (Level 4) Environmental failure testing (EFT) shall involve a combination of analysis, simulation, and testing of the cryptographic module to provide reasonable assurance that environmental conditions or fluctuations (accidental or induced) outside the module's normal operating ranges for temperature and voltage will not compromise the security of the module.

Note: This assertion is tested as part of AS05.68.

AS05.67: (Level 4) EFT shall demonstrate that, if the operating temperature or voltage falls outside the normal operating range of the cryptographic module resulting in a failure of the electronic devices or circuitry within the module, at no time shall the security of the cryptographic module be compromised.

Note: This assertion is tested as part of AS05.68.

AS05.68: (Level 4) The temperature range to be tested shall be from -100° to +200° Celsius (-150° to +400° Fahrenheit). The voltage range to be tested shall be from the smallest negative voltage (with respect to ground) that causes the zeroization of the electronic devices or circuitry to the smallest positive voltage (with respect to ground) that causes the zeroization of the electronic devices or circuitry, including reversing the polarity of the voltages.

Required Vendor Information

VE05.68.01: If EFT is chosen for a particular condition, the module shall be tested within the temperature and voltage ranges specified in AS05.68. The module shall either:

1. Continue to operate normally; or

2. Shut down; or

3. Zeroize all plaintext secret and private keys and other unprotected CSPs

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

Required Test Procedures

TE05.68.01: The tester shall configure the environmental condition (ambient temperature and voltage) as specified in AS05.68, and verify that the module either continues to operate normally, or shuts down to prevent further operations, or zeroizes all plaintext secret and private keys and other unprotected CSPs.

Note: This test can be verified in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
    - Rationale must be included that explains why tester could not perform the tests
    - Tester must develop the required test plan and required tests
    - Tester must directly observe the tests being performed

TE05.68.02: If the module is designed to zeroize all plaintext secret and private keys and other unprotected CSPs, and the module was still operational after returning to the normal environmental range, the tester shall perform services that require keys and verify that the module does not perform these services

Note: This test can be verified in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
    - Rationale must be included that explains why tester could not perform the tests
    - Tester must develop the required test plan and required tests
    - Tester must directly observe the tests being performed

AS05.69: (Level 4) Documentation shall specify the normal operating ranges of the cryptographic module and the environmental failure tests performed.

Note: This assertion is tested as part of AS05.68.

6. OPERATIONAL ENVIRONMENT

AS06.01: (Levels 1, 2, 3, and 4) If the operational environment is a modifiable operational environment, the operating system requirements in Section 4.6.1 shall apply.

Note: This assertion is not separately tested.

AS06.02: (Levels 1, 2, 3, and 4) Documentation shall specify the operational environment for the cryptographic module, including, if applicable, the operating system employed by the module, and for Security Levels 2, 3, and 4, the Protection Profile and the CC assurance level.

Required Vendor Information

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

Required Test Procedures

TE06.02.01: The tester shall verify that the information specified in VE06.02.01 is included. If this information is not included, then this assertion fails.

6.1 Operating System Requirements

AS06.03: (Levels 1, 2, 3, and 4) The following requirements shall apply to operating systems for Security Level 1.

Note: This assertion is tested as part of AS06.04 through AS06.08.

AS06.04: (Level 1 Only) The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded).

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

Required Vendor Information

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

Required Test Procedures

TE06.04.01: The tester shall operate the cryptographic module as described in the crypto officer and user guidance documentation. While the cryptographic module is operating as specified, the same or another tester shall attempt to circumvent the single-user enforcement mechanism.

AS06.05: (Level 1 Only) The cryptographic module shall prevent access by other processes to plaintext private and secret keys, CSPs, and intermediate key generation values during the time the cryptographic module is executing/operational. Processes that are spawned by the cryptographic module are 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

VE06.05.01: The vendor shall provide a description of the mechanism used to ensure that no other process can access private and secret keys, intermediate key generation values, and other CSPs, while the cryptographic process is in use.

Required Test Procedures

TE06.05.01: The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to access secret and private keys, intermediate key generation values, and other CSPs.

AS06.06: (Leve1 1 Only) Non-cryptographic processes shall not interrupt the cryptographic module during execution.

Required Vendor Information

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

Required Test Procedures

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

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

Required Vendor Information

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

Required Test Procedures

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

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

Required Vendor Information

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

Required Test Procedures

TE06.08.01: The tester shall verify that the information specified in VE06.08.01 is included. If this information is not included, then this assertion fails.

TE06.08.02: The tester shall attempt to corrupt the cryptographic software and firmware components. If the integrity is maintained, this TE fails.

AS06.09: (Level 2) In addition to the applicable requirements for Security Level 1, the following requirements shall also apply for Security Level 2.

Note: This assertion is tested as part of AS06.10 through AS06.19.

AS06.10: (Level 2) All cryptographic software and firmware, cryptographic keys and CSPs, and control and status information shall be under the control of

- **an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B and is evaluated at the CC evaluation assurance level EAL2, or**
- **an equivalent evaluated trusted operating system.**

Required Vendor Information

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

Required Test Procedures

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

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

Required Vendor Information

VE06.11.01: This VE is tested as part of VE06.14.01.

Required Test Procedures

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

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

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

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

Required Vendor Information

VE06.12.01: This VE is tested as part of VE06.14.01.

Required Test Procedures

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

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

1. Cryptographic programs
2. Cryptographic data (e.g., cryptographic keys, audit data)
3. CSPs
4. Plaintext data

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

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

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

Required Vendor Information

VE06.13.01: This VE is tested as part of VE06.14.01.

Required Test Procedures

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

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

1. Cryptographic data (e.g., cryptographic keys and audit data)
2. CSPs
3. Plaintext data

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

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

AS06.14: (Levels 2, 3, and 4) To protect plaintext data, cryptographic software and firmware, cryptographic keys and CSPs, and authentication data, the discretionary access control mechanisms of the operating system shall be configured to specify the set of roles that can *enter* cryptographic keys and CSPs.

Required Vendor Information

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

Required Test Procedures

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

TE06.14.02: The tester shall assume a role with privileges to enter cryptographic keys and CSPs. The tester shall enter cryptographic keys and CSPs.

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

AS06.15: (Levels 2, 3, and 4) The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not.

Required Vendor Information

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

Required Test Procedures

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

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

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

Required Vendor Information

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

Required Test Procedures

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

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

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

Note: An assumption of this assertion is that the cryptographic module must use the audit mechanism provided by the operating system to audit the identified events. It is not sufficient for the cryptographic module software to use another file as its audit log, no matter how well protected.

Required Vendor Information

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

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

Required Test Procedures

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

TE06.17.02: The tester shall exercise the cryptographic module, with the auditing capability turned on, and perform the actions that generate auditable events. The tester shall review the system's audit log to determine if all the events were audited.

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

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

Note: This assertion is tested as part of AS06.17.

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

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

Note: This assertion is tested as part of AS06.17.

AS06.20: (Level 3) In addition to the applicable requirements for Security Levels 1 and 2, the following requirements shall apply for Security Level 3.

Note: This assertion is tested as part of AS06.21 through AS06.25.

AS06.21: (Level 3) All cryptographic software and firmware, cryptographic keys and CSPs, and control and status information shall be under the control of

- **an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B. The operating system shall be evaluated at the CC evaluation assurance level EAL3 and include the following additional requirements: Trusted_Path (FTP_TRP.1) and Informal TOE Security Policy Model (ADV_SPM.1), or**

- **an equivalent evaluated trusted operating system.**

Required Vendor Information

VE06.21.01: The vendor shall provide documentation that the operating system controlling the cryptographic module has successfully passed evaluation at EAL3 (plus Informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1)) for the functional requirements (plus Trusted Path (FTP_TRP.1)) specified in the protection profiles listed in Annex B.

Required Test Procedures

TE06.21.01: The tester shall verify that the operating system has received a certificate mutually recognized in accordance with the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.

AS06.22: (Levels 3 and 4) All cryptographic keys and CSPs, authentication data, control inputs, and status outputs shall be communicated via a trusted mechanism (e.g., a dedicated I/O physical port or a trusted path).

Required Vendor Information

VE06.22.01: The vendor shall document the trusted path mechanism used by the cryptographic module to communicate cryptographic keys and CSPs, authentication data, control inputs, and status outputs.

Required Test Procedures

TE06.22.01: The tester shall verify that the vendor has supplied the information required under VE06.22.01.

TE06.22.02: The tester shall use the trusted mechanism to communicate all cryptographic keys and CSPs, authentication data, control inputs, and status outputs

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

TE06.22.03: The tester shall attempt, for each input and output identified in AS06.22, to enter or output the information via an untrusted mechanism.

AS06.23: (Levels 3 and 4) If a trusted path is used, the Target of Evaluation Security Functions (TSF) shall support the trusted path between the TSF and the operator when a positive TSF-to-operator connection is required.

Required Vendor Information

VE06.23.01: The vendor shall document the trusted path used between the TSF and the operator when a positive TSF-to-operator connection is required.

Required Test Procedures

TE06.23.01: The tester shall verify that the vendor has supplied the information required under VE06.23.01.

AS06.24: (Levels 3 and 4) Communications via this trusted path shall be activated exclusively by an operator or the TSF and shall be logically isolated from other paths.

Required Vendor Information

VE06.24.01: The vendor shall document how the trusted path is activated exclusively by an operator or the TSF and is logically isolated from other paths.

Required Test Procedures

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

TE06.24.02: The tester shall invoke the trusted path. If the capability exists for the TSF to invoke the trusted path, the tester shall exercise the cryptographic module to cause the TSF to invoke the trusted path.

TE06.24.03: The tester shall attempt to cause the trusted path to be invoked by non-TSF software.

AS06.25: (Levels 3 and 4) In addition to the audit requirements of Security Level 2, the following events shall be recorded by the audit mechanism:

- **attempts to use the trusted path function, and**
- **identification of the initiator and target of a trusted path.**

Required Vendor Information

VE06.25.01: The vendor list of audited events shall include attempts to use the trusted path function, and identification of the initiator and target of a trusted path.

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

Required Test Procedures

TE06.25.01: The tester shall verify that the vendor has supplied the information required under VE06.25.01

TE06.25.02: The tester shall exercise the cryptographic module, with the auditing capability turned on, and perform the actions that generate the audited events. The tester shall review the system's audit log to determine if all the events were audited.

AS06.26: (Level 4) In addition to the applicable requirements for Security Levels 1, 2, and 3, the following requirements shall also apply to operating systems for Security Level 4.

Note: This assertion is tested as part of AS06.27.

AS06.27: (Level 4) All cryptographic software, cryptographic keys and CSPs, and control and status information shall be under the control of

- **an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B. The operating system shall be evaluated at the CC evaluation assurance level EAL4, or**

- **an equivalent evaluated trusted operating system.**

Required Vendor Information

VE06.27.01: The vendor shall provide documentation that the operating system controlling the cryptographic module has successfully passed evaluation at EAL4 for the functional requirements specified in the protection profiles listed in Annex B.

Required Test Procedures

TE06.27.01: The tester shall verify that the operating system has received a certificate mutually recognized in accordance with the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security.

7. CRYPTOGRAPHIC KEY MANAGEMENT

General

AS07.01: (Levels 1, 2, 3, and 4) Secret keys, private keys, and CSPs shall be protected within the cryptographic module from unauthorized disclosure, modification, and substitution.

Required Vendor Information

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

Required Test Procedures

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

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

1. Attempt to access (by circumventing the documented protection mechanisms) secret keys, private keys, and CSPs for which the tester is not authorized to access. If the module denies access or allows access only to encrypted or otherwise protected forms of the secret keys, private keys, and CSPs, the requirement is met.

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

AS07.02: (Levels 1, 2, 3, and 4) Public keys shall be protected within the cryptographic module against unauthorized modification and substitution.

Required Vendor Information

VE07.02.01: The vendor documentation shall describe the protection of all public keys against unauthorized modification and substitution.

Required Test Procedures

TE07.02.01: The vendor documentation shall describe how the public keys are protected from unauthorized modification and unauthorized substitution.

TE07.02.02: The tester shall modify all public keys using any method not specified by the vendor documentation and shall attempt to load them into the module. The module should not allow any of the keys to be successfully loaded. The tester shall attempt to perform cryptographic operations using these keys; the module should not perform the operations, indicating that the keys were not loaded.

AS07.03: (Levels 1, 2, 3, and 4) Documentation shall specify all cryptographic keys, cryptographic key components, and CSPs employed by the cryptographic module.

Required Vendor Information

VE07.03.01: The vendor documentation shall provide a list all cryptographic keys, cryptographic key components, and CSPs used by the module.

Required Test Procedures

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

7.1 Random Number Generators (RNGs)

AS07.04: (Levels 1, 2, 3, and 4) If a cryptographic module employs Approved or non-Approved RNGs in an Approved mode of operation, the data output from the RNG shall pass the continuous random number generator test as specified in Section 4.9.2.

Note: This assertion is tested in AS09.41-AS09.43.

AS07.05:

Note: There are no requirements for this assertion number.

AS07.06: (Levels 1, 2, 3, and 4) Approved RNGs shall be subject to the cryptographic algorithm test in Section 4.9.1.

Note: This assertion is tested in AS09.13.

AS07.07: (Levels 1, 2, 3, and 4) Nondeterministic RNGs shall comply with all applicable RNG requirements of this standard.

Note: This assertion is not separately tested.

AS07.08: (Levels 1, 2, 3, and 4) An Approved RNG shall be used for the generation of cryptographic keys used by an Approved security function.

Required Vendor Information

VE07.08.01: The vendor shall provide documentation stating that an Approved RNG is used to generate keys. Approved RNGs can be found in Annex C to FIPS PUB 140-2.

Required Test Procedures

TE07.08.01: The tester shall verify that the vendor has provided documentation asserting that the RNGs used for the generation of cryptographic keys used by Approved security functions are Approved RNGs found in Annex C of FIPS PUB 140-2.

TE07.08.02: The tester shall review the vendor provided documentation to verify that the implemented RNG matches the specified Approved RNG.

AS07.09: (Levels 1, 2, 3, and 4) The seed and seed key shall not have the same value.

Required Vendor Information

VE07.09.01: The vendor shall provide documentation describing the method that ensures that the seed and seed key input to the Approved RNG do not have the same value.

Required Test Procedures

TE07.09.01: The tester shall verify that the vendor provided documentation shows that the seed and seed key cannot assume the same value.

TE07.09.02: The tester shall verify that the vendor provided documentation matches the implementation.

AS07.10: (Levels 1, 2, 3, and 4) Documentation shall specify each RNG (Approved and non-Approved) employed by a cryptographic module.

Required Vendor Information

VE07.10.01: The vendor documentation shall specify all RNGs (Approved and non-Approved) used in the cryptographic module, their type (Approved or non-Approved) and how each RNG (Approved and non-Approved) is used within the cryptographic module.

Required Test Procedures

TE07.10.01: The tester shall review the vendor documentation to verify that, the information specified in VE07.10.01 is included.

7.2 Key Generation

AS07.11: (Levels 1, 2, 3, and 4) Cryptographic keys generated by the cryptographic module for use by an Approved algorithm or security function shall be generated using an Approved key generation method.

Required Vendor Information

VE07.11.01: The vendor shall provide documentation stating that an Approved key generation method is used to generate keys.

Required Test Procedures

TE07.11.01: The tester shall verify that the vendor has provided documentation asserting that the method used for the generation of cryptographic keys is an Approved key generation method.

TE07.11.02: The tester shall review the vendor provided documentation to verify that the implemented key generation method matches the specified Approved key generation method.

AS07.12: (Levels 1, 2, 3, and 4) If an Approved key generation method requires input from a RNG, then an Approved RNG that meets the requirements specified in Section 4.7.1 shall be used.

Note: This assertion is tested as part of AS07.04-AS07.08 and AS07.10.

AS07.13: (Levels 1, 2, 3, and 4) Compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic RNG) shall require as least as many operations as determining the value of the generated key.

Required Vendor Information

VE07.13.01: The vendor shall provide documentation that provides rationale stating how compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic RNG) shall require as least as many operations as determining the value of the generated key.

Required Test Procedures

TE07.13.01: The tester shall verify that the vendor provided documentation that provides rationale stating how compromising the security of the key generation method (e.g., guessing the seed value to initialize the deterministic RNG) shall require as least as many operations as determining the value of the generated key.

TE07.13.02: 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.

AS07.14: (Level 1, 2, 3, and 4) If a seed key is entered during the key generation process, entry of the key shall meet the key entry requirements specified in Section 4.7.4.

Note: This assertion is tested as part of AS07.23.

AS07.15: (Levels 1, 2, 3, and 4) If intermediate key generation values are output from the cryptographic module upon completion of the key generation process, the values shall be output either 1) in encrypted form or 2) under split knowledge procedures.

Required Vendor Information

VE07.15.01: Vendor documentation shall indicate whether any intermediate key generation values are output from the module upon completion of the key generation process.

VE07.15.02: If intermediate key generation values are output from the cryptographic module upon the completion of the key generation process, then the documentation shall specify that the values are output either 1) in encrypted form or 2) under split knowledge procedures.

Required Test Procedures

TE07.15.01: The tester shall verify that the vendor documentation indicates whether any intermediate key generation values are output from the module upon completion of the key generation process.

TE07.15.02: The tester shall verify that no intermediate key generation values are output from the cryptographic module during the key generation process.

TE07.15.03: The tester shall observe the output interface and verify that all output matches the documented output, and that no plaintext intermediate key generation values are output.

TE07.15.04: The tester shall verify that upon completion, the intermediate key generation values are output in either 1) in encrypted form, or 2) under split knowledge procedures.

AS07.16: (Levels 1, 2, 3, and 4) Documentation shall specify each of the key generation methods (Approved and non-Approved) employed by the cryptographic module.

Required Vendor Information

VE07.16.01: The vendor shall provide documentation stating the key generation methods (Approved and non-Approved) employed by the cryptographic module.

Required Test Procedures

TE07.16.01: The tester shall verify that the vendor has provided documentation describing the key generation methods (Approved and non-Approved).

TE07.16.02: The tester shall review the vendor provided documentation to verify that the implemented key generation methods match the specified key generation methods (Approved and non-Approved).

7.3 Key Establishment

AS07.17: (Levels 1, 2, 3, and 4) If key establishment methods are employed by the cryptographic module, only Approved key establishment techniques shall be used.

Required Vendor Information

VE07.17.01: The vendor shall provide documentation stating that an Approved key establishment technique is used. Approved key establishment techniques can be found in Annex D to FIPS PUB 140-2.

Required Test Procedures

TE07.17.01: The tester shall verify that the vendor has provided documentation asserting that the Approved key establishment techniques used are found in Annex D of FIPS PUB 140-2.

TE07.17.02: The tester shall review the vendor provided documentation to verify that the implemented key establishment techniques match the specified Approved key establishment techniques.

AS07.18: (Levels 1, 2, 3, and 4) If, in lieu of an Approved key establishment technique, a radio communications cryptographic module implements Over-The-Air-Rekeying (OTAR), it shall be implemented as specified in the TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, Over-The-Air-Rekeying (OTAR) Protocol, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA, January, 1996, Telecommunications Industry Association.

Required Vendor Information

VE07.18.01: Vendor documentation shall indicate whether the cryptographic module is used for radio communications. If so, and the module implements the OTAR Protocol, the vendor shall provide documentation stating that the OTAR implementation complies with APCO Project 25, OTAR Protocol.

Required Test Requirements

TE07.18.01: The tester shall verify that the vendor provided documentation provides rationale stating how the radio communications cryptographic module implements Over-The-Air-Rekeying (OTAR), as specified in the TIA/EIA Telecommunications Systems Bulletin, APCO Project 25, Over-The-Air-Rekeying (OTAR) Protocol, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA, January, 1996, Telecommunications Industry Association.

TE07.18.02: 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.

AS07.19: (Levels 1, 2, 3, and 4) Compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require as many operations as determining the value of the cryptographic key being transported or agreed upon.

Required Vendor Information

VE07.19.01: The vendor shall provide documentation that provides rationale stating how compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require as many operations as determining the value of the cryptographic key being transported or agreed upon.

Required Test Procedures

TE07.19.01: The tester shall verify that the vendor provided documentation provides rationale stating how compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require as many operations as determining the value of the cryptographic key being transported or agreed upon.

TE07.19.02: 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.

AS07.20: (Levels 1, 2, 3, and 4) If a key transport method is used, the cryptographic key being transported shall meet the key entry/output requirements of Section 4.7.4.

Note: This assertion is tested as part of AS07.23-AS07.30.

AS07.21: (Levels 1, 2, 3, and 4) Documentation shall specify the key establishment methods employed by the cryptographic module.

Required Vendor Information

VE07.21.01: The vendor shall provide documentation stating the key establishment methods employed by the cryptographic module.

Required Test Procedures

TE07.21.01: The tester shall verify that the vendor has provided documentation describing the key establishment methods.

TE07.21.02: The tester shall review the vendor provided documentation to verify that the implemented key establishment methods match the specified key establishment methods.

7.4 Key Entry and Output

AS07.22: (Levels 1, 2, 3, and 4) If cryptographic keys are entered into or output from the cryptographic module, the entry or output of keys shall be performed using either manual (e.g., via a keyboard) or electronic methods (e.g., smart cards/tokens, PC cards, or other electronic key loading devices).

Note: This assertion is tested in AS07.28.

AS07.23: (Levels 1, 2, 3, and 4) A seed key, if entered during key generation, shall be entered in the same manner as cryptographic keys.

Required Vendor Information

VE07.23.01: The key management documentation shall describe the entry of the seed key.

Required Test Procedures

TE07.23.01: The tester shall review the vendor provided documentation to determine whether a seed key is used for key generation. If so, the tester shall review the key management documentation and verify that entry of the seed key is identical to the entry of a cryptographic key.

TE07.23.02: The tester shall enter a seed key and shall verify that the method used to enter it is consistent with the documented method.

AS07.24: (Levels 1, 2, 3, and 4) All encrypted secret and private keys, entered into or output from the cryptographic module and used in an Approved mode of operation, shall be encrypted using an Approved algorithm.

Required Vendor Information

VE07.24.01: The vendor shall supply documentation specifying the Approved algorithms used to encrypt secret and private keys entered into or output from the cryptographic module.

Required Test Procedures

TE07.24.01: The tester shall verify that the vendor supplied documentation specifies the Approved algorithms used to encrypt secret and private keys entered into or output from the cryptographic module.

TE07.24.02: The tester shall review the vendor provided documentation to verify that the implemented Approved algorithms used to encrypt secret and private keys entered into or output from the cryptographic module matches the specified encryption methods.

AS07.25: (Levels 1, 2, 3, and 4) The cryptographic module shall associate a key (secret, private, or public) entered into or output from the module with the correct entity (i.e., person, group, or process) to which the key is assigned.

Required Vendor Information

VE07.25.01: The documented key entry/output procedures shall describe the mechanisms or procedures used to ensure that each key is associated with the correct entity.

Required Test Procedures

TE07.25.01: The tester shall review the documented key entry/output procedures and verify that the procedures address how an entered or output key is associated with the correct entity.

TE07.25.02: For each key that can be entered or output, the tester shall first output the key while assuming a particular entity. The tester shall then verify the association between key and entity by performing the following tests:

1. The tester shall assume a different entity from the one under which the key was output. The tester shall then attempt to enter the key and shall verify that key entry fails.

2. The tester shall, if possible, alter the key component such that the key is associated with a different entity. The tester shall then assume the entity under which the key was output, attempt to enter the key, and shall verify that key entry fails.

AS07.26: (Levels 1, 2, 3 and 4) *Manually-entered* cryptographic keys (keys entered using manual methods) shall be verified during entry into the cryptographic module for accuracy using the manual key entry test specified in Section 4.9.2.

Note: This assertion is tested as part of AS09.40.

AS07.27: (Levels 1, 2, 3, and 4) If encrypted cryptographic keys or key components are manually entered into the cryptographic module, then the plaintext values of the cryptographic keys or key components shall not be displayed.

Required Vendor Information

VE07.27.01: The documented key entry procedures shall preclude the display of plaintext secret or private keys that result from the entry of encrypted keys or key components.

Required Test Procedures

TE07.27.01: The tester shall review the documented key entry procedures and verify that the display of plaintext keys resulting from the entry of encrypted keys or key components is not allowed during the key entry process.

TE07.27.02: The tester shall enter all encrypted cryptographic keys and key components and shall monitor the output interface of the module to verify that any resulting plaintext key material is not displayed.

AS07.28: (Levels 1, 2, 3, and 4) Documentation shall specify the key entry and output methods employed by the cryptographic module.

Required Vendor Information

VE07.28.01: The vendor documentation shall specify the key entry and output methods employed by the cryptographic module.

Required Test Procedures

TE07.28.01: The tester shall review the vendor documentation to verify that the information specified in VE07.28.01 is included.

TE07.28.02: The tester shall enter and output each of the manually entered keys and shall verify that they are entered and/or output according to the documentation.

AS07.29: (Levels 1, 2, 3 and 4) For Security Levels 1 and 2, secret and private keys established using automated methods shall be entered into and output from a cryptographic module in encrypted form.

Required Vendor Information

VE07.29.01: The vendor documentation shall specify keys that are established using automated methods. The vendor documentation shall state whether these keys are entered into and output in encrypted form.

Required Test Procedures

TE07.29.01: The tester shall verify that the vendor has provided documentation asserting that secret and private keys established using automated methods are entered into and output from the cryptographic module in encrypted form.

TE07.29.02: If automated means are used to establish secret and private keys, the tester shall verify that these keys are entered into and output from the cryptographic module in encrypted form.

AS07.30: (Levels 3 and 4) Secret and private keys established using automated methods shall be entered into and output from a cryptographic module in encrypted form.

Note: This assertion is tested as part of AS07.29.

AS07.31: (Levels 3 and 4) Secret and private keys established using manual methods shall be entered into or output from the cryptographic module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext cryptographic key components).

Required Vendor Information

VE07.31.01: This VE is tested as part of VE07.28.01.

Required Test Procedures

TE07.31.01: Verification of the vendor documentation was performed under TE07.27.01.

TE07.31.02: The tester shall verify that the vendor has provided documentation asserting that secret and private keys established using manual methods are entered into or output from the cryptographic module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext cryptographic key components).

TE07.31.03: If manual methods are used to establish secret and private keys, the tester shall verify that these keys are entered into the cryptographic module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext cryptographic key components).

TE07.31.04: If manual methods are used to establish secret and private keys, the tester shall verify that these keys are output from the cryptographic module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext cryptographic key components).

AS07.32: (Levels 3 and 4) If split knowledge procedures are used, the cryptographic module shall separately authenticate the operator entering or outputting each key component.

Required Vendor Information

VE07.32.01: The vendor documentation shall specify the method the cryptographic module uses to separately authenticate the operator entering or outputting each key component.

Required Test Procedures

TE07.32.01: The tester shall check that authentication is performed for each key component and that the authentication is in accordance with the documented key entry and output procedures.

TE07.32.02: The tester shall enter each key component using split knowledge procedures and verify that each operator entering a key component is authenticated.

TE07.32.03: The tester shall output each key component using split knowledge procedures and verify that each operator outputting a key component is authenticated.

AS07.33: (Levels 3 and 4) If split knowledge procedures are used, plaintext cryptographic key components shall be directly entered into or output from the cryptographic module (e.g., via a trusted path or directly attached cable) without traveling through any enclosing or intervening systems where the key components may inadvertently be stored, combined, or otherwise processed (see Section 4.2).

Note: This assertion is tested as part of AS02.18.

AS07.34: (Levels 3 and 4) If split knowledge procedures are used, at least two key components shall be required to reconstruct the original cryptographic key.

Required Vendor Information

VE07.34.01: If manually established secret or private keys are entered or output under split knowledge procedures, the vendor documentation shall specify the number of key components that are required to construct the original key.

Required Test Procedures

TE07.34.01: The tester shall review the vendor documentation to verify that the entry of manually established secret or private keys entered under split knowledge procedures requires at least two components to construct the original key.

TE07.34.02: The tester shall review the vendor documentation to verify that the output of manually establishment secret or private keys output under split knowledge procedures does not result in the output of a single key component that can be used to construct the original key.

AS07.35: (Levels 3 and 4) If split knowledge procedures are used, documentation shall prove that if knowledge of n key components is required to reconstruct the original key, then knowledge of any n-1 key components provides no information about the original key other than the length.

Required Vendor Information

VE07.35.01: The vendor shall provide documentation that provides rationale stating how knowledge of any n –1 key components provides no information about the original key other than the length.

Required Test Procedures

TE07.35.01: The tester shall verify that the vendor provided documentation provides rationale stating if n key components are required to construct the original key, then knowledge of any n –1 key components provides no information about the original key other than the length.

TE07.35.02: 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.

AS07.36: (Levels 3 and 4) If split knowledge procedures are used, documentation shall specify the procedures employed by the cryptographic module.

Required Vendor Information

VE07.36.01: The vendor shall supply documentation specifying the split knowledge procedures employed by the cryptographic module.

Required Test Procedures

TE07.36.01: The tester shall verify that the documentation matches the implementation.

7.5 Key Storage

AS07.37: (Levels 1, 2, 3, and 4) Cryptographic keys stored within the cryptographic module shall be stored either in plaintext form or encrypted form.

Note: This assertion is tested under AS07.40.

AS07.38: (Levels 1, 2, 3, and 4) Plaintext secret and private keys shall not be accessible from outside the cryptographic module to unauthorized operators.

Note: This assertion is tested under AS07.01.

AS07.39: (Levels 1, 2, 3, and 4) The cryptographic module shall associate the cryptographic key (secret, private, or public) stored within the module with the correct entity (e.g., person, group, or process) to which the key is assigned.

Required Vendor Information

VE07.39.01: Vendor documentation on key storage shall describe the mechanisms or procedures used to ensure that each key is associated with the correct entity.

Required Test Procedures

TE07.39.01: The tester shall review the documentation on key storage and shall verify that the procedures address how a stored key is associated with the correct entity.

TE07.39.02: The tester shall alter 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.

AS07.40: (Levels 1, 2, 3, and 4) Documentation shall specify the key storage methods employed by the cryptographic module.

Required Vendor Information

VE07.40.01: The vendor documentation shall specify the following information for each stored key:

a. Type and identifier

b. Storage location

c. The form in which the key is stored (plaintext, encrypted form, under split knowledge procedures). If the keys are stored in encrypted form, specify the Approved algorithm used to encrypt the keys.

Required Test Procedures

TE07.40.01: The tester shall review the vendor documentation to verify that the information specified in VE07.40.01 is included.

7.6 Key Zeroization

AS07.41: (Levels 1, 2, 3, and 4) The cryptographic module shall provide methods to zeroize all plaintext secret and private cryptographic keys and CSPs within the module.

Required Vendor Information

VE07.41.01: The vendor documentation shall specify the following plaintext secret and private cryptographic keys and CSPs zeroization information:

a. Zeroization techniques
b. Restrictions when plaintext secret and private cryptographic keys and CSPs can be zeroized
c. Plaintext secret and private cryptographic keys and CSPs that are zeroized
d. Plaintext secret and private cryptographic keys and CSPs that are not zeroized and rationale
e. Rationale explaining how the zeroization technique is performed in a time that is not sufficient to compromise plaintext secret and private keys and CSPs

Required Test Procedures

TE07.41.01: The tester shall review the vendor documentation to verify that the information specified in VE07.41.01 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.

TE07.41.02: The tester shall note which keys are present in the module and initiate the zeroize command. Following the completion of the zeroize command, the tester shall attempt to perform cryptographic operations using each of the plaintext secret and private cryptographic keys and CSPs that were stored in the module. The tester shall verify that each plaintext secret and private cryptographic keys and CSPs cannot be accessed.

TE07.41.03: The tester shall initiate zeroization and verify the key destruction method is performed in a time that an attacker cannot access plaintext secret and private cryptographic keys and other unprotected CSPs while under the direct control of the operator of the module (i.e. present to observe the method has completed successfully or controlled via a remote management session). If the method is not under the direct control of the operator, then rationale shall be provided on how the zeroization method(s) are employed such that the secret and private cryptographic keys and other CSPs within the module cannot be obtained by an attacker.

TE07.41.04: The tester shall verify that all plaintext secret and private cryptographic keys and CSPs that are not zeroized by the zeroize 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 this standard).

AS07.42: (Levels 1, 2, 3, and 4) Documentation shall specify the key zeroization methods employed by a cryptographic module.

Note: This assertion is tested under AS07.41.

8. ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY (EMI/EMC)

AS08.01: (Levels 1, 2, 3, and 4) Cryptographic modules shall meet the following requirements for EMI/EMC.

Note: This assertion is not separately tested.

AS08.02: (Levels 1, 2, 3, and 4) Radios are explicitly excluded from these requirements but shall meet all applicable FCC requirements.

Note: The phrase "these requirements" refers to the requirements in FIPS PUB 140-2.

Required Vendor Information

VE08.02.01: The vendor shall provide the name of the FCC Accredited Laboratory.

VE08.02.02: The vendor shall provide the FCC ID number for the cryptographic module.

Required Test Procedures

TE08.02.01: The tester shall verify that the vendor has supplied the name of the FCC Accredited Laboratory required under VE08.02.01.

TE08.02.02: The tester shall verify that the vendor has supplied the FCC ID number required under VE08.02.02.

AS08.03: (Levels 1, 2, 3, and 4) Documentation shall include proof of conformance to EMI/EMC requirements.

Note: This assertion is tested as part of AS08.04 and AS08.05.

AS08.04: (Levels 1 and 2) The cryptographic module shall (at a minimum) conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

Required Vendor Information

VE08.04.01: The vendor shall provide evidence and documentation that indicates the cryptographic module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use):

Required Test Procedures

TE08.04.01: The tester shall verify that the vendor has supplied the information required under VE08.04.01.

TE08.04.02: The tester shall verify that the version of the cryptographic module that is indicated on the supplied information specified in TE08.04.01 is referenced in AS10.02.

AS08.05: (Levels 3 and 4) The cryptographic module shall (at a minimum) conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

Required Vendor Information

VE08.05.01: The vendor shall provide evidence and documentation that indicates the cryptographic module conforms to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

Required Test Procedures

TE08.05.01: The tester shall verify that the vendor has supplied the information required under VE08.05.01.

TE08.05.02: The tester shall verify that the version of the cryptographic module that is indicated on the supplied information specified in TE08.05.01 is referenced in AS10.02.

9. SELF-TESTS

General

AS09.01: (Levels 1, 2, 3, and 4) The cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly.

Note: This assertion is tested as part of AS09.07.

AS09.02: (Levels 1, 2, 3, and 4) *Power-up self-tests* shall be performed when the cryptographic module is powered up.

Note: This assertion is tested as part of AS09.07.

AS09.03: (Levels 1, 2, 3, and 4) *Conditional self-tests* shall be performed when an applicable security function or operation is invoked (i.e., security functions for which self-tests are required).

Note: This assertion is tested as part of AS09.07.

AS09.04: (Levels 1, 2, 3, and 4) If the cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status output interface.

Required Vendor Information

VE09.04.01: The vendor shall document all error states associated with each self-test and shall indicate for each error state the expected error indicator.

Required Test Procedures

TE09.04.01: The tester shall inspect the vendor documentation, check that it lists every error state that the module enters upon failure of a self-test, and indicates the error indicator associated with each error state. The tester shall compare the list of error states to those defined in the finite state model (see AS04.05) to verify that they agree.

TE09.04.02: By inspecting the vendor documentation that specifies how each self-test handles errors, the tester shall verify that:

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

TE09.04.03: The tester shall run self-tests and cause the module to enter every error state. The tester shall compare the observed error indicator with the indicator specified in the vendor documentation. If they are not the same, the assertion fails.

AS09.05: (Levels 1, 2, 3, and 4) The cryptographic module shall not perform any cryptographic operations while in an error state.

Required Vendor Information

VE09.05.01: See VE02.06.01 for the vendor design requirement. The vendor design shall ensure that cryptographic operations cannot be performed while the module is in the error state.

Required Test Procedures

TE09.05.01: Tester verification of the inhibition of output was performed under TE02.06.01 and TE02.06.02. The results of the verification shall indicate that the module inhibits all data output when the module is in an error state.

TE09.05.02: The tester shall verify that vendor documentation specifies that cryptographic functions are inhibited while the module is in an error state. Cryptographic functions include the following:

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

TE09.05.03: The tester shall put the module in the error state and verify that any cryptographic operations that the tester attempts to initiate are prevented.

AS09.06: (Levels 1, 2, 3, and 4) All data output via the data output interface shall be inhibited when an error state exists.

Required Vendor Information

VE09.06.01: See VE02.06.01 for the vendor design requirement. The vendor design shall ensure that cryptographic operations cannot be performed while the module is in an error state.

Required Test Procedures

TE09.06.01: Tester verification of the inhibition of output was performed under TE02.06.01 and TE02.06.02. The results of the verification shall indicate that the vendor documentation shows that all data output via the data output interface is inhibited whenever the module is in an error state.

TE09.06.02: The tester shall put the module in an error state and verify that all data output via the data output interface is inhibited when an error state exists.

AS09.07: (Levels 1, 2, 3, and 4) Documentation shall specify:

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

Required Vendor Information

VE09.07.01: The vendor shall provide a list of all self-tests that the module can perform. This list shall include both power-up tests and conditional tests.

VE09.07.02: For each error condition, the vendor documentation shall provide the condition name, the events that can produce the condition, and the actions necessary to clear the condition and resume normal operation.

Required Test Procedures

TE09.07.01: The tester shall inspect the list of self-tests to verify that it includes the following:

1. Power-up tests

   - Cryptographic algorithm test
   - Random number generator test
   - Software/firmware test
   - Critical functions test
   - Other self-tests that are performed at power-up and on demand

2. Conditional tests

   - Pairwise consistency test (if the module generates public and private keys)
   - Software/firmware load test
   - Manual key entry test
   - Continuous random number generator test
   - Bypass test
   - Other conditional tests

TE09.07.02: The tester shall check that the information provided above is specified for each error condition.

TE09.07.03: 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 review the code listing and or design documentation to determine whether the actions necessary to clear each error condition are consistent with the descriptions in the vendor documentation.

9.1 Power-Up Tests

General

AS09.08: (Levels 1, 2, 3, and 4) Power-up tests shall be performed by the cryptographic module when the module is powered up (after being powered off, reset, rebooted, etc.).

Note: This assertion is tested as part of AS09.09.

AS09.09: (Levels 1, 2, 3, and 4) The power-up tests shall be initiated automatically and shall not require operator intervention.

Required Vendor Information

VE09.09.01: The vendor documentation shall require that the running of power-up self-tests not involve any inputs from or actions by the operator.

Required Test Procedures

TE09.09.01: The tester shall verify that the vendor documentation includes the information required under VE09.09.01.

TE09.09.02: The tester shall power-up the module and verify that the module performs the power-up self-tests without requiring any operator intervention.

AS09.10: (Levels 1, 2, 3, and 4) When the power-up tests are completed, the results (i.e., indications of success or failure) shall be output via the "status output" interface.

Required Vendor Information

VE09.10.01: The vendor shall document the indicator that the module outputs upon successful completion of the power-up self-tests.

Required Test Procedures

TE09.10.01: The tester shall verify that the vendor documentation specifies an indicator that is output from the status output interface upon successful completion of the power-up self-tests.

TE09.10.02: The tester shall power-up the module and shall monitor the status output interface. The expected indicator from the status output interface should be consistent with the documented indicator.

AS09.11: (Levels 1, 2, 3, and 4) All data output via the output interface shall be inhibited when the tests are performed.

Note: This assertion is tested as part of AS02.06.

AS09.12: (Levels 1, 2, 3, and 4) In addition to performing the power-up tests when powered up, the cryptographic module shall permit operators to initiate the tests on demand for periodic testing of the module.

Required Vendor Information

VE09.12.01: The vendor shall describe the procedure by which an operator can initiate the power-up self-tests on demand. All of the power-up self-tests must be included.

Required Test Procedures

TE09.12.01: The tester shall inspect the vendor documentation to verify that initiation of power-up self-tests on demand is specified for all of the power-up self-tests.

TE09.12.02: The tester shall initiate the power-up on demand self-tests to verify that the initiation of the power-up self-tests on demand is consistent with vendor documentation.

AS09.13: (Levels 1, 2, 3, and 4) The cryptographic module shall perform the following power-up tests: cryptographic algorithm test, software/firmware integrity test, and critical functions test.

Required Vendor Information

VE09.13.01: See VE09.07.01 for the vendor requirement.

Required Test Procedures

TE09.13.01: Verification of the documented list of power-up self-tests was performed under TE09.07.01.

TE09.13.02: Verification that the module performs the self-tests as documented is done under validation requirements for AS09.16-AS09.28.

AS09.14:

Note: There are no requirements for this assertion number.

AS09.15:

Note: There are no requirements for this assertion number.

Cryptographic algorithm test

AS09.16: (Levels 1, 2, 3, and 4) A cryptographic algorithm test using a known answer shall be conducted for all cryptographic functions (e.g., encryption, decryption, authentication, and random number generation) of each Approved cryptographic algorithm implemented by a cryptographic module.

Required Vendor Information

VE09.16.01: See VE09.07.01 for the vendor requirement.

Required Test Procedures

TE09.16.01: By inspecting the vendor documentation, the tester shall verify that a known answer test is associated with all cryptographic functions of each Approved cryptographic algorithm implemented by the cryptographic module as indicated in AS01.12.

TE09.16.02: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

AS09.17: (Levels 1, 2, 3, and 4) If the calculated output does not equal the known answer, the known-answer test shall fail.

Required Vendor Information

VE09.17.01: The vendor documentation shall specify the method used to compare the calculated output with the known answer.

VE09.17.02: 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

TE09.17.01: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

TE09.17.02: This is tested under TE09.04.01, TE09.04.02, and TE09.04.03.

AS09.18: (Levels 1, 2, 3, and 4) Cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the Digital Signature Algorithm) shall be tested using a known-answer test or shall be tested using a pair-wise consistency test.

Required Vendor Information

VE09.18.01: See VE09.07.01 for the vendor requirement.

VE09.18.02: The vendor documentation shall specify and describe the test(s) which is implemented.

Required Test Procedures

TE09.18.01: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

TE09.18.02: By inspecting the vendor documentation, the tester shall verify if either a known-answer test or a pair-wise consistency test is associated with the cryptographic function.

TE09.18.03: Pair-wise consistency is tested in AS09.31 (encryption), AS09.32 (key agreement) and AS09.33 (digital signature creation and verification).

AS09.19: (Levels 1, 2, 3, and 4) Message digest algorithms shall have an independent known-answer test or the known-answer test shall be included with the associated cryptographic algorithm test (e.g., the Digital Signature Standard).

Required Vendor Information

VE09.19.01: See VE09.07.01 for the vendor requirement.

VE09.19.02: The vendor documentation shall specify and describe the test(s) which is implemented.

Required Test Procedures

TE09.19.01: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

TE09.19.02: The tester shall determine whether the module implements a message digest algorithm. If so, the tester shall verify that the vendor documentation specifies whether the message digest algorithm has its own known answer test or whether it is included in the known answer test of another algorithm.

TE09.19.03: By checking the code listing and/or design documentation, the tester shall verify that the module uses either a separate known answer test or the known answer test of an algorithm in order to test a message digest algorithm.

AS09.20: (Levels 1, 2, 3, and 4) If the cryptographic module includes two independent implementations of the same cryptographic algorithm, then the outputs of two implementations shall be continuously compared.

Required Vendor Information

VE09.20.01: See VE09.07.01 for the vendor requirement.

VE09.20.02: The vendor shall specify whether a known answer test or the comparison of the output of two independent cryptographic algorithm implementations (compared answer test) is used to test the module's cryptographic algorithm. If the compared answer test is used, the vendor shall document this fact.

Required Test Procedures

TE09.20.01: The tester shall determine from the vendor documentation whether a known answer test or a compared answer test is used to test the module's cryptographic algorithm. If the compared answer test is used, the tester shall determine whether the documentation of the compared answer test includes:

1. Use of two independent cryptographic algorithm implementations
2. Continual comparison of the outputs of the algorithm implementation
3. Transition into an error state and output of an error indicator when the two outputs are not equal

TE09.20.02: By checking the code and/or design documentation, the tester shall verify that the module implements the documented steps for performing a compared answer test.

TE09.20.03: Validation of whether the module enters the error state and outputs an error indicator upon failure of the self-test is performed under TE09.04.01, TE09.04.02, and TE09.04.03. If any of these tests fail, this assertion fails.

AS09.21: (Levels 1, 2, 3, and 4) If the cryptographic module includes two independent implementations of the same cryptographic algorithm then, if the outputs of two implementations are not equal, the cryptographic algorithm test shall fail.

Note: This assertion is tested as part of AS09.20.

Software/firmware integrity test

AS09.22: (Levels 1, 2, 3, and 4) A software/firmware integrity test using an error detection code (EDC) or Approved authentication technique (e.g., an Approved message authentication code or digital signature algorithm) shall be applied to all validated software and firmware components within the cryptographic module when the module is powered up.

Required Vendor Information

VE09.22.01: The vendor documentation shall specify whether an error detection code (EDC) or a Approved authentication technique (e.g., an Approved message authentication code or digital signature algorithm) is implemented as an integrity test for all software and firmware components.

VE09.22.02: The documentation shall describe the implemented integrity mechanism.

VE09.22.03: If the module implements an Approved authentication technique:

(1) The vendor shall provide a validation certificate as specified in VE01.12.01.

or

(2) In the absence of a CMVP algorithm validation certificate issuing process, the vendor organization shall provide a written affirmation asserting that the authentication technique implemented in the module is Approved.

Required Test Procedures

TE09.22.01: The tester shall determine from the vendor supplied documentation which technique is used for the software/firmware components integrity test.

TE09.22.02: The tester shall verify that if an Approved authentication technique is implemented, the vendor documentation either include requirements in TE01.12.01 or in the absence of a CMVP algorithm validation certificate issuing process, the vendor organization shall provide a written affirmation of conformance.

TE09.22.03: If the module implements EDCs for software/firmware integrity, the tester shall verify that the vendor documentation of the software/firmware test includes:

1. Description of EDC algorithm.
2. Identification of software and firmware that is protected using EDCs.
3. Calculation of the EDCs when the software and firmware is installed.
4. Recalculation of the EDCs when the self-test is initiated.

5. Comparison of the stored EDC against the recalculated EDC.

6. Failure of the self-test when the two EDCs are not equal.

TE09.22.04: If the module implements a DAC for software/firmware integrity, the tester shall verify that the vendor documentation of the software/firmware test fully describes the process by which the DAC is calculated and verified.

TE09.22.05: If the module implements an Approved digital signature for software/firmware integrity, the tester shall verify that the vendor documentation of the software/firmware test includes the following:

1. Specify the Approved digital signature algorithm implemented.

2. Identification of software and firmware that is protected using the Approved digital signatures.

3. Calculation of the Approved digital signatures when the software and firmware is installed.

4. Verification of the Approved digital signature when the self-test is initiated.

5. Failure of the self-test upon failure of the Approved digital signature verification.

TE09.22.06: By checking the code and/or design documentation, the tester shall verify that the implementation of the software/firmware test is consistent with TE09.22.01, TE09.22.02, TE09.22.03, or TE09.22.04.

TE09.22.07: If possible, the tester shall test the module by modifying the stored software, firmware, or the implemented integrity mechanism and initiating the self-tests, and observing the output from the status output interface. If no indicator is output that indicates that the software/firmware self-test failed, the assertion fails.

AS09.23: (Levels 1, 2, 3, and 4) If the calculated result does not equal the previously generated result, the software/firmware test shall fail.

Note: This assertion is tested as part of AS09.22.

AS09.24: (Levels 1, 2, 3, and 4) If an EDC is used, the EDC shall be at least 16 bits in length.

Required Vendor Information

VE09.24.01: If the module implements EDCs for software/firmware integrity, the vendor documentation shall indicate that the EDC is at least 16 bits in length.

Required Test Procedures

TE09.24.01: The tester shall verify that the implemented EDCs are at least 16 bits in length.

Critical functions test

AS09.25: (Levels 1, 2, 3, and 4) Other security functions critical to the secure operation of the cryptographic module shall be tested when the module is powered up as part of the power-up tests.

Note: This assertion is tested as part of AS09.27.

AS09.26: (Levels 1, 2, 3, and 4) Other critical security functions performed under specific conditions shall be tested as conditional tests.

Note: This assertion is tested as part of AS09.27.

AS09.27: (Levels 1, 2, 3, and 4) Documentation shall specify all security functions critical to the secure operation of the cryptographic module and shall identify the applicable power-up tests and conditional tests performed by the module.

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 number generation, operation of the cryptographic algorithm, and cryptographic bypass.

Required Vendor Information

VE09.27.01: The vendor shall provide documentation of all critical functions. For each critical function, the vendor shall indicate:

1. The purpose of the critical function
2. Which critical functions are tested by which power-up tests
3. Which critical functions are tested by which conditional tests

Required Test Procedures

TE09.27.01: The tester shall review the vendor provided documentation of the critical functions and the self-tests that are designed to test them. This documentation shall include the following:

1. Identification and description of all critical functions
2. Identification of at least one self-test for every critical function

TE09.27.02: By checking the code and/or design documentation, the tester shall verify that the module performs the specified self-tests for each critical function.

AS09.28:

Note: There are no requirements for this assertion number.

9.2 Conditional Tests

AS09.29: (Levels 1, 2, 3, and 4) Conditional tests shall be performed by the cryptographic module when the conditions specified for the following tests occur: pair-wise consistency test, software/firmware load test, manual key entry test, continuous random number generator test, and bypass test.

Note: This assertion is not separately tested.

Pair-wise consistency test (for public and private keys).

AS09.30: (Levels 1, 2, 3, and 4) If the cryptographic module generates public or private keys, then the following pair-wise consistency tests for public and private keys shall be performed.

Note: This assertion is tested as part of AS09.31 and AS09.33.

AS09.31: (Levels 1, 2, 3, and 4) If the keys are used to perform an approved key transport method, then the public key shall encrypt a plaintext value. The resulting ciphertext value shall be compared to the original plaintext value. If the two values are equal, then the test shall fail. If the two values differ, then the private key shall be used to decrypt the ciphertext and the resulting value shall be compared to the original plaintext value. If the two values are not equal, the test shall fail.

Required Vendor Information

VE09.31.01: If public and private keys are to be used to perform an approved key transport method, the cryptographic module shall test for pairwise consistency by applying the public key to a plaintext value. 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 and the result shall be compared to the original plaintext.
- If the two values are not equal, then the test shall fail.

Required Test Procedures

TE09.31.01: If public and private keys are to be used to perform an approved key transport method, the tester shall verify that the implementation of the pairwise consistency check, as defined in AS09.31, is consistent with the vendor documentation by checking the code and/or design documentation.

AS09.32:

Note: There are no requirements for this assertion number.

AS09.33: (Levels 1, 2, 3, and 4) If the keys are used to perform the calculation and verification of digital signatures, then the consistency of the keys shall be tested by the calculation and verification of a digital signature. If the digital signature cannot be verified, the test shall fail.

Required Vendor Information

VE09.33.01: If the public and private keys are to be used only for the calculation and/or verification of digital signatures, then the cryptographic module shall test for pairwise consistency by calculation and verification of a signature. If the signature cannot be verified, the test shall fail.

Required Test Procedures

TE09.33.01: If the public and private keys are used for the calculation and/or verification of digital signatures, then the tester shall verify that the implementation of the pairwise consistency check as defined in AS09.33 is consistent with the vendor documentation by checking the code and/or design documentation.

Software/firmware load test

AS09.34: (Levels 1, 2, 3, and 4) If software or firmware components can be externally loaded into the cryptographic module, then the following software/firmware load tests shall be performed.

Note: This assertion is tested as part of AS09.34, AS09.35, and AS09.36.

AS09.35: (Levels 1, 2, 3, and 4) An Approved authentication technique (e.g., an Approved message authentication code, digital signature algorithm, or HMAC) shall be applied to all validated software

and firmware components when the components are externally loaded into the cryptographic module.

Required Vendor Information

VE09.35.01: The vendor documentation shall describe the Approved authentication technique used to protect the integrity of all externally loaded software and firmware components.

VE09.35.02: If the module implements an Approved authentication technique:

(1) The vendor shall provide a validation certificate as specified in VE01.12.01.

or

(2) In the absence of a CMVP algorithm validation certificate issuing process, the vendor organization shall provide a written affirmation asserting that the authentication technique implemented in the module is Approved.

Required Test Procedures

TE09.35.01: The tester shall determine from the vendor supplied documentation which Approved authentication technique is used for the software/firmware load test.

TE09.35.02: The tester shall verify that if an Approved authentication technique is implemented, the vendor documentation either include requirements in TE01.12.01 or in the absence of a CMVP algorithm validation certificate issuing process, the vendor organization shall provide a written affirmation of conformance.

TE09.35.03: 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:

1. Specify the Approved authentication technique implemented.
2. Identification of software and firmware that is protected using the Approved authentication technique.
3. Calculation of the Approved authentication technique when the software and firmware is loaded.
4. Verification of the Approved authentication technique when the load test is initiated.
5. Failure of the self-test upon failure of the Approved authentication technique verification.

TE09.35.04: By checking the code and/or design documentation, the tester shall verify that the implementation of the software/firmware load test is consistent with TE09.35.01, TE09.35.02 and TE09.35.03.

TE09.35.05: If possible, the tester shall test the module by modifying the software or firmware to be loaded, or the implemented authentication mechanism and initiating the self-tests, 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.

AS09.36: (Levels 1, 2, 3, and 4) The calculated result shall be compared with a previously generated result. If the calculated result does not equal the previously generated result, the software/firmware integrity test shall fail.

Note: This assertion is tested as part of AS09.35.

Manual key entry test

AS09.37: (Levels 1, 2, 3, and 4) If cryptographic keys or key components are manually entered into the cryptographic module, then the following manual key entry tests shall be performed.

Note: This assertion is not separately tested.

AS09.38: (Levels 1, 2, 3, and 4) The cryptographic key or key components shall have an EDC applied, or shall be entered using duplicate entries.

Note: This assertion is tested as part of AS09.40.

AS09.39: (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 tested as part of AS09.40.

AS09.40: (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

VE09.40.01: The vendor shall document the manual key entry test. Depending on whether error detection codes or duplicate key entries are used, the manual key entry test shall include the following:

1. Error detection codes (EDCs):
   - Description of EDC calculation algorithm
   - Description of verification process
   - Expected outputs for success or failure of test
2. Duplicate key entries:
   - Description of verification process
   - Expected outputs for success or failure of test

VE09.40.02: If EDCs are associated with keys, then the vendor documentation that describes the format of the cryptographic keys (see AS07.03) shall include fields for the error detection codes.

Required Test Procedures

TE09.40.01: Verification of vendor documentation is performed under TE07.28.01.

TE09.40.02: The tester shall determine 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 determine whether the following information is included:

1. Error detection codes:
   - Key format for all manually-entered keys, including fields for EDCs (see AS07.03)

- Description of EDC algorithm
- Description of EDC verification process
- All expected outputs for success or failure of the test

2. Duplicate key entries:
   - Duplicate key entries for all manually-entered keys
   - Description of duplicate key, entry verification process
   - All expected outputs for success or failure of the test

TE09.40.03: For manual key entry tests using EDCs, the tester shall perform the following tests:

1. The tester shall enter every manually entered key and verify that the procedure used to enter each key is in accordance with the documented procedure, including the form that the keys are in when they are entered.
2. The tester shall enter each type of manually-entered key without any errors and shall observe the status output interface. If no indicator is detected, or if the indicator does not match the documented indicator for the success of the manual key entry test, the test is failed.
3. The tester shall attempt to perform cryptographic operations with each entered key to verify that it was entered correctly.
4. The tester shall change either the EDC associated with each manually-entered key or the key itself and shall enter them into the module. The tester shall observe the indicator that is output from the status output interface; if no output is detected, or the indicator does not match the documented indicator for the failure of the manual key entry test, the test is failed.
5. The tester shall attempt to perform cryptographic operations with each key that was not successfully entered. Each operation using each key should fail, verifying that the key was not entered.

TE09.40.04: For manual key entry tests using duplicate key entries, the tester shall perform the following tests:

1. The tester shall enter each type of manually-entered key without any errors and shall observe the status output interface. If no indicator is detected, or if the indicator does not match the documented indicator for the success of the manual key entry test, the test is failed.
2. The tester shall attempt to perform cryptographic operations with each entered key to verify that it was entered correctly.
3. The tester shall alter the accuracy of one of the manually entered keys, either the first or second duplicate entry, and shall enter them into the module. The tester shall observe the indicator that is output from the status output interface; if no output is detected, or the indicator does not match the documented indicator for the failure of the manual key entry test, the test is failed.
4. The tester shall attempt to perform cryptographic operations with each key that was not successfully entered. Each operation using each key should fail, verifying that the key was not entered.

Continuous Random Number Generator Test

AS09.41: (Levels 1, 2, 3, and 4) If a cryptographic module employs Approved or non-Approved RNGs in an Approved mode of operation, the module shall perform the following continuous random number generator test on each RNG that tests for failure to a constant value.

Note: This assertion is tested as part of AS09.42 and AS09.43.

AS09.42: (Levels 1, 2, 3, and 4) If each call to a RNG produces blocks of n bits (where n > 15), the first n-bit block generated after power-up, initialization, or reset shall not be used, but shall be saved for comparison with the next n-bit block to be generated. Each subsequent generation of an n-bit block shall be compared with the previously generated block. The test shall fail if any two compared n-bit blocks are equal.

Required Vendor Information

VE09.42.01: If the module implements a random number generator, the vendor shall document the continuous random number generator test.

Required Test Procedures

TE09.42.01: The tester shall determine whether the module implements a random number generator. If so, the tester shall check the documentation, code and/or design documentation that specifies the continuous random number generator test to verify that it implements the specifics of the test. If the generator generates blocks of n bits, where n > 15, then the tester shall verify that the implementation of the test includes:

1. Storage of first block for comparison against the next block
2. Comparison of each subsequently generated block against the previously generated block
3. Failure of the test if two compared blocks are equal

If the generator consistently generates fewer than 16 bits, then the tester shall verify that the implementation of the test includes the following:

1. Storage of the first n bits, where n > 15, for comparison against the next n generated bits
2. Comparison of each subsequently generated n bits against the previously generated n bits
3. Failure of the test if two compared n-bit sequences are equal

AS09.43: (Levels 1, 2, 3, and 4) If each call to a RNG produces fewer than 16 bits, the first n bits generated after power-up, initialization, or reset (for some n > 15) shall not be used, but shall be saved for comparison with the next n generated bits. Each subsequent generation of n bits shall be compared with the previously generated n bits. The test fails if any two compared n-bit sequences are equal.

Required Vendor Information

VE09.43.01: If the module implements a random number generator, the vendor shall document the continuous random number generator test.

Required Test Procedures

TE09.43.01: The tester shall determine whether the module implements a random number generator. If so, the tester shall check the documentation, code and/or design documentation that addresses of the continuous random number generator test to verify that it implements the specifics of the test. If the generator generates blocks of n bits, where n > 15, then the tester shall verify that the implementation of the test includes:

1. Storage of first block for comparison against the next block
2. Comparison of each subsequently generated block against the previously generated block
3. Failure of the test if two compared blocks are equal

If the generator consistently generates fewer than 16 bits, then the tester shall verify that the implementation of the test includes the following:

1. Storage of the first n bits, where n > 15, for comparison against the next n generated bits
2. Comparison of each subsequently generated n bits against the previously generated n bits
3. Failure of the test if two compared n-bit sequences are equal

Bypass Test

AS09.44: (Levels 1, 2, 3, and 4) If the 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 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 not separately tested.

AS09.45: (Levels 1, 2, 3, and 4) The 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

VE09.45.01: 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.

VE09.45.02: The vendor shall provide a description of the test as defined in AS09.48. The bypass test shall demonstrate that, when switched to an exclusive cryptographic service, the module does not output plaintext information as defined in AS09.47. The test fails if the cryptographic module outputs plaintext information.

Required Test Procedures

TE09.45.01: 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.

TE09.45.02: 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.

TE09.45.03: The tester shall switch the module from the exclusive bypass service to the exclusive cryptographic service and verify that plaintext information is not output.

AS09.46: (Levels 1, 2, 3, and 4) If the 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

VE09.46.01: 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.

VE09.46.02: The vendor shall provide a description of the test as defined in AS09.48. The bypass test shall demonstrate that when the mechanism governing the switching procedure is modified:

1. 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.

2. The correct operation of the cryptographic service is verified by demonstrating that the module does not output plaintext information as defined in AS09.47. The test fails if the module outputs plaintext information.

Required Test Procedures

TE09.46.01: 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.

TE09.46.02: The tester shall verify that the vendor is consistent with the bypass test implementation through the review of the source code and/or design documentation.

TE09.46.03: The tester shall verify the correct operation of the bypass test by:

1. 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 alter the mechanism to test the method used.

2. 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.

AS09.47: (Levels 1, 2, 3, and 4) No single point of failure shall result in the unintentional output of plaintext.

Note: This assertion is tested as part of AS09.45 and AS09.46.

AS09.48: (Levels 1, 2, 3, and 4) Documentation shall specify the mechanism or logic governing the switching procedure.

Note: This assertion is tested as part of AS09.45 and AS09.46.

10. DESIGN ASSURANCE

10.1 Configuration Management

AS10.01: (Levels 1, 2, 3, and 4) A configuration management system shall be implemented for the cryptographic module and module components within the cryptographic boundary, and for associated module documentation.

Required Vendor Information

VE10.01.01: The vendor documentation shall describe the configuration management (CM) system for the cryptographic module, module components, and associated module documentation.

Required Test Procedures

TE10.01.01: The tester shall review the vendor provided documents to verify that a CM system has been implemented.

AS10.02: (Levels 1, 2, 3, and 4) Each version of each configuration item (e.g., cryptographic module, module components, user guidance, security policy, and operating system) that comprises the module and associated documentation shall be assigned and labeled with a unique identification number.

Required Vendor Information

VE10.02.01: The vendor CM documentation shall include a configuration list of all configuration items. The CM documentation shall describe the method used to uniquely identify the configuration items.

VE10.02.02: The vendor documentation shall describe the method used to uniquely identify the version of each configuration item being validated.

Required Test Procedures

TE10.02.01: The tester shall review the vendor provided configuration list to verify inclusion of configuration items.

TE10.02.02: The tester shall verify that the CM documentation specifies the method used to uniquely identify all configuration items.

TE10.02.03: The tester shall review the vendor provided CM documentation to verify that it includes a description of the method used to uniquely identify each version of a configuration item being validated.

TE10.02.04: The tester shall verify that the CM documentation uniquely identifies the version of each configuration item being validated.

10.2 Delivery and Operation

AS10.03: (Levels 1, 2, 3, and 4) Documentation shall specify the procedures for secure installation, initialization, and startup of the cryptographic module.

Required Vendor Information

VE10.03.01: The vendor documentation shall describe the steps necessary for the secure installation, initialization, and start-up of the cryptographic module.

Required Test Procedures

TE10.03.01: The tester shall review the vendor provided documentation to verify that it includes installation, initialization, and start-up procedures that result in a secure configuration.

TE10.03.02: The tester shall perform the procedures for the secure installation, initialization, and startup of the cryptographic module and verify their correctness.

AS10.04: (Levels 2, 3, and 4) In addition to the requirements of Security Level 1, documentation shall specify the procedures required for maintaining security while distributing and delivering versions of the cryptographic module to authorized operators.

Required Vendor Information

VE10.04.01: The delivery documentation shall describe the procedures necessary to maintain security when distributing the cryptographic module to authorized operators.

Required Test Procedures

TE10.04.01: The tester shall review the vendor provided documentation to verify that procedures required for maintaining security while distributing and delivering versions of the cryptographic module to authorized operators are correct.

10.3 Development

AS10.05: (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 AS10.06 and AS10.07.

AS10.06: (Levels 1, 2, 3, and 4) Documentation shall specify the correspondence between the design of the hardware, software, and firmware components of the cryptographic module and the cryptographic module security policy.

Required Vendor Information

VE10.06.01: The vendor documentation shall describe how the hardware, software, and firmware design(s) corresponds to the security policy (rules of operation) of the cryptographic module.

Required Test Procedures

TE10.06.01: The tester shall review the vendor documentation to verify that the security policy (rules of operation) of the cryptographic module is correct. The tester shall verify that each security rule is reflected in the design, and that the design implements the rule.

AS10.07: (Levels 1, 2, 3, and 4) If the cryptographic module contains software or firmware components, documentation shall specify the source code for the software and firmware components, annotated with comments that clearly depict the correspondence of the components to the design of the module.

Required Vendor Information

VE10.07.01: The vendor shall supply a list of the names of all the software and firmware components contained in the cryptographic module.

VE10.07.02: The vendor shall supply an annotated source listing of each software and firmware component contained in the cryptographic module.

Required Test Procedures

TE10.07.01: 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.

AS10.08: (Levels 1, 2, 3, and 4) If the cryptographic module contains hardware components, documentation shall specify the schematics and/or Hardware Description Language (HDL) listings for the hardware components.

Required Vendor Information

VE10.08.01: The vendor shall supply a list of the hardware components contained in the cryptographic module.

Required Test Procedures

TE10.08.01: 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.

AS10.09: (Levels 2, 3, and 4) In addition to the requirements for Security Level 1, the following requirement shall apply to cryptographic modules for Security Level 2.

Note: This assertion is tested as part of AS10.10.

AS10.10: (Levels 2, 3, and 4) Documentation shall specify a functional specification that informally describes the cryptographic module, the external ports and interfaces of the module, and the purpose of the interfaces.

Required Vendor Information

VE10.10.01: The vendor functional specification shall describe the cryptographic module, and each external interface and port.

VE10.10.02: The vendor functional specification shall describe the purpose of each external interface.

Required Test Procedures

TE10.10.01: The tester shall review the vendor functional specification to verify that the information specified in the VE10.10.01 is included. If this information is not included, then this assertion fails.

TE10.10.02: The tester shall review the vendor functional specification to verify that the information specified in the VE10.10.02 is included. If this information is not included, then this assertion fails.

AS10.11: (Levels 3 and 4) In addition to the requirements for Security Levels 1 and 2, the following requirements shall apply to cryptographic modules for Security Level 3.

Note: This assertion is tested as part of AS10.12 and AS10.13.

AS10.12: (Levels 3 and 4) All software and firmware components within the cryptographic module shall be implemented using a high-level language, except that the limited use of a low-level language (e.g., assembly language or microcode) is allowed if essential to the performance of the module or when a high-level language is not available.

Required Vendor Information

VE10.12.01: 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

TE10.12.01: The tester shall examine the source code for each of the software and/or firmware components to determine which ones are written in a low-level language. The tester must verify that there are no software and/or firmware components written in a low-level language that were not identified by the vendor in VE10.12.01.

AS10.13: (Levels 3 and 4) All hardware components within the cryptographic module shall be implemented using a high-level specification language.

Required Vendor Information

VE10.13.01: The vendor shall supply documentation on the hardware components that are implemented using a high-level specification language.

Required Test Procedures

TE10.13.01: The tester shall review the vendor documentation to verify that the information specified in VE10.13.01 is included. If this information is not included, then this assertion fails.

AS10.14: (Level 4) In addition to the requirements for Security Levels 1, 2, and 3, the following requirements shall apply to cryptographic modules for Security Level 4.

Note: This assertion is tested as part of AS10.15 through AS10.20.

AS10.15: (Level 4) Documentation shall specify a formal model that describes the rules and characteristics of the cryptographic module security policy.

Required Vendor Information

VE10.15.01: The vendor shall provide a formal model documented in a formal specification language of the security policy of the cryptographic module. The formal model shall include, at a minimum, a list of elements of the model, the operations performed on these elements, and the security rules these operations must obey.

Required Test Procedures

TE10.15.01: The tester shall analyze the formal model to verify that:

1. The statements of the formal model are written correctly in the vendor's chosen formal specification language.

2. The formal model contains:

    a) a definition of a secure state,

    b) a representation of the initial state of the module,

    c) a model of the way in which the module progresses from one state to another (i.e., state transitions).

Note: Additional guidelines on clarity of presentation for security models may be found in Section 2.4 of NCSC-TG-10, *A Guide to Understanding Security Modeling in Trusted Systems*, National Computer Security Center, October 1992.

AS10.16: (Level 4) The formal model shall be specified using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory.

Note: This assertion is tested as part of AS10.15.

AS10.17: (Level 4) Documentation shall specify a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module security policy.

Required Vendor Information

VE10.17.01: The vendor documentation shall describe how the formal model corresponds to the security policy (rules of operation) of the cryptographic module.

VE10.17.02: The model shall include a rationale that demonstrates that it is consistent and complete with respect to all the policies that can be modeled.

Required Test Procedures

TE10.17.01: The tester shall review the vendor provided documentation (security policy, formal model, and the security-policy-to-formal-model correspondence documentation) for completeness and correctness in representing the rules specified in the security policy of the cryptographic module.

AS10.18: (Level 4) Documentation shall specify an informal proof of the correspondence between the formal model and the functional specification.

Required Vendor Information

VE10.18.01: The vendor shall provide an informal proof of the correspondence between the formal model and the functional specification.

Required Test Procedures

TE10.18.01: The tester shall review the informal proof to verify that the information specified in VE10.18.01 is included. If this information is not included, then this assertion fails.

AS10.19: (Level 4) For each cryptographic module hardware, software, and firmware component, the source code shall be annotated with comments that specify (1) the preconditions required upon entry into the module component, function, or procedure in order to execute correctly and (2) the postconditions expected to be true when execution of the module component, function, or procedure is complete.

Required Vendor Information

VE10.19.01: The source code listings for all hardware, software, and firmware components, shall include as comments, pre- and post-conditions as required in AS10.19.

Required Test Procedures

TE10.19.01: The tester shall review the source code listings to verify that the information specified in VE10.19.01 is included. If this information is not included, then this assertion fails.

AS10.20: (Level 4) Documentation shall specify an informal proof of the correspondence between the design of the cryptographic module (as reflected by the precondition and postcondition annotations) and the functional specification.

Required Vendor Information

VE10.20.01: The vendor documentation shall include an informal proof of the correspondence between the design of the cryptographic module and the functional specification.

Required Test Procedures

TE10.20.01: The tester shall review the informal proof to verify that the information specified in VE10.20.01 is included. If this information is not included, then this assertion fails.

10.4 Guidance Documents

AS10.21: (Levels 1, 2, 3, and 4) Crypto officer 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.

Note: This assertion is tested as part of AS10.23.

AS10.22: (Levels 1, 2, 3, and 4) Crypto officer guidance shall specify procedures on how to administer the cryptographic module in a secure manner.

Note: This assertion is tested as part of AS10.23.

AS10.23: (Levels 1, 2, 3, and 4) Crypto officer guidance shall specify assumptions regarding user behavior that is relevant to the secure operation of the cryptographic module.

Required Vendor Information

VE10.23.01: The vendor documentation shall include the information listed in AS10.21, AS10.22 and AS10.23.

VE10.23.02: The crypto officer nonproprietary guidance shall be available to the crypto officer.

Required Test Procedures

TE10.23.01: The tester shall verify that the information specified in VE10.23.01 and VE10.23.02 are included. If this information is not included, then this assertion fails.

AS10.24: (Levels 1, 2, 3, and 4) User guidance shall specify the Approved security functions, physical ports, and logical interfaces available to the users of the cryptographic module

Note: This assertion is tested as part of AS10.25.

AS10.25: (Levels 1, 2, 3, and 4) User guidance shall specify all user responsibilities necessary for the secure operation of the cryptographic module.

Required Vendor Information

VE10.25.01: The vendor documentation shall include the information listed in AS10.24 and AS10.25.

VE10.25.02: The user nonproprietary guidance shall be available to the user.

Required Test Procedures

TE10.25.01: The tester shall verify that the information specified in VE10.25.01 and VE10.25.02 are included. If this information is not included, then this assertion fails.

11. MITIGATION OF OTHER ATTACKS

AS11.01: (Levels 1, 2, 3, and 4) If the cryptographic module is designed to mitigate one or more specific attacks, then the module's security policy shall specify the security mechanisms employed by the module to mitigate the attack(s).

Required Vendor Information

VE11.01.01: The vendor provided nonproprietary security policy shall specify whether the cryptographic module is designed to mitigate specific attacks. The vendor shall specify in the nonproprietary security policy the security mechanism(s) implemented by the cryptographic module to mitigate the attack(s).

VE11.01.02: The vendor provided nonproprietary security policy shall indicate how the implemented mechanism(s) were shown to mitigate the attack(s).

Required Test Procedures

TE11.01.01: The tester shall verify that the vendor provided nonproprietary security policy specifies the mechanism(s) implemented to mitigate the attack(s).

TE11.01.02: The tester shall verify that the vendor provided nonproprietary security policy indicates how the implemented mechanism(s) were shown to mitigate the attack(s).

APPENDIX A: SUMMARY OF DOCUMENTATION REQUIREMENTS

AS12.01: (Levels 1, 2, 3, and 4) All documentation shall be provided to the validation facility by the vendor of a cryptographic module.

Note: This assertion is not separately tested.

APPENDIX B: RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES

Note: There are no requirements for this section.

APPENDIX C: CRYPTOGRAPHIC MODULE SECURITY POLICY

AS14.01: (Levels 1, 2, 3, and 4) The cryptographic module security policy shall be included in the documentation provided by the vendor.

Required Vendor Information

VE14.01.01: A diagram or image of the physical cryptographic module (if appropriate) shall be included in the security policy. The image may be used to indicate the security relevant features of the cryptographic module (e.g., tamper evidence, status indicator(s), user interface(s), power connection(s), etc).

Required Test Procedures

TE14.01.01: The tester shall verify that the diagram or image is representational of the cryptographic module tested.

C.1 Definition of Cryptographic Module Security Policy

AS14.02: (Levels 1, 2, 3, and 4) The cryptographic module security policy shall consist of: a specification of the security rules, under which the cryptographic module shall operate, including the security rules derived from the requirements of the standard and the additional security rules imposed by the vendor.

Note: This assertion is tested as part of AS14.05-AS14.09.

AS14.03: (Levels 1, 2, 3, and 4) The specification shall be sufficiently detailed to answer the following questions:

- **What access does operator X, performing service Y while in role Z, have to security-relevant data item W for every role, service, and security-relevant data item contained in the cryptographic module?**
- **What physical mechanisms are implemented to protect the cryptographic module and what actions are required to ensure that the physical security of the module is maintained?**
- **What security mechanisms are implemented in the cryptographic module to mitigate against attacks for which testable requirements are not defined in the standard?**

Note: This assertion is tested as part of AS14.05-AS14.09.

C.2 Purpose of Cryptographic Module Security Policy

Note: This assertion is not separately tested.

C.3 Specification of the cryptographic Module Security Policy

AS14.04: (Levels 1, 2, 3, and 4) The cryptographic module security policy shall be expressed in terms of roles, services, and cryptographic keys and CSPs. At a minimum, the following shall be specified:

- **an identification and authentication (I&A) policy,**
- **an access control policy,**

- **a physical security policy, and**

- **a security policy for mitigation of other attacks.**

Note: This assertion is tested as part of AS14.05-AS14.09.

C.3.1 Identification and Authentication Policy

AS14.05: (Levels 1, 2, 3, and 4) The cryptographic module security policy shall specify an identification and authentication policy, including

- **all roles (e.g., user, crypto officer, and maintenance) and associated type of authentication (e.g., identity-based, role-based, or none) and**

- **the authentication data required of each role or operator (e.g., password or biometric data) and the corresponding strength of the authentication mechanism.**

Required Vendor Information

VE14.05.01: The vendor shall specify all roles that may be assumed by an operator of the cryptographic module. This list shall include the User Role and the Crypto Officer Role (see AS03.03). If the cryptographic module allows for maintenance, the list shall include a Maintenance Role (see AS03.04). All other authorized roles shall be specified (see AS03.06).

VE14.05.02: For Security Levels 2, 3, and 4, the vendor shall specify whether the type of authentication is identity-based or role-based for each of the roles listed in VE14.05.01. The vendor shall specify the authentication data required for each role (see AS03.17, AS03.19 and AS03.23). The vendor shall specify the strength of corresponding authentication mechanisms (see AS03.24, AS03.25, and AS03.28).

VE14.05.03: The vendor shall utilize the tabular formats specified in Appendix C of FIPS PUB 140-2.

Required Test Procedures

TE14.05.01: The tester shall check the security policy to ensure that all authorized roles are specified and are consistent with the information required by assertions AS03.03, AS03.04 and AS03.06.

TE14.05.02: The tester shall verify that the type of authentication is specified for each role, the required authentication data is specified for each role, and the strength of all corresponding authentication mechanisms implemented by the module. The tester shall ensure that this information is consistent with the information required by assertions AS03.17, AS03.19, AS03.23, AS03.24, AS03.25, and AS03.28.

C.3.2 Access Control Policy

AS14.06: (Levels 1, 2, 3, and 4) The cryptographic module shall specify an access control policy. The specification shall be of sufficient detail to identify the cryptographic keys and CSPs the operator has access to while performing a service, and the type(s) of access the operator has to these parameters.

Note: This assertion is not separately tested.

AS14.07: (Levels 1, 2, 3, and 4) The security policy shall specify:

- **all roles supported by the cryptographic module,**

- **all services provided by the cryptographic module,**

- **all cryptographic keys and CSPs employed by the cryptographic module, including**
    - **secret, private, and public cryptographic keys (both plaintext and encrypted),**
    - **authentication data such as passwords or PINs, and**
    - **other security-relevant information (e.g., audited events and audit data),**
- **for each role, the services an operator is authorized to perform within that role, and**
- **for each service within each role, the type(s) of access to the cryptographic keys and CSPs.**

Required Vendor Information

VE14.07.01: The vendor shall specify all services that are provided to an authorized role. This list must include the Show Status Service and all Self-Test Services (see AS03.11). All other authorized roles shall be specified (see AS03.06).

VE14.07.02: For each provided service within each authorized role, the vendor shall specify the allowed type(s) of access to security-related information, including secret and private cryptographic keys (both plaintext and encrypted), authentication data CSPs, and other protected information (see AS01.15).

VE14.07.03: The vendor shall utilize the tabular format specified in Appendix C in FIPS PUB 140-2.

Required Test Procedures

TE14.07.01: The tester shall verify the security policy to ensure that the services provided to each role are specified (VE14.07.01), consistent with the information required by assertion AS03.14.

TE14.07.02: The tester shall verify the security policy to ensure that it specifies the authorized type of access, allowed by services within roles, to all security-relevant information (VE14.07.01). The tester shall verify that the information is consistent with the requirements of assertion AS03.14.

C.3.3 Physical Security Policy

AS14.08: (Levels 1, 2, 3, and 4) The cryptographic module security policy shall specify a physical security policy, including:

- **the physical security mechanisms that are implemented in the cryptographic module (e.g., tamper-evident seals, locks, tamper response and zeroization switches, and alarms) and**
- **the actions required by the operator(s) to ensure that physical security is maintained (e.g., periodic inspection of tamper-evident seals and zeroization switches).**

Required Vendor Information

VE14.08.01: The vendor shall specify the physical security mechanisms that are implemented in the cryptographic module.

VE14.08.02: The vendor shall specify the actions required by the operator(s) to ensure that physical security is maintained.

Required Test Procedures

TE14.08.01: The tester shall verify the security policy to ensure that the security mechanisms that are implemented are consistent with information required by assertion AS05.01.

C.3.4 Mitigation of Other Attacks Policy

AS14.09: (Levels 1, 2, 3, and 4) The cryptographic module security policy shall specify a security policy for mitigation of other attacks, including the security mechanisms implemented to mitigate the attacks.

Required Vendor Information

VE14.09.01: The vendor shall specify the security mechanisms of the cryptographic module that are designed to mitigate specific attacks. This specification shall indicate how the implemented mechanism(s) were shown to mitigate the attack(s) and shall describe any limitations of these mechanisms (i.e., specific conditions or circumstances under which the mechanisms are known to be ineffective).

VE14.09.02: The vendor shall utilize the tabular format specified in Appendix C in FIPS PUB 140-2.

Required Test Procedures

TE14.09.01: The tester shall verify that the security policy specifies the mechanism(s) employed in the specific attacks, describes how the implemented mechanism(s) were shown to mitigate the attack(s), and lists any known limitations.

CHANGE NOTICES

DTR Change Notice 1 – 02/12/2003

Change Notice 2 to FIPS 140-2 required changes to the Derived Test Requirements for FIPS 140-2. The changes affect the following assertions:

a. AS07.05, AS09.14, AS09.15 and AS09.28 no longer have requirements.

b. AS07.06 and AS09.16 have their requirements changed.

c. AS09.07 has a minor change in the description of a tester requirement (TE).

AS07.05: ~~**(Levels 1, 2, 3, and 4) Depending on the security level, the data output from an Approved RNG shall pass all statistical tests for randomness as specified in Section 4.9.1.**~~

Note: ~~This assertion is tested in AS09.28.~~ There are no requirements for this assertion number.

AS07.06: (Levels 1, 2, 3, and 4) Approved ~~**deterministic**~~ **RNGs shall be subject to the cryptographic algorithm test in Section 4.9.1.**

Note: ~~This assertion is not separately tested.~~ This assertion is tested in AS09.13

AS09.07: (Levels 1, 2, 3, and 4) Documentation shall specify:

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

Required Vendor Information

VE09.07.01: The vendor shall provide a list of all self-tests that the module can perform. This list shall include both power-up tests and conditional tests.

VE09.07.02: For each error condition, the vendor documentation shall provide the condition name, the events that can produce the condition, and the actions necessary to clear the condition and resume normal operation.

Required Test Procedures

TE09.07.01: The tester shall inspect the list of self-tests to verify that it includes the following:

3. Power-up tests

- Cryptographic algorithm test
- Random number generator test
- Software/firmware test
- Critical functions test
- ~~Statistical random number generator tests (required at Security Levels 3 and 4)~~
- Other self-tests that are performed at power-up and on demand

4. Conditional tests

   - Pairwise consistency test (if the module generates public and private keys)
   - Software/firmware load test
   - Manual key entry test
   - Continuous random number generator test
   - Bypass test
   - Other conditional tests

TE09.07.02: The tester shall check that the information provided above is specified for each error condition.

TE09.07.03: 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 review the code listing and or design documentation to determine whether the actions necessary to clear each error condition are consistent with the descriptions in the vendor documentation.

~~**Random number generator test**~~

AS09.14: ~~**(Level 3 and 4) In addition to the tests specified for Security Levels 1 and 2, the cryptographic module shall perform all of the statistical random number tests on demand by the operator and may perform the tests when the module is powered up.**~~

Note: There are no requirements for this assertion number.

~~**Required Vendor Information**~~

~~VE09.14.01: See VE09.07.01 for the vendor requirement.~~

~~VE09.14.02: In addition, the vendor shall describe the procedure by which an operator can initiate the statistical random number generator tests on demand.~~

~~**Required Test Procedures**~~

~~TE09.14.01: Verification of the documented list of power-up self-tests is performed under TE09.07.01.~~

~~TE09.14.02: In addition, the tester shall inspect the vendor documentation to verify that initiation of the statistical random number generator tests on demand is specified. The documentation shall also include what steps an operator must take in order to initiate the self-tests.~~

~~TE09.14.03: To test that the necessary steps to initiate the statistical random number generator tests (e.g., the actual command that the operator must send to the module) are consistent with that specified in the vendor documentation, the tester shall command the module to perform the statistical random number generator tests.~~

~~TE09.14.04: Verification that the module performs the self-tests as documented is done under validation requirements for AS09.28.~~

AS09.15: ~~(Level 4) In addition to the tests specified for Security Levels 1 through 3, the cryptographic module shall also perform all of the statistical random number generator tests when the module is powered up.~~

Note: There are no requirements for this assertion number.

~~**Required Vendor Information**~~

~~VE09.15.01: See VE09.07.01 for the vendor requirement.~~

~~**Required Test Procedures**~~

~~TE09.15.01: Verification of the documented list of power-up self-tests was performed under TE09.07.01.~~

~~TE09.15.02: Verification that the module performs the self-tests as documented is done under validation requirements for AS09.28.~~

Cryptographic algorithm test

AS09.16: (Levels 1, 2, 3, and 4) A cryptographic algorithm test using a known answer shall be conducted for all ~~modes~~ cryptographic functions (e.g., encryption, decryption, ~~and~~ authentication, and random number generation) of each Approved cryptographic algorithm implemented by the cryptographic module.

Required Vendor Information

VE09.16.01: See VE09.07.01 for the vendor requirement.

Required Test Procedures

TE09.16.01: By inspecting the vendor documentation, the tester shall verify that a known answer test is associated with all ~~modes~~ cryptographic functions of each Approved cryptographic algorithm implemented by the cryptographic module as indicated in AS01.12.

TE09.16.02: The tester shall verify that the documentation is consistent with the implementation of the cryptographic module.

~~**Statistical Random Number Generator Tests**~~

AS09.28: ~~(Levels 1, 2, 3 and 4) If statistical random number generator tests are required (i.e., depending on the security level), the cryptographic module employing RNGs shall perform the following statistical tests for randomness. A single bit stream of 20,000 consecutive bits of output from each RNG shall be subjected to the following four tests: monobit test, poker test, runs test, and long runs test.~~

Note: There are no requirements for this assertion number.

~~**Required Vendor Information**~~

~~VE09.28.01: At levels 3 and 4, if the cryptographic module implements a random number generator, the vendor documentation shall specify statistical tests for randomness. The following tests are specified in Section 9.1 of FIPS PUB 140-2:~~

~~1. Monobit Test~~

~~2. Poker Test~~

~~3. Runs Test~~

~~4. Long Run Test~~

~~**Required Test Procedures**~~

~~TE09.28.01: At all levels, the tester shall test the random number generator using all of the statistical and continuous random number generator tests specified in section 4.9.1 of FIPS PUB 140-2.~~

~~TE09.28.02: At levels 3 and 4, if the module implements a random number generator, the tester shall check the vendor documentation to verify that statistical tests for randomness are specified.~~

~~TE09.28.03: At levels 3 and 4, the tester shall determine from the vendor documentation whether the module implements the statistical tests specified in Section 4.9.1 of FIPS PUB 140-2. If so, the tester shall review the specification of the statistical tests in the code and/or design documentation to determine whether they have been implemented as specified in FIPS PUB 140-2 and that the module enters an error state if any of the tests fail.~~

DTR Change Notice 2 – 02/12/2003

Change Notice 3 to FIPS 140-2 required changes to the Derived Test Requirements for FIPS 140-2. The changes affect the following assertions:

a. AS09.30 had reference removed in the Note.

b. AS09.31 has its requirements changed.

c. AS09.32 no longer has requirements.

Pair-wise consistency test (for public and private keys).

AS09.30: (Levels 1, 2, 3, and 4) If the cryptographic module generates public or private keys, then the following pair-wise consistency tests for public and private keys shall be performed.

Note: This assertion is tested as part of AS09.31~~, AS09.32,~~ and AS09.33.

AS09.31: (Levels 1, 2, 3, and 4) If the keys are used to perform an approved key transport method ~~or encryption~~, then the public key shall encrypt a plaintext value. The resulting ciphertext value shall be compared to the original plaintext value. If the two values are equal, then the test shall fail. If the two values differ, then the private key shall be used to decrypt the ciphertext and the resulting value shall be compared to the original plaintext value. If the two values are not equal, the test shall fail.

Required Vendor Information

VE09.31.01: If public and private keys are to be used to perform an approved key transport method ~~or encryption~~, the cryptographic module shall test for pairwise consistency by applying the public key to a

plaintext value. 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 and the result shall be compared to the original plaintext.
- If the two values are not equal, then the test shall fail.

Required Test Procedures

TE09.31.01: If public and private keys are to be used to perform an approved key transport method ~~or encryption~~, the tester shall verify that the implementation of the pairwise consistency check, as defined in AS09.31, is consistent with the vendor documentation by checking the code and/or design documentation.

AS09.32: ~~(Levels 1, 2, 3, and 4) If the keys are used to perform key agreement, then the cryptographic module shall create a second, compatible key pair. The cryptographic module shall perform both sides of the key agreement algorithm and shall compare the resulting shared values. If the shared values are not equal, the test shall fail.~~

Note: There are no requirements for this assertion number.

~~**Required Vendor Information**~~

~~VE09.32.01: If the public and private keys are to be used to perform key agreement, then the cryptographic module shall implement a pairwise consistency test where the cryptographic module shall create a second, compatible key pair. The module shall perform both sides of the key agreement algorithm and shall verify that the resulting secret keys are the same. If the secret keys are not the same, the test shall fail.~~

~~**Required Test Procedures**~~

~~TE09.32.01: If the public and private keys are used to perform key agreement, the tester shall verify that the implementation as defined in AS09.32 is consistent with the vendor documentation by checking the code and/or design documentation.~~

DTR Change Notice 3 – 03/02/2004

Following are corrections to the FIPS 140-2 DTR.

AS02.05: (Levels 1, 2, 3, and 4) All data (except status data output via the status output interface) that is output from the cryptographic module (including plaintext data, ciphertext data, cryptographic keys and CSPs, authentication data, and control information for another module) shall exit via the "data output" interface.

TE02.05.02: The tester shall verify if vendor documentation specifies any external output devices to be used with the cryptographic module for the output of data from the data ~~input~~ output interface, such as smart cards, tokens, displays, and/or other storage devices. The tester shall output data from the data output interface using the identified external output device(s), and verify that output of data using the external output device functions as specified.

AS02.06: (Levels 1, 2, 3, and 4) All data output via the data output interface shall be inhibited when an error state exists and during self-tests.

TE02.06.01: The tester shall verify that vendor documentation specifies that all data output via the data output interface is inhibited whenever the cryptographic module is in an error state. The tester shall verify from vendor documentation that once an error condition is detected and the error state is entered, all data output via the data output interface is inhibited, until error recovery occurs. Status information to identify the type of error may be allowed from the status output interface, as long as the tester can verify that no CSPs, plaintext data, or other information that if misused could lead to a compromise. The tester shall also verify that the error states specified in response to this assertion are identical to the error states specified under ~~AS04.06~~ AS04.05.

AS02.11: (Levels 1, 2, 3, and 4) All input data entering the cryptographic module via the "data input" interface shall only pass through the input data path.

TE02.11.02: The tester shall verify from 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 ~~comprise~~ compromise of CSPs, plaintext data, or other information.

AS04.05: (Levels 1, 2, 3, and 4) Documentation shall include a representation of the finite state (or equivalent) using a state transition diagram and/or state transition table that shall specify:

- **all operational and error states of the cryptographic module,**
- **the corresponding transitions from one state to another,**
- **the input events, including data inputs and control ~~outputs~~ inputs, that cause transitions from one state to another, and**
- **the output events, including internal module conditions, data outputs, and status outputs resulting from transitions from one state to another.**

AS05.44: (Multiple Chip Embedded – Level 4) Upon the detection of tampering, the tamper response and zeroization circuitry shall immediately zeroize all plaintext secret and private cryptographic keys and CSPs.

Required Test Procedures

TE05.44.01: The tester shall verify from vendor documentation that the module contains tamper response and zeroization 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 zeroizes all plaintext secret and private keys and other unprotected CSPs.

~~**Note:** This test can be verified in one or more of the following manners:~~

~~4. Tester perform tests at the tester's facility~~
~~5. Tester perform tests at vendor facility~~
~~6. Tester supervises vendor performing tests at vendor facility~~
   - ~~Rationale must be included that explains why tester could not perform the tests~~
   - ~~Tester must develop the required test plan and required tests~~
   - ~~Tester must directly observe the tests being performed~~

TE05.44.02: The tester shall breach the tamper detection envelope barrier and then verify that the module zeroizes all plaintext secret and private keys and other unprotected CSPs.

Note: This test can be verified in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

AS05.58: (Multiple-Chip Standalone – Level 4) The tamper response and zeroization circuitry shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroize all plaintext secret and private cryptographic keys and CSPs.

Required Test Procedures

TE05.58.01: The tester shall verify from vendor documentation that the module contains tamper response and zeroization 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 zeroizes all plaintext secret and private keys and other unprotected CSPs.

~~**Note:** This test can be verified in one or more of the following manners:~~

~~4. Tester perform tests at the tester's facility~~
~~5. Tester perform tests at vendor facility~~
~~6. Tester supervises vendor performing tests at vendor facility~~
   - ~~Rationale must be included that explains why tester could not perform the tests~~
   - ~~Tester must develop the required test plan and required tests~~
   - ~~Tester must directly observe the tests being performed~~

TE05.58.02: The tester shall breach the tamper detection envelope barrier and then verify that the module zeroizes all plaintext secret and private keys and other unprotected CSPs.

Note: This test can be verified in one or more of the following manners:

1. Tester perform tests at the tester's facility
2. Tester perform tests at vendor facility
3. Tester supervises vendor performing tests at vendor facility
   - Rationale must be included that explains why tester could not perform the tests
   - Tester must develop the required test plan and required tests
   - Tester must directly observe the tests being performed

AS06.20: (Level~~s~~ 3 ~~and 4~~) In addition to the applicable requirements for Security Levels 1 and 2, the following requirements shall apply for Security Level 3.

Note: This assertion is tested as part of AS06.21 through AS06.25.

AS06.21: (Level~~s~~ 3 ~~and 4~~) All cryptographic software and firmware, cryptographic keys and CSPs, and control and status information shall be under the control of

- **an operating system that meets the functional requirements specified in the Protection Profiles listed in Annex B. The operating system shall be evaluated at the CC evaluation assurance level EAL3 and include the following additional requirements: Trusted_Path**

(FTP_TRP.1) and Informal TOE Security Policy Model (ADV_SPM.1), or

- **an equivalent evaluated trusted operating system.**

AS07.29: (Levels 1, 2, 3 and 4) For Security Levels 1 and 2, secret and private keys established using automated methods shall be entered into and output from ~~the~~ a cryptographic module in encrypted form.

Required Vendor Information
VE07.29.01: The vendor documentation shall specify keys that are established using automated methods. The vendor documentation shall state whether these keys are entered into and output in encrypted form.

Required Test Procedures
TE07.29.01: The tester shall verify that the vendor has provided documentation asserting that secret and private keys established using automated methods are entered into and output from the cryptographic module in encrypted form.
TE07.29.02: If automated means are used to establish secret and private keys, the tester shall verify that these keys are entered into and output from the cryptographic module in encrypted form.

AS07.30: (Levels 3 and 4) Secret and private keys established using automated methods shall be entered into and output from ~~the~~ a cryptographic module in encrypted form.

Note: This assertion is tested as part of AS07.29.

AS09.11: (Levels 1, 2, 3, and 4) All data output via the output interface shall be inhibited when the tests are performed.

Note: This assertion is tested as part of ~~AS06.02~~ AS02.06.

AS10.04: (Levels 2, 3, and 4) In addition to the requirements of Security Level 1, documentation shall specify the procedures required for maintaining security while distributing and delivering versions of the cryptographic module to authorized operators.

Required Test Procedures
TE10.04.01: The tester shall review the vendor provided documentation to verify that procedures required for maintaining security while distributing and delivering versions of the cryptographic module to authorized ~~operations~~ operators are correct.

AS11.01: (Levels 1, 2, 3, and 4) If the cryptographic module is designed to mitigate one or more specific attacks, then the module's security policy shall specify the security mechanisms employed by the module to mitigate the attack(s).

Required Test Procedures
TE11.01.01: The tester shall verify that the vendor provided nonproprietary security policy specifies the mechanism(s) implemented to ~~migigate~~ mitigate the attack(s).

AS14.01: (Levels 1, 2, 3, and 4) The cryptographic module security policy shall be included in the documentation provided by the vendor.

Required Vendor Information

VE14.01.01: A diagram or image of the physical cryptographic module (if appropriate) shall be included in the security policy. The image may be used to indicate the security relevant features of the cryptographic module (e.g., tamper evidence, status indicator(s), user interface(s), power connection(s), etc).

Required Test Procedures

TE14.01.01: The tester shall verify that the diagram or image is representational of the cryptographic module tested.

DTR Change Notice 4 – 03/23/2004

Following are corrections to the FIPS 140-2 DTR.

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

TE03.11.03: Verification that the module provides for the initiation of the running of power-up self-tests, as specified in Section 4.9, is performed under ~~TE03.15.02~~ TE03.14.02.

DTR Change Notice 5 – 03/24/2004

Following are corrections to the FIPS 140-2 DTR.

AS06.05: (Level 1 Only) The cryptographic module shall prevent access by other processes to plaintext private and secret keys, CSPs, and intermediate key generation values during the time the cryptographic module is executing/operational. Processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.

DTR Change Notice 6 – 01/04/2011

Following are updates to the FIPS 140-2 DTR.

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

~~**Note:** This assertion is not separately tested.~~

Required Vendor Information - Firmware Module (Level 1 only)

VE05.01.01: The vendor shall provide a description of the mechanism used to ensure that no other process can access private and secret keys, intermediate key generation values, and other CSPs, while the cryptographic process is in use.

VE05.01.02: The vendor shall provide a description of the mechanism used to ensure that no other process can interrupt the cryptographic module during execution.

VE05.01.03: The vendor shall provide a list of the cryptographic firmware that are stored on the cryptographic module and shall provide a description of the protection mechanisms used to prevent unauthorized disclosure and modification.

Required Test Procedures – Firmware Module (Level 1 only)

TE05.01.01: The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are executing, the same or another tester shall attempt to access secret and private keys, intermediate key generation values, and other CSPs.

TE05.01.02: The tester shall perform cryptographic functions as described in the crypto officer and user guidance documentation. While the cryptographic functions are operating, the same or another tester shall attempt to execute another process.

TE05.01.03: The tester shall attempt to perform unauthorized accesses and unauthorized modifications to software and firmware source and executable code.

DTR Change Notice 7 – 01/04/2011

Following are updates to the FIPS 140-2 DTR.

AS07.41: (Levels 1, 2, 3, and 4) The cryptographic module shall provide methods to zeroize all plaintext secret and private cryptographic keys and CSPs within the module.

TE07.41.03: The tester shall initiate zeroization and verify the key destruction method is performed in a time that ~~is not sufficient to compromise~~ an attacker cannot access plaintext secret and private cryptographic keys and other unprotected CSPs~~.~~ while under the direct control of the operator of the module (i.e. present to observe the method has completed successfully or controlled via a remote management session). If the method is not under the direct control of the operator, then rationale shall be provided on how the zeroization method(s) are employed such that the secret and private cryptographic keys and other CSPs within the module cannot be obtained by an attacker.

DTR Change Notice 8 – 01/04/2011

Following are updates to the FIPS 140-2 DTR.

AS01.12: (Levels 1, 2, 3, and 4) Documentation shall list all security functions, both Approved and non-Approved, that are employed by the cryptographic module and shall specify all modes of operation, both Approved and non-Approved.

Required Vendor Information

VE01.12.03: The vendor shall provide a list of all vendor affirmed security methods.

VE01.12.04: The vendor provided nonproprietary security policy shall include reference to all vendor affirmed security methods.

Required Test Procedures

TE01.12.03: The tester shall verify that the vendor has provided the list of vendor affirmed security methods as described above.

TE01.12.04: The tester shall verify that the vendor provided documentation specifies how the implemented vendor affirmed security methods conform to the relevant standards.

End of Document