FIPS PUB 140-2

FEDERAL INFORMATION PROCESSING STANDARD PUBLICATION
(Supersedes FIPS PUB 140-1, 1994 January 11)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

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

Issued MONTH DAY, 1999

U.S. Department of Commerce
William M. Daley, Secretary

Technology Administration
Cheryl L. Shavers, Under Secretary for Technology

National Institute of Standards
and Technology
Raymond G. Kammer, Director

Foreword

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235). These mandates have given the Secretary of Commerce and NIST important responsibilities for improving the utilization and management of computer and related telecommunications systems in the Federal government. The NIST, through its Information Technology Laboratory, provides leadership, technical guidance, and coordination of government efforts in the development of standards and guidelines in these areas.

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

William Mehuron, Director
Information Technology Laboratory

Abstract

The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security in its computer and telecommunication systems. This publication provides a standard to 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 are to be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module interfaces; roles, services, and authentication; finite state machine model; physical security; operating system security; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

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

National Institute of Standards
and Technology
FIPS PUB 140-2
59 pages (MONTH DAY, 1999)

U.S. Government Printing Office
Washington, 1999

For Sale by the National
Technical Information
Service
U.S. Department of Commerce

Federal Information
Processing Standards Publication 140-2

1999 MONTH DAY

Announcing the Standard for

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Management Reform Act of 1996 (Public Law 104-106) and the Computer Security Act of 1987 (Public Law 100-235).

1. Name of Standard. Security Requirements for Cryptographic Modules (FIPS PUB 140-2).

2. Category of Standard. Computer Security Standard, Cryptography.

3. Explanation. This standard specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting sensitive information. The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module interfaces; roles, services, and authentication; finite state machine model; physical security; operating system security; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks. This standard supersedes FIPS 140-1, *Security Requirements for Cryptographic Modules*, in its entirety.

The Cryptographic Module Validation Program (CMVP) validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-2 and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated Information (Canada). The goal of the CMVP is to promote the use of validated products and provide Federal agencies with a security metric to use in procuring equipment containing cryptographic modules.

In the CMVP, vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested. There are several National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories that perform FIPS 140-2 compliance testing, located in the U.S. and in Canada.

4. Approving Authority. Secretary of Commerce.

5. Maintenance Agency. Department of Commerce, National Institute of Standards and Technology, Information Technology Laboratory (ITL).

6. Cross Index.

a. FIPS PUB 46-3, Data Encryption Standard.
b. FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard.
c. FIPS PUB 81, DES Modes of Operation.

d. FIPS PUB 112, Password Usage.
e. FIPS PUB 113, Computer Data Authentication.
f. FIPS PUB 171, Key Management Using ANSI X9.17.
g. FIPS PUB 180-1, Secure Hash Standard.
h. FIPS PUB 186-2, Digital Signature Standard
i. Special Publication 800-2, Public Key Cryptography.

Other NIST publications may be applicable to the implementation and use of this standard. A list (NIST Publications List 91) of currently available computer security publications, including ordering information, can be obtained from NIST.

7. Applicability. This standard is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. This standard shall be used in designing and implementing cryptographic-based security systems that Federal departments and agencies operate or are operated for them under contract. Federal agencies, that use cryptographic-based security systems for protecting classified information, may use those systems for protecting unclassified information in lieu of systems that comply with this standard. Adoption and use of this standard is available to private and commercial organizations.

8. Applications. Cryptographic-based security systems may be utilized in various computer and telecommunication applications (e.g., data storage, access control and personal identification, network communications, radio, facsimile, and video) and in various environments (e.g., centralized computer facilities, office environments, and hostile environments). The cryptographic services (e.g., encryption, authentication, digital signature, and key management) provided by a cryptographic module will be based on many factors that are specific to the application and environment. The security level of a cryptographic module shall 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 and the security services that the module is to provide. The security requirements for a particular security level include both the security requirements specific to that level and the security requirements that apply to all modules regardless of the level.

9. Specifications. Federal Information Processing Standard (FIPS) 140-2, Security Requirements for Cryptographic Modules (affixed).

10. Implementations. This standard covers implementations of cryptographic modules including, but not limited to, hardware components or modules, software programs or modules, computer firmware, or any combination thereof. Cryptographic modules that are validated under the CMVP will be considered as complying with this standard. Information about the CMVP can be obtained from the National Institute of Standards and Technology, Information Technology Laboratory, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

11. Approved Security Functions. Cryptographic modules that comply with this standard shall employ cryptographic algorithms, cryptographic key generation algorithms and key management techniques, and authentication techniques that have been approved for protecting Federal government sensitive information. Approved cryptographic algorithms and techniques include those that are either:

a. specified in a Federal Information Processing Standard (FIPS), or
b. adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS.

If a cryptographic module is required to incorporate a trusted operating system, then the module shall employ trusted operating systems that have been evaluated by an accredited evaluation authority.

12. Interpretation. Resolution of questions regarding this standard will be provided by NIST. Questions concerning the content and specifications should be addressed to: Director, Information Technology Laboratory, ATTN: FIPS 140-2 Interpretation, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

13. Export Control. Certain cryptographic devices and technical data regarding them are subject to Federal export controls and exports of cryptographic modules implementing this standard and technical data regarding them must comply with these Federal regulations and be licensed by the Bureau of Export Administration of the U.S. Department of Commerce. Applicable Federal government export controls are specified in Title 15, Code of Federal Regulations (CFR) Part 740.17; Title 15, CFR Part 742; and Title 15, CFR Part 774, Category 5, Part 2.

14. Implementation Schedule. This standard becomes effective six months after approval by the Secretary of Commerce. A transition period from MONTH DAY, YEAR until six months after the effective date is provided to enable all agencies to develop plans for the acquisition of products that are compliant with FIPS 140-2. Agencies may retain and use FIPS 140-1 validated products that have been purchased before the end of the transition period. After the transition period, modules will no longer be tested against the FIPS 140-1 requirements. Figure 1 summarizes the FIPS 140-2 implementation schedule.

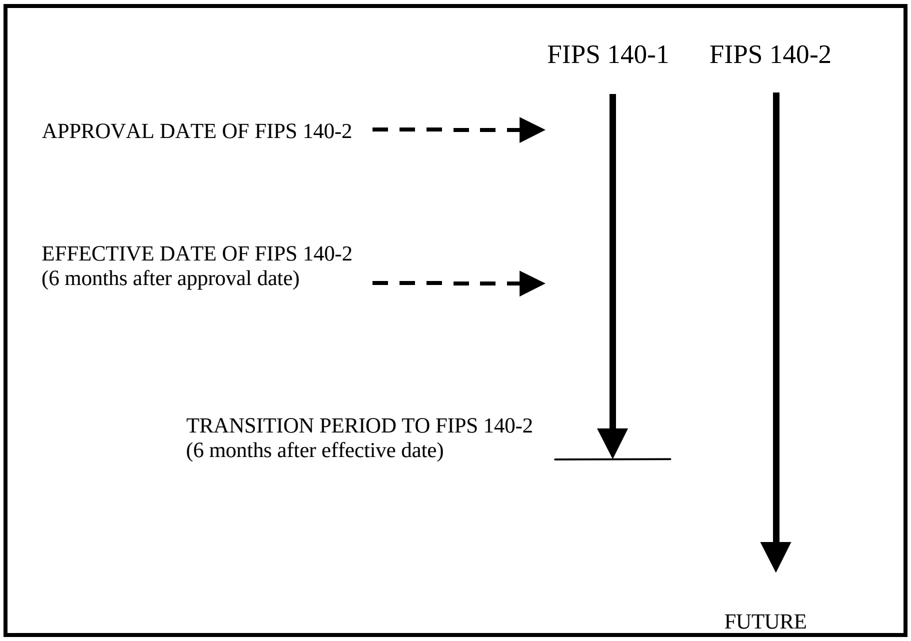
FIPS 140-1
FIPS 140-2
APPROVAL DATE OF FIPS 140-2
EFFECTIVE DATE OF FIPS 140-2
(6 months after approval date)
TRANSITION PERIOD TO FIPS 140-2
(6 months after effective date)
FUTURE

Figure 1. *FIPS 140-2 Implementation Schedule*

15. Qualifications. The security requirements specified in this standard are based upon information provided by many sources within the Federal government and private industry. The requirements are designed to protect against adversaries mounting cost-effective attacks on sensitive government or commercial data (e.g., hackers, organized crime, and economic competitors). The primary goal in designing an effective security system is to make the cost of any attack greater than the possible payoff.

While the security requirements specified in this standard are intended to maintain the security of a cryptographic module, conformance to this standard does not guarantee that a particular module is secure. It is the responsibility of the manufacturer of a cryptographic module to build the module in a secure manner.

Similarly, the use of a cryptographic module that conforms to this standard in an overall system does not guarantee the security of the overall system. The responsible authority in each agency shall assure that an overall system provides an acceptable level of security.

Since a standard of this nature must be flexible enough to adapt to advancements and innovations in science and technology, this standard will be reviewed every five years in order to consider new or revised requirements that may be needed to meet technological and economic changes.

16. Waiver Procedure. Under certain exceptional circumstances, the heads of Federal agencies, or their delegates, may approve waivers to Federal Information Processing Standards (FIPS). The heads of such agencies may redelegate such authority only to a senior official designated pursuant to Section 3506(b) of Title 44, U.S. Code. Waivers shall be granted only when compliance with a standard would

a. adversely affect the accomplishment of the mission of an operator of Federal computer system or

b. cause a major adverse financial impact on the operator that is not offset by government-wide savings.

Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine which conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision that explains the basis on which the agency head made the required finding(s). A copy of each such decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decision, Information Technology Laboratory, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

In addition, notice of each waiver granted and each delegation of authority to approve waivers shall be sent promptly to the Committee on Government Operations of the House of Representatives and the Committee on Government Affairs of the Senate and shall be published promptly in the Federal Register.

When the determination on a waiver applies to the procurement of equipment and/or services, a notice of the waiver determination must be published in the Commerce Business Daily as a part of the notice of solicitation for offers of an acquisition or, if the waiver determination is made after that notice is published, by amendment to such notice.

A copy of the waiver, any supporting documents, the document approving the waiver and any supporting and accompanying documents, with such deletions as the agency is authorized and decides to make under Section 552(b) of Title 5, U.S. Code, shall be part of the procurement documentation and retained by the agency.

17. Where to obtain copies. Copies of this publication are available for sale by the National Technical Information Service, U.S. Department of Commerce, Springfield, VA 22161. When ordering, refer to Federal Information Processing Standards Publication 140-2 (FIPSPUB1402) and identify the title. When microfiche is desired, this should be specified. Prices are published by NTIS in current catalogs and other issuances. Payment may be made by check, money order, deposit account, or charged to a credit card accepted by NTIS.

TABLE OF CONTENTS

1. OVERVIEW

This standard specifies the security requirements that are to be satisfied by 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. Cryptographic modules conforming to this standard shall meet the applicable security requirements described herein.

FIPS 140-1 was developed by a government and industry working group composed of both users 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 are specified for each of 11 requirement areas. Each security level offers an increase in security over the preceding level. These four increasing levels of security will allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments. FIPS 140-2 incorporates changes in applicable standards and technology since the development of FIPS 140-1 and changes based on comments received from the vendor, laboratory, and user communities.

While the security requirements specified in this standard are intended to maintain the security of a cryptographic module, conformance to this standard does not guarantee that a particular module is secure. It is the responsibility of the vendor of a cryptographic module to build the module in a secure manner.

Similarly, the use of a cryptographic module that conforms to this standard in an overall system does not guarantee the security of the overall system. The overall security level of a cryptographic module should 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 and for the security services that the module is to provide. The responsible authority in each organization should assure 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. Since information security requirements will vary for different applications, organizations should identify their information resources and determine the sensitivity to and the potential impact of losses. Controls should be based on the potential risks and should be selected from available controls, including administrative policies and procedures, physical and environmental controls, information and data controls, software development and acquisition controls, and backup and contingency planning.

The following sections provide an overview of the four security levels. Common examples, given to illustrate how the requirements might be met, are not intended to be restrictive or exhaustive. Cryptographic modules, incorporated into commercially available products, have been validated to meet every security level specified by this Standard. All requirements of this Standard are described in detail in Section 4.

1.1 Security Level 1

Security Level 1 provides the lowest level of security. It specifies basic security requirements for a cryptographic module (e.g., the encryption algorithm shall be an Approved algorithm (Section 2)), but it differs from the higher levels of security in several aspects. For example, no physical security mechanisms are required in the cryptographic module beyond the requirement for production-grade equipment. An example of a Security Level 1 system is a personal computer (PC) encryption board.

Security Level 1 also allows software cryptographic functions to be performed in a general purpose PC. Such implementations may be appropriate for low-level security applications. The implementation of PC cryptographic software may be more cost-effective than hardware-based mechanisms. This will enable organizations to select from alternative cryptographic solutions to meet lower-level security requirements.

1.2 Security Level 2

Security Level 2 improves the physical security of a Security Level 1 cryptographic module by adding the requirement for tamper-evident coatings or seals or for pick-resistant locks. Tamper-evident coatings or seals are placed on a cryptographic module so that the coating or seal would have to be broken in order to attain physical access to the plaintext cryptographic keys and other 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, at a minimum, 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 also allows software cryptography in multi-user timeshared systems when used with an operating system that

- meets the functional requirements specified in the Common Criteria (CC) Controlled Access Protection Profile (CAPP) and

- is evaluated at the CC evaluation assurance level EAL2.

An equivalent evaluated trusted operating system may be used. A trusted operating system is needed in order for software cryptography to be implemented with a level of trust comparable to hardware cryptography.

1.3 Security Level 3

In addition to the tamper-evident security requirements of Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. For example, a multiple-chip embedded cryptographic module must be contained in a strong enclosure and, if a removable cover is removed or a door is opened, any unprotected CSPs are zeroized.

Security Level 3 requires identity-based authentication, which is stronger than the role-based authentication 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 the data ports used for entering and outputting CSPs to be physically separated from other data ports. Furthermore, the parameters are either entered into or output from the cryptographic module in encrypted form (in which case they may travel through enclosing or intervening systems) or are directly entered into or output from the module (without passing through enclosing or intervening systems) using split knowledge procedures.

Security Level 3 allows software cryptography in multi-user timeshared systems when used with an operating system that:

- meets the functional requirements specified in the CAPP with the additional functional requirement of a Trusted Path (FTP_TRP.1) and

- is evaluated at the CC evaluation assurance level EAL3 with the additional assurance requirement of an Informal Target of Evaluation (TOE) Security Policy Model (ADV_SPM.1).

An equivalent evaluated trusted operating system may be used. The trusted path has the capability to protect cryptographic software and CSPs from other untrusted software that may run on the system. Such a system prevents plaintext from being mixed with ciphertext and it prevents the unintentional transmission of plaintext keys**.**

1.4 Security Level 4

Security Level 4 provides the highest level of security. At this level, physical security provides an envelope of protection around the cryptographic module with the intent of detecting a penetration from any direction. For example, an attempt to cut through the enclosure of the cryptographic module is detected and all CSPs are zeroized. Security Level 4 cryptographic modules are useful for operation in physically unprotected environments.

Security Level 4 also protects a cryptographic module against a compromise of its security due to environmental conditions or fluctuations outside of the module's normal operating ranges for voltage and temperature. Intentional excursions beyond the normal operating ranges may be used by an attacker to thwart a cryptographic module's defense during an attack. 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 in order to provide a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

Security Level 4 allows software cryptography in multi-user timeshared systems when used with an operating system that

- meets the functional requirements specified for Security Level 3 and

- is evaluated at the CC evaluation assurance level EAL4 with the additional assurance requirements of Formal TOE Security Policy Modeling (ADV_SPM.3), Covert Channel Analysis (AVA_CCA.1), and Modularity (ADV_INT.1).

An equivalent evaluated trusted operating system may be used. An operating system evaluated at EAL4 with the additional listed requirements provides assurances of the correct operation of the security features of the operating system.

2. GLOSSARY OF TERMS AND ACRONYMS

2.1 Glossary of Terms

The following definitions are used throughout this standard:

Approved: FIPS-Approved

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

Approved security function: for this Standard, an Approved security function (e.g., cryptographic algorithm, cryptographic key generation algorithm, cryptographic key distribution technique, authentication technique, or evaluation criteria) that is either a) specified in a FIPS or b) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS. (Approved security functions are listed in the Implementation Guidance for this Standard.)

Authentication code: a cryptographic checksum based on an Approved security function (also known as a Message Authentication Code (MAC) in ANSI standards).

Automated key distribution: the distribution of cryptographic keys, usually in encrypted form, using electronic means such as a computer network (e.g., key exchange/agreement protocols or ANSI X9.17).

Compromise: the unauthorized disclosure, modification, substitution, or use of sensitive data (including plaintext cryptographic keys and other CSPs).

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

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

Critical security parameter (CSP): security-related information (e.g., secret and private cryptographic keys, and authentication data such as passwords and PINs) appearing in plaintext or otherwise unprotected form and whose disclosure or modification can compromise the security of a cryptographic module or the security of the information protected by the module.

Cryptographic boundary: an explicitly defined contiguous perimeter that establishes the physical bounds of a cryptographic module.

Cryptographic key (key): a parameter used in conjunction with a cryptographic algorithm that determines

- 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: the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Cryptographic module security policy: a precise specification of the security rules under which a cryptographic module will operate, including the rules derived from the requirements of this standard and additional rules imposed by the vendor.

Crypto officer: an individual or process (subject), acting on behalf of the individual, accessing a cryptographic module in order to perform cryptographic initialization or management functions.

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 variations of the electrical power consumption of a device, using advanced statistical methods and/or error correction techniques, for the purpose of extracting information correlated to encryption keys used in a cryptographic algorithm.

Digital signature: a non-forgeable transformation of data that allows proof of the source (with non-repudiation) and verification of the integrity of that data.

Electromagnetic compatibility (EMC): the ability of electronic systems to operate in their intended environments without suffering an unacceptable degradation of the performance as a result of unintentional electromagnetic radiation or response.

Electromagnetic interference (EMI): electromagnetic phenomena that either directly or indirectly can contribute to a degradation in the performance of an electronic system.

Electronic key entry: the entry of cryptographic keys into a cryptographic module in electronic form using a key-loading device. The operator entering the key may have no knowledge of the value of the key being entered.

Encrypted key: a cryptographic key that has been encrypted with a key encrypting key, a PIN, or a password in order to disguise the value of the underlying plaintext key.

Environmental failure protection (EFP): the use of features designed 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 (EFT): the use of testing to provide a reasonable assurance that a cryptographic module will not be affected by environmental conditions or fluctuations outside of the module's normal operating range in a manner that can compromise the security of the module.

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

Finite state machine (FSM): a mathematical model of a sequential machine that is comprised of a finite set of states, a finite set of inputs, a finite set of outputs, a mapping from the sets of inputs and states into the set of states (i.e., state transitions), and a mapping from the sets of inputs and states onto the set of outputs (i.e., an output function).

Firmware: the programs and data stored in hardware (e.g., ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution.

Hardware: the physical equipment used to process programs and data in a cryptographic module.

Hash-based message authentication code (HMAC): a message authentication code that utilizes a keyed hash.

Initialization vector (IV): a vector used in defining the starting point of an encryption process within a cryptographic algorithm.

Input data: information that is entered into a cryptographic module for the purposes of transformation or computation.

Integrity: the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Interface: a logical section of a cryptographic module that defines a set of entry or exit points that provide access to the module, including information flow or physical access.

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

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., IVs and passwords) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, and deletion or destruction.

Manual key distribution: a non-electronic means of distributing cryptographic keys.

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

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

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 to be exported from a cryptographic module.

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

Personal identification number (PIN): a 4 or more character alphanumeric code or password used to authenticate an identity (commonly used in banking applications).

Physical protection: the safeguarding of a cryptographic module, cryptographic keys, or other CSPs using physical means.

Plaintext key: an unencrypted cryptographic key.

Port: a functional unit of a cryptographic module through which data or signals can enter or exit the module. Physically separate ports do not share the same physical pin or wire.

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

Protection Profile: an implementation-independent set of security requirements for a category of Targets of Evaluation (TOEs) that meet specific consumer needs.

Public key: a cryptographic key, used with a public key cryptographic algorithm, 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 unambiguously identifies an entity, contains the entity's public key, is digitally signed by a trusted party, binding the public key to the entity.

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, given the public key, it is computationally infeasible to derive the private key.

Removable cover: a cover designed to permit physical access to the contents of a cryptographic module.

Secret key: a cryptographic key, used with a secret key cryptographic algorithm that is uniquely associated with one or more entities and should not be made public. The use of the term "secret" in this context does not imply a classification level; rather the term implies the need to protect the key from disclosure or substitution.

Secret key (symmetric) cryptographic algorithm: a cryptographic algorithm that uses a single secret key for both encryption and decryption.

Security policy: see cryptographic module security policy.

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

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 device, for the purpose of revealing the features and implementations of cryptographic algorithms and subsequently the values of cryptographic keys.

Software: the programs and associated data that can be dynamically written and modified.

Split knowledge: a condition under which two or more entities separately have key components that individually convey no knowledge of the plaintext key that will be produced when the key components are combined in the cryptographic module.

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

System software: the special software (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, programs, and data.

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

Tamper evidence: the indication that physical tampering of the cryptographic module has occurred.

Tamper response: the automatic action taken by a cryptographic module when it detects that physical tampering has occurred (minimum response action is the zeroization of plaintext keys and other CSPs).

Target of Evaluation (TOE): an information technology product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

Transient Electromagnetic Pulse Standard (TEMPEST): the standard by which the government measures electromagnetic computer emissions and details what is safe (allowed to leak) from monitoring.

TOE Security Functions (TSF): A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TOE Security Policy.

TOE Security Policy (TSP): A set of rules that regulate how assets are managed, protected, and distributed within a Target of Evaluation.

Trusted path: a means by which an operator and a TOE Security Function can communicate with the necessary confidence to support the TOE Security Policy.

User: an individual or a process (subject), operating on behalf of the individual, accessing a cryptographic module in order to obtain cryptographic services.

Zeroization: a method of erasing electronically stored data by altering or deleting the contents of the data storage so as to prevent the recovery of the data.

2.2 Acronyms

The following acronyms and abbreviations are used throughout this standard:

ANSI	American National Standards Institute
API	Application Program Interface
CAPP	Controlled Access Protection Profile
CBC	Cipher Block Chaining
CC	Common Criteria
CSE	Communications Security Establishment of the Government of Canada
CSP	Critical Security Parameter
CMVP	Cryptographic Module Validation Program
DAC	Discretionary Access Control
DES	Data Encryption Standard
DOC	Department of Commerce
DOD	Department of Defense
DPA	Differential Power Analysis
DTR	Derived Test Requirements
EAL	Common Criteria Evaluation Assurance Level
EDC	Error Detection Code
EEPROM	Electronically-Erasable Programmable Read-Only Memory
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMC	Electromagnetic Compatibility

EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read-Only Memory
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
FSM	Finite State Machine
HDL	Hardware Description Language
HMAC	Hash-Based Message Authentication Code
IC	Integrated Circuit
IG	Implementation Guidance
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
IV	Initialization Vector
LED	Light Emitting Diode
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
PC	Personal Computer
PIN	Personal Identification Number
PRNG	Pseudo-Random Number Generator
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read-Only Memory
SPA	Simple Power Analysis
TEMPEST	Transient Electromagnetic Pulse Standard
TOE	Target of Evaluation
TSF	Target of Evaluation Security Functions
TSP	Target of Evaluation Security Policy

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 protect a cryptographic module from unauthorized operation or use.

- To prevent the unauthorized disclosure of the contents of the cryptographic module, including plaintext cryptographic keys and other CSPs.

- To prevent the unauthorized and undetected modification of the cryptographic module, including the unauthorized modification, substitution, insertion, and deletion of cryptographic keys and other CSPs.

- To employ Approved security functions for the protection of sensitive information.

- 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.

- To detect errors in the operation of the cryptographic module and to prevent the compromise of sensitive data and CSPs as a result of those errors.

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 and implementation of a cryptographic module. These areas include cryptographic module specification; module interfaces; roles, services, and authentication; finite state machine model; physical security; operating system security; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; and design assurance. An additional area concerned with mitigation of other attacks is currently not tested but the vendor is required to document implemented controls (e.g., differential power analysis, and TEMPEST). Table 1 summarizes the security requirements in each of these areas.

	Security Level 1	***Security Level 2***	***Security Level 3***	***Security Level 4***
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Machine Model	Specification of finite state machine model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP and EFT.
Operating System Security	Executable code. Authenticated software. Single operator.	CAPP evaluated at EAL2.	CAPP plus trusted path evaluated at EAL3 plus security policy modeling.	CAPP plus trusted path evaluated at EAL4 plus security policy modeling, covert channel analysis, and modularity.
Cryptographic Key Management	Approved key generation/distribution techniques.		Entry/output of keys in encrypted form or direct entry/exit with split knowledge procedures.	
EMI/EMC	FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for voice).		FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.		Statistical RNG/PRNG tests – callable on demand.	Statistical RNG/PRNG tests – performed at power-up.
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification. Functional testing.	High-level language implementation. Test Coverage analysis.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Table 1: *Summary of security requirements*

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. Several areas provide for increasing levels of security with cumulative security requirements for each security level. In these areas, the cryptographic module shall 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 cryptographic module shall receive a rating commensurate with the overall level of security.

In addition to receiving independent ratings for each of the security areas, a cryptographic module shall also receive an overall rating. The overall rating shall indicate the minimum of the independent ratings received in the areas.

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

4.1 Cryptographic Module Specification

A cryptographic module shall be a set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms and key generation, and is contained within a defined cryptographic boundary. A cryptographic module shall implement at least one Approved algorithm or Approved security function used in an Approved mode of operation. Other algorithms or security functions may also be included for use in non-Approved modes of operation. The operator shall be able to determine when an Approved mode of operation is selected. (Approved algorithms and Approved security functions are listed in *Implementation Guidance* 1.1 for this Standard.)

A cryptographic boundary shall be an explicitly defined contiguous perimeter that establishes the physical bounds of the cryptographic module. If a cryptographic module contains software or firmware, the cryptographic boundary shall be defined such that it contains the processor and other hardware that store and protect code, unprotected keys, and other unprotected CSPs. Hardware, software, and firmware components of a cryptographic module can be excluded from the requirements of this standard if it can be shown that these components do not affect the security of the module.

The following documentation requirements shall apply to all security-specific hardware, software, and firmware contained within a cryptographic module. These requirements do not apply to microcode or system software whose source code is not available to the vendor or to any hardware, software, or firmware that can be shown not to affect the security of the cryptographic module.

- Documentation shall specify the hardware, software, and firmware components of a cryptographic module, specify the cryptographic boundary surrounding these components, and describe the physical configuration of the module (see Section 4.5).

- Documentation shall specify any hardware, software, or firmware components of a cryptographic module that are excluded from the security requirements of this standard and explain the rationale for the exclusion.

- Documentation shall specify the interfaces of a cryptographic module, including any physical or logical ports and any physical covers or doors.

- Documentation shall specify the manual or logical controls of a cryptographic module, physical or logical status indicators, and their physical, logical, or electrical characteristics.

- Documentation shall specify all cryptographic algorithms and security functions, both Approved and non-Approved, employed by a cryptographic module and all modes of operation, both Approved and non-Approved.

- Documentation shall specify

  ❑ a block diagram depicting all of the major hardware components of a cryptographic module and their interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory, and

  - ❑ a detailed specification of the design of the hardware, software, and firmware contained within a cryptographic module. High-level specification languages for software/firmware or schematics for hardware should be used to document the design.

- Documentation shall specify a cryptographic module security policy. The security policy shall include the rules derived from the requirements of this standard and the rules derived from any additional requirements imposed by the vendor. (See Appendix C.)

4.2 Cryptographic Module Interfaces

A cryptographic module shall be designed to restrict all information flow and physical access to 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 and output data may enter and 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). An Application Program Interface (API) of a software component of a cryptographic module may constitute a logical interface.

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

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

Data output interface. All data (except status data output via the status output interface) that is to be output from a cryptographic module (including plaintext data, ciphertext data, cryptographic keys and other key management data, authentication data, and control information for another module) shall exit via the "data output" interface. All data output via the data output interface shall be inhibited when an error state exists and during self-tests.

Control input interface. All input commands, signals, and control data (including 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 status codes and physical indicators such as Light Emitting Diodes (LEDs) and displays) used to indicate the status of a cryptographic module shall exit via the "status output" interface.

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

For Security Levels 1 and 2, the data input and output physical port(s) used for cryptographic keys, authentication data, and other CSPs may be shared with other ports of the cryptographic module.

For Security Levels 3 and 4, the data input and output physical port(s) used for plaintext cryptographic key components, plaintext authentication data, and other unprotected CSPs shall be physically separated from all other ports of the cryptographic module. Plaintext cryptographic key components, plaintext authentication data, and other unprotected CSPs shall be directly entered into the cryptographic module (as required in Section 4.7.4). The keys referred to here are secret and/or private keys. Public keys fall under the category of “other data” and do not need to be logically protected.

All input data entering the cryptographic module via the "data input" interface shall only pass through the input data path. All output data exiting the cryptographic module via the "data output" interface shall only pass through the output data path. In order to prevent the inadvertent output of sensitive information, two independent internal actions shall be required in order to output data via any output interface through which plaintext cryptographic keys or other CSPs or sensitive data could be output (e.g., two different software flags are set, one of which may be user-initiated; or two hardware gates are set serially from two separate actions). The output data path shall be logically disconnected from the circuitry and processes while performing key generation, manual key entry, or key zeroization.

If a cryptographic module includes a power interface, all external electrical power shall enter or exit via the "power interface". A power interface is not required when all power is provided or maintained internally to the cryptographic module.

Documentation shall include a complete specification of the defined input and output data paths.

4.3 Roles, Services, and Authentication

A cryptographic module shall support authorized roles and their corresponding services. 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 and services performed by each operator. Furthermore, depending on the security level, a cryptographic module may be required to employ access control mechanisms to authenticate an operator accessing the module and to verify that the operator is authorized to assume the desired role and to perform the services within that role. An operator is not required to assume an authorized role for services where cryptographic keys and CSPs are not modified, disclosed, or substituted (e.g., *show status, self-tests,* or other services that do not affect the security of the module).

4.3.1 Roles

A cryptographic module shall support the following authorized roles for operators:

> *User role.* The role assumed to obtain security services and to perform cryptographic operations or other authorized functions.
>
> *Crypto officer role*: The role assumed to perform a set of cryptographic initialization or management functions (e.g., cryptographic key and parameter entry, audit functions, and alarm resetting).

If the cryptographic module allows for maintenance, then the module shall support the following authorized role for operators:

> *Maintenance role:* The role assumed to perform physical maintenance and/or logical maintenance (e.g., hardware/software diagnostics). All plaintext secret and private keys and other unprotected CSPs shall be zeroized when entering or exiting the maintenance role.

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

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

4.3.2 Services

Services shall refer to all of the services, operations, or functions that can be performed by a cryptographic module. *Service inputs* shall consist of all data or control inputs to the cryptographic module that initiate or obtain specific services, operations, or functions. *Service outputs* shall consist of all data and status outputs that result from services, operations, or functions initiated or obtained by service inputs. Each service shall result in a service output.

A cryptographic module shall, at a minimum, provide the following services:

Show status. Output the current status of the module.

Self-tests. Initiate and run the self-tests as specified in Section 4.9.

If a cryptographic module implements a *bypass* capability, where services are provided without cryptographic processing (e.g., transferring plaintext through the module), then

- two independent internal actions shall be implemented to activate the capability in order to prevent inadvertent bypass of data due to a single error, and

- the module shall show status to indicate whether 1) the module is exclusively providing a cryptographic service, 2) the bypass service is exclusively activated, or 3) the module is alternating between a cryptographic service and a bypass service.

Documentation shall specify the authorized services that can be performed by the cryptographic module. For each service, the service inputs, corresponding service outputs, and the authorized role (or set of roles) in which the service can be performed, shall be specified. Specific services may be performed in more than one role (e.g., key entry may be performed in the user role, the crypto officer role, and the maintenance role). Documentation shall specify any services that can be performed by the operator without assuming an authorized role, and specify how these services do not modify, disclose, or substitute cryptographic keys and CSPs, or otherwise affect the security of the cryptographic module.

4.3.3 Operator Authentication

Authentication data within the cryptographic module (e.g., passwords and biometric information) shall be protected against unauthorized disclosure, modification, and substitution. Depending on the security level, a cryptographic module shall perform either role-based authentication or identity-based authentication.

Role-based authentication: A cryptographic module shall authenticate that the operator is authorized to assume a specific role (or set of roles). The cryptographic module shall require that the operator select one or more roles, and the module shall authenticate that the operator is authorized to assume the selected roles and to request the corresponding services. The cryptographic module is not required to authenticate the individual identity of each operator. The selection of roles and the authentication of the authorization to perform those roles may be combined. If a cryptographic module permits an operator to change roles, then the module shall verify the authorization of the operator to assume any role that was not previously authenticated.

Identity-based authentication: A cryptographic module shall authenticate the identity of an operator and verify that the identified operator is authorized to assume a specific role (or set of roles). The cryptographic module shall require that the operator be individually identified and that the specified identity be authenticated. The cryptographic module shall require that the operator select one or more roles and, based on the authenticated identity, verify that the operator is authorized to assume the selected role and to request the corresponding services. The authentication of the identity of the operator, selection of roles, and verification of the authorization to assume those roles may be combined. If a cryptographic module permits an operator to change roles without reauthenticating the identity of the operator, then the module shall verify the authorization of the authenticated operator to assume the new role.

A cryptographic module may permit an operator to perform all of the services allowed within an authorized role, or may require separate authorizations for each service or for different sets of services. When a cryptographic module is powered up, the results of previous authentications shall not be retained (i.e., the module shall reauthenticate the authorization of the operator to assume a desired role).

A cryptographic module may implement any of a variety of authentication mechanisms including (but not limited to): 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).

The initialization of access control information may warrant special treatment. If, during the first time that an operator attempts to access a cryptographic module, the module does not contain the required authentication and authorization information needed for the operator to assume the crypto officer role, then other means (e.g., procedural controls or factory-set or default authentication and authorization information) shall be used to control access to the cryptographic module.

The strength of the authentication mechanism shall satisfy the following specifications:

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

- For multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur.

- Feedback of authentication data to an operator shall be obscured during authentication (e.g., no visible display of characters when entering a password).

- Feedback provided to an operator during an attempted authentication shall not weaken the strength of the authentication mechanism.

Documentation shall provide a description of the authentication mechanism(s) employed by the cryptographic module and the corresponding strength of the mechanism(s).

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 mechanisms of the operator accessing the module in order to verify that the operator is authorized to perform desired services within a role.

SECURITY LEVELS 3 AND 4

For Security Levels 3 and 4, a cryptographic module shall employ *identity-based* authentication mechanisms of the operator accessing the module in order to verify that the operator is authorized to perform desired services.

4.4 Finite State Machine Model

A cryptographic module shall be designed using a finite state machine model (or equivalent) that explicitly specifies every operational and error state of the module.

A cryptographic module shall include, at a minimum, the following states:

> *Power on/off states*. States for primary, secondary, or backup power. These states may distinguish between power applied to different portions of a cryptographic module.
>
> *Crypto officer states*. States in which the crypto officer services are performed (e.g., cryptographic initialization and key management).
>
> *Key/CSP entry states*. States for entering cryptographic keys and other CSPs into the cryptographic module and for checking their validity.
>
> *User states*. States in which authorized users obtain security services, perform cryptographic operations, or perform other authorized user functions.
>
> *Self-test states*. States in which the cryptographic module is performing self-tests.
>
> *Error states*. States when the cryptographic module has encountered an error (e.g., failed a self-test or attempted to encrypt when missing operational keys or other CSPs). Error states may include "hard" errors that indicate an equipment malfunction and that may require maintenance, service or repair of the cryptographic module, or recoverable "soft" errors that may require initialization or resetting of the module. Recovery from error states shall be possible except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.

A cryptographic module may contain other states including the following:

> *Uninitialized states*. States in which no cryptographic keys or other CSPs are loaded into the cryptographic module.
>
> *Idle states*. States in which the cryptographic module is operational but is not currently providing services or performing cryptographic functions.
>
> *Safety states*. States in which the cryptographic module is not currently operational but cryptographic keys and parameters are loaded. These states are used to protect the cryptographic module from unauthorized use during the temporary absence of the operator. The safety states shall require an explicit authenticated action to return to a user/crypto officer service state.
>
> *Bypass states*. States for providing services without cryptographic processing (e.g., transferring plaintext through the cryptographic module).
>
> *Maintenance states*. States for maintaining and servicing a cryptographic module, including maintenance testing. If a cryptographic module contains a maintenance role, then it shall include maintenance states.

Documentation shall identify and describe all states of the cryptographic module and shall describe all of the corresponding state transitions. The descriptions of the state transitions shall include the internal cryptographic module conditions and data inputs and control inputs that cause transitions from one state to another, and shall include the internal module conditions and data outputs and status outputs resulting from transitions from one state to another.

4.5 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 (including substitution of the entire module) when installed. All hardware, software, firmware, and data within the cryptographic boundary shall be protected.

Physical security requirements are specified for three distinct 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 device 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 security level of a cryptographic module, the physical security mechanisms shall be designed such that unauthorized attempts at physical access, use, or modification will have a high probability of being detected

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

and/or

- during an attempt so that appropriate actions can be taken by the cryptographic module to protect itself (i.e., tamper response).

In general, Security Level 1 requires minimal physical protection. Security Level 2 requires the addition of tamper-evident mechanisms. Security Level 3 additionally requires the use of strong enclosures with tamper detection and response mechanisms for removable covers and doors. Security Level 4 additionally requires the use of strong enclosures with tamper detection and response mechanisms for the entire enclosure. Tamper detection is not a substitute for tamper evidence. Environmental failure protection and testing (EFP/EFT) are required at Security Level 4.

All physical access paths, including removable covers or doors that are designed to permit physical access to the contents of a cryptographic module, shall be defined as part of the "maintenance access" interface. Any removable covers or doors defined as part of the maintenance access interface shall be safeguarded using the appropriate physical security mechanisms. If the cryptographic module has a maintenance access interface, all plaintext secret and private keys and other unprotected CSPs contained in the cryptographic module shall be zeroized when the maintenance access interface is accessed. Table 2 summarizes the physical security requirements for each of the four security levels.

	Single-Chip Cryptographic Modules	**Multiple-Chip Embedded Cryptographic Modules**	**Multiple-Chip Standalone Cryptographic Modules**
Security Level 1	Production-grade chip (with standard passivation).	Production-grade chips, production-grade multiple-chip embodiment. Production-grade enclosure or cover.	Production-grade chips, production-grade multiple-chip embodiment, and production-grade enclosure.
Security Level 2	Security Level 1 requirements. Opaque tamper-evident coating or enclosure.	Security Level 1 requirements. Opaque tamper-evident coating or enclosure, with tamper-evident seals for removable covers.	Security Level 1 requirements. Opaque enclosure with mechanical locks or tamper-evident seals for removable covers and doors.
Security Level 3	Security Levels 1 and 2 requirements. Hard opaque tamper-evident coating or strong enclosure. Protected vents.	Security Levels 1 and 2 requirements. Hard opaque potting material, strong enclosure or strong removable cover with tamper detection and zeroization circuitry. Protected vents.	Security Levels 1 and 2 requirements. Hard opaque potting material or strong enclosure with tamper response and zeroization circuitry for removable covers and doors. Protected vents.
Security Level 4	Security Levels 1, 2, and 3 requirements. Hard opaque removal-resistant coating. EFP/EFT for temperature and voltage.	Security Levels 1, 2, and 3 requirements. Tamper detection envelope with tamper response and zeroization circuitry. EFP/EFT for temperature and voltage.	Security Levels 1, 2, and 3 requirements. Tamper detection/response envelope with tamper response and zeroization circuitry. EFP/EFT for temperature and voltage.

Table 2: Summary of physical security requirements

4.5.1 General Physical Security Requirements

The following requirements shall apply to all physical embodiments.

- Documentation shall include a complete specification of the physical embodiment and the security level for which the physical security mechanisms of a cryptographic module are designed, as well as a complete description of the applicable physical security mechanisms employed by the module. Documentation shall specify the authorized physical maintenance procedures defined for the cryptographic module and how plaintext secret and private keys and other unprotected CSPs are to be zeroized when accessing the maintenance access interface.

SECURITY LEVEL 1

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

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

. SECURITY LEVEL 2

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

- The cryptographic module shall provide evidence of tampering (e.g., cover, enclosure, and seal).

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.

- When performing physical maintenance, zeroization of all plaintext secret and private keys and other unprotected CSPs contained in the cryptographic module shall be performed automatically by the module.
- If the cryptographic module contains any doors or removable covers, then the module shall contain tamper response and zeroization circuitry. Upon the opening of a door or the removal of a cover, the circuitry shall immediately zeroize all plaintext secret and private keys and other unprotected CSPs. The circuitry shall be operational when plaintext cryptographic keys or other unprotected CSPs are contained within the cryptographic module.
- If the cryptographic module contains any ventilation holes or slits, then they 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 either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in Section 4.5.5.

4.5.2 Single-Chip Cryptographic Modules

In addition to the general security requirements specified in Section 4.5.1, 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 chip shall be covered with a tamper-evident coating (e.g., a tamper-evident passivation material or a tamper-evident material covering the passivation) or contained in a tamper-evident enclosure to deter direct observation, probing, or manipulation of the surface features of the chip.
- The coating or enclosure shall be opaque within the visible spectrum.

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.

Either

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

or

- the chip shall be contained within a strong enclosure.

  The enclosure shall be such that attempts at removal or penetration 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.

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

- The solvency characteristics of the coating shall be such that dissolving the coating will have a high probability of dissolving or seriously damaging the chip.

4.5.3 Multiple-Chip Embedded Cryptographic Modules

In addition to the general security requirements specified in Section 4.5.1, the following requirements are specific to multiple-chip embedded cryptographic modules.

SECURITY LEVEL 1

The following requirement shall apply to multiple-chip embedded cryptographic modules for Security Level 1.

- If used, an enclosure or removable cover shall be of production-grade quality.

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.

Either

- the cryptographic module shall be encapsulated within a tamper-evident material (e.g., etch-resistant coating or bleeding paint) or contained in a tamper-evident enclosure in order to prevent direct observation of cryptographic module components and to provide evidence of attempts to tamper with or remove module components, and

- the material or enclosure shall be opaque within the visible spectrum,

or

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

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

- if the enclosure includes any doors or removable covers, then they shall be locked with pick-resistant mechanical locks that employ physical or logical keys or they shall be protected with tamper-evident seals (e.g., evidence tape or holographic seals).

SECURITY LEVEL 3

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

Either

- the cryptographic module shall be encapsulated within a hard potting material (e.g., a hard opaque epoxy)

or

- the applicable Security Level 3 requirements for multiple-chip standalone cryptographic modules shall apply.

SECURITY LEVEL 4

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

- The contents of the cryptographic module shall be encapsulated within 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 drilling, milling, grinding, or dissolving of the potting material or enclosure to an extent sufficient for accessing plaintext cryptographic keys or other unprotected CSPs within the cryptographic module.

- The cryptographic module shall contain tamper response and zeroization circuitry. The circuitry shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroize all plaintext cryptographic keys and other unprotected CSPs. The circuitry shall be operational when plaintext cryptographic keys or other unprotected CSPs are contained within the cryptographic module.

4.5.4 Multiple-Chip Standalone Cryptographic Modules

In addition to the general security requirements specified in Section 4.5.1, the following requirements are specific to multiple-chip standalone cryptographic modules.

SECURITY LEVEL 1

The following requirement shall apply to multiple-chip standalone cryptographic modules for Security Level 1.

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

SECURITY LEVEL 2

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

- The enclosure shall be opaque within the visible spectrum.

- If the enclosure includes any doors or removable covers, then they shall be locked with pick-resistant mechanical locks that employ physical or logical keys or they shall be protected with tamper-evident seals (e.g., evidence tape or 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.

Either

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

or

- the cryptographic module shall be contained within a strong enclosure such that attempts to remove it will have a high probability of causing serious damage to the circuitry within 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 multiple-chip standalone cryptographic modules for Security Level 4.

- The enclosure shall contain tamper detection mechanisms that provide a tamper detection envelope 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. These mechanisms shall be designed to detect tampering by means such as cutting, drilling, milling, grinding, or dissolving of the potting material or enclosure, to an extent sufficient for accessing plaintext cryptographic keys and other unprotected CSPs within the cryptographic module.
- The cryptographic module shall contain tamper response and zeroization circuitry. The circuitry shall continuously monitor the tamper detection envelope and, upon the detection of tampering, shall immediately zeroize all plaintext cryptographic keys and other unprotected CSPs. The circuitry shall be operational when plaintext cryptographic keys and other CSPs are contained within the cryptographic module.

4.5.5 Environmental Failure Protection/Testing

Electronic devices and circuitry are designed to operate within a particular range of environmental conditions. Deliberate or accidental excursions outside the specified normal operating range can cause erratic operation or failure of the electronic devices or circuitry within a cryptographic module that can compromise the security of the module. In order to provide reasonable assurance that the security of a cryptographic module cannot be compromised by environmental conditions, the module may either employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT).

For Security Levels 1, 2, and 3, a cryptographic module is not required to employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT). At Security Level 4, a cryptographic module shall either employ environmental failure protection (EFP) features or undergo environmental failure testing (EFT).

4.5.5.1 Environmental Failure Protection Features (Alternative 1)

Environmental failure protection (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. In particular, the cryptographic module shall monitor and correctly respond to fluctuations in the operating *temperature* and *voltage* outside of the specified normal operating ranges.

The protection features shall involve electronic circuitry or devices that shall continuously measure these environmental conditions. If a condition is determined to be outside of the cryptographic module's normal operating range, the protection circuitry shall either (1) shutdown the module to prevent it from operating outside the normal range or (2) immediately zeroize all plaintext cryptographic keys and other unprotected CSPs.

Documentation shall provide a complete specification and description of the environmental failure protection features employed by a cryptographic module.

4.5.5.2 Environmental Failure Testing Procedures (Alternative 2)

Environmental failure testing shall involve a combination of analysis, simulation, and testing of a cryptographic module in order to give a reasonable guarantee that environmental conditions or fluctuations (accidental or induced) outside the module's normal operating range will not result in the compromise of security. The vendor of a cryptographic module shall perform the required testing and shall provide documentation that completely specifies the nature of the environmental failure tests performed and the results of those tests.

In particular, environmental failure testing shall show that varying the operating temperature and voltage outside of a cryptographic module's specified normal operating ranges does not cause electronic devices or circuitry within the module to fail in a manner that can compromise the security of the module. The temperature range to be tested shall be from -100 to +200 degrees Celsius. The voltage range to be tested shall be from the smallest negative voltage (with respect to ground) that causes the destruction of the electronic devices or circuitry to the smallest positive voltage (with respect to ground) that causes the destruction of the electronic devices or circuitry, including reversing the polarity of the voltages. The cryptographic module shall be subjected to excursions outside its specified normal operating range while being operated in a normal manner. The electronic devices or circuitry may fail at any point outside the normal operating ranges but at no time shall the security of the cryptographic module be compromised. If at any time during the test, the security of the cryptographic module is compromised due to the failure of electronic circuitry or devices, then the design of the electronic circuitry or devices shall be corrected and the module shall be retested.

The documentation shall provide a complete description of the environmental failure testing procedures performed on the cryptographic module along with associated results.

4.6 Operating System Security

The operating system requirements in this section shall apply to a cryptographic module only if the module provides a means whereby an operator can load and execute software or firmware that was not included as part of the validation of the module. An example of a cryptographic module for which the operating system requirements apply is a general purpose computer running cryptographic software as well as untrusted user-supplied software (e.g., a spreadsheet or word processing program). In this case, the hardware, operating system, and cryptographic software are considered part of the cryptographic module.

Documentation shall identify the operating system employed by a cryptographic module and the evaluation assurance level.

SECURITY LEVEL 1

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

- For Security Level 1 only, the operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded).

- All cryptographic software shall be installed only as executable code in order to discourage scrutiny and modification by users.

- A cryptographic mechanism shall use an Approved authentication technique (e.g., the computation and verification of an authentication code or digital signature algorithm) for all cryptographic software within the cryptographic module. This cryptographic mechanism requirement may be incorporated as part of the Software/Firmware Integrity Test (Section 4.9.1) if an Approved authentication technique is employed for that test.

- For Security Level 1 only, the cryptographic module shall prevent access by other processes to private and secret keys, intermediate key generation values, and other CSPs during the time the cryptographic process is in use.

SECURITY LEVEL 2

In addition to the applicable requirements for Security Level 1, the following functional and assurance security requirements shall also apply for Security Level 2.

- All cryptographic software, cryptographic keys and other CSPs, and control and status information shall be under the control of

    - ❑ an operating system that meets the functional requirements specified in the Common Criteria (CC) Controlled Access Protection Profile (CAPP) evaluated at the CC evaluation assurance level EAL2, or

    - ❑ an equivalent evaluated trusted operating system.

- In order to protect plaintext data, cryptographic software, cryptographic keys, authentication data, and other CSPs, the discretionary access control (DAC) mechanisms of the evaluated operating system shall be employed to:

    - ❑ Specify the set of roles that can *execute* stored cryptographic software.

    - ❑ Specify the set of roles that can *modify* (i.e., write, replace, and delete) the following cryptographic module software components stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., cryptographic keys and audit data), other CSPs, and plaintext data.

      The operating system shall provide the capability to prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not.

    - ❑ Specify the set of roles that can *read* the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., cryptographic keys and audit data), other CSPs, and plaintext data.

The operating system shall provide the capability to prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary.

- □ Specify the set of roles that can *enter* cryptographic keys and other CSPs.

- The operating system shall provide an audit capability to record modifications, accesses, deletions, and additions of cryptographic data and other CSPs.

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

    - start-up and shutdown of the audit functions,
    - any attempt to modify or delete the audit trail,
    - all modifications of the values of security attributes,
    - all attempts to revoke security attributes,
    - all modifications to the audit configuration that occur while the audit collection functions are operating,
    - attempts to provide invalid input for crypto officer functions, and
    - the addition or deletion of a user to/from a crypto officer role.

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

    - any specific operation performed to process audit data stored in the audit trail,
    - any attempt to read the audit trail,
    - all requests to use authentication data management mechanisms,
    - all requests to perform an operation on an object covered by the security policy,
    - success and failure of binding user security attributes to a subject,
    - all modifications of the values of security attributes,
    - use of a security-relevant crypto officer function,
    - modifications to the group of users that are part of a role,
    - every use of the rights of a role,
    - changes to the time,
    - all requests to access user authentication data,
    - any use of an authentication mechanism (e.g., login),
    - all attempts to use the user identification mechanism, including the user identity provided,
    - explicit requests to assume a crypto officer role,
    - the allocation of a function to a crypto officer role, and
    - execution of the tests of the underlying machine and the results of the tests.

SECURITY LEVEL 3

In addition to the applicable requirements for Security Levels 1 and 2, the following functional and assurance security requirements shall also apply to operating systems for Security Level 3.

- All cryptographic software, cryptographic keys and other CSPs, and control and status information shall be under the control of

  - □ an operating system that meets the CAPP functional requirements with the additional requirement of a Trusted Path (FTP_TRP.1). The operating system shall be evaluated against the CC evaluation assurance level EAL3 with the additional requirement of Informal TOE Security Policy Model (ADV_SPM.1), or

  - □ an equivalent evaluated trusted operating system.

- All cryptographic keys, authentication data, other CSPs, control inputs, and status outputs shall be communicated only via a trusted mechanism (e.g., a dedicated I/O port or a trusted path). When a trusted path is used, the Target of Evaluation Security Functions (TSF) shall support the trusted path between itself and the operators for use when a positive TSF-to-operator connection is required. Communications via this trusted path shall be activated exclusively by an operator or the TSF and shall be logically isolated and unmistakably distinguishable from other paths.

- The operating system shall implement a policy that will prevent Trojan horse attacks.

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

  - ❑ all attempted uses of a trusted path function, and

  - ❑ identification of the initiator and target of a trusted path.

SECURITY LEVEL 4

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

- All cryptographic software, cryptographic keys and other CSPs, and control and status information shall be under the control of

  - ❑ an operating system that is evaluated against the CC evaluation assurance level EAL4, with the additional requirements of Formal TOE Security Policy Modeling (ADV_SPM.3), Covert Channel Analysis (AVA_CCA.1), and Modularity (ADV_INT.1), or

  - ❑ an equivalent evaluated trusted operating system.

4.7 Cryptographic Key Management

The requirements for cryptographic key management encompass the entire lifecycle of cryptographic keys used by the cryptographic module. This includes key generation, distribution, entry/output, storage, and destruction. A cryptographic module may also use the key management features of another cryptographic module. The requirements for key management shall be met by all cryptographic modules that implement secret key and/or public key algorithms.

Secret keys and private keys shall be protected from unauthorized disclosure, modification, and substitution. Public keys shall be protected within the cryptographic module against unauthorized modification and substitution.

4.7.1 Random and Pseudorandom Number Generators (RNG/PRNG)

A cryptographic module may implement true random number generators (RNGs) and/or pseudorandom number generators (PRNGs). If a cryptographic module implements an RNG/PRNG, then values output from the RNG/PRNG shall pass all statistical tests for randomness as specified in Section 4.9.

An Approved RNG/PRNG shall be used for key generation. The output from a non-Approved RNG/PRNG may be used to 1) seed an Approved PRNG or 2) generate initialization vectors (IVs).

Documentation shall specify the type of RNG/PRNG employed by the cryptographic module.

4.7.2 Key Generation

Internal key generation is optional. Keys generated by the cryptographic module for use in an Approved algorithm shall be generated using an Approved key generation method. If a key generation method requires input from an RNG/PRNG, then an RNG/PRNG that meets the requirements specified in Section 4.7.1 shall be used. It shall be no easier (i.e., at least as many operations are required) to compromise the key generation method than it is to guess the generated key.

Intermediate key generation values shall not be accessible outside of the cryptographic module in plaintext or otherwise unprotected form.

Documentation shall specify the key generation methods employed by the cryptographic module.

4.7.3 Key Exchange/Agreement

Key exchange/agreement may be performed by manual methods, automated methods, or a combination of automated and manual methods. When implemented by the cryptographic module, only Approved key exchange/agreement techniques shall be used. It shall be no easier (i.e., at least as many operations are required) to compromise the key exchange/agreement technique than it is to guess the agreed upon or exchanged key. When a *key exchange* method is used, the key being exchanged shall meet the key entry/output requirements of Section 4.7.4. When a *key agreement* method is used, in which a key value is derived from shared material, the key material does not have to meet the key entry/output requirements of Section 4.7.4.

Approved *public key*-based key exchange/agreement techniques may be used to exchange or agree on secret or private key values. Until such time as an Approved key exchange/agreement technique is established, commercially available public key methods may be used. Public, private, and secret keys used to perform key exchange/agreement shall meet key generation requirements in Section 4.7.2.

Documentation shall specify the key exchange/agreement techniques employed by the cryptographic module.

4.7.4 Key Entry and Output

Cryptographic keys may be entered into or output from a cryptographic module using manual (e.g., via a keyboard) or electronic methods (e.g., cards and integrated circuit (IC) chip devices, smart cards/tokens, PC cards, or other electronic key loaders).

A seed key, if entered during key generation, shall be entered in the same manner as cryptographic keys.

Documentation shall specify the key entry and output methods employed by the cryptographic module.

All encrypted secret and private keys, entered into or output from the cryptographic module and used in an Approved mode of operation, shall be encrypted using an Approved algorithm. Public keys may be entered/output in plaintext form. A means shall be provided to ensure that a key (secret, private, or public) entered into or output from a cryptographic module is associated with the correct entity (i.e., person, group, or process) to which the key is assigned.

Manually-entered cryptographic keys (keys entered using manual methods) shall be verified during entry into a cryptographic module for accuracy using the manual key entry test specified in Section 4.9.2. During key entry, the entered values may be temporarily displayed to allow visual verification and to improve accuracy. If encrypted cryptographic keys or key components are entered into the cryptographic module, then the plaintext values of the cryptographic keys or key components shall not be displayed.

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2:

Electronically distributed secret and private keys shall be entered and output in encrypted form.

SECURITY LEVELS 3 AND 4

For Security Levels 3 and 4:

- *Manually distributed* secret and private keys shall be entered or output either (1) in encrypted form or (2) using split knowledge procedures (i.e., as two or more plaintext key components).

  When split knowledge procedures are used:

  - ❑ The cryptographic module shall provide the capability to separately authenticate the operator entering or outputting each key component.

  - ❑ The key components shall be directly entered into or output from the cryptographic module (e.g., via a trusted path or directly attached cable) without traveling through any enclosing or intervening systems where the components could be stored, combined, or otherwise processed.

  - ❑ The split knowledge procedure shall ensure that at least two components are required to construct the original key. Documentation shall include proof that if knowledge of n key components is required, then knowledge of any n-1 key components provides no information about the original key other than the length.

- *Electronically-distributed* secret and private keys shall be entered and output in encrypted form.

4.7.5 Key Storage

When contained within a cryptographic module, secret and private keys shall be stored in plaintext form or shall be encrypted using an Approved algorithm. Plaintext keys shall not be accessible from outside the cryptographic module.

All secret and private keys shall be associated with the correct entity (e.g., person, group, or process) to which the keys are assigned.

Documentation shall specify the key storage mechanism(s) employed by the cryptographic module.

4.7.6 Key Destruction

A cryptographic module shall provide the capability to zeroize all plaintext secret and private cryptographic keys and other unprotected CSPs within the module. Zeroization of cryptographic keys and other CSPs is not required if the keys and CSPs are either encrypted (using an Approved algorithm) or otherwise physically or logically protected within an additional embedded validated cryptographic module (validated by the Cryptographic Module Validation Program (CMVP)).

Documentation shall specify the key destruction mechanism(s) employed by the cryptographic module.

4.8 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Cryptographic modules shall meet the following requirements for EMI/EMC. Radios are explicitly excluded from these requirements but shall meet all applicable FCC requirements.

Documentation shall include proof of conformance to EMI/EMC requirements.

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, a cryptographic module shall (at a minimum) conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

SECURITY LEVELS 3 AND 4

For Security Levels 3 and 4, a cryptographic module shall (at a minimum) conform to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).

4.9 Self-Tests

A cryptographic module shall perform self-tests to ensure that the module is functioning properly. Self-tests shall be performed when the cryptographic module is powered up (i.e., Power-Up Tests). Self-tests shall be performed under various conditions, typically when a particular function or operation is performed (i.e., Conditional Tests). Resetting, rebooting, and power recycling are acceptable means for on demand initiation of power-up self-tests. A cryptographic module may optionally perform other self-tests in addition to the tests specified in this standard.

When a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status interface. The cryptographic module shall not perform any cryptographic operations while in the error state and no data shall be output via the data output interface while the error condition exists.

Each possible error condition shall be documented along with the conditions and actions necessary to clear the error and resume normal operation (possibly including maintenance, servicing, or repair of the cryptographic module).

Documentation shall provide a list of all self-tests that the cryptographic module can perform, including both power-up tests and conditional tests.

4.9.1 Power-Up Tests

When powered up, the cryptographic module shall perform all of the following self-tests: cryptographic algorithm test, software/firmware integrity test, critical functions test, and statistical random number generator tests. The tests shall not require operator intervention in order to run. If all of the tests are passed successfully, such an indication shall be output via the "status output" interface. All data output via the output interface shall be inhibited when these tests are performed. The cryptographic module shall provide a means to initiate the tests on demand for periodic testing of the module.

> *Cryptographic algorithm test*. A known-answer test shall be conducted for each Approved cryptographic function (e.g., encryption, decryption, and authentication) that is implemented by the cryptographic module. A known-answer test involves operating the algorithm on data for which the correct output is already known and determining if the calculated output equals the previously generated output (the known answer). Algorithms whose outputs vary for a given set of inputs (e.g., the Digital Signature Algorithm) shall be tested using a known-answer test or shall be tested using a pair-wise consistency test. Message digest algorithms shall have an independent known-answer test or the known-answer test shall be included with the associated cryptographic algorithm test (e.g., the Digital Signature Algorithm).

A cryptographic module may omit the cryptographic algorithm test if the module includes two independent implementations of the same cryptographic algorithm. Outputs shall be continually compared in order to ensure the correct functioning of the cryptographic algorithm. When the outputs of the two implementations are not equal, the cryptographic module shall enter an error state and output an error indicator via the status interface.

Software/firmware integrity test. An error detection code (EDC) or Approved authentication technique (e.g., the computation and verification of an Approved authentication code or digital signature algorithm) shall be applied to all CMVP-validated software and firmware residing in the cryptographic module (e.g., within EEPROM and RAM). The EDC shall be at least 16 bits in length. This error detection code, authentication code, or digital signature shall then be verified when the power-up tests are run.

Critical functions test. All other functions that are critical to the secure operation of the cryptographic module that can be tested as part of the power-up tests shall be tested. Other critical functions that are performed under certain specific conditions shall be tested as part of the conditional tests.

Documentation shall provide a complete specification of all critical functions and the power-up self-tests designed to test those functions.

Statistical random number generator tests. Cryptographic modules that implement a random or pseudorandom number generator shall have the capability to perform statistical tests for randomness. A single bit stream of 20,000 consecutive bits of output from each generator shall be subjected to the all of the following four tests: monobit test, poker test, runs test, and long runs test. For Levels 1 and 2, the tests are not required. For Security Level 3, the tests shall be callable upon demand. For Security Level 4, the tests shall be performed at power-up and shall also be callable upon demand.

The monobit test

1. Count the number of ones in the 20,000 bit stream. Denote this quantity by X.

2. The test is passed if 9,725 < X < 10,275 (Type I Error of .0001).

The poker test

1. Divide the 20,000 bit stream into 5,000 contiguous 4 bit segments. Count and store the number of occurrences of the 16 possible 4 bit values. Denote *f(i)* as the number of each 4 bit value *i* where $0 \leq i \leq 15$.

2. Evaluate the following:

$$X = (16/5000) * \left(\sum_{i=0}^{15} [f(i)]^2 \right) - 5000$$

3. The test is passed if 2.16 < X < 46.17 (Type I Error of .0001).

The runs test

1. A run is defined as a maximal sequence of consecutive bits of either all ones or all zeros that is part of the 20,000 bit sample stream. The incidences of runs (for both consecutive zeros and consecutive ones) of all lengths (≥ 1) in the sample stream should be counted and stored.

2. The test is passed if the runs that occur (of lengths 1 through 6) are each within the corresponding interval specified in the table below. This must hold for both the zeros and

ones (i.e., all 12 counts must lie in the specified interval). For the purposes of this test, runs of greater than 6 are considered to be of length 6.

Length of Run	Required Interval (Type I Error of .0001)
1	2,343 – 2,657
2	1,135 – 1,365
3	542 - 708
4	251 - 373
5	111 - 201
6+	111 - 201

Table 3. *Required intervals for length of runs test*

The long runs test

1. A long run is defined to be a run of length 26 or more (of either zeros or ones) for a Type 1 Error of .0001.

2. On the sample of 20,000 bits, the test is passed if there are no long runs.

4.9.2 Conditional Tests

A cryptographic module shall perform the following tests under the conditions specified for each test: pair-wise consistency test, software/firmware load test, manual key entry test, continuous random number test, and bypass test.

Pair-wise consistency test (for public and private keys). Cryptographic modules that generate public and private keys shall test the keys for pair-wise consistency.

1. If the keys can be used to perform encryption, then the public key shall be applied to a plaintext value. The resulting ciphertext shall be compared to the original plaintext to verify that they differ. If the two values are equal, then the cryptographic module shall enter an error state and output an error indicator via the status interface. If the two values differ, then the private key shall be applied to the ciphertext and the result shall be compared to the original plaintext. If the two values are not equal, then the test shall fail.

2. If the keys are to be used to perform key agreement then the cryptographic module shall create a second, compatible key pair. It shall then perform both sides of the key agreement algorithm and shall verify that the resulting secret keys are the same. If the secret keys are not the same, the test shall fail.

3. If the keys are to be used only for the calculation and verification of digital signatures, then the consistency of the keys shall be tested by the calculation and verification of a signature. If the signature cannot be verified, the test shall fail.

Software/firmware load test. A cryptographic mechanism using an Approved authentication technique (e.g., an authentication code, digital signature algorithm, or HMAC) shall be applied to all CMVP-validated software and firmware that can be externally loaded into a cryptographic module. This test shall verify the authentication code or digital signature when the software or firmware is externally loaded into the cryptographic module.

Manual key entry test. When cryptographic keys or key components are manually entered into a cryptographic module, the keys shall have an EDC or shall use duplicate entries in order to verify the accuracy of the entered keys. The EDC shall be at least 16 bits in length. A cryptographic module shall verify the error detection code or duplicate entries and provide an indication of the success or failure of the entry process.

Continuous random number generator test. Cryptographic modules that implement a random or pseudorandom number generator (Approved and non-Approved) shall test the generator for failure to a constant value. If the generator produces blocks of n bits (where n > 15), the first block generated after power-up shall not be used, but shall be saved for comparison with the next block to be generated. Upon each subsequent generation, the newly generated block is compared with the previously generated block. The test fails if the two compared blocks are equal. If each call to the generator produces fewer than 16 bits, then the first n bits generated after power-up (for some n > 15) shall not be used, but shall be saved for comparison with the next n generated bits. Each subsequent generation of n bits shall be compared with the previously generated n bits. The test fails if two compared n-bit sequences are equal.

Bypass test. Cryptographic modules that implement a bypass service shall test for the correct operation of the cryptographic service when a switch takes place between an exclusive bypass service and an exclusive cryptographic service. If the cryptographic module is designed to automatically alternate between a bypass service and a cryptographic service, then the module shall test for the correct operation of the cryptographic service when the mechanism governing the switching procedure is modified (e.g., IP address source/destination table). No single point of failure shall result in the unintentional output of plaintext. The intent of these bypass service requirements is to ensure that a failure of equipment will not result in the unintentional output of plaintext. Documentation shall provide a complete specification of the logic or mechanism used to govern the switching procedure and, in addition, the conditional self-test designed to test for the correct operation of the cryptographic service.

4.10 Design Assurance

Design assurance requirements are specified for configuration management, delivery and operation, development, guidance documents, and functional testing and test coverage.

4.10.1 Configuration Management

Configuration Management (CM) is concerned with assurances that the functional requirements and specifications are realized in the implementation of the cryptographic module.

SECURITY LEVEL 1

The cryptographic module and associated documentation shall meet the following requirements:

- Each configuration item (e.g., cryptographic module, user guidance, security policy, hardware platform, and operating system) shall be assigned and labeled with a unique identification number.

- The identification number shall be unique for each version.

SECURITY LEVELS 2, 3, AND 4

In addition to the requirements for Security Level 1, the following requirements shall apply:

- A configuration management system shall be implemented.

- The configuration management documentation shall describe the method used to uniquely identify the configuration items.

- Documentation shall uniquely identify all configuration items that comprise the cryptographic module and associated documentation.

4.10.2 Delivery and Operation

Delivery and operation specifies the security requirements for correct delivery, installation, and start-up of a cryptographic module.

SECURITY LEVEL 1

- Documentation shall specify the procedures for secure installation, and start-up of the cryptographic module.

SECURITY LEVELS 2, 3, AND 4

- In addition to the requirements for Security Level 1, documentation shall specify all procedures necessary to maintain security when distributing versions of the cryptographic module. This shall include how the integrity of the hardware and software are protected from modification and substitution.

4.10.3 Development

Development encompasses requirements for representing the cryptographic module security functionality at various levels of abstraction from the functional interface to the implementation representation.

SECURITY LEVEL 1

Documentation for Security Level 1 shall include:

- a detailed explanation of the correspondence between the design of the hardware, software, and firmware and the cryptographic module security policy (see Appendix C), and

- source code listings for software and firmware, or schematics for hardware contained within the cryptographic module. If a Hardware Description Language (HDL) is employed in the design, the listing shall be included. The relations of the functions, components, and procedures to the design specifications or schematics of the hardware, software, and firmware shall be clearly depicted.

SECURITY LEVEL 2

The functional specification is a high-level description of the interface visible to the user and the behavior of the cryptographic module. In addition to the requirements for Security Level 1, the following requirements shall be satisfied for Security Level 2:

- The functional specification shall be provided that informally describes the cryptographic module and its external interfaces.

- The functional specification shall be internally consistent and completely represent the cryptographic module.

- The functional specification shall describe the purpose and method of use of all external cryptographic module interfaces, providing details of effects, exceptions, and error messages.

SECURITY LEVEL 3

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

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

- All hardware within the cryptographic module shall be implemented using an HDL (or equivalent).

SECURITY LEVEL 4

In addition to the applicable requirements for Security Levels 1, 2, and 3, the following documentation requirements shall apply for Security Level 4:

- Documentation shall include rationale that the cryptographic module is completely represented by the functional specification.

- Documentation shall include 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.

- Documentation shall include a rationale that demonstrates that the formal model is consistent and complete with respect to the cryptographic module security policy.

- Documentation shall include a detailed explanation (informal proof) of the correspondence between the formal model and functional specification.

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

- Documentation shall include a detailed explanation (informal proof) of the correspondence between the design (as reflected by the precondition and postcondition annotations) and the functional specification.

RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES FOR ALL LEVELS

- All software components should be implemented using the recommended development practices listed in Appendix B. These practices will facilitate the analysis of the components for conformance to the requirements of this standard and will reduce the chances of design errors.

4.10.4 Guidance Documents

Crypto officer guidance is concerned with the correct configuration, maintenance, and administration of the cryptographic module. User guidance describes the security functions of the cryptographic module along with instructions, guidelines, and warnings for its secure use.

SECURITY LEVELS 1, 2, 3, AND 4

The crypto officer guidance documentation shall include:

- a description of the administrative functions, security events, security parameters (and their values, as appropriate), and interfaces available to the crypto officer,

- procedures on how to administer the cryptographic module in a secure manner,

- assumptions regarding user behavior that is relevant to the secure operation of the cryptographic module, and

- if applicable, a description of all security requirements for the IT environment that are relevant to the crypto officer.

The user guidance documentation shall include:

- a description of the functions and interfaces available to the users of the cryptographic module,

- a description of the user-accessible security functions provided by the cryptographic module,

- all user responsibilities necessary for the secure operation of the cryptographic module, and

- if applicable, a description of all security requirements for the IT environment that are relevant to the user.

4.10.5 Functional Testing and Test Coverage

Functional testing is performed to establish that the cryptographic module exhibits the properties necessary to satisfy the functional requirements. Test coverage is concerned with the extent to which the cryptographic module has been tested, and whether or not the testing is sufficiently extensive to demonstrate that the module operates as specified.

SECURITY LEVEL 1

There are no security requirements for Security Level 1.

SECURITY LEVEL 2

- Test documentation shall include tests, test plans, test procedure descriptions, expected test results, and actual test results.

- Documentation shall show that the cryptographic module was tested against the functional specification.

SECURITY LEVELS 3 AND 4

In addition to the requirements for Security Levels 1 and 2:

- The analysis of test coverage shall demonstrate that the cryptographic module was tested against the functional specification in a systematic and complete manner.

4. 11 Mitigation of Other Attacks

Certain types of cryptographic modules may be susceptible to attacks for which testable security requirements were not available at the time this standard was issued (e.g., power analysis, timing analysis, and fault induction) or the attacks were outside of the scope of the standard (e.g., TEMPEST). Susceptibility to these attacks depends on module type, implementation, and implementation environment. These attacks are of particular concern for cryptographic modules implemented in hostile environments or where the attackers may be the users of the module. These types of attacks generally rely on the analysis of information obtained from sources physically external to the module. In all cases, the attacks attempt to determine some knowledge about the cryptographic keys and CSPs contained in the module. Brief summaries of currently known attacks are provided below.

Power Analysis: Attacks based on the analysis of power consumption can be divided into two general categories, Simple Power Analysis (SPA) and Differential Power Analysis (DPA). SPA involves a direct (primarily visual) analysis of electrical power consumption patterns and timings derived from the execution of individual instructions carried out by a cryptographic module during a cryptographic process. The patterns are 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 values of cryptographic keys. DPA has the same goals but utilizes advanced statistical methods and/or error correction techniques to analyze the variations of the electrical power consumption of a cryptographic module. Cryptographic modules that utilize external power (direct current) sources appear to be at greatest risk. At the time this standard was issued, there were no specific methods to guarantee complete mitigation of Power Analysis attacks. However, there are several methods that may reduce the overall risk of this attack. These include the use of capacitors to level the power consumption, use of internal power sources, and manipulation of the individual operations of the algorithms or processes to level the rate of power consumption during cryptographic processing.

Timing Analysis: Timing Analysis attacks rely on precisely measuring the time required by a cryptographic module to perform specific mathematical operations associated with a cryptographic algorithm or process. The timing information collected is analyzed to determine the relationship between the inputs to the module and the cryptographic keys used by the underlying algorithms or processes. The analysis of the relationship may be used to exploit the timing measurements to reveal the cryptographic key or critical security parameters. Timing Analysis attacks assume that the attacker has knowledge of the design of the cryptographic module. Manipulation of the individual operations of the algorithms or processes to reduce timing fluctuations during processing is one method to reduce the risk of this attack.

Fault Induction: Fault Induction attacks utilize external forces such as microwaves, temperature extremes, and voltage manipulation to cause processing errors within the cryptographic module. An analysis of these errors and their patterns can be used in an attempt to reverse engineer the cryptographic module, revealing certain features and implementations of cryptographic algorithms and subsequently revealing the values of cryptographic keys. Cryptographic modules with limited physical security appear to be at greatest risk. Proper selection of physical security features may be used to reduce the risk of this attack.

TEMPEST: TEMPEST attacks involve the remote or external detection and collection of the electromagnetic signals emitted from a cryptographic module and associated equipment during processing. This attack can be used to obtain actual keystroke information, messages displayed on a video screen, and other forms of critical security information (e.g., cryptographic keys). Special shielding of all components, including network cabling, is the mechanism used to reduce the risk of this attack. Shielding reduces and, in some cases, prevents the emission of electromagnetic signals.

If a cryptographic module is designed to mitigate one or more specific attacks, then the module’s security policy shall specify the security mechanisms employed by the cryptographic module to mitigate the attack(s). The existence of these mechanisms and their proper functioning will be validated as requirements and associated tests are developed.

APPENDIX A: SUMMARY OF DOCUMENTATION REQUIREMENTS

The following check list summarizes the documentation requirements of this standard. The CMVP may require additional documentation. All documentation shall be provided to the validation facility by the vendor of a cryptographic module. Requirements for user documentation are beyond the scope of this standard. However, copies of the user and installation manuals shall also be provided to the validation facility.

CRYPTOGRAPHIC MODULE SPECIFICATION

- Specification of the hardware, software, and firmware components of a cryptographic module, the cryptographic boundary surrounding these components, and the physical configuration of the module. *(Security Levels 1, 2, 3, and 4)*

- Specification of any hardware, software, or firmware components of a cryptographic module that are excluded from the security requirements of this standard and an explanation of the rationale for the exclusion. *(Security Levels 1, 2, 3, and 4)*

- Specification of the interfaces of a cryptographic module, including any physical or logical ports, physical covers or doors, manual or logical controls, physical or logical status indicators, and their physical, logical, or electrical characteristics. *(Security Levels 1, 2, 3, and 4)*

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

- Block diagram depicting all of the major hardware components of the cryptographic module and their interconnections, including any microprocessors, input/output buffers, plaintext and ciphertext buffers, control buffers, key storage, working memory, and program memory. *(Security Levels 1, 2, 3, and 4)*

- Detailed specification of the design of the hardware, software, and firmware within the cryptographic module. *(Security Levels 1, 2, 3, and 4)*

- Specification of the cryptographic module security policy (i.e., the security rules under which a module must operate, including the rules derived from the requirements of this standard and the rules derived from any additional requirements). *(Security Levels 1, 2, 3, and 4)*

CRYPTOGRAPHIC MODULE INTERFACES

- Specification of the defined input and output data paths. *(Security Levels 1, 2, 3, and 4)*

ROLES, SERVICES, AND AUTHENTICATION

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

- Specification of each of the authorized services, operations, and functions that can be performed with the cryptographic module. For each service, the service inputs, corresponding service outputs, and the authorized role (or set of roles) in which the service can be performed, shall be specified. *(Security Levels 1, 2, 3, and 4)*

- Description of the authentication mechanism(s) employed by the cryptographic module and the corresponding strength of the mechanism(s). *(Security Levels 2, 3, and 4)*

FINITE STATE MACHINE MODEL

- Specification and description of all states of the cryptographic module and of all the corresponding state transitions. The descriptions of the state transitions shall include the internal cryptographic module conditions, data inputs, and control inputs that cause transitions from one state to another, and shall include data outputs and status outputs resulting from transitions from one state to another. *(Security Levels 1, 2, 3, and 4)*

PHYSICAL SECURITY

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

- Specification of the authorized physical maintenance procedures defined for the cryptographic module and how cryptographic keys and CSPs are to be zeroized. *(Security Levels 1, 2, 3, and 4)*

- Specification and description of the environmental failure protection features employed within a cryptographic module, or a description of the environmental failure tests performed and the results of those tests. *(Security Level 4)*

OPERATING SYSTEM SECURITY

- Specification of the operating system employed by the cryptographic module along with its evaluation assurance level. *(Security Levels 2, 3, and 4)*

CRYPTOGRAPHIC KEY MANAGEMENT

- Specification of the type of RNG/PRNG employed by the cryptographic module. *(Security Levels 1, 2, 3, and 4)*

- Specification of the Approved key generation algorithms that are implemented by the cryptographic module. *(Security Levels 1, 2, 3, and 4)*

- Specification of the key exchange/agreement techniques that are implemented by the cryptographic module. *(Security Levels 1, 2, 3, and 4)*

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

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

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

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

ELECTROMAGNETIC INTERFERENCE/ELECTROMAGNETIC COMPATIBILITY

- Proof of conformance to EMI/EMC requirements. *(Security Levels 1, 2, 3, and 4)*

SELF-TESTS

- Specification of each possible error condition, including the conditions and actions necessary to clear the error and resume normal operation (possibly including maintenance, servicing, or repair of the cryptographic module). *(Security Levels 1, 2, 3, and 4)*

- A list of all self-tests that the cryptographic module can perform, including both power-up tests and conditional tests. *(Security Levels 1, 2, 3, and 4)*

- Specification of all critical functions and the power-up self-tests designed to test those functions. *(Security Levels 1, 2, 3, and 4)*

- If a bypass service is provided, specification of the logic or mechanism used to govern the switching procedure and the conditional self-test for the correct operation of the cryptographic service. *(Security Levels 1, 2, 3, and 4)*

DESIGN ASSURANCE

- Specification that each configuration item (and each version of the item) is uniquely identified. *(Security Levels 1, 2, 3, and 4)*

- Specification of the method used to uniquely identify the configuration items. *(Security Levels 2, 3, and 4)*

- Unique identification of all configuration items that comprise the cryptographic module and associated documentation. *(Security Levels 2, 3, and 4)*

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

- Specification of procedures for maintaining security when distributing versions of the cryptographic module. *(Security Level 2, 3, and 4)*

- Detailed explanation of the correspondence between the design of the hardware, software, and firmware and the cryptographic module security policy (i.e., the rules of operation). *(Security Levels 1, 2, 3, and 4)*

- Source code listings for all software and firmware, or schematics for hardware contained within the cryptographic module. The relations of the functions, components, and procedures to the design specifications or schematics of the hardware, software, and firmware shall be clearly depicted. *(Security Levels 1, 2, 3, and 4)*

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

- A description of the purpose and method of use of all external interfaces, providing details of effects, exceptions, and error messages. *(Security Levels 2, 3, and 4)*

- High-level language listings of all software and firmware within the cryptographic module. (Low-level listings allowed for all performance-critical software or if a high-level language is not available.) *(Security Levels 3 and 4)*

- HDL listings (or equivalent) of all hardware within the cryptographic module. *(Security Levels 3 and 4)*

- Rationale that the functional specification for the cryptographic module is completely represented. *(Security Level 4)*

- 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)*

- Rationale that demonstrates that the formal model is consistent and complete with respect to the cryptographic module security policy. *(Security Level 4)*

- Detailed explanation (informal proof) of the correspondence between the formal model and the functional specifications. *(Security Level 4)*

- Annotations in the source code listing for each hardware and software component, clearly specifying (1) the preconditions required upon entry into the module, function or procedure in order to execute correctly and (2) the postconditions expected to be true when execution of the module, function, or procedure is complete. *(Security Level 4)*

- Detailed explanation (informal proof) of the correspondence between the design (as reflected by the pre- and postcondition annotations) and the functional specifications. *(Security Level 4)*

- For crypto officer guidance:

  - ❑ A description of administrative functions, security events, security parameters (and their values, as appropriate), and interfaces available to the crypto officer of the cryptographic module. *(Security Levels 1, 2, 3, and 4)*

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

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

  - ❑ If applicable, a description of all security requirements for the IT environment that are relevant to the crypto officer. *(Security Levels 1, 2, 3, and 4)*

- For non-administrative user guidance:

  - ❑ A description of the functions and interfaces available to non-administrative users of the cryptographic module. *(Security Levels 1, 2, 3, and 4)*

  - ❑ A description of user-accessible security functions provided by the cryptographic module. *(Security Levels 1, 2, 3, and 4)*

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

  - ❑ If applicable, a description of all security requirements for the IT environment that are relevant to the user. *(Security Levels 1, 2, 3, and 4)*

- Description of tests, test plans, test procedures, expected test results, and actual test results. *(Security Levels 2, 3, and 4)*

- Documentation that shows the cryptographic module was tested against the functional specifications. *(Security Level 2, 3, and 4)*

- An analysis of test coverage that demonstrates the cryptographic module was tested against the functional specifications in a systematic and complete manner. *(Security Levels 3 and 4)*

MITIGATION OF OTHER ATTACKS

- Specification of the security mechanisms employed in the cryptographic module to mitigate attacks for which testable requirements are not currently available. *(Security Levels 1, 2, 3, and 4)*

SECURITY POLICY

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

APPENDIX B: RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES

This Appendix is provided for informational purposes only and is not a part of this standard.

Life-cycle software engineering recommendations (dealing with specification, construction, verification, testing, maintenance, and documentation) should be followed. Software engineering practices may include such things as 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 programs and to reduce chances of programming errors. Deviations from these practices may be appropriate in some instances.

MODULAR DESIGN

- A modular design using an object-oriented paradigm is recommended, especially for moderate to large-scale software development efforts. Each software module or object should have well-defined and readily understood interfaces.

- Software modules, consisting of data plus one or more associated procedures, should be constructed according to the principle of encapsulation/information-hiding. If available, a strongly-typed, object-oriented high-level language that supports the construction of software modules should be used.

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

SOFTWARE MODULE/PROCEDURE INTERFACES

- Entries to a software module 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 error exits and one for normal 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 language).

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 program 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.

IN-LINE DOCUMENTATION

- Each software module, procedure, and major programming construct should be documented as to the specific function(s) it performs along with a (formal or informal) specification of preconditions and postconditions.

- 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 that identifies the role it plays along with its range of allowable values. If the range is unrestricted, this should be noted.

- If concurrency is employed, the documentation should explicitly state 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. Deviations from these practices may be appropriate in some instances.

- 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 should contain comments describing register use in the unit.

APPENDIX C: CRYPTOGRAPHIC MODULE SECURITY POLICY

The following paragraphs provide a general discussion of the security policy that shall be included in the documentation provided by the vendor.

C.1 Definition of Cryptographic Module Security Policy

A cryptographic module security policy shall consist of:

- a precise specification of the security rules under which a cryptographic module shall operate, including the security rules derived from the requirements of this standard and the additional security rules imposed by the vendor.

The specification shall be complete and sufficiently detailed to provide answers to the following questions:

- What access does operator X, performing service Y while in role Z, have to data item W?" for every role, service, and security-relevant data item contained in the cryptographic module?

- What physical features are implemented to protect the cryptographic module and what actions are required to ensure that the physical security is maintained?

- What features are implemented in the cryptographic module that are intended to mitigate against attacks for which testable requirements are not defined in the Standard?

C.2 Purpose of Cryptographic Module Security Policy

There are two major reasons for developing and following a precise cryptographic module security policy:

- To provide a precise specification of the cryptographic security to allow individuals and organizations (e.g., validators) to determine whether the cryptographic module, as implemented, does obey (satisfy) a stated security policy.

- To describe to the cryptographic module user (organization or individual operator) the capabilities, protections, and access rights provided by the cryptographic module, thereby allowing an assessment of whether the cryptographic module will adequately serve the user's security requirements.

C.3 Specification of a Cryptographic Module Security Policy

A cryptographic module security policy shall be expressed in terms of roles, services, and cryptographic keys and other critical security parameters (CSPs). It shall specify, at a minimum,

- an identification and authentication (I&A) policy,

- an access control policy, and

- a physical security policy.

C.3.1 Identification and Authentication Policy

Each cryptographic module shall have identification and authentication components within its security policy. The security policy shall specify

- all roles (e.g., user, crypto officer, and maintenance) and associated type of authentication (e.g., identity-based or role-based) and

- the identification information required of each role (e.g., password or finger print) and the corresponding strength of the identification mechanism.

C.3.2 Access Control Policy

The access control policy enforced by the cryptographic module shall be sufficiently precise and of sufficient detail to allow the operator and testers to know what CSPs the operator has access to while performing a service, and the modes of access the operator has to these parameters.

C.3.2.1 Elements of the Access Control Policy

In specifying an access control policy, the following elements shall be defined:

- all roles,

- all services,

- all CSPs, e.g.,

    - ❑ cryptographic keys - both plaintext and encrypted keys and

    - ❑ other CSPs (e.g., authentication data (passwords)), and

- other protected information (e.g., audited events and audit data)

C.3.2.2 Access Control Constraints

- For each role, the vendor shall define (specify) what services an operator may perform while in that role.

- For each service within a role, the vendor shall specify the type of access to all keys and CSPs identified in part 3 of section C.3.3.1 above.

The vendor may make a general statement such as "For all CSPs not included within the list for a given service within a given role, the operator performing that service in that role has no access."

C.3.3 Physical Security Policy

The physical security policy shall specify

- the physical security features that are implemented in the cryptographic module (e.g., tamper-evident seals, zeroization triggers, and alarms) and

- the actions that are required by the operator(s) to ensure that physical security is maintained (e.g., must periodically inspect the seals and test zeroization triggers).

C.3.4 Mitigation of Other Attacks Policy

The security policy shall specify security mechanisms employed by the cryptographic module to mitigate attacks for which testable requirements are not stated in the Standard.

C.3.5 Security Policy Check Lists

The following types of tables may be used as guides in determining whether or not the security policy is complete and contains the appropriate details:

Identification Mechanism	**Strength of Mechanism**
…	**…**
…	**…**

Table C1. *Identification Mechanism and Corresponding Strengths*

Role	**Type of Authentication**	**Type of Identification**
…	**…**	**…** **…**
…	**…**	**…** **…**

Table C2. *Roles and Required Authentication and Identification*

Role	**Authorized Services**
…	**…** **…**
…	**…** **…**

Table C3. *Services Within Roles*

Service	**Accessible CSPs**	**Type of Access (e.g., RWE)**
…	… …	… …
…	… …	… …

Table C4. *CSP Access Rights Within Services*

Physical Security Feature	**Frequency of Inspection/Test**	**Inspection/Test Guidance Details**
…	… …	… …
…	… …	… …

Table C5. *Inspection/Testing of Physical Security Features*

Other Attacks	**Mitigation Mechanism**	**Specific Limitations**
…	… …	… …
…	… …	… …

Table C6. *Mitigation of Other Attacks*

APPENDIX D: SELECTED BIBLIOGRAPHY

American Bankers Association, *American National Standard for Financial Institution Key Management (Wholesale),* ANSI X9.17, Washington, D.C., 1995.

American Bankers Association, *Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* ANSI X9.31-1998, Washington, D.C., 1998.

American Bankers Association, *Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures, ANSI TG-19, Washington, D.C., 1999.*

American Bankers Association, *Triple Data Encryption Algorithm Modes of Operation*, ANSI X9.52-1998, Washington, D.C., 1998.

American Bankers Association, *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Diffie-Hellman and MQV Algorithms*, Working Draft American National Standard X9.42-1998, May 21, 1998.

American Bankers Association, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm*, American National Standard X9.62-1998, Washington, D.C., 1998.

American Bankers Association, *Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Transport Protocols*, Working Draft American National Standard X9.63, October 5, 1997.

Canadian System Security Centre, Communications Security Establishment, Government of Canada, *Canadian Trusted Computer Product Evaluation Criteria*, Version 3.0, January 1993.

Common Criteria Implementation Board (CCIB), *International Standard (IS) 15408*, *Common Criteria for Information Technology Security Evaluation*, Version 2, May 1998, ISO/IEC JTC 1 and Common Criteria Implementation Board.

Computer Security Act of 1987, 40 U.S. Code 759, (Public Law 100-235), January 8, 1988.

Department of Defense, *Department of Defense Trusted Computer System Evaluation Criteria*, DOD 5200.28-STD, December 1985.

Information Technology Management Reform Act of 1996, U.S. Code, (Public Law 104-106), 10 February *1996.*

Information Technology Security Evaluation Criteria (ITSEC), Harmonized Criteria of France – Germany - the Netherlands - the United Kingdom, Version 1.1, January 1991.

Keller, Sharon and Miles Smid, *Modes of Operation Validation System (MOVS): Requirements and Procedures*, Special Publication 800-17, Gaithersburg, MD, National Institute of Standards and Technology, February 1998.

National Institute of Standards and Technology, *Computer Data Authentication*, Federal Information Processing Standards Publication 113, 30 May 1985.

National Institute of Standards and Technology, *Data Encryption Standard*, Federal Information Processing Standards Publication 46-3, October 25, 1999.

National Institute of Standards and Technology, *DES Modes of Operation*, Federal Information Processing Standards Publication 81, December 2, 1980.

National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2, **MONTH DAY**, 1999.

National Institute of Standards and Technology, *Implementation Guidance for FIPS 140-2*, available at web site: csrc.nist.gov/cryptval.

National Institute of Standards and Technology, *Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules*, available at web site: csrc.nist.gov/cryptval.

National Institute of Standards and Technology, *Digital Signature Standard Validation System (DSSVS) User's Guide*, June 20, 1997.

National Institute of Standards and Technology, *Entity Authentication Using Public Key Cryptography*, Federal Information Processing Standards Publication 196, February 18, 1997.

National Institute of Standards and Technology, *Guideline for the Use of Advanced Authentication Technology Alternatives*, Federal Information Processing Standards Publication 190, September 28, 1994.

National Institute of Standards and Technology, *Key Management using ANSI X9.17*, Federal Information Processing Standards Publication 171, April 27, 1992.

National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-1, April 17, 1995.

National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, Federal Information Processing Standards Publication 140-1, January 11, 1994.

National Security Agency, *Controlled Access Protection Profile, Versions 1.c.* January 29, 1999.

Office of Management and Budget, *Security of Federal Automated Information Resources*, Appendix III to OMB Circular No. A-130, February 8, 1996.