FIPS PUB 140-3 (DRAFT)

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

Technology Administration
Under Secretary for Technology

National Institute of Standards and Technology
Director

DRAFT

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 publication provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides five 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 and implementation 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).

DRAFT

TABLE OF CONTENTS

1. OVERVIEW 1
1.1 Security Level 1 2
1.2 Security Level 2 2
1.3 Security Level 3 2
1.4 Security Level 4 3
1.5 Security Level 5 4
2. GLOSSARY OF TERMS AND ACRONYMS 5
2.1 Glossary of Terms 5
2.2 Acronyms 11
3. FUNCTIONAL SECURITY OBJECTIVES 13
4. SECURITY REQUIREMENTS 14
4.1 Cryptographic Module Specification 16
4.1.1 Types of Cryptographic Modules 16
4.1.2 Cryptographic Boundary 16
4.1.3 Multiple Approved Modes of Operations 17
4.1.4 Degraded Functionality 17
4.1.5 Security Strength of the Module 17
4.2 Cryptographic Module Physical Ports and Logical Interfaces 17
4.3 Roles, Authentication, and Services 18
4.3.1 Roles 19
4.3.2 Operator Authentication 19
4.3.3 Services 21
4.4 Software Security 22
4.5 Operational Environment 24
4.5.1 Operating System Requirements for Modifiable Operational Environments 25
4.6 Physical Security 27
4.6.1 General Physical Security Requirements 29
4.6.2 Single-Chip Cryptographic Modules 30
4.6.3 Multiple-Chip Embedded Cryptographic Modules 31
4.6.4 Multiple-Chip Standalone Cryptographic Modules 33
4.6.5 Environmental Failure Protection/Testing 34
4.7 Physical Security – Non-Invasive Attacks 35
4.8 Sensitive Security Parameter Management 36
4.8.1 Random Bit Generators 36
4.8.2 SSP Generation 37
4.8.3 SSP Establishment 37
4.8.4 SSP Entry and Output 37
4.8.5 SSP Storage 38
4.8.6 SSP Zeroization 39
4.9 Self-Tests 40
4.9.1 Pre-Operational Self-Tests 40
4.9.2 Conditional Self-Tests 41
4.9.3 Critical Functions Tests 43
4.10 Life-Cycle Assurance 43
4.10.1 Configuration Management 43
4.10.2 Design 44
4.10.3 Finite State Model 45
4.10.4 Development 46
4.10.5 Vendor Testing 47
4.10.6 Delivery and Operation 47
4.10.7 Guidance Documents 48
4.11 Mitigation of Other Attacks 48
APPENDIX A: SUMMARY OF DOCUMENTATION REQUIREMENTS 50

DRAFT

APPENDIX B: RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES 54
APPENDIX C: CRYPTOGRAPHIC MODULE SECURITY POLICY..... 56
APPENDIX D: SELECTED BIBLIOGRAPHY..... 59

DRAFT

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 an additional security level and incorporates extended and new security features that reflect recent advances in technology. In FIPS 140-3, each of the eleven requirement areas in redefined. Software requirements are given greater prominence in a new area dedicated to software security, and an area specifying requirements to protect against non-invasive attacks is provided.

While the security requirements specified in this standard are intended to maintain the security provided by a cryptographic module, conformance to this standard is not sufficient to ensure that a particular module is secure. The operator of a cryptographic module is responsible for ensuring that the security provided by the module 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 validated 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 five 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, and D, which are referenced herein, can be found in APPENDIX D of this standard, SELECTED BIBLIOGRAPHY.

DRAFT

1.1 Security Level 1

Security Level 1 provides the lowest level of assurance. Basic security requirements are specified for a cryptographic module (e.g., at least one Approved security function must be used). No specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components.

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. Such implementations may be appropriate for security applications where controls, such as physical security, network security, and administrative procedures are provided outside of the module. The implementation of Level 1 cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements.

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 the authorization of an operator to assume a specific role and perform a corresponding set of services.

Security Level 2 allows the software components of a cryptographic module to be executed on a general purpose computing system using an operating system that

- provides discretionary access controls that protect against unauthorized execution, modification, and reading of cryptographic software, and

- provides audit mechanisms to record modifications, accesses, deletions, and additions of cryptographic data and sensitive security parameters.

An operating system implementing these controls provides a level of trust (logical protection) so that cryptographic modules executing on general purpose computing platforms are comparable to cryptographic modules implemented using dedicated hardware systems.

1.3 Security Level 3

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent 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 that provide direct physical access, and use of or modification of the cryptographic module. 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 ports that are physically separated from other ports, or

DRAFT

interfaces that are logically separated using a trusted channel from other interfaces. CSPs may either be entered into or output from the cryptographic module in encrypted form or using a split knowledge procedure.

Security Level 3 requires mechanisms to protect CSPs against timing analysis attacks.

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

Security Level 3 allows the software components of a cryptographic module to be executed on a general purpose computing system using an operating system that

- prevents operators in the user role from modifying cryptographic module software, system Sensitive Security Parameters (SSPs), and audit data stored in the operational environment of the module,
- communicates all SSPs, authentication data, control inputs, and status outputs via a trusted channel, and
- audits the operation of the trusted channel.

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.

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

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 two-factor authentication requirement for operator authentication. 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 rigorous 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.

Level 4 modules require the protection of CSPs against simple power analysis and differential power analysis attacks.

DRAFT

Level 4 modules that contain software must provide for the encryption and authentication of CSPs and integrity test code when the module is not in use. This provides for the strong protection of CSPs from unauthorized disclosure and modification when the module is inactive.

Security Level 4 allows the software components of a cryptographic module to be executed on a general purpose computing system using an operating system that provides for the auditing of all operator accesses to audit data, all requests to use authentication data management mechanisms, all use of security-relevant crypto officer functions, and all requests to access authentication data associated with the cryptographic module.

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.

1.5 Security Level 5

Security Level 5 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.

Level 5 modules that contain software must provide for the encryption and authentication of all retained SSPs and integrity test code when the module is not in use. This provides strong cryptographic protection to detect and prevent the disclosure and modification of Public Security Parameters (PSPs) as well as CSPs when the module is inactive.

Level 5 modules have environmental failure protection mechanisms that protect the module from fluctuations in temperature and voltage. Level 5 modules are opaque to non-visual radiation examination and the tamper detection and zeroization circuitry is protected against disablement. When zeroization is required, PSPs as well as CSPs are zeroized.

At Level 5, CSPs are protected from electromagnetic emanation attacks.

The design of a Level 5 module is verified by a formal model and informal proof of correspondence between the formal model and the functional specification.

DRAFT

2. GLOSSARY OF TERMS AND ACRONYMS

2.1 Glossary of Terms

The following definitions are tailored for use in this standard:

Allowed security function: a non-Approved security function that is allowed, by the CMVP, in an Approved mode of operation.

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

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 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: for this standard, a security function (e.g., cryptographic algorithm that can be tested, cryptographic key management technique, or authentication technique) that is either

- specified in an Approved NIST Standard or NIST Recommendation, or
- adopted in an Approved NIST Standard or NIST Recommendation and specified either in an appendix of the Approved NIST Standard or Recommendation or in a document referenced by the Approved NIST Standard or Recommendation, or
- specified in the list of Approved security functions.

Bypass Capability: the ability of a service to partially or wholly circumvent encryption or cryptographic authentication. If, as the result of one or more service invocations, the module can output a particular data or status item in encrypted or cryptographically authenticated form, but instead (as a result of module configuration or operator intervention) outputs the item in a non-protected form, then a bypass capability exists.

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

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

DRAFT

Cryptographic 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 continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware and software 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 security function to form a plaintext cryptographic key or perform a cryptographic function.

Cryptographic module (module): the set of hardware and/or software that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within 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 C.)

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 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 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.)

Differential power analysis (DPA): an analysis of the variations of the electrical power consumption of a cryptographic module, using advanced statistical methods and/or other techniques, for the purpose of extracting information correlated to cryptographic keys used in a cryptographic algorithm.

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

Electrostatic discharge (ESD): the 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 security function with a key encrypting key.

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

Entropy: the uncertainty of a random variable.

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

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.

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 equipment within the cryptographic boundary used to process programs and data (includes non-reprogrammable software).

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

Hash value: the output of a cryptographic hash function.

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

DRAFT

Implementation guidance: a set of documents published during the lifetime of the standard which provides additional clarification, testing guidance and interpretations of the standard. (Implementation guidance cannot change or add requirements to the standard.)

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 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 securely contributed 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.

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.

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.

Min-entropy: the worst-case (that is, greatest lower bound) measure of uncertainty for a random variable.

Modifiable operational environment: an operational environment that is designed to contain some non-validated software.

Module software interface (MSI): a set of commands used to request the services of the module, including parameters that enter or leave the module's cryptographic boundary as part of the requested service.

Multiple-chip embedded cryptographic module: a physical embodiment in which two or more integrated circiut 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-invasive attack: an attack that can be performed on a cryptographic module without direct physical contact with the module.

Non-modifiable operational environment: an operational environment that is designed to contain only validated software.

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.

Personal identification number: a numeric code, used to authenticate an identity.

Physical protection: the safeguarding of a cryptographic module, cryptographic keys, or 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 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.

DRAFT

Public security parameter: 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.

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.

Security strength: a number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or module. The average amount of work needed is $2^{\text{security strength - 1}}$.

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: 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.

Simple power analysis (SPA): a direct (primarily visual) analysis of patterns of instruction execution (or execution of individual instructions), obtained through monitoring the variations in electrical power consumption of a cryptographic module, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys.

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: the programs within the cryptographic boundary, usually stored on erasable media (e.g., disk), that can be dynamically written and modified or reprogrammed.

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

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.

DRAFT

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.

Timing analysis (TA): an attack on a cryptographic module that is based on an analysis of time periods between the time a command is issued and the time the result is obtained.

Trusted channel: a mechanism through which a cryptographic module provides a trusted, safe and discrete communication pathway for SSPs and other critical information between the cryptographic module and the module's intended communications endpoint. A trusted channel exhibits a verification component that the operator or 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 realized in one or more of the following ways:

- A communication pathway between the cryptographic module and endpoint that is entirely local, directly attached to the cryptographic module and has no intervening systems.

- A mechanism that cryptographically protects SSPs during entry and output and does not allow misuse of any transitory SSPs.

Two-factor authentication: a type of authentication that requires two independent methods to establish identity and authorization to perform services. The three most recognized factors are:

- "Something you are" (e.g., biometrics)
- "Something you know" (e.g., password)
- "Something you have" (e.g., smart card)

User: an individual or a 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.

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:

CMS	Configuration Management System
CSP	Critical Security Parameter
DPA	Differential Power Analysis

EDC	Error Detection Code
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EME	Electromagnetic Emanation
ESD	Electrostatic Discharge
FIPS	Federal Information Processing Standard
FSM	Finite State Model
HDL	Hardware Description Language
HMAC	Hash-Based Message Authentication Code
IC	Integrated Circuit
IV	Initialization Vector
KAT	Known Answer Test
MSI	Module Software Interface
NIST	National Institute of Standards and Technology
PSP	Public Security Parameters
RBG	Random Bit Generator
SPA	Simple Power Analysis
SSP	Sensitive Security Parameter
TA	Timing Analysis
URL	Uniform Resource Locator

DRAFT

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 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.

DRAFT

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 and operation of a cryptographic module. These areas include cryptographic module specification; module ports and interfaces; roles, services, and authentication; software 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 is currently not tested, 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 indicate the minimum of the independent ratings received in the areas.

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.

DRAFT

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*	*Security Level 5*
1. Cryptographic Module Specification	Specification of module, boundary, Approved algorithms and Approved modes of operation. Description of module hardware and software. Module documentation.				
	Security Policy defines Approved mode of operation.		Module indication of Approved mode of operation.		
2. Cryptographic Module Ports and Interfaces	Required and Optional Interfaces. Specification of all interfaces and of all input and output data paths.		Input and output of critical security parameters either physically separated or logically separated using trusted channel from other ports and interfaces.		
3. Roles, Services and Authentication	Definition of module's roles and services.	Role-based or identity-based authentication.	Identity-based operator authentication	Two-factor authentication.	
4. Software Security	Executable code, Approved integrity technique, MSI, read and modify restrictions, zeroization upon unload, format checking.	Digital signature-based integrity test.	MSI command to initiate the software integrity test. Hash value zeroization.	Encryption and decryption of CSPs and integrity test code.	Encryption and decryption of PSPs and integrity test code.
5. Operational Environment	Single user OS or discretionary access control.	Audit mechanisms. Discretionary access control.	Crypto software, SSP, and audit data protection. Trusted channel. Extended auditing.	Extended auditing requirements.	
6. Physical Security	Production grade components.	Tamper evidence. Opaque covering or enclosure.	Tamper response and zeroization circuitry on removable covers and doors. Vents protected from probing. Hard opaque coating or enclosure.	EFP or EFT for temperature and voltage. Tamper detection and zeroization circuitry for multi-chip modules.	EFP for temperature and voltage. Opaque to non-visual radiation examination. Protection from tamper detection and zeroization circuitry disablement.
7. Physical Security-Non-invasive Attacks	No additional requirements.		Protection of CSPs against timing analysis attacks.	Protection of CSPs against SPA and DPA attacks.	Protection of CSPs from EME attacks.
8. SSP Management	Requirements for random bit generators, SSP generation, SSP establishment, SSP entry and output, SSP storage, and CSP zeroization.				
	Non-electronically transported SSPs may be entered or output in plaintext form.		Non-electronically transported SSPs entered or output either in encrypted form or using split-knowledge procedures.		Zeroization of PSPs.
9. Self-Tests	Pre-operational self-tests: software integrity test, cryptographic algorithm test, and pre-operational bypass test. Conditional self-tests: pair-wise consistency test, software load test, manual key entry test, continuous RBG test, RBG entropy source test, and conditional bypass test.				
10. Life-Cycle Assurance (CMS)	CMS for module, components, and documentation. Each uniquely identified and tracked throughout lifecycle.		Automated CMS.		
(Design)	Correspondence between module and Security Policy.	Functional Specification.	Detailed design.	Informal proof of correspondence between pre and post conditions and the functional specification.	Formal model and informal proof of correspondence between formal model and functional specification.
(FSM)	Finite state model.				
(Development)	Annotated source code, schematics or HDL.	Software high-level language. Hardware high level descriptive language.			
(Vendor Testing)	Functional Testing.		Low-level Testing.		
(Delivery and Operator)	Start-up procedures.	Delivery Procedures.	Operator authentication using vendor provided authentication information.		
(Guidance Docs)	Administrator and non-administrator guidance.				
11. Mitigation of Other Attacks	Any mitigation mechanisms are specified in Security Policy.				

Table 1: Summary of Security Requirements

DRAFT

4.1 Cryptographic Module Specification

A cryptographic module **shall** be a set of hardware and software that implements cryptographic functions or processes, including cryptographic algorithms and, optionally, key generation, and is contained within a defined cryptographic boundary. In an Approved mode of operation a cryptographic module **shall** implement at least one Approved (listed in Annex A) or Allowed (listed in Annex B) security function. Certain non-Approved security functions are allowed for use in an Approved mode of operation. Allowed security functions used in an Approved mode of operation **shall** meet all of the applicable requirements specified in Annex B. The operator **shall** be able to determine when an Approved mode of operation is selected. All Approved modes of operation **shall** be specified in the module Security Policy (see Appendix C.)

Approved security functions are listed in Annex A of this standard. Non-Approved security functions that are Allowed in an Approved mode, and the rules that govern their use, are listed in Annex B of this standard and in the FIPS 140-3 Implementation Guidance. Non-Approved functions can be performed if they are not used to provide security relevant functionality (e.g., a non-Approved algorithm may be used to encrypt data or keys but the result is considered plaintext and provides no security relevant functionality until encrypted with an Approved algorithm). Non-Approved security functions may also be used in non-Approved modes of operation.

The hardware and software of a cryptographic module can be excluded from the requirements of this standard if the vendor can demonstrate that the excluded hardware and software does not affect the security of the module.

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, the cryptographic module Security Policy **shall** specify when a cryptographic module is performing in an Approved mode of operation.

SECURITY LEVELS 3, 4 AND 5

In addition to the requirements of Security Level 2, for Security Levels 3, 4 and 5, a cryptographic module **shall** indicate when an Approved mode of operation is selected.

4.1.1 Types of Cryptographic Modules

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

- ***Hardware module*** is a module composed primarily of hardware, which may also contain some software.
- ***Software module*** is a module that is composed solely of software.
- ***Hybrid module*** is a module whose cryptographic functionality is primarily contained in software, which also includes some special purpose hardware within the cryptographic boundary of the module.

4.1.2 Cryptographic Boundary

A cryptographic boundary **shall** consist of an explicitly defined perimeter that establishes the physical boundary of a cryptographic module. The requirements of this standard **shall** apply to all components within this boundary, including all hardware and software. The cryptographic boundary **shall** include the processor(s) and other hardware components that provide for the operational environment of the module.

DRAFT

4.1.3 Multiple Approved Modes of Operations

A cryptographic module may be designed to support multiple Approved modes of operation. 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 not** be changed when configured for different Approved modes of operation.
- The Security Policy **shall** describe each Approved mode of operation implemented in the cryptographic module and how each mode is configured.
- 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).
- Pre-operational self-tests **shall** be performed for all Approved and Allowed security functions used in the selected Approved mode of operation.
- If re-configuration from one Approved mode of operation to another alters the physical security level of the module without changing the overall security level of the cryptographic module, then the cryptographic module **shall** perform a zeroization of all CSPs within the module.

4.1.4 Degraded Functionality

A cryptographic module may be designed to support degraded functionality (e.g., a module may fail the self-test for one encryption algorithm and alternately use another encryption algorithm) within an Approved mode of operation. For a cryptographic module to implement a degraded functionality in an Approved mode of operation, the following **shall** apply:

- Degraded operation **shall** be entered only upon the failure of pre-operational self-tests.
- When the cryptographic module operates with degraded functionality, 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 until failed test(s) have all been passed.

4.1.5 Security Strength of the Module

The security strength of the module **shall** be specified. The security strength of the module **shall** be one of the recommended security strengths, and **shall** be no larger than the minimum security strength of the Approved and Allowed security functions and SSPs in the Approved mode of operation.

4.2 Cryptographic Module Physical Ports and Logical Interfaces

A cryptographic module **shall** restrict all information flow and physical access points to physical ports and logical interfaces that define all entry and exit points to and from the module. 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).

A cryptographic module may utilize multiple independent communication channels. The data output, for a given communication channel, **shall** be disabled while performing key generation, manual key entry, self-tests, software loading and zeroization.

DRAFT

LOGICAL INTERFACES

A cryptographic module **shall** have the following four logical 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) from a cryptographic module (including plaintext, ciphertext, SSPs, and control information for another module) **shall** exit via the "data output" interface. For a given communication channel, all data output via the "data output" interface **shall** be prohibited when an error state exists and prior to successfully passing the pre-operational Software Integrity Test (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.

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.

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

All electrical power externally provided to a cryptographic module (including power from an external power source or batteries) **shall** enter via a power port. A power port is not required when all power is provided or maintained within the cryptographic boundary of the cryptographic module (e.g., by an internal battery).

During manual SSP entry, the entered values may be temporarily displayed to allow visual verification to improve accuracy.

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

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, 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.

SECURITY LEVELS 3, 4, AND 5

The module **shall** utilize a separate, dedicated physical port for the input or output of CSP's, or a Trusted Channel **shall** be utilized to protect the CSPs entering and leaving the cryptographic module. If a Trusted Channel is used, the documentation **shall** specify the security strength of the Trusted Channel.

4.3 Roles, Authentication, and Services

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

DRAFT

4.3.1 Roles

A cryptographic module **shall** support a *Cryptographic Officer Role*. The *Cryptographic 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 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.

Authorized roles are applicable to all callable services utilizing Approved security functions 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 Operator 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. For Security Levels 2-5, a cryptographic module **shall** support at least one of the following mechanisms to control access to the 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.
>
> *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.

For a software cryptographic module, the operating system can implement the authentication mechanism. If the operating system implements the authentication mechanism, then the authentication mechanism **shall** meet the requirements of this section.

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 powered off and subsequently powered on, the results of previous authentications **shall not** be retained and the module **shall** require the operator to be re-authenticated.

DRAFT

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 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 combined strength of the authentication mechanism **shall** conform to the following specifications:

- For each attempt to use the authentication mechanism, the probability **shall** be equal to or less than one in 100,000,000 that a single attempt will succeed or a false acceptance will occur (e.g., guessing a password, false acceptance error rate of a biometric device, or some combination of authentication methods.)

- For multiple attempts to use the authentication mechanism during a one-minute period, the probability **shall** be equal to or less than one in 10,000,000 that a single attempt will succeed or a false acceptance will occur.

- Authentication strength requirements **shall** be met by the module's implementation and **shall not** rely on documented procedural controls or security rules (e.g., password size restrictions).

- If passwords are utilized as an authentication mechanism, then restrictions **shall** be enforced by the module on password selection to prevent the use of weak passwords that are more susceptible to attacks (e.g., dictionary attacks).

- Feedback of authentication data to an operator **shall** be obscured during authentication (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 not** weaken the strength of the authentication mechanism beyond the required authentication strength.

If the module employs default authentication data to control access to the module for first-time authentication, then the default authentication data **shall** be unique per module unit delivered.

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.

DRAFT

SECURITY LEVEL 3

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

SECURITY LEVELS 4 AND 5

In addition to the requirements of Security Level 3, Security Levels 4 and 5 **shall** also meet the following requirement.

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

4.3.3 Services

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

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

Show the Module's Version Number: Output the name and the version number of the cryptographic module.

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

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

Zeroize: Perform zeroization as specified in Section 4.8.6.

A cryptographic module may provide other services, both Approved 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).

Bypass Capability. 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, but instead (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 deactivate the mechanisms that are designed to prevent the inadvertent bypass of security functions due to a single error. The two independent internal actions **shall** alter software and/or hardware behavior that is dedicated to mediate the bypass.
- 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).

External Software Loading: If a cryptographic module has the capability of loading software from an external source, then

- The logic performing the external software loading **shall** be logically disconnected from all data output.

- The cryptographic module **shall not** execute the loaded code until after the *Software Load Test* specified in Section 4.9.2 has successfully verified the validity of the externally loaded code.

- The cryptographic module **shall not** execute any loaded Approved security functions until after the Cryptographic Algorithm self-tests specified in Section 4.9.1 have been successfully executed.

- The module **shall** support an Approved authentication technique to verify the validity of software that may be loaded. 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 not** be permitted.

4.4 Software Security

The requirements of this section apply to modules containing software.

SECURITY LEVEL 1

The following requirements **shall** apply to software contained within a cryptographic module for Security Level 1.

- All cryptographic code within the module **shall** be in executable form.

- A cryptographic mechanism using an Approved integrity technique (e.g., an Approved message authentication code or a digital signature algorithm) that uses a cryptographic key **shall** be applied to all software within the cryptographic module. The key may reside within the module.

- The input and output of the module **shall** be directed through a defined MSI.

- The MSI **shall not** permit the operator of the service to read the software.

- The MSI **shall not** permit the operator to modify module software without invoking the Software Load Test as specified in Section 4.9.2.

- Any modifications to module software other than a complete reload **shall** pass the Software Load Test as specified in Section 4.9.2.

- If a specific format for externally provided data is expected, then the module **shall** verify the format.

SECURITY LEVEL 2

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

- The Approved integrity technique used in the Software Integrity Test **shall** consist of the generation of a digital signature using an Approved digital signature algorithm. The entity requesting validation **shall** generate the private key used to sign the code and the public key used to verify the code. The private signing key **shall not** reside within the module. The public verification key may reside with the module code.

DRAFT

SECURITY LEVEL 3

In addition to the requirements of Security Level 2, the following requirements **shall** apply to software contained within a cryptographic module for Security Level 3.

- An MSI command (i.e., callable service) permitting a cryptographic officer to initiate the Software Integrity Test without instituting a power-down of the module **shall** be incorporated. The MSI command **shall** return an indication as to whether the Software Integrity Test was successful and a newly computed hash value.[1]

- The hash value of the module's software **shall** be zeroized from the module upon completion of the MSI command which initiates the Software Integrity Test.

SECURITY LEVEL 4

In addition to the requirements of Security Level 3, the following requirements **shall** apply to software contained within a cryptographic module for Security Level 4.

- The module **shall** have the capability to decrypt portions of the software that is encrypted when the module is first loaded. All CSPs as well as the Software Integrity Test software (including the public verification key and digital signature) **shall** be encrypted by the vendor using a symmetric key. The symmetric key, or key components, **shall** initially be generated by the vendor (Section 4.8.2) and transported to the module site (Sections 4.8.3 and 4.8.4). The symmetric key **shall not** be retained within the module when the module is transported to the customer. When the software is loaded into the module, the Cryptographic Officer(s) **shall** enter the symmetric key or key components (Section 4.8.4) to decrypt the encrypted portions. The Software Integrity Test, including the symmetric key (as data), **shall** then be performed as part of the pre-operational tests.

- Before the module subsequently transitions to the pre-operational state, the Cryptographic Officer(s) may supply a new symmetric key, or key components (otherwise the current symmetric key **shall** be used). The CSPs, and Software Integrity Test software (including the public verification key and digital signature) **shall** be encrypted and all plaintext copies of these values within the module **shall** be automatically zeroized.

- A new key pair used by the Software Integrity Test, and a new symmetric encryption key **shall** be initially generated (Section 4.8.2) for each instance of this cryptographic module.

- The mode of encryption used to protect CSPs and the Software Integrity Test software (including the public verification key and digital signature) **shall** be Approved encryption with an authentication mode.

SECURITY LEVEL 5

In addition to the requirements of Security Level 4, the following requirement **shall** apply to software contained within a cryptographic module for Security Level 5.

- In addition to all CSPs and the Software Integrity Test software (including the public verification key and digital signature), the symmetric encryption described in Level 4 **shall** be applied to all PSPs.

[1]Initially, the hash value on the module software may be transmitted to the cryptographic officer independently of the module. The cryptographic officer may manually compare the newly computed hash value to the one provided by the module vendor. If the hash values do not match or the digital signature does not validate, the cryptographic officer should assume that the module software is not valid.

DRAFT

4.5 Operational Environment

The requirements of this section apply only to modules containing software that run in a modifiable operational environment. The requirements of this section do not apply to hardware only modules or any modules with a non-modifiable operational environment.

The operational environment of a cryptographic module is the set of all software and hardware required for the module to operate securely. For example, the operational environment of a software module includes the module itself, the processor on which the software is executed, and the operating system that controls the execution of the software. An operational environment can be non-modifiable or modifiable.

A non-modifiable operational environment is designed to contain only validated software. This environment may be software operating in a non-programmable computer (e.g., a non-programmable PC card or non-programmable smartcard), or software whose update is controlled using Approved data authentication processes (i.e., through the Software Load Test specified in Section 4.9.2). If the operational environment is non-modifiable, then the operational environment components that enforce the non-modifiability **shall** be bound to the software module.

A modifiable operational environment is designed to allow loading of non-validated software. This environment may include general purpose operating system capabilities (e.g., use of a computer O/S or configurable smart card O/S). Operating systems are considered to be modifiable operational environments if software 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 non-modifiable and modifiable operational environments are provided in the following table.

Configuration	Operational Environment
A cryptographic module that does not permit the loading of software and does not permit operators to modify the configuration of the operating system or cryptographic module.	Non-modifiable
A cryptographic module that allows the loading of additional software that is authenticated and meets all applicable requirements of this standard.	Non-modifiable
Software on a computer that does not isolate input data.	Modifiable
Software on a processor that allows the input of non-validated executable code.	Modifiable
Software 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, the operating system requirements in Section 4.5.1 do not apply. If the operational environment is modifiable, the operating system requirements in Section 4.5.1 **shall** apply. The goal of the requirements in Section 4.5.1 is to logically protect the cryptographic module running in a modifiable operational environment from unauthorized access (execute, modify, or read) by untrusted processes. Section 4.5.1 does not address physical protection to the module.

Documentation **shall** specify the operational environment for a cryptographic module, including, if applicable, the operating system employed by the module.

DRAFT

4.5.1 Operating System Requirements for Modifiable Operational Environments

At Security Level 1 only, the operating system requirements are different for the cryptographic modules restricted to a single operator session at any given time and for those that allow multiple concurrent operators.

SECURITY LEVEL 1

The following requirements **shall** apply to operating systems restricted to a single operator session at any given time (i.e., concurrent operators are explicitly excluded) for Security Level 1.

- All MSI commands in a session **shall** be run on behalf of a single operator.
- All CSPs **shall** be zeroized before each operator's session is terminated and a new operator's session is begun.
- Processes that are spawned by the cryptographic module **shall** be owned by the module and **shall not** be owned by external processes/operators.

If the operating system allows multiple concurrent operators, then the following requirements apply:

- All cryptographic software, SSPs, and control and status information **shall** be under the control of an operating system that implements discretionary access controls that protect against unauthorized execution, modification, and reading.
- To protect plaintext data, cryptographic software, SSPs, and authentication data, the access control mechanisms of the operating system **shall** be configured to:
    - Enforce the set of roles that can execute stored cryptographic software.
    - Enforce the set of roles that can 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.
    - Enforce the set of roles that can read the following cryptographic software stored within the cryptographic boundary: cryptographic data (e.g., cryptographic audit data), CSPs, and plaintext data.
    - Enforce the set of roles that can enter SSPs.
- The following specifications **shall** be consistent with the roles and services as defined in the Security Policy.
    - The operating system **shall** prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not.
    - The operating system **shall** prevent operators from gaining either read or write access to SSPs of other operators.
    - The operating system **shall** prevent operators and external executing processes from reading cryptographic software stored within the cryptographic boundary.

DRAFT

- The configuration of the operating system to meet the above requirements **shall** be specified in a Crypto Officer guideline. The Crypto Officer guideline **shall** state that the operating system must be configured as specified, before the module contents can be considered as protected.

SECURITY LEVEL 2

In addition to the applicable requirements of Level 1 for the cryptographic modules that allow multiple concurrent operators, the following requirements **shall** apply for Security Level 2.

- 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 module, then the module **shall** use Approved cryptographic mechanisms to protect the information when external to the module from unauthorized disclosure and modification.

  - The following events **shall** be recorded by the audit mechanism:

    - attempts to provide invalid input for Cryptographic Officer functions, and
    - addition or deletion of an operator to and from a cryptographic Officer role.

  - 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 module Security Policy **shall** specify whether identification and authentication of module operators is performed by operating system code or vendor supplied code. In either case, the identification and authentication mechanism **shall** meet the requirements of Section 4.3.2.

SECURITY LEVEL 3

In addition to the applicable requirements for Security Level 2, the following requirements **shall** apply for Security Level 3.

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

- A Trusted Channel **shall** be implemented between the authenticated 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.

- In addition to the audit requirements of **Security** Level 2, the following events **shall** be recorded by the audit mechanism:

DRAFT

- attempts to use the trusted channel function.
- identification of the initiator and target of a trusted channel.

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

SECURITY LEVELS 4 AND 5

In addition to the applicable requirements for Security Level 3, the following requirements **shall** apply for Security Levels 4 and 5.

- The audit mechanism **shall** be permanently configured so that the following events are always audited:
  - 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 Cryptographic Officer functions.
  - requests to access authentication data associated with the cryptographic module.

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, 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 are applicable to hardware and 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 will have a high probability of being detected

DRAFT

- subsequent to an attempt by leaving visible signs (i.e., tamper evidence)

  and / or

- during an access attempt so that appropriate immediate actions **shall** be taken by the cryptographic module to protect SSPs (i.e., tamper response).

Table 3 summarizes the physical security requirements, both the general and the three specific embodiments for each of the five 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 uniquely numbered tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with uniquely numbered tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Tamper response and zeroization circuitry. Vents protected 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.
Security Level 5	EFP for temperature and voltage. Opaque to non-visual radiation examination (e.g. x-rays, MRI, etc). ESD and Radiation Fault-Induction.	No additional requirements.	Tamper detection response circuitry mitigation.	

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). The Security Level 5 requires EFP protection from non-visual radiation examination, protection from electro-static discharge and radiation fault induced attacks and for multi-chip embodiments, as well as protection of the tamper detection response circuitry from disablement.

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 (also, PSPs if Security Level 5) **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 physical maintenance, all 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.

- 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 by direct visual observation using artificial light sources in the visual spectrum of the module's internal construction or components.

DRAFT

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 cryptographic module contains ventilation holes or slits, then the holes or slits shall be constructed in 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, 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., require at least one 90 degree bend or obstruction with a substantial blocking material).

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.

SECURITY LEVEL 5

In addition to the general requirements for Security Levels 1, 2, 3, and 4, the following requirement **shall** apply to all cryptographic modules for Security Level 5:

- The cryptographic module **shall** include EFP features for both temperature and voltage.

- The cryptographic module **shall** be opaque to non-visual radiation examination (e.g. x-rays, MRI, thermal imaging, etc).

- The cryptographic module **shall** include fault-tolerant features to provide protection from electrostatic discharge and electromagnetic radiation induced faults.

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

DRAFT

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).

SECURITY LEVEL 5

There are no additional Security Level 5 requirements for single-chip cryptographic modules.

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 uniquely numbered tamper-evident seals (e.g., uniquely numbered evidence tape or uniquely numbered holographic 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.

SECURITY LEVEL 5

In addition to the requirements for Security Levels 1, 2, 3, and 4, the following requirements **shall** apply to multiple-chip embedded cryptographic modules for Security Level 5:

- The cryptographic module tamper detection response circuitry or components **shall** be protected from disablement,

DRAFT

or

- CSPs **shall** be protected from disclosure if the tamper detection response circuitry or components are disabled.

Possible attacks against the cryptographic module include but are not limited to the catastrophic and sudden disabling of the tamper detection response circuitry or components. If the disabling method renders the response circuitry disabled such that CSPs are no longer protected from disclosure, this requirement is not met. If the disabling method renders the response circuitry disabled and either concurrently zeroizes the CSPs and PSPs or renders the CSPs and PSPs destroyed then this requirement is met.

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 uniquely numbered tamper-evident seals (e.g., uniquely numbered evidence tape or uniquely numbered holographic 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.

SECURITY LEVEL 5

In addition to the requirements for Security Levels 1, 2, 3, and 4, the following requirements **shall** apply to multiple-chip standalone cryptographic modules for Security Level 5.

- The cryptographic module tamper detection response circuitry or components **shall** be protected from disablement,

  or

- CSPs **shall** be protected from disclosure if the tamper detection response circuitry or components are disabled.

Possible attacks against the cryptographic module include but are not limited to the catastrophic and sudden disabling of the tamper detection response circuitry or components. If the disabling method renders the response circuitry disabled such that CSPs are no longer protected from disclosure, this requirement is not met. If the disabling method renders the response circuitry disabled and either concurrently zeroizes the CSPs or renders the CSPs destroyed this requirement is met.

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. At Security Level 5, a cryptographic module **shall** employ EFP features for both temperature and voltage.

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

DRAFT

- Immediately zeroize all CSPs and PSPs.

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 tested **shall** be gradually decreasing from a temperature within the normal operating temperature range to a lower temperature that either (1) shuts down the module to prevent further operation or (2) immediately zeroizes all CSPs (also, PSPs if Security Level 5); and **shall** be gradually increasing from a temperature within the normal operating temperature range to a higher temperature that either (1) shuts down the module to prevent further operation or (2) immediately zeroize all CSPs (also, PSPs if Security Level 5). The temperature range 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 (also, PSPs if Security Level 5) 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 (also, PSPs if Security Level 5); 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 (also, PSPs if Security Level 5), 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

Attacks on the operations of the module that are physical (not logical) in nature and do not require physical contact or direct observation of the module are specified in this section. These attacks include Simple Power Analysis, Differential Power Analysis, Electromagnetic Emanation and Timing Analysis. Other non-invasive attacks may exist but defense against them is currently considered optional at all Security Levels.

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 listed in this section.

SECURITY LEVEL 3

At Security Level 3, the cryptographic module **shall** protect the module's CSPs against TA attacks. Documentation **shall** specify the mitigation techniques against applicable TA attacks.

DRAFT

SECURITY LEVEL 4

In addition to the requirements for Security Level 3, the following requirements **shall** apply to all cryptographic modules for Security Level 4:

- The cryptographic module **shall** protect the CSPs against SPA attacks. Documentation **shall** specify the mitigation techniques against applicable SPA attacks.

- The cryptographic module **shall** protect the module's CSPs against DPA attacks. Documentation **shall** specify the mitigation techniques against applicable DPA attacks.

SECURITY LEVEL 5

In addition to the requirements for Security Level 4, the following requirement **shall** apply to all cryptographic modules for Security Level 5:

- The cryptographic module **shall** protect the module's CSPs against EME. Documentation **shall** specify the mitigation techniques against applicable EME attacks.

4.8 Sensitive Security Parameter Management

Sensitive Security Parameters consist of Critical Security Parameters and Public Security Parameters.

The security requirements for SSP management encompass the entire lifecycle of SSPs employed by the module. SSP management includes random bit generators, 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 security function. CSPs encrypted using a non-Approved security function are considered plaintext within the scope of this standard.

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

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

Keys used only to test the cryptographic algorithms as specified in Section 4.9.2 are PSPs.

For a software module, the Software Integrity Test key is a CSP. For a hardware module that contains software components, the Software Integrity Test key is a PSP. For the hybrid module, the key used for the Software Integrity Test is a CSP. If another key is used to test the integrity of software in the hardware portion of the hybrid module, this key is not a SSP.

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, and/or one or more RBG entropy sources. The cryptographic module may be solely an RBG or an RBG entropy source. Documentation **shall** list each RBG and RBG entropy source contained in the module. All RBGs used in an Approved mode **shall** be Approved and listed in Annex A.

If a module contains an RBG or an RBG entropy source in an Approved mode then:

- RBG entropy sources **shall** be subject to the RBG Entropy Source Test as specified in Section 4.9.2.

DRAFT

- Deterministic components of an RBG **shall** be subject to the Cryptographic Algorithm Test in Section 4.9.1.

- Data output from the RBG **shall** pass the Continuous RBG Test as specified in Section 4.9.2.

If entropy is provided from outside of the module then the claimed minimum entropy value **shall** be provided to the module. The module **shall** verify that the claimed minimum entropy provided by the RBG entropy source is sufficient to support the intended security strength of RBG that uses the entropy.

If random values are required in an IV, used by an Approved security function(s), then an Approved RBG **shall** be used to generate this IV.

4.8.2 SSP Generation

A module may generate SSPs internally or they may be loaded from an external source. Documentation **shall** specify each SSP generation method employed by a module. Documentation **shall** specify each SSP generation method that makes use of an RBG.

Any SSPs (other than seeds and seed keys) generated in the Approved mode of the module using an RBG **shall** be generated using an Approved RBG meeting the requirements specified in Section 4.8.1. When using an Approved RBG to generate SSPs, the security strength of the RBG **shall** be sufficient to support the security strength of the cryptographic security function that makes use of the SSPs.

SSPs (other than seed keys) generated by the module for use by an Approved security function **shall** be generated using an Approved SSP generation method[2].

4.8.3 SSP Establishment

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

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[3].

If an SSP establishment method in an Approved mode requires random values as an input, an Approved 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.

4.8.4 SSP Entry and Output

SSPs may be entered into or output from a module. 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 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 correct entity (i.e., person, group, role, or process) to which the SSP is assigned.

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

---

[2] Approved SSP generation and derivation methods are listed in Annex C.
[3] See Annexes C and D.

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.

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. PSPs may be entered into or output from a module in plaintext form.

Electronically transported CSPs **shall** enter into and output from a module in encrypted form and their integrity **shall** be protected (e.g., by an Approved security function or an Approved or Allowed key establishment method). Electronically transported PSPs **shall** enter into and output from the module with their integrity protected by either an Approved digital signature algorithm or an Approved MAC or an Approved key transport method.

Non-electronically transported PSPs may be entered into or output from a module in plaintext form and need not be cryptographically authenticated regardless of whether they are entered manually or electronically.

SECURITY LEVELS 1 AND 2

There are no additional security requirements for Security Levels 1 and 2.

SECURITY LEVELS 3, 4 AND 5

For Security Levels 3, 4, and 5, non-electronically transported CSPs **shall** be entered into or output from a module either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext components.)

If split knowledge procedures are used:

- The module **shall** separately authenticate the operator entering or outputting each component as a separate identity.
- The module **shall** verify that no two operators entering or outputting key components have the same identities.
- In order to prevent misuse of any SSP, a cryptographic module **shall** utilize a Trusted Channel for the input or output of all SSPs, whether or not cryptographically protected. If a Trusted Channel is established and maintained using the cryptographic algorithms, the algorithms **shall** by Approved and meet or exceed the documented security strength of the module.
- 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.

4.8.5 SSP Storage

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

which the SSP is assigned. An SSP may also be stored within an embedded cryptographic module that meets or exceeds the requirements of the standard relative to the larger module.

Documentation **shall** specify:

- The SSPs stored in the module.
- How CSPs are protected from unauthorized access when stored in the module.
- How PSPs are protected from unauthorized modification and 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.

Plaintext CSPs **shall not** be accessible to unauthorized operators from outside the module. PSPs **shall not** be modifiable by unauthorized operators from outside the module.

4.8.6 SSP Zeroization

A module **shall** provide methods to zeroize all CSPs (including temporarily stored values) within the module. Once a CSP is zeroized, the CSP **shall not** be retrievable 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 at levels below Security Level 5. Keys used only to perform pre-operational self-tests **shall** be considered as PSPs. Hash values of passwords that, if known, would be subject to an off-line exhaustion attack **shall** be considered as CSPs. RBG state information **shall** be considered a CSP.

Documentation **shall** specify the CSP zeroization method(s) employed by a module and the rationale as to why the method(s) prevent the retrieval and reuse the zeroized CSPs.

Temporary CSPs (e.g., ephemeral keys) **shall** be zeroized when they are no longer in use.

SECURITY LEVELS 1 AND 2

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

SECURITY LEVEL 3

The cryptographic module **shall** control the zeroization of the CSPs.

SECURITY LEVEL 4

There are no additional requirements for Security Level 4.

SECURITY LEVEL 5

The following security requirements **shall** be met:

- A module **shall** provide methods to zeroize all PSPs (including temporarily stored values) within the module.
- Documentation **shall** specify the PSP zeroization methods employed by a module and the rationale as to why the methods prevent the retrieval and reuse of the zeroized data.
- Temporary PSPs **shall** be zeroized when they are no longer needed.

4.9 Self-Tests

A cryptographic module **shall** perform pre-operational self-tests, conditional self-tests and, if applicable, critical functions tests to ensure that the module is functioning properly. The pre-operational self-tests must be performed and passed successfully prior to the module providing any services. Conditional self-tests **shall** be performed when an applicable security function is invoked (i.e., security functions for which self-tests are required). A cryptographic module may perform other 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 via the status output interface. 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.

Documentation **shall** specify:

- The self-tests performed by a cryptographic module.
- The error states that a cryptographic module can enter when a self-test fail.
- 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, or returning the module to the vendor for servicing).

4.9.1 Pre-Operational Self-Tests

The pre-operational tests **shall** be performed by a cryptographic module between the time a cryptographic module is powered on, either from a power-off state or a quiescent state (e.g., low power, suspend or hibernate) and the time that the cryptographic module uses a function or provides a service using the function to be tested. Prior to using a security function, the pre-operational test(s) of that security function **shall** pass successfully. The pre-operational self-tests **shall** be initiated automatically and **shall not** require operator intervention. The vendor **shall** specify a critical time period that specifies the maximum operational time before pre-operational tests must be repeated. When a pre-operational test is completed, the results (i.e., indications of success or failure) may be output via the "status output" interface. 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.

A cryptographic module **shall** permit operators to initiate the pre-operational tests on demand for periodic testing of the module.

A cryptographic module **shall** repeat the pre-operational self-tests as documented. Documentation **shall** specify the time period and the policy regarding the interruption of the module's operations.

A cryptographic module **shall** perform the following pre-operational tests, as applicable: Software Integrity Test, Cryptographic Algorithm Test, and Pre-Operational Bypass Test.

Software Integrity Test: a test using an Approved data authentication technique **shall** be applied to all validated software within a cryptographic module when the module is powered up. This pre-operational self-test **shall** be successfully completed before the cryptographic module provides any services. The Software Integrity Test is not required for any software excluded from the security requirements of this standard or for any executable code stored in non-reconfigurable memory. If the integrity of the executable code cannot be verified, the Software Integrity Test **shall** fail.

DRAFT

SECURITY LEVEL 1

The Approved data authentication technique **shall** include the use of a MAC or a digital signature.

SECURITY LEVELS 2, 3, 4 AND 5

The Approved data authentication technique **shall** include the use of a digital signature.

Cryptographic Algorithm Test. This test **shall** be conducted for all Approved and Allowed cryptographic algorithms (e.g., encryption, decryption, data authentication, and random bit generation) of each cryptographic algorithm implemented by a cryptographic module via any of the following methods.

- A known-answer test involves operating the cryptographic algorithm on data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer). If the calculated output does not equal the known answer, the known-answer test **shall** fail. Cryptographic algorithms whose outputs do not vary for a given set of inputs (i.e., no random data is obtained and used during the execution of the algorithm) **shall** be tested using a known answer test (KAT).

- Public key cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the DSA or the ECDSA) **shall** be tested using a known-answer test if the random number responsible for the variability of the output can be fixed, or **shall** be tested using a Pair-Wise Consistency Test (see Section 4.9.2) with a fixed pair of public and private keys.

- 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,

    or

  - perform a KAT for each cryptographic algorithm and mode to be tested in accordance with the specified condition. A KAT is not required for the security function in the Approved Data Authentication technique used by the Software Integrity Test.

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. This test shall be performed before the bypass capability is first exercised.

4.9.2 Conditional Self-Tests

Conditional tests **shall** be performed by a cryptographic module when the conditions specified for the following tests occur: Pair-Wise Consistency Test, Software Load Test, Manual Key Entry Test, Continuous RBG Test, RBG Entropy Source Test, and Conditional Bypass Test.

Pair-Wise Consistency Test (for public and private keys). If a cryptographic module generates public or private keys, then the following pair-wise consistency tests for every pair of generated public and private keys **shall** be performed:

- If the keys are used to perform key transport, then the public key **shall** encrypt a plaintext value. The resulting ciphertext value **shall** be compared to the original plaintext value. If the two values are equal, then the test **shall** fail. If the two values differ, then the private key **shall** be used to decrypt the ciphertext and the resulting value **shall** be compared to the original plaintext value. If the two values are not equal, the test **shall** fail.

- If the keys are used to perform the calculation and verification of digital signatures then the consistency of the keys **shall** be tested by the complete calculation and verification of a digital signature. If the digital signature cannot be verified, the test **shall** fail.

- If the keys are used to perform key agreement, then the arithmetic validity of the keys **shall** be tested by verifying the correct mathematical relationship between the public key and private key values.

Software Load Test. If software can be externally loaded into a cryptographic module, then the following Software Load Tests **shall** be performed:

- An Approved digital signature technique **shall** be applied to all validated software when externally loaded into a cryptographic module. The Software Load Test is not required for any software that is loaded onto and solely executed on hardware which has been excluded from the security requirements of this standard (see Section 4.1).

- The applied Approved data authentication technique **shall** be successfully verified or the Software Load Test **shall** fail.

- Before the newly loaded software is operationally used, the requirements of Section 4.9.1 **shall** be satisfied.

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.

Continuous RBG Test. If a cryptographic module employs an Approved RBG or an RBG entropy source in an Approved mode of operation, the module **shall** perform the following continuous random bit generator test on each RBG and RBG entropy source that tests for failure to a constant value.

- If each call to a RBG produces blocks of n bits (where $n > 63$), the first n-bit block generated after power-up, initialization, or reset **shall not** be used, but **shall** be saved for comparison with the next n-bit block to be generated. Each subsequent generation of an n-bit block **shall** be compared with the previously generated block. The test **shall** fail if any two compared n-bit blocks are equal.

- If each call to a RBG produces fewer than 64 bits, the first n bits generated after power-up, initialization, or reset (for some $n > 63$) **shall not** be used, but **shall** be saved for comparison with the next n generated bits. Each subsequent generation of n bits **shall** be compared with the previously generated n bits. The test fails if any two compared n-bit sequences are equal.

RBG Entropy Source Test. If an RNG entropy source is contained within the operational environment, then the min-entropy assessment **shall** be performed on each output of the entropy source. This test **shall** fail if the assessed min-entropy is less than the min-entropy required by the Approved RBG.

Conditional Bypass Test. 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.

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

4.9.3 Critical Functions Tests

SECURITY LEVEL 1

There are no requirements for testing critical functions at Security Level 1.

SECURITY LEVELS 2, 3, 4 AND 5

There may be other security functions critical to the secure operation of the cryptographic module that **shall** be tested either when the module is powered up or when certain conditions are met. Documentation **shall** specify all identified critical functions and testing methods.

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, deployment, and operation of a cryptographic module, providing assurance that the module is properly 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 security 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 requirement **shall** apply to cryptographic modules for Security Levels 1 and 2.

- A configuration management system **shall** be implemented for a cryptographic module and module components within the cryptographic boundary, and for 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.

SECURITY LEVELS 3, 4, AND 5

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

DRAFT

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 the implemented functionality to this standard, where possible without compromising the security of the module, so that all the services of the cryptographic module can be tested.

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 and/or software 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** specify 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.

SECURITY LEVEL 5

In addition to the requirements for Security Levels 1, 2, 3, and 4, the following requirements **shall** apply to cryptographic modules for Security Level 5.

- Documentation **shall** specify a formal model that describes the rules and characteristics of the cryptographic module Security Policy. The formal model **shall** be specified using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory.

DRAFT

- Documentation **shall** specify a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module Security Policy.

- Documentation **shall** specify an informal proof of the correspondence between the formal model 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/or 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/or 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 the following operational and error states:

Power on/off state. A state in which the module is powered off or in standby 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.

General initialization state: A state in which the cryptographic module is initializing non-cryptographic services.

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 or non-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., fail a self-test or attempt to encrypt without operational keys or CSPs). 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.

DRAFT

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

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, documentation **shall** specify the compilers, configuration settings, and methods to compile the source code into an executable form. The documentation **shall** also include the source code for the software, annotated with comments that depict the correspondence of the software 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.

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 within a cryptographic module **shall** be implemented using a high-level, non-proprietary language, except that the limited use of a low-level language (e.g., assembly language or microcode) is allowed if essential to the performance of the module or when a high-level language is not available.

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

SECURITY LEVELS 4 AND 5

In addition to the requirements for Security Levels 1, 2 and 3, the following requirement **shall** apply to cryptographic modules for Security Levels 4 and 5:

- 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.

RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES FOR ALL LEVELS

Implementation of software within a cryptographic module using the recommended development practices listed in Appendix B will facilitate the analysis of the software for conformance to the requirements in this standard and will reduce the chance of design errors.

4.10.5 Vendor Testing

This section specifies the security requirements for *vendor testing* of the cryptographic module, including testing 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.

Functional testing refers to the testing of the cryptographic module functionality as defined by the Functional Specification required by Section 4.10.2.

SECURITY LEVELS 3, 4, AND 5

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.

Low-level testing refers to the testing of the individual components or group of components of the cryptographic module and their physical ports and logical interfaces as defined by the documentation required by Section 4.10.2 for Security Level 3.

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 LEVEL 2

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

SECURITY LEVELS 3, 4, AND 5

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

DRAFT

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 a secure manner. *Guidance documentation* consists of administrator and non-administrator guidance.

Administrator guidance is 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.

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

Non-administrator guidance is written material that is used by the User and/or other non-administrative roles for operating the cryptographic module in a secure manner. 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-administrator guidance (if the User role is implemented) **shall** specify:

- The Approved and non-Approved security functions, physical ports, and logical interfaces available to the users of a cryptographic module.
- All User responsibilities necessary for the secure 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), then the module's Security Policy or other 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.

DRAFT

SECURITY LEVELS 4 AND 5

In addition to the requirements for Security Levels 1, 2 and 3, the following requirement **shall** apply to cryptographic modules for Security Levels 4 and 5:

If the mitigation of other attacks is claimed, documentation **shall** specify the methods used to mitigate the attacks and the methods to test the effectiveness of mitigation techniques.

DRAFT

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 and software 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, 4, and 5)*

- Specification of any hardware or software 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, 4, and 5)*

- Specification of the physical ports and logical interfaces of a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- 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, 4, and 5)*

- List of all security functions, both Approved and non-Approved, that are employed by a cryptographic module and specification of all modes of operation, both Approved and non-Approved. *(Security Levels 1, 2, 3, 4, and 5)*

- 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, 4, and 5)*

- Specification of the design of the hardware and software of a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- 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.

- 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, 4, and 5)*

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, 4, and 5)*

ROLES, AUTHENTICATION, AND SERVICES

- Specification of all authorized roles supported by a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- 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

DRAFT

service output, and the authorized role(s) in which the service can be performed. *(Security Levels 1, 2, 3, 4, and 5)*

- 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, 4, and 5)*

- 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, 4, and 5)*

SOFTWARE SECURITY

- Documentation **shall** specify which Approved integrity techniques are used.

- Documentation **shall** specify the MSI commands employed by the module.

OPERATIONAL ENVIRONMENT

- Specification of the operational environment for the cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

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, 4, and 5)*

- 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, 4, and 5)*

- 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 and 5)*

PHYSICAL SECURITY – NON-INVASIVE ATTACKS

- Specification of the mitigation techniques against applicable Timing Analysis attacks. *(Security Levels 3, 4, and 5)*

- Specification of the mitigation techniques against applicable SPA attacks. *(Security Levels 4 and 5)*

- Specification of the mitigation techniques against applicable DPA attacks. *(Security Levels 4 and 5)*

- Specification of the mitigation techniques against applicable EME attacks. *(Security Level 5)*

SENSITIVE SECURITY PARAMETER MANAGEMENT

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

DRAFT

- Specification of each RBG (Approved RBGs and non-Approved RBG entropy sources) employed by a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- Specification of each of the key generation methods (Approved and non-Approved) employed by a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- Specification of the key establishment methods employed by a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- Specification of the key entry and output methods employed by a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- 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, 4, and5)*

- Specification of the SSP storage methods employed by a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- Specification of the SSP zeroization methods employed by a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

SELF-TESTS

- Specification of self-tests performed by a cryptographic module, including pre-operational, conditional, and critical functions tests. *(Security Levels 1, 2, 3, 4, and 5)*

- 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, 4, and 5)*

- 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, 4, and 5)*

- If a cryptographic module implements a bypass capability, specification of the mechanism or logic governing the switching procedure. *(Security Levels 1, 2, 3, 4, and 5)*

LIFE-CYCLE ASSURANCE

- Specification of procedures for secure installation, generation, and start-up of a cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- Specification of the procedures for maintaining security while distributing and delivering versions of a cryptographic module to authorized operators. *(Security Level 2, 3, 4, and 5)*

- 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, 4, and 5)*

- 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, 4, and 5)*

- If a cryptographic module contains hardware, specification of the schematics and/or the HDL listings for the hardware. *(Security Levels 1, 2, 3, 4, and 5)*

- 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, 4, and 5)*

- Specification of a formal model that describes the rules and characteristics of the cryptographic module Security Policy, using a formal specification language that is a rigorous notation based on established mathematics, such as first order logic or set theory. *(Security Level 4)*

- Specification of a rationale that demonstrates the consistency and completeness of the formal model with respect to the cryptographic module Security Policy. *(Security Level 4)*

- Specification of an informal proof of the correspondence between the formal model 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)*

- Specification of an informal proof of the correspondence between the design of the cryptographic module (as reflected by the pre-condition and post-condition annotations) and the functional specification. *(Security Level 4)*

- For Cryptographic Officer 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, 4, and 5)*,

  - procedures on how to administer the cryptographic module in a secure manner *(Security Levels 1, 2, 3, 4, and 5)*, and

  - assumptions regarding user behavior that is relevant to the secure operation of the cryptographic module. *(Security Levels 1, 2, 3, 4, and 5)*

- For User 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, 4, and 5)*, and

  - all user responsibilities necessary for the secure operation of the module. *(Security Levels 1, 2, 3, 4, and 5)*

MITIGATION OF OTHER ATTACKS

- If a cryptographic module is designed to mitigate one or more specific attacks, specification in the module's Security Policy of the security mechanisms employed by the cryptographic module to mitigate the attack(s). *(Security Levels 1, 2, 3, 4, and 5)*

SECURITY POLICY

- See Appendix C. *(Security Levels 1, 2, 3, 4, and 5)*

DRAFT

APPENDIX B: RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES

This Appendix is provided for informational purposes only and does not contain security requirements applicable to cryptographic modules within the scope of the standard.

Life-cycle software engineering recommendations (dealing with the specification, construction, verification, testing, maintenance, and documentation of software) should be followed. Software engineering practices may include documented unit testing, code reviews, explicit high-level and low-level design documents, explicit requirements and functional specifications, structure charts and data flow diagrams, function-point analysis, defect and resolution tracking, configuration management, and a documented software development process.

For all software development, both large and small, the following programming techniques are consistent with current practices and should be used to facilitate analysis of software components of a cryptographic module and to reduce chances of programming errors.

MODULAR DESIGN

- A modular design is recommended, especially for moderate to large-scale software development efforts. Each software module should have well-defined and readily understood logical interfaces.

- Software components should be constructed using the principles of data abstraction. If available, an object-oriented, high-level language that supports the construction of abstract data types should be used.

- The software should be hierarchically structured as a series of layers.

SOFTWARE MODULE/PROCEDURE INTERFACES

- Entries to a software module or procedure should be through external calls on explicitly defined interfaces.

- Each procedure should have only one entry point and at most two exit points, one for normal exits and one for error exits.

- Data should be communicated between software modules and between procedures through the use of argument lists and/or explicit return values. Global variables should not be used among procedures except where necessary for the implementation of abstract data types. Input values should be checked for range errors using assertion statements (if provided by the programming language in use).

INTERNAL CONSTRUCTION

- Each procedure should perform only a single, well-defined function.

- Control flow within a single thread of execution should be defined using only sequencing, structured programming constructs for conditionals (e.g., if-then-else or case), and structured constructs for loops (e.g., while-do or repeat-until).

- If concurrent execution is employed (e.g., via multiple threads, tasks, or processes), the software components should enforce limits on the maximum allowable degree of concurrency and should use structured synchronization constructs to control access to shared data.

- Equivalence of variables should not be used to permit multiple memory usage for conflicting purposes.

- Robust command parsing and range checking mechanisms should be implemented to guard against malformed requests, out-of-range parameters, and I/O buffer overflows.

IN-LINE DOCUMENTATION

- Each software module, procedure, and major programming construct should be documented specifying the functions performed along with a (formal or informal) specification of pre-conditions and post-conditions.

- Each loop should be preceded by a convincing argument (as a comment) that termination is guaranteed.

- Variable names should be used in only one context within the same procedure.

- Each variable should have an associated comment identifying the purpose of the variable and noting the range of allowable values, including if the range is unrestricted.

- If concurrency is employed, the documentation should specify how limits are enforced on the maximum allowable degree of concurrency and how accesses to shared data are synchronized in order to avoid (possibly undetected) run-time errors.

ASSEMBLY LANGUAGE

The following additional programming practices should be used when the implementation is in assembly language.

- All code should be position independent except where appropriate security concerns, efficiency, or hardware constraints require position dependency.

- All register references should use symbolic register names.

- Self-modifying code should not be used.

- All procedures should be responsible for saving and restoring the contents of any register that is used within the procedure.

- Control transfer instructions should not use numeric literals.

- Each unit of code should contain comments describing register use in the unit.

DRAFT

APPENDIX C: 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 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 physical boundary so that all the logical and physical layers between the logical object and the physical 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 physical boundary.
- Description of Module(s).
  - Provide explicit version/identification of the module and all components (hardware, software or firmware).
- Hardware, Software, or Hybrid designation.
  - For software 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 boundary.
- 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.
- The overall Security Strength of the module.
- 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.

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.

3. Roles, Services, and Authentication

- Specify all roles.
- Table of Roles, with corresponding services commands with input and output.

DRAFT

- 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 is loaded, specify the controls on loading and the isolation of code that deter unauthorized access to and use of the module.
- Describe the installation process and the cryptographic authentication mechanism(s).

4. Software Security

- Define the module boundary, contents, and logical security mechanisms.
- Separately list the security and non-security services.
- 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 modifiable or non-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, 4, and 5 modules, describe how the module provides protection for the CSPs against timing analysis attacks.
- For Security Level 4, and 5 modules, describe does the module provides protection for the CSPs against SPA and DPA attacks.
- For Security Level 5 modules, describe how the module provides protection for the CSPs from EME attacks.

8. SSP 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, indicate any related keys.
- Present a table of other CSPs and how they are generated.
- Specify the Random Bit Generators (Approved or Non-Approved).
- 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 and, if applicable, the PSP zeroization method(s) and rationale, and operator initiation capability.

9. Self-Tests

- Provide the list of pre-operational and conditional tests with defined parameters and list conditions under which the tests are performed.

DRAFT

- Describe all error states and status indicators.
- Describe operation initiation, if applicable.

10. Life-Cycle Assurance

- Provide a statement of the configuration management system and its unique identification. Name the commercial system, if used.
- Describe how design requirements are met.
- Describe the correspondence between the design, the security policy and the FSM (may be a separate document).
- Describe how development requirements are met.
- Describe the vendor testing.
- Specify the procedures for delivery and operation.
- Specify any maintenance requirements.
- Provide the Crypto Officer and User guidance (may be a separate document).

11. Mitigation of Other Attacks

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

DRAFT

APPENDIX D: SELECTED BIBLIOGRAPHY

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

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

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

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

DRAFT