FIPS PUB 140-3 (Revised DRAFT 09/11/09)

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Will Supersede FIPS PUB 140-2, 2001 May 25)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

U.S. Department of Commerce
Secretary Gary Locke

Technology Administration
Under Secretary for Technology

National Institute of Standards and Technology
Deputy Director Dr. Patrick D. Gallagher

FOREWORD

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to Standards and Guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002.

Comments concerning FIPS publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

Cita Furlani, Director
Information Technology Laboratory

Abstract

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security in its computer and telecommunication systems. This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106 and the Federal Information Security Management Act of 2002, Public Law 107-347. This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design, implementation, operation and disposal of a cryptographic module. These areas include cryptographic module specification; cryptographic module physical ports and logical interfaces; roles, authentication, and services; software security; operational environment; physical security; physical security – non-invasive attacks; sensitive security parameter management; self-tests; life-cycle assurance; and mitigation of other attacks.

Key words: computer security, telecommunication security, physical security, software security, cryptography, cryptographic modules, Federal Information Processing Standard (FIPS).

TABLE OF CONTENTS

1. OVERVIEW

This standard specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, (Public Law 104-106) and the Federal Information Security Management Act of 2002 (Public Law 107-347).

FIPS 140-1, first published in 1994, was developed by a government and industry working group composed of both operators and vendors. The working group identified requirements for four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and life protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Four security levels were specified for each of 11 requirement areas. Each security level offered an increase in security over the preceding level. These four increasing levels of security allowed cost-effective solutions that were appropriate for different degrees of data sensitivity and different application environments.

In 2001, FIPS 140-2 superseded FIPS 140-1. FIPS 140-2 incorporated changes in applicable standards and technology since the development of FIPS 140-1 as well as changes that were based on comments received from the vendor, laboratory, and user communities.

FIPS 140-3 adds new security features that reflect recent advances in technology and security methods. Software and firmware requirements are addressed in a new area dedicated to software and firmware security, and a new area specifying requirements to protect against non-invasive attacks is provided.

While the security requirements specified in this standard apply to a cryptographic module, conformance to this standard is not sufficient to ensure that a particular module is used or deployed in a manner to provide security or protection of information. The operator of a cryptographic module is responsible for ensuring that the security or features provided by the module is used in a manner that is sufficient and acceptable to the owner of the information that is being protected, and that any residual risk is acknowledged and accepted.

Similarly, the use of a cryptographic module in a computer or telecommunications system is not sufficient to ensure the security of the overall system. The overall security level of a cryptographic module must be chosen to provide a level of security appropriate for the security requirements of the application and environment in which the module is to be utilized as well as for the security services that the module is to provide. The responsible authority in each organization should ensure that their computer and telecommunication systems that utilize cryptographic modules provide an acceptable level of security for the given application and environment.

The importance of security awareness and of making information security a management priority should be communicated to all users, managers and system administrators. Since information security requirements vary for different applications, organizations should identify their information resources and determine the sensitivity to and the potential impact of losses. Controls should be based on the potential risks and should be selected from available controls, including administrative policies and procedures, physical and environmental controls, information and data controls, software development and acquisition controls, and backup and contingency planning.

The following sections provide an overview of the four security levels. Common examples, given to illustrate how the requirements might be met, are not intended to be restrictive or exhaustive.

The location of Annexes A, B, C, D, E, F and G, which are referenced herein, can be found in APPENDIX C of this standard, SELECTED BIBLIOGRAPHY.

1.1 Security Level 1

Security Level 1 provides a minimum set of assurance requirements. At a minimum, at least one Approved security function must be implemented in an Approved mode of operation. The module does not provide protection of Critical Security Parameters (CSPs) used or generated by the module.

Security Level 1 allows the software components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system. No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components.

Such implementations are ideally appropriate for security applications where controls, such as physical security, network security, and administrative procedures are provided outside of the module within the environment which it is to be deployed. For example, the implementation of Security Level 1 cryptographic module may be more cost-effective in such environments than corresponding modules at higher assurance levels which provide greater security of the modules CSPs, enabling organizations to select alternative cryptographic solutions to meet security requirements where attention to the environment the module is operating is crucial in providing overall security.

1.2 Security Level 2

Security Level 2 enhances the physical security mechanisms of a Security Level 1 cryptographic module by adding the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals, or for pick-resistant locks on removable covers or doors of the module. Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal must be broken to attain physical access to the Critical Security Parameters (CSPs) within the module. Tamper-evident seals or pick-resistant locks are placed on covers or doors to protect against unauthorized physical access.

Security Level 2 requires role-based authentication in which a cryptographic module authenticates and verifies the authorization of an operator to assume a specific role and to perform a corresponding set of services.

Security Level 2 allows a software cryptographic module to be executed in a modifiable environment that implements role-based access controls or, at the minimum, a discretionary access control with robust mechanism of defining new groups and assigning restrictive permissions through access control lists (ACLs), and with the capability of assigning each user to more than one group, and that protects against unauthorized execution, modification, and reading of cryptographic software.

1.3 Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 provides requirement to mitigate the unauthorized access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at direct physical access, and use or modification of the cryptographic module and probing through ventilation holes or slits. The physical security mechanisms may include the use of strong enclosures and tamper detection and response circuitry that zeroizes all plaintext CSPs when the removable covers or doors of the cryptographic module are opened.

Security Level 3 requires identity-based authentication mechanisms, enhancing the security provided by the role-based authentication mechanisms specified for Security Level 2. A cryptographic module authenticates the identity of an operator and verifies that the identified operator is authorized to assume a specific role and perform a corresponding set of services.

Security Level 3 requires that the entry or output of CSPs (including the entry or output of CSPs using split knowledge procedures) be performed using a Trusted Channel either via ports that are physically separated from other ports, or via interfaces that are logically separated from other interfaces. CSPs may either be

entered into or output from the cryptographic module in encrypted form or using a split knowledge procedure. The implementation of a Trusted Channel protects plaintext CSPs and the software of the cryptographic module from other untrusted software that may be executing on the system and from spoofing by a remote system.

Security Level 3 addresses mitigation assurance requirements for non-invasive attacks.

If a module may operate in both an Approved and non-Approved mode, Security Level 3 requires an unambiguous indication when the module is in the Approved mode.

Security Level 3 is not offered in all sections of this standard for software cryptographic modules, therefore, the overall maximum security level achievable by software cryptographic modules is limited to Security Level 2.

Level 3 modules require additional life-cycle assurances, such as automated configuration management, detailed design, low-level testing, and operator authentication using vendor-provided authentication information.

1.4 Security Level 4

Security Level 4 provides the highest level of security in the standard. This level includes all the appropriate security features of the lower levels, as well as extended features.

At Security Level 4, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a high probability of being detected, resulting in the immediate zeroization of all plaintext CSPs. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 introduces the multi-factor authentication requirement for operator authentication. At minimum, this requires two of the following three attributes:

- something known, such as a secret password,
- something possessed, such as a physical key or token,
- a physical property, such as a biometric.

Security Level 4 also protects a cryptographic module against a security compromise due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. A cryptographic module is required to either include special environmental protection features designed to detect fluctuations and zeroize CSPs, or to undergo environmental failure testing to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

Security Level 4 modules require the protection of CSPs against non-invasive attacks based on testing to a set of defined metrics.

Security Level 4 is not offered in all sections of this standard for software cryptographic modules, therefore, the overall maximum security level achievable by software cryptographic modules is limited to Security Level 2.

The design of a Level 4 module is verified by an informal proof of correspondence between both pre- and post-conditions and the functional specification.

2. GLOSSARY OF TERMS AND ACRONYMS

2.1 Glossary of Terms

The following definitions are tailored for use in this standard:

Administrator guidance: written material that is used by the Crypto Officer and/or other administrative roles for the correct configuration, maintenance, and administration of the cryptographic module. The *administrator guidance* contains information and procedures for administering the cryptographic module in a secure manner.

Allowed: NIST allowed or permitted.

Allowed security function: a security function that is allowed in an Approved mode of operation and specified in Annex B.

Approved: FIPS-Approved and/or NIST-recommended.

Approved cryptographic module: a cryptographic module that has been tested and validated by a validation authority.

Approved data authentication technique: an Approved method that may include the use of a digital signature, message authentication code or keyed hash (e.g. HMAC).

Approved integrity technique: an Approved hash, message authentication code or a digital signature algorithm.

Approved mode of operation: a mode of the cryptographic module that employs only Approved or Allowed security functions (not to be confused with a specific mode of an Approved security function, e.g., AES CCM mode).

Approved security function: a security function (e.g., cryptographic algorithm) that is specified in Annex A.

Bypass Capability: the ability of a service to partially or wholly circumvent a cryptographic function.

Compromise: the unauthorized disclosure, modification, substitution, or use of sensitive data or an unauthorized breach of physical security.

Conditional Self-Test: a test performed by a cryptographic module when the conditions specified for the test occur.

Confidentiality: the property that sensitive information is not made available or disclosed to unauthorized individuals, entities, or processes.

Configuration Management System (CMS): the management of security features and assurances through control of changes made to hardware, software and documentation of a cryptographic module.

Control information: information that is entered into a cryptographic module for the purposes of directing the operation of the module.

Critical Security Parameter (CSP): any security-related secret information (e.g., secret and private cryptographic keys, a shared secret, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic module.

Crypto Officer: an operator or process (subject), acting on behalf of the operator, performing cryptographic initialization or management functions.

Cryptographic algorithm: a well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output.

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

Cryptographic hash function: a computationally efficient function mapping binary strings of arbitrary length to binary strings of fixed length, such that it is computationally infeasible to find two distinct values that hash into a common value.

Cryptographic key: *(key*) a parameter used in conjunction with a cryptographic algorithm that determines such operations as:

- the transformation of plaintext data into ciphertext data,
- the transformation of ciphertext data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data,
- an authentication code computed from data, or
- an exchange agreement of a shared secret.

Cryptographic key component (key component): a parameter used in conjunction with other key components in an Approved or Allowed security function to form a plaintext cryptographic key or perform a cryptographic function.

Cryptographic module (module): a set of hardware, software and/or firmware that implements Approved or Allowed security functions (e.g. cryptographic algorithms and key establishment) and encompasses the cryptographic boundary.

Cryptographic module Security Policy: a description of how the specific module meets the security requirements of the standard, including the rules derived from the requirements of this standard and additional rules imposed by the vendor. (See Appendix B.)

Cryptographically protected CSP: a CSP that is cryptographically protected against unauthorized disclosure, modification and substitution and for which the protection mechanism's strength rationale relies only on Approved or Allowed security functions.

Cryptographically protected PSP: a PSP that is cryptographically protected against unauthorized modification and substitution and for which the protection mechanism's strength rationale relies only on Approved or Allowed security functions.

Cryptographically protected SSP: either a Cryptographically protected CSP or a Cryptographically protected PSP.

Data path: the physical or logical route over which data passes; (a physical data path may be shared by multiple logical data paths.)

Digital signature: the result of a cryptographic transformation of data which, when properly implemented, provides the services of:

- origin authentication,
- data integrity, and
- signer non-repudiation

*Electromagnetic emanations (EME)***:** an intelligence-bearing signal, which, if intercepted and analyzed, potentially discloses the information that is transmitted, received, handled, or otherwise processed by any information-processing equipment.

Electronic Key Entry: the entry of cryptographic keys into a cryptographic module using electronic methods such as a smart card or a key-loading device. (The operator entering the key may have no knowledge of the value of the key being entered.)

Electronic key transport: a transport mechanism of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key transport/agreement protocols).

Electrostatic discharge (ESD): a sudden and momentary electric current that flows when an excess of electric charge, stored on an electrically insulated object, finds a path to an object at a different electrical potential (such as ground).

Encrypted key: a cryptographic key that has been encrypted using an Approved or Allowed security function with a key encrypting key.

Entity: a person, a group, a device, or a process.

Entropy: the measure of the disorder, randomness or variability in a closed system. The entropy of a random variable *X* is a mathematical measure of the amount of information provided by an observation of *X*.

Environmental failure protection: the use of features to protect against a compromise of the security of a cryptographic module due to environmental conditions or fluctuations outside of the module's normal operating range.

Environmental failure testing: the use of specific test methods to provide reasonable assurance that the security of a cryptographic module will not be compromised by environmental conditions or fluctuations outside of the module's normal operating range.

Error detection code (EDC): a code computed from data and comprised of redundant bits of information designed to detect, but not correct, unintentional changes in the data.

Executable form: a form of the code in which the software or firmware is managed and controlled completely by the operational environment of the module.

Finite state model (FSM): a mathematical model of a sequential machine that is comprised of a finite set of input events, a finite set of output events, a finite set of states, a function that maps states and input to output, a function that maps states and inputs to states (a state transition function), and a specification that describes the initial state.

Firmware: for the purpose of this document, an encoded set or collection of computer instructions (referred to as code) that is designed to execute in a non-modifiable or limited environment.

Firmware module: a module that is composed solely of firmware.

Functional specification: a high-level description of the ports and interfaces visible to the operator and a high-level description of the behavior of the cryptographic module.

Functional testing: the testing of the cryptographic module functionality as defined by the Functional Specification.

Hard / hardness: the relative resistance of a metal or other material to denting, scratching, or bending; physically toughened; rugged, and durable. The relative resistances of the material to be penetrated by another object.

Hardware: the physical devices within the physical and/or cryptographic boundary used to process programs and data.

Hardware module: a module composed primarily of hardware, which may also contain firmware.

Hardware Module Interface (HMI): the total set of commands used to request the services of the hardware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

Hash value: the output of a cryptographic hash function.

Hybrid module: a module whose cryptographic functionality is contained in software or firmware, which also includes some special purpose hardware within the cryptographic boundary of the module.

Hybrid Firmware Module Interface (HFMI): the total set of commands used to request the services of the hybrid hardware/firmware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

Hybrid Software Module Interface (HSMI): the total set of commands used to request the services of the hybrid hardware/software module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

Initialization vector: a vector used in defining the starting point of a cryptographic process within a cryptographic algorithm.

Input data: information that is entered into a cryptographic module for the purposes of transformation or computation using an Approved or Allowed security function.

Integrity: the property that sensitive data has not been modified or deleted in an unauthorized manner without detection.

Interface: a logical entry or exit point of a cryptographic module that provides access to the module for logical information flows representing physical signals.

Key agreement: a key establishment procedure (either manual or electronic) where the resultant key is a function of information by two or more participants, so that no party can predetermine the value of the key independently of the other party's contribution.

Key encrypting key: a cryptographic key that is used for the encryption or decryption of other keys.

Key establishment: the process by which cryptographic keys are securely established among cryptographic modules using key transport and/or key agreement procedures.

Key loader: a self-contained unit that is capable of storing at least one plaintext or encrypted cryptographic key or key component that can be transferred, upon request, into a cryptographic module.

Key management: the activities involving the handling of cryptographic keys and other related security parameters (e.g., initialization vectors (IVs) and passwords) during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

Key transport: secure transport of cryptographic keys (CSPs) from one cryptographic entity to another entity.

Limited operational environment: an operational environment that, post validation, is designed to accept only controlled functional changes that successfully passed the Software/Firmware Load Test.

Logical protection: protection against unauthorized access (including unauthorized use, modification, substitution, and, in the case of CSPs, disclosure) by means of the Module Software Interface under operating system control. Logical protection of software SSPs does not protect against physical tampering.

Low-level testing: testing of the individual components or group of components of the cryptographic module and their physical ports and logical interfaces.

Maintenance Role: The Maintenance Role is a role assumed during the physical and/or logical maintenance services (e.g. opening service covers, performing certain diagnostics such as built in self-test (BIST)).

Manual key (SSP) entry: the entry of cryptographic keys into a cryptographic module, using devices such as a keyboard.

Message Authentication Code: a cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of data (example: a Hash Based Message Authentication Code.)

Microcode: the elementary processor instructions that correspond to an executable program instruction.

Minimum entropy: a lower bound of entropy that is useful in determining a worst-case estimate of sample entropy. For the purpose of this standard, the minimum entropy is considered to be the min-entropy as defined in NIST SP 800-90, "Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)", as amended.

Modifiable operational environment: an operational environment that is designed, post validation, to accept functional changes that may contain non-validated software.

Multi-factor authentication: authentication with at least two independent authentication factors. An authentication factor is a piece of information and process used to authenticate or verify the identity of a person. Independent authentication factor categories are: something you know, something you have, and something you are.

Multiple-chip embedded cryptographic module: a physical embodiment in which two or more integrated circuit chips are interconnected and are embedded within an enclosure or a product that may not be physically protected. (Example: adapters and expansion boards.)

Multiple-chip standalone cryptographic module: a physical embodiment in which two or more integrated circuit chips are interconnected and the entire enclosure is physically protected. (Example: encrypting routers or secure radios.)

Non-administrator guidance: written material that is used by the User and/or other non-administrative roles for operating the cryptographic module in an Approved mode of operation. The *non-administrator guidance* describes the security functions of the cryptographic module and contains information and procedures for the secure use of the cryptographic module, including instructions, guidelines, and warnings.

Non-invasive attack: an attack that can be performed on a cryptographic module without direct physical contact with components within the cryptographic boundary of the module.

Non-modifiable operational environment: an operational environment that contains only validated software and that is designed to not accept functional changes post validation.

Non-security relevant: Requirements that are not addressed within the scope of this standard.

Opaque: impenetrable by light (i.e., light within the visible spectrum of wavelength range of 400nm to 750nm); neither transparent nor translucent within the visible spectrum.

Operational environment: the set of all software and hardware required for the module to operate securely.

Operator: an individual accessing a cryptographic module or a process (subject) operating on behalf of the individual, regardless of the assumed role.

Output data: information that is produced from a cryptographic module.

Passivation: a process in the construction of semiconductor devices in which junctions, surfaces of components and integrated circuits are afforded a means of protection against the modification of circuit behavior.

Password: a string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Periodic Self-Tests: a suit of pre-conditional and conditional self-tests executed either upon operator's request (Security Levels 1 and 2) or repeated after a maximum operational time and in the conditions specified in the Security Policy (Security Level 3 and 4).

Personal Identification Number (PIN): a numeric code, used to authenticate an identity.

Physical protection: the safeguarding of a cryptographic module or its CSPs using physical means.

Plaintext key: an unencrypted cryptographic key.

Port: a physical entry or exit point of a cryptographic module that provides access to the module for physical signals represented by logical information flows (physically separated ports do not share the same physical pin or wire).

Pre-operational Self-Test: a test performed by a cryptographic module between the time a cryptographic module is powered on and the time that the cryptographic module uses a function or provides a service using the function being tested.

Private key: a cryptographic key, used with a public key cryptographic algorithm, that is uniquely associated with an entity and is not made public.

Production grade: industry standard manufacturing.

Public key: a cryptographic key used with a public key cryptographic algorithm that is uniquely associated with an entity and that may be made public. (Public keys are not considered CSPs.)

Public key certificate: a set of data that contains a unique identifier associated with an entity, contains the public key associated withy the identifier, and is digitally signed by a trusted party, thereby binding the public key to the identifier.

Public key (asymmetric) cryptographic algorithm: a cryptographic algorithm that uses two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible.

Public Security Parameter (PSP): any security-related public information whose modification can compromise the security of a cryptographic module.

Radiation hardening: improving the ability of a device or piece of equipment to withstand nuclear or other radiation; applies chiefly to dielectric and semiconductor materials.

Random Bit Generator (RBG): a device or algorithm that outputs a sequence of bits that appears to be statistically independent and unbiased.

Removable cover: a part of a cryptographic module's enclosure that permits physical access to the contents of the module.

Runtime environment: a runtime environment is a virtual machine state which provides software services for processes or programs while a computer is running. It may pertain to the operating system itself, or the software that runs beneath it. The primary purpose is to accomplish the objective of "platform independent" programming.

Secret (symmetric) key: a cryptographic key, used with a symmetric secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public.

Security Policy: see Cryptographic module Security Policy.

Seed key: a secret value used to initialize a cryptographic function or operation.

Sensitive Data: data that, in user's view, requires protection.

Sensitive Security Parameters (SSP): Critical Security Parameters and Public Security Parameters.

Service input: all data or control information utilized by the cryptographic module that initiates or obtains specific operations or functions.

Service output: all data and status information that results from operations or functions initiated or obtained by service input.

Service: any externally invoked operation and/or function that can be performed by a cryptographic module.

Single-chip cryptographic module: a physical embodiment in which a single integrated circuit (IC) chip may be used as a standalone device or may be embedded within an enclosure or a product that may not be physically protected. (Examples: single integrated circuit (IC) chips or smart cards with a single IC chip.)

Software: for the purpose of this document, an encoded set or collection of computer instructions (referred to as code) in a format that allows the code to satisfy this standard's requirements, and that is designed to execute in a modifiable operational environment.

Software module: a module that is composed solely of software.

Software/Firmware Load Test: a set of tests a software or firmware has to pass successfully before it can be loaded into the cryptographic module and executed.

Software/Firmware Module Interface (SFMI): a set of commands used to request the services of the software or firmware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

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

Status information: information that is output from a cryptographic module for the purposes of indicating certain operational characteristics or states of the module.

Strong: not easily defeated; having strength or power greater than average or expected; able to withstand attack; solidly built.

System software: the special software within the cryptographic boundary (e.g., operating system, compilers or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, and associated programs, and data.

Tamper detection: the automatic determination by a cryptographic module that an attempt has been made to compromise the physical security of the module.

Tamper evidence: the external indication that an attempt has been made to compromise the physical security of a cryptographic module. (The evidence of the tamper attempt should be observable by an operator subsequent to the attempt.)

Tamper response: the automatic action taken by a cryptographic module when a tamper attempt has been detected.

Temporary Key Values (TKV): any temporary variables or memory locations used to store intermediate SSP components during cryptographic calculations. These values include, but are not limited to, memory locations or variables used to store key schedule values, intermediate values of modular exponentiation operations, shared secrets and intermediate keyed digest values.

Trusted channel: a trusted and safe communication link established between the cryptographic module and the module's operator, generally established for the transport of the SSPs, data and other critical information shared by the cryptographic module and the other operator. A Trusted Channel exhibits a verification component that the operator or a module may use to confirm that the Trusted Channel exists. A Trusted Channel protects against eavesdropping, as well as physical or logical tampering by unwanted operators/entities, processes or other devices, both within the module and along the module's communication link with the intended endpoint (e.g., the Trusted Channel will not allow man-in-the-middle or replay types of attacks). A Trusted Channel may be of one of the following types:

- *Internal*: a communication link established between the cryptographic module and an operator that is entirely local, directly attached to the host system and has no intervening systems. In this case, it is generally assumed that the host operating system physically protects the transmission of the SSPs and other critical information, and no additional cryptographic protection is necessary.

- *External*: a communication link established between the cryptographic module and a remote communication endpoint. In this case, the Trusted Channel is intended to cryptographically protect the SSPs and other critical data, during entry and output, and does not allow misuse of any transitory SSPs. This type of Trusted Channel uses only Approved or Allowed security functions to establish the channel and transfer data.

Trusted Role: a state of the module, achieved only upon configuration by a Crypto Officer, where the module can perform cryptographic operations and other Approved or Allowed security functions without any outside entities authenticated to the module.

User: an individual or process (subject) acting on behalf of the individual that accesses a cryptographic module in order to obtain cryptographic services.

Validated: validated by the validation authority.

Validation authority: the entity that will validate the testing results for conformance to this standard.

Vendor: for the purpose of this standard, the vendor is the entity, group or association that submits the cryptographic module for validation.

Zeroization: a method of erasing electronically stored data to prevent the recovery of the data.

2.2 Acronyms

The following acronyms and abbreviations are used throughout this standard:

CBC	Cipher Block Chaining
CCM	Counter with Cipher block chaining-Message authentication code
CSP	Critical Security Parameter
ECB	Electronic Codebook
EDC	Error Detection Code
EFP	Environmental Failure Protection

EFT	Environmental Failure Testing
ESD	Electrostatic Discharge
FIPS	Federal Information Processing Standard
FSM	Finite State Model
HDL	Hardware Description Language
HFMI	Hybrid Firmware Module Interface
HMI	Hardware Module Interface
HSMI	Hybrid Software Module Interface
HMAC	Hash-Based Message Authentication Code
IC	Integrated Circuit
IV	Initialization Vector
KAT	Known Answer Test
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PSP	Public Security Parameters
RBG	Random Bit Generator
SFMI	Software/Firmware Module Interface
SSP	Sensitive Security Parameter
TKV	Temporary Key Value
URL	Uniform Resource Locator

3. FUNCTIONAL SECURITY OBJECTIVES

The security requirements specified in this standard relate to the secure design and implementation of a cryptographic module. The requirements are derived from the following high-level functional security objectives for a cryptographic module:

- To employ and correctly implement the Approved or Allowed security functions for the protection of sensitive information.
- To protect a cryptographic module from unauthorized operation or use.
- To prevent the unauthorized disclosure of the contents of the cryptographic module.
- To prevent the unauthorized and undetected modification of the cryptographic module and cryptographic algorithms, including the unauthorized modification, substitution, insertion, and deletion of SSPs.
- To provide indications of the operational state of the cryptographic module.
- To ensure that the cryptographic module performs properly when operating in an Approved mode of operation of the module.
- To detect errors in the operation of the cryptographic module and to prevent the compromise or the modification of sensitive data and SSPs resulting from these errors.
- To ensure the proper design, distribution and implementation of the cryptographic module.

4. SECURITY REQUIREMENTS

This section specifies the security requirements that **shall** be satisfied by cryptographic modules conforming to this standard. The security requirements cover areas related to the design, implementation, operation and disposal of a cryptographic module. These areas include cryptographic module specification; module ports and interfaces; roles, services, and authentication; software and firmware security; operational environment; physical security; security against non-invasive attacks; sensitive security parameter management; self-tests; and life-cycle assurance. An optional area concerned with the mitigation of other attacks cover areas where testing requirements will be available as metrics and tests methods are developed, but the vendor is required to document implemented controls. Table 1 summarizes the security requirements in each of these areas.

A cryptographic module **shall** be tested against the requirements of each area addressed in this section. The cryptographic module **shall** be independently rated in each area. In addition to receiving independent ratings for each of the security areas, a cryptographic module will also receive an overall rating. The overall rating will be set to the lowest rating received in the section ratings.

Each area provides for increasing levels of security with cumulative security requirements for each security level. In these areas, the cryptographic module will receive a rating that reflects the maximum security level for which the module fulfills all of the requirements of that area. In areas that do not provide for different levels of security (i.e., standard set of requirements), the area will receive a rating commensurate with the overall security level of the module.

All documentation, including copies of the user and installation manuals, **shall** be provided to the testing laboratory by the vendor. Many of the security requirements of this standard include specific documentation requirements that are summarized in Appendices A and C.

Annexes A through F provide references to Approved and Allowed security functions, Approved and Allowed Key Establishment mechanisms, Approved Authentication techniques and test metrics.

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
1. Cryptographic Module Specification	Specification of module, cryptographic boundary, Approved and Allowed algorithms and key establishment methods and Approved modes of operation. Description of module hardware, software and/or firmware. Module documentation.			
	Approved modes of operation are defined.		Module indication of Approved mode of operation.	
2. Cryptographic Module Interfaces	Required and Optional Interfaces. Specification of all interfaces and of all input and output data paths.			
			Trusted Channel.	
3. Roles, Authentication, and Services	Definition of module's roles and services.	Role-based or identity-based authentication.	Identity-based operator authentication	Multi-factor authentication.
4. Software/Firmware Security	Approved integrity technique, defined SFMI, HFMI and HSMI.	Approved digital signature or keyed message authentication code- based integrity test.	Approved digital signature based integrity test	
5. Operational Environment (*non-modifiable*)	Operational environment components bound to the firmware module.			
(*limited*)	Operational environment components bound to the firmware module. Controlled loading of additional through the Software/Firmware Load Test.			
(modifiable)	Control of SSPs and prevent outside processes access to CSPs.	Role-based or discretionary (with robust mechanism, ACLs, one-user to many-groups assignment) access control. Audit mechanism.	The OVERALL Security Levels 3 and 4 are NOT offered for software cryptographic modules, therefore no requirements for modifiable environment are provided.	
6. Physical Security	Production grade components.	Tamper evidence. Opaque covering or enclosure.	Tamper response and zeroization circuitry on removable covers and doors. Protection from probing from module openings. Hard opaque coating or enclosure.	EFP or EFT for temperature and voltage. Tamper detection and zeroization circuitry for multi-chip modules. Fault Injection Mitigation.
7. Physical Security-Non-invasive Attacks	No additional requirements.		Review of documented mitigation techniques against applicable non-invasive attacks listed in Annex F (mandatory for single-chip cryptographic modules and optional for all other hardware module embodiments).	Mitigation against non-invasive attacks with specific test requirements for this security level, specified by the validation authority (mandatory for single-chip cryptographic modules and optional for all other hardware module embodiments).
8. SSP Management	Requirements for Random Bit Generators, SSP generation, SSP establishment, SSP entry and output, SSP storage, and CSP zeroization. Electronically transported CSPs entered or output only encrypted.			
	Manually transported SSPs may be entered or output in plaintext form regardless of the entry or output method (manual or electronic).		Trusted Channel required.	
			Manually transported SSPs entered or output either in encrypted form or using split-knowledge procedures, regardless of the entry or output method (manual or electronic).	
9. Self-Tests	Pre-operational self-tests: software/firmware integrity test, bypass test and critical functions tests. Conditional self-tests: cryptographic algorithm test, pair-wise consistency test, software/firmware load test, manual key entry test, conditional bypass test and critical functions test. Cryptographic algorithm tests specified in Annexes A through E.			
			Pair-wise consistency test for key pairs entered into module. Periodic self-tests.	
10. Life-Cycle Assurance (Configuration Management)	Configuration management system for module, components, and documentation. Each uniquely identified and tracked throughout lifecycle.		Automated configuration management system.	

(Design)	Correspondence between module and Security Policy.	Functional Specification.	Detailed design.	Informal proof of correspondence between pre and post conditions and the functional specification.
(FSM)	Finite state model.			
(Development)	Annotated source code, schematics or HDL.	Software high-level language. Hardware high level descriptive language.		Documentation annotated with pre- conditions upon entry into module components and post-conditions expected to be true when components is completed.
(Vendor Testing)	Functional Testing.		Low-level Testing.	
(Delivery and Operation)	Start-up procedures.	Delivery Procedures.		Operator authentication using vendor provided authentication information.
(Guidance Docs)	Administrator and non-administrator guidance.			
11. Mitigation of Other Attacks	Documentation enumerates the mitigated attacks, other than the ones specified in this standard elsewhere.			Documentation includes the methods used to mitigate attacks not specified anywhere else in this standard, and the methods to test the effectiveness of mitigation techniques.

Table 1: Summary of Security Requirements

4.1 Cryptographic Module Specification

A cryptographic module **shall** be a set of hardware, software and/or firmware that implements Approved cryptographic algorithms, functions or processes.

4.1.1 Types of Cryptographic Modules

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

- ***Hardware module*** is a module whose cryptographic boundary is specified at the hardware perimeter. Firmware, which may also include an operating system, may be included within this hardware cryptographic boundary.
- ***Software module*** is a module whose cryptographic boundary delimits the software solely component(s) (may be one or multiple software components) that execute(s) in a modifiable operational environment.
- ***Firmware module*** is a module whose cryptographic boundary delimits the firmware solely component(s) that execute(s) in a limited or non-modifiable environment.
- ***Hybrid module*** is a module whose cryptographic boundary delimits the composite of a software or firmware component and a disjoint hardware component (i.e. the software or firmware component is not contained within the cryptographic hardware physical boundary).

For software modules executing in a modifiable environment, the physical security and non-invasive security requirements found in Sections 4.6 and 4.7 are optional.

For hardware and firmware modules, the physical security and non-invasive security requirements found in Sections 4.6 and 4.7 **shall** apply.

For hybrid modules, the software and firmware component(s) **shall** meet all applicable requirements of Sections 4.4 and 4.5. The hardware component **shall** meet all applicable requirements of Sections 4.6 and 4.7. Sections 4.6 and 4.7 requirements **shall** be met at the composite cryptographic boundary of a hybrid module.

4.1.2 Cryptographic Boundary

A cryptographic boundary **shall** consist of an explicitly defined perimeter (i.e. set of hardware, software or firmware components) that establishes the boundary of all components of a cryptographic module. The requirements of this standard **shall** apply to all functions and components within the module's cryptographic boundary. The cryptographic boundary **shall,** at a minimum, encompass all security relevant functions and components of a cryptographic module. Non-cryptographic or non-security relevant functions or components may be included within the cryptographic boundary. The defined name of a cryptographic module **shall** be representative of the composition of the components within the cryptographic boundary.

Hardware, software and/or firmware components within the cryptographic boundary may be excluded from the requirements of this standard if the excluded hardware, software or firmware components do not affect the security of the cryptographic module's security relevant components defined within the cryptographic boundary. Excluded components **shall** not affect or compromise the correct operation or requirements of this standard of the security relevant components within the cryptographic boundary. The excluded hardware, software or firmware **shall** be specified (see Appendix B).

4.1.2.1 Definitions of Cryptographic Boundary

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

- The set of hardware components which may include:
  - physical structures, including circuit boards, substrates or other mounting surfaces that provide the interconnecting physical wiring between components,
  - active electrical components such as semi-integrated, custom-integrated or common-integrated circuits, processors, memory, power supplies, converters, etc.
  - physical structures, such as enclosures, potting or encapsulation materials, connectors, and interfaces,
  - physical structures that implement the requirements of Section 4.6,
  - firmware, which may include an operating system,
  - other components types not listed above.

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

- The file or set of files saved on the storage media that constitute the cryptographic module; and
- The instantiation of the cryptographic module saved in memory and executed by one or more processors.

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

- The file or set of files saved on the storage media that constitute the cryptographic module; and
- The instantiation of the cryptographic module saved in memory and executed by the processor.

The cryptographic boundary of a **hybrid cryptographic module**:

- **shall** be the composite of the module's hardware component boundary and software or firmware component(s) boundary; and
- **shall** include the collection of all ports and interfaces from each component.

4.1.3 Modes of Operations

The operator **shall** be able to operate the module in an Approved mode of operation. An Approved mode of operation **shall** provide services for at least one Approved security function or key establishment mechanism. The module's security policy **shall** describe how the operator can operate the module in an Approved mode of operation. All Approved modes of operation **shall** be specified (see Appendix B.)

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, the operation of the cryptographic module in an Approved mode **shall**, at a minimum, be by policy (see appendix B.)

SECURITY LEVELS 3 AND 4

In addition to the requirements of Security Levels 1 and 2, for Security Levels 3 and 4, a cryptographic module **shall** indicate when the module is operating in an Approved mode of operation. The indication **shall** be explicit and unambiguous as to the state of the module or service operating in an Approved or non-Approved mode. For multi-threaded modules, the indication **shall** be provided for each called service.

4.1.3.1 Multiple Approved Modes of Operations

A cryptographic module may be designed to support multiple Approved modes of operation. Different Approved modes of operation are defined as each mode having services that provide a different suite of Approved or Allowed security functions or key establishment mechanisms. For a cryptographic module to implement more than one Approved mode of operation, the following **shall** apply:

- The overall security level of the module **shall** be maintained when configured for different Approved modes of operation.
- Each Approved mode of operation implemented in the cryptographic module and how each mode is configured **shall** be described (see appendix B.)
- Upon re-configuration from one Approved mode of operation to another, the cryptographic module **shall** perform the pre-operational self-tests (Section 4.9.1).
- Upon re-configuration, the conditional self-tests **shall** be reset and re-performed on condition for all Approved and Allowed security functions used in the selected Approved mode of operation.
- Security Levels 1 and 2: Upon re-configuration from one Approved mode of operation to another, CSPs **shall not** be shared or accessed between the Approved modes.
    - Upon re-configuration of Approved modes at Security Levels 1 and 2, the RBG state does not need to be reset, re-seeded or re-initialized.
- Security Levels 3 and 4: Upon re-configuration from one Approved mode of operation to another, the cryptographic module **shall** zeroize (Reference Section 4.8.6) all CSPs within the module.

- Upon re-configuration of Approved modes at Security Levels 3 and 4, the RBG state shall be re-seeded.

4.1.3.2 Degraded Mode of Operation

A cryptographic module may be designed to support degraded functionality (e.g., a module may fail the self-test for one encryption algorithm or detect an error during operation) within an Approved mode of operation. Security functions that tested correctly are considered operational, and those that failed are considered non-operational. For a cryptographic module to implement a degraded functionality in an Approved mode of operation, the following **shall** apply:

- Degraded mode of operation **shall** be entered only upon the detection of a failure and after the module has transitioned through the error state.
- When the cryptographic module operates in a degraded mode of operation, each operational security function **shall** pass all applicable self-tests.
- Non-operational security functions **shall** be isolated from the remaining security functions of the cryptographic module.
- The module **shall** remain in the degraded mode of operation until all pre-operational and conditional self-tests have been completed successfully.
- If the module fails the pre-operational self-tests, the module **shall not** enter a degraded mode of operation.

4.1.3.3 Non-Approved Mode of Operation

A cryptographic module may be designed to support non-Approved modes of operation. A non-Approved mode of operation is one where only non-Approved services are provided or the requirements of this standard are not met.

For a cryptographic module to implement a non-Approved mode of operation, the following **shall** apply:

- CSPs **shall not** be shared or access provided between Approved and non-Approved modes of operation. However the output of an Approved RBG may be provided to a non-Approved mode without the zeroization of the RBG seed as long as the seed cannot be accessed in the non-Approved mode.

A module **shall** not switch from an Approved mode, to a non-Approved mode, and then back to a different (not the original) Approved mode without meeting the requirements in 4.1.3.1.

4.1.4 Security Functions and Techniques

In an Approved mode of operation, a cryptographic module **shall** implement at least one Approved or Allowed (listed in Annexes A, B, C, D or E) security function or technique.

For cryptographic modules that implement Allowed security functions or techniques used in an Approved mode of operation, the following **shall** apply:

- The Allowed security functions or technique **shall** meet all of the applicable requirements specified in Annexes B or D.

- The Allowed security function or technique **shall** meet all the applicable security function requirements of this standard.

Non-Approved functions can be performed in an Approved mode if they are not used to provide security relevant functionality (e.g., a non-Approved algorithm or non-Approved generated key may be used to obfuscate data or keys but the result is considered plaintext and provides no security relevant functionality until encrypted with an Approved algorithm).

Testing of the algorithmic implementations, as applicable, **shall** be performed on the same operational environment as the cryptographic module is tested.

4.2 Cryptographic Module Interfaces

A cryptographic module **shall** restrict all logical information flow to only those physical access points and logical interfaces that are identified as entry and exit points to and from the cryptographic boundary of the module. The cryptographic module interfaces **shall** be logically distinct from each other although they may share one physical port, (e.g., input data may enter and output data may exit via the same port) or may be distributed over one or more physical ports, (e.g., input data may enter via both a serial and a parallel port).

4.2.1 Types of Interfaces

- *Hardware Module Interface (HMI):* The total set of commands used to request the services of the hardware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

- *Software or Firmware Module Interface (SFMI):* The total set of commands used to request the services of the software or the firmware module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

- *Hybrid Software or Hybrid Firmware Module Interface (HSMI or HFMI):* The total set of commands used to request the services of the hybrid hardware/software module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

4.2.2 Definition of Interfaces

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

- *Data output interface*: All output data (except status data output via the status output interface or control data output via the control output interface) from a cryptographic module (including plaintext, ciphertext, SSPs, and control information for another module) **shall** exit via the "data output" interface. All data output via the "data output" interface **shall** be inhibited while performing manual key entry, pre-operational self-tests, software/firmware loading and zeroization; or when the cryptographic module is in an error state due to failing to successfully pass the pre-operational self-tests (Section 4.9.1).

- *Data input interface*: All input data (except control data entered via the control input interface) processed by a cryptographic module (including plaintext, ciphertext, SSPs, and status information from another module) **shall** enter via the "data input" interface. Data may be accepted by the module through the data input interface while the module is performing self-tests.

- *Control output interface:* All output commands, signals, and control data (including function calls and manual controls such as switches, buttons, and keyboards) used to control the operation of a cryptographic module **shall** exit via the “control output” interface.

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

- *Status output interface*: All output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of a cryptographic module **shall** exit via the "status output" interface. Status output may be either implicit or explicit.

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

- *Power interface:* All power ports used to provide electrical power to or from the cryptographic module. A power port is not required, and a power interface may not exist when all power is provided or maintained within the cryptographic boundary of the cryptographic module (e.g., by an internal battery).

All electrical power externally provided to a cryptographic module (including power from an external power source or batteries) **shall** enter via a power interface.

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

The cryptographic module specification **shall,** unambiguously, specify format of input data, including size restrictions for all variable length inputs. During execution the module **shall** verify the input data format for all input data. If a particular input violates the input data format, it **shall** be rejected by the module.

Documentation **shall** include all module interfaces including the power interface.

Documentation **shall** specify all physical access points and logical interfaces

4.2.3 Trusted Channel

A cryptographic module which provides a Trusted Channel over a dedicated interface or port (see Sections 1.3, 2.1, 4.5 and 4.8), **shall** use this channel to securely communicate SSPs, service requests and service responses over unprotected communications channels.

If a Trusted Channel is provided, then the following requirements **shall** be met:

- The module documentation **shall** specify the protocols and Approved or Allowed security functions used to support the Trusted Channel.

- Only Approved or Allowed cryptographic security functions **shall** be used by the module to support the Trusted Channel.

- The module **shall** provide an indication to the module operator as to whether or not the Trusted Channel is operational.

SECURITY LEVELS 1 AND 2

At Security Levels 1 and 2, modules have no requirements for a Trusted Channel service.

SECURITY LEVELS 3 AND 4

The module **shall** implement a Trusted Channel service.

A Trusted Channel **shall** be implemented between the operators and the cryptographic module.

All SSPs, authentication data, control inputs, and status outputs **shall** be communicated via a Trusted Channel. Communications via this Trusted Channel **shall** be activated exclusively by an operator or the cryptographic module. The Trusted Channel **shall** provide source authentication and **shall** prevent unauthorized modification, substitution, disclosure, and playback of sensitive security parameters.

The following events **shall** be recorded by an audit mechanism:

- attempts to use the Trusted Channel function and whether the request was granted.
- identification of the initiator and target of a Trusted Channel.

4.3 Roles, Authentication and Services

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

4.3.1 Roles

A cryptographic module **shall, at a minimum,** support a *Crypto Officer Role*. The *Crypto Officer Role* **shall** be assumed to perform cryptographic initialization or management functions, and general security services (e.g., module initialization, management of cryptographic keys, CSPs, and audit functions).

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

A cryptographic module may support a *Trusted Role*. The *Trusted Role* is a state of the module where the module can perform cryptographic operations and other Approved security functions without any outside entities authenticated to the module. The operation of the *Trusted Role* **shall** be configured by the Crypto Officer.

A cryptographic module may support a *Maintenance Role*. The Maintenance Role is a role assumed during the physical and/or logical maintenance services (e.g. opening service covers, performing certain diagnostics such as built in self-test (BIST)). All unprotected SSPs **shall** be zeroized when entering or exiting the Maintenance Role.

A cryptographic module may support other roles in addition to the roles specified above.

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

An Authorized role **shall** perform all callable services utilizing Approved or Allowed security functions or Approved or Allowed key establishment mechanisms or where the security of the module is affected. An operator is not required to assume an authorized role to perform services where CSPs are not used, modified, disclosed, or substituted and PSPs are not used, modified or substituted (e.g., *show status* or other services that do not affect the security of the module).

Documentation **shall** specify all authorized roles supported by the cryptographic module.

4.3.2 Authentication

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. The following types of mechanisms are used to control access to the cryptographic module:

Role-Based Authentication: If role-based authentication mechanisms are supported by a cryptographic module, the module **shall** require that one or more roles either be implicitly or explicitly selected by the operator and **shall** authenticate the assumption of the selected role (or set of roles). The cryptographic module is not required to authenticate the individual identity of the operator. The selection of roles and the authentication of the assumption of selected roles may be combined. If a cryptographic module permits an operator to change roles, then the module **shall** authenticate the assumption of any role that was not previously authenticated for that operator.

Identity-Based Authentication: If identity-based authentication mechanisms are supported by a cryptographic module, the module **shall** require that the operator be individually and uniquely identified, **shall** require that one or more roles either be implicitly or explicitly selected by the operator, and **shall** authenticate the identity of the operator and the authorization of the operator to assume the selected role or set of roles. The authentication of the identity of the operator, selection of roles, and the authorization of the assumption of the selected roles may be combined. If a cryptographic module permits an operator to change roles, then the module **shall** verify the authorization of the identified operator to assume any role that was not previously authorized.

Except for the Trusted Role(s) and Trusted Channel establishment, services using Approved or Allowed security functions **shall** not be available to an operator until the operator's authentication is completed successfully. A cryptographic module may permit an authenticated operator to perform all of the services allowed within an authorized role, or may require separate authentication for each service or for different sets of services. When a cryptographic module is reset, rebooted, powered off and subsequently powered on, the module **shall** require the operator to be authenticated.

Various types of authentication data may be required by a cryptographic module to implement the supported authentication mechanisms, including (but not limited to) the knowledge or possession of a password, PIN, cryptographic key, or equivalent; possession of a physical key, token, or equivalent; or verification of personal characteristics (e.g., biometrics). Authentication data within a cryptographic module **shall** be protected against unauthorized use, disclosure, modification, and substitution.

The initialization of authentication mechanisms may warrant special treatment. If a cryptographic module does not contain the authentication data required to authenticate the operator for the first time the module is accessed, then other authorized methods (e.g., procedural controls or use of factory-set or default authentication data) **shall** be used to control access to the module and initialize the authentication mechanisms. If default authentication data is used to control access to the module, then default authentication data **shall** be replaced upon first-time authentication. This default authentication data does not need to meet the zeroization requirements (see Section 4.8.)

The authentication mechanism may be a group of mechanisms of different authentication properties that jointly meet the strength of authentication requirements of this section. If the cryptographic module uses cryptographic functions to authenticate the operator, then those cryptographic functions **shall** be Approved or Allowed cryptographic functions.

- The module **shall** implement an Approved authentication mechanism as specified in Annex E.
- The Approved Authentication mechanism **shall** be met by the module's implementation and not rely on documented procedural controls or security rules (e.g., password size restrictions).

  For a software cryptographic module at Security Level 2, the operating system may implement the

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

- Feedback of authentication data to an operator **shall** be obscured during the authentication process (e.g., no visible display of characters when entering a password). Non-significant characters may be displayed in place of the actual authentication data.

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

The strength of authentication mechanism **shall** be described (see Appendix B.)

SECURITY LEVEL 1

For Security Level 1, a cryptographic module is not required to employ authentication mechanisms to control access to the module.

SECURITY LEVEL 2

For Security Level 2, a cryptographic module **shall** employ *role-based* authentication to control access to the module.

SECURITY LEVEL 3

For Security Level 3, a cryptographic module **shall** employ *identity-based* authentication mechanisms to control access to the module.

SECURITY LEVEL 4

In addition to the requirements of Security Level 3, Security Level 4 **shall** also meet the following requirement:

- The cryptographic module **shall** enforce multi-factor identity-based authentication.

4.3.3 Services

A cryptographic module **shall** provide the following services to operators:

Status: Output the current status of the cryptographic module. This may include the output of status indicators in response to a service request.

Module's Version Number: Output the name or module identifier and the versioning information of the cryptographic module that can be correlated with a validation certificate (e.g. hardware, software and/or firmware versioning information).

Self-Tests: Initiate and run pre-operational self-tests as specified in Section 4.9.1.

Approved Security Function: Perform at least one Approved security function used in an Approved mode of operation, as specified in Section 4.1.

Zeroize: Perform zeroization of all parameters as specified in Section 4.8.6 (may be performed procedurally).

A cryptographic module may provide other services, both Approved, Allowed and non-Approved, in addition to the services specified above. Specific services may be provided in more than one role (e.g., key entry services may be provided in the User role and the Crypto Officer role).

4.3.3.1 Bypass Capability

Bypass capability is the ability of a service to partially or wholly circumvent a cryptographic function. If the module can output a particular data or status item in a cryptographically protected form, or (as a result of module configuration or operator intervention) can also output the item in a non-protected form, then a bypass capability **shall** be defined.

If a cryptographic module implements a bypass capability, then

- The operator **shall** assume an authorized role before configuring the bypass capability.
- Two independent internal actions **shall** be required to activate the capability to prevent the inadvertent bypass of plaintext data due to a single error. The two independent internal actions **shall** modify software and/or hardware behavior that is dedicated to mediate the bypass capability.
- The module **shall** show its status to indicate whether:
    - the module is providing services *without* the use of cryptographic functions (the bypass capability *is* activated), or
    - the module is providing services *with* the use of a cryptographic function (the bypass capability *is not* activated).
    - the bypass capability *is alternately* activated and deactivated and the module is providing some services with cryptographic processing and some services without cryptographic processing (e.g. for modules with multiple communication channels, plaintext data is or is not encrypted depending on each channel configuration).

Documentation **shall** specify the mechanism or logic governing the bypass capability.

4.3.3.2 Software or Firmware Loading

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

- The logic performing the external software or firmware loading **shall** be logically disconnected from all data output.
- The *Software/Firmware Load Test* specified in Section 4.9.2 **shall** be performed before the loaded code is executed.
- The cryptographic module **shall** withhold execution of any loaded Approved security functions until after the Cryptographic Algorithm self-tests specified in Section 4.9.2 have been successfully executed.
- The module **shall** support an Approved authentication technique to verify the validity of software/firmware that may be loaded.

4.4 Software/Firmware Security

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

SECURITY LEVEL 1

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

- All software and firmware **shall** be in a form that satisfies the requirements of this standard without modification installation (Section 4.10.6).

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

  - by the cryptographic module itself, or
  - by another Validated cryptographic module.

- If the integrity test fails, the module **shall** enter the error state. The integrity technique may consist of a single encompassing authentication code or signature, or multiple disjoint authentication codes or signatures of which failure of any disjoint authentication code or signature **shall** cause the module to enter the error state. The expected referenced output of the integrity technique mechanism may be considered data and itself not subject to the integrity technique. The temporary value(s) generated during the integrity test of the module's software or firmware **shall** be zeroized from the module upon completion of the integrity test.

- An operator **shall** be able to perform the *Approved integrity technique* on demand via an SFMI, HSMI or HFMI service.

- All data and control inputs, and data and status outputs as specified in Section 4.2 of the module and services **shall** be directed through a defined SFMI, HFMI or HSMI (defined in Section 4.2).

- Any replacements or modifications to the software or firmware components of the module other than a complete replacement **shall** pass the Software/Firmware Load Test as specified in Section 4.9.2. A complete replacement **shall** constitute a new module which would require its own validation as a whole.

SECURITY LEVEL 2

In addition to the requirements of Security Level 1, the following requirements **shall** apply to software or firmware components of a cryptographic module for Security Level 2.

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

- The SFMI, HFMI or HSMI **shall not** provide a service to allow the operator to examine the executable code.

- A cryptographic mechanism only using an Approved *digital signature* or *keyed message authentication code* **shall** be applied to all software or firmware within the module's defined cryptographic boundary. The Approved digital signature or keyed message authentication code that **shall** be applied to the software or firmware **shall** consist of the verification of a digital signature or keyed message authentication code which was used to originally sign the code (by the vendor) using an Approved digital signature algorithm or Approved keyed message authentication code. If the test fails, the module **shall** enter the error state. The digital signature or keyed message authentication code technique may consist of a single encompassing signature or keyed message authentication code or multiple disjoint signatures of which failure of any disjoint signature or

keyed message authentication code **shall** cause the module to enter the error state. The public verification key or keyed message authentication key may reside within the module code (if so, the key is still not considered a CSP).

- The Approved *digital signature* or *keyed message authentication code* may be performed by the operating system.

SECURITY LEVELS 3 AND 4

In addition to the requirements of Security Level 2, the following requirements **shall** apply to software or firmware components of a cryptographic module for Security Level 3 and 4:

- A cryptographic mechanism using an Approved *digital signature* **shall** be applied to all software or firmware components within the module's defined cryptographic boundary. The Approved digital signature that **shall** be applied to the software or firmware **shall** consist of the verification of a digital signature which was used by the vendor to originally sign the code using an Approved digitally signing algorithm. If the signature test fails, the module **shall** enter the error state. The digital signature technique may consist of a single encompassing signature or multiple disjoint signatures of which failure of any disjoint signature **shall** cause the module to enter the error state. The private signing key **shall** reside outside the module. The public verification key may reside within the module code (if so, the key is not considered a CSP).

4.5 Operational Environment

The *operational environment* of a software, firmware, hybrid software or hybrid firmware cryptographic module refers to the set of all software, firmware and hardware required for the cryptographic module to operate correctly. This section is not applicable for a hardware module. The operational environment of a software or firmware module includes, at a minimum, the module itself and the computing platform including the operating system that controls or allows the execution of the software or firmware module. The operating system is considered to include, when applicable, the virtual machine(s) (system and/or process) and the runtime environment (e.g. Java Runtime Environment –JRE). An operational environment can be non-modifiable (e.g. an environment that can not be modified), *limited* (e.g. an environment which allows controlled modification meeting the requirements of Section 4.9.2.3), or *modifiable* (e.g. an environment which allows uncontrolled modifications).

For a *non-modifiable* or *limited* environment, the controlling components which maintain the specific environment may include attributes of the computing platform, the operating system or the cryptographic module itself *or* all of the above.

Code which is executed in a *non-modifiable* or *limited* environment is referred to as *firmware* within this standard.

Code which is executed in a *modifiable* environment is referred to as *software* within this standard.

1. A ***non-modifiable operational environment*** is designed to contain only firmware or hardware. This environment may consist of a firmware module operating in a non-programmable computing platform or a hardware module and its computing platform which can not be modified.

2. A ***limited operational environment*** is designed to contain only firmware or hardware but allows controlled modifications. This environment may be firmware operating in a programmable computer (e.g., a programmable hardware module) where the loading of additional firmware is controlled through the Software/Firmware Load Test specified in Section 4.9.2.3.

3. A ***modifiable operational environment*** refers to an operating environment that may be reconfigured to add/delete/modify functionality, and/or may include general-purpose operating system capabilities (e.g., use of a computer O/S, configurable smartcard O/S, or programmable software). Operating systems are considered to be modifiable operational environments if

software components can be modified by the operator and/or the operator can load and execute software (e.g., a word processor) that was not included as part of the validation of the module.

Some examples of operational environments are provided in the following table.

Configuration Examples	Operational Environment
A computing platform that does not permit the loading of code and does not permit operators to modify the configuration of the operating system or cryptographic module.	Non-Modifiable
A computing platform containing an operating system that allows the loading of additional *validated* code that is authenticated and meets all applicable requirements of this standard.	Limited
A computing platform containing code on a computing platform that allows the input of non-validated code.	Modifiable
A computing platform containing code on a computer whose operating system is reconfigurable by the operator allowing the removal of the security protections.	Modifiable

Table 2: Examples of Operational Environments

If the operational environment is *non-modifiable* or *limited*, then the operational environment components that enforce the *non-modifiable* or *limited* environment **shall** be bound to the firmware module and the operating system requirements in Section 4.5.1 do not apply.

If the operational environment is *limited*, then the loading of additional firmware **shall** be controlled through the Software/Firmware Load Test specified in Section 4.9.2.3.

Defining a limited or non-modifiable operational environment by means of procedurally-enforced security rules prohibiting the use of the external software loading capability **shall** be prohibited.

If the operational environment is *modifiable*, the operating system requirements in Section 4.5.1 **shall** apply.

Documentation **shall** specify the operational environment for the cryptographic module. If the operational environment is *non-modifiable* or *limited*, the documentation **shall** specify all hardware and firmware components that enforce the *non-modifiable* or *limited* environment.

If the operational environment includes an evaluated operating system under a recognized program, the documentation **shall** specify the evaluation certificates, protection profiles and extensibility as applicable.

4.5.1 Operating System Requirements for Modifiable Operational Environments

The requirements in this section are intended to logically protect the cryptographic module and its SSPs while running in a *modifiable* operational environment, from unauthorized or untrusted processes.

SECURITY LEVEL 1

The following requirements **shall** apply to operating environments for Security Level 1.

- Each instance of a cryptographic module **shall** have control over its own SSPs.
- The operational environment **shall** be configured to prevent processes outside the cryptographic boundary of the cryptographic module from having uncontrolled access to the modules CSPs.

SECURITY LEVEL 2

In addition to the requirements of Security Level 1 for the operating system, the following requirements **shall** apply for Security Level 2. In lieu of the following requirements, an operating environment may be used as allowed by the validation authority as specified in Annex G.

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

- To protect plaintext data, cryptographic software, SSPs, and authentication data, the access control mechanisms of the operating system **shall** be configured to:

  - Define and enforce the set of roles or the groups and their associated ACLs that have exclusive rights to *execute* the stored cryptographic software.

  - Define and enforce the set of roles or the groups and their associated ACLs that have exclusive rights to *modify* (i.e., write, replace, and delete) the following cryptographic module software stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., cryptographic audit data), SSPs, and plaintext data.

  - Define and enforce the set of roles or the groups and their associated ACLs that have exclusive rights to *read* cryptographic data (e.g., cryptographic audit data), CSPs, and plaintext data.

  - Define and enforce the set of roles or the groups and their associated ACLs that have exclusive rights to enter SSPs.

- The following specifications **shall** be consistent with the roles or designated groups' rights and services as defined in the Security Policy.

  - When not in the maintenance mode, the operating system **shall** prevent all operators and running processes from *modifying* running cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, running processes refer to all processes, cryptographic or not, not owned or initiated by the operating system (i.e., operator-initiated).

  - The operating system **shall** prevent processes in user role or user groups from gaining either *read* or *write* access to SSPs owned by other processes and to system SSPs.

  - The configuration of the operating system that meets the above requirements **shall** be specified in the Administrative Guidance. The Administrative Guidance **shall** state that the operating system must be configured as specified for the module contents to be considered protected.

The identification and authentication mechanism to the operating system **shall** meet the requirements of Section 4.3.2 and be specified in the modules Security Policy.

All cryptographic software, SSPs, and control and status information **shall** be under the control of:

- An operating system which **shall** have, at a minimum, the following attributes:

    - The operating system **shall** provide an audit mechanism to record modifications, accesses, deletions, and additions of cryptographic data and SSPs. If audit information is stored outside of the operational environment, then the module **shall** use Approved cryptographic functions to protect the information when external to the module from unauthorized disclosure and modification.

    - The following events and their date and time of occurrence **shall** be recorded by the audit mechanism:

        - attempts to provide invalid input for Crypto Officer functions, and
        - addition or deletion of an operator to and from a Crypto Officer role.
        - attempts to use the Trusted Channel function and whether the request was granted, when Trusted Channel is supported at this security level.
        - identification of the initiator and target of a Trusted Channel, when Trusted Channel is supported at this security level.

    - The audit mechanism **shall** be capable of auditing the following events:

        - all operator read or write accesses to audit data stored in the audit trail,
        - requests to use authentication data management mechanisms,
        - the use of a security-relevant Crypto Officer function,
        - requests to access authentication data associated with the cryptographic module,
        - the use of an authentication mechanism (e.g., login) associated with the cryptographic module, and
        - explicit requests to assume a Crypto Officer role.

    - The operating system **shall** be configured to prevent operators in the user role (if supported) or members of the users group from modifying cryptographic module software and audit data stored within the operational environment of the cryptographic module.

    - Only operating systems that are configured to meet the above security requirements **shall** be permitted at this security level, whether or not the cryptographic module operates in an Approved mode of operation.

4.6 Physical Security

A cryptographic module **shall** employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module when installed. All hardware, software, firmware, and SSPs within the cryptographic boundary **shall** be protected.

A cryptographic module that is implemented completely in software such that the physical security is provided solely by the host platform is not subject to the requirements of this section.

The requirements of this section **shall** be applicable to hardware, firmware and hardware components of hybrid modules.

Physical security requirements are specified for three defined physical embodiments of a cryptographic module:

- ***Single-chip cryptographic modules*** are physical embodiments in which a single integrated circuit (IC) chip may be used as a standalone module or may be embedded within an enclosure or a product that may not be physically protected. Examples of single-chip cryptographic modules include single IC chips or smart cards with a single IC chip.

- ***Multiple-chip embedded cryptographic modules*** are physical embodiments in which two or more IC chips are interconnected and are embedded within an enclosure or a product that may not be physically protected. Examples of multiple-chip embedded cryptographic modules include adapters and expansion boards.

- ***Multiple-chip standalone cryptographic modules*** are physical embodiments in which two or more IC chips are interconnected and the entire enclosure is physically protected. Examples of multiple-chip, standalone cryptographic modules include encrypting routers or secure radios.

Depending on the physical security mechanisms of a cryptographic module, unauthorized attempts at physical access, use, or modification **shall** have a high probability of being detected

- subsequent to an attempt by leaving visible signs

  and / or

- during an access attempt,

and appropriate immediate actions **shall** be taken by the cryptographic module to protect SSPs.

Table 3 summarizes the physical security requirements, both the general and the three specific embodiments for each of the four security levels. The embodiment-specific physical security requirements at each security level enhance the general requirements at the same level, and the embodiment-specific requirements of the previous level.

	General Requirements for all Embodiments	Single-Chip Cryptographic Modules	Multiple-Chip Embedded Cryptographic Modules	Multiple-Chip Standalone Cryptographic Modules
Security Level 1	Production-grade components.	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure.
Security Level 2	Evidence of tampering. Opaque covering.	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Tamper response and zeroization circuitry. Protection from probing.	Hard opaque tamper-evident coating on chip or strong opaque removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-chip standalone security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong opaque enclosure with removal/penetration attempts causing serious damage.
Security Level 4	Either EFP or EFT for temperature and voltage.	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroization capability.	Tamper detection envelope with tamper response and zeroization capability.

Table 3: Summary of Physical Security Requirements

In general, Security Level 1 requires minimal physical protection. Security Level 2 requires the addition of tamper-evident mechanisms and the inability to gather information about the internal operations of the critical areas of the module (opaqueness). Security Level 3 adds requirements for the use of strong enclosures with tamper detection and response mechanisms for removable covers and doors and resistance to probing via ventilation openings. Security Level 4 adds requirements for the use of strong enclosures with tamper detection and response mechanisms for the entire enclosure as well as either environmental failure protection (EFP) or environmental failure testing (EFT) and protection from fault induced attacks.

Security requirements are specified for a maintenance access interface when a cryptographic module is designed to permit physical access (e.g., by the module vendor or other authorized individuals).

Tamper detection and tamper response are not substitutes for tamper evidence.

4.6.1 General Physical Security Requirements

The following requirements **shall** apply to all physical embodiments:

- Documentation **shall** specify the physical embodiment and the security level for which the physical security mechanisms of a cryptographic module are implemented.
- Whenever zeroization is performed for physical security purposes, the zeroization **shall** occur in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time of detection and the actual zeroization.
- If a module includes a maintenance role that requires physical access to the contents of the module or if the module is designed to permit physical access (e.g., by the module vendor or other authorized individual), then:
    - A maintenance access interface **shall** be defined.
    - The maintenance access interface **shall** include all physical access paths to the contents of the cryptographic module, including any removable covers or doors.
    - Any removable covers or doors included within the maintenance access interface **shall** be safeguarded using the appropriate physical security mechanisms.
    - All CSPs **shall** be zeroized when the maintenance access interface is accessed.

SECURITY LEVEL 1

The following requirements **shall** apply to all cryptographic modules for Security Level 1:

- The cryptographic module **shall** consist of production-grade components that **shall** include standard passivation techniques (e.g., a conformal coating or a sealing coat applied over the module's circuitry to protect against environmental or other physical damage).
- When performing maintenance, all unprotected CSPs contained in the cryptographic module **shall** be zeroized. Zeroization **shall** either be performed procedurally by the operator or automatically by the cryptographic module.

SECURITY LEVEL 2

In addition to the general requirements for Security Level 1, the following requirement **shall** apply to all cryptographic modules for Security Level 2:

- The cryptographic module **shall** provide evidence of tampering (e.g., on the cover, enclosure, or seal) when physical access to the module is attempted. Tamper evidence protections **shall** only be applied between adjoining solid surfaces.
- The tamper-evident material, coating or tamper-evident enclosure **shall** either be opaque or translucent within the visible spectrum (i.e., light of wavelength range of 400nm to 750nm) to prevent the gathering of information about the internal operations of the critical areas of the module.

- If the cryptographic module contains ventilation holes or slits, then the holes or slits **shall** be constructed in a manner to prevent the gathering of information of the module's internal construction or components by direct visual observation using artificial light sources in the visual spectrum of the module's internal construction or components.

SECURITY LEVEL 3

In addition to the general requirements for Security Levels 1 and 2, the following requirements **shall** apply to all cryptographic modules for Security Level 3:

- If the module contains any doors or removable covers or if a maintenance access interface is defined, then the module **shall** contain tamper response and zeroization circuitry. The tamper response and zeroization circuitry **shall** immediately zeroize all CSPs when a door is opened, a cover is removed, or when the maintenance access interface is accessed. The tamper response and zeroization circuitry **shall** remain operational when CSPs are contained within the cryptographic module.

- If the cryptographic module contains ventilation holes or slits, then the holes or slits **shall** be constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., prevent probing by a single articulated probe).

- If tamper evident seals are employed, they **shall** be uniquely numbered or independently identifiable (e.g., uniquely numbered evidence tape or uniquely identifiable holographic seals).

SECURITY LEVEL 4

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

- The cryptographic module **shall** be protected either by a hard opaque removal-resistant coating, or by a tamper detection envelope with tamper response and zeroization capability.

- The module **shall** either include EFP features or undergo EFT.

- The cryptographic module **shall** provide protection from fault induction.

4.6.2 Single-Chip Cryptographic Modules

In addition to the general security requirements specified in Section 4.6.1, the following requirements are specific to single-chip cryptographic modules.

SECURITY LEVEL 1

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

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirements **shall** apply to single-chip cryptographic modules for Security Level 2.

- The cryptographic module **shall** be covered with a tamper-evident coating (e.g., a tamper-evident passivation material or a tamper-evident material covering the passivation) or contained in a tamper-evident enclosure to deter direct observation, or manipulation of the module and to provide evidence of attempts to tamper with or remove the module.

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements **shall** apply to single-chip cryptographic modules for Security Level 3:

- The module **shall** be covered with a hard opaque tamper-evident coating (e.g., a hard opaque epoxy covering the passivation),

  or

- The enclosure **shall** be implemented so that attempts at removal or penetration of the enclosure **shall** have a high probability of causing serious damage to the cryptographic module (i.e., the module will not function).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements **shall** apply to single-chip cryptographic modules for Security Level 4.

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

- The removal-resistant coating **shall** have solvency characteristics such that dissolving the coating will have a high probability of dissolving or seriously damaging the module (i.e., the module will not function).

4.6.3 Multiple-Chip Embedded Cryptographic Modules

In addition to the general security requirements specified in Section 4.6.1, the following requirements are specific to multiple-chip embedded cryptographic modules.

SECURITY LEVEL 1

If the cryptographic module is contained within an enclosure or within an enclosure that has a door or a removable cover, then a production-grade enclosure or enclosure with a door or a removable cover **shall** be used.

SECURITY LEVEL 2

In addition to the requirement for Security Level 1, the following requirements **shall** apply to multiple-chip embedded cryptographic modules for Security Level 2:

- The module **shall** satisfy one of the following requirements.

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

    or

- The module's components **shall** be contained in a tamper-evident enclosure to deter direct observation or manipulation of module components and to provide evidence of attempts to tamper with or remove module components,

  or

- The module **shall** be entirely contained within a metal, hard plastic or equivalent production-grade material enclosure that may include doors or removable covers.

- If the enclosure includes any doors or removable covers, then the doors or covers **shall** be locked with pick-resistant mechanical locks employing physical or logical keys or **shall** be protected with tamper-evident seals

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements **shall** apply to multiple-chip embedded cryptographic modules for Security Level 3.

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

  or

- The module **shall** be contained within a strong enclosure such that attempts at removal or penetration of the enclosure will have a high probability of causing serious damage to the module (i.e., the module will not function).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements **shall** apply to multiple-chip embedded cryptographic modules for Security Level 4.

- The cryptographic module components **shall** be covered by potting material or contained within an enclosure encapsulated by a tamper detection envelope (e.g., a flexible mylar printed circuit with a serpentine geometric pattern of conductors or a wire-wound package or a non-flexible, brittle circuit or a strong enclosure) that **shall** detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure to an extent sufficient for accessing or modifying the internal components and the SSPs of the module.

- The cryptographic module **shall** contain tamper response and zeroization circuitry that **shall** continuously monitor the tamper detection envelope and, upon the detection of tampering, **shall** immediately zeroize all CSPs. The tamper response and zeroization circuitry **shall** remain operational when CSPs are contained within the cryptographic module.

4.6.4 Multiple-Chip Standalone Cryptographic Modules

In addition to the general security requirements specified in Section 4.6.1, the following requirements are specific to multiple-chip standalone cryptographic modules.

SECURITY LEVEL 1

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

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirement **shall** apply to multiple-chip standalone cryptographic modules for Security Level 2.

If the enclosure of the cryptographic module includes any doors or removable covers, then the doors or covers **shall** be locked with pick-resistant mechanical locks employing physical or logical keys or **shall** be protected with tamper-evident seals.

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements **shall** apply to multiple-chip standalone cryptographic modules for Security Level 3:

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

  or

- the module **shall** be contained within a strong enclosure such that attempts at removal or penetration of the enclosure will have a high probability of causing serious damage to the module (i.e., the module will not function).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirements **shall** apply to multiple-chip standalone cryptographic modules for Security Level 4.

- The potting material or enclosure of the cryptographic module **shall** be encapsulated within a tamper detection envelope that uses tamper detection mechanisms such as cover switches (e.g., microswitches, magnetic Hall effect switches, permanent magnetic actuators, etc.), motion detectors (e.g., ultrasonic, infrared, or microwave), or other tamper detection mechanisms as described above for multiple-chip embedded cryptographic modules. The tamper detection mechanisms **shall** detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure, to an extent sufficient for accessing the contents of the module.

- The cryptographic module **shall** contain tamper response and zeroization circuitry that **shall** continuously monitor the tamper detection envelope and, upon the detection of tampering, **shall** immediately zeroize CSPs. The tamper response and zeroization circuitry **shall** remain operational when CSPs are contained within the cryptographic module.

4.6.5 Environmental Failure Protection/Testing

The electronic devices and circuitry are designed to operate within a particular range of environmental conditions. Deliberate or accidental excursions outside the specified normal operating ranges of voltage and temperature can cause erratic operation or failure of the electronic devices or circuitry that can compromise the security of the cryptographic module. Reasonable assurance that the security of a cryptographic module cannot be compromised by extreme environmental conditions can be provided by having the module employ EFP features or undergo EFT.

For Security Levels 1, 2, and 3, a cryptographic module is not required to employ EFP features or undergo EFT. At Security Level 4, a cryptographic module **shall** either employ EFP features or undergo EFT.

4.6.5.1 Environmental Failure Protection Features

EFP features **shall** protect a cryptographic module against unusual environmental conditions or fluctuations (accidental or induced) outside of the module's normal operating range that can compromise the security of the module.

The cryptographic module **shall** monitor and correctly respond to fluctuations in the operating *temperature* and *voltage* outside of the specified normal operating ranges.

The EFP features **shall** involve electronic circuitry or devices that continuously measure the operating temperature and voltage of a cryptographic module. If the temperature or voltage falls outside of the cryptographic module's normal operating range, the protection circuitry **shall** either,

- Shut down the module to prevent further operation,

  or

- Immediately zeroize all CSPs.

Documentation **shall** specify the normal operating ranges of a cryptographic module and the EFP features employed by the module.

4.6.5.2 Environmental Failure Testing Procedures

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

EFT **shall** demonstrate that, if the operating temperature or voltage falls outside the normal operating range of the cryptographic module resulting in a failure, at no time **shall** the security of the cryptographic module be compromised.

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

The voltage range tested **shall** be gradually decreasing from a voltage within the normal operating voltage range to a lower voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroizes all CSPs; and **shall** be gradually increasing from a voltage within the normal operating voltage range to a higher voltage that either (1) shuts down the module to prevent further operation or (2) immediately zeroizes all CSPs, including reversing the polarity of the voltages .

Documentation **shall** specify the normal operating ranges of the cryptographic module and the environmental failure tests performed.

4.7 Physical Security – Non-Invasive Attacks

Non-invasive attacks attempt to compromise a cryptographic module by acquiring knowledge of the module's CSPs without physically modifying or invading the module. The non-invasive attacks and their associated security functions addressed by this standard are specified in Annex F. Annex F may be updated periodically as new non-invasive attacks or security functions relevant to these attacks are added within the scope of this standard.

The requirements of this section **shall** be applicable to single-chip cryptographic modules and single-chip components of hybrid modules. The requirements of this section are optional for all other hardware module embodiments.

SECURITY LEVELS 1 AND 2

At Security Levels 1 and 2, a cryptographic module is not required to employ protection features against the non-invasive attacks.

SECURITY LEVEL 3

At Security Level 3, the cryptographic module **shall** protect the module's CSPs against all of the applicable non-invasive attacks Annex F specifies and associates with Approved or Allowed security functions. Documentation **shall** specify the mitigation techniques employed against these attacks and how these techniques mitigate access to the module's CSPs. The effectiveness of the mitigation techniques **shall** be specified.

SECURITY LEVEL 4

In addition to the requirements for Security Level 3, the module **shall** undergo testing, and **shall** meet the requirements defined by the validation authority, for each of the applicable non-invasive attacks and the Approved or Allowed security functions which are relevant to those attacks, as specified in Annex F.

4.8 Sensitive Security Parameter Management

Sensitive Security Parameters (SSPs) consist of Critical Security Parameters (CSPs) and Public Security Parameters (PSPs). The security requirements for SSP management encompass the entire lifecycle of SSPs employed by the module. SSP management includes random bit generators (RBGs), SSP generation, SSP establishment, SSP entry/output, SSP storage, and SSP zeroization. A module may contain one or more embedded modules each performing SSP management functions.

Encrypted CSPs refer to CSPs that are encrypted using an Approved or Allowed security function. CSPs encrypted using non-Approved and non-Allowed security functions are considered unprotected plaintext within the scope of this standard.

CSPs **shall** be protected within the module from unauthorized access, use, disclosure, modification, and substitution.

PSPs **shall** be protected within the module against unauthorized modification and substitution.

Keys used for self-tests specified in Section 4.9 are not considered SSPs. Hash values of passwords, RBG state information and intermediate key generation values **shall** be considered CSPs.

Documentation **shall** specify all SSPs employed by a module.

4.8.1 Random Bit Generators

A cryptographic module may contain RBGs, a chain of RBGs, or may be solely an RBG. All RBGs and their usage **shall** be defined and documented. All RBGs used in an Approved mode **shall** be Approved or Allowed and listed in Annexes A or B.

If entropy is collected from outside the cryptographic boundary of the module, the datastream generated using this entropy input **shall** be considered a CSP, and the module documentation **shall** specify the minimum entropy required by the module for each entered entropy input parameter. If the entropy is collected from within the cryptographic boundary of the cryptographic module, the minimum entropy and the generation method of the claimed minimum entropy **shall** be documented.

4.8.2 Sensitive Security Parameter Generation

A module may generate SSPs internally or they may be entered into the module. Documentation **shall** specify each SSP generation method employed by a module.

Any SSPs generated in the Approved mode of the module using an RBG **shall** be generated using an Approved or Allowed RBG meeting the requirements specified in Section 4.8.1. Compromising the security of the SSP generation method (e.g., guessing the seed value to initialize the deterministic RBG) **shall** require as least as many operations as determining the value of the generated key. Documentation **shall** specify each SSP generation method that makes use of an RBG.

SSPs generated by the module for use by an Approved or Allowed security function or key establishment technique **shall** be generated using an Approved or Allowed SSP generation method listed in Annexes C and D.

If random values are required in an Approved or Allowed security function(s), then an Approved or Allowed RBG **shall** be used to provide these values.

4.8.3 Sensitive Security Parameter Establishment

SSP establishment may consist of SSP transport followed by SSP entry or output, or it may consist of a SSP agreement process. The SSP transport process may be manual or electronic. SSP establishment may be performed by electronic SSP establishment methods (i.e., using SSP transport or SSP agreement schemes). All electronic SSP establishment methods employed in an Approved mode of operation **shall** be Approved or Allowed for use in an Approved mode listed in Annexes C and D.

If an SSP establishment method in an Approved mode requires random values as an input, an Approved or Allowed RBG **shall** be used to provide these values.

If an SSP transport method is used by a module, the SSPs transported in the process **shall** meet the requirements of Section 4.8.4.

Electronically transported CSPs **shall** be in encrypted form. The integrity of all electronically transported SSPs **shall** be cryptographically protected (e.g., by an Approved or Allowed security function or an Approved or Allowed key establishment method).

SECURITY LEVELS 1 AND 2

Manually transported CSP may be in plaintext or encrypted form.

SECURITY LEVELS 3 AND 4

Manually transported CSPs shall be either in encrypted form or split into components (see Split Knowledge). Electronically transported CSPs **shall** be encrypted. Other than when first establishing a Trusted Channel, SSPs **shall** be transported electronically over the Trusted Channel, whether or not they

are otherwise cryptographically protected. The Trusted Channel **shall** use only Approved or Allowed security functions.

Documentation **shall** specify all SSP establishment methods employed by a module.

4.8.4 Sensitive Security Parameter Entry and Output

SSPs may be entered into or output from a module manually or electronically. If SSPs are entered into or output from a module, the entry or output **shall** be through the defined HMI, SFMI, HFMI or HSMI (Section 4.2) interfaces. If SSPs are entered into or output from a module, the entry or output of SSPs is performed using manual (e.g., entered via a keyboard or number pad, or output via a visual display) or electronic (e.g., via a smart card/tokens, PC card, other electronic key loading device, or the module operating system) methods or some combination thereof.

Documentation **shall** specify the SSP entry and output methods employed by a module.

A module **shall** associate an SSP entered into or output from the module with the entity (i.e., person, group, role, or process) to which the SSP is assigned.

All cryptographically protected SSPs, entered into or output from the module and used in an Approved mode of operation, **shall** be encrypted using an Approved or Allowed security function.

During manual SSP entry, the entered values may be temporarily displayed to allow visual verification and to improve accuracy. If encrypted CSPs are manually entered into the module, then the plaintext values of the CSPs **shall not** be displayed. Manually entered (plaintext or encrypted) cryptographic keys (including seed keys) **shall** be verified during entry into a module for accuracy using the Manual Key Entry Test specified in Section 4.9.2.

To prevent the inadvertent output of sensitive information, two independent internal actions **shall** be required in order to output any CSP. These two independent internal actions **shall** be dedicated to mediating the output of the CSPs.

PSPs and CSPs that are not secret or private keys (e.g. passwords, authentication data) may be entered into or output from a module in plaintext form.

PSPs do not need to be cryptographically authenticated regardless of whether they are entered manually or electronically.

If split knowledge procedures are used:

- The module **shall** separately authenticate the operator entering or outputting each component as a separate identity.
- At least two components **shall** be required to reconstruct the original CSP.
- Documentation **shall** demonstrate that if knowledge of *n* components is required to reconstruct the original CSP, then knowledge of any *n-1* components provides no information about the original CSP other than the length.
- Documentation **shall** specify the split knowledge procedures employed by a module.

SECURITY LEVELS 1 AND 2

Plaintext CSPs may be entered and output via physical port(s) and logical interface(s) shared with other physical ports and logical interfaces of the cryptographic module. Input and output of CSPs over unencrypted wireless connections is not allowed.

For software modules, CSPs may be entered into or output from the module in either encrypted or plaintext form under control of the module operating system provided that the CSPs are maintained within the operational environment.

SECURITY LEVELS 3 AND 4

In addition to the requirements specified for Security Level 2, a cryptographic module **shall** utilize a Trusted Channel for the input or output of all SSPs, whether or not cryptographically protected. The Trusted Channel **shall** use only Approved or Allowed security functions.

Secret and private keys **shall** be entered into or output from the module using either one of the following methods:

- Encrypted
- Plaintext using a dedicated physical port
- Plaintext using split knowledge procedures (i.e. as two or more plaintext components)

If the module employs split knowledge procedures, then the module **shall** meet Security Level 3 or higher authentication (Section 4.3.2), and each key component **shall** be obtained from a different identity. The module **shall** verify that no two operators entering or outputting key components have the same identity.

4.8.5 Sensitive Security Parameter Storage

SSPs stored within a module may be stored either in plaintext or encrypted form. A module **shall** associate every SSP stored within the module with the entity (e.g., operator, role, or process) to which the SSP is assigned.

Documentation **shall** specify:

- The SSPs stored in the module.
- How CSPs are protected from unauthorized access, use, disclosure, modification, and substitution when stored in the module.
- How PSPs are protected from unauthorized modification and substitution when stored within the module.
- How the module associates a PSP stored in the module with the entity (operator, role, or process) to which the parameter is assigned.

Access to plaintext CSPs by unauthorized operators from outside the module **shall** be prohibited.
Modification of PSPs by unauthorized operators from outside the module **shall** be prohibited.

4.8.6 Sensitive Security Parameter Zeroization

A module **shall** provide methods to zeroize all CSPs within the module. Temporarily stored values (e.g. entropy input, RBG state, shared secret used in key establishment mechanism, etc.), key components owned by the module and CSPs should be zeroized when they are no longer needed for future use.

A zeroized SSP **shall** be unrecoverable from the module.

Zeroization of PSPs, encrypted CSPs, or CSPs otherwise physically or logically protected within an additional embedded validated module (meeting the requirements of this standard) is not required.

Documentation **shall** specify the zeroization method(s) employed by a module and the rationale as to how the method(s) prevent(s) the retrieval and reuse of the zeroized values.

SSPs need not meet these zeroization requirements if they are used exclusively to reveal plaintext data to processes that are authentication proxies (e.g. a CSP that is a module initialization key)

SECURITY LEVEL 1

The zeroization of CSPs may be performed procedurally by the module operator, and independent of the module's control (e.g., reformatting of a hard drive, the atmospheric destruction of a module during reentry).

SECURITY LEVELS 2 AND 3

In addition to the requirements of Security Level 1, the cryptographic module **shall** perform the zeroization of the CSPs (e.g. overwriting with all zeros or all ones or with random data). Zeroization **shall** exclude the overwriting of the CSP with another CSP. Temporary SSPs **shall** be zeroized when they are no longer needed. The module **shall** provide an output status indication when the zeroization is complete.

SECURITY LEVEL 4

In addition to the requirements of Security Level 3, the following requirements **shall** be met:

- The zeroization **shall** be immediate and non-interruptible and **shall** occur in a sufficiently small time period so as to prevent the recovery of the sensitive data between the time zeroization is initiated and the actual zeroization completed
- All CSPs **shall** be zeroized whether plaintext or cryptographically protected, such that the module is returned to the factory state

4.9 Self-Tests

A cryptographic module **shall** perform pre-operational self-tests and conditional self-tests to ensure that the module is functioning properly. All self-tests **shall** be performed, and determination of pass or fail **shall** be made by the module, without external controls, procedures or operator intervention.

The pre-operational self-tests **shall** be performed and passed successfully prior to the module providing any data output via the data output interface.

Conditional self-tests **shall** be performed when an applicable security function or process is invoked (i.e., security functions for which self-tests are required).

The module **shall** provide a status indication when it is operating in a degraded mode of operation. It is desirable for the module to indicate the conditional self-test(s) that failed

All self-tests identified in underlying algorithmic standards (Annexes A through E) **shall** be implemented as applicable within the cryptographic module. All self-tests identified in addition or in lieu of those specified in the underlying algorithmic standards (Annexes A through E) **shall** be implemented as specified in Annexes A through E for each cryptographic algorithm.

A cryptographic module may perform other pre-operational or conditional critical function tests in addition to the tests specified in this standard.

If a cryptographic module fails a self-test, the module **shall** enter an error state and **shall** output an error indicator as specified in Section 4.2.2. . The cryptographic module **shall not** perform any cryptographic operations or output data via the data output interface while in an error state. The cryptographic module **shall not** utilize any functionality that relies upon a function or algorithm that failed a self-test until the

relevant self-test has been repeated and successfully passed. If a module does not output an error status upon failure of a module self-test, the operator of the module **shall** be able to determine if the module has entered an error state through a procedure documented in the Security Policy.

At Security Levels 3 and 4, the module **shall** maintain an error log that is accessible by an authorized operator of the module. The error log **shall** provide information, at a minimum, the most recent error event (i.e. which self-test failed).

Documentation **shall** specify:

- The self-tests performed by a cryptographic module.
- The error states that a cryptographic module can enter when a self-test fails.
- The self-test success and failure status indicator
- The conditions and actions necessary to exit the error states and resume normal operation of a cryptographic module (e.g., this may include maintenance of the module, re-powering the module, automatic module recovery, entering a degraded mode of operation or returning the module to the vendor for servicing).

4.9.1 Pre-Operational Self-Tests

The pre-operational tests **shall** be performed and passed successfully by a cryptographic module between the time a cryptographic module is powered on or instantiated (after being powered off, reset, rebooted, cold-start, power interruption, etc.) and transition to the operational state. All data output via the data output interface **shall** be inhibited while performing the pre-operational self-tests.

A cryptographic module **shall** perform the following pre-operational tests, as applicable:

- Pre-Operational Software/Firmware Integrity Test,
- Pre-Operational Bypass Test and
- Pre-Operational Critical Functions Test.

4.9.1.1 Pre-Operational Software/Firmware Integrity Test

All software and firmware components within the cryptographic boundary **shall** be verified using an Approved *integrity technique* as specified in Section 4.4. If the verification fails, the Pre-Operational Software/Firmware Integrity Test **shall** fail. The Pre-Operational Software/Firmware Integrity Test is not required for any software or firmware excluded from the security requirements of this standard or for any executable code stored in non-reconfigurable memory.

4.9.1.2 Pre-Operational Bypass Test

If a cryptographic module implements a *bypass* capability, then the module **shall** ensure the correct operation of the logic governing activation of the bypass capability by exercising that logic. The module **shall** also verify the data path by:

- setting the bypass switch to provide cryptographic processing and verify that data transferred through the bypass mechanism is cryptographically processed, and
- setting the bypass switch to not provide cryptographic processing and verify that data transferred through the bypass mechanism is not cryptographically processed.

4.9.1.3 Pre-Operational Critical Functions Test

There may be other security functions critical to the secure operation of a cryptographic module that **shall** be tested as a pre-operational test. Documentation **shall** specify the pre-operational critical functions that are tested.

4.9.2 Conditional Self-Tests

Conditional self-tests **shall** be performed by a cryptographic module when the conditions specified for the following tests occur: Cryptographic Algorithm Self-Test, Pair-Wise Consistency Test, Software/Firmware Load Test, Manual Key Entry Test, Conditional Bypass Test and Conditional Critical Functions Test.

4.9.2.1 Conditional Cryptographic Algorithm Self-Test

Cryptographic Algorithm Self-Test. A cryptographic algorithm test **shall** be conducted for all cryptographic functions (e.g. security functions, key establishment techniques and authentication) of each Approved or Allowed cryptographic algorithm implemented in the cryptographic module as specified in Annexes A through E. The conditional test **shall** be performed prior to the first operational use of the cryptographic algorithm. The cryptographic algorithm self-test may be performed as a pre-operational test.

In lieu of the conditional algorithm self-test, the following may be implemented:

- If a cryptographic module includes two independent implementations of the same cryptographic algorithm, then the module **shall** continuously compare the outputs of the two implementations, and, if the outputs of the two implementations are not equal, the cryptographic algorithm test **shall** fail,

4.9.2.2 Conditional Pair-Wise Consistency Test

If a cryptographic module generates public or private key pairs, a pair-wise consistency test **shall** be performed for every generated public and private key pair as specified in Annexes A through E for the applicable cryptographic algorithm.

4.9.2.3 Conditional Software/Firmware Load Test

If software or firmware can be externally loaded into a cryptographic module, then the following Software/Firmware Load Tests **shall** be performed:

- An Approved digital signature technique **shall** be applied to all *validated* software or firmware when externally loaded into a cryptographic module. All loaded software and firmware **shall** be validated. When the applied Approved digital signature technique is used, requirements in clause 4.9.2.1 **shall** also be met.

- The applied Approved digital signature technique **shall** be successfully verified or the Software/Firmware Load Test **shall** fail. Loaded software or firmware **shall not** be used if the Software/Firmware Load Test fails.

4.9.2.4 Conditional Manual Key Entry Test

If cryptographic keys or key components are manually entered into a cryptographic module or if error on the part of the human operator could result in the incorrect entry of the intended key, then the following manual key entry tests **shall** be performed:

- The cryptographic key or key components **shall** have an error detection code (EDC) applied, or **shall** be entered using duplicate entries.

- If an EDC is used, the EDC **shall** be at least 32 bits in length.

- If the EDC cannot be verified, or the duplicate entries do not match, the test **shall** fail.

4.9.2.5 Conditional Bypass Test

If a cryptographic module implements a bypass capability where the services may be provided without cryptographic processing (e.g., transferring plaintext through the module), then the tests mentioned below are defining the suite of bypass tests and **shall** be performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext.

A cryptographic module **shall** test for the correct operation of the services providing cryptographic processing when a switch takes place between an exclusive bypass service and an exclusive cryptographic service.

If a cryptographic module can automatically alternate between a bypass service and a cryptographic service, providing some services with cryptographic processing and some services without cryptographic processing, then the module **shall** test for the correct operation of the services providing cryptographic processing when the mechanism governing the switching procedure is modified (e.g., an IP address source/destination table).

If a cryptographic module maintains internal information that governs the bypass capability, then the module **shall** verify the integrity of the governing information through an Approved integrity technique immediately preceding modification of the governing information, and **shall** generate a new integrity value using the Approved integrity technique immediately following the modification.

The mechanism or logic governing the switching procedure **shall** be defined and documented.

4.9.2.6 Conditional Critical Functions Tests

There may be other security functions critical to the secure operation of a cryptographic module that **shall** be tested as a conditional self-test. Documentation **shall** specify the conditional critical functions that are tested.

4.9.3 Periodic Self-Tests

SECURITY LEVELS 1 AND 2

At Security Levels 1 and 2, a cryptographic module **shall** permit operators to initiate the pre-conditional and conditional self-tests on demand for periodic testing of the module. Acceptable means for the on-demand initiation of periodic self-tests are: resetting, rebooting, and power.

SECURITY LEVELS 3 AND 4

At Security Levels 3 and 4, the module vendor **shall** specify a critical time period that identifies the maximum operational time before self-tests must be repeated and any conditions associated with repeating these self-tests. The time period and the policy regarding any conditions that may result in the interruption of the module's operations during the time to repeat the self-tests **shall** be specified (see Appendix B.)

4.10 Life-Cycle Assurance

Life-cycle assurance refers to the use of best practices by the vendor of a cryptographic module during the design, development, and operation of a cryptographic module, providing assurance that the module is properly designed, developed, tested, configured, delivered, and installed, and that the proper operator guidance documentation is provided. Security requirements are specified for configuration management, design, finite state model, development, testing, delivery and operation, and guidance documentation.

4.10.1 Configuration Management

Configuration management specifies the requirements for a configuration management system implemented by a cryptographic module vendor, providing assurance that the integrity of the cryptographic module is preserved by requiring discipline and control in the processes of refinement and modification of the cryptographic module and related documentation. A configuration management system is put in place to prevent accidental or unauthorized modifications to, and provide change traceability for, the cryptographic module and related documentation.

SECURITY LEVELS 1 AND 2

The following security requirements **shall** apply to cryptographic modules for Security Levels 1 and 2.

- A configuration management system **shall** be used for the development of a cryptographic module and module components within the cryptographic boundary, and of associated module documentation.
- Each version of each configuration item (e.g., cryptographic module, module hardware parts, module software components, module HDL, user guidance, Security Policy, etc.) that comprises the module and associated documentation **shall** be assigned and labeled with a unique identification number.
- The configuration management system **shall** track and maintain the changes to the identification and version or revision of each configuration item throughout the life-cycle of the validated cryptographic module.
- Documentation **shall** specify and describe the configuration management system used for the cryptographic module.
- Documentation **shall** describe the support for the development of the cryptographic module and associated documents provided by the configuration management system.

SECURITY LEVELS 3 AND 4

In addition to the requirements for Security Levels 1 and 2, the configuration items **shall** be managed using an automated configuration management system.

4.10.2 Design

A design is an engineering solution that addresses the functional specification for a cryptographic module. The design is intended to provide assurance that the functional specification of a cryptographic module corresponds to the intended functionality described in the Security Policy.

Cryptographic modules **shall** be designed to allow the testing of all provided security related services.

SECURITY LEVEL 1

The following requirements **shall** apply to a cryptographic module for Security Level 1:

- Documentation **shall** specify the correspondence between the design of the hardware, software and/or firmware components of a cryptographic module, and the cryptographic module's Security Policy and FSM.

SECURITY LEVEL 2

In addition to the requirement for Security Level 1, the following requirement **shall** apply to a cryptographic module for Security Level 2:

- Documentation **shall** include a functional specification that informally describes the cryptographic module, the functionality of the cryptographic module, the external physical ports and logical interfaces of the cryptographic module, and the purpose of the physical ports and logical interfaces.

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirements **shall** apply to a cryptographic module for Security Level 3:

- Documentation **shall** specify the detailed design that describes the internal functionality of the cryptographic module's major components, the internal component interfaces, the purpose of the component interfaces, and the internal information flow (within the cryptographic boundary as a whole and also within the major components).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2, and 3, the following requirement **shall** apply to cryptographic modules for Security Level 4:

- Documentation **shall** specify an informal proof (including the pre-conditions and the post-conditions) of the correspondence between the design of the cryptographic module and the functional specification.

4.10.3 Finite State Model

The operation of a cryptographic module **shall** be specified using a Finite State Model (or equivalent) represented by a state transition diagram and a state transition table and state descriptions. The FSM **shall** be sufficiently detailed to demonstrate that the cryptographic module complies with all of the requirements of this standard.

Documentation **shall** include the FSM (or equivalent) using a state transition diagram and state transition table and state descriptions that **shall** specify:

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

The FSM of a cryptographic module **shall** include, as a minimum, the following operational and error states:

Power on/off state. A state in which the module is powered off, placed in standby mode (volatile memory maintained), or the operational state preserved in non-volatile memory (e.g. hibernation mode) and in which primary, secondary, or backup power is applied to the module. This state may distinguish between power sources being applied to a cryptographic module. For a software module, power on is the action of spawning an executable image of the cryptographic module.

General initialization state: A state in which the cryptographic module is undergoing initializing before the module transitions to the Approved state.

Crypto Officer State: a state in which the Crypto Officer services are performed (e.g., cryptographic initialization, secure administration, and key management).

CSP entry state: a state for entering the CSPs into the cryptographic module.

User state: (if a User role is implemented): a state in which authorized users obtain security services, perform cryptographic operations, or perform other Approved functions.

Approved state: a state in which Approved security functions are performed.

Self-test state: a state in which the cryptographic module is performing self-tests.

Error state: a state when the cryptographic module has encountered an error condition (e.g., failed a self-test). There may be one or more error conditions that result in a single module error state. Error states may include "hard" errors that indicate an equipment malfunction and that may require maintenance, service or repair of the cryptographic module, or recoverable "soft" errors that may require initialization or resetting of the module. Recovery from error states **shall** be possible, except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.

Each distinct cryptographic module service, security function use, error state, self-test, or operator authentication **shall** be depicted as a separate state.

Changing to the Crypto Officer state from any other role other than the Crypto Officer **shall** be prohibited.

A cryptographic module may contain other states including, but not limited to, the following:

Bypass state: a state in which a service, as a result of module configuration or operator intervention, causes the plaintext output of a particular data or status item that would normally be output in encrypted form.

Quiescent state: a state in which the cryptographic module is dormant (e.g., low power, suspended or in hibernation.)

4.10.4 Development

A proper *development* process provides assurance that the implementation of a cryptographic module corresponds to the module functional specification and Security Policy, that the cryptographic module is maintainable, and that the validated cryptographic module is reproducible. This section specifies the security requirements for the representation of a cryptographic module's security functionality at various levels of abstraction from the functional specification to the implementation representation.

SECURITY LEVEL 1

The following requirements **shall** apply to cryptographic modules for Security Level 1:

- If a cryptographic module contains software or firmware, the source code, language reference, the compilers, compiler versions and compiler options, the linker and linker options, the runtime libraries and runtime library settings, configuration settings, build processes and methods, the build options, environmental variables and all other resources used to compile and link the source code into an executable form **shall** be tracked using the configuration management system.

- The documentation **shall** also include the source code for the software or firmware, annotated with comments that depict the correspondence of the software or firmware to the design of the module.

- If a cryptographic module contains hardware, documentation **shall** specify the schematics and/or Hardware Description Language (HDL), as applicable. The HDL **shall** be annotated with comments that depict the correspondence of the hardware to the design of the module.

- For software and firmware cryptographic modules and the software or firmware component of a hybrid module:

  - The result of the integrity and authentication technique mechanisms specified in Sections 4.4 and 4.9 **shall** be calculated and integrated into the software or firmware module by the vendor during the module development.

  - The cryptographic module documentation **shall** specify the compiler, configuration settings and methods to compile the source code into an executable form.

  - The cryptographic module **shall** be developed using production-grade development tools (e.g., compilers).

SECURITY LEVELS 2 AND 3

In addition to the requirements for Security Level 1, the following requirements **shall** apply to cryptographic modules for Security Levels 2 and 3:

- All software or firmware within a cryptographic module **shall** be implemented using a high-level, non-proprietary language. Rationale **shall** be provided for the use of a low-level language (e.g., assembly language or microcode) if essential to the performance of the module or when a high-level language is not available.

- Custom integrated circuits within a cryptographic module **shall** be implemented using a high-level Hardware Description Language (HDL) (e.g., VHDL or Verilog).

- Software cryptographic modules **shall** be designed and implemented in a manner that avoids the use of code, parameters or symbols not necessary for the module's functionality and execution.

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2 and 3, the following requirement **shall** apply to cryptographic modules for Security Level 4:

- For each cryptographic module hardware and software component, the documentation **shall** be annotated with comments that specify (1) the pre-conditions required upon entry into the module component, function, or procedure in order to execute correctly and (2) the post-conditions expected to be true when the execution of the module component, function, or procedure is complete. The pre-conditions and post-conditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of the cryptographic module component, function, or procedure.

4.10.5 Vendor Testing

This section specifies the requirements for *vendor testing* of the cryptographic module, including testing of the security functionality implemented in the cryptographic module, providing assurance that the cryptographic module behaves in accordance with the module Security Policy and functional specifications.

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, documentation **shall** specify the functional testing performed on the cryptographic module.

For software or firmware cryptographic modules and the software or firmware component of a hybrid module, the vendor **shall** use current automated security diagnostic tools (e.g. detect buffer overflow, etc).

SECURITY LEVELS 3 AND 4

In addition to the requirements for Security Levels 1 and 2, documentation **shall** specify the procedures for and the results of low-level testing performed on the cryptographic module.

4.10.6 Delivery and Operation

This section specifies the security requirements for the secure delivery, installation, and startup of a cryptographic module, providing assurance that the module is securely delivered to authorized operators, and is installed and initialized in a correct and secure manner.

SECURITY LEVEL 1

For Security Level 1, documentation **shall** specify the procedures for secure installation, initialization, and startup of the cryptographic module.

SECURITY LEVELS 2 AND 3

In addition to the requirement of Security Level 1, documentation **shall** specify the procedures required for maintaining security while distributing, installation and the initialization of versions of a cryptographic module to authorized operators. The procedures **shall** specify how to detect tamper during the delivery, installation and initialization of the module to the authorized operators.

SECURITY LEVELS 4

In addition to the requirements of Security Levels 2 and 3, the procedures **shall** require the authorized operator to authenticate to the module using authentication data provided by the vendor.

4.10.7 Guidance Documents

The requirements in this section are intended to ensure that all entities using the cryptographic module have adequate guidance and procedures to administer and use the module in an Approved mode of operation.

Guidance documentation consists of administrator and non-administrator guidance.

Administrator guidance **shall** specify:

- The administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the Crypto Officer and/or other administrative roles.

- Procedures required to keep independent operator authentication mechanisms functionally independent.

- Procedures on how to administer the cryptographic module in an Approved mode of operation,

- Assumptions regarding User behavior that are relevant to the secure operation of the cryptographic module.

Non-administrator guidance **shall** specify:

- The Approved, Allowed and non-Approved security functions, physical ports, and logical interfaces available to the users of a cryptographic module.

- All User responsibilities necessary for the Approved mode of operation of a cryptographic module.

4.11 Mitigation of Other Attacks

Susceptibility of a cryptographic module to attacks not defined elsewhere in this standard depends on the module type, implementation, and implementation environment. Such attacks may be of particular concern for cryptographic modules implemented in hostile environments (e.g., where the attackers may be the authorized operators of the module). These attacks generally rely on the analysis of information obtained from sources that are physically external to the module. In all cases, the attacks attempt to determine some knowledge about the CSPs within the cryptographic module.

SECURITY LEVELS 1, 2 AND 3

If a cryptographic module is designed to mitigate one or more specific attack(s) not defined elsewhere in this standard, then the module's supporting documents **shall** enumerate the attack(s) the module is designed to mitigate. The existence and proper functioning of the security mechanisms used to mitigate the attack(s) will be validated when requirements and associated tests are developed.

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2 and 3, the following requirement **shall** apply to cryptographic modules for Security Levels 4:

- If the mitigation of specific attacks not defined elsewhere in this standard is claimed, documentation **shall** specify the methods used to mitigate the attacks and the methods to test the effectiveness of mitigation techniques.

APPENDIX A: SUMMARY OF DOCUMENTATION REQUIREMENTS

The following check list summarizes the documentation requirements of this standard. All documentation **shall** be provided to the testing facility by the vendor of a cryptographic module.

CRYPTOGRAPHIC MODULE SPECIFICATION

- Specification of the hardware, software and firmware configuration items of a cryptographic module, specification of the cryptographic boundary surrounding these items, and description of the physical configuration of the module. *(Security Levels 1, 2, 3 and 4)*
- Specification of any hardware, software or firmware configuration items of a cryptographic module that are excluded from the security requirements of this standard and an explanation of the rationale for the exclusion. *(Security Levels 1, 2, 3 and 4)*
- Specification of the physical ports and logical interfaces of a cryptographic module. *(Security Levels 1, 2, 3 and 4)*
- Specification of the manual or logical controls of a cryptographic module, physical or logical status indicators, and applicable physical, logical, and electrical characteristics. *(Security Levels 1, 2, 3 and 4)*
- List of all security functions, both Approved, Allowed and non-Approved, that are employed by a cryptographic module and specification of all modes of operation, both Approved, Allowed and non-Approved. *(Security Levels 1, 2, 3 and 4)*
- Block diagram depicting all of the major hardware components of a cryptographic module and component interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory. *(Security Levels 1, 2, 3 and 4)*
- Specification of the design of the hardware, software and firmware of a cryptographic module. *(Security Levels 1, 2, 3 and 4)*
- Specification of all security-related information, including secret and private cryptographic keys (both plaintext and encrypted), authentication data (e.g., passwords, PINs), other CSPs, and other protected information (e.g., audited events, audit data) whose disclosure or modification can compromise the security of the cryptographic module.
- Description of how to set the module in an Approved mode of operation.
- Vendor testing documentation
- Specification of a cryptographic module Security Policy including the rules derived from the requirements of this standard and the rules derived from any additional requirements imposed by the vendor. *(Security Levels 1, 2, 3 and 4)*

CRYPTOGRAPHIC MODULE PHYSICAL PORTS AND LOGICAL INTERFACES

- Specification of the physical ports and logical interfaces of a cryptographic module and all defined input and output data paths. *(Security Levels 1, 2, 3 and 4)*
- Specification of the Trusted Channel. *(Security Levels 2 - when optionally implemented, 3 and 4)*

ROLES, AUTHENTICATION, AND SERVICES

- Specification of all authorized roles supported by a cryptographic module. *(Security Levels 1, 2, 3 and 4)*

- Specification of the services, operations, or functions provided by a cryptographic module, both Approved and non-Approved. For each service, specification of the service input, corresponding service output, and the authorized role(s) in which the service can be performed. *(Security Levels 1, 2, 3 and 4)*

- Specification of any services provided by a cryptographic module for which the operator is not required to assume an authorized role, and how these services do not modify, disclose, or substitute cryptographic keys and other CSPs, or otherwise affect the security of the module. *(Security Levels 1, 2, 3 and 4)*

- Specification of the authentication mechanisms supported by a cryptographic module, the types of authentication data required to implement supported authentication mechanisms, the authorized methods used to control access to the module for the first time and initialize the authentication mechanism, and the strength of the authentication mechanisms supported by the module, including the rationale supporting the use of multiple authentication mechanisms. *(Security Levels 2, 3 and 4)*

SOFTWARE/FIRMWARE SECURITY

- Specification of Approved integrity techniques used *(Security Levels 1, 2, 3 and 4).*

- Specification of the SFMI, HSMI and HFMI commands employed by the module *(Security Levels 1, 2, 3 and 4).*

OPERATIONAL ENVIRONMENT

- Specification of the modifiable operational environment for the cryptographic module. *(Security Levels 1 and 2).*

PHYSICAL SECURITY

- Specification of the physical embodiment and security level for which the physical security mechanisms of a cryptographic module are implemented. Specification of the physical security mechanisms that are employed by a module. *(Security Levels 1, 2, 3 and 4)*

- If a cryptographic module includes a maintenance role that requires physical access to the contents of the module, or if the module is designed to permit physical access, specification of the maintenance access interface and how plaintext secret and private keys and other CSPs are to be zeroized when the maintenance access interface is accessed. *(Security Levels 1, 2, 3 and 4)*

- Specification of the normal operating ranges of a cryptographic module. Specification of the environmental failure protection features employed by a cryptographic module or specification of the environmental failure tests performed. *(Security Levels 4)*

PHYSICAL SECURITY – NON-INVASIVE ATTACKS

- Specification of the mitigation techniques against non-invasive attacks listed in Annex F. *(Security Levels 3 and 4)*

SENSITIVE SECURITY PARAMETER MANAGEMENT

- Specification of all cryptographic keys, cryptographic key components, and other SSPs employed by a cryptographic module.

- Specification of each RBG (Approved RBGs, Allowed RBGs, and entropy sources) employed by a cryptographic module. *(Security Levels 1, 2, 3 and 4)*

- Specification of each of the key generation methods (Approved and Allowed) employed by a cryptographic module. *(Security Levels 1, 2, 3 and 4)*

- Specification of the key establishment methods employed by a cryptographic module. *(Security Levels 1, 2, 3 and 4)*

- Specification of the key entry and output methods employed by a cryptographic module. *(Security Levels 1, 2, 3 and 4)*

- If split knowledge procedures are used, proof that if knowledge of *n* key components is required to reconstruct the original key, then knowledge that any *n*-1 key components provides no information about the original key other than the key's length. *(Security Levels 3 and 4)*

- Specification of the SSP storage methods employed by a cryptographic module. *(Security Levels 1, 2, 3 and 4)*

- Specification of the CSP zeroization methods employed by a cryptographic module. *(Security Levels 1, 2, 3 and 4)*

SELF-TESTS

- Specification of self-tests performed by a cryptographic module, including pre-operational, conditional, and critical functions tests. *(Security Levels 1, 2, 3 and 4)*

- Specification of the error states that a cryptographic module can enter when a self-test fails, and the conditions and actions necessary to exit the error states and resume normal operation of a module. *(Security Levels 1, 2, 3 and 4)*

- Specification of all security functions critical to the secure operation of a cryptographic module and identification of the applicable pre-operational, conditional, and critical functions tests performed by the module. *(Security Levels 1, 2, 3 and 4)*

- If a cryptographic module implements a bypass capability, specification of the mechanism or logic governing the switching procedure. *(Security Levels 1, 2, 3 and 4)*

LIFE-CYCLE ASSURANCE

- Specification of procedures for secure installation, generation, and start-up of a cryptographic module. *(Security Levels 1, 2, 3 and 4)*

- Specification of the procedures for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators. *(Security Levels 2, 3 and 4)*

- Specification of the correspondence between the design of the hardware and software of a cryptographic module and the cryptographic module Security Policy (i.e., the rules of operation). *(Security Levels 1, 2, 3 and 4)*

- If a cryptographic module contains software, specification of the source code for the software, annotated with comments that clearly depict the correspondence of the software to the design of the module. *(Security Levels 1, 2, 3 and 4)*

- If a cryptographic module contains hardware, specification of the schematics and/or the HDL listings for the hardware. *(Security Levels 1, 2, 3 and 4)*

- Functional specification that informally describes a cryptographic module, the external ports and interfaces of the module, and the purpose of the interfaces. *(Security Levels 2, 3 and 4)*

- Specification of an informal proof (including the pre-conditions and the post conditions) of the correspondence between the design of the cryptographic module and the functional specification. *(Security Level 4)*

- For each hardware and software component, source code annotation with comments that specify (1) the pre-conditions required upon entry into the module component, function or procedure in order to execute correctly and (2) the post-conditions expected to be true when the execution of the module component, function, or procedure is complete. *(Security Level 4)*

- For Administrator guidance, specification of:

  - the administrative functions, security events, security parameters (and parameter values, as appropriate), physical ports, and logical interfaces of the cryptographic module available to the Crypto Officer *(Security Levels 1, 2, 3 and 4)*,

  - procedures on how to administer the cryptographic module in a secure manner *(Security Levels 1, 2, 3 and 4)*, and

  - assumptions regarding user behavior that is relevant to the secure operation of the cryptographic module. *(Security Levels 1, 2, 3 and 4)*

- For non-administrator guidance, specification of

  - the Approved security functions, physical ports, and logical interfaces available to the users of the cryptographic module *(Security Levels 1, 2, 3 and 4)*, and

  - all user responsibilities necessary for the secure operation of the module. *(Security Levels 1, 2, 3 and 4)*

MITIGATION OF OTHER ATTACKS

- If a cryptographic module is designed to mitigate one or more specific attacks not defined elsewhere in this standard, enumerate in the module's documentation the security mechanisms employed by the cryptographic module to mitigate the attack(s). *(Security Levels 1, 2,and 3)*

- If a cryptographic module is designed to mitigate one or more specific attacks not defined elsewhere in this standard, document the methods used to mitigate the attacks and the methods to test the effectiveness of mitigation techniques. *(Security Levels 4)*

SECURITY POLICY

- See Appendix B. *(Security Levels 1, 2, 3 and 4)*

APPENDIX B: CRYPTOGRAPHIC MODULE SECURITY POLICY

The following list summarizes requirements that **shall** be provided in the non-proprietary Security Policy. The format of the Security Policy **shall** be presented in the order indicated in this Appendix. The Security Policy **shall not** be marked as proprietary or copyrighted without a statement allowing copying or distribution.

0. Introduction

- The security policy **shall** discuss how the cryptographic module complies with the requirements of the standard.

1. Cryptographic Module Specification

- Purpose of the module.
- Illustrative diagram, schematic or photograph of the module. If a hardware module, a photograph **shall** be included. If the Security policy encompasses multiple versions of the module, each version **shall** be represented separately or annotated that the representation is illustrated for all versions. For a software or firmware cryptographic module, the security policy **shall** include a block diagram that illustrates:
  - The location of the logical object of the software or firmware module with respect to the operating system, other supporting applications and the cryptographic boundary so that all the logical and physical layers between the logical object and the cryptographic boundary are clearly defined.
  - The interactions of the logical object of the software or firmware module with the operating system and other supporting applications resident within the cryptographic boundary.
- Description of Module(s).
  - Provide explicit version/identification of the module and all components (hardware, software or firmware).
- Hardware, Software, Firmware, or Hybrid designation.
  - For software, firmware and hybrid cryptographic modules, list the Operating system(s) the module was tested on and list the Operating system(s) that the vendor affirms can be used by the module.
- Overall Security Level of the module and the Security Levels of individual areas.
- Precise definition of the module's physical and cryptographic boundaries.
  - The hardware, software or firmware excluded from the cryptographic boundaries **shall** be specified in the security policy.
- Approved and non-Approved modes of operation and how to enter/exit each mode.
- Table of all security functions, with specific key strengths employed in both Approved and Non-Approved modes, as well as the implemented modes of operation (e.g. CBC, CCM), if appropriate.
- Table of all callable services.
- Block Diagram, as applicable.
- Table of all SSPs, with information about their input/output, generation, zeroization, etc.
- Overall security design and the rules of operation.
- For Security Levels 1 and 2, the operation of the cryptographic module in an Approved mode **shall**, at a minimum, be by policy as specified in the security policy.
- The security policy **shall** describe each Approved mode of operation implemented in the cryptographic module and how each mode is configured

2. Cryptographic Module Ports and Interfaces

- Table listing of all ports and interfaces (physical and logical).
- Define the information passing over the four logical interfaces.

- Specify physical ports and data that pass over them.
- Specify Trusted Channel.

3. Roles, Services, and Authentication

- Specify all roles.
- Table of Roles, with corresponding service commands with input and output.
- Specify each authentication method, whether the method is Identity or Role-based and the method is required.
- How is the strength of authentication requirement met?
- If there is a bypass capability, what are the two independent actions?
- If there is a bypass capability, how is the status indicated?
- If external software or firmware is loaded, specify the controls on loading and the isolation of code that deter unauthorized access to and use of the module.
- Separately list the security and non-security services.
- Describe the installation process and the cryptographic authentication mechanism(s).

4. Software/Firmware Security

- Define the module's physical and cryptographic boundaries, contents, and logical security mechanisms.
- How is the code protected from replacement?
- How is the code obfuscated?
- What are the tamper detection and response capabilities?

5. Operational Environment

- Is the module non-modifiable, limited, or modifiable?
- Identify the operating system and tested platform.
- For applicable level, explain how requirements are met.

6. Physical Security

- Specify the embodiment (single-chip, multi-chip embedded or multi-chip standalone).
- List the physical security mechanisms, how requirements for the embodiment and security level are met, and how the operator can determine that there has been a compromise.

7. Physical Security – Non-Invasive Attacks

- For Security Level 3 and 4 modules, describe how the single-chip cryptographic module and single-chip components of hybrid module provides protection for the CSPs against non-invasive attacks and the effectiveness of the mitigation techniques, for all attacks listed in Annex F.

8. Sensitive Security Parameters Management

- Provide a key table specifying the key type(s), strength(s) in bits, security function(s), security function certification number(s), where and how the key(s) is generated, whether the key(s) is imported or exported, any key establishment method used and indicate any related keys.
- Present a table of other SSPs and how they are generated.
- Specify the Random Bit Generators (Approved or Allowed).
- Describe the uses of RBG output(s).
- Specify the RBG entropy source(s).
- Specify the electronic and manual key I/O method(s).
- Specify the SSP storage technique(s).
- Specify the CSP zeroization method(s) and rationale, and operator initiation capability.

9. Self-Tests

- Provide the list of pre-operational and conditional self-tests with defined parameters and list conditions under which the tests are performed.
- Specify the time period and the policy regarding any conditions that may result in the interruption of the module's operations during the time to repeat the period self-tests.
- Describe all error states and status indicators.
- Describe operation initiation, if applicable.

10. Life-Cycle Assurance

- Specify the procedures for secure installation, initialization, startup and operation of the module.
- Specify any maintenance requirements.
- Provide the Administrator and non-Administrator guidance (may be a separate document).

11. Mitigation of Other Attacks

- List what other attacks are mitigated.
- List security-relevant guidance and constraints.

APPENDIX C: SELECTED BIBLIOGRAPHY

National Institute of Standards and Technology, *FIPS 140-3 Annex A: Approved Security Functions*, available at URL: http://csrc.nist.gov/publications/PubsFIPS.html.

National Institute of Standards and Technology, *FIPS 140-3 Annex B: Allowed Security Functions*, available at URL: http://csrc.nist.gov/publications/PubsFIPS.html.

National Institute of Standards and Technology, *FIPS 140-3 Annex C: Approved SSP Management Techniques*, available at URL: http://csrc.nist.gov/publications/PubsFIPS.html.

National Institute of Standards and Technology, *FIPS 140-3 Annex D: Allowed SSP Management Techniques*, available at URL: http://csrc.nist.gov/publications/PubsFIPS.html.

National Institute of Standards and Technology, *FIPS 140-3 Annex E: Approved Authentication Mechanisms*, available at URL: http://csrc.nist.gov/publications/PubsFIPS.html

National Institute of Standards and Technology, *FIPS 140-3 Annex F: Non-invasive attack Methods*, available at URL: http://csrc.nist.gov/publications/PubsFIPS.html.

National Institute of Standards and Technology, *FIPS 140-3 Annex G: Allowed Operating Environments*, available at URL: http://csrc.nist.gov/publications/PubsFIPS.html.

National Institute of Standards and Technology, *SP 800-90: Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)*, available at URL: http://csrc.nist.gov/publications/PubsSPs.html.