U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards and Technology

FIPS

FIPS PUB 140-1

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS PUB 140—1982 April 14)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

1994 January 11

FIPS PUB 140-1

FIPS PUB 140-1

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION
(Supersedes FIPS PUB 140—1982 April 14)

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

CATEGORY: COMPUTER SECURITY **SUBCATEGORY: CRYPTOGRAPHY**

Computer Systems Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899

Issued January 11, 1994

U.S. Department of Commerce
Ronald H. Brown, Secretary

Technology Administration
Mary L. Good, Under Secretary for Technology

National Institute of Standards
and Technology
Arati Prabhakar, Director

Foreword

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official publication relating to standards and guidelines adopted and promulgated under the provisions of Section 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by 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 Computer Systems 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, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899.

James H. Burrows, Director
Computer Systems 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 telecommunications 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 basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/electromagnetic compatibility (EMI/EMC), and self-testing. This revision supersedes FIPS 140 in its entirety.

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

National Institute of Standards and Technology
FIPS PUB 140-1
41 pages (Jan. 11, 1994)
CODEN: FIPPAT

U.S. Government Printing Office
Washington: 1994

For sale by the National Technical Information Service
U.S. Department of Commerce
Springfield, VA 22161

Federal Information Processing Standards Publication 140-1

1994 January 11

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 111(d) of the Federal Property and Administrative Services Act of 1949 as amended by the Computer Security Act of 1987, Public Law 100-235.

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

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

3. **Explanation.** This standard specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting unclassified information within computer and telecommunication systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/electromagnetic compatibility (EMI/EMC), and self-testing. This standard supersedes FIPS 140, General Security Requirements for Equipment Using the Data Encryption Standard, in its entirety.

4. **Approving Authority.** Secretary of Commerce.

5. **Maintenance Agency.** Department of Commerce, National Institute of Standards and Technology, Computer Systems Laboratory.

6. **Cross Index.**
   a. FIPS PUB 46-2, Data Encryption Standard.
   b. FIPS PUB 48, Guidelines on Evaluation of Techniques for Automated Personal Identification.
   c. FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard.
   d. FIPS PUB 81, DES Modes of Operation.
   e. FIPS PUB 83, Guideline of User Authentication Techniques for Computer Network Access Control.
   f. FIPS PUB 112, Password Usage.
   g. FIPS PUB 113, Computer Data Authentication.
   h. FIPS PUB 171, Key Management Using ANSI X9.17.
   i. FIPS PUB 180, Secure Hash Standard.
   j. Special Publication 500-157, Smart Card Technology: New Methods for Computer Access Control.
   k. Special Publication 800-2, Public Key Cryptography.
   l. Federal Information Resources Management Regulations (FIRMR) subpart 201.20.303, Standards, and subpart 201.39.1002, Federal Standards.

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 unclassified information within computer and telecommunication systems (including voice systems) that are not subject to Section 2315 of Title 10, U.S. Code, or Section 3502(2) of Title 44, U.S. Code. This standard shall be used in designing, acquiring and implementing cryptographic-based security systems within computer and telecommunication systems (including voice systems), operated by a Federal agency or by a contractor of a Federal agency or other organization that processes information (using a computer or telecommunications system) on behalf of the Federal Government to accomplish a Federal function. Federal agencies which 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. Non-Federal government organizations are encouraged to adopt and use this standard when it provides the desired security for protecting valuable or sensitive information.

8. Applications. Cryptographic-based security systems may be utilized in various computer and telecommunication (including voice) applications (e.g., data storage, access control and personal identification, radio, facsimile, video) and in various environments (e.g., centralized computer facilities, office environments, hostile environments). The cryptographic services (e.g., encryption, authentication, digital signature, key management) provided by a cryptographic module will be based on many factors which 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 which 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. System characteristics not related to security (e.g., telecommunications interoperability) are beyond the scope of this standard.

9. Specifications. Federal Information Processing Standard (FIPS) 140-1, *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 by NIST, or that comply with the requirements of the FIPS 140-1 implementation and FIPS 140 acquisition schedules in Section 14 of the announcement of this standard, will be considered as complying with this standard. Information about the FIPS 140-1 validation program can be obtained from the National Institute of Standards and Technology, Computer Systems Laboratory, Gaithersburg, MD 20899.

11. FIPS Approved Security Methods. Cryptographic modules that comply with this standard shall employ cryptographic algorithms, cryptographic key generation algorithms and key distribution techniques, and authentication techniques that have been FIPS approved for protecting Federal Government unclassified information. FIPS approved cryptographic algorithms, cryptographic key generation algorithms and key distribution techniques, and authentication 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 a NIST accredited evaluation authority and against a FIPS approved evaluation criteria.

Information about approved cryptographic methods and approved operating system evaluation authorities and criteria can be obtained from NIST.

12. Interpretation. Resolution of questions regarding this standard will be provided by NIST. Questions concerning the content and specifications should be addressed to: Director, Computer Systems Laboratory, ATTN: FIPS 140-1 Interpretation, National Institute of Standards and Technology, Gaithersburg, MD 20899.

13. Export Control. Certain cryptographic devices and technical data regarding them are deemed to be defense articles (i.e., inherently military in character) and are subject to Federal government export controls as specified in Title 22, Code of Federal Regulations, Parts 120-128. Some exports of cryptographic modules conforming to this standard and technical data regarding them must comply with these Federal regulations and be licensed by the U.S. Department of State. Other exports of cryptographic modules conforming to this standard and technical data regarding them fall under the licensing authority of the Bureau of Export Administration of the U.S. Department of Commerce. The Department of Commerce is responsible for licensing cryptographic devices used for authentication, access control, proprietary software, automatic teller machines (ATMs), and certain devices used in other equipment and software. For advice concerning which agency has licensing authority for a particular cryptographic device, please contact the respective agencies.

14. Implementation Schedule. Figure 1 summarizes the implementation schedule for FIPS 140-1. The effective date of this standard is June 30, 1994.

From approval of FIPS 140-1 to its effective date, agencies may purchase equipment with FIPS 140-1 cryptographic modules that have been affirmed in writing from the manufacturer as complying with this standard. From June 30, 1994 until six months after the establishment of the FIPS 140-1 validation program by NIST, agencies that have determined a need for equipment with cryptographic modules shall purchase equipment with FIPS 140-1 cryptographic modules that have been affirmed in writing by the manufacturer as complying with this standard. A copy of the written affirmation shall have been sent to the Director, Computer Systems Laboratory, National Institute of Standards and Technology, Gaithersburg, MD 20899.

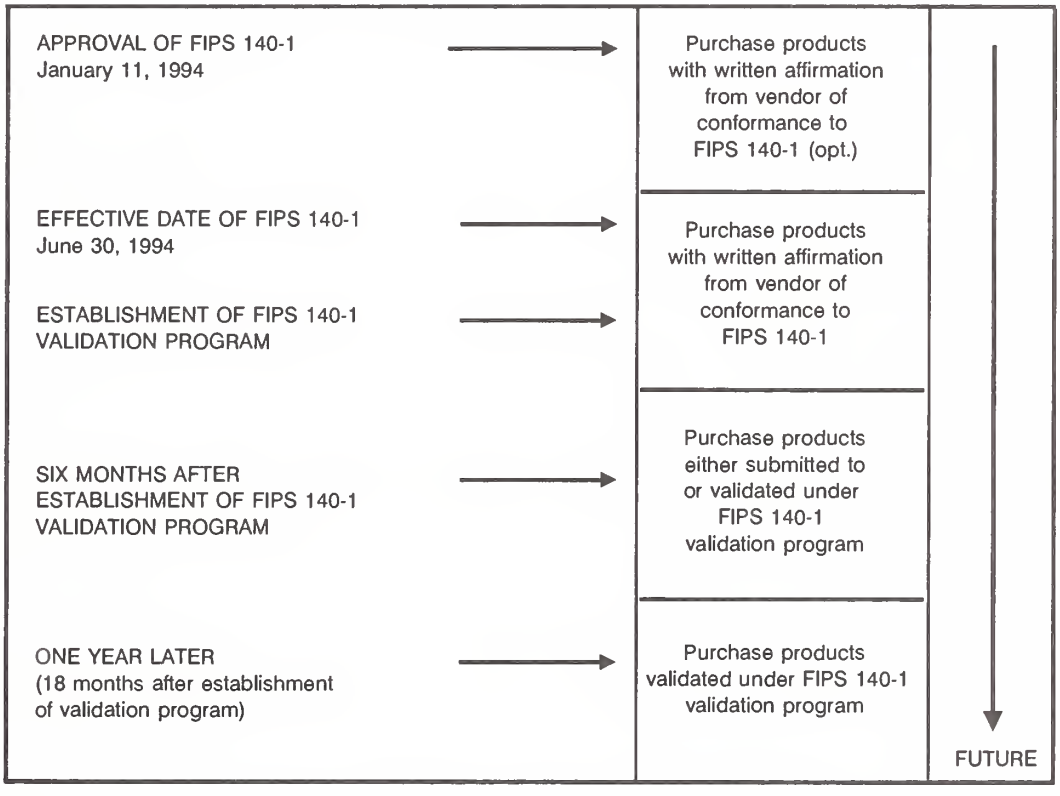

Figure 1. *FIPS 140-1 Implementation Schedule.*

For a one year period following the six months after the establishment of the FIPS 140-1 validation program, agencies shall purchase either equipment with validated FIPS 140-1 cryptographic modules, or equipment whose cryptographic modules have been submitted for FIPS 140-1 validation. After this period, only FIPS 140-1 validated cryptographic modules will be considered as meeting the provisions of this standard.

Figure 2 summarizes the schedule for acquisition of FIPS 140 compliant equipment. For up to three years following June 30, 1994, equipment with cryptographic modules complying to FIPS 140, General Security Requirements for Equipment Using the Data Encryption Standard (formerly Federal Standard 1027), may be purchased in lieu of equipment with modules that comply with this standard. These modules either shall have been endorsed by the National Security Agency (NSA) as complying to Federal Standard 1027, or shall be affirmed in writing by the manufacturer as complying to FIPS 140. NSA endorsed modules shall have been endorsed prior to January 11, 1994. A list of endorsed products (NSA Endorsed Data Encryption Standard (DES) Products List) is available from the NSA. For modules affirmed by the manufacturer as complying with FIPS 140, a copy of the written affirmation shall have been sent by the manufacturer to the Director of the Computer Systems Laboratory at NIST prior to June 30, 1994. A list of these modules is available from NIST.

Equipment purchased under the above conditions may continue to be used for the lifetime of the equipment without the need for further affirmation or validation for conformance to this standard.

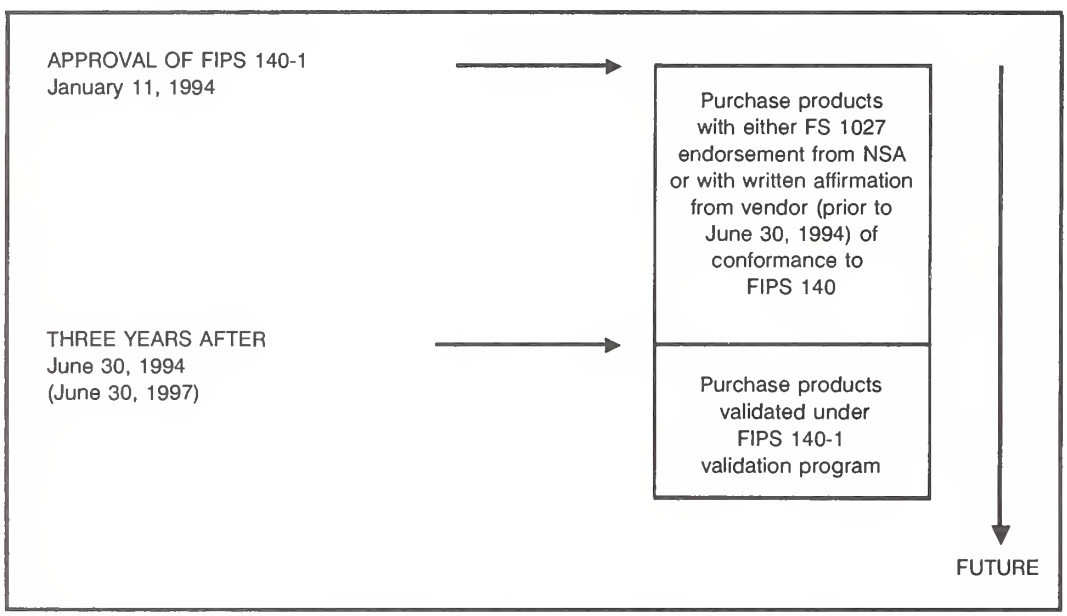

Figure 2. *FIPS 140 Schedule for Acquisition of Validated Products.*

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 unclassified government or commercial data (e.g., hackers, organized crime, 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 5 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 may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency 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:

a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system, or

b. cause a major adverse financial impact on the operator which 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 that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which 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 Decisions, Technology Building, Room B154; Gaithersburg, MD 20899.

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 Governmental 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 140-1 (FIPSPUB140-1), and title. When microfiche is desired, this should be specified. Payment may be made by check, money order, credit card, or deposit account.

Federal Information Processing Standards Publication 140-1

1994 January 11

Specifications for the

SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

1. OVERVIEW

This standard specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting unclassified information in computer and telecommunication systems (including voice systems) that are not subject to Section 2315 of Title 10, U.S. Code, or Section 3502(2) of Title 44, U.S. Code. Cryptographic modules conforming to this standard shall meet the applicable security requirements described herein.

This standard 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). 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.

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 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 which the module is to provide. The responsible authority in each agency or department shall assure that the agency or department's computer or telecommunication systems which utilize a cryptographic module provide an acceptable level of security for the given application and environment.

NIST emphasizes the importance of computer security awareness and of making information security a management priority that is communicated to all employees. Since computer security requirements will vary for different applications, organizations should identify their information resources and determine the sensitivity to and potential impact of losses. Controls should be based on the potential risks and 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.

NIST has developed many of the needed basic controls to protect computer information, and has issued standards and guidelines covering both management and technical approaches to computer security. These include standards for cryptographic functions which will be implemented in cryptographic modules as specified in this standard. This standard is expected to be the foundation for NIST's current and future cryptographic standards.

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 must be a FIPS approved algorithm), but it differs from the higher levels in several respects. No physical security mechanisms are required in the module beyond the requirement for production-grade equipment.

Examples of Level 1 systems include Integrated Circuit (IC) cards and add-on security products. It is commonly felt that IC cards enhance the security of most systems. IC cards may be used as a secure storage medium when distributing cryptographic keys and may also implement cryptographic algorithms. Many vendors produce personal computer (PC) encryption boards which will meet the Level 1 requirements. NIST has validated the correct implementation of NIST cryptographic standards in several IC cards and encryption boards.

Level 1 allows software cryptographic functions to be performed in a general purpose personal computer (PC). NIST believes that such implementations are often appropriate in low-level security applications. The implementation of PC cryptographic software may be more cost-effective than hardware-based mechanisms. This will enable agencies to avoid the situation that exists today whereby the decision is often made not to cryptographically protect data because hardware is considered too expensive.

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, which are available today, would be 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 within the module. Pick-resistant locks would be placed on covers or doors to protect against unauthorized physical access. These requirements provide a low cost means for physical security and avoid the cost of the higher level of protection involving hard opaque coatings or significantly more expensive tamper detection and zeroization circuitry.

Level 2 provides for role-based authentication in which a module must authenticate that an operator is authorized to assume a specific role and perform a corresponding set of services.

Level 2 also allows software cryptography in multi-user timeshared systems when used in conjunction with a C2 or equivalent trusted operating system. The ratings C2, B1 and B2 ratings are in accordance with the TCSEC (see Appendix C). Many security experts feel that a trusted operating system is needed in order for software cryptography to be implemented with a level of trust comparable to hardware cryptography. This enables multi-user timeshared systems to implement cryptographic functions in software when this level of security is cost effective.

1.3 Security Level 3

Security Level 3 requires enhanced physical security which is generally available in many existing commercial security products. Unlike Security Level 2 which employs locks to protect against tampering with a cryptographic module, or employs coatings or seals to detect when tampering has occurred, Level 3 attempts to prevent the intruder from gaining access to critical security parameters held within the module. For example, a multi-chip embedded module must be contained in a strong enclosure, and if a cover is removed or a door is opened, the critical security parameters are zeroized. As another example, a module must be enclosed in a hard, opaque potting material to deter access to the contents.

Level 3 provides for identity-based authentication, which is stronger than the role based-authentication used in Level 2. A module must authenticate the identity of an operator and verify that the identified operator is authorized to assume a specific role and perform a corresponding set of services.

Level 3 provides stronger requirements for entering and outputting critical security parameters. The data ports used for critical security parameters must be physically separated from other data ports. Furthermore, the parameters must either be entered into or output from the module in encrypted form (in which case they may travel through enclosing or intervening systems) or be directly entered into or output from the module (without passing through enclosing or intervening systems) using split knowledge procedures.

Level 3 allows software cryptography in multi-user timeshared systems when a B1 or equivalent trusted operating system is employed along with a trusted path for the entry and output of critical security parameters. A B1 or better trusted operating system with a trusted path would have the capability to protect cryptographic software and critical security parameters from other untrusted software that may run on the system. Such a system could prevent plaintext from being mixed with ciphertext, and it could prevent the unintentional transmission of plaintext keys.

1.4 Security Level 4

Security Level 4 provides the highest level of security. Although most existing products do not meet this level of security, some products are commercially available which meet many of the Level 4 requirements. Level 4 physical security provides an envelope of protection around the cryptographic module. Whereas the tamper detection circuits of lower level modules may be bypassed, the intent of Level 4 protection is to detect a penetration of the device from any direction. For example, if one attempts to cut through the enclosure of the cryptographic module, the attempt should be detected and all critical security parameters should be zeroized. Level 4 devices are particularly useful for operation in a physically unprotected environment where an intruder could possibly tamper with the device.

Level 4 also protects a 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 could be used to thwart a module's defense during an attack. A module is required to either include special environmental protection features designed to detect fluctuations and zeroize critical security parameters, or to undergo rigorous environmental failure testing that provides a reasonable assurance that the module will not be affected by fluctuations outside of the normal operating range in a manner that can compromise the security of the module.

Level 4 allows software cryptography in multi-user timeshared systems when a B2 or equivalent trusted operating system is employed. A B2 trusted operating system provides additional assurances of the correct operation of the security features of the operating system.

2. DEFINITIONS AND ACRONYMS

2.1 Definitions

The following definitions are used throughout this standard:

Automated key distribution: the distribution of cryptographic keys, usually in encrypted form, using electronic means, such as a computer network (e.g., down-line key loading, the automated key distribution protocols of ANSI X9.17).

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

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 parameters: security-related information (e.g., cryptographic keys, 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, or
- a data authentication code (DAC) computed from data.

Cryptographic key component (key component): a parameter which is combined via a bit-wise exclusive-OR operation with one or more other identically sized key component(s) to form a plaintext cryptographic key.

Cryptographic module: the set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

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

Data authentication code (DAC): a cryptographic checksum, based on DES (see FIPS PUB 113); also known as a Message Authentication Code (MAC) in ANSI standards.

Data key: a cryptographic key which is used to cryptographically process data (e.g., encrypt, decrypt, sign, authenticate).

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

Digital signature: a nonforgeable transformation of data that allows the proof of the source (with non-repudiation) and the 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 which either directly or indirectly can contribute to a degradation in the performance of an electronic system.

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.

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

Encrypted key (ciphertext 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.

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 which 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).

FIPS approved security method: a security method (e.g., cryptographic algorithm, cryptographic key generation algorithm or 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.

Firmware: the programs and data (i.e., software) permanently stored in hardware (e.g., in ROM, PROM, or EPROM) such that the programs and data cannot be dynamically written or modified during execution. Programs and data stored in EEPROM are considered as software.

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

Initialization vector (IV): a vector used in defining the starting point of an encryption process within a cryptographic algorithm (e.g., the DES Cipher Block Chaining (CBC) mode of operation).

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.

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

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

Key loader: a self-contained unit which is capable of storing at least one plaintext or encrypted cryptographic key or key component which 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, counters) during the entire life cycle of the keys, including their generation, storage, distribution, entry and use, deletion or destruction, and archiving.

Manual key distribution: the distribution of cryptographic keys, often in a plaintext form requiring physical protection, but using a nonelectronic means, such as a bonded courier.

Manual key entry: the entry of cryptographic keys into a cryptographic module from a printed form, using devices such as buttons, thumb wheels or a keyboard.

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

Operator: an individual accessing a cryptographic module, either directly or indirectly via a process operating on his or her behalf, regardless of the specific role the individual assumes.

Output data: information that is to be output from a cryptographic module that has resulted from a transformation or computation in the module.

Password: a string of characters used to authenticate an identity or to verify access authorization.

Personal Identification Number (PIN): a 4 to 12 character alphanumeric code or password used to authenticate an identity, commonly used in banking applications.

Physical protection: the safeguarding of a cryptographic module or of cryptographic keys or other critical security parameters using physical means.

PIN: see Personal Identification Number.

Plaintext key: an unencrypted cryptographic key which is used in its current form.

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, uniquely associated with an entity, and not made public.

Public key: a cryptographic key used with a public key cryptographic algorithm, uniquely associated with an entity, and which may be made public.

Public key certificate: a set of data that unambiguously identifies an entity, contains the entity's public key, and is digitally signed by a trusted party.

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.

Secret key: a cryptographic key used with a secret key cryptographic algorithm, uniquely associated with one or more entities, and which shall 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.

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

Split knowledge: a condition under which two or more entities separately have key components which individually convey no knowledge of the plaintext key which 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.

Trusted path: a mechanism by which a person or process can communicate directly with a cryptographic module and which can only be activated by the person, process or module, and cannot be imitated by untrusted software within the module.

Zeroization: a method of erasing electronically stored data by altering 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
ATM	Automated Teller Machine
CBC	Cipher Block Chaining
DAC	Data Authentication Code
DES	Data Encryption Standard
DOC	Department of Commerce
DOD	Department of Defense
EDC	Error Detection Code
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read-Only Memory
E^2PROM	Electronically-Erasable Programmable Read-Only Memory
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FIPS PUB	FIPS Publication
FSM	Finite State Machine
IC	Integrated Circuit
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
IV	Initialization Vector
LCD	Liquid Crystal Display
LED	Light Emitting Diode
MAC	Message Authentication Code
NBS	National Bureau of Standards
NIST	National Institute of Standards and Technology (formerly the National Bureau of Standards)

NSA	National Security Agency
PC	Personal Computer
PIN	Personal Identification Number
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
ROM	Read-Only Memory
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria

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 operations or use.
- To prevent the unauthorized disclosure of the nonpublic contents of the cryptographic module, including plaintext cryptographic keys and other critical security parameters.
- To prevent the unauthorized and undetected modification of the cryptographic module, including the unauthorized modification, substitution, insertion, and deletion of cryptographic keys and other critical security parameters.
- To employ FIPS approved security methods for the protection of unclassified information.
- To provide indications of the operational state of the cryptographic module.
- To ensure the proper operation of the cryptographic module.
- To detect errors in the operation of the cryptographic module and to prevent the compromise of sensitive data and critical security parameters 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 basic design and documentation, module interfaces, authorized roles and services, physical security, software security, operating system security, key management, cryptographic algorithms, electromagnetic interference/electromagnetic compatibility (EMI/EMC), and self-testing. Table 1 summarizes the security requirements in each of these areas.

A cryptographic module shall be tested against the requirements of each area addressed in this section. The 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 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, the module shall receive a rating that reflects fulfillment of all of the requirements for that area.

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 (1) the minimum of the independent ratings received in the areas with levels, and (2) fulfillment of all the requirements in the other areas.

Many of the security requirements of this standard include specific documentation requirements. These requirements are summarized in Appendix A. The FIPS 140-1 validation procedures may require additional documentation. All documentation shall be provided to the validation facility by the manufacturer of a cryptographic module. Requirements for user documentation are beyond the scope of this standard, however, copies of the user and installation manuals for a cryptographic module shall also be provided to the validation facility.

Table 1. *Summary of Security Requirements*

<table>
<tr><th></th><th>Security Level 1</th><th>Security Level 2</th><th>Security Level 3</th><th>Security Level 4</th></tr>
<tr><td>Crypto Module</td><td colspan="4">Specification of cryptographic module and cryptographic boundary. Description of cryptographic module including all hardware, software, and firmware components. Statement of module security policy.</td></tr>
<tr><td>Module Interfaces</td><td colspan="2">Required and optional interfaces. Specification of all interfaces and of all internal data paths.</td><td colspan="2">Data ports for critical security parameters physically separated from other data ports.</td></tr>
<tr><td>Roles & Services</td><td>Logical separation of required and optional roles and services</td><td>Role-based operator authentication.</td><td colspan="2">Identity-based operator authentication.</td></tr>
<tr><td>Finite State Machine</td><td colspan="4">Specification of finite state machine model. Required states and optional states. State transition diagram and specification of state transitions.</td></tr>
<tr><td>Physical Security</td><td>Production grade equipment.</td><td>Locks or tamper evidence.</td><td>Tamper detection and response for covers and doors.</td><td>Tamper detection and response envelope.</td></tr>
<tr><td>EFP/EFT</td><td colspan="3">No requirements.</td><td>Temperature and voltage.</td></tr>
<tr><td>Software Security</td><td colspan="2">Specification of software design. Relate software to finite state machine model.</td><td>High-level language implementation.</td><td>Formal model. Pre- and post- conditions.</td></tr>
<tr><td>Operating System Security</td><td>Executable code. Authenticated. Single user, single process.</td><td>Controlled access protection (C2 or equiv.).</td><td>Labelled protection (B1 or equiv.). Trusted communications path.</td><td>Structured protection (B2 or equiv.).</td></tr>
<tr><td>Key Management</td><td colspan="2">FIPS approved generation/distribution techniques.</td><td colspan="2">Entry/exit of keys in encrypted form or direct entry/exit with split knowledge procedures.</td></tr>
<tr><td>Cryptic Algorithms</td><td colspan="4">FIPS approved cryptographic algorithms for protecting unclassified information.</td></tr>
<tr><td>EMI/EMC</td><td colspan="2">FCC Part 15, Subpart J, Class A (Business use). Applicable FCC requirements (for voice).</td><td colspan="2">FCC Part 15. Subpart J, Class B (Home use.)</td></tr>
<tr><td>Self-Tests</td><td colspan="4">Power-up tests and conditional tests.</td></tr>
</table>

4.1 Cryptographic Modules

A *cryptographic module* shall be a set of hardware, software, firmware, or some combination thereof, that implements cryptographic logic or processes. 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 which executes the code. Parts of a cryptographic module can be excluded from the requirements of this standard if it can be shown that these parts do not affect the security of the module.

This standard allows three different physical configurations of a cryptographic module: single-chip modules, multi-chip embedded modules, and multi-chip standalone modules (see Section 4.5).

Documentation shall identify 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. The documentation shall include a block diagram depicting all of the major hardware components of the module and their interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory. The documentation shall also indicate any hardware, software or firmware components of a module that are excluded from the security requirements of this standard, and explain the rationale for the exclusion.

Documentation shall also completely specify the cryptographic module security policy, i.e., the security rules under which a module must operate. In particular, the security policy shall include the security rules derived from the security requirements of this standard and the security rules derived from any additional security requirements imposed by the manufacturer.

4.2 Module Interfaces

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

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 data entered via the control input interface) that is to be input to and processed by a 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 data output via the status output interface) that is to be output from a 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 whenever an error state exists and during self-tests.

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

Status Output Interface. All output signals, indicators, and data (including status codes and physical indicators such as lights, LEDs, buzzers, bells, and displays) used to indicate or display the status of a module shall exit via the "status output" interface.

For Security Levels 1 and 2, the data input and output port or ports used for cryptographic keys, authentication data, and other critical security parameters may be shared with other ports of the module.

For Security Levels 3 and 4, the data input and output port or ports used for plaintext cryptographic key components, plaintext authentication data, and other unprotected critical security parameters shall be physically separated from all other ports of the module. Furthermore, these ports shall allow for direct entry of plaintext cryptographic key components, plaintext authentication data, and other unprotected critical security parameters, as required in Section 4.8.3.

A cryptographic module optionally may include the following interfaces:

Power Interface. All external electrical power shall enter or exit via the "power interface." The power interface is not required when all power is provided or maintained internally to the cryptographic module.

Maintenance Access Interface. Any data, control and status information used to maintain, service or repair a module shall enter and exit via the "maintenance access interface." All physical access paths, including removable covers or doors, used to gain physical access to the contents of a 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, as specified in Section 4.5. All access to the maintenance access interface, including physical modifications to the contents of the module, shall be restricted to the authorized maintenance role as specified in Section 4.3.1. All plaintext secret and private keys, and other critical security parameters contained in the module shall be zeroized when accessing the maintenance interface.

Documentation shall include a complete 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. If a cryptographic module includes a maintenance access interface, then documentation shall include a complete specification of the set of authorized maintenance procedures for the module.

All physical and logical input and output data paths within the module shall be explicitly defined. All input data entering the module via the "data input" interface shall only pass through the input data path. All output data exiting the module via the "data output" interface shall 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 critical security parameters or sensitive data could be output. The output data path shall be logically disconnected from the circuitry and processes performing key generation, manual key entry or key zeroization. Documentation shall include a complete specification of the defined input and output data paths.

4.3 Roles and Services

A cryptographic module shall be designed to support authorized roles and the corresponding services that can be performed within those roles. If a module can support multiple 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 (either directly or indirectly via a computer process acting on his or her behalf) and to verify that the operator is authorized to perform the desired roles and to perform the desired services within that role.

4.3.1 Roles

A cryptographic module shall support the following authorized roles:

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

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

If a cryptographic module includes a maintenance access interface as specified in Section 4.2, then the module shall also support the maintenance role.

Maintenance Role: The role assumed by an authorized maintenance person accessing the maintenance access interface and/or performing specific maintenance tests and obtaining interim results in order to maintain, service or repair the module. A cryptographic module shall clear all plaintext secret and private keys and other critical security parameters when entering the maintenance role. A cryptographic module shall clear all maintenance keys and other critical security parameters when exiting the maintenance role.

A module may support other roles or sub-roles in addition to the roles specified above. Documentation shall provide a complete specification of all of the authorized roles supported by the 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 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 4.11.

A cryptographic module may optionally provide the following service:

Bypass. Activate or deactivate a bypass capability whereby services are provided without cryptographic processing (e.g., transferring plaintext through the module). If a cryptographic module implements a bypass capability, then (1) in order to prevent the inadvertent bypass of data due to a single failure, two independent internal actions shall be implemented to activate the bypass capability, and (2) the current status of the module (e.g., the response to a "Show Status" service request) shall indicate whether or not the bypass capability is activated.

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

4.3.3 Operator Authentication

For Security Levels 2, 3 and 4, a cryptographic module shall perform either role-based authentication or identity-based authentication of the operator accessing the module (either directly or indirectly via a computer process acting on his or her behalf) in order to verify that the operator is authorized to perform desired roles and services.

Role-Based Authentication: A cryptographic module shall authenticate that the operator is authorized to assume a specific role (or set of roles). The module shall require that the operator either implicitly or explicitly 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 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 (e.g., a physical key may both indicate one or more roles and verify the authorization to perform those roles). A module may permit an operator to change roles, but the module shall authenticate the authorization of the operator to assume any role that was not previously authenticated.

Identity-Based Authentication: A cryptographic module shall authenticate the identity of an operator and verify that the identified operator is authorized to assume a specific role (or set of roles). The module shall require that the operator be individually identified and that the specified identity be authenticated. The module shall require that the operator either implicitly or explicitly select one or more roles, and, based on the authenticated identity, verify that the operator is authorized to assume the selected roles 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 (e.g., an IC card may both identify, authenticate and authorize the operator to assume specific roles). A module may permit an operator to change roles without re-authenticating the identity of the operator, but the module shall verify the authorization of the authenticated operator to 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 module is powered up after being powered off (e.g., power failure) or after repair or servicing, the results of previous authentications shall not be retained, i.e., the module shall re-authenticate the authorization of the operator to assume a desired role.

A 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 (i.e., biometrics).

Services that are used to initialize the access control information needed to implement the access control mechanisms required herein, may require special treatment. For example, the first time that a crypto officer attempts to access a module, the module may not contain the authentication and authorization information required to authenticate the identity of the crypto officer and to verify his or her authorization to assume the crypto officer role. In these cases, other means (such as procedural controls, or factory-set or default authentication and authorization information) may be used to control access to the module.

SECURITY LEVEL 1

For Security Level 1, a cryptographic module is not required to employ authentication mechanisms to control access to the module. A module optionally may employ either *role-based* or *identity-based* authentication mechanisms in order to verify the authorization of the operator to assume the desired roles and to request corresponding services.

SECURITY LEVEL 2

For Security Level 2, a cryptographic module shall employ either *role-based* authentication mechanisms or identity-based mechanisms in order to verify the authorization of the operator to assume the desired roles and to request corresponding services.

SECURITY LEVELS 3 AND 4

For Security Levels 3 and 4, a cryptographic module shall employ *identity-based* authentication mechanisms in order to verify the authorization of the operator to assume the desired roles and to request corresponding services. Furthermore, plaintext authentication data (e.g., passwords and PINs), plaintext cryptographic key components, and other unprotected critical security parameters shall be entered via a port or ports that are physically separated from other ports, and that allow for direct entry (as required in Section 4.2).

4.4 Finite State Machine Model

All cryptographic modules shall be designed using a finite state machine model that explicitly specifies every operational and error state of the module.

A cryptographic module shall be designed using the following types of states:

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

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

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

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

Self-test states. States for performing self-tests on the module (see Section 4.11).

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

All data output via the data output interface shall be inhibited during all error states. All error states shall be able to be reset to an acceptable operational or initialization state except for those hard errors which require maintenance, service or repair of the module.

A cryptographic module may contain other types of states including the following:

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

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

Safety states. States in which the module is not currently operational, but cryptographic keys and parameters are loaded. These states are used to protect the module from unauthorized use during the temporary absence of the operator. The safety states shall require an explicit authenticated action to return to a user/crypto service state. These states are equivalent to the "standby" mode of former Federal Standard 1027.

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

Maintenance states. States for maintaining and servicing a module, including maintenance testing. If a cryptographic module includes a maintenance access interface (see Section 4.2), then the module shall include maintenance states.

All states of a cryptographic module shall be explicitly defined in sufficient detail to assure the verification of the conformance of the module to this standard. Documentation shall identify and describe all states of the module and shall describe all of the corresponding state transitions. The descriptions of the state

transitions shall include the internal module conditions, data inputs and control inputs that cause transitions from one state to another, and shall include the internal module conditions, data outputs and status outputs resulting from transitions from one state to another. Documentation shall also include finite state diagrams in sufficient detail to assure the verification of conformance to this standard.

4.5 Physical Security

A cryptographic module shall be designed to employ physical security mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or unauthorized modification of the module (including substitution of the entire module) when installed. The entire contents of a cryptographic module, including all hardware, firmware, software and data (including plaintext cryptographic keys and unprotected critical security parameters) shall be protected.

The physical security mechanisms employed by a cryptographic module depend largely on the physical embodiment of the module. The physical security requirements are separated into three distinct physical embodiments: single-chip modules, multiple-chip embedded modules, and multiple-chip standalone modules. Table 2 summarizes the physical security requirements for the three different physical embodiments of a module for each of the four security levels.

Depending on the security level of a cryptographic module, the physical security mechanisms may be designed such that unauthorized attempts at access, use or modification will either have a high probability of being detected subsequent to the attempt by leaving visible signs (i.e., tamper evident), or have a high probability of being detected during the attempt (i.e., tamper detection) so that appropriate actions can be taken by the module to protect itself (i.e., tamper response). Generally speaking, Security Level 1 simply requires minimal physical protection through the use of production-grade enclosures, Security Level 2 requires the addition of tamper evident counter measures, Security Level 3 requires the use of strong

Table 2. *Summary of Physical Security Requirements*

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

enclosures with tamper detection and response counter measures for covers and doors, and Security Level 4 requires the use of strong enclosures with tamper detection and response counter measures for the entire enclosure.

Documentation shall include a complete specification of the physical embodiment and security level for which the physical security mechanisms of a cryptographic module are designed, as well as a complete description of the applicable physical security mechanisms that are employed by the module.

4.5.1 Single-Chip Cryptographic Modules

Single-chip cryptographic modules are implementations in which a single integrated circuit (IC) chip may be used as a standalone device or may be physically embedded within some other module or enclosure which may not be physically protected. Single-chip modules include single IC chips, smart cards with a single IC chip, and other systems that incorporate a single IC chip to implement cryptographic functions. Because of its small size and its fabrication, a single chip has some inherent tamper resistance. A few additional requirements provide reasonable physical security.

SECURITY LEVEL 1

The following requirement shall apply to a single-chip cryptographic module for Security Level 1.

- The chip shall be of production-grade quality, which shall include standard passivation techniques (i.e., a sealing coat applied over the chip circuitry to protect it against environmental or other physical damage).

SECURITY LEVEL 2

In addition to the Security Level 1 requirement, the following requirement shall apply to a single-chip cryptographic module for Security Level 2.

- The chip shall be covered with an opaque tamper evident coating (e.g., an opaque tamper evident passivation material, or an opaque tamper evident material covering the passivation) to deter direct observation, probing or manipulation of the surface features of the chip. The material shall be opaque within the visible spectrum.

SECURITY LEVEL 3

In addition to the requirements for Security Levels 1 and 2, the following requirement shall also apply to a single-chip cryptographic module for Security Level 3.

- A hard, opaque tamper evident coating shall be used (e.g., a hard opaque epoxy covering the passivation).

SECURITY LEVEL 4

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

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

- The module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in Section 4.5.4.

4.5.2 Multiple-Chip Embedded Cryptographic Modules

Multiple-chip embedded cryptographic modules are implementations in which two or more IC chips are interconnected and are physically embedded within some other module or enclosure which may not be physically protected. Multiple-chip embedded cryptographic modules include adaptors and expansion boards, and other modules that are not single chips and are not contained within physically protected stand-alone modules. Typical size and space constraints restrict the physical security mechanisms that can be effectively employed.

SECURITY LEVEL 1

The following requirements shall apply to a multiple-chip embedded cryptographic module for Security Level 1.

- The chips shall be of production-grade quality, which shall include standard passivation techniques (i.e., a sealing coat applied over the chip circuitry to protect it against environmental or other physical damage).

- The module shall be implemented as a production-grade multiple-chip embodiment (i.e., an IC printed circuit board, a ceramic substrate, etc.).

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirement shall apply to a multiple-chip embedded cryptographic module for Security Level 2.

- The module shall be encapsulated within an opaque tamper evident material (e.g., conformal coating, bleeding paint) in order to prevent direct observation of module components, and to provide evidence of attempts to tamper with or remove module components. The material 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 a multiple-chip embedded cryptographic module for Security Level 3.

- A hard opaque potting material (e.g., a hard opaque epoxy).

  –or–

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

  –or–

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

- If the module is contained within a cover or enclosure and if the cover or enclosure contains any ventilation holes or slits, then they shall be small and constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., require at least one 90 degree bend or block with a substantial blocking material).

SECURITY LEVEL 4

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

- The contents of the module shall be completely contained *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) which will detect tampering by means such as drilling, milling, grinding or dissolving of the potting material or cover.

- The module shall contain tamper response and zeroization circuitry. The circuitry shall continuously monitor the tamper detection envelope for tampering, and upon the detection of tampering, shall immediately zeroize all plaintext cryptographic keys and other unprotected critical security parameters (see Section 4.8.5). The circuitry shall be operational whenever plaintext cryptographic keys or other unprotected critical security parameters are contained within the cryptographic module.

- The module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in Section 4.5.4.

4.5.3 Multiple-Chip Standalone Cryptographic Modules

Multiple-chip standalone cryptographic modules are implementations in which the entire enclosure is physically protected. The modules may contain two or more IC chips that are interconnected (e.g., an IC printed circuit board or ceramic substrate). Typical size and space constraints may no longer restrict the physical security mechanisms that can be effectively employed.

SECURITY LEVEL 1

The following requirements shall apply to a standalone cryptographic module for Security Level 1.

- The chips shall be of production-grade quality, which shall include standard passivation techniques (i.e., a sealing coat applied over the chip circuitry to protect it against environmental or other physical damage).

- The circuitry within the module shall be implemented as a production-grade multiple-chip embodiment (i.e., an IC printed circuit board, a ceramic substrate, etc.).

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

SECURITY LEVEL 2

In addition to the requirements for Security Level 1, the following requirements shall also apply to a standalone cryptographic module for Security Level 2.

- The enclosure shall be opaque within the visible spectrum.

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

SECURITY LEVEL 3

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

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

  –or–

- The module shall be contained within a strong enclosure. The enclosure shall be designed such that attempts to remove it will have a high probability of causing serious damage to the circuitry within the module (i.e., the module does not function). If the enclosure contains any removable covers or doors, then the module shall contain tamper response and zeroization circuitry. The circuitry shall continuously monitor the covers and doors, and upon the removal of a cover or the opening of a door, shall immediately zeroize all plaintext cryptographic keys and other unprotected critical security parameters. The circuitry shall be operational whenever plaintext cryptographic keys or other unprotected critical security parameters are contained within the cryptographic module.

- If the enclosure contains any ventilation holes or slits, then they shall be small and constructed in a manner that prevents undetected physical probing inside the enclosure (e.g., require at least one 90 degree bend or block with a substantial blocking material).

SECURITY LEVEL 4

In addition to the requirements for Security Levels 1, 2 and 3, the following requirements shall also apply to a standalone cryptographic module 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 modules. These mechanisms shall be designed to detect tampering by means such as cutting, drilling, milling, grinding or dissolving of the potting material or cover.

- The module shall contain tamper response and zeroization circuitry. The circuitry shall continuously monitor the tamper detection mechanisms for tampering, and upon the detection of tampering, shall immediately zeroize all plaintext cryptographic keys and other unprotected critical security parameters. The circuitry shall be operational whenever plaintext cryptographic keys or other unprotected critical security parameters are contained within the cryptographic module.

- The module shall either include environmental failure protection (EFP) features or undergo environmental failure testing (EFT) as specified in Section 4.5.4.

4.5.4 Environmental Failure Protection/Testing

Electronic devices and circuitry are designed to operate within a particular range of environmental conditions. If the devices or circuitry are operated outside of this range, their correct operation is not guaranteed. 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 nor 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).

4.5.4.1 Environmental Failure Protection Features (Alternative 1)

Environmental failure protection (EFP) features shall be designed to 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 module shall monitor and correctly respond to fluctuations in the operating *temperature* and *voltage* outside of a module's specified normal operating ranges.

The protection features shall involve additional electronic circuitry or devices that shall continuously measure these environmental conditions. If a condition is determined to be outside of the module's normal operating range, the protection circuitry shall either (1) shutdown the module to prevent it from operating outside the normal range, or (2) immediately zeroize all plaintext cryptographic keys and other unprotected critical security parameters. Documentation shall provide a complete specification and description of the environmental failure protection features employed within a module.

4.5.4.2 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 the security of the module. The manufacturer of a 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) which causes the destruction of the electronic devices or circuitry, to the smallest positive voltage (with respect to ground) which causes the destruction of the electronic devices or circuitry, including reversing the polarity of the voltages. The 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 module be compromised. If at any time during the test, the security of the 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.

4.6 Software Security

The following software security requirements shall apply to all software and firmware contained within a cryptographic module. These requirements do not apply to microcode or system software whose source code is not available to the module manufacturer. These requirements do not apply to any software or firmware that can be shown not to affect the security of the module. Documentation shall identify any software or firmware that is excluded from the software security requirements and explain the rationale for the exclusion.

SECURITY LEVELS 1 AND 2

The following requirements shall apply for Security Levels 1 and 2.

- Documentation shall include a detailed description of the design of the software within the module (e.g., the finite state machine specification required in Section 4.4).

- Documentation shall include a detailed explanation of the correspondence between the design of the software and the cryptographic module security policy (i.e., the rules of operation as documented per the requirements of Section 4.1) (Security Levels 1, 2, and 3 only).

- Documentation shall include a complete source code listing for all software contained within the module. For each software module, software function and software procedure, the source code listing shall be annotated with comments that clearly depict the relationship of these software entities to the design of the software.

SECURITY LEVEL 3

In addition to the applicable requirements for Security Levels 1 and 2, the following requirement shall apply for Security Level 3.

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

SECURITY LEVEL 4

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

- Documentation shall include a specification of a formal model (i.e., a precise mathematical statement) of the cryptographic module security policy (i.e., the security rules under which the module must operate) as documented per the requirements of Section 4.1. 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. Examples include, but are not limited to INAJO, GYPSY, VDM, Z, LOTOS, EHDM and ESTELLE.

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

- For each software module, software function and software procedure, the source code listing shall be annotated with comments that clearly specify (1) the pre-conditions required upon entry into the module, function or procedure in order for it to execute correctly, and (2) the post-conditions expected to be true when execution of the module, function or procedure is complete. These conditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of a module, function or procedure. While a mechanically checked proof is not required, it shall be possible to prove from the pre- and post-conditions that a module, function or procedure is consistent with the formal model.

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

RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES

- It is highly recommended that all software within a cryptographic module be implemented using the set of recommended software development practices listed in Appendix B. These practices will facilitate the analysis of the software for conformance to the requirements of this standard, and will reduce the chances of programming errors.

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

SECURITY LEVEL 1

For Security Level 1, the following requirements apply. Note that as a consequence of these requirements, multi-user, multi-processing operating systems are explicitly excluded from Security Level 1, and hence, must satisfy the requirements for Security Levels 2, 3 or 4.

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

- A cryptographic mechanism using a FIPS approved authentication technique (e.g., the computation and verification of a data authentication code or NIST digital signature algorithm) shall be applied to the cryptographic software within the cryptographic module. This cryptographic mechanism requirement may be incorporated as part of the Software/Firmware Test (Section 4.11.1) if a FIPS approved authentication technique is employed for that test.

- Use of the cryptographic module shall be limited to a single user at a time (Security Level 1 only).

- Use of the cryptographic module shall be dedicated to the cryptographic process during the time the cryptographic process is in use (Security Level 1 only).

SECURITY LEVEL 2

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

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

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

  1. The operating system shall provide the capability to specify a set of operators who can *execute* cryptographic program images contained on the cryptographic module's secondary storage.

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

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

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

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

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

   The operating system shall provide the capability to prevent all operators and processes from reading the following cryptographic module software components:

   – cryptographic program images contained on secondary storage
   – executing cryptographic program images

4. The operating system shall provide the capability to specify a set of operators who are authorized to *enter* cryptographic keys and other critical security parameters.

SECURITY LEVEL 3

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

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

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

- The operating system shall provide the capability to audit the entry of cryptographic keys, other critical security parameters, and control inputs and status outputs.

SECURITY LEVEL 4

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

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

4.8 Cryptographic Key Management

Cryptographic key management is concerned with the entire life cycle of the cryptographic keys employed with a cryptographic-based security system, including their generation, distribution, entry and use, storage, destruction and archiving. Cryptography may play an important role in key management. A cryptographic module will not only have its own key management requirements, but may also be utilized as part of the key management process for another cryptographic module or cryptographic-based security system.

Key management is required for all cryptographic modules, whether the module implements a secret key (symmetric) algorithm or a public key (asymmetric) algorithm. Secret keys and private keys shall be protected from unauthorized disclosure, modification and substitution. Public keys shall be protected against unauthorized modification and substitution.

4.8.1 Key Generation

A cryptographic module may optionally implement an internal key generation function. The module shall implement a FIPS approved key generation algorithm. Documentation shall specify the FIPS approved key generation algorithm that is implemented by the module.

When a random number generator is used in the key generation process, all values shall be generated randomly or pseudo-randomly such that all possible combinations of bits and all possible values are equally likely to be generated. A seed key, if used, shall be entered in the same manner as cryptographic keys (see Section 4.8.3). Intermediate key generation states and values shall not be accessible outside of the module in plaintext or otherwise unprotected form.

4.8.2 Key Distribution

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

4.8.3 Key Entry and Output

Manually-distributed cryptographic keys may be entered into or output from a cryptographic module either by purely manual methods (e.g., via a keyboard, rotary switches, thumbwheels, or LCD displays) or by electronic methods (e.g., via memory cards/tokens such as magnetic-striped cards and integrated circuit (IC) chip devices, smart cards/tokens, or other electronic key loaders).

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 4.11.2. During key entry, keys and key components may be temporarily displayed to allow visual verification and to improve accuracy. When encrypted keys or key components are entered, the resulting plaintext secret or private keys shall not be displayed.

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

SECURITY LEVELS 1 AND 2

For Security Levels 1 and 2, when manually-distributed secret keys or private keys are entered into or output from a cryptographic module they may be entered or output as plaintext keys. Optionally, the keys may be entered or output either (1) in encrypted form, or (2) under split knowledge procedures (i.e., as two or more plaintext key components), as required below for Security Levels 3 and 4. 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 not be entered into or output from a cryptographic module in plaintext form. When manually-distributed secret or private keys are entered into or output from a cryptographic module, they 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 a secret key or private key is entered or output under split knowledge procedures, the module shall provide the capability to separately authenticate the operator for each key component. Furthermore, the key components shall be entered directly into the cryptographic module or output directly from the cryptographic module (e.g., via a trusted path or directly attached cable), without traveling through any enclosing or intervening systems where the components could be stored, combined, or otherwise processed. Electronically distributed secret and private keys shall be entered and output in encrypted form.

4.8.4 Key Storage

When contained within a cryptographic module, secret and private keys may be stored in plaintext form. These plaintext keys shall not be accessible from outside the module.

A means shall be provided to ensure that all keys are associated with the correct entities (i.e., person, group, or process) to which the keys are assigned.

4.8.5 Key Destruction

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

4.8.6 Key Archiving

A cryptographic module optionally may output keys for archiving purposes. Keys output for archiving shall be encrypted.

4.9 Cryptographic Algorithms

Cryptographic modules shall employ FIPS approved cryptographic algorithms.

4.10 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Radios shall meet all applicable FCC requirements. All other modules shall meet the following requirements. TEMPEST protection is not required by, and is beyond the scope of, this standard.

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 FCC Part 15, Subpart J, 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 FCC Part 15, Subpart J, Class B (i.e., for home use).

4.11 Self-Tests

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

Whenever a cryptographic module fails a self-test, the module shall enter an error state and output an error indicator via the status interface. The 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 to including maintenance, servicing or repair of the module).

4.11.1 Power-Up Tests

After a cryptographic module is powered up, the module shall enter the self-test state and perform all of the following 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 module shall provide a means to initiate the tests on demand for periodic testing of the module.

Cryptographic algorithm test. The cryptographic algorithm shall be tested by operating the algorithm on data for which the correct output is already known (i.e., a "known-answer" test). The test is passed if the calculated output equals the previously generated output (the known answer). A known answer test shall be run for each cryptographic function (e.g., encryption, decryption, authentication) that is implemented. Message digest algorithms shall either have an independent known-answer test or shall be included in the known-answer test of the cryptographic algorithm in which they are included (e.g., a digital signature algorithm).

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

Software/firmware test. An error detection code (EDC) or FIPS approved authentication technique (e.g., the computation and verification of a data authentication code or NIST digital signature algorithm) shall be applied to all validated software and firmware residing in the module (e.g., within EEPROM and RAM). This error detection code, data authentication code, or digital signature shall then be verified when the power-up tests are run. Software and firmware that has been validated by the FIPS 140-1 Validation Program is considered to be validated software and firmware.

Critical functions test. All other functions that are critical to the secure operation of the module and can be tested as part of the power-up tests shall be tested. Documentation shall provide a complete specification of all critical functions, and the nature of the power-up self-tests designed to test those functions. Other critical functions that are performed under certain specific conditions are tested as part of the conditional tests.

Statistical random number generator tests. Cryptographic modules that implement a random or pseudo random number generator shall incorporate the capability to perform statistical tests for randomness. For Levels 1 and 2, the tests are not required. For Level 3, the tests shall be callable upon demand. For level 4, the tests shall be performed at power-up and shall also be callable upon demand. The tests specified below are recommended. However, alternative tests which provide equivalent or superior randomness checking may be substituted.

A single bit stream of 20,000 consecutive bits of output from the generator is subjected to each of the following tests. If any of the tests fail, then the module shall enter an error state.

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 9,654 < X < 10,346.

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 each 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 1.03 < X < 57.4.

The Runs Test

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

2. The test is passed if the number of runs that occur (of lengths 1 through 6) is each within the corresponding interval specified below. This must hold for both the zeros and ones; that is, all 12 counts must lie in the specified interval. For the purpose of this test, runs of greater than 6 are considered to be of length 6.

Length of Run	*Required Interval*
1	2,267–2,733
2	1,079–1,421
3	502–748
4	223–402
5	90–223
6+	90–223

The Long Run Test

1. A long run is defined to be a run of length 34 or more (of either zeros or ones).

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

4.11.2 Conditional Tests

The following tests shall be performed under the conditions specified for each 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. For example, if the keys can be used to perform inverse operations, then one key (the public) shall be applied to a plaintext value, and the resulting ciphertext shall be compared to the original plaintext to verify that the application of the key did not result in the original plaintext (i.e., the identity mapping). If the two values are equal, then the test shall be failed. Then, the other key (the private) 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 be failed. 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.

Software/firmware load test. A cryptographic mechanism using a FIPS approved authentication technique (e.g., a data authentication code or NIST digital signature algorithm) shall be applied to all validated software and firmware that can be externally loaded into a cryptographic module. This test shall verify the data authentication code or digital signature whenever the software or firmware is externally loaded into the module. Software and firmware that has been validated by the FIPS 140-1 Validation Program is considered to be validated software and firmware.

Manual key entry test. When cryptographic keys or key components are manually entered into a cryptographic module, the keys shall have an error detection code (e.g., a parity check value) or shall use duplicate entries in order to verify the accuracy of the entered keys. A cryptographic module shall verify the error detection code or duplicate entries and provide an indication of the success or failure of the entry process.

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

APPENDIX A: SUMMARY OF DOCUMENTATION REQUIREMENTS

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

The following check list summarizes the documentation requirements of this standard. The FIPS 140-1 validation procedures may require additional documentation. All documentation shall be provided to the validation facility by the manufacturer 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 MODULES

[ ] 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.

[ ] Block diagram depicting all of the major hardware components of the module and their interconnections, including any microprocessors, input/output buffers, plaintext/ciphertext buffers, control buffers, key storage, working memory, and program memory.

[ ] Specification of any hardware, software or firmware components of a module that are excluded from the security requirements of this standard, and an explanation of the rationale for the exclusion.

[ ] Specification of the cryptographic module security policy, i.e., the security rules under which a module must operate, including the security rules derived from the security requirements of this standard and the security rules derived from any additional security requirements imposed by the manufacturer.

MODULE INTERFACES

[ ] 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.

[ ] Specification of the set of authorized maintenance procedures for the module.

[ ] Specification of the defined input and output data paths.

ROLES AND SERVICES

[ ] Specification of all of the authorized roles supported by the module.

[ ] Specification of each of the authorized services, operations, and functions that can be performed with the module. For each service, the service inputs, corresponding service outputs, and the authorized role (or set of roles) in which the service can be performed, shall be specified.

FINITE STATE MACHINE MODEL

[ ] Specification and description of all states of the module and of all the corresponding state transitions. The descriptions of the state transitions shall include the internal module conditions, data inputs and control inputs that cause transitions from one state to another, and shall include the internal module conditions, data outputs and status outputs resulting from transitions from one state to another.

[ ] Finite state diagrams in sufficient detail to assure the verification of conformance to this standard.

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.

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

SOFTWARE SECURITY

[ ] Specification of any software or firmware that is excluded from the software security requirements, and explanation of the rationale for the exclusion.

[ ] Detailed description of the design of the software within the module (e.g., the finite state machine model specification).

[ ] Detailed explanation of the correspondence between the design of the software and the cryptographic module security policy (i.e., the rules of operation). (Security Levels 1 and 2 only).

[ ] Complete source code listing for all software contained within the module. For each software module, software function and software procedure, the source code listing shall be annotated with comments that clearly depict the relationship of these software entities to the design of the software.

[ ] Specification of a formal model (i.e., a precise mathematical statement) of the cryptographic module security policy (i.e., the security rules under which the module must operate) as documented per the requirements of Section 4.1). 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. Examples include, but are not limited, INAJO, GYPSY, VDM, Z, LOTOS, EHDM and ESTELLE. (Security Level 4).

[ ] Detailed explanation (informal proof) of the correspondence between the formal model and the cryptographic module security policy. (Security Level 4).

[ ] Annotations in the source code listing for each software module, software function and software procedure, clearly specifying (1) the pre-conditions required upon entry into the module, function or procedure in order for it to execute correctly, and (2) the post-conditions expected to be true when execution of the module, function or procedure is complete. These conditions may be specified using any notation that is sufficiently detailed to completely and unambiguously explain the behavior of a module, function or procedure. (Security Level 4).

[ ] Detailed explanation (informal proof) of the correspondence between the software design (as reflected by the pre- and post-condition annotations) and the formal model. (Security Level 4).

KEY MANAGEMENT

[ ] Specification of the FIPS approved key generation procedures that are implemented by the module.

[ ] Specification of the FIPS approved key distribution techniques that are implemented by the module.

CRYPTOGRAPHIC ALGORITHMS

[ ] Specification of the FIPS approved cryptographic algorithms that are implemented by the module.

SELF-TESTS

[ ] Specification of each possible error condition, including the conditions and actions necessary to clear the error and resume normal operation (possibly to include maintenance, servicing or repair of the module).

[ ] Specification of all critical functions, and the nature of the power-up self-tests designed to test those functions.

APPENDIX B: RECOMMENDED SOFTWARE DEVELOPMENT PRACTICES

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

The following programming techniques should be used to facilitate analysis of the program, and to reduce the chances of programming errors. Deviations from these practices may be appropriate in some instances.

- Each variable should have an associated comment that gives the range of allowable values for the variable. If the range is unrestricted, this should be noted.
- Each procedure should have only one entry point. Each procedure should have at most two exit points, one for error exits and one for normal exits.
- Control flow within a procedure should be defined using only the following constructs: sequence, if-then-else, while-do, case, repeat-until, for, and other structured loop constructs.
- Data should be communicated between procedures through the use of argument lists and/or explicit return values. Global variables should not be used except where necessary for the implementation of an abstract data type.
- Modules (which consist of data plus one or more associated procedures) should be constructed according to the principle of encapsulation/information-hiding.
- Each loop should be preceded by a convincing argument (as a comment) that termination is guaranteed.
- Each procedure should perform only a single, well-defined function.
- Each procedure should be preceded by a comment explaining the function performed by the procedure.
- Floating point comparisons should not be used.
- Where possible, variable names should be used in only one context within the same procedure.
- Equivalence of variables should not be used to permit multiple memory usage for conflicting purposes.
- Upon entry to a procedure, input parameters should be checked for appropriate values where possible.
- The software should be hierarchically structured as a series of layers.

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 which 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: SELECTED REFERENCES

[ANSIX9.9] ANSI X9.9-1986, Financial Institution Message Authentication (Wholesale), American Bankers Association, Approved August 15, 1986.

[ANSIX9.17] ANSI X9.17-1985, Financial Institution Key Management (Wholesale), American Banker's Association, Approved April 4, 1985, Reaffirmed 1991.

[ANSIX9.23] ANSI X9.23-1988, Financial Institution Encryption of Wholesale Financial Messages, American Banker's Association, Approved May 16, 1988.

[ANSIX9.26] ANSI X9.26-1990, Financial Institution Sign-On Authentication for Wholesale Financial Transactions, Approved February 28, 1990.

[DOT86] Criteria and Procedures for Testing, Evaluating, and Certifying Message Authentication Devices, U.S. Department of Treasury, Second Edition, September 1, 1986.

[EHDM] Crow, J. S., R. Lee, J. M. Rushby, F. W. von Henke and R. A. Whitehurst, EHDM Verification Environment, Proceedings 11th National Computer Security Conference, October 1988.

[ESTELLE87] Budkowski, S. and P. Dembinski, An Introduction to Estelle: A Specification Language for Distributed Systems, Computer Networks and ISDN Systems, Vol. 14, North-Holland, 1987.

[ESTELLE89] ISO/IEC 9074, Estelle: A Formal Description Technique Based on an Extended State Transition Model, 1989.

[FIPS101] FIPS PUB 101, Guideline for Lifecycle Validation, Verification, and Testing of Computer Software, US DOC/NBS, June 6, 1983.

[GYPSY] Good, D. I., R. L. Akers and L. M. Smith, Report on Gypsy 2.05, Computational Logic, Inc., 1986.

[IEEE729] ANSI/IEEE Standard 729-1983, IEEE Standard Glossary of Software Engineering Terminology, IEEE, 1983.

[IEEE828] IEEE Standard 828-1983, IEEE Standard for Software Configuration Management Plans, IEEE, 1983.

[IEEE1012] ANSI/IEEE Standard 1012-1986, IEEE Standard for Software Verification and Validation Plans, IEEE, 1986 (FIPS PUB 132, Guideline for Software Verification and Validation Plans, U.S. DOC/NBS, November 19, 1987).

[IEEE1016] ANSI/IEEE Standard 1016-1987, IEEE Recommended Practice for Software Design Descriptions, IEEE, 1987.

[INAJO] Kemmerer, R. A., Integrating Formal Methods into the Development Process, IEEE Software, Volume 7, IEEE, September 1990.

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

[KEMM90] Kemmerer, Richard A., Integrating formal methods into the development process, IEEE Software, September 1990, pp. 37–50.

[LOTOS] ISO/DP 8807, LOTOS—A Formal Description Technique Based on the Temporal Ordering of Observational Behavior, March 1985.

[NEUM86] Neumann, Peter G., On hierarchical design of computer systems for critical applications, IEEE Transactions on Software Engineering, Volume SE-12, Number 9, September 1986, pp. 905–920.

[TCSEC] DOD 5200.28-STD, Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) ("The Orange Book"), National Computer Security Center, December 1985.

[VDM] Jones, C.B., Software Development, A Rigorous Approach, Prentice-Hall, 1980.

[Z] Hayes, I., Specification Case Studies, Prentice-Hall, 1987.

☆ U.S. GOVERNMENT PRINTING OFFICE: 1994 - 300-633 - 814/12646

U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Road
Springfield, VA 22161