ITL Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

A COMPARISON OF THE SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES IN FIPS 140-1 AND FIPS 140-2

By Stanley R. Snouffer and Annabelle Lee, Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology

Federal agencies, industry, and the public now rely on cryptography to protect information and communications used in critical infrastructures, electronic commerce, and other application areas. Cryptographic modules are implemented in these products and systems to provide cryptographic services such as confidentiality, integrity, non-repudiation and identification and authentication. Adequate testing and validation of the cryptographic module against established standards is essential for security assurance. Both federal agencies and the public benefit from the use of tested and validated products. Without adequate testing, weaknesses such as poor design, weak algorithms, or incorrect implementation of the cryptographic module can result in insecure products.

This *ITL Bulletin* summarizes the differences between FIPS 140-1 and FIPS 140-2. Information on the actual line-by-line differences between FIPS 140-1 and FIPS 140-2 may be found in the full version of this document, NIST Special Publication 800-29, located at: http://csrc.nist.gov/publications/nistpubs/index.html.

The Cryptographic Module Validation Program and FIPS 140-2

On July 17, 1995, NIST's Information Technology Laboratory established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standard (FIPS) 140-1, *Security Requirements for Cryptographic Modules,* and other FIPS cryptography-based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment (CSE) of the Government of Canada. Products validated as conforming to FIPS 140-1 are accepted by the federal agencies of both countries for the protection of sensitive information. Vendors of cryptographic modules use independent, accredited testing laboratories to test their modules. NIST's Computer Security Division and CSE jointly serve as the validation authorities for the program, validating the test results. Currently, there are several National Voluntary Laboratory Accreditation Program (NVLAP) accredited laboratories that perform FIPS 140-1 compliance testing. These laboratories and the Validated Products List are available at http://csrc.nist.gov/cryptval. As of July 2001, over 175 cryptographic modules from more than 40 separate vendors have been validated through the program. The number of validated modules has nearly doubled each year of the program's existence.

The underlying philosophy of the CMVP is that the user community needs strong independently tested and commercially available cryptographic products. The CMVP must also work with the commercial sector and the cryptographic community to achieve security, interoperability, and assurance. Directly associated with this philosophy is the goal of the CMVP to promote the use of validated products and provide federal agencies with a security metric to use in procuring cryptographic modules. The testing performed by accredited laboratories provides this metric. Federal agencies, industry, and the public can choose products from the CMVP Validated Modules List and have confidence that the products meet the claimed level of security. The program validates a wide variety of modules including general encryption products, secure radios, Virtual Private Network (VPN) devices, Internet browsers, cryptographic tokens, and modules that support Public Key

Continued on page 2

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. **Bulletins are issued on an as-needed basis** and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8901, Gaithersburg, MD 20899-8901, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since February 2000

Infrastructure (PKI). Currently, validation services are provided for FIPS 140-1&2, the Data Encryption Standard (DES and Triple DES), the Digital Signature Standard, the Secure Hash Standard, and the Skipjack Algorithm.

The CMVP offers a documented methodology for conformance testing through a defined set of security requirements in FIPS 140-1&2 and other cryptographic standards. NIST developed the standard and an associated metric (the Derived Test Requirements for FIPS 140-1) to ensure repeatability of tests and equivalency in results across the testing laboratories. The five commercial laboratories provide vendors of cryptographic modules a choice of testing facilities and promote healthy competition. (Note, there is no limit to the number of testing laboratories, and additional testing laboratories may be added to the program.)

A government and industry working group composed of both users and vendors developed FIPS 140-1. The working group identified 11 areas of security requirements with four increasing levels of security for cryptographic modules. The security levels allow for a wide spectrum of data sensitivity (e.g., low-value administrative data, million-dollar funds transfers, and health 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. The four security levels allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments. This structure also allows great flexibility when specifying or identifying users needs. Modules may meet different levels in the security requirements areas (e.g., a module meets level 2 overall, level 3 physical security with additional level 4 requirements). The Validated Modules List now contains modules representing all four security levels.

Who we are
The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our web site is http://www.itl.nist.gov/.

FIPS 140-1&2 define a framework and methodology for NIST's current and future cryptographic standards. The standard provides users with:

- a specification of security features that are required at each of four security levels;
- flexibility in choosing security requirements;
- a guide to ensuring the cryptographic modules incorporate necessary security features; and
- the assurance that the modules are compliant with cryptography-based standards.

The Secretary of Commerce made FIPS 140-1 mandatory and binding for U.S. Government agencies and organizations. The standard is specifically applicable when a federal agency determines that cryptography is necessary for protecting sensitive information. The standard is used in designing and implementing cryptographic modules that federal departments and agencies operate or are operated for them. FIPS 140-1 is applicable if the module is incorporated in a product, application, or functions as a standalone device.

From the beginning, the CMVP has been dynamic with a constant reexamination of the underlying standard, test methodology, reporting structure, and associated documentation. In addition, questions from the vendor and user communities have provided valuable input and an implementation perspective. NIST and CSE have continually kept pace with new security methods, changes in technology, and required interpretations of the standard by issuing official *Implementation Guidance* for FIPS 140-1 and associated *Derived Test Requirements* (DTR). The *Implementation Guidance* covers program policy, technical questions, and general guidance needed for module validation.

In addition to constant reexamination, the standard is officially reexamined and reaffirmed every five years. In the fall of 1998, FIPS 140-1 entered a regularly scheduled five-year review to consider new and/or revised requirements needed to meet technological and economic change. A request for comments on FIPS 140-1 was published on October 23, 1998, in the *Federal Register*. The official comment period for the request closed January 21, 1999. A revised draft standard was produced based on the public comments received, previously issued implementation guidance, and a line-by-line review by the NIST, CSE, and testing laboratory staff. A second request for comments on the resulting FIPS 140-2 draft was published on November 17, 1999, in the *Federal Register* with a closing date of February 15, 2000. In December 2000, the FIPS 140-1 update to FIPS 140-2 was completed. The implementation schedule for FIPS 140-2 begins with the approval date of May 25, 2001. One year after the approval date (May 25, 2002), modules will no longer be tested against FIPS 140-1. However, FIPS 140-1 validated modules may continue to be procured. (Note: All FIPS 140-1 testing laboratories will become FIPS 140-2 testing laboratories.)

Summary of Differences Between FIPS 140-1 and FIPS 140-2

FIPS 140-1 is one of NIST's most successful standards and forms the very foundation of the CMVP. FIPS 140-1 is widely recognized as the "defacto" standard for cryptographic modules and is referenced and/or used in its entirety by numerous standards bodies and international testing organizations. Therefore, great care was given to the update process beginning with a complete line-by-line review and examination of the standard and all *Implementation Guidance* issued during the initial five years of FIPS 140-1. The underlying question asked by the authors of FIPS 140-2 was "How does one improve a successful and proven standard?" The answer was simple – include lessons learned from ques-

tions and comments, reflect changes in technology, and strengthen the standard, but do not change the focus or emphasis. The authors also improved the format of the standard by minimally restructuring the content (see table below), standardizing the language and terminology to add clarity and consistency, removing redundant and extraneous information to make the standard more concise, and revising or removing vague requirements. Looking to the future, the authors added a section detailing new types of attacks on cryptographic modules that currently do not have specific testing available. The result is a stronger, more concise, and readable standard that still embodies the spirit of the original standard.

The following provides a brief discussion of each of the requirements areas and a summary of the major changes.

1.1. Security Requirements

This section summarizes the changes from FIPS 140-1 to FIPS 140-2.

1.1.1. Cryptographic Module Specification

This section defines those requirements for identifying and establishing the cryptographic boundary of the module. This includes the specification of the hardware, software, and/or firmware; the module interfaces; manual or logical controls; identification of the implemented algorithms and modes of operation; and the module's security policy.

The primary modification to this section is the inclusion of the approved cryptographic algorithms and security functions. FIPS 140-1 separated the algorithm identification into a short standalone section. However, given that the cryptographic algorithm is the basis of the module, inclusion of the algorithm specification in the first section of FIPS 140-2 was a logical restructuring.

1.1.2. Cryptographic Module Ports and Interfaces

This section defines the requirements used to restrict information flow and physical access to the logical interfaces for all entry and exit points both internal and external to the module. The standard defines four specific logical interfaces including data input, data output, control input, and status output, and the associated requirements by security level.

Tables of Content

FIPS 140-1	FIPS 140-2
1. Overview	1. Overview
2. Glossary of Terms and Acronyms	2. Glossary of Terms and Acronyms
3. Functional Security Requirements	3. Functional Security Requirements
4. Security Requirements	4. Security Requirements
4.1 Cryptographic Modules	4.1 Cryptographic Module Specification*
4.2 Cryptographic Module Interfaces	4.2 Cryptographic Module Ports and Interfaces
4.3 Roles and Services	4.3 Roles, Services, and Authentication*
4.4 Finite State Machine Model	4.4 Finite State Model
4.5 Physical Security	4.5 Physical Security*
4.6 Software Security	4.6 Operational Environment*
4.7 Operating System Security	4.7 Cryptographic Key Management
4.8 Cryptographic Key Management	4.8 EMI/EMC
4.9 Cryptographic Algorithms	4.9 Self-Tests*
4.10 EMI/EMC	4.10 Design Assurance*
4.11 Self-Tests	4.11 Mitigation of Other Attacks*
Appendixes	**Appendixes**
A: Summary of Documentation Requirements	A: Summary of Documentation Requirements
B: Recommended Software Development Practices	B: Recommended Software Development Practices*
C: Selected References	C: Cryptographic Module Security Policy*
	D: Selected Bibliography*

** Section added or significantly revised.*

The major change in this section involves the underlying requirement for plaintext input/output (I/O) to be separated from other types of I/O. FIPS 140-1 met this requirement by specifying the use of physically separate ports beginning at security level 3 for plaintext I/O. Due to changes in technology (e.g., timing separation, dedicated threads, multiplexing, etc.), the standard now allows both physically separate ports and logical separation within existing physical ports via trusted path.

1.1.3. Roles, Services, and Authentication

This section is divided into three subsections covering the requirements for the authorized operator roles: services, functions and operations provided by the modules, and the authentication needed to obtain these services.

The major modification to this section is the addition of strength of mechanism requirements for authentication. This represents a strengthening of the standard and the first time the concept of strength of mechanism has been specified. These new requirements address minimum probabilities for guessing authentication data (e.g., pins, passwords, etc.), false acceptance error rates, and restrictions placed on the feedback of authentication data to the user.

1.1.4. Finite State Model

This section specifies the underlying design requirements for the identification and specification of the module's operational and error states and associated transitions between states. The name of this section was changed from Finite State Machine (FSM) to Finite State Model to more accurately

reflect the requirements. FIPS 140-1 mandated the use of an FSM Model in the module's design. The FSM is often associated with hardware design and development. To better represent both hardware and software modules, this section now includes the concept of utilizing a Finite State Model or an equivalent design methodology.

1.1.5. Physical Security

This section details all of the requirements surrounding the physical security of the cryptographic module. Cryptographic modules are separated into three different embodiment categories: single chip, multi-chip embedded, and multi-chip standalone.

The majority of changes to this section involve a reorganization of the subsections that define the requirements for the three different module embodiments. FIPS 140-1 was structured with a separate section of requirements for each of three module embodiments, plus a subsection detailing the Environmental Failure Protection (EFP)/Environmental Failure Testing (EFT) requirements for security level 4. For consistency and clarity, FIPS 140-2 moves all of the redundant requirements from the three embodiments into a general section defining requirements applicable to all. The requirements that are unique to each of the embodiments follow the general section concluding with EFP/EFT. In addition to the restructuring, new requirements were added for single chip and multi-chip embedded modules to allow the use of physical enclosures for the protection of the module.

1.1.6. Operational Environment

This section details the requirement specific to modules where an operator can load and execute software or firmware that was not included as part of the module validation. An example of a cryptographic module for which the operational environment requirements apply is a general-purpose computer running cryptographic software as well as untrusted user-supplied software (e.g., a spreadsheet or word processing program). In this case, the hardware, operating system, and cryptographic software are considered part of the module. FIPS 140-2 relies on an evaluated operating system to mitigate part of the security concerns over "Trojan Horse" attacks, where the user-supplied software or firmware can access, obtain, or corrupt the module's critical security parameters (e.g., cryptographic keys, passwords, etc.).

The major modification to this section was the replacement of criteria for evaluating operating systems. FIPS 140-1 required evaluated operating systems that referenced the Trusted Computer System Evaluation Criteria (TCSEC) classes C2, B1, and B2. The TCSEC is no longer in use and has been replaced by the Common Criteria. Consequently, FIPS 140-2 now references the *Common Criteria for Information Technology Security Evaluation* (CC), ISO/IEC 15408:1999.

1.1.7. Cryptographic Key Management

This section contains the security requirements for cryptographic key management that encompasses the entire lifecycle of the cryptographic keys used by a cryptographic module. This includes random number generation, key generation, establishment, entry/output, storage, and zeroization. The requirements are applicable to modules that implement secret key and/or public key algorithms.

The major modification to this section was the addition of requirements for Over-The-Air-Rekeying (OTAR) for radio communication modules. Other modifications included clarification of the deterministic and nondeterministic random number generators (RNGs) subsection to allow RNGs approved for classified processing for use in key generation; addition of strength of mechanism requirements in the Key Establishment subsection; and the deletion of the Key Archive subsection.

1.1.8. Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC)

This section specifies the Federal Communications Commission (FCC) requirements applicable to cryptographic modules. These requirements are specific to the module's ability to operate in a manner that does not interfere electromagnetically with other devices. Requirements necessary to mitigate cryptographic attacks based on electromagnetic emanations (TEMPEST) are not included in this section. The Mitigation of Other Attacks section of the standard contains the requirements related to TEMPEST attacks. During the update process, the EMI/EMC section was modified to reflect minor changes in FCC requirements and references.

1.1.9. Self-Tests

This section provides the requirements necessary to ensure that the module is functioning properly. Self-testing is required at both module power-up and when specific conditions are met. These tests include public/private key generation, software/firmware loading, manual key entry, random number generation, and cryptographic bypass (plaintext in, plaintext out).

The update to the standard resulted in no dramatic change in scope or format for self-test requirements; however, previously issued guidance was included. The major changes in the Self-Test section were strengthening the required tests and better addressing the bypass mode of operation. To strengthen the requirements, the new standard now mandates all four statistical random number generator tests. FIPS 140-1 only required one of the four. Further, the statistical limits for passing these tests were tightened to provide additional assurance for random number generation. Public comments recommended that the Self-Test section better address modules (i.e., routers) that are designed to automatically switch between bypass and secure mode (plaintext in, ciphertext out). This was accomplished by including requirements specific to the secure operation of the module during the switch between modes. These new requirements facilitate the underlying requirement of fail-secure,

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message **HELP**. To have the bulletin sent to an e-mail address other than the From address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov.

where plaintext information is not released inadvertently. In addition, FIPS 140-1 tested bypass capabilities only at module power-up. The new standard moves bypass to the conditional testing area.

1.1.10. Design Assurance

The Design Assurance section, which was formerly Software Security in FIPS 140-1, defines the requirements for configuration management, delivery and operation, development and guidance documents. The intent of this section is to provide security assurance from design and development of the module through delivery and initial start-up.

Originally this section only specified requirements for software, but to provide greater security assurance, the section has now been expanded to address software, hardware, and firmware. Though the entire section was rewritten, the consolidated design assurance requirements found in FIPS 140-1 form the base. These requirements included reviews of source code, functional specifications, and formal modeling. Requirements new to the standard include configuration management, correct delivery and start-up, and mandatory guidance documents for users and cryptographic officers.

1.1.11. Mitigation of Other Attacks

This section is the first new section of the standard and provides information, recommendations, and requirements for several new types of cryptographic attacks. Susceptibility to these attacks depends on module type, implementation, and implementation environment. These attacks are of particular concern for cryptographic modules implemented in hostile environments or where the attackers may be the users of the module. Generally, these types of attacks rely on the analysis of information obtained from sources physically external to the module. In all cases, the attacks attempt to determine some knowledge about the cryptographic keys and critical security parameters (CSPs) contained in the module.

This section was developed as a direct result of numerous public comments recommending that power analysis, timing analysis, fault induction, and TEMPEST attacks be addressed by FIPS 140-2. Certain types of cryptographic modules may be susceptible to these attacks (e.g., tests for power analysis, timing analysis, and fault induction), but testable security requirements were not available at the time this standard was issued or the attacks were outside of the scope of the standard (e.g., TEMPEST attacks). The new standard specifies that if a cryptographic module is designed to mitigate one or more specific attacks, then the module's security policy shall specify the security mechanisms employed by the cryptographic module to mitigate the attack(s). The existence of these mechanisms and their proper functioning will be validated when requirements and associated tests are developed. Brief summaries of currently known attacks are provided in the standard.

1.1.12. Appendixes

FIPS 140-1 contains three appendixes, A, B, and D below. Appendix C has been added to FIPS 140-2.

A. *Summary of Documentation Requirements*

This section was updated to reflect modifications in the standard.

B. *Recommended Software Development Practices*

This section was updated to reflect current practices.

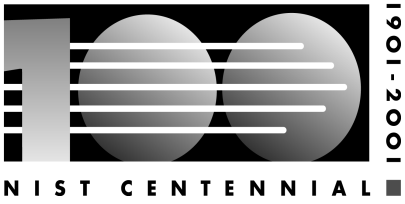
C. *Security Policy*

Appendix C specifies the information and structure of the required cryptographic module security policy. This document is available by request and often provides the only information users have access to prior to purchasing the module. FIPS 140-1 required a security policy, which contained the security rules of the module. However, no format or specific content requirements were mandated. Therefore, cryptographic module security policies submitted by vendors often varied greatly in detail and quality. FIPS 140-2 mandates more stringent requirements for both the contents of a security policy and the structure. The vendors now must provide information concerning the identification and authentication, access control, and physical security mechanisms, and any mechanisms implemented for mitigation of other attacks. Two types of security policies may exist: a proprietary security policy used by the testing laboratory to perform necessary tests and a required non-proprietary version, which is available to public release.

D. *Selected Bibliography*

This section was updated to reflect current standards and documents.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.



U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8901
Gaithersburg, MD 20899-8901