National Institute of Standards and
Technology

Derived Test Requirements for FIPS PUB 140-1, *Security Requirements for Cryptographic Modules*

March 1995
Final

William N. Havener
Roberta J. Medlock
Lisa D. Mitchell
Robert J. Walcott

INTRODUCTION

Federal Information Processing Standards Publication (FIPS PUB) 140-1, *Security Requirements for Cryptographic Modules*, specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting unclassified 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 a cryptographic module. These areas include the following:

1. Cryptographic Module Design and Documentation
2. Module Interfaces
3. Roles and Services
4. Finite State Machine Model
5. Physical Security
6. Software Security
7. Operating System Security
8. Cryptographic Key Management
9. Cryptographic Algorithms
10. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
11. Self Tests

The National Institute of Standards and Technology (NIST) intends to establish a FIPS 140-1 validation program using the National Laboratory Accreditation Program (NVLAP) to accredit laboratories to perform testing of cryptographic modules for conformance to FIPS 140-1. Under the proposed process, NIST would issue validation certificates based on test reports produced by NVLAP-accredited laboratories. Organizations wishing to have validations performed would contract with the laboratories for the required services.

Purpose

The purpose of this document is to describe the methods that will be used by accredited laboratories to test whether a cryptographic module conforms to the requirements of FIPS 140-1. 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 140-1 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 140-1 requirements. This document may be used by vendors as a guide in trying to determine if their cryptographic modules meet the security requirements of FIPS 140-1 before they apply to the laboratory for testing.

Document Organization

This document includes eleven sections, corresponding to the eleven areas of security requirements of FIPS 140-1.

Within each section, the corresponding security requirements from FIPS 140-1 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 either direct quotations from FIPS 140-1, or are directly derivable from these requirements. 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 140-1 (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 are 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 are 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.

1. CRYPTOGRAPHIC MODULES

AS01.01: Documentation shall completely identify all hardware, software, and firmware components of the cryptographic module. (1, 2, 3, and 4)

Required Vendor Information

VE01.01.01: All components that implement cryptographic logic or processes 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 used in the module

VE01.01.02: The above list of components shall be consistent with the information provided for all other assertions of this section.

Required Test Procedures

TE01.01.01: The tester shall verify that the documentation includes a master components list that is stated to include all hardware, software, and firmware components of the cryptographic module.

TE01.01.02: 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] or electrically erasable PROM [EEPROM])

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, 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 cryptographic module

11. Software modules, defined as executable code or data that could be changed in the future or is readily accessible to programmers

12. Firmware modules, defined as executable code or data that is unlikely to be changed (e.g., because it performs a standardized fixed function) and is not readily accessible to programmers

13. Other component types used in the module

TE01.01.03: 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 AS01.02: 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

AS01.03: 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 AS01.03.

3. The specification of the physical configuration under assertion AS01.04: 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 AS01.04.

4. The specification of the block diagram under assertion AS01.05: Verify that any individual components called out in the block diagram (e.g., processors, application-specific integrated circuits, and large memory units) are also listed in the master components list.

5. Any components which are to be excluded from the requirements of FIPS PUB 140-1 under the provisions of assertion AS01.06: Verify that components to be so excluded are still listed in the master components list.

AS01.02: Documentation shall completely specify the module's cryptographic boundary surrounding the components. (1, 2, 3, and 4)

Required Vendor Information

VE01.02.01: 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 perimeter definition shall define module components and connections (ports), and also module information flows, processing, and input/output signals.

VE01.02.02: 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.

Required Test Procedures

TE01.02.01: 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 signals that are input and output to the exterior of the cryptographic boundary. Alternatively, a detailed functional block diagram showing the cryptographic boundary may be used to meet some or all of the above requirements for perimeter definition, as long as there is sufficient detail to provide the information

required above. (Annotations on component lists or block diagrams provided for other purposes may also be used, if the cryptographic boundary is clearly identified.)

TE01.02.02: The tester shall verify that the vendor-provided documentation includes sufficient detail for components at the cryptographic boundary to precisely define the cryptographic boundary.

TE01.02.03: The tester shall verify that the cryptographic boundary is physically contiguous. This means that there must be 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 140-1.) The module design must also ensure that there are no uncontrolled interfaces into or out of the cryptographic module that could pass sensitive information.

TE01.02.04: The tester shall verify that the cryptographic boundary encompasses all components that are identified in the block diagram under assertion AS01.05 in this section as inputting, outputting, or processing plaintext, keys, authorization data, or other information that if misused or malfunctioned could lead to a compromise.

TE01.02.05: As a partial exception to the above requirements, the vendor is allowed to exclude certain components from the requirements of FIPS PUB 140-1 after satisfying the requirements under assertion AS01.06 in this section. The vendor may then treat such excluded components as effectively outside the cryptographic boundary of the module, in the sense that they will not be further analyzed. In that case, the tester shall verify that any interfaces or physical connections between such excluded components and the rest of the module cannot allow uncontrolled release of sensitive information outside the module.

AS01.03: If the cryptographic module contains software or firmware, the cryptographic boundary shall be defined such that it contains any processor which executes the code. (1, 2, 3, and 4)

Required Vendor Information

VE01.03.01: For each processor in the module, the vendor shall identify, by major function, the software or firmware that are executed by the processor, and the memory devices that contain the executable code and data.

VE01.03.02: For each processor, the vendor shall identify any hardware with which it interfaces.

Required Test Procedures

TE01.03.01: The tester shall verify that each processor identified under this assertion is contained in the master components list under assertion AS01.01 and in the cryptographic boundary defined under assertion AS01.02.

TE01.03.02: The tester shall verify that, for each processor, the vendor has identified the software or firmware code modules executed by that processor, the functions performed by that processor and its code, and the memory devices containing the executable code and data.

TE01.03.03: The tester shall verify that, for each processor, the vendor has identified any hardware with which it interfaces. This must include, as applicable, any hardware components that provide input data, control, or status signals to the processor and its software/firmware, and any hardware components that receive output data, control, or status signals from the processor and its software/firmware. Such hardware components may be within the cryptographic module, or may be user equipment outside the module such as input/output devices.

AS01.04: Documentation shall completely describe the physical configuration of the module. (1, 2, 3, and 4)

Required Vendor Information

VE01.04.01: The vendor shall identify which of the three possible physical configurations the module has: single-chip module; multi-chip embedded module; or multi-chip, stand-alone module as defined in Section 4.5 of FIPS PUB 140-1.

VE01.04.02: 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.

VE01.04.03: 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

TE01.04.01: 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 140-1.

TE01.04.02: 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. (These need not be blueprints. The vendor can use his own internal format if desired and if the information is detailed and accurate enough to meet the requirements of this section.)

TE01.04.03: 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.

TE01.04.04: 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 air flow, heat exchanger, cooling fins, fans, or other arrangements for removing heat from the module

AS01.05: Documentation shall include a block diagram depicting all of the major hardware components of the module and their interconnections. (1, 2, 3, and 4)

Required Vendor Information

VE01.05.01: The vendor documentation shall include a functional 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. Any other significant components used

VE01.05.02: The block diagram shall also include any (semi-) custom integrated circuits, such as predesigned cryptographic circuitry, gate arrays, or other programmable logic. Independent functions within such components shall be identified separately in the block diagram.

VE01.05.03: The block diagram shall include the functions of major module components or subassemblies.

VE01.05.04: The block diagram shall show interconnections among major components of the module and between the module and outside equipment.

VE01.05.05: The block diagram shall show the cryptographic boundary of the module.

Required Test Procedures

TE01.05.01: 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 AS01.01 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 for cryptovariables

6. Working memory for processing information

7. Program memory containing executable software or firmware code

8. (Semi-) custom integrated circuits such as predesigned cryptographic circuitry, application-specific integrated circuits, gate arrays, programmable logic arrays, or other programmable logic devices. (These must be specified to the level of independent functions. If more than one function is performed by a given module, the functions shall be shown separately in the block diagram.)

9. Any other significant components used

TE01.05.02: The tester shall verify that the block diagram indicates the major functions performed by the components or subassemblies that are blocks in the diagram. These must include at least plaintext and ciphertext message processing and routing, cryptologic (algorithms and other cryptographic processing), memory buffering and storage, control logic, key handling, zeroization, alarms and protection, and power.

TE01.05.03: 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.

TE01.05.04: The tester shall verify that the block diagram indicates the cryptographic boundary for the cryptographic module, as required under assertion AS01.02 in this section.

AS01.06: Documentation shall indicate any hardware, software, or firmware components of the module that are excluded from the security requirements of the standard and explain why these parts do not effect the security of the module. (1, 2, 3, and 4)

Required Vendor Information

VE01.06.01: All components that are to be excluded from the security requirements shall be explicitly listed in the vendor documentation.

VE01.06.02: The rationale for excluding each of the components listed in response to requirement VE01.06.01 shall be provided in the vendor documentation. The vendor shall show that each such component, even if malfunctioning or misused, cannot cause a compromise under any reasonable conditions.

Required Test Procedures

TE01.06.01: The tester shall determine whether the vendor indicates that any components of the module are to be excluded from the requirements of FIPS PUB 140-1. If none are so listed, all components must meet the other requirements of this and all other sections.

TE01.06.02: If the vendor has indicated that certain components of the module are to be excluded from the requirements of FIPS PUB 140-1, the tester shall determine that a rationale for the exclusion is provided. The rationale must show that even if the component is misused or malfunctions, it could not cause a compromise via potential release of sensitive information. Some reasons that might be acceptable, if adequately supported by backup information and discussion, include:

1. The component does not process sensitive information and is not connected with sensitive areas of the rest of the module in any way that would allow inappropriate transfer of sensitive information (e.g., structural components or filter power circuitry)

2. 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 (e.g., internal housekeeping timing circuits that are reclocked before use by components that do contact outside equipment such as input/output devices)

3. The component's inputs or outputs are compared against similar redundant information elsewhere in the module that would detect and protect against any malfunction which could otherwise have released sensitive information

The tester shall determine the correctness of any rationale for exclusion such as the above. 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.

AS01.07: Documentation shall completely specify the cryptographic module security policy, i.e., the security rules under which a module must operate. In particular, the security policy shall include the security rules derived from the security requirements of this standard and the security rules derived from any additional security requirements imposed by the manufacturer. (1, 2, 3, and 4)

Required Vendor Information

VE01.07.01: The vendor shall provide a separate document, or section of a document, that specifies the security policy (i.e., the security rules under which a module must operate) enforced by the cryptographic module.

Required Test Procedures

TE01.07.01: The tester shall review the security policy specification provided by the vendor. Specifically, he or she must determine that it identifies all roles, services, and security relevant data items of the cryptographic module, and specifies what access, if any, a user, performing a service within the context of a given role, has to each of the security relevant data items. The specification should be complete, and detailed enough to be able to answer the following question: "What access does operator X, performing service Y while in role Z have to security relevant data item K?" for every role, service, and security relevant data item contained in the cryptographic module.

General: The vendor is encouraged to include, or reference by page number or figure in documentation, any useful supporting information. This could include data sheets, user manuals, results of prior security analyses (in-house or with NSA), etc. Such supporting information would be particularly useful where it helps evaluate the module against specific tester requirements.

2. MODULE INTERFACES

AS02.01: The module shall be designed to restrict all information flow and physical access to the module to logical interfaces that define all entry and exit points to and from the module. The module interfaces shall be logically distinct from each other. (1, 2, 3, and 4)

Required Vendor Information

VE02.01.01: The vendor documentation shall itemize the module information flows and access points by highlighting or annotating copies of the block diagram required in section 1, and providing any other documentation necessary to clearly specify the logical interfaces. For each input to the module or output from the module, the documentation shall specify the logical interface to which the input or output belongs, and the physical entry/exit point. The information provided under this requirement shall be consistent with component information provided for assertions AS01.01, AS01.02, and AS01.05 under section 1.

VE02.01.02: The vendor design shall separate the module interfaces into logically isolated categories using at least the categories defined in assertion AS02.02 and (if applicable) AS02.03 in this section. If two or more interfaces share the same physical port, the vendor shall specify how the information from different interface categories is kept logically separate.

Required Test Procedures

TE02.01.01: The tester shall verify that the vendor documentation includes the following information:

1. A listing or diagram of all logical inputs to the module and outputs from the module

2. A listing of all physical input (entry) and output (exit) ports of the module

3. A mapping from the logical inputs/outputs to the physical input/output ports of the module

4. A highlighted or annotated copy of the block diagram showing the logical input/output interfaces

The tester shall compare the above information with the information provided under assertions AS01.01, AS01.04, and AS01.05 and verify that there are no inconsistencies in the description of components and physical layout for the input/output ports. (Note that separate pins within one connector may be considered separate ports.)

TE02.01.02: The tester shall verify from vendor documentation that the module interfaces are

separate for the categories of interfaces specified in assertions AS02.02 and (if applicable) AS02.03 of this section. In particular, the tester shall verify that the information flows for the input, output, control, and status interfaces are not mingled by merging any of them into the same physical interface signal line at the same time. Note that a module interface may be physically distributed across more than one port, or two or more module interfaces may physically share one port as long as the information flows are kept logically separate. However, if two or more interfaces share the same physical port, the tester shall verify that the vendor describes a workable scheme for keeping separate the information flowing through the interfaces.

AS02.02: The module shall have at least the following four logical interfaces: (1, 2, 3, and 4)

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

Required Vendor Information

VE02.02.01: The module shall have a data input interface that is defined in the vendor documentation, including:

1. Plaintext data
2. Ciphertext data
3. Cryptographic keys
4. Other key management data
5. Authentication data
6. Status information
7. Any other input data

VE02.02.02: The module shall have a data output interface that is defined in the vendor documentation including:

1. Plaintext data
2. Ciphertext data
3. Cryptographic keys
4. Other key management data
5. Authentication data
6. Control information
7. Any other output data

VE02.02.03: The module shall have a control input interface that is defined in the vendor documentation used to control operation of the module, including input commands, signals, data, and manual inputs.

VE02.02.04: The module shall have a status output interface that is defined in the vendor documentation used to indicate or display the status of the module including output data, signals, indicators, and physical indicators.

Required Test Procedures

TE02.02.01: The tester shall verify from vendor documentation that the module has a data input interface that includes any of the following to be input or processed by the module:

1. Plaintext data that is to be encrypted or authenticated in the module.

2. Ciphertext data that is to be decrypted in the module.

3. Cryptographic keys that are input into and used by the module.

4. Other key management data that is input into the module (depending on the module functions, this might include initialization vectors, counters, zeroization commands, split key information, or key accounting information). (Other key management requirements are covered in section 8.)

5. Authentication data that is input into the module.

6. Status information from outside the module (for example received from another module).

7. Any other information that is input into the module for processing or storage except for control information which is covered separately in VE02.02.03 and TE02.02.03 below.

8. Note that for security levels 1 and 2, the data input port or ports for cryptographic keys, authentication data, and other critical security parameters may be shared with other ports of the module. (Corresponding requirements for security levels 3 and 4 are covered separately under assertion AS02.13 in this section.)

TE02.02.02: The tester shall verify from vendor documentation that the module has a data output interface that includes any of the following to be output by the module:

1. Plaintext data that has been decrypted by the module.

2. Ciphertext data that has been encrypted by the module.

3. Cryptographic keys that are generated within and output from the module.

4. Other key management data that is output from the module (depending on the module functions, this might include initialization vectors, counters, zeroization commands, split key information, or key accounting information). (Other key management requirements are covered in section 8.)

5. Authentication data that is output from the module.

6. Control information sent outside the module (for example to be sent to another module).

7. Any other information that is output from the module after processing or storage except for status information that is covered separately in VE02.02.04 and TE02.02.04 below.

Note that for security levels 1 and 2, the data output port or ports for cryptographic keys, authentication data, and other critical security parameters may be shared with other ports of the module. (Corresponding requirements for security levels 3 and 4 are covered separately under assertion AS02.13 in this section.)

TE02.02.03: The tester shall verify from vendor documentation that the module has a control input interface that is used to enter information that controls the operation of the module (as opposed to input data which is processed or stored by the module as defined in VE02.02.01 and TE02.02.01 in this section), including any:

1. Input commands
2. Input signals
3. Input data
4. Manual inputs (such as switches, buttons, and keyboards)

TE02.02.04: The tester shall verify from vendor documentation that the module has a status output interface that is used to output information that indicates or displays the status of the module (as opposed to data output as defined in VE02.02.02 and TE02.02.02 in this section) including any:

1. Output data
2. Output signals
3. Output indicators
4. Status codes

5. Physical indicators (such as lights, LEDs, buzzers, and displays)

AS02.03: The module may include the following logical interfaces: (1, 2, 3, and 4)

- **Power interface**
- **Maintenance access interface**

Required Vendor Information

VE02.03.01: If the module accepts or provides external power, it shall have a power interface well defined in the vendor documentation that includes any entry or exit points for the power.

VE02.03.02: If the module allows access for maintenance purposes, it shall have a maintenance access interface, well defined in the vendor documentation, that includes any of the following inputs, outputs, or accesses used to maintain, service, or repair the module:

1. Data
2. Control information
3. Status information
4. All physical access paths

Any data, control, or status information used to maintain, service, or repair the module shall enter and exit via the maintenance access interface.

Required Test Procedures

TE02.03.01: The tester shall determine whether the module uses power from an external source or provides power to an external source. If either or both of these conditions are met, the tester shall verify from vendor documentation that the vendor documentation shows that a logically separate power interface is provided. Note that a power interface is not required when all power is provided or maintained internally to the module (e.g., battery power or solar power).

TE02.03.02: The tester shall determine whether the module allows access for maintenance purposes. If so, the tester shall verify from vendor documentation that the vendor documentation shows a logically separate maintenance interface is provided. The tester shall verify that documentation on the maintenance interface, if present, includes all of the following information that is used to maintain, service, or repair the module:

1. Data input into the module that may include test data to fill module storage with known data or to put the module into a known state.

2. Data output from the module (for example: for checking against known correct data or for other correctness checks).

3. Control information that puts the module into specific states required for maintenance.

4. Status information that indicates the state of the module before, during, or after maintenance actions.

5. All physical access paths including removable covers and doors used to gain physical access to the contents of the module.

6. (Other requirements on the maintenance interface are covered separately under assertions AS02.05 through AS02.08 in this section. Some requirements relating to physical access are covered in section 5.)

AS02.04: All data output via the data output interface shall be inhibited whenever an error state exists and during self-tests. (1, 2, 3, and 4)

Required Vendor Information

VE02.04.01: The vendor design shall ensure that all data output via the data output interface is inhibited whenever the module is in an error state, as documented in section 4, and the vendor documentation shall describe how this is done.

VE02.04.02: The vendor design shall ensure that all data output via the data output interface is inhibited whenever the module is in a self-test condition, as documented in section 11, and the vendor documentation shall describe how this is done.

Required Test Procedures

TE02.04.01: The tester shall verify that the vendor documentation shows that all data output via the data output interface is inhibited whenever the module is in any error state. In particular, 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 must be inhibited, unless and until error recovery, if any, is complete. (Some status output may be allowed to assist in determining the type of error, as long as it is clear that no potentially sensitive information could be released.) The tester shall also verify that the error states discussed in vendor documentation in response to this requirement are identical to those documented in the finite state machine model of section 4 (requirement VE04.00).

TE02.04.02: To the extent the module design and operating procedures allow, the tester shall put the module in each error state and verify that all data output via the data output interface is disallowed. (Limited status information that may be useful in determining the type of error is allowed as long as no potentially sensitive information is released.) The error state should be induced by at least the following actions, if applicable and practical: opening a tamper protected area, entering an incorrect

key, reducing input voltage,and any other possible error-inducing actions.

TE02.04.03: The tester shall verify that the vendor documentation shows all data output is inhibited whenever the module is in any self-test condition. The tester shall also verify that the self-test conditions discussed in vendor documentation in response to this requirement are identical to those documented in the self tests of section 11 (requirements VE11.01.01 and TE11.01.01).

TE02.04.04: If the module design and operating procedures allow it, the tester shall put the module in a self-test state and verify that data output is disallowed.

TE02.04.05: The tester shall verify that the vendor documentation shows how the data output is to be inhibited, to ensure that the alarm or self-test indications can logically inhibit the data output interface, and that the data output lines are, in fact, inhibited under any reasonable conditions (for example: a logical switch connected to an alarm indicator line could open an output line).

AS02.05: If a maintenance access interface is provided, any removable covers or doors defined as part of it shall be safeguarded using the appropriate physical security mechanisms of section 5. (1, 2, 3, and 4)

Required Vendor Information

VE02.05.01: The vendor documentation shall specify how the design ensures that any removable covers or doors of a maintenance access interface meet the physical security requirements of section 5.

Required Test Procedures

TE02.05.01: The tester shall determine whether the vendor documentation states that a maintenance access interface is provided and any removable covers or doors are provided. If so, the tester shall refer to the evaluation of requirements in section 5 to ensure that all applicable physical security requirements of that section are met (requirements TE05.10.04, TE05.17.01, TE05.19.01, or TE05.20.04 as appropriate for the physical configuration and security level of module).

AS02.06: If a maintenance access interface is provided, all access defined under assertion AS02.08 in this section, including physical modifications to the contents of the module, shall be restricted to the authorized maintenance role of section 3.1. (1, 2, 3, and 4)

Required Vendor Information

VE02.06.01: The vendor documentation shall specify how the module design and maintenance accesses, if any, ensure that any maintenance actions or physical modifications are restricted to the maintenance role(s) defined under section 3.1.

Required Test Procedures

TE02.06.01: If vendor documentation states that a maintenance access interface is provided, the tester shall verify that the vendor documentation required under assertion AS02.08 in this section defines these actions in sufficient detail to allow the tester to determine whether the requirements of this assertion are met. The tester shall verify that the maintenance actions defined here are consistent with those defined in the maintenance role requirements of section 3.1 and shall also verify that the evaluation against section 3.1 shows that all applicable maintenance role requirements are met.

AS02.07: If a maintenance access interface is provided, all plaintext secret and private keys and other critical security parameters contained in the module shall be zeroized when accessing the maintenance interface. (1, 2, 3, and 4)

Required Vendor Information

VE02.07.01: The vendor shall ensure that all of the module's plaintext keys and other critical security parameters, as defined in section 2.1 of FIPS PUB 140-1, are actively zeroized when the maintenance interface is accessed. The vendor documentation shall show how this requirement is met.

Required Test Procedures

TE02.07.01: If vendor documentation states that a maintenance access interface is provided, the tester shall verify that the vendor documentation shows that all operational plaintext keys and other unprotected critical security parameters contained in the module are actively zeroized as defined in TE02.07.02 when accessing the maintenance interface. Critical security parameters are defined in section 2.1 of FIPS PUB 140-1 to consist of cryptographic keys, authentication data such as passwords and personal identification numbers, and any other security-related information that is in a plaintext or other unprotected form, and that, if disclosed or modified, could compromise the security of the module or the security of information handled by the module.

TE02.07.02: If the module has a maintenance access interface, the tester shall verify from vendor documentation that zeroization includes actively erasing keys and parameters by overwriting or otherwise altering them. Zeroization techniques may include overwriting memory, or shorting memory to ground if the vendor shows that this drains off all charge within a few seconds. However, just removing power to memory and allowing charge to slowly dissipate is not sufficient. If the module design and operating procedures allow it, the tester shall access the maintenance interface while the unit is powered up, and verify that all operational keys are zeroized (for example by attempting to encrypt or decrypt data and observing that these actions are not possible, by obtaining a report of active keys and observing that no normal keys are usable, etc.)

AS02.08: If a maintenance access interface is provided, documentation shall include a complete specification of the set of authorized maintenance procedures for the module. (1, 2, 3, and 4)

Required Vendor Information

VE02.08.01: Vendor documentation shall define in detail all procedures, if any, by which authorized maintenance actions for the module are performed. These procedures shall be consistent with documentation provided under other requirements of this and all other sections.

Required Test Procedures

TE02.08.01**:** If vendor documentation states that a maintenance access interface is provided, the tester shall verify that the vendor documentation specifies all maintenance actions that are authorized for the module in sufficient detail to allow evaluation of the requirements of other sections. In particular, the tester shall verify that the maintenance procedures defined here are consistent with the maintenance roles of section 3.1, the maintenance states of section 4, and any physical tamper protection of section 5.

AS02.09: Documentation shall include a complete specification describing each of the logical interfaces of the module. (1, 2, 3, and 4)

Required Vendor Information

VE02.09.01: Documentation shall include a complete specification describing each of the interfaces of the module, including any:

1. Physical or logical ports and their pin assignments
2. Physical covers and doors or openings
3. Manual or logical controls
4. Physical or logical status indicators
5. Physical, logical, and electrical characteristics, as applicable, of the above interfaces

Required Test Procedures

TE02.09.01: The tester shall verify that vendor documentation specifies the required interfaces of the module in sufficient detail to allow evaluation of the requirements under section 4.2 of FIPS PUB 140-1. The tester shall verify that this documentation is consistent with, or combined with, the description of information flows required under assertions AS01.01 and AS02.01. The required interfaces and their associated documentation shall include:

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

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

3. Manual or logical controls, including their physical location within the module and a summary of the control signals that are input via the control interface.

4. Physical or logical status indicators, including their physical location within the module and a summary of the status indication signals that are output via the status interface.

5. Physical, logical, and electrical characteristics, as applicable, of the above interfaces, including summaries of pin placements, 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.

6. Any other logical interfaces that the module possesses that are necessary for proper functioning of the module.

AS02.10: Documentation shall explicitly define and specify all physical and logical input and output data paths within the module. (1, 2, 3, and 4)

Required Vendor Information

VE02.10.01: The vendor documentation shall describe all physical and logical input and output data paths in sufficient detail to specify all major categories of information input, processed, and output by the module. All input data entering the module via the data input interface shall only pass through the input data path. All output data exiting the module via the data output interface shall only pass through the output data path.

Required Test Procedures

TE02.10.01: The tester shall verify that the vendor documentation defines the physical and logical paths, for both input and output, to the level of detail required below. The data paths must be systematically itemized (for example: by highlighting or annotating copies of the block diagram or other information required under AS01.01, AS01.02, and AS01.05). The data paths must be defined in sufficient detail to completely specify which information passes through each port and to summarize the processing performed on the information by each module subsection between input and output.

TE02.10.02: The tester shall verify from vendor documentation that all input data, other than control information, enters the module only via the defined data input interface port or ports and then flows

only through the defined input data path. The tester shall also verify from vendor documentation that all output data, other than status information, flows only through the defined output data path and then leaves the module only via the defined data output interface port or ports. The tester shall examine both logical information flows, concentrating on the processing performed upon data and the logical relationships between data, and physical data flows, concentrating on the physical location in the module of data paths and data processing. If the tester finds any potential conflicts that could lead to misrouting of sensitive data, clarifying information shall be requested from the vendor if necessary.

AS02.11: Two independent, internal actions shall be required in order to output data via any output interface through which plaintext cryptographic keys or other critical security parameters could be output. (1, 2, 3, and 4)

Required Vendor Information

VE02.11.01: If there is any possibility that the module design could allow plaintext cryptographic keys or other critical security parameters to be output on any ports, the design shall require two independent internal actions before output occurs at such ports. In this case, the vendor documentation shall define what these actions are and how they protect against inadvertent release of critical security parameters. This documentation shall include specification of the module functional areas (whether in hardware and/or software) in which the two independent actions are performed.

Required Test Procedures

TE02.11.01: The tester shall determine from vendor documentation whether it is possible to output plaintext keys or other critical security parameters (as defined in section 2.1 of FIPS PUB 140-1). If so, the tester shall verify that the documentation specifies two independent internal actions that must take place before release of any data is allowed on any ports that could release critical security parameters. The independent actions must be logical or physical changes to two areas of the module that are sufficiently independent in function, and separated in location, that a malfunction to one area will not affect the proper functioning of the other area.

TE02.11.02: The tester shall verify that the dual internal actions specified in TE02.11.01 above, and the module areas which are exercised, are consistent with the module description required under assertions AS01.01 and AS01.05. If any software or firmware is executed in the process of outputting data , the tester shall examine the source code listings, if practical, to ensure that the software supports the requirement for two independent actions before data is output from the affected ports.

AS02.12: The output data path shall be logically disconnected from the circuitry and processes performing key generation, manual key entry, or key zeroization. (1, 2, 3, and 4)

Required Vendor Information

VE02.12.01: The vendor documentation shall show that the design of the module ensures logical separation of the output data path from processes performing generation, manual entry, and zeroization of cryptographic keys.

Required Test Procedures

TE02.12.01: The tester shall verify that vendor documentation demonstrates that the output data path, as defined under AS02.10, is logically disconnected from processes performing key generation, manual key entry, and key zeroization. This requirement implies that the specified key processes cannot pass information to the output data path, and that the output data path cannot interfere in any way with the key processes. If the key and data paths are physically shared to any extent (which is allowed for levels 1 and 2), the tester shall verify that the vendor documentation shows how the module design enforces separation of the key and other output data under any reasonable conditions, including any checks, alarms, or shut-offs that enforce this separation. Such protective measures might include separation of key and output data processes in location (separate paths and ports for keys versus other data), or time (so that no output is allowed during key processing, for example), or the use of software isolation (header tags and checking, multilevel security isolation, etc.)

TE02.12.02: If it is practical, and the module design and operating procedures permit it, the tester shall record or observe data on the output data port or ports while performing possible key functions (such as generation, manual entry, and zeroization) and verify that no critical security parameters (as defined in section 2.1 of FIPS PUB 140-1) are released.

AS02.13: For security levels 3 and 4, data input and output ports used for plaintext cryptographic keys, plaintext authentication data, and other unprotected critical security parameters shall be physically separated from all other ports of the module. (3 and 4)

Required Vendor Information

VE02.13.01: For security levels 3 and 4, if the module design requires use of unprotected critical security parameters, including plaintext cryptographic keys or plaintext authentication data, data ports for input or output of these parameters shall be physically separated from all other ports. The vendor documentation shall show how this is done.

Required Test Procedures

TE02.13.01: For security levels 3 and 4, the tester shall determine from vendor documentation whether the module requires input or output of unprotected critical security parameters as defined in section 2.1 of FIPS PUB 140-1. If so, the tester shall verify, from vendor documentation and also by physical inspection of the ports on the module, that both the corresponding critical security parameter input and output ports are physically separate from all other ports. The tester shall also verify that only unprotected critical security parameters, including plaintext cryptographic keys or plaintext authentication data, enter or exit the module through these ports. The tester shall verify that

any documentation on data paths provided by the vendor in connection with this requirement is consistent with, or contained in, documentation provided in connection with assertion AS02.10. (Note that separate pins within one connector may be considered separate ports.)

AS02.14: For security levels 3 and 4, data input and output ports used for plaintext cryptographic keys, plaintext authentication data, and other unprotected critical security parameters shall allow for direct entry of these items. (3 and 4)

Required Vendor Information

VE02.14.01: For security levels 3 and 4, if the module design requires use of unprotected critical security parameters, including plaintext cryptographic keys or plaintext authentication data, data ports for input or output of these parameters shall be directly connected to the cryptographic boundary without passing through any processors, complex logic blocks, or module areas performing functions unrelated to key handling which are outside the cryptographic boundary. The vendor documentation shall show how this is done.

Required Test Procedures

TE02.14.01: For security levels 3 and 4, the tester shall determine from vendor documentation whether the module requires input or output of unprotected critical security parameters as defined in section 2.1 of FIPS PUB 140-1. If so, the tester shall verify that the vendor documentation defines the path between the input or output ports and the cryptographic boundary. The tester shall then verify that the above security parameters pass directly between the input/output ports and the cryptographic boundary without unnecessarily passing through other module components. In particular, while outside the cryptographic boundary, the security parameters must not pass through any general-purpose processors that have functions other than handling security parameters, nor through any areas handling unrelated input or output functions. (Temporary display of manually entered encrypted keys is allowed as described under AS08.12.)

General: Documentation of input, output, control, or status interfaces must also include identification of any external input/output devices to be used with module, such as keypads, displays, smart cards, etc.

3. ROLES AND SERVICES

Roles

AS03.01: Documentation shall provide a complete specification of all of the authorized roles supported by the module. (1, 2, 3, and 4)

Required Vendor Information

VE03.01.01: Vendor documentation shall specify each distinct authorized role, including its name, purpose, and the services that are performed in the role.

Required Test Procedures

TE03.01.01: The tester shall review the vendor documentation and verify that, for each defined role, the name, purpose, 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 (one or more)
3. Maintenance role (only if the module includes a maintenance interface)
4. Other roles

TE03.01.02: 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 AS03.07.

AS03.02: The cryptographic module shall, at a minimum, support the following authorized roles: (1, 2, 3, and 4)

- **User role: The role assumed by an authorized user obtaining security services, performing cryptographic operations, or other authorized functions.**

- **Crypto-officer role: The role assumed by an authorized crypto officer performing a set of cryptographic initialization or management functions (e.g., cryptographic key and parameter entry, cryptographic key cataloging, audit functions, and alarm resetting).**

Required Vendor Information

VE03.02.01: In the documentation required to satisfy VE03.01.01 above, the vendor shall include at

least one user role and one crypto-officer role.

Required Test Procedures

TE03.02.01: The tester shall review the vendor documentation and verify that, in the specification of the authorized roles, at least one user role and at least one crypto-officer role are defined. These roles shall be specified by name, purpose, and allowed services. These roles shall be described as specified in AS03.02.

AS03.03: If a cryptographic module includes a maintenance access interface as specified in section 4.2, the module shall also support the maintenance role. (1, 2, 3, and 4)

- **Maintenance role: The role assumed by an authorized maintenance person accessing the maintenance access interface and/or performing specific maintenance tests and obtaining interim results in order to maintain, service or repair the module.**

Required Vendor Information

VE03.03.01: 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, purpose, and allowed services. Note that the maintenance role involves accessing and running tests on the module while it is operational; it does not involve any physical maintenance. The maintenance is a role that can be assumed by an operator and recognized by the module.

Required Test Procedures

TE03.03.01: The tester shall check the specifications of the module interfaces to determine whether a maintenance interface is specified (see AS02.03). 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.

AS03.04: If the maintenance role is supported, a cryptographic module shall clear all plaintext secret and private keys and other critical security parameters when entering the maintenance role. A related assertion is AS02.07. (1, 2, 3, and 4)

Required Vendor Information

VE03.04.01: The vendor shall ensure all of the module's plaintext secret and plaintext private keys and critical security parameters, as defined in section 2.1 of FIPS PUB 140-1, are actively zeroized when the maintenance role is entered. Note that the maintenance role is an active role (i.e., the module must still be powered up in order to assume the role). The vendor documentation shall specify how this requirement is met. Methods for zeroization could include, but not be limited to,

software or firmware code or the automatic assertion of certain signals within the module.

Required Test Procedures

TE03.04.01: 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 plaintext secret and plaintext private keys and critical security parameters are zeroized when the maintenance role is entered. Critical security parameters are defined in section 2.1 of FIPS PUB 140-1 to consist of cryptographic keys, authentication data such as passwords and personal identification numbers (PINs) and any other security-related information that is in plaintext or otherwise unprotected form and that, if disclosed or modified, could compromise the security of the module or of information handled by the module.

TE03.04.02: If the module implements a maintenance role, the tester shall verify from vendor documentation that zeroization is performed as defined in TE02.07.02.

AS03.05: If the maintenance role is supported, a cryptographic module shall clear all maintenance keys and other critical security parameters when exiting the maintenance role. (1, 2, 3, and 4)

Required Vendor Information

VE03.05.01: The vendor shall ensure all of the module's maintenance keys and other critical security parameters are actively zeroized when the maintenance role is exited. The vendor documentation shall specify how this requirement is met. Methods for zeroization could include, but not be limited to, software or firmware code or the automatic assertion of certain signals within the module.

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 maintenance keys and other critical security parameters are zeroized when the maintenance role is exited. Critical security parameters are defined in section 2.1 of FIPS PUB 140-1 to consist of cryptographic keys, authentication data such as passwords and personal identification numbers (PINs) and any other security-related information that is in plaintext or otherwise unprotected form and that, if disclosed or modified, could compromise the security of the module or of information handled by the module.

TE03.05.02: If the module implements a maintenance role, the tester shall verify from vendor documentation that zeroization is performed as defined in TE02.07.02.

AS03.06: If a module can support multiple concurrent operators, then the module shall internally maintain the separation of the authorized roles and services performed by each operator. (1, 2, 3, and 4)

Required Vendor Information

VE03.06.01: The vendor documentation shall specify whether multiple concurrent operators are allowed. If so, 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

TE03.06.01: The tester shall review the vendor documentation and verify that the method is described by which the module enforces separation between the roles and services performed by concurrent operators.

TE03.06.02: The tester shall take on the identity of two independent operators: Operator1 and Operator2. The operators shall assume two different roles. The tester shall verify that only the services allocated to the role assumed by each operator 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.

TE03.06.03: 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.

Services

AS03.07: Documentation shall provide a complete specification of each of the authorized services, operations, and functions that can be performed by the module. For each service, the service inputs, corresponding service outputs, and the authorized role or set of roles in which the service can be performed shall be specified. (1, 2, 3, and 4)

Required Vendor Information

VE03.07.01: The vendor documentation shall fully describe each service including its purpose and function. The possible services may include, but not be limited to, the following:

1. Cryptographic operations, such as:

   – Encryption
   – Decryption
   – Message integrity

– Digital signature generation

– Digital signature verification
– Other operations that require the use of cryptography

2. Key management operations, such as:

- Key and parameter entry
- Key generation
- Key output
- Key archiving
- Key zeroization
- Other key management functions

3. Cryptographic management functions, such as:

- Audit parameter entry and setting
- Alarm handling and resetting
- Other cryptographic management functions

4. Performance of operator-selectable self tests, such as:

- Cryptographic algorithm tests
- Software/firmware tests
- Critical functions tests
- Statistical random number generator tests
- Any additional tests that can be initiated by an operator

5. "Show Status" that would indicate the following:

- Active role(s)
- Cryptographic state of module (zeroized, tampered, loaded, initialized, etc.)
- If module is in error state, error code.
- If bypass capability exists, whether the bypass capability is enabled or disabled.

6. Performance of maintenance tests

7. Cryptographic bypass

VE03.07.02: 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. The vendor may supply a matrix that displays the services that can be performed in each role.

Required Test Procedures

TE03.07.01: 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.

TE03.07.02: The tester shall check the vendor documentation and verify that, for the indicated roles, the listed services, at a minimum, may be allowed:

1. User role, such as:

    - Cryptographic operations (may be allowed to access a subset of those listed in VE03.07.01)
    - Key management functions
    - "Show Status"
    - Performance of operator selectable self-tests
    - Cryptographic bypass

2. Crypto-officer role, such as:

    - Key management functions
    - Cryptographic management functions
    - "Show Status"
    - Performance of operator selectable tests
    - Cryptographic bypass

3. Maintenance role, such as:

    - Subset of key management functions (for entry of maintenance keys)
    - Cryptographic operations (may be allowed to access a subset of those listed in VE03.07.01)
    - "Show Status"
    - Performance of operator-selectable self-tests
    - Performance of maintenance tests
    - Cryptographic bypass

TE03.07.03: The tester shall verify the accuracy of the vendor-supplied documentation. The tester shall perform the following tests 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.

AS03.08: A cryptographic module shall, at a minimum, provide the following services: (1, 2, 3, and 4)

- **Show Status: Output the current status of the module**

- **Self-test: Initiate and run the self-tests as specified in section 4.11.**

Required Vendor Information

VE03.08.01: 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 VE03.07.01.

Required Test Procedures

TE03.08.01: The tester shall check the vendor documentation to verify that the "Show Status" 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.03.07.

TE03.08.02: Verification that the "Show Status" can be initiated for designated roles was performed under TE03.07.03. In addition, the tester shall verify that what the "Show Status" reports matches the vendor documentation.

TE03.08.03: Verification that the module provides for the initiation and running of self-tests as specified in section 4.11 was performed under TE03.07.03. If the module does not provide this service for at least one authorized role, this assertion fails.

AS03.09: A cryptographic module may optionally provide the following service: (1, 2, 3, and 4)

- **Bypass: Activate or deactivate a bypass capability whereby services are provided without cryptographic processing (e.g., transferring plaintext through the module).**

Required Vendor Information

VE03.09.01: If the module implements a bypass capability, the vendor documentation shall describe the bypass service as specified in AS03.09.

Required Test Procedures

TE03.09.01: The tester shall determine whether the bypass capability is implemented by the module. If so, the tester shall check the vendor documentation to verify that the bypass capability is allocated to at least one authorized role. The tester shall verify that this service is described as specified in AS.03.09.

TE03.09.02: Verification that the bypass capability can be performed for designated roles was tested in TE03.07.03. If the bypass capability cannot be initiated by at least one role, this assertion fails.

AS03.10: If a cryptographic module implements a bypass capability, then: (1, 2, 3, and 4)

- **In order to prevent the inadvertent bypass of data due to a single failure, two independent internal actions shall be implemented to activate the bypass capability.**

- **The current status of the module (e.g., the response to a "Show Status" service request) shall indicate whether or not the bypass capability is activated.**

Note: *Internal actions may be software actions or operator physical actions performed as a consequence of the request for a transition to a bypass state. The changing of an internal variable to a known value or the sensing of a keyboard toggle switch are examples of internal actions.*

Required Vendor Information

VE03.10.01: The finite state machine diagram and description documentation shall indicate, for all transitions into a bypass state, the two independent internal actions that are required to transition into that bypass state. In the vendor documentation for the "Show Status" service, the ability to output whether the bypass capability is enabled or disabled must be included.

Required Test Procedures

TE03.10.01: The tester shall review the finite state diagram and description to determine whether each transition into a bypass state shows two independent internal actions that must occur in order for the cryptographic module to transition into the bypass state.

TE03.10.02: 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.

TE03.10.03: Tester verification of the vendor documentation for the "Show Status" service was performed under TE03.08.01 and TE03.08.02. If the bypass capability exists, then the results of the verification should indicate that a "Show Status" service request shows that the bypass capability is enabled or disabled; otherwise, this assertion fails.

AS03.11: Each service input shall result in a service output. (1, 2, 3, and 4)

Required Vendor Information

VE03.11.01: The vendor documentation shall indicate service outputs for each service input.

Required Test Procedures

TE03.11.01: The validation of the specification of a service output for each service input is covered by TE03.07.01. The testing of the status inputs and outputs is covered by TE03.07.03. The results of the verification should indicate that each service input has a corresponding service output as documented by the vendor; otherwise, this assertion fails.

Operator Authentication

General

AS03.12: For services that are used to initialize the access control information needed to implement the access control mechanisms, means such as procedural controls, or authentication and authorization information, factory-set or default, may be used to control access to the module. (1, 2, 3, and 4)

Required Vendor Information

VE03.12.01: If means are provided to control access to the module before it has been initialized, the vendor shall document them in detail.

Required Test Procedures

TE03.12.01: The tester shall check the vendor documentation to determine what means, if any, are provided for access control prior to initialization of the module. If the module supports these means, the documentation should specifically describe the procedure by which the crypto-officer is authenticated upon accessing the module for the first time. No other role shall be allowed to access the module until the module has been initialized.

TE03.12.02: If access to the module before initialization is controlled, the tester shall make an error (e.g., enter an incorrect password) while assuming the crypto-officer role on an uninitialized module and shall verify that the module denies access to the role. The tester shall then successfully assume the crypto-officer 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.

AS03.13: When a module is powered up after being powered off (e.g. power failure) or after repair or servicing, the results of previous authentications shall not be retained, i.e., the module shall re-authenticate the authorization of the operator to assume a desired role. (1, 2, 3, and 4)

Required Vendor Information

VE03.13.01: The vendor documentation shall describe how the results of previous authentications are cleared when the module is powered down.

Required Test Procedures

TE03.13.01: The tester shall review the vendor documentation and verify that the clearing of previous authentications upon power down of the module is described clearly and correctly.

TE03.13.02: The tester shall authenticate himself/herself to the module by assuming one or more roles, power down the module, power up the module, and attempt to perform services in those roles. The module should deny access to the services and require that the tester be re-authenticated.

Role-Based Authentication

AS03.14: For role-based authentication, a cryptographic module shall authenticate that the operator is authorized to assume a specific role or set of roles. The module shall perform the following actions: (2)

- **Require that the operator explicitly or implicitly select one or more roles**
- **Authenticate that the operator is authorized to assume the selected roles and corresponding services**

Required Vendor Information

VE03.14.01: 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 authorization of the operator to assume the role(s). Note that role-based authentication is based only on the presentation of information that allows access to a role or set of roles. This information must be different for each role, but it is the

same for everyone that wants to access the same role; two operators that want to assume the same role will present the same information to the module.

Required Test Procedures

TE03.14.01: The tester shall review the sections of the vendor documentation that describe how role-based authentication is performed. The tester shall check that the documentation specifies and describes the mechanisms used for the selection of a role or roles and the authentication of the authorization of the operator to assume a role. The documentation may specify and describe the usage of one or more of the following mechanisms:

1. Password
2. Personal Identification Number (PIN)
3. Cryptographic key or equivalent
4. Possession of a physical key, token, or equivalent
5. Biometrics (e.g., fingerprint, retina scan, keystroke dynamics)

TE03.14.02: The tester shall assume the role and shall make some error (e.g., entry of an incorrect password) during the authentication procedure. The tester shall observe that the module denies access to the role.

AS03.15: For role-based authentication, a module may permit an operator to change roles, but the module shall authenticate the authorization of the operator to assume any role that was not previously authenticated. (2)

Required Vendor Information

VE03.15.01: The vendor shall document whether the module allows an operator to change roles. If so, the vendor documentation shall describe the ability of an operator to change roles and shall explicitly state that authentication of the operator for a new role is required.

Required Test Procedures

TE03.15.01: The tester shall check the vendor documentation to verify that the method by which an operator can change roles includes the authentication of the operator for a role not previously authenticated.

TE03.15.02: 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 requires authentication for 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 denies access.

Identity-Based Authentication

AS03.16: For identity-based authentication, a cryptographic module shall authenticate the identity of an operator and verify that the identified operator is authorized to assume a specific role or set of roles. The module shall perform the following actions: (3 and 4)

- **Require that the operator be individually identified**
- **Authenticate the specified identity of the operator**
- **Require that the operator either implicitly or explicitly select one or more roles**
- **Based on the authenticated identity, verify that the operator is authorized to perform the selected roles and corresponding services**

Required Vendor Information

VE03.16.01: The vendor shall document the mechanisms 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 authorization of the operator to assume the role(s). Note that identity-based authentication takes into account the identity of the operator assuming a role. This applies not only between roles but within the same role; two operators that want to assume the same role will present different information to the module because their identities are different. If, for example, operators must enter a PIN when attempting to assume a role, each operator should have a different PIN because the PIN identifies the operator to the module.

Required Test Procedures

TE03.16.01: The tester shall review the sections of the vendor documentation that describe how identity-based authentication is performed. The tester shall check that the 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. The documentation may specify and describe the usage of one or more of the following mechanisms:

1. Password
2. Personal Identification Number (PIN)

3. Cryptographic key or equivalent

4. Possession of a physical key, token, or equivalent
5. Biometrics (e.g., fingerprint, retina scan, keystroke dynamics)

TE03.16.02: The tester shall make some error (e.g., entry of an incorrect password) during the authentication procedure and shall observe that the module does not allow the tester to proceed beyond the authentication procedure.

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

AS03.17: For identity-based authentication, a module may permit an operator to change roles without re-authenticating the identity of the operator, but the module shall verify the authorization of the authenticated operator to perform the new role. (3 and 4)

Required Vendor Information

VE03.17.01: The vendor shall document whether the module allows an operator to change roles without re-authenticating his/her identity. If it does, the vendor documentation shall describe the ability of an operator to change roles and shall explicitly state that verification of the authentication of the operator for a new role is required.

Required Test Procedures

TE03.17.01: The tester shall check 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.

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

1. Assume a 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 re-authenticated, 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 a 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.

Security Level 1

AS03.18: For Security Level 1, a cryptographic module is not required to employ

anthentication mechanisms to control access to the module. A module optionally may employ either role-based or identity-based authentication mechanisms in order to verify the authorization of the operator to assume the desired roles and to request corresponding services. (1)

Required Vendor Information

VE03.18.01: The vendor shall explicitly document what type of authentication will be performed for the module. If the module does not require either role-based or identity-based authentication, the vendor documentation shall explicitly state this requirement. The vendor documentation shall describe the authentication mechanisms used as specified in VE03.14.01 and VE03.16.01.

Required Test Procedures

TE03.18.01: The tester shall review the vendor documentation to determine the following:

1. Type of authentication specified for the module (role-based, identity-based, or none)

2. Specification and description of the authentication mechanisms

TE03.18.02: For each role, the tester shall perform the documentation, verification, and test procedures specified in TE03.14.01-02 and TE03.15.01-02 for role-based authentication and TE03.16.01-03 and TE03.17.01-02 for identity-based authentication.

Security Level 2

AS03.19: For Security Level 2, a cryptographic module shall at a minimum employ role-based authentication mechanisms in order to verify the authorization of the operator to assume the desired roles and to request corresponding services. A module optionally may employ identity-based mechanisms. (2)

Required Vendor Information

VE03.19.01: The vendor shall explicitly document whether either role-based or identity-based authentication is performed for the module. The vendor documentation shall describe the authentication mechanisms used as specified in VE03.14.01 and VE03.16.01.

Required Test Procedures

TE03.19.01: The tester shall review the documentation to determine the following:

1. Type of authentication specified for the module (role-based or identity-based)

2. Specification and description of the authentication mechanisms

TE03.19.02: For each role, the tester shall perform the documentation verification and test procedures specified in TE03.14.01-02 and TE03.15.01-02 for role-based authentication and TE03.16.01-03 and TE03.17.01-02 for identity-based authentication.

Security Levels 3 and 4

AS03.20: A cryptographic module shall employ identity-based (i.e., based on operator identification) authentication mechanisms in order to verify the authorization of the operator to assume the desired roles and to request corresponding services. Furthermore, plaintext authentication data (e.g., passwords and PINs), plaintext cryptographic key components, and other unprotected critical security parameters shall be entered via a port or ports that are physically separated from other ports, and that allow for direct entry (as required in section 2). Related assertions are AS02.13 and AS02.14. (3 and 4)

Required Vendor Information

VE03.20.01: The vendor documentation shall explicitly state that identity-based authentication is performed for the module. The vendor documentation shall also describe the authentication mechanisms used as specified in VE03.16.01.

VE03.20.02: Requirements for vendor documentation addressing the entry of plaintext authentication data via dedicated, directly connected ports are covered under VE02.13.01 and VE02.14.01.

Required Test Procedures

TE03.20.01: For each role, the tester shall perform the documentation verification and test procedures specified in TE03.16.01-03 and TE03.17.01-02 for identity-based authentication.

TE03.20.02: Tester verification of the entry of plaintext authentication data, plaintext cryptographic key components, and other unprotected critical security parameters via dedicated, directly connected ports was performed under TE02.13.01 and TE02.14.01. The results of the verification should indicate that physically separated ports are used for the entry of these items into the module; otherwise, this assertion fails.

4. FINITE STATE MACHINE MODEL

AS04.01: All cryptographic modules shall be designed using a finite state machine model that explicitly specifies every operational and error state of the module. (1, 2, 3, and 4)

Required Test Procedures

TE04.01.01: This assertion is tested by testing the following assertions.

AS04.02: Documentation shall identify and describe all states of the module and shall describe all of the corresponding state transitions. (1, 2, 3, and 4)

Required Vendor Information

VE04.02.01: The vendor shall provide a description of the finite state machine 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 and internal module conditions, data outputs and status outputs resulting from transitions from one state to another.

Required Test Procedures

TE04.02.01: The tester shall verify that the vendor has provided a description of the finite state machine model. This description shall contain the identification and description of all states of the module, and a description of all corresponding state transitions.

AS04.03: The descriptions of the state transitions shall include the internal module conditions, data inputs and control inputs that cause transitions from one state to another, and shall include the internal module conditions, data outputs and status outputs resulting from transitions from one state to another. (1, 2, 3, and 4)

Required Test Procedures

TE04.03.01: 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, and the internal module conditions, data outputs and status outputs resulting from transitions from one state to another.

AS04.04: Documentation shall also include finite state diagrams in sufficient detail to assure the verification of conformance to FIPS PUB 140-1. (1, 2, 3, and 4)

Required Vendor Information

VE04.04.01: The vendor shall provide finite state machine diagram(s) in sufficient detail to assure the verification of conformance to FIPS PUB 140-1.

Required Test Procedures

TE04.04.01: The tester shall verify that the vendor has provided finite state machine diagram(s) in sufficient detail to assure the verification of conformance to FIPS PUB 140-1.

AS04.05: A cryptographic module shall be designed using the following types of states: (1, 2, 3, and 4)

- **Power on/off states. States for primary, secondary, or backup power. These states may distinguish between power applied to different portions of the module.**

- **Crypto officer states. States in which the crypto officer functions are performed (e.g., cryptographic initialization and key management functions).**

- **Key entry states. States for entering cryptographic keys and other critical security parameters into the module, and for checking their validity.**

- **User service states. States in which authorized users obtain security services, perform cryptographic operations, or perform other authorized user functions.**

- **Self test states. States for performing self-tests on the module (see section 11, "Self Tests").**

- **Error states States when the module has encountered an error (e.g., failed a self-test, attempting to encrypt while missing operational keys or other critical security parameters, or cryptographic errors). Error states may include "hard" errors which indicate an equipment malfunction and which may require maintenance, service or repair of the module, or error states may include recoverable "soft" errors which may require initialization or resetting of the module.**

Required Test Procedures

TE04.05.01: 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
9. Show status service
10. Self-tests
11. Other authorized services, operations, and functions (if applicable)
12. Error states

TE04.05.02: The tester shall verify that the operation of the module is consistent with the finite state diagrams and descriptions.

AS04.06: A cryptographic module may contain other types of states including the following: (1, 2, 3, and 4)

- **Un-initialized states. States in which no operational security parameters are loaded into the module.**

- **Idle states. States in which the module is potentially operational, but is not currently providing security services or performing cryptographic functions. Cryptographic keys and security parameters are loaded, and the module is waiting for data or control inputs.**

- **Safety states. States in which the module is not currently operational, but cryptographic keys and parameters are loaded. These states are used to protect the module from unauthorized use during the temporary absence of the operator.**

- **Bypass states. States for providing services without cryptographic operations (e.g., transferring plaintext through the module).**

- **Maintenance states. States for maintaining and servicing a module,**

including maintenance testing.

Required Test Procedures

TE04.06.01: The tester shall verify that the finite state diagrams and the descriptions are consistent with the vendor documentation that describes the following:

1. Bypass service (if applicable)
2. Maintenance interface (if applicable)
3. Maintenance role (if a maintenance interface is provided)
4. Key generation services (if applicable)
5. Key output services (if applicable)

TE04.06.02: The tester shall verify that the operation of the module while in an un-initialized, idle, safety, bypass, or maintenance state is consistent with the finite state diagrams and descriptions.

AS04.07: All data output via the data output interface shall be inhibited during all error states. (1, 2, 3, and 4)

Note: *This assertion is similar to assertion AS02.04 under section 2, "Module Interfaces."*

Required Test Procedures

TE04.07.01: This assertion is tested under TE02.04.02.

AS04.08: All error states shall be able to be reset to an acceptable operational or initialization state except for those hard errors which require maintenance, service or repair of the module. (1, 2, 3, and 4)

Required Test Procedures

TE04.08.01: From each error state that does not require maintenance 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 in such a state, and second, that the cryptographic 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).

AS04.09: If safety states are included in the module, then the safety states shall require an explicit authenticated action to return to a user/crypto service state. These states are equivalent to the "standby" mode of former Federal Standard 1027. (1, 2, 3, and 4)

Required Test Procedures

TE04.09.01: The tester shall attempt to issue all user and crypto-officer commands from each safety state to demonstrate that no operator commands can be issued until the module leaves the safety state.

TE04.09.02: For each defined safety state, the tester shall perform an explicit authentication action to exit the safety state. For each safety state, this explicit authentication action must be described in the vendor's operational documentation.

AS04.10: If a cryptographic module includes a maintenance access interface (see Section 2, "Module Interfaces"), then the module shall include maintenance states. (1, 2, 3, and 4)

Required Test Procedures

TE04.10.01: If the module includes a maintenance interface, then the tester shall make sure that the finite state machine model has at least one maintenance state defined. All such maintenance states must be contained in the finite state diagram(s) and described in the description of the finite state machine model.

AS04.11: All states of a cryptographic module shall be explicitly defined in sufficient detail to assure the verification of the conformance of the module to FIPS PUB 140-1. (1, 2, 3, and 4)

Note: *Refer back to the corresponding portions of requirement 1, "Cryptographic Module," and requirement 2, "Module Interface," for completeness.*

Required Test Procedures

TE04.11.01: The tester shall review the descriptions of the states of the cryptographic module to determine if the descriptions clearly define disjoint states.

TE04.11.02: 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.

TE04.11.03: The tester shall verify that every state that is identified in the finite state diagram(s) is also identified and described in the description.

TE04.11.04: The tester shall verify that every state that is identified and described in description is also identified in the finite state diagram(s).

TE04.11.05: 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.

TE04.11.06: The tester shall verify that there exists a chain of transitions from each nonpower off state to a power off state of the model.

Note: *TE04.11.05 and TE04.11.06 imply that there may be more than one possible initial state and more than one possible final state.*

TE04.11.07: The tester shall verify that the action of the finite state machine, as the result of all possible data and control inputs, is defined. An example of an acceptable inclusive statement is:

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

TE04.11.08: The tester shall verify that all possible combinations of data and control nputs can be partitioned into disjoint sets, depending on the transition that would be taken in response to the input. This requirement guarantees that the finite state machine is deterministic; that is, for each possible pair of data and control inputs, the finite state machine must take one and only one transition.

5. PHYSICAL SECURITY

AS05.01: Documentation shall include a complete specification of the physical embodiment and security level for which the physical security mechanisms of a cryptographic module are designed, as well as a complete description of the applicable security mechanisms that are employed by the module. (1, 2, 3, and 4)

Required Vendor Information

VE05.01.01: The vendor documentation shall specify which one of three physical embodiments the module is: single-chip cryptographic module, multiple-chip embedded cryptographic module, or multiple-chip stand-alone cryptographic module, as defined in the initial paragraphs of sections 4.5.1, 4.5.2, or 4.5.3, respectively, of FIPS PUB 140-1. The specified physical embodiment shall be consistent with the actual module physical design. The vendor documentation shall also explicitly state which security level (1 through 4) the module is intended to meet.

VE05.01.02: The vendor documentation shall completely describe the applicable physical security mechanisms that are employed by the module. The entire contents of the module, including all hardware, firmware, software, and data (including plaintext cryptographic keys and unprotected critical security parameters) shall be protected.

Required Test Procedures

TE05.01.01: The tester shall verify that the vendor documentation specifies which physical embodiment the module is. However, the tester shall make an independent determination, by evaluation against the definitions below, of the physical embodiment that the module actually meets. If the tester's determined physical embodiment is different than the vendor's specified physical embodiment, the tester shall contact the vendor and resolve the differences before completing the validation. The tester shall utilize the module definition required under the requirements of section 1, along with any other appropriate vendor documentation, to determine the physical embodiment of the module. 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 stand-alone device or physically embedded within some other module or enclosure that may not be physically protected. The chip normally will consist of one die, or multiple dice connected on a substrate, that is 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 module or enclosure that may not be physically protected. Examples: Adapters, expansion boards or other modules that are not single chips and are not contained within their own physically protected enclosures.

3. Multiple-chip stand-alone cryptographic module. Characteristics: Two or more IC chips interconnected and physically embedded in an enclosure that is entirely physically protected as defined in the requirements for the applicable security level. Examples: An IC-printed circuit board or chips on a ceramic substrate with a protected enclosure.

TE05.01.02: The tester shall verify that the vendor documentation states which security level the module is intended to meet. However, the tester shall make an independent determination, via evaluation against the requirements of this section of the validation process, of the security level that the module actually meets. If the tester's determined security level is obviously different than the vendor's intended security level, the tester shall contact the vendor and resolve the differences before completing the validation.

TE05.01.03: The tester shall verify that the vendor documentation completely describes the applicable physical security mechanisms that are employed by the module. The physical security mechanisms may include any of the following list that depend on and determine the physical embodiment and the security level met by the module:

1. Passivation

2. Coating or potting that may be opaque, hard, tamper-evident, removal-resistant, or a combination of the above characteristics

3. Enclosure that may be nonremovable or have removable covers or doors

4. Tamper protection (locks, seals, tamper detection, or tamper response)

5. Probe-protected ventilation holes

6. Environmental failure protection or environmental failure testing

The tester shall verify in each case claimed above, and in the analyses that follow from the validation requirements below, that the entire module is physically protected. For example, passivation must apply to all ICs in the module; a coating, enclosure or tamper protection must protect the entire module; etc. This requirement specifically includes all hardware containing firmware, software, and data (including plaintext cryptographic keys and unprotected critical security parameters).

AS05.02: For a single-chip cryptographic module at security level 1 or higher, the chip shall be

of production quality that shall include standard passivation techniques. Single-chip; 1, 2, 3, and 4)

Required Vendor Information

VE05.02.01: The module shall be a standard, production-quality IC, designed to meet at least typical commercial-grade specifications for power, temperature, reliability, shock/vibration, etc. In particular, the module shall use standard passivation techniques for the entire chip. The vendor documentation shall describe the IC quality. If an ICs is used which is not a standard device, its passivation design shall also be described.

Required Test Procedures

TE05.02.01: The tester shall verify by inspection that the module is a standard, integrated circuit with a uniform, exterior material and standard connectors. The tester shall verify from vendor documentation that the module is at least typical commercial grade in regard to reliability and shock and vibration. This documentation may consist of data sheets, special documentation submitted for this validation effort, comparisons to other physically similar commercial products, etc. If the tester cannot determine the module's quality from the submitted documentation, the vendor shall be required to provide additional information as needed.

TE05.02.02: 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. It is sufficient for the documentation to show that the IC is an industry-standard part from an established manufacturer. If this is not true, the documentation must specify the exact passivation material and technique used; and if it is not a standard passivation, then must also provide information to indicate why it is at least equivalent to a standard passivation approach.

AS05.03: For a single-chip cryptographic module at security level 2 or higher, the chip shall be covered with an opaque, tamper-evident coating. (Single-chip; 2, 3, and 4)

Required Vendor Information

VE05.03.01: The module shall be covered with an opaque tamper-evident coating. The coating may be either the passivation material or a material covering the passivation. 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

TE05.03.01: The tester shall verify by inspection and from vendor documentation that the module is covered with an opaque, tamper-evident coating. The inspection shall verify that the tamper-evident

coating completely covers the module; is visibly opaque when inspected with bright white light shining on and (if possible) against it; and deters direct observation, probing, or manipulation of the surface features of the chip. The tester shall verify, by scratching the coating with a sharp object, that it leaves marks that make it obvious the module has been tampered with.

AS05.04: For a single-chip cryptographic module at security level 3 or higher, a hard, opaque tamper-evident coating shall be used. (Single-chip; 3 and 4)

Required Vendor Information

VE05.04.01: The module shall be covered with a hard, opaque tamper-evident coating. The coating may be a hard, opaque epoxy covering the passivation, or another type of coating providing an equivalent level of protection. The material shall be opaque within the visible spectrum. The vendor documentation shall identify the kind of hard, opaque, tamper-evident coating used and its characteristics.

Required Test Procedures

TE05.04.01: 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 exactly which coating is used; if it is not hard epoxy, then supporting documentation on its hardness should be provided to show that it is roughly equivalent to epoxy. The tester shall verify, by scratching the coating with a sharp object, that it cannot be easily penetrated to the depth of the underlying circuitry, and that it leaves marks that make it obvious the module has been tampered with. The inspection must verify that the coating completely covers the module, is visibly opaque when inspected with bright, white light shining on and (if possible) against it, and deters direct observation, probing, or manipulation of the surface features of the chip. (Portions of this verification may already have been performed at level 2 in TE05.03.01.)

AS05.05: For a single-chip cryptographic module at security level 4, a hard, opaque removal-resistant coating shall be used. (Single-chip; 4)

Required Vendor Information

VE05.05.01: 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 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. 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

TE05.05.01: The tester shall verify by inspection and from vendor documentation that the module is covered with a hard, opaque removal-resistant coating. The documentation should specify exactly which coating is used and provide supporting data on its hardness and removal resistance. The tester shall verify, by scratching the coating with a sharp object, that it cannot be easily penetrated to the depth of the underlying circuitry, and [that it leaves marks that make it obvious the module has been tampered with. The inspection must verify that the coating completely covers the module and is visibly opaque when inspected with bright white light shining on and (if possible) against it. (Portions of this verification may already have been performed at level 2 or 3 in TE05.03.01 or TE05.04.01.)

TE05.05.02: The tester shall verify the removal-resistant properties of the module coating. The tester can obtain the information to perform this verification in one or both of the following two ways:

1. By supervising tests at a vendor facility

2. By performing tests at the tester's own facility

Whichever approach is chosen, the tester shall verify that all of the following tests were performed or reported, to the extent possible:

A. The tester (tester or vendor) setup the module in an operational state and verified that it was performing normally.

B. The tester then attempted to peel or pry the material from the module with a sharp object to expose the underlying circuitry, and verified that this was impossible with a reasonable application of force, or that the module ceased to function (e.g., ceased to provide normal output, entered a non-operational state, or provided other clear evidence of failure as appropriate), or that the module circuitry was obviously physically destroyed.

C. The solvency characteristics were tested similarly, using the application of a strong acid (such as buffered hydrofluoric acid or nitric acid) in place of peeling or prying.

AS05.06: For a single-chip cryptographic module at security level 4, the module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT). (Single-chip; 4)

Required Vendor Information

VE05.06.01: The vendor shall use either of the following:

1. EFP features

2. EFT

as specified in section 4.5.4 of FIPS PUB 140-1, 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.

VE05.06.02: If EFP is chosen for a particular condition, the module shall monitor and correctly respond to fluctuations in the operating temperature or voltage, as appropriate, outside of the module's specified normal operating range for that condition. The protection features shall involve additional electronic circuitry or devices that 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

2. Immediately actively zeroize all plaintext cryptographic keys and other unprotected critical security parameters

Documentation shall state which of these approaches was chosen and provide a complete specification and description of the environmental failure protection features employed within the module.

VE05.06.03: If EFT is chosen for a particular condition, the manufacturer of the module (or an organization designated by the manufacturer/vendor) shall perform required testing, involving a combination of analysis, simulation, and testing of the module as necessary to give a reasonable guarantee that the condition outside the module's normal operating range will not compromise the security of the module. The tests to be performed shall be as specified in section 4.5.4.2 of FIPS PUB 140-1. The manufacturer shall provide documentation that completely specifies the nature of the environmental failure tests performed and the results of those tests.

Required Test Procedures

TE05.06.01: If EFP is chosen for a particular condition, the tester shall determine by test that the

requirements are met. The tester can obtain the information to perform this verification in one or both of the following two ways:

1. By supervising tests at a vendor facility

2. By performing tests at the tester's own facility

Whichever approach is chosen, the tester shall verify that all of the following tests were performed or reported, to the extent possible:

A. The tester (tester or vendor) setup the module in an operational state, brought the environmental condition (either ambient temperature, using an environmental chamber if necessary, or supply voltage) close to the appropriate extreme of the normal operating range specified for the module, and verified that the module was performing normally.

B. The tester then continuously extended the temperature or voltage outside of the specified range, and determined that the module quickly either shut down (e.g., powered down or ceased to provide any output) or else zeroized the keys and other critical security parameters. (Zeroization is defined in TE02.07.02.)

C. The tester noted if any outputs indicated possible security problems with the module (e.g., sensitive data being outputted inappropriately, a failure to report key zeroization when expected, etc.).

D. If the vendor chose to zeroize the module and it was still operational after returning to the normal environmental range, the tester attempted to perform normal operations that required keys and verified that the module no longer performed these functions.

TE05.06.02: If EFT is chosen for a particular condition, the tester shall review the test reports provided by the vendor to determine that the requirements are met. The tester shall verify that the vendor test report included approximately the following types of test, to the extent possible:

1. The tester set up the module in an operational state, brought the environmental condition (ambient temperature, using an environmental chamber if necessary, or supply voltage) close to the appropriate extreme of the normal operating range specified for the module, and verified that the module was performing normally.

2. The tester then continuously extended the temperature or voltage outside of the specified operating range, ultimately to the limits required in FIPS PUB 140-030-1 (for temperature, – 100° C or + 200° C; for voltage,

until the module showed evidence of circuit destruction). Evidence of circuit breakdown could include the failure of output lines to provide expected data, a loss of power on interfaces, etc.

3. The tester noted if any outputs indicated possible security problems with the module, in particular keys or sensitive data being outputted inappropriately, but also inappropriate status reports such as a failure to report key zeroization when expected, etc. If suspicious activity was noted, the tester analyzed the information to determine if, in fact, there was a compromise of security functions. To the extent practical, all critical output lines that might reasonably be expected to malfunction under abnormal conditions were monitored for possible evidence of security compromise.

AS05.07: For a multiple-chip, embedded cryptographic module at security level 1 or higher, the chips in the module shall be of production quality that shall include standard passivation techniques. (Multiple-chip embedded; 1, 2, 3, and 4)

Required Vendor Information

VE05.07.01: The chips in the multiple-chip embedded module shall be standard production-quality ICs, designed to meet at least typical, commercial-grade specifications for power, temperature, reliability, shock/vibration, etc. In particular, the module shall use standard passivation techniques for the each chip. The vendor documentation shall describe the IC's quality. If any ICs are used which are not standard devices, their passivation design shall also be described.

Required Test Procedures

TE05.07.01: 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 at least typical commercial grade in regards to power and voltage ranges, temperature, reliability, and shock and vibration. This documentation may consist of data sheets, special documentation submitted for this validation effort, comparisons to other physically similar products, etc. If the tester cannot determine the chip's quality from the submitted documentation, the vendor shall be required to provide additional information as needed.

TE05.07.02: The tester shall verify from vendor documentation that the chips in the module have a standard passivation applied to them. The passivation must be a sealing coat applied over the chip circuitry to protect it against environmental or other physical damage. It is sufficient for the documentation to show that chips are industry-standard parts from established manufacturers. If this is not true, the documentation must specify the exact passivation material and technique used; and if it is not a standard passivation, then must also provide information to indicate why it is at least equivalent to a standard passivation approach.

AS05.08: For a multiple-chip, embedded cryptographic module at security level 1 or higher, the module shall be implemented as a production-grade multiple-chip embodiment. (Multiple-chip embedded; 1, 2, 3, and 4)

Required Vendor Information

VE05.08.01: The module shall be implemented as a typical production-grade, multiple-chip device, such as an IC printed circuit board or ICs on a ceramic substrate. The vendor documentation shall describe the production implementation of the module.

Required Test Procedures

TE05.08.01: The tester shall verify by inspection and from vendor documentation that the module has been implemented as a standard multiple-chip design, such as a circuit board, a multi-chip ceramic-substrate module, or a functionally-equivalent multi-chip design. The vendor must either specify a typical industry-standard design approach that was used; or if a unique approach is used, the vendor must provide design-and-test-data that shows that the module is equivalent in quality and function to a more traditional approach.

AS05.09: For a multiple-chip, embedded cryptographic module at security level 2 or higher, the module shall be encapsulated with an opaque, tamper-evident material. (Multiple-chip embedded; 2, 3, and 4)

Required Vendor Information

VE05.09.01: The module shall be encapsulated with an opaque, tamper-evident coating such as conformal 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

TE05.09.01: 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 when inspected with bright white light shining on and (if possible) against it; furthermore, by scratching the tamper-resistant material with a sharp object, thereby producing marks, the tester shall verify that the module provides evidence of attempts to tamper with or remove module components.

AS05.10: For a multiple-chip, embedded cryptographic module at security level 3 or higher, one of the following three requirements shall apply to the module: (Multiple-chip embedded; 3 or 4)

- A hard opaque potting material shall be used.

- The module shall be contained within a strong non-removable enclosure.

- The module shall be enclosed within a strong removable cover and shall include tamper response and zeroization circuitry.

Required Vendor Information

VE05.10.01: The vendor documentation shall state which of the three approaches specified in AS05.10 are used to meet the requirement, and provide supporting detailed design information. Depending on this choice, the corresponding vendor requirement (one of the following, respectively) must be met:

1. The multi-chip circuitry of the module shall be completely covered with a hard, opaque potting material. The potting material may be a hard, opaque epoxy, or another type of material providing an equivalent level of protection. The material shall be opaque within the visible spectrum.

2. The module shall be entirely contained within a strong nonremovable enclosure. The enclosure shall be designed such that attempts to remove or penetrate it will have a high probability of causing serious damage to the module (i.e., the module does not function).

3. The module shall be entirely enclosed within a strong removable cover and shall include tamper response and zeroization circuitry. The circuitry shall continuously monitor the cover, and upon the removal of the cover, shall immediately actively zeroize all plaintext cryptographic keys and other unprotected critical security parameters. The circuitry shall be operational whenever plaintext cryptographic keys, or other unprotected critical security parameters, are contained within the module.

Required Test Procedures

TE05.10.01: The tester shall verify that the vendor documentation specifies which requirements option in VE05.10.01 is to be met, and provides any necessary supporting documentation with details of the design approach. If this is not true, the tester shall obtain the necessary information from the vendor before proceeding with the validation. Depending on the requirement option chosen by the vendor, one of the following three tester requirements (TE05.10.02 through TE05.10.04) shall also be verified.

TE05.10.02: Option 1: Utilize a hard, opaque potting material. The tester shall verify by inspection

and from vendor documentation that the module is covered with a hard opaque potting material. The documentation should specify exactly which potting material is used; if it is not hard epoxy, then supporting documentation should be provided to show that its hardness is roughly equivalent to epoxy. The tester shall verify, by scratching the potting material with a sharp object, that it can not be easily penetrated to the depth of the underlying circuitry. The tester must verify that the potting material completely covers the module and is visibly opaque when inspected with bright white light shining on and (if possible) against it. (Portions of this verification may already have been performed at level 2 in TE05.09.01.)

TE05.10.03: Option 2: Utilize a strong, nonremovable enclosure. The tester shall verify the strength and nonremovable properties of the module enclosure by inspection and from vendor documentation. The tester shall also determine by test that this requirement is met. This can be verified in one or both of the following two ways:

1. By supervising tests at a vendor facility

2. By performing tests at the tester's own facility

Whichever approach is chosen, the tester shall verify that all of the following tests were performed or reported, to the extent possible: The tester (tester or vendor) set up the module in an operational state, and verified that it is performing normally. The tester then attempted to pry the enclosure from the module with a sharp object and to damage it via the manual application of force with a sharp object, to expose the underlying circuitry. The tester verified that this is impossible with a reasonable application of force, or that the module ceased to function (e.g., ceased to provide normal output, entered a non-operational state, or provided other clear evidence of failure as appropriate), or that the module circuitry was obviously physically destroyed.

TE05.10.04: Option 3: Utilize a strong removable cover with tamper response/zeroization. The tester shall verify from vendor design data that the module includes arrangements to zeroize all critical security parameters described in VE05.10.01 when the cover is removed, for example using tamper switches, motion detectors, etc. (Zeroization is defined in TE02.07.02.) The tester shall determine the strength of the cover by attempting to damage it via the manual application of force with a sharp object and verifying that the cover is not easily breached. The tester shall then set up the module in an operational state that requires intact crypto-variables and verify that it is performing normally. The tester shall remove the cover and verify that the module immediately ceases to function (e.g., ceases to provide normal output, enters a non-operational state, or provides other clear evidence of operational failure as appropriate). The tester shall then replace the cover, obtain a status report if the module has that capability, and determine that the module no longer contains critical security material and does not function until reset or rekeyed.

If the module can retain critical security parameters while powered down or deactivated, the tester shall verify that a deactivated module is tamper-protected: The tester shall load critical security parameters, deactivate the module, and remove a cover. The tester shall then replace the cover,

reactivate the module if possible, and determine that it no longer contains critical security material. The tester shall also verify from vendor documentation that the module would retain power to zeroize after deactivation for the maximum time commensurate with its operational use.

AS05.11: For a multiple-chip embedded cryptographic module at security level 3 or higher, if the module has any ventilation openings, they shall be constructed to prevent undetected probing. (Multiple-chip embedded; 3 or 4)

Required Vendor Information

VE05.11.01: If the module is contained within a cover or enclosure and if the cover or enclosure contains any ventilation holes or slits, then they shall be small and 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

TE05.11.01: 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/enclosure. Any openings must be small (normally no more than about 1/16" wide at any point) and designed to make direct linear access to the interior impossible. Suitable mechanical design approaches could include placing at least one 90 degree bend in each ventilation path, placing a substantial blocking material slightly behind the opening, use of a strong mesh or grille behind the opening, or similar blocking techniques. Ventilation openings and any blocking material must either be strong enough to resist attempts to force access to the interior, or be constructed such that forced access would require obvious damage visible from the exterior.

AS05.12: For a multiple-chip, embedded cryptographic module at security level 4, the module shall be contained within a tamper detection envelope. (Multiple-chip embedded; 4)

Required Vendor Information

VE05.12.01: The contents of the module shall be completely contained within a tamper detection envelope that will detect tampering attacks against the potting material or cover. The vendor documentation shall describe the tamper detection envelope design.

Required Test Procedures

TE05.12.01: The tester shall verify from vendor design data and by inspection that the module contains a tamper detection envelope that forms a barrier completely surrounding the module components. This barrier must be designed such that any breach of it by means such as drilling, milling, grinding, or dissolving to access the module components inside can be detected by

monitoring components in the module. Suitable tamper-detection envelope design techniques could include use of a flexible mylar printed circuit with a serpentine geometric pattern of conductors, a wire-wound package, a nonflexible brittle circuit, or equivalent techniques, any of which would cause a detectable change (e.g., an open circuit) upon breaching. (TE05.13.01 contains related requirements for tamper response.)

AS05.13: For a multiple-chip, embedded cryptographic module at security level 4, the module shall contain tamper response and zeroization circuitry. (Multiple-chip embedded; 4)

Required Vendor Information

VE05.13.01: 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 immediately actively zeroize all plaintext cryptographic keys and other unprotected critical security parameters. The circuitry shall be operational whenever plaintext cryptographic keys, or other unprotected critical security parameters, are contained within the module. The vendor documentation shall describe the tamper response and zeroization design.

Required Test Procedures

TE05.13.01: The tester shall verify from vendor design data that the module contains tamper response and zeroization circuitry that must continuously monitor the tamper detection envelope (refer to TE05.12.01); detect any breaches by means such as drilling, milling, grinding or dissolving any portion of the envelope; and then immediately zeroize all critical security parameters described in VE05.13.01. (Zeroization is defined in TE02.07.02.) The tester shall also determine by test that this requirement is met. This can be verified in one or both of the following two ways:

1. By supervising tests at a vendor facility

2. By performing tests at the tester's own facility.

Whichever approach is chosen, the tester shall verify that all of the following tests were performed or reported, to the extent possible:

A. The tester (tester or vendor) set up the module in an operational state that required intact crypto-variables and verified that it was performing normally.

B. The tester then breached the tamper-detection envelope barrier by any convenient means, and verified that the module immediately ceased to function (e.g., ceased to provide normal output, entered a non-operational state, or provided other clear evidence of operational failure as appropriate).

C. The tester also noted if the module reported a key zeroization or other failure

at this point (if it has that capability).

D. If the module can retain critical security parameters while deactivated: the tester loaded critical security parameters, deactivated the module, breached the tamper-detection envelope, reactivated the module if possible, and determined that it no longer contained critical security material. The tester also verified from vendor documentation that the module would retain power to zeroize after deactivatation for the maximum time commensurate with its operational use.

AS05.14: For a multiple-chip, embedded cryptographic module at security level 4, the module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT). (Multiple-chip embedded; 4)

Required Vendor Information

VE05.14.01: (This requirement is identical to VE05.06.01.)

VE05.14.02: (This requirement is identical to VE05.06.02.)

VE05.14.03: (This requirement is identical to VE05.06.03.)

Required Test Procedures

TE05.14.01: (This requirement is identical to TE05.06.01.)

TE05.14.02: (This requirement is identical to TE05.06.02.)

AS05.15: For a multiple-chip, stand-alone cryptographic module at security level 1 or higher, the chips in the module shall be of production quality that shall include standard passivation techniques. (Multiple-chip stand-alone; 1, 2, 3, and 4)

Required Vendor Information

VE05.15.01: The chips in the multiple-chip, stand-alone module shall be standard production quality ICs, designed to meet at least typical commercial-grade specifications for power, temperature, reliability, shock/vibration, etc. In particular, the module shall use standard passivation techniques for the each chip. The vendor documentation shall describe the IC's quality. If any ICs are used which are not standard devices, their passivation design shall also be described.

Required Test Procedures

TE05.15.01: 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 at least typical commercial grade in regards to power and voltage ranges, temperature, reliability, and shock and vibration. This documentation may consist of data sheets, special documentation submitted for this validation effort, comparisons to other physically similar products, etc. If the tester can not determine the chip's quality from the submitted documentation, the vendor shall be required to provide additional information as needed.

TE05.15.02: The tester shall verify from vendor documentation that the chips in the module have a standard passivation applied to them. The passivation must be a sealing coat applied over the chip circuitry to protect it against environmental or other physical damage. It is sufficient for the documentation to show that chips are industry-standard parts from established manufacturers. If this is not true, the documentation must specify the exact passivation material and technique used; and if it is not a standard passivation, then must also provide information to indicate why it is at least equivalent to a standard passivation approach.

AS05.16: For a multiple-chip, standalone cryptographic module at security level 1 or higher, the circuitry within the module shall be implemented as a production-grade, multiple-chip embodiment. (Multiple-chip standalone; 1, 2, 3, and 4)

Required Vendor Information

VE05.16.01: The circuitry in the module shall be implemented as a typical production-grade, multiple-chip device, such as an IC printed circuit board or ICs on a ceramic substrate. The vendor documentation shall describe the production implementation of the module.

Required Test Procedures

TE05.16.01: The tester shall verify by inspection and from vendor documentation that the module has been implemented as a standard multiple-chip design, such as a circuit board, a multi-chip ceramic-substrate module, or a functionally-equivalent, multi-chip design. The vendor must either specify a typical, industry-standard design approach that was used; or if a unique approach is used, the vendor must provide design-and-test-data that shows that the module is equivalent in quality and function to a more traditional approach.

AS05.17: For a multiple-chip, standalone cryptographic module, at security level 1 or higher, the module shall be contained within an enclosure that may include removable covers or doors. (Multiple-chip standalone; 1, 2, 3, and 4)

Required Vendor Information

VE05.17.01: 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

TE05.17.01: The tester shall verify by observation and from vendor documentation that the module is contained within an enclosure that meets the following requirements:

1. The enclosure must completely surround and protect the entire module.

2. The enclosure material must be metal or hard plastic 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 has properties adequate for the application or equivalent to a commercial product.

4. The enclosure may have removable covers or doors. At security level 1, there are no protection requirements for these covers or doors, but the tester shall verify that they are at least firmly attached and closed under normal use.

AS05.18: For a multiple-chip, standalone cryptographic module at security level 2 or higher, the enclosure shall be opaque. (Multiple-chip standalone; 2, 3, and 4)

Required Vendor Information

VE05.18.01: The enclosure shall be opaque within the visible spectrum. The vendor documentation shall describe the enclosure's opacity characteristics.

Required Test Procedures

TE05.18.01: The tester shall verify by inspection that the enclosure is visibly opaque when inspected with bright white light shining on and (if possible) against it.

AS05.19: For a multiple-chip, standalone cryptographic module at security level 2 or higher, if the enclosure includes any removable covers or doors, then either they shall be locked with pick-resistant mechanical locks or they shall be protected via tamper-evident seals. (Multiple-chip standalone; 2, 3, and 4)

Required Vendor Information

VE05.19.01: 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 chosen tamper-protection approach.

Required Test Procedures

TE05.19.01: The tester shall determine whether the enclosure contains any removable covers or doors. If so, the tester shall verify that each cover and door meets at least 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 to unlock it. (For example, a logical key could be a number that must be entered at a keypad.) The tester shall attempt to open the locked cover or door without use of the key (including attempts to physically pry it open with an object such as a screwdriver) and determine that the door will not open without signs of damage being evident.

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 without leaving detectable signs.

AS05.20: For a multiple-chip, standalone cryptographic module at security level 3 or higher, one of the following two requirements shall apply to the module: (Multiple-chip standalone; 3 or 4)

- **The module shall be encapsulated within a hard opaque potting material.**

- **The module shall be contained within a strong enclosure that either has no removable elements or contains tamper response and zeroization circuitry.**

Required Vendor Information

VE05.20.01: The vendor documentation shall state which of the two approaches specified in AS05.20 are used to meet the requirement, and provide supporting detailed design information. Depending on this choice, the corresponding vendor requirement (one of the following, respectively) must be met:

1. The multi-chip embodiment of the circuitry within the module shall be completely encapsulated within a hard, opaque potting material. The potting material may be a hard, opaque epoxy, or another type of material providing an equivalent level of protection. 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 immediately actively zeroize all plaintext cryptographic keys and other unprotected critical security parameters. The circuitry shall be operational whenever plaintext cryptographic keys, or other unprotected critical security parameters, are contained within the module.

Required Test Procedures

TE05.20.01: The tester shall verify that the vendor documentation specifies which requirements option in VE05.20.01 is to be met and provides any necessary supporting documentation with details of the design approach. If this is not true, the tester shall obtain the necessary information from the vendor before proceeding with the validation. Depending on the requirement option chosen by the vendor, one or two of the following three tester requirements shall also be verified: TE05.20.02 if option 1 is chosen, or else TE05.20.03 plus possibly TE05.20.04 if option 2 is chosen.

TE05.20.02: Option 1: Utilize a hard, opaque potting material. The tester shall verify from vendor documentation and by inspection if internal access is possible (for example via a removable cover or door), that the circuitry within the module is encapsulated within a hard, opaque potting material. The documentation should specify exactly which potting material is used; if it is not hard epoxy, then supporting documentation should be provided to show that its hardness is roughly equivalent to epoxy. If access is possible, the tester shall verify, by scratching the potting material with a sharp object, that it cannot be easily penetrated to the depth of the underlying circuitry. If access is possible, the tester shall also verify that the potting material completely encapsulates the circuitry within the module and is visibly opaque when inspected with bright white light shining on and (if possible) against it.

TE05.20.03: Option 2: Utilize a strong enclosure. The tester shall determine the strength of the enclosure by attempting to damage it via the manual application of force with a sharp object and verifying that the cover is not easily breached. The tester shall verify by inspection and from vendor documentation that the enclosure cannot be removed (except for removable covers or doors that are covered in TE05.20.04.) The tester shall also determine by test that this requirement is met. This can be verified in one or both of the following two ways:

1. By supervising tests at a vendor facility

2. By performing tests at the tester's own facility

Whichever approach is chosen, the tester shall verify that all of the following tests were performed or

reported, to the extent possible: The tester (tester or vendor) set up the module in an operational state and verified that it was performing normally. Then the tester attempted to pry the enclosure from the module with a sharp object to expose the underlying circuitry. The tester verified that this was impossible with a reasonable application of force or that the module ceased to function (e.g., ceased to provide normal output, entered a non-operational state, or provided other clear evidence of failure as appropriate), or that the module circuitry was obviously physically destroyed.

TE05.20.04: If a strong enclosure is used (option 2), and it has removable covers or doors: The tester shall verify from vendor design data that the module includes arrangements to zeroize all critical security parameters described in VE05.20.01 when a cover or door is removed (for example using tamper switches, motion detectors, etc.) (Zeroization is defined in TE02.07.02.) The tester shall also set up the module in an operational state that requires intact crypto-variables, and verify that it is performing normally. The tester shall remove a cover or door and verify that the module immediately ceases to function (e.g., ceases to provide normal output, enters a non-operational state, or provides other clear evidence of operational failure as appropriate). The tester shall then replace the cover or door, obtain a status report if the module has that capability, determine that the module no longer contains critical security material, and does not function until reset or rekeyed.

If the module can retain critical security parameters while powered down or deactivated, the tester shall verify that a deactivated module is tamper-protected: The tester shall load critical security parameters, deactivate the module, and remove a cover. The tester shall then replace the cover, reactivate the module if possible, and determine that it no longer contains critical security material. The tester shall also verify from vendor documentation that the module would retain power to zeroize after deactivation for the maximum time commensurate with its operational use.

AS05.21: For a multiple-chip, standalone cryptographic module at security level 3 or higher, if the module has any ventilation openings, they shall be constructed to prevent undetected probing. (Multiple-chip, standalone; 3 or 4)

Required Vendor Information

VE05.21.01: If the enclosure contains any ventilation holes or slits, they shall be small and 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 ventilation holes, slits, or other openings, and if so, whether they are constructed to deter undetected probing inside the cover/enclosure. Any openings must be small (normally no more than about 1/16" wide at any point) and designed to make direct linear access to the interior impossible. Suitable mechanical design approaches could include placing at least one 90 degree bend in each ventilation path, placing a substantial blocking material slightly behind the opening, use of a strong

mesh or grille behind the opening, or similar blocking techniques. Ventilation openings and any blocking material must either be strong enough to resist attempts to force access to the interior, or be constructed such that forced access would require obvious damage visible from the exterior.

AS05.22: For a multiple-chip standalone cryptographic module at security level 4, the module shall provide a tamper-detection envelope. (Multiple-chip standalone; 4)

Required Vendor Information

VE05.22.01: The enclosure shall contain tamper detection mechanisms that provide a tamper-detection envelope, such as cover switches, motion detectors, or other tamper detection mechanisms which will detect tampering attacks against the potting material or cover. The vendor documentation shall describe the tamper detection envelope design.

Required Test Procedures

TE05.22.01: The tester shall verify from vendor design data and by inspection that the module enclosure contains tamper detection mechanisms, which must form a tamper-detection envelope completely protecting the module components. The mechanisms must be designed such that any breach of the enclosure, potting material, or cover by means such as drilling, milling, grinding or dissolving to access the module components inside can be detected by monitoring components in the module. Suitable tamper-detection envelope design techniques could include use of cover switches (e.g., micro-switches, magnetic Hall effect switches, permanent magnetic actuators, etc.), motion detectors (e.g., ultrasonic, infrared, or microwave), or other tamper detection mechanisms as described in TE05.12.01 (such as a flexible mylar printed circuit with a serpentine geometric pattern of conductors, a wire-wound package, a non-flexible brittle circuit, or equivalent techniques). Any of these techniques should cause a detectable change (e.g., an open circuit) when the tamper detection envelope is breached. (TE05.23.01 contains related requirements for tamper response.)

AS05.23: For a multiple-chip standalone, cryptographic module at security level 4, the module shall contain tamper response and zeroization circuitry. (Multiple-chip standalone; 4)

Required Vendor Information

VE05.23.01: 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 immediately actively zeroize all plaintext cryptographic keys, and other unprotected critical security parameters. The circuitry shall be operational whenever plaintext cryptographic keys, or other unprotected critical security parameters are contained within the module. The vendor documention shall describe the tamper response and zeroization design.

Required Test Procedures

TE05.23.01: The tester shall verify from vendor design data that the module contains tamper response and zeroization circuitry that must continuously monitor the tamper detection mechanisms (refer to TE05.22.01); detect any breaches by means such as drilling, milling, grinding or dissolving any portion of the enclosure potting material or cover; and then immediately zeroize all critical security parameters described in VE05.23.01. (Zeroization is defined in TE02.07.02.) The tester shall also determine by test that this requirement is met. This can be verified in one or both of the following two ways:

1. By supervising tests at a vendor facility

2. By performing tests at the tester's own facility.

Whichever approach is chosen, the tester shall verify that all of the following tests were performed or reported, to the extent possible:

A. The tester (tester or vendor) set up the module in an operational state that required intact crypto-variables and verified that it was performing normally.

B. The tester then breached the enclosure by any convenient means and verified that the module immediately ceased to function (e.g., ceased to provide normal output, entered a non-operational state, or provided other clear evidence of operational failure as appropriate).

C. The tester also noted if the module reported a key zeroization or other failure at this point (if it has that capability).

D. If the module can retain critical security parameters while deactivated: the tester loaded critical security parameters, deactivated the module, breached the tamper-detection envelope, reactivated the module if possible, and determined that it no longer contained critical security material. The tester also verified from vendor documentation that the module would retain power to zeroize after deactivatation for the maximum time commensurate with its operational use.

AS05.24: For a multiple-chip standalone cryptographic module at security level 4, the module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in section 4.5.4 of FIPS PUB 140-1. (Multiple-chip standalone; 4)

Required Vendor Information

VE05.24.01: (This requirement is identical to VE05.06.01.)

VE05.24.02: (This requirement is identical to VE05.06.02.)

VE05.24.03: (This requirement is identical to VE05.06.03.)

Required Test Procedures

TE05.24.01: (This requirement is identical to TE05.06.01.)

TE05.24.02: (This requirement is identical to TE05.06.02.)

6. SOFTWARE SECURITY

Note: *The following software security requirements shall apply to all software and firmware contained within a cryptographic module.*

These requirements do not apply to microcode or system software whose source code is not available to the module manufacturer. These requirements do not apply to any software or firmware that can be shown not to affect the security of the module.

AS06.01: Documentation shall identify any software or firmware that is excluded from the software security requirements and explain the rationale for the exclusion. (1, 2, 3, and 4)

Required Vendor Information

VE06.01.01: The vendor documentation requirement to satisfy this assertion is the same as VE01.06.01 and VE01.06.02 of this document.

Required Test Procedures

TE06.01.01: This requirement is tested under TE01.06.01 and TE01.06.02 of this document.

AS06.02: Documentation shall include a detailed description of the design of the software within the module (e.g., the finite state machine specification required in Section 4.4 of FIPS PUB 140-1). (1, 2, 3, and 4)

Required Vendor Information

VE06.02.01: The vendor shall provide detailed software design documentation. This documentation shall include, but in no way be limited to, the finite state machine model diagram(s) and description referred to in Section 4.4 of FIPS PUB 140-1. If the relationship between the finite state machine specification and the source code is not clear, the vendor shall provide additional documentation that describes the relationship between the finite state machine specification and the source code.

Required Test Procedures

TE06.02.01: The tester shall compare the software design documentation against the list of names of all the software and firmware modules, functions, and procedures (as documented in VE06.04.01) to verify that the relationship between the finite state machine specification and the source code can be determined.

AS06.03: Documentation shall include a detailed explanation of the correspondence between the design of the software and the cryptographic module security policy (i.e., the rules of operation as documented per the requirements of Section 4.1 of FIPS PUB 140-1. (1, 2, and 3)

Required Vendor Information

VE06.03.01: The vendor documentation shall contain a separate section or chapter describing, explicitly, how the software/firmware design corresponds to the security policy (rules of operation) of the cryptographic module.

Required Test Procedures

TE06.03.01: The tester shall review the vendor documentation for completeness and correctness in representing the security policy (rules of operation) of the cryptographic module. He or she must determine that each security rule is reflected in the design, and that the design faithfully implements the semantics of the rule. That is to say, the design shows that the rule will be invoked under those conditions, and only those conditions, expressed in the rule; and that once invoked, the system will correctly execute the rule (e.g., perform the proper check on the correct security attributes of the correct entities).

AS06.04: Documentation shall include a complete source code listing for all software contained within the module. (1, 2, 3, and 4)

Required Vendor Information

VE06.04.01: The vendor shall supply a list of the names of all the software and firmware modules, functions, and procedures contained in the cryptographic module. This list may be a list of entities used in the linking process to create executable program images.

VE06.04.02: The vendor shall supply an annotated source listing of each of the software and firmware modules, functions, and procedures contained in the cryptographic module as indicated in the software/firmware list supplied by the vendor.

Required Test Procedures

TE06.04.01: The tester shall use the list supplied by the vendor to make sure that he or she has a source listing for each software or firmware module, function, and procedure contained in the module. The source listings must contain listings of data structures (e.g., header or include files) as well as source code.

AS06.05: For each software module, software function and software procedure, the source code listing shall be annotated with comments that clearly depict the relationship of these software entities to the design of the software. (1, 2, 3, and 4)

Required Vendor Information

VE06.05.01: The vendor documentation requirement to satisfy this assertion is the same as VE06.04.02 for assertion AS06.04.

Required Test Procedures

TE06.05.01: The tester shall determine that each module, function, or procedure of software and firmware contains comments and that the relationship between the software entities and the design (as documented in VE06.02.01) is clear.

TE06.05.02: The tester shall read the comments of each module, function, and procedure to determine, in the tester's judgment, that they explain the structure and function of the module, function, or procedure. This shall include expected inputs, algorithms used in the module, control flow, and expected outputs from the module, function, or procedure.

AS06.06: All software within a cryptographic module shall be implemented using a high-level language, except that the limited use of low-level languages (e.g., assembly languages) is allowed when it is essential to the performance of the module or when a high-level language is not available. (3 and 4)

Required Vendor Information

VE06.06.01: The vendor shall identify each of the software modules that is not written in a high-level language and provide a rationale or justification for why the module is 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. In the case of a performance rationale, the rationale shall give the technical explanation of why the high-level language does not provide sufficient performance.

Required Test Procedures

TE06.06.01: The tester shall examine the source code for each of the software modules to determine which ones are written in assembler language. He or she must verify that there are no software modules written in assembler language that were not identified by the vendor in VE06.06.01.

TE06.06.02: The tester shall review the vendor-supplied rationale for each software module written in assembler language and make a judgment as to whether the rationale is convincing. If the rationale is not convincing, he or she shall ask the vendor for a more convincing rationale. If the vendor cannot provide a convincing rationale, the vendor must write the subject module in a high-level language.

AS06.07: Documentation shall include a specification of a formal model (i.e., a precise mathematical statement) of the cryptographic module security policy (i.e., the security rules

under which the module must operate) as documented per the requirements of Section 4.1 of FIPS PUB 140-1. 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. (4)

Note: *Examples include, but are not limited to, INAJO, GYPSY, VDM, Z, LOTOS, EHDM, and ESTELLE.*

Required Vendor Information

VE06.07.01: The vendor shall provide documentation of a formal model, specified in a formal specification language, of the security policy of the cryptographic module, as documented in AS01.07. The formal model shall include, at least, a list of elements of the model, the operations performed on these elements, and the security rules these operations must obey.

Required Test Procedures

TE06.07.01: The tester shall analyze the formal model to establish that it has the following properties:

1. That the statements of the formal model are written correctly (syntactically correct) in the vendor's chosen formal specification language.

2. That the formal model contains:

    a) a definition of a "secure" state (i.e., the security policy),

    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), and

    d) a formal proof that if the initial state of the module satisfies the definition of a "secure" state and if all assumptions required by the model hold, then all future states of the module will be secure.[1]

The definition of the cryptographic module security policy must cover all security-policy requirements given in FIPS PUB 140-1. Validation that the formal model corresponds to the cryptographic module's security policy is covered in assertion AS06.08.

---

[1]This definition has been derived from the definition of "Formal Security Policy Model," *Department of Defense Trusted Computer System Evaluation Criteria*, National Computer Security Center, DOD 5200.28-STD, December 1985.

The state transitions must be compatible with (and could, under some circumstances, coincide with), the finite state machine model required by Section 4.4 of FIPS PUB 140-1.

If the cryptographic module is sufficiently simple, it may be feasible for the state transitions constraints to coincide with the pre- and post-conditions required as part of the annotated source code. In this case, the required proof of correspondence between the software design and the formal model is directly included in the model itself.

Validation that the module's software design corresponds to the rules of operation in the formal model is covered in assertion AS06.10.

In the likely event that a state-machine model is used, the formal proof should establish that the system will (a) always be in a secure state, and (b) that state transitions obey appropriate policy requirements. Item (a) would ordinarily be proved by state induction, by showing that the initial state is secure and that each operation induces a new secure state, if applied in a secure state. Item (b) is proved by case analysis, by showing that each operation satisfies each state-transition constraint given in the policy.

The primary criteria for judging acceptability of a rigorous proof is its ability to inform and convince its reviewers. Proof modularity is essential both to successful review and to product maintenance. The proof should be constructed hierarchically in terms of lemmas that rest, ultimately, on axioms and commonly accepted facts of mathematics. Additional guidelines on clarity of presentation for security models may be found in Section 2.4 of [NCSC-TG-10][2].

AS06.08: Documentation shall include a detailed explanation (informal proof) of the correspondence between the formal model and the cryptographic module security policy. (4)

Required Vendor Information

VE06.08.01: The vendor documentation shall contain a separate section or chapter describing, explicitly, how the formal model corresponds to the security policy (rules of operation) of the cryptographic module.

Required Test Procedures

TE06.08.01: The tester shall review the vendor-supplied documentation (security policy, formal model, and the security-policy-to-formal-model correspondence documentation) for completeness and correctness in representing the security policy of the cryptographic module. He or she must determine that each rule contained in the security policy is reflected in the formal model, and that the formal model faithfully implements the semantics of the rule. That is to say, the formal model shows

[2][NCSC-TG-10]: *A Guide to Understanding Security Modeling in Trusted Systems*, National Computer Security Center, October 1992.

that the rule will be invoked under those conditions, and only those conditions, under which it is applied in the security policy; and that, once invoked, the formal model shows that it will correctly execute the rule.

Note: *The tester must review all three documents identified in TE06.08.01. The security policy and formal model may, in fact, correspond, while the correspondence document is wrong, or either the security policy or formal model may contain more, or less, or something different than the other document.*

AS06.09: For each software module, software function and software procedure, the source code listing shall be annotated with comments that clearly specify (1) the pre-conditions required upon entry into the module, function or procedure in order for it to execute correctly, and (2) the post-conditions expected to be true when execution of the module, function or procedure is complete. (4)

Note: *These conditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of the module, function or procedure.*

Note: *While a mechanically checked proof is not required, it shall be possible to prove from the pre- and post-conditions that a module, function or procedure is consistent with the formal model.*

Required Vendor Information

VE06.09.01: For level 4, the source code listings of all the software modules, functions, or procedures provided by the vendor in AS06.04 shall include, as comments, pre- and post-conditions as required in this assertion (AS06.09).

Required Test Procedures

TE06.09.01: The tester shall verify, by inspection, that each module, function, or procedure contained in the cryptographic module software contains pre- and post-conditions as specified in this assertion (AS06.09).

TE06.09.02: The tester shall examine the source code for each software module, function, and/or procedure contained within the cryptographic module. He or she shall determine, by analyzing the unit's internal logic, that the unit will produce the specified post-condition upon completion of its execution, if the specified pre-condition exists immediately prior to the unit's start of execution. The term "unit" here refers to a software module, function, or procedure.

AS06.10: Documentation shall include a detailed explanation (informal proof) of the correspondence between the software design (as reflected by the pre- and post-condition annotations) and the formal model. (4)

Required Vendor Information

VE06.10.01: The vendor documentation shall contain a separate section or chapter describing, explicitly, how the software design corresponds to the formal model of the cryptographic module. The correspondence shall be a mapping or equivalent from the operations and elements of the model to the software design.

Required Test Procedures

TE06.10.01: The tester shall review the vendor-supplied documentation (formal model, software design, and the formal-model-to-software-design documentation) for completeness and correctness. He or she must determine that each action or transition contained in the formal model is reflected in the design, and that the design faithfully implements the semantics of the action or rule. That is to say that the design shows that the action or transition will be invoked under those conditions, and only those conditions, under which it is invoked in the formal model, and that, once invoked, the system will correctly execute the action or transition, as expressed in the formal model.

Note: *The tester must review all three documents identified in TE06.10.01. The formal model and the software design may, in fact, correspond, while the correspondence document is wrong; or either the formal model or the software design may contain more, or less, or something different than the other document.*

7. OPERATING SYSTEM SECURITY

Note: *The operating system requirements in this section shall apply to a cryptographic module only if the module provides a means whereby an operator can load and execute software or firmware that was not included as part of the validation of the module.*

An example of a cryptographic module for which the operating system requirements apply is a cryptographic module which is a general purpose computer running cryptographic software as well as untrusted user-supplied software (e.g., a spreadsheet or word processing program). In this case, the hardware, operating system and cryptographic software are considered part of the cryptographic module, and hence, the operating system requirements apply.

AS07.01: All cryptographic software shall be installed only as executable code in order to discourage scrutiny and modification by users. (1, 2, 3, and 4)

Required Test Procedures

TE07.01.01: The tester shall check all the files stored on secondary storage and determine that there are no source code files for software modules, functions, or procedures contained on the secondary storage. This review shall involve some scrutiny of the contents of each file, since a source file could have any name.

AS07.02: A cryptographic mechanism using a FIPS approved authentication technique (e.g., the computation and verification of a data authentication code or NIST digital signature algorithm) shall be applied to the cryptographic software within the cryptographic module. This cryptographic mechanism requirement may be incorporated as part of Software/Firmware test if a FIPS approved authentication technique is employed for that test. (1, 2, 3, and 4)

Required Vendor Information

VE07.02.01: The vendor shall provide documentation that identifies the technique used to maintain the integrity of the cryptographic software and describe how the software integrity is verified.

Required Test Procedures

TE07.02.01: The tester shall review the documentation to determine that it is complete, correct, and of sufficient detail to allow the tester to understand the cryptographic mechanism.

TE07.02.02: The tester shall attempt to corrupt the cryptographic executable code in various ways in order to test the effectiveness of the implementation of the integrity-maintaining mechanism.

AS07.03: Use of the cryptographic module shall be limited to a single user at a time. (1)

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

Required Vendor Information

VE07.03.01: The vendor shall provide a description of the mechanism used to ensure that only one user at a time can use the module. Mechanisms to provide this enforcement include, but are not limited to, having only one terminal hooked up to the cryptographic module and only one user logged on at a time.

Required Test Procedures

TE07.03.01: The tester shall operate the cryptographic module in the manner described by the vendor in the operation's manual. While the module is in correct operation, the same or another tester shall attempt to use the module, circumventing the single-user enforcement mechanism.

AS07.04: Use of the cryptographic module shall be dedicated to the cryptographic process during the time the cryptographic process is in use. (1)

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

Required Vendor Information

VE07.04.01: The vendor shall provide a description of the mechanism used to ensure that no other process can be executed in the cryptographic module while the cryptographic process is in use.

Required Test Procedures

TE07.04.01: The tester shall perform cryptographic functions in the manner described by the vendor in the operation's manual. While the cryptographic functions are operating correctly, the same or another tester shall attempt to execute another process while the cryptographic process is in use. Examples of how the other executable software is made unrunnable during the performance of cryptographic functions are as follows:

1. That the cryptographic module can only execute one program at a time and, therefore, cannot execute other software while the cryptographic software is running. (It should not be possible to interrupt the cryptographic process, run it in the background, and start another process before the cryptographic process is complete.)

2. That the cryptographic software is invoked through a menu interface that prevents the operator from invoking other software while the cryptographic software is running.

AS07.05: All cryptographic software, cryptographic keys and other critical security parameters, and control and status information shall be under the control of an operating system that provides controlled access protection (i.e., C2 protection in accordance with the Trusted Computer System Evaluation Criteria (TCSEC) or FIPS approved equivalent). Only operating systems that have been evaluated by a NIST accredited evaluation authority and against a FIPS approved criteria shall be used. (2)

Note: *The discretionary access control mechanisms provided by a C2 or equivalent operating system shall be employed to protect all plaintext data, cryptographic software, cryptographic keys, authentication data, and other critical security parameters from unauthorized access, per the following requirements:*

Required Vendor Information

VE07.05.01: The vendor shall provide proof that the operating system controlling the cryptographic module has successfully passed evaluation for "controlled access protection" (C2 in the TCSEC or FIPS-approved equivalent) by a NIST-accredited evaluation authority and against a FIPS-approved criteria. Two ways a vendor may provide this proof are 1) to present the tester with a certificate from a NIST-accredited evaluation authority certifying that the operating system successfully passed an evaluation, or 2) to show that the operating system is listed on a FIPS-approved evaluated products list or equivalent as having passed an evaluation.

Required Test Procedures

TE07.05.01: The tester shall check that the evaluation authority identified in the proof evidence is a NIST-accredited evaluation authority. This may be accomplished by referring to NIST-supplied list of accredited evaluation authorities to see if the evaluation authority identified in the proof evidence is on that list.

TE07.05.02: The tester shall check that this operating system was, in fact, evaluated by this evaluation authority and that the evaluation authority used a FIPS-approved criteria in performing the evaluation.

AS07.06: The operating system shall provide the capability to specify a set of operators who can execute cryptographic program images contained on the cryptographic module's secondary storage. (2, 3, and 4)

Required Vendor Information

VE07.06.01: The vendor shall include in the installation procedures specific instructions on how, by employing the protection mechanisms provided by a controlled access operating system, one

can configure the cryptographic module to protect it from unauthorized execution of cryptographic program images contained on the module's secondary storage.

Required Test Procedures

TE07.06.01: The tester shall review the installation procedures provided by the vendor, and examine the actual configuration of the cryptographic module, to verify that the cryptographic module is indeed configured in accordance with these vendor's instructions to protect the cryptographic program images contained on the module's secondary storage from unauthorized execution.

TE07.06.02: The tester shall become an operator in the set who can execute the various types of cryptographic program images. He or she must verify that he or she can, in fact, execute them.

TE07.06.03: The tester shall become an operator who is not in the set who can execute the various types of cryptographic program images. He or she must verify that he or she can not, in fact, execute them.

AS07.07: The operating system shall provide the capability to specify a separate set of operators for each of the following cryptographic module software components, such that only elements within that component's set can modify (i.e., write, replace, delete) entities within that component: (2, 3, and 4)

- **cryptographic program images on secondary storage**
- **cryptographic data (e.g. cryptographic keys, audit data) stored on secondary storage**
- **cryptographic data (e.g. cryptographic keys, audit data) stored in computer memory**
- **other critical security parameters stored on secondary storage**
- **other critical security parameters contained in computer memory.**

Required Vendor Information

VE07.07.01: The vendor shall include in the installation procedures specific instructions on how, by employing the protection mechanisms provided by a controlled access operating system, one can configure the cryptographic module software components to protect them from unauthorized modification.

Required Test Procedures

TE07.07.01: The tester shall review the installation procedures provided by the vendor, and examine the actual configuration of the cryptographic module, to verify that the cryptographic module is indeed configured in accordance with the vendor's instructions to protect the cryptographic module software components from unauthorized modification.

TE07.07.02: The tester shall verify that it is possible to specify a distinct set of operators for each of the following components:

1. cryptographic program images on secondary storage

2. cryptographic data (e.g., cryptographic keys, audit data) stored on secondary storage

3. cryptographic data (e.g., cryptographic keys, audit data) stored in computer memory

4. other critical security parameters stored on secondary storage

5. other critical security parameters contained in computer memory

TE07.07.03: The tester shall become an operator in the set who can modify each of the types of cryptographic module software components. He or she must verify that he or she can, in fact, modify them.

TE07.07.04: The tester shall become an operator who is not in the set who can modify each of the types of cryptographic module software components. He or she must verify that he or she can not, in fact, modify them.

AS07.08: The operating system shall provide the capability to prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). Executing processes, in this case, means all non-operating system (i.e., all operator initiated) processes, cryptographic or not. (2, 3, and 4)

Required Vendor Information

VE07.08.01: The vendor shall include in the installation procedures specific instructions on how, by employing the protection mechanisms provided by a controlled access operating system, one can configure the system to protect executing cryptographic processes from unauthorized modification.

Required Test Procedures

TE07.08.01: The tester shall review the installation procedures provided by the vendor in VE07.08.01, and examine the actual configuration of the cryptographic module, to verify that the cryptographic module is indeed configured in accordance with the vendor's instructions to protect executing cryptographic processes from unauthorized modification.

TE07.08.02: The tester shall try to modify executing cryptographic processes. The tester shall construct a test process that attempts to modify cryptographic processes both within and outside its address space. He or she must verify that no operator or executing process can modify an executing cryptographic process.

AS07.09: The operating system shall provide the capability to specify a separate set of operators and cryptographic processes for each of the following cryptographic module software components, such that only elements within a given component's set can read entities within that component: (2, 3, and 4)

- **cryptographic data (e.g. cryptographic keys, audit data) stored on secondary storage**
- **cryptographic data (e.g. cryptographic keys, audit data) stored computer memory**
- **other critical security parameters stored on secondary storage**
- **other critical security parameters contained in computer memory**
- **plaintext data stored either within the module's memory or on secondary storage**

Required Vendor Information

VE07.09.01: The vendor shall include in the installation procedures specific instructions on how, by employing the protection mechanisms provided by a controlled access operating system, one can configure the cryptographic module software components to protect the them from being read by unauthorized operators or processes.

Required Test Procedures

TE07.09.01: The tester shall review the installation procedures provided by the vendor, and examine the actual configuration of the cryptographic module, to verify that the cryptographic module is indeed configured in accordance with the vendor's instructions to protect the cryptographic module software components from unauthorized reading.

TE07.09.02: The tester shall verify that it is possible to specify a distinct set of operators for each of the following components:

1. cryptographic program images on secondary storage

2. cryptographic data (e.g., cryptographic keys, audit data) stored on secondary storage

3. cryptographic data (e.g., cryptographic keys, audit data) stored in computer memory

4. other critical security parameters stored on secondary storage

5. other critical security parameters contained in computer memory

TE07.09.03: The tester shall become an operator in the set who can read each of the types of cryptographic module software components. He or she must verify that he or she can, in fact, read them. If the set consists only of cryptographic processes, the tester may use an operational cryptographic process to attempt to read the software components, or may construct a test process that has the same authorization as the operational processes within the set (e.g., be in the same group as the operational processes).

TE07.09.04: The tester shall become an operator who is not in the set who can read each of the types of cryptographic module software components. He or she must verify that he or she can not, in fact, modify them. The tester may also modify the authorizations of an operational cryptographic process and attempt to read the software components, or may construct a test process that does not have read authorization (e.g., is not in the same group as the operational processes).

AS07.10: The operating system shall provide the capability to prevent all operators and processes from reading the following cryptographic module software components: (2, 3, and 4)

- **cryptographic program images contained on secondary storage**

- **executing cryptographic program images**

Required Vendor Information

VE07.10.01: The vendor shall include in the installation procedures specific instructions on how, by employing the protection mechanisms provided by a controlled access operating system, one can configure the system to prevent all operators and processes from reading the software components identified in AS07.10.

Required Test Procedures

TE07.10.01: The tester shall review the installation procedures provided by the vendor in VE07.10.01, and examine the actual configuration of the cryptographic module, to verify that the cryptographic module is indeed configured in accordance with the vendor's instructions to prevent all operators and processes from reading the software components identified in AS07.10.

TE07.10.02: The tester shall try to read cryptographic program images contained on secondary storage and executing cryptographic program images. The tester shall construct a test process that attempts to read the cryptographic program images both within and outside its address space and on secondary storage. He or she must verify that no operator or executing process can read a cryptographic program image.

AS07.11: The operating system shall provide the capability to specify a set of operators who are authorized to enter cryptographic keys and other critical security parameters. (2, 3, and 4)

Required Vendor Information

VE07.11.01: The vendor shall include in the installation procedures specific instructions on how, by employing the protection mechanisms provided by a controlled access operating system, one can configure the cryptographic module to protect cryptographic keys and other critical security parameters from being entered by unauthorized operators.

Required Test Procedures

TE07.11.01: The tester shall review the installation procedures provided by the vendor, and examine the actual configuration of the cryptographic module, to verify that the cryptographic module is, indeed, configured in accordance with the vendor's instructions to protect cryptographic keys and other critical security parameters from being entered by unauthorized operators.

TE07.11.02: The tester shall become an operator in the set who can enter cryptographic keys and other critical security parameters. He or she must verify that he or she can, in fact, enter them.

TE07.11.03: The tester shall become an operator who is not in the set who can enter cryptographic keys and other critical security parameters. He or she must verify that he or she can not, in fact, enter them.

AS07.12: All cryptographic software, cryptographic keys and other critical security parameters, control and status information shall be labelled and under the control of an operating system that provides labelled protection (i.e., B1 protection in accordance with the Trusted Computer System Evaluation Criteria (TCSEC) or FIPS approved equivalent). Only operating systems that have been evaluated by a NIST accredited evaluation authority and against a FIPS approved criteria shall be used. (3)

Required Vendor Information

VE07.12.01: The vendor shall provide documentation that describes how the cryptographic software, cryptographic keys, other critical security parameters, and control and status information are labelled and how these labels prevent unauthorized disclosure and modification.

Note: *Operating systems that allow subjects to write to objects whose label strictly dominates the subject's label (i.e., write up) might not be able to prevent unauthorized modification.*

VE07.12.02: The vendor shall provide proof that the operating system that controls the cryptographic module has successfully passed evaluation for "labeled protection" (B1 in the TCSEC or FIPS-approved equivalent) by a NIST-accredited evaluation authority and against a FIPS-approved criteria. Two of the ways that a vendor may provide this proof are 1) to present the tester with a certificate from a NIST-accredited evaluation authority certifying that the operating system successfully passed an evaluation, or 2) to show that the operating system is listed on a FIPS-approved evaluated products list or equivalent as having passed an evaluation.

Required Test Procedures

TE07.12.01: The tester shall check that the operating system enforces labelling of cryptographic software, cryptographic keys, other critical security parameters, and control and status information in such a way that unauthorized disclosure and modification is prevented.

Note: *Operating systems that allow subjects to write to objects whose label strictly dominates the subject's label (i.e., write up) might not be able to prevent unauthorized modification.*

TE07.12.02: The tester shall check that the evaluation authority identified in the proof evidence is a NIST-accredited evaluation authority. This may be accomplished by referring to a NIST-supplied list accredited evaluation authorities to see if the evaluation authority identified in the proof evidence is on that list.

TE07.12.03: The tester shall check that this operating system was, in fact, evaluated by this evaluation authority; and that the evaluation authority used a FIPS-approved criteria in performing the evaluation.

AS07.13: All cryptographic keys, authentication data, other critical security parameters, control inputs and status outputs shall be communicated only via a trusted mechanism (e.g., a dedicated I/O port or a trusted path). (3 and 4)

Required Vendor Information

VE07.13.01: The vendor shall identify and describe the trusted path mechanism used by the cryptographic module to communicate cryptographic keys, authentication data, other critical security parameters, control inputs, and status outputs.

Required Test Procedures

TE07.13.01: For each input and output that AS07.13 requires to be communicated via the trusted mechanism, the tester shall demonstrate, by actual use, that the trusted mechanism can, in fact, be used to communicate such data.

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, on the other hand, 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.*

TE07.13.02: Through his or her knowledge of the design and implementation of the module, as well as knowledge of the operator documentation, the tester shall attempt, for each input or output identified in AS07.13, to enter or output the information via an untrusted mechanism (untrusted path or I/O port).

AS07.14: When a trusted path is used, the trusted computing base (TCB) of the operating system shall support the trusted path between itself and the operators for use when a positive TCB-to-operator connection is required. (3 and 4)

Required Test Procedures

TE07.14.01: By reviewing and analyzing the cryptographic module software design, any operating system design and documentation available, and vendor arguments, the tester shall determine that it is the TCB of the operating system that supports (provides and protects) the trusted path capability.

AS07.15: When a trusted path is used, communications via this trusted path shall be activated exclusively by an operator or the TCB and shall be logically isolated and unmistakably distinguishable from other paths. (3 and 4)

Required Test Procedures

TE07.15.01: Through his or her knowledge of the cryptographic module user documentation, the tester shall invoke the trusted path in accordance with the documentation guidance. Also, if the capability exists during the operation (normal or abnormal) of the cryptographic module, for the TCB to invoke the trusted path, the tester shall exercise (operate) the module in such a way as to cause the TCB to invoke the trusted path.

TE07.15.02: Through his or her knowledge of the cryptographic module design and documentation, the tester shall attempt to cause the trusted path to be invoked by non-TCB software (e.g., a user process or a cryptographic module software module that is not part of the operating system TCB).

TE07.15.03: The tester shall perform independent invocations of the trusted path to determine that it is unmistakably distinguishable from all other paths. He or she must invoke the trusted path as an operator, and also cause the TCB to invoke the trusted path, if possible. These tests are to be separate from the other trusted mechanism tests to force the tester to focus on the "unmistakably distinguishable" aspect of the trusted path feature. This test may require the tester to invoke (utilize) other paths (I/O ports) to perform various functions to convince him or herself that the trusted path is, indeed, unmistakably distinguishable from all other paths.

TE07.15.04: By reviewing and analyzing the cryptographic module software design, any operating system design and documentation available, and vendor arguments, the tester shall determine that the trusted path is logically isolated from all other paths.

AS07.16: The operating system shall provide the capability to audit the entry of cryptographic keys, other critical security parameters and control inputs and status outputs. (3 and 4)

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, no matter how well protected, as its audit log.*

Note: *It is also assumed that the assertion requires that each of the events identified in the assertion be auditable by the cryptographic module software. The cryptographic module software may have the capability for turning off auditing of one or all of the identified events, but they must all be potentially auditable. This assertion sets no requirement on which events must be audited by a given site.*

Note: *The operating system must have the capability to allow non-TCB processes to use (write to) the system audit log. This capability is not inherent (guaranteed) in a B1 system, or in a system evaluated at any class.*

Required Vendor Information

VE07.16.01: The vendor shall identify the mechanism whereby a non-TCB process can write records to the system's audit log.

VE07.16.02: The vendor shall identify all the events that are auditable by the cryptographic module software.

VE07.16.03: For each of the auditable events so identified, the vendor shall provide the types of information and its format for all information contained in the audit record for the event.

Note: *Both the format and type of information must be provided because the tester must have the capability to read and interpret the audit records for all cryptographic events audited in order to*

check it against the information that is claimed to be in the record.

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

Required Test Procedures

TE07.16.01: The tester shall review all of the actions that can be taken by users and the cryptographic officer and identify all of those that produce the events identified in AS07.16, namely the entry of cryptographic keys, other critical security parameters, and control inputs, or the output of status information.

TE07.16.02: The tester shall then compare the event list provided by the vendor in VE07.16.02 with the events he or she identified through independent analysis of the actions of the cryptographic module. If the vendor's event list does not contain all the events identified by the tester, the vendor and tester must discuss and come to agreement concerning all the events that meet the criteria of AS07.16.

TE07.16.03: The tester shall review the types of information contained in the audit records for each distinct event in the event list, to determine if all the necessary information is there. This information is provided by the vendor in VE07.16.03.

TE07.16.04: The tester shall exercise the cryptographic module, with the auditing capability turned on, performing all the actions that generate events that must be auditable. He or she will then review the system's audit log to determine first if all the events were, indeed, audited, and second that all the required information was contained in the resulting audit record.

Note: *TE07.16.04 may be satisfied in whole or in part by examining the audit log produced during other testing of the cryptographic module. It is only required that audit records be examined for all actions of the cryptographic module that produce events that must be audited, no matter when these actions were performed.*

AS07.17: All cryptographic software, cryptographic keys and other critical security parameters, control and status information shall be labelled and under the control of an operating system that provides structured protection (i.e., B2 protection in accordance with the Trusted Computer System Evaluation Criteria (TCSEC), or FIPS approved equivalent). Only operating systems that have been evaluated by a NIST accredited evaluation authority and against a FIPS approved criteria shall be used. (4)

Required Vendor Information

VE07.17.01: The vendor shall provide proof that the operating system controlling the cryptographic module has successfully passed evaluation for "structured protection" (B2 in the TCSEC or FIPS-

approved equivalent) by a NIST-accredited evaluation authority and against a FIPS-approved criteria. Two of the ways that a vendor may provide this proof are 1) to present the tester with a certificate from a NIST-accredited evaluation authority certifying that the operating system successfully passed an evaluation, or 2) to demonstrate that the operating system is listed on a FIPS-approved, evaluated products list, or equivalent, as having passed such an evaluation.

Required Test Procedures

TE07.17.01: The tester shall check that the evaluation authority identified in the proof evidence is a NIST-accredited evaluation authority. This may be accomplished by referring to a NIST-supplied list of accredited evaluation authorities to see if the evaluation authority identified in the proof evidence is on that list.

TE07.17.02: The tester shall check that this operating system was, in fact, evaluated by this evaluation authority; and that the evaluation authority used a FIPS-approved criteria in performing the evaluation.

8. CRYPTOGRAPHIC KEY MANAGEMENT

General

AS08.01: Documentation shall specify all aspects of key management for the cryptographic module. (1, 2, 3, and 4)

Required Vendor Information

VE08.01.01: The vendor documentation shall describe key management for the module. At a minimum, the documentation shall specify the following information:

1. Key material, such as:
    a. List all types of keys used by the module, both internally and externally generated
    b. Explain function of each key
    c. Specify format of all entered and output keys
    d. Discuss how all keys are protected
2. Key generation, such as:
    a. Describe the key-generation process
    b. Specify whether the key generation algorithm is FIPS-approved
    c. Specify which types of keys are generated
3. Key distribution, such as:
    a. Describe key distribution technique
    b. Indicate whether technique is FIPS-approved
    c. Indicate which types of keys must be distributed
4. Key entry and output, such as:
    a. Describe key entry procedures
    b. Describe key output procedures
    c. Indicate whether manual or electronic key entry is used
    d. Indicate whether manual or electronic key output is used
    e. Indicate which types of keys are manually entered or output
    f. Indicate which types of keys are electronically entered or output
    g. Indicate form in which keys are entered or output (plaintext, encrypted form, under split knowledge procedures)
    h. Indicate use of a manual key entry test for verification of entered keys

5. Key storage, such as:

    a. Indicate which types of keys are stored
    b. Indicate where they are stored
    c. Indicate the form in which they are stored (plaintext, encrypted form, under split knowledge procedures)

6. Key destruction, such as:

    a. Describe key destruction technique and mechanisms
    b. Indicate any restrictions on when the module can be zeroized
    c. Indicate which types of keys are zeroized and why
    d. Indicate which security parameters are zeroized and why
    e. Indicate which types of keys and security parameters are not zeroized and why

7. Key archiving, such as:

    a. Whether key archiving is used
    b. Describe key archiving technique
    c. Indicate which types of keys can be archived
    d. Indicate whether keys are encrypted for archiving

Required Test Procedures

TE08.01.01: The tester shall review the vendor documentation to verify that, at a minimum, the information specified in VE08.01.01 is included.

TE08.01.02: The tester shall perform tests in these categories as specified by AS08.04-AS08.20.

AS08.02: Secret keys and private keys shall be protected from unauthorized disclosure, modification and substitution. (1, 2, 3, and 4)

Required Vendor Information

VE08.02.01: The vendor documentation shall describe the protection of all secret and/or private keys internal to the module as required by item 1 under VE08.01.01. Protection shall include the implementation of mechanisms that protect against unauthorized disclosure, unauthorized modification, and unauthorized substitution.

Required Test Procedures

TE08.02.01: The tester shall check the vendor documentation that describes the protection of secret

and/or private keys. The tester shall verify that the documentation describes how these

keys will be protected from unauthorized disclosure, unauthorized modification, and unauthorized substitution. The tester shall verify that, for each threat, the following topics are addressed:

1. Mechanisms used to protect against the threat

2. Which keys are protected by the mechanisms

The mechanisms used may include, but not be limited to, the following:

A. Entry or output of the keys in encrypted form or under split knowledge procedures (unauthorized disclosure)

B. Use of a cryptographic checksum or some other mechanism that can detect modifications (unauthorized modification and substitution)

C. Physical controls (unauthorized disclosure, modification, and substitution)

D. Mechanisms that are part of the underlying operating system (unauthorized disclosure, modification, and substitution)

TE08.02.02: The tester shall perform the following tests:

1. Attempt to access (by circumventing the documented protection mechanisms) secret and private keys 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 the keys, the requirement is met.

2. Modify all secret and private keys 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 keys to be successfully loaded. The tester should also attempt to perform cryptographic operations using these keys; the module should not perform the operations, indicating that the keys were not loaded.

AS08.03: Public keys shall be protected against unauthorized modification and substitution. (1, 2, 3, and 4)

Required Vendor Information

VE08.03.01: If the module supports public keys, the vendor documentation shall describe the protection of all public keys as required by item 1 under VE08.01.01. Protection shall include the implementation of mechanisms that protect against unauthorized modification and substitution.

Required Test Procedures

TE08.03.01: If the module supports public keys, the tester shall verify that the vendor documentation describes how these keys will be protected from unauthorized modification and unauthorized substitution. The tester shall verify that, for each threat, the following topics are addressed:

1. Mechanisms used to protect against the threat

2. Which keys are protected by the mechanisms

The mechanisms used may include, but not be limited to, the following:

A. Use of a cryptographic checksum or some other mechanism that can detect modifications (unauthorized modification and substitution)

B. Physical controls (unauthorized modification and substitution)

C. Mechanisms that are part of the underlying operating system (unauthorized modification and substitution)

TE08.03.02: 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 should also attempt to perform cryptographic operations using these keys; the module should not perform the operations, indicating that the keys were not loaded.

Key Generation

AS08.04: A cryptographic module may optionally implement an internal key generation function. The module shall implement a FIPS-approved key generation algorithm. Documentation shall specify the FIPS-approved key generation algorithm that is implemented by the module. (1, 2, 3, and 4)

Required Vendor Information

VE08.04.01: See items 2a and 2b under VE08.01.01 for vendor documentation requirements. They include a description of the key generation process and the specification of the FIPS-approved key generation algorithm. The vendor shall also provide proof that the key generation algorithm is FIPS-approved. This proof shall consist of a validation certificate from a NIST-accredited laboratory asserting that the algorithm implemented in the module is a FIPS-approved algorithm. In the absence of a NIST-accredited laboratory that can validate the algorithm, the vendor organization shall provide a written affirmation asserting that the algorithm implemented in the module is a FIPS-approved algorithm.

Require Test Procedures

TE08.04.01: Verification of vendor documentation was performed under TE08.01.01. If the vendor cannot prove that the key generation algorithm is FIPS-approved or if the algorithm is not documented, the assertion fails. In addition, the tester shall verify that the implemented algorithm matches the specified FIPS-approved algorithm and that it is implemented correctly.

AS08.05: When a random number generator is used in the key generation process, all values shall be generated randomly or pseudo-randomly such that all possible combinations of bits and all possible values are equally likely to be generated. (1, 2, 3, and 4)

Required Vendor Information

VE08.05.01: If the module uses a random number generator, the vendor documentation of the key generation procedures specified in item 2 under VE08.02.01 shall also describe how the random number generator works.

Require Test Procedures

TE08.05.01: If the module uses a random number generator, the tester shall test the random or pseudo random number generator using one or more of the statistical and continuous random number generator tests specified in section 4.11 of FIPS PUB 140-1.

AS08.06: A seed key, if used, shall be entered in the same manner as cryptographic keys. (1, 2, 3, and 4)

Required Vendor Information

VE08.06.01: The key management documentation shall specify whether a seed key is used for key generation. If so, the key management documentation shall address entry of the seed key as well as of other keys.

Require Test Procedures

TE08.06.01: The tester shall review the vendor documentation to determine whether a seed key is used for key generation. If so, the tester shall also review the key management documentation and verify that entry of the seed key is addressed and is identical to the entry of a cryptographic key.

TE08.06.02: The tester shall enter a seed key and shall verify that the method used to enter it is consistent with the documented method.

AS08.07: Intermediate key generation states and values shall not be accessible outside of the module in plaintext or otherwise unprotected form. (1, 2, 3, and 4)

Required Vendor Information

VE08.07.01: Key generation can be considered as one of the user service states (see AS04.05). Intermediate key generation states are those states through which the module passes between initiation and completion of the key generation process. Intermediate key generation values are interim results from mathematical calculations which eventually result in a cryptographic key. The finite state machine model (see requirement 4, "Finite State Machine Model") should not include these states and should not output any intermediate key states or values. The key generation procedures should not allow any output during the key generation process unless those values are encrypted.

Required Test Procedures

TE08.07.01: The tester shall review the finite state machine model and shall verify that no states are defined between the initiation and the completion of the key generation process. The tester shall verify that intermediate values are not associated with either the initiation or completion states of the key generation process. The tester shall also check the key generation procedures and verify that any specified outputs are encrypted.

TE08.07.02: The tester shall generate a key and shall attempt to access cryptographic key values during the key generation process. The module should not display any intermediate values unless they are encrypted. The tester shall also observe the output interface of the module and shall verify that any output matches the documented output and therefore is not a plaintext intermediate value.

Key Distribution

AS08.08: Key distribution may be performed by manual methods, automated methods, or a combination of automated and manual methods. A cryptographic module shall implement FIPS-approved key distribution techniques (e.g., FIPS 171--Key Management Using ANSI X9.17). Until such time as a FIPS-approved public key-based key distribution technique is established, commercially available public key methods may be used. Documentation shall specify the key distribution techniques that are implemented by the module. (1, 2, 3, and 4)

Required Vendor Information

VE08.08.01: See items 3a and 3b under VE08.01.01 for vendor documentation requirements. These include a description of the key distribution technique and an indication of whether the technique is FIPS-approved. If the key distribution technique is FIPS-approved, the vendor shall provide proof in the form of a validation certificate issued by a NIST-accredited laboratory for the key distribution technique. In the absence of the certificate, the vendor organization shall provide written affirmation that the key distribution technique is FIPS-approved. If the key distribution technique is not FIPS-approved, the vendor documentation shall explicitly state this.

Required Test Procedures

TE08.08.01: Verification of vendor documentation was performed under TE08.01.01. The tester shall determine whether the key distribution techniques are FIPS-approved; if not, the tester shall verify from the vendor documentation that a commercial public key-based key distribution technique is used. In addition, the tester shall verify that the implemented techniques match the specified FIPS-approved techniques, and that they are implemented correctly.

Key Entry and Output

AS08.09: Manually distributed cryptographic keys may be entered into or output from a cryptographic module either by purely manual methods or by electronic methods. (1, 2, 3, and 4)

Required Vendor Information

VE08.09.01: See items 4a through 4f under VE08.01.01 for vendor documentation requirements.

VE08.09.02: In implementing key entry and output procedures and mechanisms, the vendor shall follow the following guidelines:

1. If purely manual methods are used for key entry or key output, they may be one or more of, but not limited to, the following:

    - Keyboard
    - Rotary switches
    - Thumbwheels
    - LCD displays

2. If electronic means are used for key entry or key output, they may be one or more of, but not limited to, the following:

    - Memory card/token (e.g., magnetic-striped cards, IC chip devices)
    - Smart card/token
    - Electronic key loader

Required Test Procedures

TE08.09.01: Verification of vendor documentation was performed under TE08.01.01. The vendor documentation should provide the required information on key entry and output procedures and the keys that are entered into and output by the module; if not, the assertion fails.

TE08.09.02: The tester shall enter and output each of the manually distributed keys and shall verify that they are entered and/or outputted according to the documentation.

AS08.10: Electronically distributed secret and private keys shall be entered and output in encrypted form. (1, 2, 3, and 4)

Required Vendor Information

VE08.10.01: The vendor documentation shall specify which types of keys are electronically distributed and the form in which electronically distributed keys are entered into and output from the module.

Required Test Procedures

TE08.10.01: If the module supports electronically distributed keys, the tester shall determine from the vendor documentation whether secret and private keys are electronically distributed. If so, the tester shall verify that the vendor documentation specifies that secret and private keys are entered and output only in encrypted form. If the documentation specifies that the keys are in any other form, the assertion fails.

TE08.10.02: The tester shall enter every electronically distributed secret and private key type and shall 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.

TE08.10.03: The tester shall output every electronically distributed secret and private key type and shall verify that the procedure used to output each key is in accordance with the documented procedure, including the form that the keys are in when they are output.

AS08.11: Manually entered cryptographic keys shall be verified during entry into a cryptographic module for accuracy using the manual key entry test specified in section 4.11.2. (1, 2, 3, and 4)

Required Vendor Information

VE08.11.01: See item 4h under VE08.01.01.01 for vendor documentation requirements.

Required Test Procedures

TE08.11.01: Verification of vendor documentation was performed under TE08.01.01. The results of the verification should indicate that the vendor documentation specifies that a manual key entry test is used to verify all manually entered keys; if not, the assertion fails.

TE08.11.02: The tester shall test the manual key entry test as documented in AS11.21. If the manual

key entry test does not match the one specified in AS11.21 and if the validation of AS11.21 fails, this assertion fails.

AS08.12: During key entry, keys and key components may be temporarily displayed to allow visual verification and to improve accuracy. When encrypted keys or key components are entered, the resulting plaintext secret or private keys shall not be displayed. (1, 2, 3, and 4)

Required Vendor Information

VE08.12.01: The documented key entry procedures shall allow, if necessary, the display of encrypted keys or key components during the key entry process, but shall preclude the display of plaintext secret or private keys that result from the entry of encrypted keys or key components.

Required Test Procedures

TE08.12.01: The tester shall review the documented key entry procedures and shall determine whether encrypted keys or key components can be displayed during the key entry process. If so, the tester shall verify that the display of plaintext secret or private keys resulting from the entry of encrypted keys or key components is not allowed during the key entry process.

TE08.12.02: The tester shall enter every cryptographic key and shall verify that the keys can be temporarily displayed. When entering encrypted keys or key components, the tester shall also monitor the output interface of the module to verify that any resulting key material which is displayed is encrypted.

AS08.13: A means shall be provided to ensure that a key entered into or output from a module is associated with the correct entities (i.e., person, group, or process) to which the key is assigned. (1, 2, 3, and 4)

Required Vendor Information

VE08.13.01: The documented key entry/output procedures shall describe the mechanisms or procedures used to ensure that each key will be associated with the correct entity.

Required Test Procedures

TE08.13.01: The tester shall review the documented key entry/output procedures and shall verify that the procedures address how an entered or output key will be associated with the correct entity. This association can consist of two components; one resides with the key and the other resides with the entity. These components are pairwise unique in that only the combination of a particular entity component with the correct key component will result in the correct association. These components can include, but not be limited to:

1. Key component, such as:

   - Keytag
   - Certificate
   - Key encrypted under a hash of the entity component

2. Entity component, such as:

   - Password
   - Personal Identification Number (PIN)
   - Possession of a physical key, token, or equivalent
   - Biometrics (e.g., fingerprint, retina scan, keystroke dynamics)

TE08.13.02: 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 one or more of 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.

AS08.14: For security levels 1 and 2, when manually distributed secret keys or private keys are entered into or output from a cryptographic module, they may be entered or output as plaintext keys. Optionally, the keys may be entered or output either as follows: (1 and 2)

(1) In encrypted form

(2) Under split knowledge procedures

Required Vendor Information

VE08.14.01: See item 4g under VE08.01 for vendor documentation requirement.

Required Test Procedures

TE08.14.01: Verification of the vendor documentation was performed under TE08.01.01. The results of the verification should indicate that the vendor documentation specifies the form in which all types of keys are entered and output.

TE08.14.02: The tester shall enter every manually distributed secret and private key and shall 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.

TE08.14.03: The tester shall output every manually distributed secret and private key and shall verify that the procedure used to output each key is in accordance with the documented procedure, including the form that the keys are in when they are output.

AS08.15: For Security Levels 3 and 4, manually distributed secret keys or private keys shall not be entered into or output from a cryptographic module in plaintext form. When manually distributed, secret keys or private keys are entered into or output from a cryptographic module, they shall be output or entered in either of the following ways: (3 and 4)

(1) In encrypted form

(2) Using split knowledge procedures (i.e., as two or more plaintext key components)

Required Vendor Information

VE08.15.01: See item 4g under VE08.01.01 for vendor documentation requirement.

Required Test Procedures

TE08.15.01: Verification of the vendor documentation was performed under TE08.01.01. The results of the verification should indicate that the vendor documentation specifies the form in which all types of keys are entered or output (e.g., encrypted, plaintext, under split knowledge procedures). The tester shall also check the vendor documentation to verify that entry or output in plaintext form is not specified for a secret or private key.

TE08.15.02: The tester shall enter every manually distributed secret and private key and shall 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.

TE08.15.03: The tester shall output every manually distributed secret and private key and shall verify that the procedure used to output each key is in accordance with the documented procedure, including the form that the keys are in when they are output.

AS08.16: When a manually distributed secret key or private key is entered or output under split knowledge procedures, the module shall provide the capability to separately authenticate the operator for each key component. Furthermore, the key components shall be entered directly into the cryptographic module or output directly from the cryptographic module (e.g., via a trusted path or directly attached cable) without traveling through any enclosing or

intervening systems where the components could be stored, combined, or otherwise processed. (3 and 4) A related assertion is AS02.14.

Required Vendor Information

VE08.16.01: If manually distributed secret or private keys are entered or output under split knowledge procedures, the vendor documentation shall specify, in the description of the key entry procedure, that the operator is separately authenticated for each key component.

VE08.16.02: The vendor requirement for the direct entry of the key components is covered under VE02.14.01.

Required Test Procedures

TE08.16.01: If manually distributed, secret or private keys are entered or output under split knowledge procedures, the tester shall check the vendor documentation to verify that operator authentication is specified for each key component.

TE08.16.02: In addition to performing the validation specified by TE08.14.02-03, 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.

TE08.16.03: Validation of the direct entry of the split knowledge key components was performed under TE02.14.01. If the tester finds that split key components are not directly entered into the module, the assertion fails.

Key Storage

AS08.17: When contained within a cryptographic module, secret and private keys may be stored in plaintext form. These plaintext keys shall not be accessible from outside the module. This assertion is related to assertion AS08.02. (1, 2, 3, and 4)

Required Vendor Information

VE08.17.01: See items 5a and 5c under VE08.01.01 for vendor documentation requirements.

VE08.17.02: The vendor documentation shall describe the protection of all secret and private keys internal to the module as specified in VE08.02.01. Protection shall include the implementation of mechanisms that protect against unauthorized disclosure, modification, and substitution.

Required Test Procedures

TE08.17.01: Verification of the vendor documentation specified in VE08.17.01 was performed under

TE08.01.01. The results of the verification should indicate that the vendor documentation specifies which types of keys are stored and the form in which they are stored (plaintext, encrypted form, or under split knowledge procedures). Specifically, the vendor documentation shall indicate whether plaintext secret and private keys are stored in plaintext form.

TE08.17.02: As specified in TE08.02.01 and TE08.02.02, the tester shall check the vendor documentation to verify that it includes the specification of protection mechanisms for all secret and private keys and descriptions of how the mechanisms will protect against unauthorized disclosure, modification and substitution.

TE08.17.03: By using unauthorized means, the tester shall perform the tests specified in TE08.02.03 that attempt to access plaintext secret and/or private keys which the documentation designates as being stored in plaintext form. Note that, at Levels 1 and 2, manually distributed secret and private keys can be output from the module in plaintext form (see AS08.14). If any of the tests fail, this assertion fails.

AS08.18: A means shall be provided to ensure that all keys are associated with the correct entities (i.e., person, group, or process) to which the keys are assigned. (1, 2, 3, and 4)

Required Vendor Information

VE08.18.01: Vendor documentation on key storage shall describe the mechanisms or procedures used to ensure that each key will be associated with the correct entity.

Required Test Procedures

TE08.18.01: The tester shall review the documentation on key storage and shall verify that the procedures address how a stored key will be associated with the correct entity. This association can consist of two components; one resides with the key and the other resides with the entity. These components are pairwise unique in that only the combination of a particular entity component with the correct key component will result in the correct association. These components can include, but not be limited to:

1. Key component, such as:

    - Keytag
    - Certificate
    - Key encrypted under a hash of the entity component

2. Entity component, such as:

    - Password
    - Personal Identification Number (PIN)

- Possession of a physical key, token, or equivalent
- Biometrics (e.g., fingerprint, retina scan, keystroke dynamics)

TE08.18.02: The tester shall alter the association of key and entity (e.g., swap keys that belong to two different entities). The tester shall then attempt to perform cryptographic functions as one of the entities and shall verify that these functions fail.

Key Destruction

AS08.19: A cryptographic module shall provide the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the module. Zeroization of cryptographic keys and other critical security parameters is not required if the keys and parameters are either encrypted or otherwise physically or logically protected (e.g., contained within an additional embedded FIPS PUB 140-1 cryptographic module. (1, 2, 3, and 4)

Required Vendor Information

VE08.19.01: See items 6 under VE08.01.01 for vendor documentation requirements.

Required Test Procedures

TE08.19.01: Verification of the vendor documentation was performed under TE08.01.01. The results of the verification should indicate that the vendor documentation describes the key destruction mechanism and specifies any restrictions on when the module can be zeroized, which keys and security parameters are zeroized, and which keys and security parameters are not zeroized. In addition, the tester shall verify that all other keys and parameters that are not zeroized by the zeroize command are encrypted or are physically or logically protected.

TE08.19.02: 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 keys that were stored in the module and that he or she can access. The tester shall verify that each key that could be accessed and used had been protected within the module and that every key that could not be accessed was stored in the module in plaintext form and was therefore zeroized.

Key Archiving

AS08.20: A cryptographic module optionally may output keys for archiving purposes. Key outputs for archiving shall be encrypted. (1, 2, 3, and 4)

Required Vendor Information

VE08.20.01: If the module supports key archiving, see items 7a through 7d under VE08.01.01 for vendor documentation requirements.

Required Test Procedures

TE08.20.01: Verification of the vendor documentation was performed under TE08.01.01. The results of the verification should indicate that the vendor documentation specifies whether key archiving is used, describes the key archiving technique, and specifies which types of keys can be archived and whether archived keys are encrypted.

TE08.20.02: The tester shall enter each key that can be archived and shall archive them. The tester shall compare the archived keys with the plaintext keys and shall verify that the archived keys are encrypted versions of the plaintext keys.

9. CRYPTOGRAPHIC ALGORITHMS

AS09.01: Cryptographic modules shall employ FIPS-approved cryptographic algorithms. (1, 2, 3, and 4)

Required Vendor Information

VE09.01.01: The vendor shall provide a NIST certificate that certifies that the cryptographic module uses FIPS-approved cryptographic algorithms, and that the implementation of these FIPS-approved cryptographic algorithms has been tested and passed NIST-approved procedures and tests at a NIST-accredited facility.

Note: *The vendor may also incorporate other (i.e., nonFIPS-approved) cryptographic algorithms in the cryptographic module.*

Required Test Procedures

TE09.01.01: The tester shall check to make sure that the vendor has provided a NIST certificate as described above.

10. ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY (EMI/EMC)

AS10.01: Radios shall meet all applicable FCC requirements. (1, 2, 3, and 4)

Required Vendor Information

VE10.01.01: The vendor shall provide an FCC certificate certifying that the cryptographic module radio meets all applicable FCC requirements.

Required Test Procedures

TE10.01.01: The tester shall check that the vendor has supplied the FCC certificate required under VE10.01.01.

AS10.02: A cryptographic module shall conform to the EMI/EMC requirements specified in FCC Part 15, Subpart J, Class A (i.e., for business use). (1 and 2)

Required Vendor Information

VE10.02.01: The vendor shall provide an FCC certificate certifying that the cryptographic module conforms to the EMI/EMC requirements specified in FCC Part 15, Subpart J, Class A.

Required Test Procedures

TE10.02.01: The tester shall check that the vendor has supplied the FCC certificate required under VE10.02.01.

AS10.03: A cryptographic module shall conform to the EMI/EMC requirements specified in FCC Part 15, Subpart J, Class B (i.e., for home use). (3 and 4)

Required Vendor Information

VE10.03.01: The vendor shall provide an FCC certificate certifying that the cryptographic module conforms to the EMI/EMC requirements specified in FCC Part 15, Subpart J, Class B.

Required Test Procedures

TE10.03.01: The tester shall check that the vendor has supplied the FCC certificate required under VE10.03.01.

11. SELF-TESTS

11.1. General

AS11.01: A cryptographic module shall be able to perform self-tests in order to ensure that the module is functioning properly. Certain self-tests shall be performed when the module is powered up (i.e., Power-Up Tests) and other self-tests shall be performed under various conditions, typically when a particular function or operation is performed (i.e., Conditional Tests). A module may optionally perform other self-tests in addition to the tests specified in this standard. (1, 2, 3, and 4)

Required Vendor Information

VE11.01.01: The vendor shall provide a list of all self-tests, both mandatory and optional, that the module can perform. This list shall include both power-up tests and conditional tests.

Required Test Procedures

TE11.01.01: The tester shall inspect the list of self-tests to verify that it includes the following:

1. Power-up tests

    - Cryptographic algorithm test
    - Software/firmware test
    - Critical functions test
    - Statistical random number generator tests (required at Levels 3 and 4)
    - Other self-tests which are performed at power-up and on demand

All of the power-up and conditional self-tests are defined in section 4.11 of the FIPS and will be explicitly defined later in the appropriate assertions.

2. Conditional tests

    - Pairwise consistency test (if the module generates public and private keys)
    - Software/firmware load test
    - Manual key entry test
    - Statistical random number generator test
    - Other conditional tests

TE11.01.02: Specific validation requirements for these self-tests are specified under AS11.05 through AS11.22. Note that, in general, power-up self-tests cannot be verified by actual testing because they involve internals of the module to which the tester would not have access, such as the cryptographic

algorithm. Causing the module to fail a particular self-test in order to verify that the correct failure indicator is output, for example, would be an appropriate test, but the module generally would not have a mechanism that would allow the tester to force it to fail. Therefore, the tester may have to resort to code and/or design review.

AS11.02: Whenever a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status interface. (1, 2, 3, and 4)

Required Vendor Information

VE11.02.01: 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

TE11.02.01: 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 machine model (see AS04.01) to verify that they agree.

TE11.02.02: By inspecting the code and/or design 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 machine model.

3. The module outputs an error indicator.

4. The error indicator is consistent with the documented error indicator.

TE11.02.03: If the module design and operating procedures allow it, 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 is failed.

AS11.03: The module shall not perform any cryptographic functions while in the error state and no data shall be output via the data output interface while the error condition exists. Related assertions are AS02.04 and AS04.07. (1, 2, 3, and 4)

Required Vendor Information

VE11.03.01: See VE02.04.01 for the vendor design requirement. Also, the vendor design shall ensure that cryptographic operations cannot be performed while the module is in the error state.

Required Test Procedures

TE11.03.01: Tester verification of the inhibition of output was performed under TE02.04.01, TE02.04.02, and TE04.07.01. The results of the verification should indicate that:

1. The vendor documentation shows that all data output via the data output interface is inhibited whenever the module is in an error state.

2. If testable, the module inhibits all data output when the module is in an error state.

TE11.03.02: The tester shall check that vendor documentation indicates 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

TE11.03.03: If the module design and operating procedures allow it, the tester shall put the module in an error state and verify that any cryptographic operations that the tester attempts to initiate are prevented.

AS11.04: Each possible error condition shall be documented along with the actions necessary to clear the error and resume normal operation (possibly including maintenance, servicing or repair of the module). (1, 2, 3, and 4)

Required Vendor Information

VE11.04.01: The vendor documentation shall provide for each error condition, its name, the events that can produce it, and the actions necessary to clear it and resume normal operation. Note that necessary action may include sending the module to the manufacturer for repair.

Required Test Procedures

TE11.04.01: The tester shall check that the information provided above is specified for each error condition.

TE11.04.02: If the module design and operating procedures allow it, 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.

11.2. Power-Up Tests

General

AS11.05: After a cryptographic module is powered up, the module shall enter the self-test state and perform at least the following tests: cryptographic algorithm test, software/firmware test, critical functions test and statistical random number generator tests. The module may optionally perform additional tests. (1, 2, 3, and 4)

Required Vendor Information

VE11.05.01: See VE11.01.01 for the vendor requirement. Note that the running of statistical random number generator tests at power up is required for Level 4 and optional for the other levels. Also, the vendor shall document any optional power-up self-tests.

Required Test Procedures

TE11.05.01: Verification of the documented list of power-up self-tests was performed under TE11.01. Verification that the module performs the self-tests as documented is done under validation requirements for AS11.10-AS11.18.

TE11.05.02: If the module design and operating procedures allow it, the tester shall perform all optional power-up self-tests and shall verify that they perform as documented. If the tester cannot perform tests on the self-tests to validate them, the tester shall review the code listing and/or design documentation to determine whether the optional self-tests have been implemented as documented. If the module has the capability of displaying which self-tests are running, the tester shall run the optional self-tests to verify that the module performs them.

AS11.06: The power-up tests shall not require operator intervention in order to run. (1, 2, 3, and 4)

Required Vendor Information

VE11.06.01: 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

TE11.06.01: To test that, upon power-up, the module performs the power-up self-tests without requiring any operator intervention, the tester shall power-up the module. If the tester must enter any inputs or perform any actions while the self-tests are running, the assertion fails.

TE11.06.02: To test that, upon command from an operator, the module performs the power-up self-tests without requiring any operator intervention, the tester shall command the module to perform the self-tests. If the tester must enter any inputs or perform any actions while the self-tests are running, the assertion fails.

AS11.07: If all of the power-up tests are passed successfully, such an indication shall be output via the "status output" interface. (1, 2, 3, and 4)

Required Vendor Information

VE11.07.01: The vendor shall document the indicator that the module outputs upon successful completion of all of the power-up self-tests.

Required Test Procedures

TE11.07.01: The tester shall check the vendor documentation and shall verify that it specifies an indicator that is output from the status output interface upon successful completion of all of the power-up self-tests.

TE11.07.02: To test the assertion, 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.

TE11.07.03: To test the assertion, the tester shall command the module to perform the self-tests and shall monitor the status output interface. The expected indicator from the status output interface should be consistent with the documented indicator.

AS11.08: All data output shall be inhibited when these tests are performed. A related assertion is AS02.04. (1, 2, 3, and 4)

Required Vendor Information

VE11.08.01: See VE02.04.02 for the vendor documentation requirement.

Required Test Procedures

TE11.08.01: Tester verification of the inhibition of output during self-tests was performed under TE02.04.03 and TE02.04.04. The results of the verification should indicate that:

1. The vendor documentation shows that all data output is inhibited when the module is in a self-test condition.

2. If testable, the module inhibits all data output when running a self-test.

AS11.09: The module shall provide a means to initiate the tests on demand for periodic testing of the module. (1, 2, 3, and 4)

Required Vendor Information

VE11.09.01: 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. Note that operator initiation of the statistical random number generator tests are optional for Levels 1 and 2.

Required Test Procedures

TE11.09.01: The tester shall inspect the vendor documentation to verify that initiation of self-tests on demand is specified for all of the power-up self-tests. Note that, for Levels 1 and 2, operator initiation of statistical random number generator tests is optional. The documentation shall also include what steps an operator must take in order to initiate the self-tests.

TE11.09.02: To test that the necessary steps to initiate the self-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 power-up self-tests. If the steps that the tester performs are not consistent with those in the documentation, the assertion is failed.

Cryptographic algorithm test

AS11.10: The cryptographic algorithms shall be tested by operating the algorithm on data for which the correct output is already known (i.e., a "known answer" test). The test is passed if the calculated output equals the previously generated output. (1, 2, 3, and 4)

Required Vendor Information

VE11.10.01: The vendor shall document the known answer test that should be performed for the cryptographic algorithm test.

Required Test Procedures

TE11.10.01: The tester shall inspect the vendor documentation to determine whether it includes the following steps for the cryptographic algorithm test:

1. Use of a known answer
2. Calculations that should equal the known answer
3. Comparison of the calculated answer against the known answer
4. Successful indication if calculated equals known, otherwise failure

TE11.10.02: By reviewing the code listing and/or design documentation and comparing it with the vendor documentation, the tester shall verify that the implementation of the known answer test is consistent with the vendor documentation.

AS11.11: A known answer test shall be run for each cryptographic function (e.g., encryption, decryption, authentication) that is implemented. (1, 2, 3, and 4)

Required Vendor Information

VE11.11.01: In the vendor documentation of the known answer test, the vendor shall indicate that all of the cryptographic functions are tested by the known answer test and shall list them.

Required Test Procedures

TE11.11.01: By checking the vendor documentation, the tester shall verify that a known answer test is associated with each cryptographic function. The list of cryptographic functions shall 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

TE11.11.02: By analyzing the code listing and/or design documentation, the tester shall verify that the implementation of the cryptographic algorithm test includes the initiation of known answer tests

for all of the cryptographic functions.

AS11.12: Message digest algorithms shall either have an independent known answer test or shall be included in the known answer test of the cryptographic algorithm in which they are included. (1, 2, 3, and 4)

Required Vendor Information

VE11.12.01: If the module implements message digest algorithms, the vendor shall specify which known answer test is used to test it.

Required Test Procedures

TE11.12.01: 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.

TE11.12.02: 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.

AS11.13: A cryptographic module may omit the cryptographic algorithm test if the module includes two independent cryptographic algorithm implementations whose output are continually compared in order to ensure the correct functioning of the cryptographic algorithm. Whenever the output of the two implementations are not equal, the module shall enter an error state and output an error indicator via the status interface. (1, 2, 3, and 4)

Required Vendor Information

VE11.13.01: 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 it.

Required Test Procedures

TE11.13.01: 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

TE11.13.02: 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.

TE11.13.03: Validation of whether the module enters the error state and outputs an error indicator upon failure of the self-test is performed under TE11.02.01, TE11.02.02, and TE11.02.03. If any of these tests fail, this assertion fails.

Software/firmware test

AS11.14: An error detection code (EDC) or FIPS-approved authentication technique (e.g. the computation and verification of a data authentication code or NIST digital signature algorithm) shall be calculated on and stored with all software and firmware residing in the module (e.g., within EEPROM and RAM). This error detection code, data authentication code, or digital signature shall then be verified when the power-up self-tests are run. (1, 2, 3, and 4)

Required Vendor Information

VE11.14.01: The vendor documentation shall specify whether an error detection code (EDC) or a FIPS-approved authentication technique (e.g., FIPS-approved data authentication code (DAC) or NIST digital signature) will be used to provide integrity for all resident software and firmware. If the module implements a FIPS-approved authentication technique, the vendor shall provide proof that shall consist of a validation certificate from a NIST-approved laboratory asserting that the authentication technique implemented in the module is FIPS-approved. In the absence of such a validation certificate, the vendor organization shall provide a written affirmation asserting that the authentication technique implemented in the module is FIPS-approved. The documentation shall describe the implemented integrity mechanism.

Required Test Procedures

TE11.14.01: The tester shall determine from the proof provided by the vendor whether the authentication technique implemented in the module is FIPS-approved. If the tester cannot determine this, the assertion fails.

TE11.14.02: 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

TE11.14.03: 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. The following example is the DES cipher-block chaining method for calculating DACs:

1. Divide software into 64-bit blocks

2. Compute the XOR of the first block and an initialization vector

3. Encrypt the result

4. XOR the encrypted result with the next block and encrypt

5. Repeat the XOR and encryption until the last block has been processed. The last block to be processed is the DAC.

TE11.14.04: If the module implements the NIST digital signature for software/firmware integrity, the tester shall verify that the vendor documentation of the software/firmware test includes the following:

1. Description of digital signature algorithm

2. Identification of software and firmware that is protected using digital signatures.

3. Calculation of digital signatures when the software and firmware is installed

4. Verification of the digital signature when the self-test is initiated

5. Failure of the self-test upon failure of the digital signature verification

TE11.14.05: By checking the code and/or design documentation, the tester shall verify that the implementation of the software/firmware test is consistent with either TE11.14.01, TE11.14.02, or TE11.14.03.

TE11.14.06: 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 which indicates that the software/firmware self-test failed, the assertion fails.

Critical functions test

AS11.15: All other functions that are critical to the secure operation of the module and can be tested as part of the power-up tests shall be tested. Documentation shall provide a complete specification of all critical functions and the nature of the power-up self-tests designed to test those functions. Other critical functions that are performed under certain specific conditions

are tested as part of the conditional tests. (1, 2, 3, and 4)

Required Vendor Information

VE11.15.01: Critical functions can be defined as those functions that could lead to the disclosure of plaintext information, including data and cryptographic keys, if they fail. Examples of critical functions include random/pseudo-random number generation, operation of the cryptographic algorithm, and cryptographic bypass.

VE11.15.02: The vendor shall provide a matrix of all critical functions. For each critical function, the vendor shall indicate:

1. Its purpose (e.g., why is it a "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

TE11.15.01: The tester shall review the vendor-supplied matrix that identifies 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

The critical functions must include, but not be limited to, random number generation and operation of the cryptographic algorithm. Optional critical functions, such as pseudo-random number generation and cryptographic bypass, must have critical functions tests only if they are implemented in the module.

TE11.15.02: By checking the code and/or design documentation, the tester shall verify that the module performs the specified self-tests for each critical function.

Statistical Random Number Generator Tests

AS11.16: Cryptographic modules that implement a random or pseudorandom number generator shall incorporate the capability to perform statistical tests for randomness. The four tests specified in FIPS PUB140-1 are recommended. However, alternative tests which provide equivalent or superior randomness checking may be substituted. If any of the tests fail, the module shall enter an error state. A related assertion is AS11.02. (3 and 4)

Required Vendor Information

VE11.16.01: If the module implements a random or pseudorandom number generator, the vendor documentation shall specify statistical tests for randomness. These tests are optional at Levels 1 and 2. The randomness tests implemented by the module can consist of, but are not limited to, all of the following tests that are recommended by section 4.11.1 of FIPS PUB 140-1:

1. Monobit Test

2. Poker Test

3. Runs Test

4. Long Run Test

Required Test Procedures

TE11.16.01: If the module implements a random or pseudorandom number generator, the tester shall check the vendor documentation to verify that statistical tests for randomness are specified if the module is meant to meet either Level 3 or Level 4; if the module is a Level 1 or 2 module, the statistical random number generator tests are optional.

TE11.16.02: The tester shall determine from the vendor documentation whether the statistical tests recommended in section 4.11.1 of FIPS PUB 140-1 are implemented by the module. 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 140-1 and that the module enters an error state if any of them fail. The specifications of the recommended tests are based on a single bit stream of 20,000 consecutive bits of output and are as follows:

1. Monobit Test

   - Count the number of ones in the 20,000 bit stream. Denote this quantity by X.

   - The test is passed if $9{,}654 < X < 10{,}346$.

2. Poker Test

   - Divide the 20,000 bit stream into 5,000 contiguous 4 bit segments. Count and store the number of occurrences of each of the 16 possible 4 bit values. Denote f(i) as the number of each 4 bit value i where $0 <= i <= 15$.

- Evaluate the following:

$$X = (16/5000) * (\sum_{i=0}^{15} [f(i)]^2) - 5000$$

- The test is passed if $1.03 < X < 57.4$.

3. Runs Test

- A run is defined as a maximal sequence of consecutive bits of either all ones or all zeros, which is part of the 20,000 bit sample stream. The incidences of runs (for both consecutive zeros and consecutive ones) of all lengths (>= 1) in the sample stream should be counted and stored.

- The test is passed if the number of runs that occurs (of length 1 through 6) is each within the corresponding interval specified below. This must hold for both the zeros and ones; that is, all 12 counts must lie in the specified interval. For the purpose of this test, runs of greater than 6 are considered to be of length 6.

Length of Run	**Required Interval**
1	2,267 - 2,733
2	1,079 - 1,421
3	502 - 748
4	223 - 402
5	90 - 223
6+	90 - 223

4. Long Run Test

- A long run is defined to be a run of length 34 or more (of either zeros or ones).

- On the sample of 20,000 bits, the test is passed if there are NO long runs.

TE11.16.03: If the module implements statistical tests other than those recommended in FIPS PUB 140-1, the tester shall determine from the vendor documentation whether they provide equivalent or superior randomness checking. If not, this assertion fails.

AS11.17: For Level 3, the statistical tests shall be callable upon demand. A related assertion is AS11.09. (3)

Required Vendor Information

VE11.17.01: See VE11.09.01 for the vendor documentation requirement for tests that can be initiated by the operator.

Required Test Procedures

TE11.17.01: Verification of the vendor documentation and the ability to initiate the tests upon demand was performed under TE11.09.01-02. If the statistical tests cannot be initiated from at least one authorized role upon demand, this assertion fails.

AS11.18: For Level 4, the statistical tests shall be performed at power-up and shall also be callable upon demand. Related assertions are AS11.05 and AS11.09. (4)

Required Vendor Information

VE11.18.01: See VE11.05.01 for the vendor requirement that statistical tests be performed at power-up. See VE11.09.01 for the vendor requirement that these tests be callable upon demand by an operator.

Required Test Procedures

TE11.18.01: Verification of the vendor documentation was performed under TE11.05.01 and TE11.09.01. Verification that the tests are performed at power-up was performed under TE11.05.02. Verification that the tests can be initiated on demand by an operator was performed under TE11.09.02. If either of the verifications fail, this assertion fails.

11.3. Conditional Tests

Pairwise consistency test

AS11.19: Cryptographic modules that generate public and private keys shall test the keys for pairwise consistency. If the keys are to be used only for the calculation and verification of digital signatures, then the consistency of the keys shall be tested by the calculation and verification of a signature. (1, 2, 3, and 4)

Required Vendor Information

VE11.19.01: If the module generates public and private keys, the vendor documentation shall describe how the keys are used by the module. If the keys are used for encryption/decryption, the documentation shall describe a pairwise consistency test that is based on encryption/decryption. If the keys are used for the calculation and verification of digital signatures, either in addition to or in lieu of being used for encryption/decryption, the documentation shall describe a pairwise consistency test which is based on the calculation and verification of a digital signature.

Required Test Procedures

TE11.19.01: The tester shall determine from the vendor documentation whether the module generates public and private keys. If so, the tester shall check that the documentation describes one or more pairwise consistency tests based on how the keys are used by the module (encryption/decryption, digital signatures, or both).

TE11.19.02: If public and private keys are used for encryption/decryption, the tester shall verify that the implementation of the pairwise consistency check is consistent with the vendor documentation by checking the code and/or design documentation. In performing the verification, the tester shall consider the following example of a pairwise consistency test for keys that are used to perform inverse functions:

1. Apply the public key to a plaintext value.

2. Compare the result to the original plaintext; if they are the same, the test is failed.

3. Apply the private key to the ciphertext value.

4. Compare the result to the plaintext value; if they are not the same, the test is failed.

TE11.19.03: If public and private keys are used for the calculation and verification of digital signatures, the tester shall verify the implementation of the pairwise consistency check is consistent with the vendor documentation by checking the code and/or design documentation. In performing the verification, the tester shall consider the following example, based on the NIST Digital Signature Standard (DSS), of a pairwise consistency test for keys that are used to calculate and verify digital signatures:

1. Apply a secure hash algorithm to a message to create a message digest

2. Input the message digest and the private key into a digital signature algorithm to create the signature

3. Input the message digest, the public key, and the signature into the verification algorithm

4. The assertion is satisfied only if the verification succeeds

Software/firmware load test

AS11.20: A cryptographic mechanism using a FIPS-approved authentication technique (e.g., a data authentication code or NIST digital signature algorithm) shall be applied to all validated software and firmware that can be externally loaded into a cryptographic module. This test shall verify the data authentication code or digital signature whenever the software or firmware is externally loaded into the module. (1, 2, 3, and 4)

Required Vendor Information

VE11.20.01: The vendor documentation shall describe the FIPS-approved authentication technique used to protect the integrity of all externally loaded software and firmware. The vendor shall provide proof that the technique is FIPS-approved. This proof shall consist of a validation certificate from a NIST-approved laboratory asserting that the authentication technique implemented in the module is FIPS-approved. In the absence of the validation certificate, the vendor organization shall provide a written affirmation asserting that the authentication technique implemented in the module is FIPS-approved.

Required Test Procedures

TE11.20.01: The tester shall determine from the proof provided by the vendor whether the authentication technique implemented in the module is FIPS-approved. If the tester cannot determine this, the assertion fails.

TE11.20.02: If the module implements a DAC, the tester shall check the vendor documentation, code, and/or design documentation to verify that the software/firmware load test in the module fully implements the process by which the DAC is calculated and verified. The following example is the DES cipher-block chaining method for calculating DACs:

1. Divide software into 64-bit blocks

2. Compute the XOR of the first block and an initialization vector

3. Encrypt the result

4. XOR the encrypted result with the next block and encrypt

5. Repeat the XOR and encryption until the last block has been processed. The

last block to be processed is the DAC.

TE11.20.03: If the module implements the NIST digital signature for software/firmware integrity, the tester shall check the vendor documentation, code, and/or design documentation to verify that the software/firmware load test implemented in the module includes the following:

1. Description of digital signature algorithm

2. Identification of software and firmware that is protected using digital signatures.

3. Calculation of digital signatures when the software and firmware is installed

4. Verification of the digital signature when the self-test is initiated

5. Failure of the self-test upon failure of the digital signature verification

TE11.20.04: The tester shall modify the software, firmware, DAC, or digital signature associated with software/firmware that must be loaded, load the software/firmware, and verify that the module fails the self-test.

Manual key entry test

AS11.21: When cryptographic keys or key components are manually entered into a cryptographic module, the keys shall have an error detection code (e.g., a parity check value) or shall use duplicate entries in order to verify the accuracy of the entered keys. A cryptographic module shall verify the error detection code or duplicate entries and provide an indication of the success or failure of the entry process. (1, 2, 3, and 4)

Required Vendor Information

VE11.21.01: 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

VE11.21.02: If EDCs are associated with keys, then the vendor documentation that describes the format of the cryptographic keys (see AS08.01) shall include fields for the error detection codes.

Required Test Procedures

TE11.21.01: 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 addresses 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 AS08.01)

    - 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

TE11.21.02: For manual key entry tests using EDCs, 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 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.

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.

TE11.21.03: 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

AS11.22: Cryptographic modules that implement a random or pseudorandom number generator shall test the generator for failure to a constant value. If the generator produces blocks of n bits, where n > 15, the first block generated after power-up shall not be used, but shall be saved for comparison with the next block to be generated. Upon each subsequent generation, the newly generated block is compared with the previously generated block. The test fails if the two compared blocks are equal. If each call to the generator produces fewer than 16 bits, then the first n bits generated after power-up, 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 two compared n-bit sequences are equal. (1, 2, 3, and 4)

Required Vendor Information

VE11.22.01: If the module implements a random or pseudorandom number generator, the vendor shall document the continuous random number generator test.

Required Test Procedures

TE11.22.01: The tester shall determine whether the module implements a random or pseudorandom 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:

4. Storage of the first n bits, where n > 15, for comparison against the next n generated bits

5. Comparison of each subsequently generated n bits against the previously generated n bits

6. Failure of the test if two compared n-bit sequences are equal