Frequently Asked Questions
for the
Cryptographic Module Validation Program

National Institute of Standards and Technology
Communications Security Establishment

Initial Release: April 25, 2003

Last Update: December 04, 2007

New FAQ's and Modified FAQ's (Issued within the last 45 days)

- **12-04-07** Added addition detail regarding removal of FIPS waiver provision: Use of Unvalidated Cryptographic Modules by Federal Agencies and Departments
- **11-30-07** Added text: "A non-compliance change to a validation will be posted in the CMVP Notices." in section What process does the CMVP follow if informed by 3rd parties regarding module non-compliance issues?
- **10-18-07** Updated links
- **06-06-07** Minor editorial modification in Section 5.1: How do the four security levels of cryptographic modules correlate to the three risk-impact levels required by FIPS 199 and the minimum security controls in FIPS 200 and 800-53?.
- **12-08-06** Numerous editorial changes and clarifications.
- **08-24-06** What are the differences between the four cryptographic module security levels?
- **08-24-06** How do the four security levels of cryptographic modules correlate to the three risk-impact levels required by FIPS 199 and the minimum security controls in FIPS 200 and 800-53?

Table of Contents

1. OVERVIEW

What is the purpose of the CMVP?

On July 17, 1995, the National Institute of Standards and Technology (NIST) established the Cryptographic Module Validation Program (CMVP) that validates cryptographic modules to Federal Information Processing Standards (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.

FIPS 140-2, *Security Requirements for Cryptographic Modules,* was released on May 25, 2001 and supersedes FIPS 140-1. **However, agencies may continue to purchase, retain and use FIPS 140-1 validated modules after May 25, 2002.** Modules validated as conforming to FIPS 140-1 and FIPS 140-2 are accepted by the Federal Agencies of both countries for the protection of sensitive information. However, a federal agency may choose to only procure a FIPS 140-2 validated module. Vendors of cryptographic modules use independent, accredited Cryptographic Module Testing (CMT) laboratories to test their modules. The CMT laboratories use the *Derived Test Requirements [DTR] for FIPS PUB 140-2, Security Requirements for Cryptographic Modules* and *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program* to test cryptographic modules against FIPS 140-2. NIST's Computer Security Division and CSE jointly serve as the Validation Authorities for the program, validating the test results. Standards applicable to the CMVP, Notices and Announcements, CMT contacts, NIST and CSE contacts and the listings of validated cryptographic modules can be found at the CMVP website: www.nist.gov/cmvp Shown below in **Figure 1** is a summary of the CMV process:

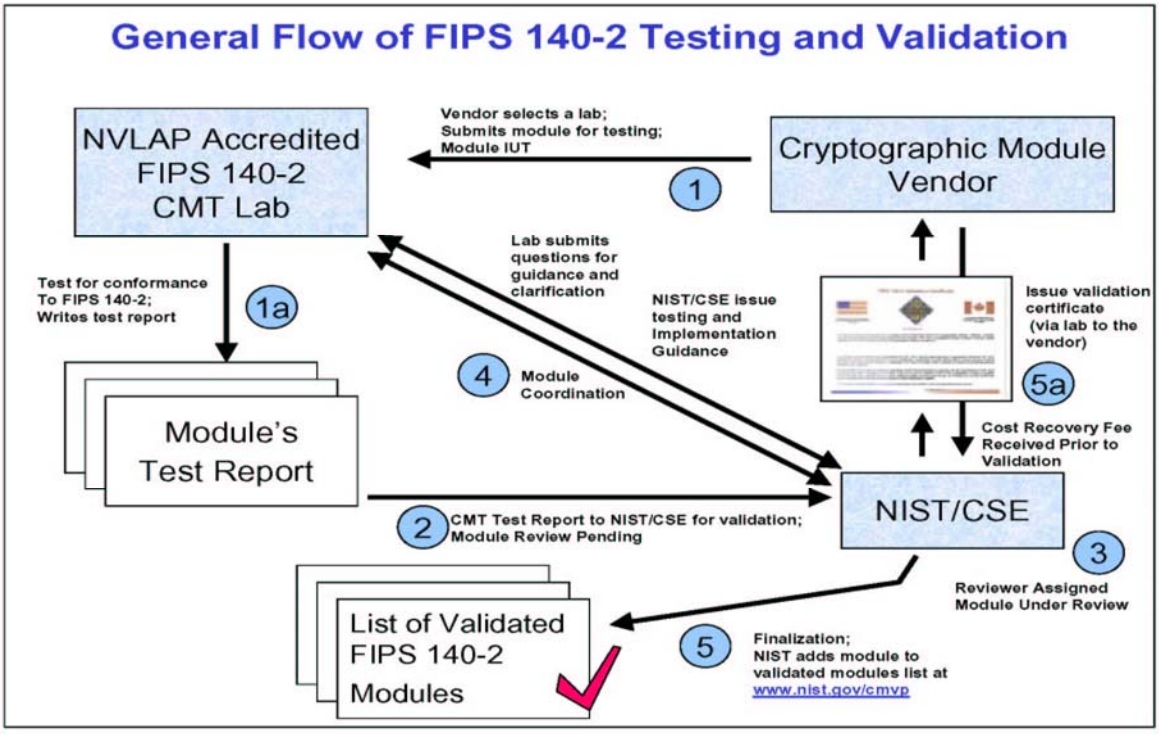


Figure 1: Cryptographic Module Validation Process

A cryptographic module must implement at least one Approved Security Function. The list of FIPS-approved or NIST-recommended security functions are available in *Annex A: Approved Security Functions for FIPS 140-2, Security Requirements for Cryptographic Modules*.

What are FIPS PUBs?

FIPS PUBs are Federal Information Processing Standards (FIPS) Publications (PUBs). FIPS PUBs are issued by NIST. The NIST FIPS PUBS related to cryptographic modules and cryptographic algorithms are used as the framework for the CMVP.

With the passage of the Federal Information Security Management Act of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards.

2. INTRODUCTION TO THE CRYPTOGRAPHIC MODULE VALIDATION PROGRAM (CMVP)

2.1 I AM A CUSTOMER

This Is my first time working with FIPS 140-1 and FIPS 140-2, the CMVP, or this FAQ. What do I need to know?

First, become familiar with FIPS and CMVP - a brief description of each is provided in Section 1.

This Frequently Asked Questions (FAQ) is laid out from high-level to detailed. The first two sections in this FAQ contain high level information aimed towards individuals who aren't familiar with the CMVP, FIPS 140-2, or this FAQ.

- Part 1: Overview: This section provides an overview of the Cryptographic Module Validation Program (CMVP) and how CMVP addresses the needs of U.S. and Canadian governments.
- Part 2: Introduction to the CMVP**:** This section offers information on how to use the FAQ and lists web sites for those who would like to learn more detailed information about topics addressed in this FAQ.
- Part 3: General CMVP Information**:** This section gives an overview of the CMVP, cryptographic modules, cryptographic algorithms, and the applicable standards. Part 3 also includes the roles of the participants in the CMVP, including customers.
- Part 4: Standards**:** This section gives an overview of the following: a) the current Cryptographic Module and Cryptographic Algorithm standards that are available, b) a brief overview of the content of each standard and c) the status of each standard.
- Part 5: Cryptographic Module Validation: This section provides a brief overview of the security requirements that must be met by each cryptographic module that is submitted to a CMT laboratory for conformance testing. Included are: FIPS 140-2, *Security Requirements for Cryptographic Modules*, the Implementation Guidance and the Derived Testing Requirements (DTR) for the standard. Each subsection includes an overview and specific vendor requirements.

- Part 6: Cryptographic Algorithm Testing: This part describes the Cryptographic Algorithm Testing. Topics include the purpose of algorithm testing, deterministic and non-deterministic random number generators (RNGs) and references to FIPS and Special Publications (SPEC PUBs) that describe, in detail, the algorithm tests.
- Part 7: Revalidation: This section discusses revalidating a cryptographic module if a change has been made to a previously validated cryptographic module. This includes a FIPS 140-1 validated cryptographic module that is submitted to a CMT laboratory for FIPS 140-2 revalidation.
- Part 8 Reference material: This Section includes a list of acronyms, a glossary, and a list of references and useful web sites.

Where can I find a list of FIPS 140-1 and FIPS 140-2 validated cryptographic modules?

The list of FIPS 140-1 and 140-2 validated cryptographic modules can be found on the NIST web site at http://csrc.nist.gov/groups/STM/cmvp/validation.html or CSE web site at http://www.cse-cst.gc.ca/en/services/industrial_services/cmv_val_products.html.

Can FIPS 140-1 validated cryptographic modules still be used and still meet the regulatory requirements?

Yes; cryptographic modules validated against FIPS 140-1 are still valid. However, as of May 26, 2002 all cryptographic modules submitted to the CMT laboratories will be tested against FIPS 140-2, only.

Are all IT security features tested by a CMT lab?

No. Cryptographic modules are tested for conformance against the requirements in FIPS 140-2, which specifically focuses on requirements for cryptographic modules.

Does the validation certificate of a cryptographic module expire?

No, the validation for a cryptographic module remains effective unless a change is made to the cryptographic module. (The life cycle of some modules, such as software modules, may be as short as 3 to 9 months before a revision. Therefore setting an expiration date is unnecessary.) See Part 7: Revalidation.

How can a cryptographic module's validation be verified?

To verify a cryptographic modules' validation certificate, refer to http://csrc.nist.gov/groups/STM/cmvp/validation.html. To see the status of cryptographic modules currently in the Modules In Process list, refer to http://csrc.nist.gov/groups/STM/cmvp/inprocess.html.

Commonly used conformance claims

A vendor makes the following claims of conformance to FIPS 140-1 or FIPS 140-2. Are they acceptable?

- The module has been designed for compliance to FIPS 140-2. <no>

- Module has been pre-validated and is on the CMVP pre-validation list. <no>
- The module will be submitted for testing. <no>
- The module has been independently reviewed and tested to comply with FIPS 140-2. <no>
- The module meets all the requirements of FIPS 140-2. <no>
- The module implements FIPS Approved algorithms; including having algorithm certificates. <no>
- The module follows the guidelines detailed in FIPS 140-2. <no>

- The module has been validated and has received Certificate #495. <yes>

A cryptographic module does not meet the requirements or conform to the FIPS 140-1 or FIPS 140-2 standard unless a reference can be made to the validation certificate number. The module used must also be the same version/part number as annotated on the validation certificate. Any other claims are not relevant.

Making a Difference …

In an initial survey of the CMT Laboratories of the first 164 cryptographic modules and 332 algorithm validations that were validated; the question was asked if the CMVP testing and standards revealed any underlying flaws in *completed ready to market* modules that were submitted for testing. The results:

- **164 Cryptographic Modules Surveyed (during testing)**
  - 80 (48.8%) Security Flaws discovered
  - 158 (96.3%) Documentation Errors

- **332 Algorithm Validations (during testing)**
  (DES, Triple-DES, DSA and SHA-1)
  - 88 (26.5%) Security Flaws
  - 216 (65.1%) Documentation Errors

As a result of the CMVP testing, the ***quality*** of these modules were dramatically improved. What if they had been deployed without testing and validation?

I am looking for a validated module – where do I start?

A familiarity with FIPS 140-2 is needed to determine what the different security levels provide and what attributes are relevant (eg. Approved mode of operation, operational environment, etc). For example the physical environment the module is to be deployed will in many cases determine what the appropriate security level should be. In a high-risk environment where the module must provide its own protection of the internal security parameters, higher levels of physical protection may be required. However, if the environment where the module is to be deployed offers a level of adequate protection, then the module itself may not need to provide that. In those cases a Level 1 module may be very adequate.

Based on review of FIPS 140-2, the CMVP FAQ (this document) and Implementation Guidance, the minimum attributes of the module will emerge. Attributes will also include what algorithms (eg.

AES, RSA, etc), key loading methods, operating systems, software/hardware, etc. are necessary for the manner in which it is to be deployed.

Now the search begins. The CMVP provides both the HTML validation list and the underlying Microsoft access database. The database can be downloaded and used for more sophisticated searching based on the minimum attributes one may require in a module. Once a set of modules is identified, then the vendors can be contacted to discuss what solutions, products, applications they offer which utilize the validated cryptographic modules.

A vendor is selling me a crypto solution – what should I ask?

Verify with the vendor that the application or product that is being offered is either a validated cryptographic module itself (e.g. VPN, SmartCard, etc) or the application or product uses an embedded validated cryptographic module (toolkit, etc). Ask the vendor to supply a signed letter stating their application, product or module is a validated module or incorporates a validated module, the module provides all the cryptographic services in the solution, and reference the modules validation certificate number. The certificate number will provide reference to the CMVP list of validated modules. Each entry will state what version/part number/release is validated, and the operational environment (if applicable) the module has been validated. The information on the CMVP validation entry can be checked against the information provided by the vendor and verified that they agree. If they do not agree, the vendor is *not* offering a validated solution. If a software module is used, there is guidance on how the module can be ported to similar operational environments and maintain the validation. This is found in FIPS 140-2 IG **G.5**.

The Security Policy the vendor provided as part of the modules validation will provide information on how to operate the module in a FIPS Approved mode of operation. That is the only mode of operation a module may be operated in if a US Federal user. Some modules may only have one mode of operation, which is the FIPS Approved mode. There will be a caveat on the front of the validation certificate indicating if a module has both an Approved and non-Approved modes. If there is no caveat, then the module only has an Approved mode. There may be other caveats on the front of the certificate that also identifies how the module may only operate or needs to be configured in a FIPS Approved mode.

If the module is a software module, and it was tested and validated with the Operational Environment meeting Level 2, the module must operate on the evaluated operating system indicated on the certificate. Many evaluated operating systems also specify a limited or unique platform that the operating system was evaluated. If so, then that is the only platform or platform that the evaluation of the operating system is valid, and therefore the only platform or platforms the FIPS 140-2 validation is valid. The operating system evaluation may specify extensibility for running on different platforms. That information can only be found in the operating system evaluation test report which is not part of the CMVP testing and validation. If a vendor wishes to claim alternate platforms or operating systems that the validated module can operate in a validated manner, they can update the Security Policy provided to the CMVP, and have this updated on the CMVP validation list. The CMVP will review the changes, and if acceptable, will post the new Security Policy. Therefore if the platform or operating system is not identified on the module validation certificate, ask the vendor to update the Security Policy as needed and submit this to the CMVP. FIPS 140-2 IG **G.5** addresses porting of both Level 1 and Level 2 software modules.

If the module incorporates an open source distribution methodology for module build, is there any additional information that should be requested?

As suggested in the prior FAQ entry (*A vendor is selling me a crypto solution – what should I ask?*), if the module wishing to be procured has been created or built using an open source distribution methodology, the agency should also request in a signed letter from the application developer or vendor of the module (or product or application which the module is embedded within) to assert that the module was created or built as specified on the validated modules validation certificate. Any deviation from what is provided on the validation certificate will not create a validated module. As before, requesting such a letter of affirmation will provide an agency with audit information to provide if itself is audited by the agencies Inspector General or the GAO regarding compliance to the mandatory statutory requirements of FIPS 140-2.

2.2 I AM A VENDOR

This is my first introduction to FIPS 140-1, FIPS 140-2, the CMVP or this FAQ. What do I need to know?

See this same question in Section 2.1.

Additional information on the CMVP program can be found at NIST CMVP or CSE CMVP websites.

2.2.1 I am a vendor looking for requirements information

Why should I be concerned about getting my cryptographic modules validated to FIPS 140-2?

If a vendor sells a product to the US Federal Government that includes a cryptographic module for the protection of sensitive data, the cryptographic module must be FIPS 140-1 or FIPS 140-2 validated. Data provided by the CMT laboratories from the first 164 validated modules shows that approximately 50% of the cryptographic modules submitted to the laboratories for testing had a security flaw. For cryptographic algorithms, over 25% of the FIPS-approved algorithms that are tested are incorrectly implemented. Also, the Government of Canada recommends that Canadian Federal Departments use FIPS 140-1 and FIPS 140-2 validated cryptographic modules. Second, by having your cryptographic module validated, you are showing potential customers that your cryptographic module implements a minimum baseline suite of IT security and cryptography features. Third, FIPS 140-1 and FIPS 140-2 are the *de facto* international standards for cryptographic modules.

How do I find the specific requirements for functionality that must be implemented?

The CMVP offers a documented methodology for conformance testing through a defined set of security requirements in FIPS 140-2 and other cryptographic standards. The best way to identify the specific functional and assurance requirements that must be addressed by a cryptographic module is to review the Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules. NIST developed the Derived Test Requirements (DTR) for FIPS 140-

2 to ensure repeatability of tests and equivalency in results across the testing laboratories. The DTR lists all the requirements for a cryptographic module and the associated vendor requirements (VEs) and tester requirements (TEs). In addition, review the applicable algorithm standards and algorithm tests. The information is included in FIPS PUBs and SPEC PUBs.

If I require a FIPS 140-2 or DTR interpretation, where can I find guidance?

There is currently an Implementation Guidance (IG) document for FIPS PUB 140-1 and an IG for FIPS PUB 140-2.

The IGs include CMVP policy and decisions regarding the interpretation of specific requirements within the FIPS 140-1 and FIPS 140-2. The IG was developed, and continues to be updated, based on questions submitted by CMT labs, vendors, and Federal Agencies. The CMVP staff responds to specific questions on a case by case basis and, if appropriate, develops more generalized guidance to be included into the IGs.

The IG for FIPS 140-1 can be found on CMVP web site at http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-1/FIPS1401IG.pdf. The IG for FIPS 140-2 can be found on CMVP web site at http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf.

Can I incorporate another vendor's validated cryptographic module?

Yes. A cryptographic module that has already been issued a FIPS 140-1 or FIPS 140-2 validation certificate may be incorporated or embedded into another product. The new product may reference the FIPS 140-1 or FIPS 140-2 validated cryptographic module so long as the new product does not alter the original validated cryptographic module. A product which uses an embedded validated cryptographic module cannot claim itself to be validated; only that it utilizes an embedded validated cryptographic module.

There is no assurance that a product is correctly utilizing an embedded validated cryptographic module – this is outside the scope of the FIPS 140-1 or FIPS 140-2 validation.

What is the result of loading additional non-validated applications within a FIPS validated cryptographic module?

Any non-validated applications subsequently loaded and executed within a FIPS 140-1 or FIPS 140-2 validated cryptographic module invalidates the original validation.

Does FIPS 140-2 apply only to hardware cryptographic modules?

No. The precursor to FIPS 140-1 was primarily intended for conformance testing of hardware cryptographic modules. FIPS 140-1 included more requirements for software modules and FIPS 140-2 applied the requirements to all types of cryptographic modules. Therefore, FIPS 140-2 applies to *any* cryptographic module, whether implemented in hardware, software, firmware, or some combination. For example, a *hybrid* module is a combination of software and hardware.

Does the proprietary information about a cryptographic module remain confidential?

Yes. All information about a cryptographic module remains confidential within a CMT laboratory and the CMVP. The CMT laboratories typically sign Non-Disclosure Agreements (NDAs) with product vendors.

The laboratories accreditation with NVLAP extends this non-disclosure to the CMVP. The CMVP protects all information provided in the validation reports submitted by the CMT laboratories in a secure manner to prevent the disclosure of the information contained within the report.

2.2.2 I am a vendor looking for CMT laboratory information

Which are the accredited CMT Laboratories?

A list of accredited CMT labs is located on the NIST CMVP web page.

How long does it take, and how much does it cost to get my cryptographic module tested?

A fee is charged by the CMT laboratories for the testing of a cryptographic module. Testing time is variable, depending on the complexity of the cryptographic module, the overall security level and the individual security levels, and the completeness of the documentation evidence package. The test time varies depending on the following factors:

a) Cryptographic module type – e.g.,. software, firmware, hardware, single vs. multi-function;
b) Overall security level of the cryptographic module – 1, 2, 3, or 4;
c) Accuracy and completeness of documentation; and
d) The number of deficiencies identified by a CMT laboratory during the conformance testing process.

If a cryptographic module is being revalidated or if a new version based on a previously validated cryptographic module is being validated, the cost and time, typically, are less. NIST and CSE do not get involved in the contract negotiations between the vendor and a CMT lab. This is to ensure the independence of the validation authorities.

Quotes or estimates can be obtained from the CMT laboratories**.**

A cost recovery fee is also charged by NIST for the validation of cryptographic modules.

What is cost recovery?

Cost recovery is a fee provided to NIST by product vendors. A nominal fee is charged to cover the validation authority costs for the validation tasks and the program management responsibilities performed by NIST. No profit is made from this fee by NIST.

How does cost recovery work?

Billing information is provided to NIST when a new test report is submitted by the CMT laboratory. Upon receipt, NIST billing prepares an invoice and submits it to the billing contact provided. The funds should be remitted prior to the validation and posting of the certificate.

A validation certificate will be issued for a validation report submitted to NIST pending receipt of payment of the cost recovery fee. If the cost recovery fee is not received within 60 days of posting of the validation, the validation will be *suspended* by the CMVP. If the cost recovery fee is not received within 90 days of posting of the validation, the validation will be *revoked* by the CMVP. After revocation, the module may be resubmitted to the CMVP as a new test report to be reconsidered for validation

In addition, if payment is 60 days (75 days if foreign) past due, NIST billing will proceed with sending dunning letters, assessing interest charges, administrative charges, penalty charges, and if necessary, refer to the Department of the Treasury for collection assistance.

For billing inquiries contact NIST Billing Information: 301-975-3880.

An Extended fee is applicable when a validation test report requires significant additional effort by the validators. A number of factors may lead to the application of the Extended fee for a test report that is received by the CMVP from the testing CMT Laboratory. For example: the test report review uncovered a non-compliance to the standard that was not identified by the CMT Laboratory; a test report is received incomplete (Refer to FIPS 140-2 IG G.2) and this is determined once the report has moved to IN REVIEW; the quality of the received test report is unacceptable; or the review and COORDINATION took significant additional effort. The CMVP may impose the Extended fee for a particular report on other specific conditions as applicable.

The fee varies by overall Security Level. The schedule of fees can be found at the CMVP Notices.

Fees are not charged for letter revalidation or revalidations with less than 30% of the security-relevant operational requirements are modified.

The extended fee is applicable to all report submission under FIPS 140-2 IG G.8.

Can my cryptographic module fail some of the requirements during the testing process?

Yes, it is possible for a cryptographic module to fail one (or more) assertions during the testing process. The CMT laboratories work with the vendor to resolve all discrepancies that arise. The CMT laboratory should only submit validation reports to the Validation Authorities that do not contain any failed test assertions.

If during the CMVP review of a submitted test report a non-compliance is determined, the module will be returned to IUT status until the laboratory and vendor correct the issue. This may involve re-engineering of the module and subsequent re-testing by the CMT Laboratory.

If non-compliance is determined, the NIST extended cost recovery fee is automatically imposed.

What if a CMT laboratory is testing cryptographic modules from competing cryptographic vendors?

All CMT laboratories take great care to protect a company's proprietary information. Generally, a CMT laboratory signs a non-disclosure agreement (NDA) with each vendor, and would never disclose information regarding a cryptographic module to an outside organization other than the validation authorities.

CMT laboratories are required to meet the specific laboratory accreditation requirements specified in Handbook 150-17, *Cryptographic Module Testing* to maintain their laboratory accreditation, which also specifies criteria for the maintenance of confidentiality of proprietary information.

Can my in-house CMT laboratory test my own cryptographic modules?

No it cannot. The guidelines of accreditation of a CMT laboratory specify that a laboratory owned by a vendor cannot test cryptographic modules developed by the vendor. In addition, the CMVP requires that a CMT laboratory that provides engineering design support to a vendor may not also test that cryptographic module.

What if I do not want to develop the required documentation myself?

If you do not want to develop the validation evidence documentation, the CMT laboratories and some consulting companies can perform this task for you. If a CMT laboratory develops the documentation (but does not design the cryptographic module) the CMT laboratory may also test the cryptographic module. Guidelines can be found in FIPS 140-2 IG G.4.

3. GENERAL CMVP INFORMATION

3.1 STANDARDS OVERVIEW

Which cryptographic module and cryptographic algorithm standards are included in the CMVP?

The CMVP issues validation certificates for cryptographic modules against FIPS PUB 140-1 and FIPS PUB 140-2. FIPS 140-2 superseded FIPS 140-1 on May 26, 2002 and now all new validations are completed against FIPS 140-2 only. The CMVP also issues validation certificates for the FIPS-Approved algorithms that are embodied within a cryptographic module.

FIPS 140-2 has four additional annexes that list the Approved Security Functions, Approved Protection Profiles, Approved Random Number Generators, and Approved Key Establishment Techniques.

- Annex A: Approved Security Functions,
- Annex B: Approved Protection Profiles,
- Annex C: Approved Random Number Generators, and
- Annex D: Approved Key Establishment Techniques.

Additional information on Cryptographic Module validations can be located in Section 5. Additional information on Cryptographic Algorithm validations can be located in Section 6.

3.2 APPLICABILITY

What is the applicability of CMVP to the US government?

FIPS 140-1 became a mandatory standard for the protection of sensitive data when the Secretary of Commerce signed the standard on January 11, 1994. The applicability statement from FIPS 140-2 (page iv):

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

What is the applicability of CMVP to the Government of Canada?

The Government of Canada (GoC) recommends that Federal Departments purchase CMVP validated cryptographic modules. The validated cryptographic modules are available through the Communications Security Establishment (CSE). A list of validated cryptographic modules is available at the following web site: http://www.cse-cst.gc.ca/en/services/industrial_services/cmv_val_products.html

Which cryptographic algorithms are acceptable for use by the Government of Canada Federal Departments and Agencies?

The list of GoC approved cryptographic algorithms is available at http://www.cse-cst.gc.ca/en/services/crypto_services/crypto_algorithms.html

Does FIPS 140-2 apply to other countries besides Canada and the US?

The CMVP can apply to any government department, although it is only current formally accepted by the U.S., Canadian, and U.K. governments. Currently, several CC Protection Profiles require FIPS 140-1 and 140-2 validated cryptographic modules. These PPs have been developed by many organizations throughout the world. Using FIPS 140-2 validated cryptographic modules will ensure that the product has implemented the FIPS approved/NIST recommended cryptography correctly.

Does the CMVP apply to the private sector?

The use of FIPS 140-2 validated cryptographic modules is not mandatory for the private sectors in the U.S., Canada, or the U.K. However, many private sector organizations require the use of FIPS 140-2 validated cryptographic modules to conform to a minimum baseline of security functionality. Also, the cryptographic module has independently been reviewed and tested, reducing the likelihood that flaws have been inadvertently implemented within the cryptographic module.

If a private company intends to conduct business with the U.S. Federal Government, the use of FIPS 140-2 validated crypto modules is mandatory.

Does the CMVP apply to classified information?

Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against FIPS 140-1 or FIPS 140-2.

NSA's Information Assurance Directorate has a DoD/Military Customer Relations Division and a Civil Agencies Customer Relations Division. Questions regarding Information Assurance questions can be directed to those contacts.

DoD/Military Customer Relations Division: 410-854-4391
Civil Agencies Customer Relations Division: 410-854-4790

Use of Unvalidated Cryptographic Modules by Federal Agencies and Departments

FIPS 140-2 precludes the use of unvalidated cryptography **for the cryptographic protection** of sensitive or valuable data within Federal systems. Unvalidated cryptography is viewed by NIST as providing **no protection** to the information or data – in effect the data would be considered unprotected plaintext. **If the agency specifies that the information or data be cryptographically protected**, then FIPS 140-2 is applicable. In essence, if cryptography is required, then it must be validated.

As background, below is a list of facts found in FIPS 140-2 and other supporting NIST documents:

a) Cryptography:[1]
The discipline which embodies principles, means and methods for the transformation of data to hide its information content, prevent its undetected modification, prevent its unauthorized use or a combination thereof. [ANSI X9.31]

Cryptography deals with the transformation of ordinary text (plaintext) into coded form (ciphertext) by encryption and transformation of ciphertext into plaintext by decryption. [NIST SP 800-2]

b) The selective application of technological and related procedural safeguards is an important responsibility of every Federal organization in providing adequate security in its computer and telecommunication systems. **This standard [FIPS 140-2] provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data.**[2]

c) **The FIPS 140-2 standard is applicable to all Federal agencies** that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106.[3]

[1] NIST Special Publication 800-21
[2] FIPS 140-2
[3] FIPS 140-2

d) **FIPS 140-2 shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract.**[4]

e) With the passage of the Federal Information Security Management Act (FISMA) of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards (FIPS). The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supercedes that Act. Therefore, the references to the "waiver process" contained in many of the FIPS are no longer operative.

FIPS do not apply to national security systems (as defined in FISMA).

Additional detail:

The Computer Security Act of 1987 (Public Law 100-235) established a statutory basis for the waiver of Federal Information Processing Standards, or FIPS. Section 4 of the Act amended section 111(d) of the Federal Property and Administrative Services Act of 1949. As part of this amendment 40 USC 759(d)(3) authorized the Secretary of Commerce to waive FIPS under certain conditions.

Section 5131 of the Information Technology Management Reform Act (Clinger-Cohen) (Public Law 104-106) repealed 40 USC 759(d), but reenacted it in substantially identical form as 40 USC 1441. The waiver authority continued as before, as section 5131(c) of the Act, or 40 USC 1441(c).

On August 21, 2002 the President signed Public Law 102-217, which substantially revised title 40 of the United States Code. Section 5131 of Clinger-Cohen was repealed but reenacted as section 11331 of title 40. Section 11331(d) continued the FIPS waiver provisions as they had been previously.

Title X of the Homeland Security Act of 2002 (Public Law 107-296) contained the first Federal Information Security Management Act of 2002 (FISMA), and was signed into law on November 25, 2002. Section 11331 of title 40 of the United States Code was substantially amended by FISMA, and the authority to waive FIPS was repealed and not reinstated.

Title III of the E-Government Act contains the second Federal Information Security Management Act of 2002 (Public Law 107-347), signed into law on December 17, 2002. Section 11331 of title 40 of the United States Code was again substantially amended, but the authority to waive FIPS repealed by the Homeland Security Act was not reinstated.

Hence, no authority exists under current law to waive FIPS.

3.3 ROLES

What are the roles of the various participants in the CMVP?

The various participants in the CMVP program are:

a) the user,

[4] FIPS 140-2

b) the cryptographic module vendor,
c) the CMT labs, and
d) the Validation Authorities.

The flow chart shown below in **Figure 2** lists the participants and the roles that they have in the CMVP.

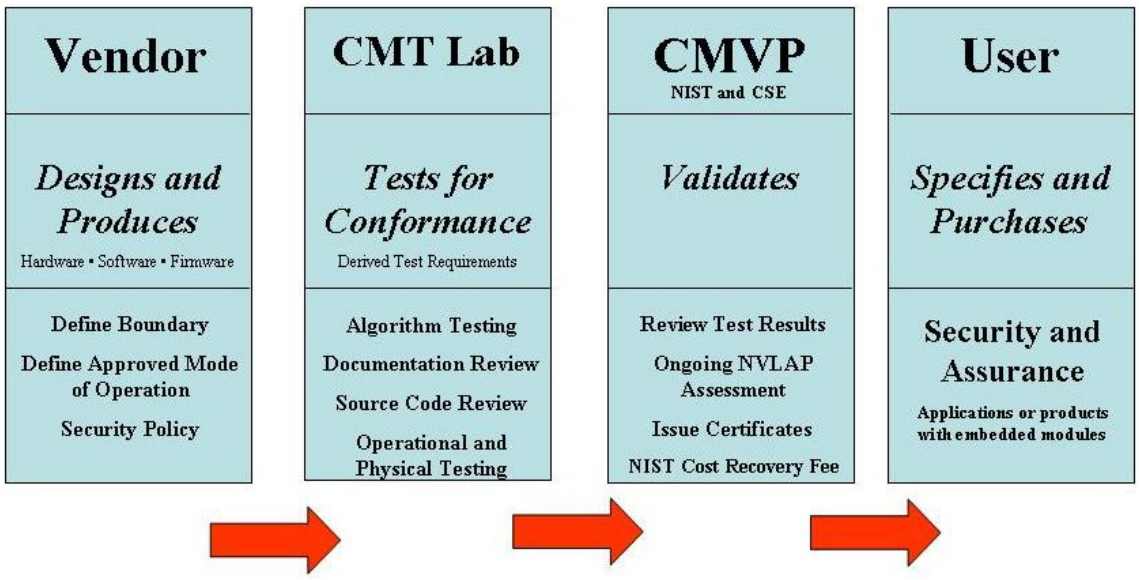


Figure 2: Participants and Roles of the CMVP

Who are the Validation Authorities and what are their responsibilities?

The Validation Authorities are as follows:

- For the U.S.: The National Institute of Standards and Technology, Information Technology Laboratory, Computer Security Division, (NIST), and
- For Canada: the Communications Security Establishment (CSE).

NIST and CSE jointly direct and run the CMVP. The role of the Validation Authorities is to validate the test results for each cryptographic module. The test results are documented in the submission package prepared by a CMT lab. If a cryptographic module is deemed to be compliant with FIPS 140-2, then a validation certificate is issued and the validation list is updated. During the validation review process, the Validation Authorities submit questions to the CMT lab. The questions focus on the technical content, specifically, to ensure that the cryptographic module meets the requirements of the standard and that the information is correct and complete. Typically, the questions will result in a resubmission of the submission package, with clarification provided in one or more of the documents, e.g., Validation Certificate, Validation Report, Security Policy, etc. During the review cycle, the CMT laboratory will work with the vendor to resolve any discrepancies raised by the validation authorities.

The Validation Authorities also validate the test results for the FIPS-approved or NIST recommended cryptographic algorithms. An algorithm validation certificate is issued for each validated cryptographic algorithm.

What is the role of the CMT Laboratories?

The role of the CMT Laboratories is to test the cryptographic module against all applicable requirements as specified in FIPS 140-2 and in the cryptographic algorithm standards and record the results. If a cryptographic module conforms to all the functional and assurance requirements as stated in the Derived Test Requirements, the CMT laboratory submits a written report to the Validation Authorities. If a cryptographic module does not meet one (or more) requirements, the CMT Laboratory will work with the vendor to resolve all discrepancies prior to resubmitting the validation package to the Validation Authorities.

Typically, for cryptographic algorithms, the CMT laboratory generates test vectors based on information provided by the vendor. The CMT laboratory and the vendor use test vectors to exercise the cryptographic algorithm implementation. The vendor submits test results to the CMT laboratory and the laboratory verifies that the results are accurate.

What is the role of the vendors?

The role of the vendors is to design and produce cryptographic modules to comply with the functional and assurance requirements specified in the applicable standards. When a cryptographic module is ready for testing, the vendor submits the module and the associated documentation to one of the CMT laboratories for testing.

For cryptographic algorithms, the vendor designs and implements the algorithm to comply with applicable standards. When a cryptographic algorithm implementation is ready for testing, the vendor notifies the CMT laboratory and provides the information required for a CMT laboratory to generate the test vectors.

What is the user's role?

A user verifies that a cryptographic module they are considering purchasing have been validated, and can verify these at Cryptographic Module Validation Lists. Also, users develop specifications that include the requirements for FIPS 140-2 validated cryptographic modules. The user should also consult the security policy for the cryptographic module to ensure that the module provides the security features that are required by the user.

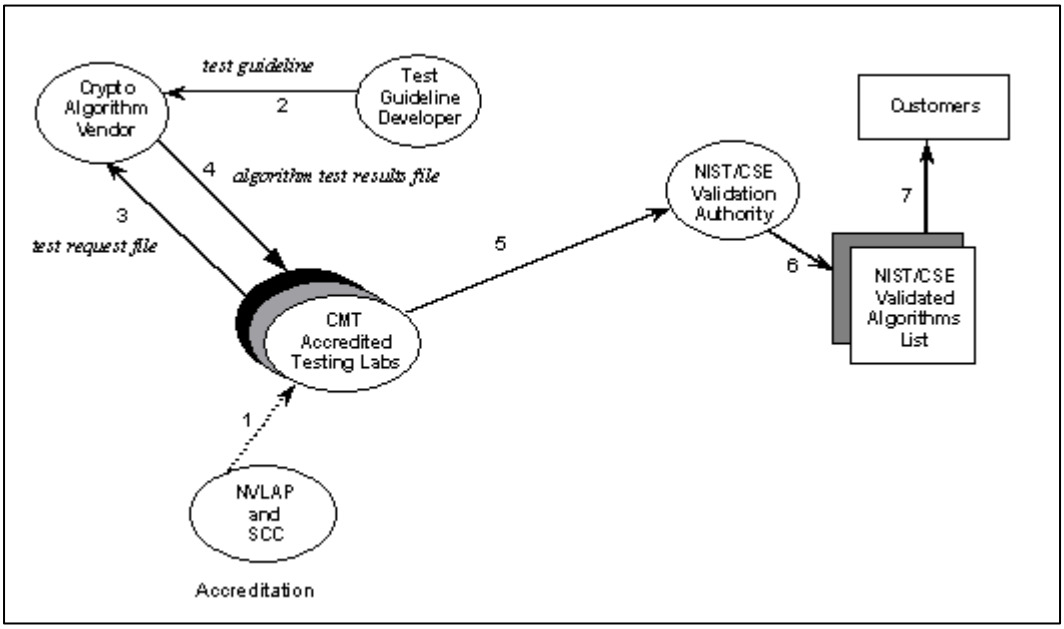
3.4 CRYPTOGRAPHIC MODULE AND CRYPTOGRAPHIC ALGORITHM VALIDATION PROCESSES

What is the cryptographic algorithm validation process?

The Cryptographic Algorithm Validation Program (CAVP) addresses both the testing process and validation of algorithms. Information can be found at: Cryptographic Algorithm Validation Program

A cryptographic algorithm must go through several steps to become validated, as shown in **Figure 3** below.

Figure 3: Cryptographic Algorithm Validation Process



The following is a summary description of the steps in the cryptographic algorithm testing process.

1. To have a cryptographic algorithm tested, the vendor contracts with one of the CMT laboratories to test the algorithm. The test guideline documentation, developed by NIST, is provided to the vendor. The documentation specifies the information that the vendor needs to submit to the CMT laboratory for the development of the *request file* data.

2. The CMT laboratory generates the *request file* and sends it to the vendor.

3. The vendor develops and conducts tests for the cryptographic algorithm using the data in the *request file(s).* When the vendor is satisfied that all the tests have executed correctly, the *response file(s)* are sent to the CMT laboratory.

4. The CMT laboratory generates response file(s) using the NIST-provided reference implementation and the information provided by the vendor. The CMT laboratory compares the results with those submitted by the vendor. If the results do not match, the CMT laboratory provides the information to the vendor. The vendor corrects the cryptographic algorithm (or the test interface), reruns the tests, and resubmits the *response file(s)* to the laboratory. When the laboratory verifies that the results are accurate, the vendor generated response file and algorithm information are forwarded to the validation authorities.

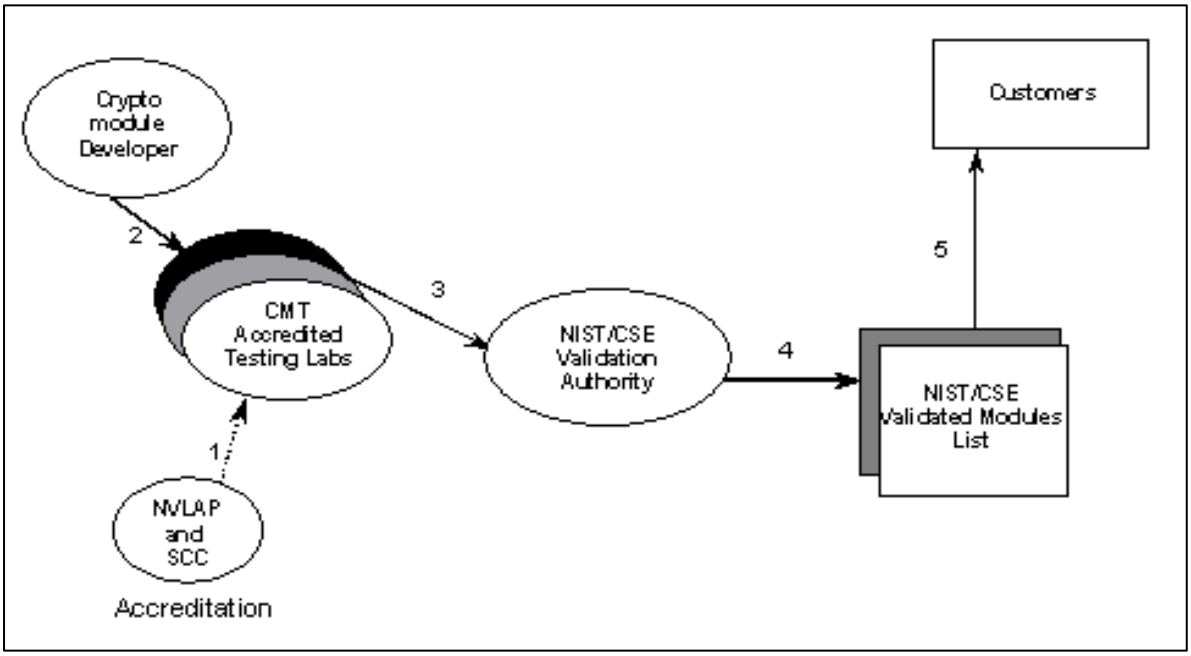
5. When the Validation Authorities are satisfied with all the report findings, a certificate is issued for the cryptographic module. NIST and CSE post information on their respective web sites about the cryptographic algorithm that has been validated.

6. Customers (vendors, federal agencies, and commercial organizations) access the validated algorithms lists to verify that an algorithm has been validated.

What is the cryptographic module validation process?

A cryptographic module must go through several steps to become validated, as shown in **Figure 4** below.

Figure 4: Cryptographic Module Validation Process



Listed below are the steps that a vendor must take to get their cryptographic module validated:

1. To have a cryptographic module tested, the vendor contracts with one of the CMT laboratories to test the module. The vendor submits the cryptographic module to one of the CMT laboratories. The CMT laboratory first reviews the documentation evidence package provided by the vendor to become familiar with the cryptographic module, working with the vendor to clarify any questions the CMT laboratory may have. (If required, the CMT laboratory personnel may test the cryptographic module onsite at the vendor's facility.)
2. The CMT laboratory tests the cryptographic module for conformance to the requirements of FIPS 140-2 using the associated Derived Test Requirements (DTR). When a CMT laboratory successfully completes testing of a cryptographic module, the results are submitted to the Validation Authorities (NIST and CSE).
3. The Validation Authorities review the test report and submit clarifying questions to the laboratory. (This step is iterative – and may require several rounds to resolve all the issues.) When the Validation Authorities are satisfied with all the report findings, a certificate is jointly issued for the cryptographic module.
4. The list of validated modules is updated accordingly.

5. Customers (vendors, federal agencies, and commercial organizations) access the FIPS 140-1 and FIPS 140-2 Cryptographic Modules Validation list to verify that a cryptographic module has been validated. Users purchase validated cryptographic modules.

What is the typical duration of the conformance testing process?

The testing process duration depends on the cryptographic module being tested. The time depends on a variety of factors including: the complexity of the cryptographic module, the overall Security Level, individual Security Levels (if higher than the overall Security Level), the current lab workload, and the content and quality of the vendor documentation submitted with the cryptographic module.

What is the typical duration of the validation process?

In addition to the testing period, the validation process can take anywhere from six to twelve weeks, again depending on the complexity of the cryptographic module, and the completeness of the validation report submission.

How long is the validation effective?

Cryptographic algorithm and module certificates remain effective as long as the validated cryptographic algorithm/module is available from the vendor; that is, there is no expiration date for the certificates.. However, a cryptographic module must be revalidated if there is a change made to the module, regardless of whether the change is security-relevant. The revalidation process in Section 7 describes the three levels of cryptographic module revalidation.

What process does the CMVP follow if informed by 3rd parties regarding module non-compliance issues?

The CMVP will review the information provided for technical merit and specificity. If the information provides specific technical characteristics that appear to question conformance issues of a validated module, the CMVP will sanitize the information and forward it to the Cryptographic Module Testing Laboratory (CMTL) responsible for the module's compliance testing. The CMTL will review the information for accuracy and merit. If the provided information appears to surface a non-compliance issue, the CMTL and CMVP will review and confirm the non-compliance. Based on the nature of the non-compliance, the CMVP will take necessary actions that may ultimately lead to the revocation of the validation certificate. A non-compliance change to a validation will be posted in the CMVP Notices.

The CMVP, working with NVLAP — the CMTL accrediting body — will also investigate the CMTLs testing methodologies and follow up with necessary corrective action.

3.5 CMT LABORATORY ACCREDITATION PROCESS

How does a CMT Laboratory become accredited?

To test cryptographic modules to FIPS 140-2, *Security Requirements for Cryptographic Modules,* and cryptographic algorithm standards, CMT laboratories become an accredited CMT laboratory

under either National Validation Laboratory Accreditation Program (NVLAP) or Standards Council of Canada (SCC).

All CMT laboratories are currently accredited by NVLAP. In Canada, SCC is preparing a CMT laboratory accreditation process under the Program for Accreditation of Laboratories – Canada (PALCAN). PALCAN will support the review of the Quality System with technical assistance from the CMVP staff.

The accreditation process is divided into a series of steps, which approximately occur sequentially. Complete information on the assessment process is available within NIST Handbook 150.

***Step 1*: Application Submission**

To receive consideration for a CMT laboratory accreditation approval request from NVLAP, the CMT laboratory must agree to the accreditation conditions, including:

- Complying at all times with criteria for accreditation as set forth in the applicable handbook and relevant technical documents;
- Fulfilling the accreditation procedure, especially to receive the assessment team;
- Accepting the charges of subsequent maintenance of the accreditation of the CMT laboratory; and
- Reporting to the accreditation authority within 30 days any major changes that affect the CMT laboratory's terms and conditions of accreditation.

The prospective laboratory must also complete a General Application form, a Program Specific Application form, pay the respective fees, and provide a quality manual to the accreditation authority. The General Application must be signed by the Authorized Representative of the applicant laboratory. Before submitting an application for accreditation, the Authorized Representative should review the entire application package and become familiar with NVLAP accreditation requirements. Each applicant should thoroughly review the NVLAP accreditation requirements in NIST Handbook 150 before submitting an application for accreditation. NIST Handbook 150 presents the basic procedures under which NVLAP operates and the general requirements for accreditation of testing and calibration laboratories. Sections 4 and 5 of the handbook include all managerial and technical requirements of ISO/IEC 17025:1999, *General Requirements For The Competence Of Testing And Calibration Laboratories*.

Program-Specific Application: A Program-Specific Application must be completed for each Field of Accreditation for which an applicant laboratory is requesting accreditation. Most Program-Specific Application forms contain a test method selection list that shows the NVLAP Test Method Code, Test Method Designation, and Title of each test method available for accreditation in a particular field. From this list, applicants select the methods to be considered for accreditation. *Program-specific* handbooks are published as part of the NIST Handbook 150 series and contain the procedures and technical requirements that are specific to a given program. The program-specific handbooks complement and supplement the information contained in NIST Handbook 150. Program-specific handbooks also contain interpretive comments that make the general NVLAP criteria specifically applicable to a program. The applicable program-specific handbook for the CMT laboratories is Handbook 150-17.

***Step 2:* Quality Documentation Development**

The NVLAP assessment team reviews the submitted quality documentation. Typically, the assessors have further discussions with the prospective CMT laboratory regarding the quality documentation prior to the on-site assessment. If a laboratory already has a well-established quality system, CMT accreditation does NOT require a separate quality system. Adding the CMT specific requirements to existing documentation and accompanying procedures is acceptable. Some specific new topics are: use of the NVLAP and FIPS logos, separation of cryptographic module design and testing, training and experience required for cryptographic module testers.

Step 3: **Proficiency Quiz**

The prospective CMT laboratory will be asked to complete a proficiency quiz using test questions developed by the CMVP staff. The quiz will be sent to the laboratory when the assessors have determined that the submitted Quality System documentation is acceptable (Step 2). The laboratory will be given a maximum of 7 calendar days to complete the proficiency quiz. The quiz is a compilation of questions and issues that the CMVP has addressed in the past. The quiz covers both FIPS 140-1 and FIPS 140-2. The primary focus is HOW the laboratory answers the questions, that is, the thought process. In general, the questions do not have one correct answer. Therefore, the laboratory needs to include the rationale for the answer.

The assessment team will review the proficiency test responses. If acceptable, the assessment team will proceed with the on-site assessment.

Step 4: **On-site Assessment**

The CMT laboratory is then required to schedule an on-site assessment to have a team of assessors examine the CMT laboratory. The assessors that are selected from accreditation authority will have a *biographical sketch* sent to the CMT laboratory ahead of time ensuring that the assessor's skills match the CMT lab's field of testing that the CMT laboratory is accredited for and shows minimum conflict of interest. If there is a conflict of interest then another person is selected based on the same criteria. The accreditation authority charges an On-Site Assessment fee.

The on-site assessment takes place over a 2-day period, at which time the quality system, including the quality documentation, will be compared against the requirements of Handbooks 150 and 150-17. Handbook 150 includes all the base requirements and Handbook 150-17 provides the specific requirements for CMT labs. The results of the assessment will be conveyed to the laboratory at the conclusion of the assessment on the second day. In addition, the on-site visit will gives the assessors an opportunity to discuss the proficiency quiz results.

Step 5**: Proficiency Testing**

Proficiency testing is an integral part of the accreditation process. The performance of tests and reporting of results from proficiency testing assists the accreditation authority in determining the overall effectiveness of the CMT laboratory. Information obtained from proficiency testing helps to identify problems in a CMT laboratory. If problems are found, the accreditation authority works with the CMT laboratory staff to resolve them. Information is kept confidential.

Step 6: Artifact Testing

At the successful conclusion of the on-site assessment, the laboratory will be provided with a sample artifact to perform a sample test validation (proficiency test). The artifact testing is

intended to assess the laboratories technical knowledge of FIPS 140-2, the applicable cryptographic algorithm standards, and cryptographic module testing – it is not intended to be an exhaustive test. The testing can be completed in four to eight weeks – if personnel are available. (The validation authorities have not set a time limit for completion of the artifact testing.)

Step 7: **Laboratory Accreditation**

The accreditation authority evaluates the results of the first six steps, including any deficiencies and how the CMT laboratory has responded to them, before making the final decision as to whether the CMT laboratory will be accredited.

Once the decision has been made to accredit the laboratory for CMV testing, the CMT laboratory is assigned to one of four renewal dates: January 1, April 1, July 1 or October 1. The renewal period is one year. The CMT laboratory receives an accreditation certificate that identifies the:

- Name and address of the CMT laboratory that has been accredited,
- Scope of the accreditation,
- CMT laboratory's authorized representative,
- Expiration date of the accreditation; and
- CMT laboratory code.

The CMT laboratory can commence testing cryptographic modules under the CMVP when the accreditation certificate is issued.

More information:

For more information on the accreditation process and application forms see CMVP Application Package and Information web site or the SCC web site at http://www.scc.ca/publicat/canp/index_e.html

How much does it cost to become and to remain a CMT accredited laboratory?

A summary of the costs for a NVLAP CMT laboratory accreditation can be found at the CMVP Application Package and Information web site.

3.6 POINTS OF CONTACT

Whom can I contact for more information on the CMVP?

Contact information for the CMVP Validation Authorities can be located at http://csrc.nist.gov/groups/STM/cmvp/contacts.html.

Whom can I contact for more information on the CAVP?

Contact information for the CAVP Validation Authorities can be located at http://csrc.nist.gov/groups/STM/cavp/contacts.html.

Whom can I contact for more information on cryptographic module testing?

A list of points of contacts for each of the CMT laboratories can be located at http://csrc.nist.gov/groups/STM/testing_labs/index.html.

4. STANDARDS

4.1 CRYPTOGRAPHIC MODULE STANDARD

What is the FIPS 140-2 standard?

FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting *sensitive* 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 cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks. FIPS 140-1 superseded FIPS 140, *General Security Requirements for Equipment Using the Data Encryption Standard*, in its entirety. FIPS 140-2 superseded FIPS 140-1, *Security Requirements for Cryptographic Modules*, in its entirety.

What are the functional security objectives of the standard?

The security requirements specified in FIPS 140-2 relate to the secure design and implementation of a cryptographic module. The requirements are derived from the following high-level functional security objectives for a cryptographic module:

- To employ and correctly implement the Approved security functions for the protection of sensitive information.
- To protect a cryptographic module from unauthorized operation or use.
- To prevent the unauthorized disclosure of the contents of the cryptographic module, including plaintext cryptographic keys and CSPs.
- To prevent the unauthorized and undetected modification of the cryptographic module and cryptographic algorithms, including the unauthorized modification, substitution, insertion, and deletion of cryptographic keys and CSPs.
- To provide indications of the operational state of the cryptographic module.
- To ensure that the cryptographic module performs properly when operating in an Approved mode of operation.

- To detect errors in the operation of the cryptographic module and to prevent the compromise of sensitive data and CSPs resulting from these errors.

Why the update, and when did FIPS 140-2 take effect?

FIPS PUBs refers to the Federal Information Processing Standards Publications, which are published by NIST, and are updated on a regular basis. Currently, each FIPS is reviewed every five years. The FIPS PUB 140-1 (hereafter referred to as FIPS 140-1) "*Security Requirements for Cryptographic Modules"* was approved on 4 January 1994. As the standard gained exposure, it was adopted by the Government of Canada in 1995, and now is the defacto International standard for cryptographic module security. In addition, the standard has been adopted by many private industry organizations. This standard is to be used by Federal Agencies when these organizations require cryptography for the protection of sensitive data. FIPS 140-1 specifies the security requirements that are to be satisfied by a cryptographic module.

In addition to constant re-examination, the standard is officially re-examined and re-affirmed every five years. In the fall of 1998, FIPS 140-1 entered a regularly scheduled 5-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. The intent of the first review period was to determine the continued usefulness of the standard. The overwhelming response from the first review period indicated that, yes indeed, the standard should be reaffirmed. A revised draft standard was produced based on the public comments received, a previously issued implementation guidance document, 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 U.S. Federal Register with a closing date of February 15, 2000. The comments received in the second request for comments were reviewed, and by December 2000, the FIPS 140-1 update to FIPS 140-2 was completed.

FIPS PUB 140-2 was signed by the Secretary of Commerce on May 25, 2001, and superseded FIPS 140-1 on May 25, 2002. As of November 2001, testing of cryptographic modules against FIPS 140-2 by the CMT laboratories began, and until May of 2002 a transition period was in place where cryptographic modules could be tested against FIPS 140-1 or FIPS 140-2. On May 25, 2002, the transition period ended, after which the CMT laboratories could test cryptographic modules against FIPS 140-2 only.

As a result of this update, all FIPS 140-1 testing laboratories have become FIPS 140-2 testing labs.

What are the differences between FIPS 140-2 and FIPS 140-1?

FIPS 140-2 superseded FIPS 140-1 standard as of May 25, 2002.

FIPS 140-1 was one of NIST's most successful standards and formed the solid-foundation of the CMVP. FIPS 140-1 was widely recognized as the "defacto" standard for cryptographic modules and was 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 FIPS 140-1's initial five years. 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 questions and comments, reflect changes in technology, and strengthen the standard, but do not change the focus or emphasis.

The authors also took the opportunity to improve the format of the standard by minimally restructuring the content, 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 end result is a stronger more concise, and readable standard that still embodies the spirit of the original standard.

Table 4.1-1 FIPS 140-1 to FIPS 140-2 Comparison

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.

A summary of the changes introduced in FIPS 140-2 includes:

- **Cryptographic Module Specification:** 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.

- **Cryptographic Module Ports and Interfaces**: 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.

- **Roles, Services, and Authentication:** 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.

- **Finite State Model:** The name of this section was changed from Finite State Machine Model (FSMM) to Finite State Model (FSM) to more accurately reflect the requirements. FIPS 140-1 mandated the use of an FSMM in the module's design. The FSMM 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.

- **Physical Security**: The majority of changes to this section involve a re-organization of the sub-sections 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.

- **Operational Environment:** 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.

- **Cryptographic Key Management:** 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 non-deterministic random number generators (RNGs) sub-section 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 sub-section.

- **Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC):** During the update process, the EMI/EMC section was modified to reflect minor changes in FCC requirements and references.

- **Self-Tests:** 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 provided 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, 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.

- **Design Assurance:** assurance the section has now been expanded to address software, hardware, and firmware. Though the entire section was re-written, the consolidated design assurance requirements found in FIPS 140-1 forms 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.

- **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.

Additional details on the changes can be found at http://csrc.nist.gov/publications/nistpubs/800-29/sp800-29.pdf.

What is the FIPS 140-3?

FIPS 140-3 is currently under development. As with the development of FIPS 140-2 which superseded FIPS 140-1, FIPS 140-3 will include lessons learned from questions and comments, reflect changes in technology, and strengthen the standard, but will not change the focus or emphasis.

The authors are taking the opportunity to improve the format of the standard by minimally restructuring the content, 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.

The authors are adding sections specifically embracing software modules, addressing both invasive and non-invasive physical security protection mechanisms and including a new Level 5 of assurance.

4.2 CRYPTOGRAPHIC ALGORITHM STANDARDS

What is the relationship of an algorithm validation to the FIPS 140-2 validation?

A FIPS 140-2 cryptographic module shall implement at least one Approved security function used in an Approved mode of operation. For an algorithm to be listed on a validation certificate as FIPS Approved, the algorithm implementation must meet all the requirements of FIPS 140-2 and must have received an algorithm validation certificate. A FIPS 140-2 validation certificate will not be issued unless the underlying FIPS Approved algorithm certificates have been completed.

A product or module does not meet the FIPS 140-2 applicability requirements by simply implementing FIPS Approved algorithms and acquiring algorithm validation certificates.

What categories of cryptographic algorithms are validated?

The currently tested cryptographic algorithm types include symmetric encryption, asymmetric encryption, hashing, and message authentication. (Note: this section will be updated as algorithms are added.)

What are the current FIPS approved/NIST recommended symmetric algorithms?

*Secret key (or symmetric) cryptographic algorithm*s use a single secret key for both encryption and decryption. The symmetric algorithms are used to protect sensitive information from attacks by encrypting data during transmission (such as email) or while in storage. Conformance testing is currently performed on the following symmetric algorithms: Triple DES, Skipjack, and AES.

Symmetric algorithms are used to provide *confidentiality* services that restrict access to the content of sensitive data to only those individuals who are authorized to view the data. Confidentiality measures prevent the *unauthorized* disclosure of information to unauthorized individuals or processes.

FIPS-Approved/NIST recommended algorithms are listed in FIPS 140-2 Annex A.

What are the current FIPS approved/NIST recommended hashing algorithms?

The current hashing algorithms are: SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. MAC and HMAC SHA-1 and HMAC SHA-2 are hashing algorithms that use a keyed hash.

FIPS-Approved/NIST recommended algorithms are listed in FIPS 140-2 Annex A.

What are the current FIPS approved/NIST recommended asymmetric algorithms?

*Public key (asymmetric) cryptographic algorithm*s use two related keys, a public key and a private key. The two keys have the property that deriving the private key from the public key is computationally infeasible. The current FIPS approved/NIST recommended asymmetric algorithms are: DSA, RSA (X9.31 and PKCS #1), and ECDSA. Typically, asymmetric algorithms are used for:

- *Data integrity* that addresses the unauthorized or accidental modification of data. This includes data insertion, deletion, and modification. To ensure data integrity, a system must be able to detect *unauthorized* data modification. The goal is for the receiver of the data to verify that the data has not been altered.

- *Authentication* that establishes the validity of a transmission, message, or an originator. (Authentication services also verify an individual's authorization to receive specific categories of information. These services are not specific to cryptography.) Therefore, this service applies to both individuals and the information itself. The goal is for the receiver of the data to determine its origin.

- *Non-repudiation* that prevents an individual from denying that previous actions had been performed. The goal is to ensure that the recipient of the data is assured of the sender's identity.

FIPS-Approved/NIST recommended algorithms are listed in FIPS 140-2 Annex A.

5. CRYPTOGRAPHIC MODULE VALIDATION

5.1 CRYPTOGRAPHIC MODULE SECURITY LEVELS

What are the different security levels?

The different security levels are: 1, 2, 3, and 4.

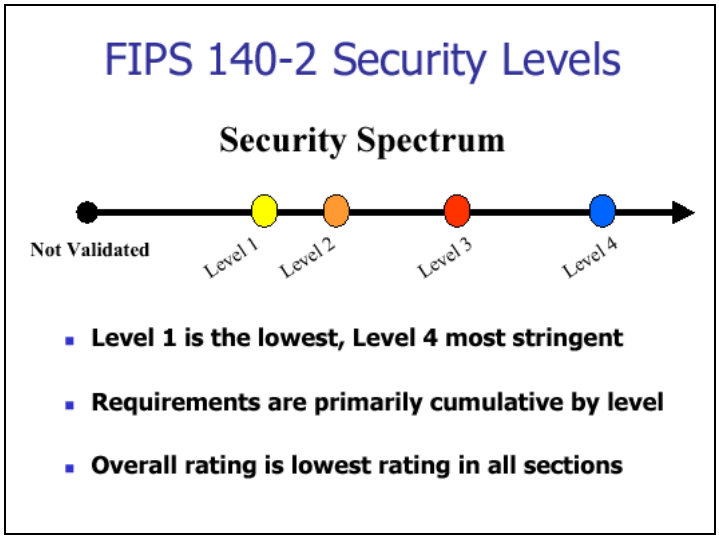


Figure 5: FIPS 140-2 Security Levels

Four security levels are specified for each of 11 requirement areas. Each security level offers an increase in security over the preceding level. These four increasing levels of security allow cost-effective solutions that are appropriate for different degrees of data sensitivity and different application environments.

What are the differences between the four cryptographic module security levels?

FIPS 140-2 validations are made at four separate security levels with level 1 being the lowest. The key difference in the levels is the way physical and logical access to the cryptographic module is limited to ensure its integrity. These levels are clearly indicated on each validation certificate and the strength and functionality of the cryptography is the same for each level.

How do the four security levels of cryptographic modules correlate to the three risk-impact levels required by FIPS 199 and the minimum security controls in FIPS 200 and 800-53?

The four levels of cryptography validation do not (and are not intended to) correlate to the three impact levels set forth in NIST's guidance on categorizing the impact of agency information and systems. Agencies may use any of the four cryptography security levels for any of the impact levels, provided they properly limit physical and logical access to the cryptographic module. For example, level 1 cryptography, which does not include any physical and only limited logical access controls, may be used on a high impact system provided the agency also uses other compensating security controls to protect the cryptographic module. The use of such compensating controls must be documented, e.g., within your certification and accreditation documents.

What security functionality does Level 1 provide?

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module (e.g., at least one FIPS-approved/NIST recommended algorithm (hereafter referred to as an Approved algorithm) or Approved security function must be used). No

specific physical security mechanisms are required in a Security Level 1 cryptographic module beyond the basic requirement for production-grade components. An example of a Security Level 1 cryptographic module is a personal computer (PC) encryption board.

Security Level 1 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an unevaluated operating system. Such implementations may be appropriate for some low-level security applications when other controls, such as physical security, network security, and administrative procedures are limited or nonexistent. The implementation of cryptographic software may be more cost-effective than corresponding hardware-based mechanisms, enabling organizations to select from alternative cryptographic solutions to meet lower-level security requirements.

What security functionality does Level 2 provide?

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

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

Security Level 2 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that meets the functional requirements specified in the Common Criteria (CC) Protection Profiles (PPs) listed in Annex B and is evaluated at the CC evaluation assurance level EAL2 (or higher).

An equivalent evaluated trusted operating system may be used. A trusted operating system provides a level of trust so that cryptographic modules executing on general purpose computing platforms are comparable to cryptographic modules implemented using dedicated hardware systems.

What security functionality does Level 3 provide?

In addition to the tamper-evident physical security mechanisms required at Security Level 2, Security Level 3 attempts to prevent the intruder from gaining access to CSPs held within the cryptographic module. Physical security mechanisms required at Security Level 3 are intended to have a high probability of detecting and responding to attempts at physical access, use or modification of the cryptographic module. The physical security mechanisms may include the use of strong enclosures and tamper detection/response circuitry that zeroizes all plaintext CSPs when the removable covers/doors of the cryptographic module are opened.

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

Security Level 3 requires the entry or output of plaintext CSPs (including the entry or output of plaintext CSPs using split knowledge procedures) be performed using ports that are physically

separated from other ports, or interfaces that are logically separated using a trusted path from other interfaces. Plaintext CSPs may be entered into or output from the cryptographic module in encrypted form (in which case they may travel through enclosing or intervening systems).

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

- meets the functional requirements specified in the PPs listed in Annex B with the additional functional requirement of a Trusted Path (FTP_TRP.1); and

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

An equivalent evaluated trusted operating system may be used. The implementation of a trusted path protects plaintext CSPs and the software and firmware components of the cryptographic module from other untrusted software or firmware that may be executing on the platform.

What security functionality does Level 4 provide?

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

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

Security Level 4 allows the software and firmware components of a cryptographic module to be executed on a general purpose computing system using an operating system that:

- meets the functional requirements specified for Security Level 3; and
- is evaluated at the CC evaluation assurance level EAL4 (or higher).

An equivalent evaluated trusted operating system may be used.

5.2 FIPS 140-1

What was the deadline for performing FIPS 140-1 testing?

All FIPS 140-1 test submission packages were submitted to the Validation Authorities by May 25, 2002, only.

After that date, testing is performed against FIPS 140-2.

The CMVP will continue to receive updates to FIPS 140-1 validation entries for non-security relevant changes. This is addressed in FIPS 140-2 IG G.8 scenario 1.

5.3 FIPS 140-2

Are there different security requirements between Levels 1 through 4?

The following table summarizes the differences between the requirements at the four security levels.

Table 5.3-1 Security Requirements

	Security Level 1	**Security Level 2**	**Security Level 3**	**Security Level 4**
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15, Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical function tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and

	Security Level 1	Security Level 2	Security Level 3	Security Level 4
	correspondence. Guidance documents.			postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

What are the cryptographic module specification types?

A *cryptographic module* is the set of hardware, software, and/or firmware that implements Approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary. A new type, *hybrid*, is a software module that also contains an underlying unique hardware component.

There are three distinct physical embodiments: single-chip modules, multiple-chip embedded modules, and multiple-chip standalone modules.

What is a cryptographic boundary?

A *cryptographic boundary* is an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

What is a security policy?

See Section 5.6 for a description of what is contained in the Security Policy.

What are module interfaces?

Module interfaces are the means by which information is passed into and out of the cryptographic module. At minimum, a cryptographic module's design must include the following interfaces:

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

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

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

d) **Status output interface**. All output signals, indicators, and status data (including return codes and physical indicators such as Light Emitting Diodes and displays) used to indicate the status of a cryptographic module must exit via the "status output" interface.

What are roles and services?

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

- *User Role.* The role assumed to perform general security services, including cryptographic operations and other Approved security functions.

- *Cryptographic Officer Role*: The role assumed to perform cryptographic initialization or management functions (e.g., module initialization, input/output of cryptographic keys and CSPs, and audit

Services refer to all of the services, operations or functions that can be performed by a cryptographic module.

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module and to verify that the operator is authorized to assume the requested role and perform services within that role. Depending on the security level, a cryptographic module must support at least one of the following mechanisms to control access to the module:

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

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

Is there a minimum security requirement for authentication?

For Security Level 1, a cryptographic module is not required to employ authentication mechanisms to control access to the module. If authentication mechanisms are not supported by a cryptographic module, the module shall require that one or more roles either be implicitly or explicitly selected by the operator. Level 1 authentication can be either role-based or identity-based, including the use of a single role or identity based account. Level 2 requires that there must be at least role-based operator authentication while Levels 3 and 4 require identity-based operator authentication.

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

a cryptographic module shall be protected against unauthorized disclosure, modification, and substitution.

Can various UNIX OSs be configured to meet the Level 1 single user mode requirement?

The following explains how to configure a UNIX system for single user. The general idea is the same across all Unix variants.

- Remove all login accounts except "root" (the superuser).
- Disable NIS and other name services for users and groups.
- Turn off all remote login, remote command execution, and file transfer daemons.

The specific procedures for each of the UNIX variants are described below.

RedHat Linux

a) Log in as the "root" user.
b) Edit the system files /etc/passwd and /etc/shadow and remove all the users except "root" and the pseudo-users. Make sure the password fields in /etc/shadow for the pseudo-users are either a star (*) or double exclamation mark (!!). This prevents login as the pseudo-users.
c) Edit the system file /etc/nsswitch.conf and make "files" the only option for "passwd", "group", and "shadow". This disables NIS and other name services for users and groups.
d) In the /etc/xinetd.d directory, edit the files "rexec", "rlogin", "rsh", "rsync", "telnet", and "wu-ftpd", and set the value of "disable" to "yes".
e) Reboot the system for the changes to take effect.

HP-UX

a) Log in as the "root" user.
b) Edit the system file /etc/passwd and remove all the users except "root" and the pseudo-users. Make sure the password fields for the pseudo-users are a star (*). This prevents login as the pseudo-users.
c) Edit the system file /etc/nsswitch.conf. Make sure that "files" is the only option for "passwd" and "group". This disables NIS and other name services for users and groups.
d) Edit the system file /etc/inetd.conf. Remove or comment out the lines for remote login, remote command execution, and file transfer daemons such as telnetd, rlogind, remshd, rexecd, ftpd, and tftpd.

e) Reboot the system for the changes to take effect.

DEC OSF1

a) Log in as the "root" user.
b) Edit the system file /etc/passwd and remove all the users except "root" and the pseudo-users. Make sure the password fields for the pseudo-users are either a star (*) or "Nologin". This prevents login as the pseudo-users.
c) Edit the system file /etc/svc.conf and make "local" the only option for "passwd" and "group". Then, remove all lines that begin with a plus sign (+) from /etc/passwd and /etc/group. This disables NIS and other name services for users and groups.
d) Edit the system file /etc/inetd.conf. Remove or comment out the lines for remote login, remote command execution, and file transfer daemons such as telnetd, rlogind, rshd, rexecd, ftpd, and tftpd.
e) Reboot the system for the changes to take effect.

IBM AIX

a) Log in as the "root" user.
b) Edit the system file /etc/passwd and remove all the users except "root" and the pseudo-users. Make sure that for the pseudo-users, either the password fields are a star (*) or the login shell fields are empty. This prevents login as the pseudo-users.
c) Remove all lines that begin with a plus sign (+) or minus sign (-) from /etc/passwd and /etc/group. This disables NIS and other name services for users and groups.
d) Edit the system file /etc/inetd.conf. Remove or comment out the lines for remote login, remote command execution, and file transfer daemons such as telnetd, rlogind, krlogind, rshd, krshd, rexecd, ftpd, and tftpd.

e) Reboot the system for the changes to take effect.

What is a finite state model?

The finite state model is a general description of the functionality and operation of the cryptographic module. Further details on what must be contained in the Finite State Model can be located in Section 5.6.

What are the required states that the cryptographic module must contain?

A cryptographic module must include the following operational and error states:

- *Power on/off states*. States for primary, secondary, or backup power. These states may distinguish between power sources being applied to a cryptographic module.

- *Cryptographic officer states*. States in which the cryptographic officer services are performed (e.g., cryptographic initialization and key management).

- *Key/CSP entry states*. States for entering cryptographic keys and CSPs into the cryptographic module.

- *User states*. States in which authorized users obtain security services, perform cryptographic operations, or perform other Approved or non-Approved functions.

- *Self-test states*. States in which the cryptographic module is performing self-tests.

- *Error states*. States when the cryptographic module has encountered an error (e.g., failed a self-test or attempted to encrypt when missing operational keys or CSPs). Error states may include "hard" errors that indicate an equipment malfunction and that may require maintenance, service or repair of the cryptographic module, or recoverable "soft" errors that may require initialization or resetting of the module. Recovery from error states shall be possible except for those caused by hard errors that require maintenance, service, or repair of the cryptographic module.

What are the optional states that a cryptographic module can include?

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

- *Bypass states*. States in which a bypass capability is activated and services are provided without cryptographic processing (e.g., transferring plaintext through the cryptographic

module).

- *Maintenance states*. States for maintaining and servicing a cryptographic module, including physical and logical maintenance testing. If a cryptographic module contains a maintenance role, then a maintenance state shall be included.

What is physical security?

A cryptographic module must employ *physical security* mechanisms in order to restrict unauthorized physical access to the contents of the module and to deter unauthorized use or modification of the module (including substitution of the entire module) when installed. All hardware, software, firmware, and data components within the cryptographic boundary must be protected. This section of FIPS 140-2 details all of the requirements surrounding the physical security of the cryptographic module. For software cryptographic modules, this section may be marked as Not Applicable.

What are the different physical embodiments?

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

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

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

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

What are the different physical security requirements at each level for each type of physical embodiments?

The following table summarizes the physical security requirements, both general and embodiment-specific, for each of the four security levels. The general physical security requirements at each security level are all three distinct physical embodiments of a cryptographic module. The embodiment-specific physical security requirements at each security level enhance the general requirements at the same level, and the embodiment-specific requirements of the previous level.

Table 5.3-2 Summary of physical security requirements

	General Requirementsfor all Embodiments	Single-Chip Cryptographic Modules	Multiple-Chip Embedded Cryptographic Modules	Multiple-Chip Standalone Cryptographic Modules

Security Level 1	Production-grade components (with standard passivation).	No additional requirements.	If applicable, production-grade enclosure or removable cover.	Production-grade enclosure.
Security Level 2	Evidence of tampering (e.g., cover, enclosure, or seal).	Opaque tamper-evident coating on chip or enclosure.	Opaque tamper-evident encapsulating material or enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.	Opaque enclosure with tamper-evident seals or pick-resistant locks for doors or removable covers.
Security Level 3	Automatic zeroization when accessing the maintenance access interface. Tamper response and zeroization circuitry. Protected vents.	Hard opaque tamper-evident coating on chip or strong removal-resistant and penetration resistant enclosure.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or applicable Multiple-Chip Standalone Security Level 3 requirements.	Hard opaque potting material encapsulation of multiple chip circuitry embodiment or strong enclosure with removal/penetration attempts causing serious damage.
Security Level 4	EFP or EFT for temperature and voltage.	Hard opaque removal-resistant coating on chip.	Tamper detection envelope with tamper response and zeroization circuitry.	Tamper detection/ response envelope with tamper response and zeroization circuitry.

What is design assurance?

Design assurance refers to the use of best practices by the vendor of a cryptographic module during the design, deployment, and operation of a cryptographic module, providing assurance that the module is properly tested, configured, delivered, installed, and developed, and that the proper operator guidance documentation is provided. Security requirements are specified for configuration management, delivery and operation, development, and guidance documents.

What is the impact of the new design assurance requirements in FIPS PUB 140-2

The CMVP staff have talked to a number of vendors, labs, consultants, etc. who have expressed concerns over the new Design Assurance requirements in FIPS 140-2, specifically, configuration management; delivery and operation; and guidance documents. The concern is the amount of documentation that the vendor must produce and deliver to the CMT lab with the crypto module. To clarify: the amount of documentation that needs to be produced for the design assurance requirements is comparable to the amount of documentation that needs to be produced for the other areas in FIPS 140-2. The CMVP does NOT mandate a specific format or structure of the information. Therefore, vendors should not expect to expend significantly more resources in meeting these new Design Assurance requirements.

What are the recommended software development practices?

Life-cycle software engineering recommendations (dealing with the specification, construction, verification, testing, maintenance, and documentation of software) should be followed. Software engineering practices may include documented unit testing, code reviews, explicit high-level and low-level design documents, explicit requirements and functional specifications, structure charts and data flow diagrams, function-point analysis, defect and resolution tracking, configuration management, and a documented software development process. The software development practices are listed in Appendix B of FIPS 140-2.

What is the operational environment?

The *operational environment* of a cryptographic module refers to the management of the software, firmware, and/or hardware components required for the module to operate. The operational environment can be non-modifiable (e.g., firmware contained in ROM, or software

contained in a computer with I/O devices disabled), or modifiable (e.g., firmware contained in RAM or software executed by a general purpose computer).

An operating system is an important component of the operating environment of a cryptographic module. There are three types of operational environments defined in FIPS 140-2.

This section of the standard 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.).

How does Common Criteria (CC) relate to FIPS 140-2?

If the operational environment is a *modifiable operational environment*, the operating system requirements of the Common Criteria are applicable at Security Levels 2 and above.

FIPS 140-1 required evaluated operating systems that referenced the Trusted Computer System Evaluation Criteria (TCSEC) classes C2, B1 and B2. However, 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.

The Common Criteria (CC) and FIPS 140-1&2 are different in the abstractness and focus of tests. FIPS 140-2 testing is against a defined cryptographic module and provides a suite of conformance tests to four security levels. FIPS 140-2 describes the requirements for cryptographic modules and includes such areas as physical security, key management, self tests, roles and services, etc. The standard was initially developed in 1994 - prior to the development of the CC. CC is an evaluation against a created protection profile (PP) or security target (ST). Typically, a PP covers a broad range of products.

A CC evaluation does not supersede or replace a validation to either FIPS 140-1 or FIPS 140-2. The four security levels in FIPS 140-1 and FIPS 140-2 do not map directly to specific CC EALs or to CC functional requirements. FIPS 140-2 is the current *de facto* standard for cryptography and NIST is not aware of any other standard (developed in the US or worldwide) that is comparable. Also, there is no document that correlates CC functionality to FIPS 140-1 and FIPS 140-2 functionality. Therefore, a CC certificate cannot be a substitute for a FIPS 140-1 or FIPS 140-2 certificate. However, NIST is looking at FIPS 140-1 and FIPS 140-2 test data to be submitted as part of a CC evaluation. The hope is that some of the similar tests will not need to be repeated.

What is an EAL?

An EAL is an *evaluation assurance level,* as defined by the Common Criteria Part 3 "Assurance Requirements" that defines a scale for measuring assurance, the individual assurance components from which the assurance levels are composed, and the criteria for evaluation of Protection Profiles (PPs) and Security Targets (STs).

Where can I find EAL requirements?

EAL requirements can be found at the Common Criteria web site at: http://www.commoncriteria.org/cc/part3/part302.html.

What are the approved protection profiles for operational environments?

The Approved Protection Profiles are listed in Annex B to the FIPS 140-2 standard.

What is 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, key establishment (including key transport), key entry/output, key storage, and key zeroization. The requirements are applicable to modules that implement secret key and/or public key algorithms. Secret and private keys must be protected from unauthorized disclosure, modification and substitution. Public keys must be protected against unauthorized modification and substitution.

What are the components of key management?

The components of Key Management are:

a) Random number generators (RNGs),
b) Key generation,
c) Key establishment (including key transport),
d) Key entry and output,
e) Key storage, and
f) Key zeroization.

What are the EMI/EMC security requirements?

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 electro-magnetically 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.

What are self-tests?

The self-tests 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 cryptographic algorithm tests, public/private key generation, software/firmware integrity, software/firmware loading, manual key entry, random number generation, and cryptographic bypass (plaintext in, plaintext out).

What types of self-tests the cryptographic module must perform?

The test types that must be performed are:

a) Power Up tests – Cryptographic algorithm test
Software/firmware Integrity test

Critical functions test

b) Conditional tests – Pairwise consistency test
Software/firmware load test
Manual key entry test
Continuous Random Number Generator test
Bypass test

Does the CMVP validate source code?

No – given current technology and the requirements of FIPS 140-2, source code itself cannot be validated.

Does the CMVP validate static libraries?

No – given current technology and the requirements of FIPS 140-2, static libraries themselves cannot be validated.

5.4 FIPS 140-2 DERIVED TEST REQUIREMENTS

What is the purpose of the DTR?

The purpose of the Derived Test Requirements (DTR) document is to describe the methods used by accredited laboratories to test whether a cryptographic module conforms to the requirements of FIPS 140-2. The DTR includes detailed procedures, inspections, and tests that the tester must follow, and the expected results that must be achieved for a cryptographic module to comply with the FIPS 140-2 requirements. These detailed methods provide a high degree of objectivity during the testing process and ensure consistency across the accredited testing laboratories.

The FIPS 140-2 DTR also details the requirements for vendor information that must be provided as supplementary evidence to demonstrate conformance to FIPS 140-2. The FIPS 140-2 DTR document may be used by vendors as a guide when designing a cryptographic module and to determine if a cryptographic module meets the requirements of FIPS 140-2.

What are the statement items types in the DTR and to whom do each apply?

Within each section, the corresponding security requirements from FIPS PUB 140-2 are divided into a set of assertions (i.e., statements that must be true for the module to satisfy the requirement of a given area at a given level). All of the assertions are direct quotations from FIPS PUB 140-2.

The assertions are denoted by the form:

AS<requirement_number>.<assertion_sequence_number>

where “requirement_number” is the number of the corresponding area specified in FIPS PUB 140-2 (i.e., one through eleven), and “sequence_number” is a sequential identifier for assertions

within a section. After the statement of each assertion, the security levels to which the assertion applies (i.e., Levels 1 through 4) are listed in parentheses.

Following each assertion is a set of requirements levied on the vendor. These requirements describe the types of documentation or explicit information that the vendor must provide for the tester to determine conformance to the given assertion. These requirements are denoted by the form:

VE<requirement_number>.<assertion_sequence_number>.<sequence_number>

where "requirement_number" and "assertion_sequence_number" are identical to the corresponding assertion requirement number and sequence number, and "sequence_number" is a sequential identifier for vendor requirements within the assertion requirement.

Also following each assertion and the requirements levied on the vendor is a set of requirements levied on the tester of the cryptographic module. These requirements instruct the tester as to what he or she must do to test the cryptographic module with respect to the given assertion. These requirements are denoted by the form:

TE<requirement_number>.<assertion_sequence_number>.<sequence_number>

where "requirement_number" and "assertion_sequence_number" are identical to the corresponding assertion requirement number and sequence number, and "sequence_number" is a sequential identifier for tester requirements within the assertion requirement.

How is testing performed?

See the answer to the same question in Section 3.4.

5.5 FIPS 140-2 IMPLEMENTATION GUIDANCE AND POLICIES

What is the purpose of the Implementation Guidance (IG) for FIPS 140-2?

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 and Policy* for FIPS 140-2 and associated *Derived Test Requirements* (DTR) and the FIPS-approved/NIST recommended cryptographic algorithms. The *Implementation Guidance* covers program policy, technical questions, and general guidance needed for cryptographic algorithm and module validation. Interpretations that are specific to a vendor's cryptographic module are kept proprietary between NIST/CSE and the CMT laboratory.

How often is the IG updated for FIPS 140-2?

The IG is updated as new interpretations are drafted.

Where is the IG located?

Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program is on the CMVP web site.

5.6 VALIDATION REPORT SUBMISSION DOCUMENTATION

What is the validation report submission documentation?

The validation report submission documentation is the documentation package that a CMT laboratory produces for a specific cryptographic module and submits to the validation authorities. The required documents can be found in the FIPS 140-2 Implementation Guidance **G.2**.

Why is a non-proprietary security policy required?

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

- To provide a specification of the cryptographic security that will allow individuals and organizations to determine whether a cryptographic module, as implemented, satisfies a stated security policy.

- To describe to individuals and organizations the capabilities, protection, and access rights provided by the cryptographic module, thereby allowing an assessment of whether the module will adequately serve the individual or organizational security requirements.

What is the minimum information required in a cryptographic module security policy?

A cryptographic module security policy consists of:

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

The specification shall be sufficiently detailed to answer the following questions:

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

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

- What security mechanisms are implemented in a cryptographic module to mitigate against attacks for which testable requirements are not defined in the standard?

When presenting information in the non-proprietary security policy regarding the cryptographic services that are included in the module validation, the security policy must include, at a minimum, the following information **for each service:**

- The service name

- A concise description of the service purpose and/or use (the service name alone may, in some instances, provide this information)

- A list of Approved security functions (algorithm(s), key management technique(s) or authentication technique) used by, or implemented through, the invocation of the service.

- A list of the cryptographic keys and/or CSPs associated with the service or with the Approved security function(s) it uses.

- For each operator role authorized to use the service:

    - Information describing the individual access rights to all keys and/or CSPs

    - Information describing the method used to authenticate each role.

The presentation style of the documentation is left to the vendor. FIPS 140-2, Appendix C, contains tabular templates that provide non-exhaustive samples and illustrations as to the kind of information to be included in meeting the documentation requirements of the Standard.

Additional Information

FIPS 140-2 requires information to be included in the module security policy which:

- Allows a user (operator) to determine when an approved mode of operation is selected (**AS01.06, AS01.16**).

- Lists all security services, operations or functions, both Approved and non-Approved, that are provided by the cryptographic module and available to operators (**AS01.12, AS03.07, AS03.14, AS14.03**).

- Provides a correspondence between the module hardware, software, and firmware components (**AS10.06**)

- Provides a specification of the security rules under which the module shall operate, including the security rules derived from the requirements of FIPS 140-2. (**AS14.02**)

- For each service, specifies a detailed specification of the service inputs, corresponding service outputs, and the authorized roles in which the service can be performed. **(AS03.14, AS14.03)**

See also to the definitions of ***Approved mode of operation*** and ***Approved security function*** in FIPS140-2.

What is the minimum information required in a finite state model?

A finite state model is 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). It is a general description of the functionality and operation of the cryptographic module and must include the required states and optional states, a state transition diagram, and a specification of state transitions.

5.7 FIPS 140-1 AND FIPS 140-2 LOGOS

What are the guidelines for the use of the FIPS 140-1 and 140-2 Logos?

The phrases *FIPS 140-1 Validated* and *FIPS 140-2 Validated* and the FIPS 140-1 and 140-2 Logos are intended for use in association with cryptographic modules validated by the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada as complying with FIPS 140-1 or FIPS 140-2, *Security Requirements for Cryptographic Modules*. Vendors with cryptographic modules that have been validated by NIST and CSE may use the phrase and logo provided that they agree in writing to the following:

1. The phrases *FIPS 140-1 Validated* and *FIPS 140-2 Validated* and the FIPS 140-1 and FIPS 140-2 Logos are Certification Marks of NIST, which retains exclusive rights to their use.

2. NIST reserves the right to control the quality of the use of the phrases *FIPS 140-1 Validated* and *FIPS 140-2 Validated* and the logos themselves.

3. Permission for advertising FIPS 140-1 and FIPS 140-2 validation and use of the logos are conditional on and limited to those cryptographic modules validated by NIST and CSE as complying with FIPS 140-1 or FIPS 140-2.

4. A cryptographic module may either be a component of a product, or a standalone product. Use of the FIPS 140-1 and FIPS 140-2 Logos on product reports, letterhead, brochures, marketing material, and product packaging must be accompanied by the following: 'TM: A Certification Mark of NIST, which does not imply product endorsement by NIST, the U.S. or Canadian Governments'. If the cryptographic module is a component of a product, the phrase "FIPS 140-1 Inside" or "FIPS 140-2 Inside" must accompany the logo.

5. Permission for the use of the phrases *FIPS 140-1 Validated* and *FIPS 140-2 Validated* and the logos may be revoked at the discretion of NIST.

6. Permission to use the phrase *FIPS 140-1 Validated* and *FIPS 140-2 Validated* and the FIPS 140-1 and FIPS 140-2 Logos in no way constitutes or implies product endorsement by NIST or CSE.

7. Photographic and electronic copies of the logo are available from NIST upon request.

How can electronic images of the logos be obtained from NIST?

A vendor must request a **Guidelines for the Use of the FIPS 140-1 Logo** or **Guidelines for the Use of the FIPS 140-2 Logo** from NIST. This form must be filled out and signed and returned to NIST for each validation certificate issued. Multiple certificate numbers may be included on a single form. Submission of the form by a vendor for one certificate does not allow use of the logos for other certificates that may have been issued.

The cryptographic module is not a product. Can I use the FIPS logo on product literature?

Yes, bullet 4 of the logo guidelines and use form allows the use of the FIPS logo on product literature. However, along with the TM annotation, the phrase “FIPS 140-1 Inside” or “FIPS 140-2 Inside” must be included.

There is no assurance that a product is correctly utilizing an embedded validated cryptographic module - this is outside the scope of the FIPS 140-1 or FIPS 140-2 validation.

What logos can accredited CMT Laboratories use?

Cryptographic Module Testing (CMT) Laboratories, subject to their NVLAP accreditation, may use the NVLAP, CMVP and FIPS 140-1 and 140-2 logos. Use of the logos shall be specified in the CMT Laboratories Quality Manual documentation. Use of the FIPS 140-1 and FIPS 140-2 logos shall follow the same CMVP logo use guidelines as appropriate and indicated in the CMT Laboratory quality manual documentation.

What process does the CMVP follow if informed by 3rd parties regarding the unapproved use of trade marked logos and phrases?

The CMVP will review the information provided and contact the parties that may be using the NIST trade marked FIPS 140-2 logos or FIPS 140-2 Validated phrases without consent. If consent was not given (based on the returned Logo Usage Agreement Form), the CMVP will ask that the use of the logo or phrases be discontinued. If not, the CMVP will pass the information to the NIST legal counsel for resolution.

5.8 VALIDATION LIST CHANGES

How can the validation list be updated for vendor, module name or versioning information changes?

A CMT Laboratory must send to NIST a signed letter requesting vendor name changes, changes to the module name, or changes to any versioning information. This letter must assert that the CMT Laboratory has verified the legal vendor name change, if a module name change, that the new named module is identically the same as the old named module, and if a versioning change, that the change is does not reflect any actual change to the module (e.g. simply a change in the vendor's release and delivery process).

How can the validation list be updated if the vendors contact information has changed (new address, phone, fax, point-of-contact)?

The vendor or CMT Laboratory can simply send an e-mail to NIST requesting the validation list update. The vendor may also request changes to the module description field.

Can the Security Policy be updated after validation?

Yes, depending on the change, a vendor may submit a new security policy to NIST for replacement of the existing posted security policy if there are no functional changes indicated. If

functional or technical content is changed, a CMT Laboratory must review and submit to NIST/CSE for review and update.

Under FIPS 140-2 IG G.5, software is ported to a new OS: can the validation list be updated?

OS's are listed on the original certificate only if the CMT Laboratory operationally tested the cryptographic module with this OS during validation testing. If the module can be ported to a new OS without underlying source code change, the new OS can only be listed and affirmed in the security policy. A vendor may submit a new security policy with this update. If the vendor wishes the new OS to be listed on the validation list, then the cryptographic module must undergo full operational testing by the CMT Laboratory. After testing, the CMT Laboratory can request the update per FIPS 140-2 IG G.8(1). If the underlying source code is changed for porting, FIPS 140-2 IG G.5 applies. If the CMT Laboratory does not perform full operational testing with this OS, the new OS may only be listed in the revised security policy, and only the new software version will be updated on the validation list.

5.9 VALIDATION CERTIFICATES

What are the criteria for the CMVP to issue a new certificate?

A new certificate is only issued upon a successful full validation or re-validation.

After a certificate is printed, a new certificate will only be re-printed if typographical errors are discovered post-issuance or at the discretion of the CMVP. Any other changes to a module's validation information will only be updated on the CMVP web site validation list. The CMVP web site validation list is the official source of validation information.

The initial printed validation certificate is for informational purposes only.

If the CMVP validation web site does not match the posted certificate, which is valid?

When a module is validated, an entry is posted on the CMVP web site valuation list along with a softcopy of the initial printed validation certificate. The hardcopy validation certificate is for informational purposes only. The CMVP web site validation list is the official source of validation information in reference to the module. If changes are made to the module that would change the referenced certificate information, only the web site validation list is updated.

What is the process for a vendor to OEM a validated module?

The following addresses a 3rd parties options to OEM a cryptographic module:

If the OEM module is already validated:

1. After the OEM module is validated, the CMT Lab can submit a non-security letter request asserting that the OEM module is identically the same as the module which the 3rd party wishes to re-brand or re-sell, and the CMT Lab has reviewed the agreement between the 3rd party and the OEM module vendor that both parties agree to this arrangement. The CMVP will then update the web site with the 2nd module information within the limits of

the existing database format. No new or additional certificates will be printed. See Certificate #141 as an example.

If the OEM module is not yet validated:

2. The CMT Laboratory may submit one test report with BOTH modules and vendors annotated on all documentation. Only one NIST cost recovery fee will be required and a single certificate will be printed with BOTH vendors and module names on the same certificate.

3. The CMT Laboratory may submit two test reports, one for each module. Both full reports will be subject to the NIST cost recovery fee. The 3rd party module cannot be considered a re-validation based on the FIPS 140-2 IG G.8 requirements. Both reports will be reviewed and a certificate issued for each per the normal validation process.

What does the term "Non-Compliant" caveat placed after a cryptographic algorithm implementation entry indicate (e.g., DES (non-compliant))?

This caveat applies to a security function entry that is annotated such that it appears to represent or is named similarly to an Approved security function listed in FIPS 140-2 Annex A. The term "non-compliant" indicates the cryptographic security function implementation is not compliant with the requirements of FIPS 140-2. The "non-compliance" could mean:

- the cryptographic algorithm implementation has not been tested and validated under the CAVP (e.g. an algorithm validation certificate does not exist); and/or
- the cryptographic algorithm implementation does not meet a FIPS 140-2 requirement (e.g. does not implement a power-up self-test); and/or
- the cryptographic algorithm implementation is not functionally similar to one of the Approved security functions but is annotated the same (e.g. DES – Dave's Encryption Scheme)

Non-compliant functions are listed as non-Approved security functions and may not be used in a FIPS Approved mode of operation.

Examples:

DES (Cert. #876, non-compliant) – A DES algorithm certificate has been obtained which signifies correct algorithmic implementation, but the implementation may not for example have implemented a Known-Answer-Test (KAT) or other requirement of FIPS 140-2.

AES (non-compliant) – AES is an Approved security function found in FIPS 140-2 Annex A. This implementation does not have an algorithm certificate and may also not have met other FIPS 140-2 requirements.

DSA (non-compliant) – This is a proprietary algorithm, "Dave's Sequencing Adder", not found in the FIPS 140-2 Annex A. However its acronym is similar to the Digital Signature Algorithm (DSA), which is an Approved security function in FIPS 140-2 Annex A.

MD5 – This security function does not require the caveat "non-compliant" as it clearly is not an Approved security function as it is not listed in FIPS 140-2 Annex A.

6. CRYPTOGRAPHIC ALGORITHM TESTING

Why is cryptographic algorithm testing performed?

Cryptographic algorithm testing is performed to ensure that a specific algorithm implementation is implemented correctly and functions correctly.

What are the FIPS-approved/NIST recommended encryption standards and tests?

For:

a. AES:

   i. The FIPS 197 standard describes the algorithm specifications.

   ii. The Advanced Encryption Standard Algorithm Validation Suite (AESAVS) describes the tests performed on the algorithm.

b. Triple-DES and DES:

   i. The FIPS 46-3 describes the algorithm specifications.

   ii. The tests are:

   - The DES tests are described in the NIST Special Publication 800-17 titled “Modes of Operation (MOVS): Requirements and Procedures”.
   - The migration from DES to Triple-DES is discussed in FIPS 46-3.
   - Triple-DES tests can be found at the NIST Special Publication 800-20 titled “Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures”.

c. Skipjack:

   i. This algorithm is referenced in FIPS 185. A complete specification is contained in the SKIPJACK and KEA specifications.

d. SHA-1:

   i. The FIPS 180-1 standard describes the algorithm specifications.
   ii. The SHA-1 testing is described in the DSSVS.

e. DSS:

i. The FIPS 186-2 standard describes the algorithm specifications. The DSA tests are described in the DSSVS guide entitled "Digital Signature Standard Validation System (DSSVS) User's Guide".

What is the future status of single DES?

As stated in FIPS PUB 46-3, Single DES will be used for legacy systems only. In general, compliance with this requirement will be determined by the user agency because most of the cryptographic modules are used in products and systems. FIPS 140-1 and FIPS 140-2 testing focus on the specific cryptographic module INDEPENDENT of how the module is used. Therefore, in general, this requirement is outside the scope of the CMT labs.

To reinforce the use of Triple-DES and AES, new DES Algorithm certificates will include the caveat, "Permitted for legacy systems only". Also, the caveat should be included in all new FIPS 140-2 Security Policy submissions that reference the DES implementation.

Finally, when the DES standard comes up for renewal, it is likely that DES will NOT be reaffirmed. If DES is not included in the next version of the DES standard, the CMVP will determine a transition strategy for those validated modules that have included single DES.

What is the specified size of the Prime Modulus p for DSA FIPS PUB 186-2?

As stated in the change notice for FIPS PUB 186-2, "... L should assume only the value 1024 for DSA as specified in FIPS 186-2, ...".

This change is not worded as a mandatory requirement - therefore a vendor may implement DSA with L at 512 bits. NIST, CSE and the CMT labs should make vendors aware of the change notice.

How do random number generators work?

Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: *deterministic* and *nondeterministic*. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed. A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control.

What is the status of random number generators?

The approved RNGs are listed in Annex C to FIPS 140-2. Currently, there are no non-deterministic RNGs that are FIPS approved.

What is the status of SHA-2 (FIPS PUB 180-2) algorithm testing?

FIPS 180-2, Secure Hash Standard (SHS), was signed August 26, 2002. CMVP SHA-2 algorithm testing is not yet available. SHA-2 will be listed (if applicable) on a FIPS 140-1 or FIPS 140-2 validation as non-FIPS-Approved until the CMVP SHA-2 algorithm testing is available.

What is the status of HMAC-SHA-1 (FIPS PUB 198) algorithm testing?

The Keyed-Hash Message Authentication Code (HMAC), FIPS 198, was signed March 6, 2002. CMVP HMAC algorithm testing is not yet available. If a cryptographic module implements HMAC-

SHA-1, to be listed as FIPS-Approved, an HMAC-SHA-1 cryptographic algorithm Known Answer Test (KAT) (re: FIPS 140-2 4.9.1 Power-Up Tests) must be implemented and the underlying SHA-1 algorithm must be validated. [Ex: HMAC-SHA-1 (Cert. #xx, vendor affirmed)].

If a KAT is implemented for the HMAC-SHA-1, a KAT is not needed for the underlying SHA-1.

What is the status of AES MAC?

Work is in progress on AES MAC definition. However at this time, any implementation within a cryptographic module is considered non-FIPS Approved.

What is the status of AES Key Wrapping?

National Institute of Standards and Technology, *Key Management using ANSI X9.17* , Federal Information Processing Standards Publication 171, April 27, 1992 specifies a standard that defines procedures for the manual and automated management of data (e.g., keys and initialization vectors) necessary to establish and maintain cryptographic keying relationships. ANSI X9.17 utilizes the Data Encryption Standard (DES) and has been extrapolated to include Triple-DES. However it does not include the use of AES.

Work is in progress on an AES key agreement specification. Until such time as an AES key agreement specification becomes FIPS-Approved or NIST recommended, AES may be used in a FIPS-Approved mode of operation for key wrapping to provide confidentially ONLY. This method cannot claim, nor be intended to provide, non-repudiation or integrity.

Two implementation options:

1. AES encryption for key wrapping (any mode)
2. AES key wrapping draft specification

What elliptic curves are recognized as FIPS-Approved by the CMVP?

FIPS 186-2, Appendix 6, *Recommended Elliptic Curves for Federal Government Use*, is a recommendation. The CMVP algorithm validation testing scheme for FIPS 186-2 will validate and provide algorithm certificates against the list of recommended curves. If a cryptographic module implements different curves, those will be annotated on the FIPS 140-1 or FIPS 140-2 certificate as *vendor affirmed* and not tested or validated.

What is the status of PKCS#1?

The CMVP continues to recognize PKCS#1 algorithm implementations as FIPS Approved.

What is the status AES MAC for use in OTAR for radios?

Effective December 12, 2003, the CMVP will recognize the use of AES MAC (CBC-MAC based on AES defined in Project 25 TIA-102.AACA-1) for the Digital Radio Over-the-Air Rekeying (OTAR) Protocol when operated in a FIPS Approved mode.

The module Security Policy shall reference this as used in FIPS Approved mode.

It will be listed on the module certificate as a non-FIPS Algorithm but will be annotated as follows:

AES MAC (Cert. #nnn, P25 AES OTAR, vendor affirmed)

nnn – references the underlying FIPS Approved AES algorithm certificate. If the underlying AES algorithm does not have an algorithm certificate, or does not meet the requirements of FIPS 140-2, then the use of AES MAC for OTAR will not be allowed for use in FIPS Approved mode.

Modules that have been validated and have annotated this function as a non-FIPS Approved mode function may have an updated Security Policy re-submitted to change this function to the FIPS Approved mode of operation if the underlying AES algorithm has been validated and AES meets all the FIPS 140-2 requirements.

7. REVALIDATION

7.1 CRYPTOGRAPHIC MODULE REVALIDATION

When do cryptographic modules need to be revalidated?

Cryptographic modules need to be revalidated whenever changes are made to the module. However, the amount of re-testing required depends on the extent of the changes (see below).

Cryptographic modules DO NOT require revalidation solely because the standard to which they were originally validated against is superseded by a new standard.

7.1.1 Revalidation of a Previously Validated FIPS 140-2 Module

Where can I find the latest revalidation guidance?

Revalidation guidance is found in FIPS 140-2 Implementation Guidance, **G.8**.

What is required to revalidate a FIPS 140-2 cryptographic module if non-security relevant changes have been made?

The contracted CMT laboratory will identify the necessary documentation to confirm that FIPS 140-2 security relevant requirements have not been affected by the modification. The vendor is then responsible for providing the applicable documentation to the CMT laboratory. Documentation may include a previous validation report, design documentation, source code, etc. The CMT laboratory will review the modifications and any associated documentation provided by the vendor and issue an explanatory letter to NIST/CSE with applicable Tester Evidences (TEs) listed and the associated laboratory assessments. The assessments must include the analysis performed by the laboratory to confirm that no security relevant requirements were affected. The updated version or release information will be posted on the Validated Modules List using the same entry as for the original cryptographic module. No new certificate will be issued.

What is required to revalidate a FIPS 140-2 cryptographic module when an existing security relevant feature is moved to FIPS Approved mode?

No modifications made to any hardware, software or firmware components of the cryptographic module. All version information is unchanged. Post validation, security relevant functions or services that were not tested during the original validation or were not Approved at the time of validation, are now tested and are being submitted for inclusion as a FIPS Approved function or

service. The CMT laboratory is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient and the vendor is responsible for submitting the requested documentation to the CMT laboratory. Documentation may include a previous validation report and applicable NIST and CSE rulings, design documentation, source code, etc.

The CMT laboratory shall identify the assertions affected and shall perform the tests associated with those assertions. This will require the CMT laboratory to:

a. Review the COMPLETE list of assertions for the module embodiment and security level;
b. Identify, from the previous validation report, the assertions that are newly tested;
c. Identify additional assertions that were previously tested but should now be re-tested; and
d. Review assertions where specific Implementation Guidance (IG) was provided at the time of the original validation to confirm that the IG is still applicable.

The CMT laboratory does not need to perform the regression test suite of operational tests since there is no change to the module.

The CMT laboratory shall document the test results in the associated assessments and all affected TEs shall be annotated as “re-tested.” The CMT laboratory shall submit a delta conformance test report describing the modification and highlighting those assertions that have been newly tested and retested (selecting the re-tested option in CRYPTIK). A new security policy shall be provided for posting that updates the new services or functions that are now included in an Approved mode of operation. Upon a satisfactory review by NIST and CSE, the updated security policy and information will be posted on the Validated FIPS 140-1 and FIPS 140-2 Cryptographic Module List web site entry associated with the original cryptographic module. If new algorithm certificates were obtained, they shall be listed. No new certificate will be issued.

What is required to revalidate a FIPS 140-2 cryptographic module if less than 30% of the operational requirements have been modified?

An updated cryptographic module qualifies for this scenario if less than 30% of the operational requirements need to be retested. The CMT laboratory is responsible for identifying the necessary documentation to determine whether a 30% revalidation is sufficient and the vendor is responsible for submitting the requested documentation to the CMT laboratory. Documentation may include a previous validation report and applicable CMVP guidance/policy, design documentation, source code, etc.

The CMT laboratory will identify the assertions affected by the modification and perform the operational tests associated with those assertions. This will require the CMT laboratory to:

1. Review the COMPLETE list of assertions for the module embodiment and security level,

2. Identify, from the previous validation report, the assertions that have been affected by the modification, and

3. Identify additional assertions that were NOT previously tested but should now be tested due to the modification.

In addition to the tests performed against the affected assertions, the CMT laboratory must also perform the regression test suite of operational tests. The CMT laboratory shall document the test results in the associated assessments and all affected TEs shall be annotated as “re-tested.” The

CMT laboratory can submit a delta conformance test report highlighting those assertions that have been modified and retested. Upon a satisfactory review by the validation authorities, a new certificate will be issued.

What is required to revalidate a FIPS 140-2 cryptographic module if only the physical enclosure has been modified?

Modifications are made only to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module. The CMT laboratory is responsible for ensuring that the change only affects the physical enclosure (integrity) and has no operational impact on the module. The CMT laboratory must also fully test the physical security features of the new enclosure to ensure its compliance to the relevant requirements of the standard. The CMT laboratory must then submit a letter to NIST and CSE that:

a. Describes the change (pictures may be required),
b. States that it is a security relevant change,
c. Provides sufficient information supporting that the physical only change has no operational impact,
d. Describes the tests performed by the laboratory that confirm that the modified enclosure still provides the same physical protection attributes as the previously validated module. For security levels 2, 3 and 4, the submission of an updated Physical Security Test Report is mandatory.

Each request will be handled on a case-by-case basis. The CMVP will accept such letters against cryptographic modules already validated to FIPS 140-1 and FIPS 140-2. Certificates will not be reissued.

An example of such a change could be the plastic encapsulation of the Level 2 token which has been reformulated or colored. Therefore the molding or cryptographic boundary has been modified. This change is security relevant as the encapsulation provides the opacity and tamper evidence requirements. But this can be handled as a letter only change with evidence that the new composition has the same physical security relevant attributes as the prior composition.

What is required to revalidate a FIPS 140-2 cryptographic module if more than 30% of the security-relevant functionality has been modified?

The module must be fully retested under FIPS 140-2 if major changes have been made. A new validation certificate will be issued.

What is required to revalidate a FIPS 140-2 cryptographic module when the overall security level has changed (e.g., from Level 2 to Level 3)?

The module must be retested against the targeted level of FIPS 140-2 requirements. A new validation certificate will be issued.

What is required to revalidate a FIPS 140-2 cryptographic module if the physical embodiment has changed (e.g., from single chip to multi-chip embedded)?

The module must be fully retested under FIPS 140-2 if physical embodiment changes have been made. A new validation certificate will be issued.

Is a revalidation required if the cryptographic module is ported to another platform? (This question applies to software and hardware cryptographic modules.)

Porting a cryptographic module from one platform to another does not affect the module's validation, if the module is not modified. Specific guidance on porting software cryptographic modules is provided found in FIPS 140-2 Implementation Guidance, **G.5**.

7.1.2 Revalidation of a Previously Validated FIPS 140-1 Module to FIPS 140-2

What is required to revalidate a FIPS 140-1 cryptographic module to comply with FIPS 140-2?

The contracted CMT laboratory will identify the necessary documentation for testing the applicable FIPS 140-2 DTR TE's, as indicated in the FIPS 140-1 to FIPS 140-2 Mapping Document. The vendor is responsible for providing the applicable documentation to the CMT laboratory. Documentation may include a previous validation report, design documentation, source code, etc. The CMT laboratory will review the vendor provided documentation, execute the new FIPS 140-2 operational tests, and then submit a written report to the validation authorities. A new certificate will be issued.

7.2 CRYPTOGRAPHIC ALGORITHM REVALIDATION

Is there an expiration date for cryptographic algorithm validations?

A cryptographic algorithm validation remains valid until any changes are made to the algorithm, that is, there is no expiration date for a cryptographic algorithm validation However, as discussed above, DES validations may expire when the next DES standard is published.

8. REFERENCES

8.1 ACRONYMS

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
ATM	Automated Teller Machine
CC	Common Criteria

CBC	Cipher Block Chaining
CM	Configuration Management
CMT	Cryptographic Module Testing
CMV	Cryptographic Module Validation
CMVP	Cryptographic Module Validation Program
CSA	Canadian Standard Association
CSE	Communications Security Establishment
CSP	Critical Security Parameter
DAC	Data Authentication Code
DES	Data Encryption Standard
DOC	Department of Commerce
DOD	Department of Defense
DSA	Digital Signature Algorithm.
DSSVS	Digital Signature Standard Validation System
DTR	Derived Test Requirements
EAL	Evaluation Assurance Level
ECB	Electronic Cookbook Mode
ECDSA	Elliptic Curve Digital Signature Algorithm
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
GoC	Government of Canada
HMAC	Hash Message Authentication Code
IC	Integrated Circuit
IEEE	Institute of Electrical and Electronics Engineers
IG	Implementation Guidance
I/O	Input/Output
ISO	International Organization for Standardization
ITSEC	Information Technology Security Evaluation Criteria
IV	Initialization Vector
KAT	Known Answer Test
KEA	Key Establishment Algorithm
LCD	Liquid Crystal Display
LED	Light Emitting Diode

MAC	Message Authentication Code
MOVS	Modes of Operation Validation System
NBS	National Bureau of Standards
NDA	Non-Disclosure Agreement
NIST	National Institute of Standards and Technology (formerly the National Bureau of Standards)
NSA	National Security Agency
NVLAP	National Validation Laboratory Accreditation Program
OEM	Original Equipment Manufacturer
OFB	Open Feedback Mode
OS	Operating System
OTAR	Over-The-Air-Rekey
PALCAN	Program for Accreditation of Laboratories – Canada
PC	Personal Computer
PIN	Personal Identification Number
PP	Protection Profile
PRNG	Pseudo Random Number Generator
PROM	Programmable Read-Only Memory
RAM	Random Access Memory
RNG	Random Number Generator
ROM	Read-Only Memory
RSA	Rivest, Shamir, Adleman
SCC	Standards Council of Canada
SHA	Secure Hash Algorithm
SPEC PUB	NIST Special Publication
SRDI	Security Relevant Data Item
ST	Security Target
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria
TMOVS	Modes of Operation Validation System for the Triple Data encryption Algorithm
TOE	Target Of Evaluation

8.2 GLOSSARY

The following definitions are from the FIPS 140-2:

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

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

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

a) specified in an Approved standard,
b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or
c) specified in the list of Approved security.

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., secret and private cryptographic keys, and authentication data such as passwords and PINs) whose disclosure or modification can compromise the security of a cryptographic

Cryptographic boundary: an explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components 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, or
- an exchange agreement of a shared secret.

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

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

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

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

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

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

1. origin authentication
2. data integrity, and
3. signer non-repudiation.

Electromagnetic compatibility (EMC): the ability of electronic devices to function satisfactorily in an electromagnetic environment without introducing intolerable electromagnetic disturbances to other devices in that environment.

Electromagnetic interference (EMI): electromagnetic emissions from a device, equipment, or system that interfere with the normal operation of another device, equipment, or system.

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

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

Environmental failure protection (EFP): the use of features 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 the security of a cryptographic module will not be compromised by environmental conditions or fluctuations outside of the module's normal operating range.

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

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

Firmware: the programs and data components of a cryptographic module that are stored in hardware (e.g., ROM, PROM, EPROM, EEPROM or FLASH) within the cryptographic boundary and cannot be dynamically written or modified during execution.

Hardware: the physical equipment within the cryptographic boundary used to process programs and data.

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

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

Input data: information that is entered into a cryptographic module for the purposes of transformation or computation using an Approved security function.
Integrity: the property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

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

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

Key establishment: the process by which cryptographic keys are securely distributed among cryptographic modules using manual transport methods (e.g., key loaders), automated methods (e.g., key transport and/or key agreement protocols), or a combination of automated and manual methods (consists of key transport plus key agreement).

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

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

Key transport: secure transport of cryptographic keys from one cryptographic module to another module.

Manual key transport: a non-electronic means of transporting cryptographic keys.

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

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

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

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

Personal identification number (PIN): an alphanumeric code or password used to authenticate an identity.

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

Plaintext key: an unencrypted cryptographic key.

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

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

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

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

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

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

Random Number Generator: Random Number Generators (RNGs) used for cryptographic applications typically produce a sequence of zero and one bits that may be combined into sub-sequences or blocks of random numbers. There are two basic classes: deterministic and nondeterministic. A deterministic RNG consists of an algorithm that produces a sequence of bits from an initial value called a seed. A nondeterministic RNG produces output that is dependent on some unpredictable physical source that is outside human control.

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

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

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

Security policy: see Cryptographic module security policy.

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

Software: the programs and data components within the cryptographic boundary, usually stored on erasable media (e.g., disk), that can be dynamically written and modified during execution.

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

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

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

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

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

Tamper response: the automatic action taken by a cryptographic module when a tamper detection has occurred (the minimum response action is the zeroization of plaintext keys and CSPs).

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

TEMPEST: a name referring to the investigation, study, and control of unintentional compromising emanations from telecommunications and automated information systems equipment.

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

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

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

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

Zeroization: a method of erasing electronically stored data, cryptographic keys, and CSPs by altering or deleting the contents of the data storage to prevent recovery of the data.

8.3 REFERENCES

Some of the material referenced as part of the creation of this FAQ include the following:

a) FIPS PUB 140-1 - "Security Requirements for Cryptographic Modules", National Institute of Standards and Technology, January 11, 1994.
b) FIPS PUB 140-2 - "Security Requirements for Cryptographic Modules", National Institute of Standards and Technology, May 25, 2001.
c) “A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2”, National Institute of Standards and Technology, June 2001.
d) “Derived Test Requirements for FIPS PUB 140-1, Security Requirements for Cryptographic Modules”, National Institute of Standards and Technology, March 1995.
e) “Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules (Draft)”, National Institute of Standards and Technology, November 15, 2001.

f) “Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program”, National Institute of Standards and Technology, November 1999.

g) “Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program”, National Institute of Standards and Technology, March 2003.

h) FIPS PUB 46-3, “Data Encryption Standard (DES)”, National Institute of Standards and Technology, October 25, 1999.

i) FIPS PUB 74, Guidelines for Implementing and Using the NBS Data Encryption Standard.

j) FIPS PUB 81, DES Modes of Operation, National Institute of Standards and Technology.

k) FIPS PUB 113, Computer Data Authentication, National Institute of Standards and Technology.

l) FIPS 171, “Key Management Using ANSI X9.17”, National Institute of Standards and Technology, April 27, 1992.

m) FIPS 180-1, “Secure Hash Standard”, National Institute of Standards and Technology, April 17, 1995.

n) FIPS 185, “Escrowed Encryption Standard”, National Institute of Standards and Technology, February 9, 1994.

o) FIPS 186-2, “Digital Signature Standard (DSS)”, National Institute of Standards and Technology, January 27, 2000.

p) FIPS 197, “Advanced Encryption Standard (AES)”, National Institute of Standards and Technology, November 26, 2001.

q) “Descriptions of SHA-256, SHA-384 and SHA-512”, National Institute of Standards and Technology, Date Unknown.

r) “Digital Signature Standard Validation System (DSSVS) User’s Guide (For version 2.3 of the DSSVS Software Tool)”, National Institute of Standards and Technology, January 25, 2001.

s) Special Publication 800-2, Public Key Cryptography.

t) NIST Special Publication 800-20, “Modes of Operation Validation System for the Triple Data Encryption Algorithm (TMOVS): Requirements and Procedures”, Sharon Keller, National Institute of Standards and Technology, April 2000.

u) “Skipjack and KEA Algorithm Specifications”, National Institute of Standards and Technology, Version 2.0, May 29, 1998.

v) “The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)”, Lawrence E. Bassham III, National Institute of Standards and Technology, April 23, 2002.

w) “The Multi-Block Message Test (MMT) for DES and TDES” used in conjunction with SP800-17 & 20, National Institute of Standards and Technology, date unknown.

x) “CMVP Status and FIPS 140-1&2”, Annabelle Lee, Director, CMVP, March 26, 2002.

y) NIST Handbook 150, “Procedures and General Requirements”, National Institute of Standards and Technology, March 20, 2001.

z) NIST Handbook 150-17, “Cryptographic Module Testing”, National Institute of Standards and Technology, June 2000.

aa) NIST Special Bulletin 800-23, “Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products – Recommendations of the National Institute for Standards and Technology”, National Institute of Standards and Technology, August 2000.

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

cc) NTISSP No. 11, “National Information Assurance Acquisition Policy”, National Security Agency, January 2000.

dd) NTISSAM INFOSEC/2-00, “Advisory Memorandum for the Strategy for Using the National Information Assurance Partnership (NIAP) for the Evaluation of Commercial Off-The-Shelf (COTS) Security Enabled information Technology Products”, National Security Agency.

8.4 WEB SITES

Some reference web-sites include:

a) National Institute of Standards and Technology (NIST)

b) Computer Security Division (CSD)

c) Cryptographic Module Validation Program (CMVP)

d) Communication Security Establishment of the Government of Canada (CSE)

e) Communications Electronics Security Group (CESG)

f) National Voluntary Laboratory Accreditation Program (NVLAP)

g) National Information Assurance Partnership (NIAP)

h) Common Criteria Evaluation and Validation Scheme (CCEVS)

i) Common Criteria Home Page (CC)

9. END OF DOCUMENT