Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program

National Institute of Standards and Technology
Communications Security Establishment

Last Update: January 10, 2002

Table of Contents

Overview

This Implementation Guidance document is issued and maintained by the U.S. Government's National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) of the Government of Canada, which serve as the validation authorities of the Cryptographic Module Validation Program (CMVP) for their respective governments. The CMVP is a program under which National Voluntary Laboratory Accreditation Program (NVLAP) accredited Cryptographic Module Testing (CMT) laboratories test cryptographic modules for conformance to Federal Information Processing Standard Publication (FIPS) 140-1, *Security Requirements for Cryptographic Modules*. In addition, this program covers the testing of FIPS-approved cryptographic algorithms, including the Data Encryption Algorithm, Digital Signature Algorithm, Secure Hash Algorithm, and Skipjack Algorithm.

This document is intended to provide clarifications of the CMVP, and in particular, clarifications and guidance pertaining to the *Derived Test Requirements for FIPS PUB 140-1* (DTR), which is used by CMT laboratories to test for a cryptographic module's conformance to FIPS PUB 140-1. Guidance presented in this document is based on responses issued by NIST and CSE to questions posed by the CMT labs, vendors, and other interested parties. *However, information in this document is subject to change by NIST and CSE.*

Each section of this document corresponds with a requirements section of FIPS PUB 140-1, with an additional first section containing general guidance that is not applicable to any particular requirements section. Within each section, the guidance is listed according to a subject phrase. For those subjects that may be applicable to multiple requirements areas, they are listed in the area that seems most appropriate. Under each subject there is a list, including the date of issue for that guidance, along relevant assertions, test requirements, and vendor requirements from the DTR. *(Note: For each subject, there may be additional test and vendor requirements which apply.)* Next, there is section containing a question or statement of a problem, along with a resolution and any additional comments with related information. This is the implementation guidance for the listed subject.

Below is a list of where the reader can find cryptographic modules validated to FIPS 140-1 and FIPS 140-2:

- Cryptographic Module Validation List

General Issues

G.1 Implementation guidance requests to NIST and CSE

Applicable Levels:	*ALL*
Effective Dates:	*2/25/97-*
Last Modified:	*12/4/2001*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

To whom should implementation guidance requests be directed? Is there a defined format for those requests?

Resolution

- *Programmatic Questions:* Questions concerning the general operation of the CMV Program can be directed to either NIST or CSE. Here are the appropriate points of contact:
  - **NIST***(12/04/2001)*

    Annabelle Lee
    (301) 975-2941

    Randall J. Easter
    (301) 975-4641

    Nelson Hastings
    (301) 975-5237

    Ray Snouffer
    (301) 975-4436
  - **CSE**
    Jean Campbell
    (613) 991-8121

- *Test-specific Questions:* If a vendor is under contract with a CMT lab for 140-1 or algorithm testing, then the vendor should contact the lab with any questions concerning the test requirements. This allows the lab representatives to use their expertise in 140-1 testing to answer those questions, and it acts as a filter for NIST and CSE.

  Agencies, departments, vendors not under contract with a CMT lab, and CMT labs themselves who have specific questions about a 140-1 test requirement should contact the appropriate NIST and CSE points of contact:
  - **NIST***(12/04/2001)*

Annabelle Lee
(301) 975-2941

Randall J. Easter
(301) 975-4641

Nelson Hastings
(301) 975-5237

Ray Snouffer
(301) 975-4436

- **CSE**
  Jean Campbell
  (613) 991-8121

All test-specific questions asking for implementation guidance shall have the following form, in order for NIST and CSE to understand the question as clearly as possible, and to provide an appropriate response:

3. Applicable statement(s) from FIPS 140-1,
4. Applicable assertion(s) from the DTR,
5. Applicable required test procedure(s) from the DTR,
6. A concise statement of the problem, followed by a clear and unambiguous question regarding the problem, and
7. A statement of the resolution that is being sought.

(4/25/97)
All questions should be presented in a detailed, implementation-specific format, rather than an academic or hypothetical format. This information should also include a brief description of the implementation and the FIPS 140-1 target level. All of this will enable a more efficient and timely resolution of 140-1 related questions by NIST and CSE. When appropriate, NIST and CSE will derive general guidance from the problem and response, and add that guidance to this document. Note that general questions may still be submitted, but these questions should be identified as not being associated with a particular validation effort.

****Note that NIST and CSE will only issue official, written responses when the original request is submitted in writing (e-mail and fax are also acceptable).*

Additional Comments

G.2 Completion of a validation - information that must be provided to NIST and CSE

Applicable Levels:	*ALL*
Effective Dates:	*2/25/97-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What information should be provided to NIST and CSE upon completion of validation testing, in order for a vendor to receive a validation certificate?

Resolution

The following information shall be provided to both NIST and CSE by the testing laboratory:

1. A *non-proprietary* version of the VALIDATION REPORT, which shall include (at a minimum):

    a. Summary Report - a single page which lists the various requirements sections, their target level, the status of each area for that level (passed/failed/not applicable), and the overall level for which the module passed validation testing.

    b. Detailed Report with assessments (and notes, if applicable) - the information in the assessments and notes fields shall include remarks about the module, and briefly explain how the requirement is passed, failed, or not applicable. If specific guidance was issued by NIST and CSE for this cryptographic module during validation testing, then this guidance shall be addressed in the appropriate area(s) of the report.

2. A *non-proprietary* version of the cryptographic module's SECURITY POLICY. For an explanation of this, see the guidance "Cryptographic module security policy" in Section 1 of this document.
3. (IF APPLICABLE) A *non-proprietary* version of the laboratory's physical testing report, for cryptographic modules with physical security at *level 2 and above*.
4. In addition to items 1-3 above, the lab has the option to provide *proprietary* versions of those items, but this is not required by NIST and CSE.

****NOTE: NIST and CSE must have items 1-3 above before a validation certificate will be issued.****

Additional Comments

A copy of each of the above items shall be mailed directly to both NIST and CSE, in order to expedite the review and certificate issuance processes.

G.3 Partial validations

Applicable Levels:	*ALL*
Effective Dates:	*2/25/97-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What is the position of NIST and CSE regarding partial validations?

Resolution

NIST and CSE will not issue a validation certificate unless a cryptographic module meets at least Level 1 security requirements for each area in section 4 of FIPS PUB 140-1. Note that in some cases, a requirements

area might not be applicable to the cryptographic module being tested (e.g., "Operating System"). In those cases, the validation certificate will indicate "N/A" for that requirement.

Additional Comments

G.4 Design and testing of cryptographic modules

Applicable Levels:	*ALL*
Effective Dates:	*11/12/97-*
Last Modified:	*4/28/00*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What activities may CMT laboratories perform, regarding the design and testing of cryptographic modules?

Resolution

The following information is supplemental to the guidance provided by NVLAP, and further defines the separation of the design, consulting, and testing roles of the laboratories. CMV Program policy in this area is as follows:

1. A CMT Laboratory *may not* perform validation testing on a module for which the laboratory has:
    a. designed any part of the module,
    b. developed original documentation for any part of the module,
    c. built, coded or implemented any part of the module, or
    d. any ownership or vested interest in the module.
2. Provided that a CMT Laboratory has met the above requirements, the laboratory *may* perform validation testing on modules produced by a company when:
    a. the laboratory has no ownership in the company,
    b. the laboratory has a completely separate management from the company, and
    c. business between the CMT Laboratory and the company is performed under contractual agreements, as done with other clients.
3. A CMT Laboratory may perform consulting services to provide clarification of FIPS 140-1, the Derived Test Requirements, and other associated documents at any time during the life cycle of the module.

Additional Comments

Item 3 in the Resolution references "other associated documents". Included in this reference are:

- Documents developed by the CMVP staff for the Cryptographic Module testing program (e.g., Implementation Guidance, CMVP Policy, Handbook 150-17, *Cryptographic Module Testing*); and

- Implementation Guidance and Policy associated with FIPS 140-1, *Security Requirements for Cryptographic Modules*.

Also see Guidance 4.1, regarding FSM and Security Policy consolidation and formatting.

G.5 Maintaining validation compliance of software cryptographic modules

Applicable Levels:	*ALL*
Effective Dates:	*11/12/97-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

For a validated software cryptographic module, how may such a module be implemented so that compliance with the validation is maintained?

Resolution

1. The tested/validated configuration is stated on the validation certificate. The certificate serves as the benchmark for the module-compliant configuration.

2. For level 1 Operating System Security, the software cryptographic module will remain compliant with the FIPS 140-1 validation when operating on any general purpose computer (GPC) provided that:

    a. the GPC uses the specified single user operating system/mode specified on the valiation certificate, or another compatible single user operating system, and

    b. the software of the cryptographic module does not require modification when ported (platform specific configuration modifications are excluded).

3. For level 2 Operating System Security the software cryptographic module will remain compliant with the FIPS 140-1 validation when operating on any GPC provided that:

    a. the GPC incorporates the specified evaluated C2 (or equivalent) operating system/mode/operational settings or another compatible evaluated C2 (or equivalent) operating system with like mode and operational settings, and

    b. the software of the cryptographic module does not require modification when ported (platform-specific configuration settings are excluded).

This policy only addresses a module's operating system configuration and does not affect requirements of the other sections of FIPS 140-1. A module must meet all requirements of the level stated. The GPC used with the cryptographic software must meet all physical requirements met by the test platform listed on the validation certificate.

Additional Comments

*Note that this guidance is particularly relevant to **USERS** who are implementing a software module.*

G.6 Modules with both a FIPS mode and a non-FIPS mode

(i.e., modules containing both FIPS-approved and non-FIPS approved security methods)

Applicable Levels:	*ALL*
Effective Dates:	*3/11/98-*
Last Modified:	*4/2/98*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

How can a module be defined, when it includes both FIPS-approved and non-FIPS approved security methods?

Resolution

(4/2/98) A module that contains both FIPS-approved and non-FIPS approved security methods shall have at least one "FIPS mode of operation" - which *only* allows for the operation of FIPS-approved security methods. This means that when a module is in the "FIPS mode", a non-FIPS approved method **SHALL NOT** be used in lieu of a FIPS-approved method (For example, if a module contains both MD5 and SHA-1, then when hashing is required in the FIPS mode, SHA-1 must be used.). The operator must be made aware of which services are FIPS 140-1 compliant.

The FIPS 140-1 validation certificate will identify the cryptographic module's "FIPS mode" of operation.

The selection of "FIPS mode" does not have to be restricted to any particular operator of the module. However, each operator of the module must be able to determine whether or not the "FIPS mode" is selected.

There is no requirement that the selection of a "FIPS mode" be permanent.

Additional Comments

FIPS 140-1 gives several examples of "FIPS approved security methods" in Section 2.1, including "e.g., cryptographic algorithm, cryptographic key generation algorithm or key distribution technique, authentication technique, or evaluation criteria".

G.7 Relationships Among Vendors, Laboratories, and NIST/CSE

Applicable Levels:	*ALL*
Effective Dates:	*4/14/98-*
Last Modified:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What is the Cryptographic Module Validation Program policy regarding the relationships among vendors, testing laboratories, and NIST/CSE?

Policy

The CMT laboratories are accredited by NVLAP to perform cryptographic module validation testing to determine compliance with FIPS 140-1. NIST/CSE rely on the CMT laboratories to use their extensive validation testing experience and expertise to make sound, correct, and independent decisions based on FIPS 140-1, the Derived Test Requirements, and Implementation Guidance. Once a vendor is under contract with a laboratory, NIST/CSE will only provide official guidance and clarification for the vendor's module through the point of contact at the laboratory.

In a situation where the vendor and laboratory are at an unresolvable impasse over a testing issue, the vendor may ask for clarification/resolution directly from NIST/CSE. The vendor should use the format required by Implementation Guidance G.1 and the point of contact at the laboratory ***must*** be carbon copied. All correspondence from NIST/CSE to the vendor on the issue will be issued through the laboratory point of contact.

Additional Comments

G.8 Revalidation Requirements

Applicable Levels:	*ALL*
Effective Dates:	*11/5/2001*
Last Modified:	*8/17/2001*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What is the Cryptographic Module Validation Program (CMVP) policy regarding revalidation requirements and validation of a new cryptographic module that is significantly based on a previously validated module?

Policy

An updated version of a previously validated cryptographic module can be considered for a revalidation rather than a full validation depending on the extent of the modifications from the previously validated version of the module. (Note: the updated version may be, for example, a new version of an existing crypto module or a new model based on an existing model.)

There are two possible scenarios:

1. Modifications are made to hardware, software or firmware components that do not affect any FIPS 140-1 security relevant items. The CMT laboratory is responsible for identifying the necessary documentation to confirm that FIPS 140-1 security relevant items have not been affected by the modification. The vendor is then responsible to provide 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 TEs listed and associated laboratory assessment. The assessment shall include the analysis performed by the laboratory to confirm that no security relevant TEs were affected. The updated version or release

information will be posted on the FIPS 140-1 Cryptographic Module Validation List entry associated with the original cryptographic module. No new certificate will be issued.

2. Modifications are made to hardware, software or firmware components that affect some of the FIPS 140-1 security relevant items. An updated cryptographic module can be considered in this scenario if it is similar to the original module with only minor changes in the security policy and FSM, and less than 30% of the assertions in the FIPS 140-1 conformance test report are affected. 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/CSE rulings, design documentation, source code, etc.

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

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

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

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

   4. Review assertions where specific Implementation Guidance (IG) was provided to confirm that the IG is still applicable.

   For example, a revision to a firmware component that added security functionality may require a change to assertions in Section 1.

   In addition to the tests performed against the affected assertions, the CMT laboratory shall also perform the regression test suite of operational tests included in Attachment A. 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 NIST/CSE, a new certificate will be issued.

3. If modifications are made to hardware, software, or firmware components that do not meet the above criteria, then the cryptographic module will be considered a new module and must undergo a full validation testing by an accredited CMT laboratory.

4. If the overall Security Level of the crypto module changes or if the physical embodiment changes, e.g., from multi-chip standalone to multi-chip embedded, then the cryptographic module will be considered a new module and must undergo full validation testing by an accredited CMT laboratory.

Additional Comments

A cryptographic module that is revalidated must meet ALL current standards and IGs. The CMT laboratory is responsible for requesting from the vendor all the documentation necessary to determine whether the cryptographic module meets the current standards and IGs. This is particularly important for features/services of the cryptographic module that required a specific ruling from NIST/CSE. For example, a cryptographic module may have been validated with an implementation of Triple DES that has not been tested. If the same cryptographic module is later submitted for revalidation, this Triple DES implementation must be tested and validated against FIPS 46-3, and the cryptographic module must meet the applicable FIPS 140-1 requirements, e.g., self tests.

ATTACHMENT A

FIPS 140-1 Revalidation: Regression Test Suite

Assertion	Test Evidence	Level 1	Level 2	Level 3	Level 4
Section 1 - Cryptographic Module					
	None				
Section 2 - Module Interfaces					
AS02.04	TE02.04.02	X	X	X	X
	TE02.04.04	X	X	X	X
AS02.12	TE02.12.02	X	X	X	X
AS02.13	TE02.13.01			X	X
Section 3 - Roles and Services					
AS03.06	TE03.06.02	X	X	X	X
	TE03.06.03	X	X	X	X
AS03.07	TE03.07.03	X	X	X	X
AS03.10	TE03.10.02	X	X	X	X
AS03.13	TE03.13.02	X	X	X	X
AS03.14	TE03.14.02		X		
AS03.15	TE03.15.02		X		
AS03.16	TE03.16.02			X	X
	TE03.16.03			X	X
AS03.17	TE03.17.02			X	X
Section 4 - Finite State Machine Model					
AS04.11	TE04.11.02	X	X	X	X
Section 5 - Physical Security					
	None				
Section 6 - Software Security					
	None				
Section 7 - Operating System Security					
AS07.02	TE07.02.02	X	X	X	X
AS07.04	TE07.04.01	X			
AS07.06	TE07.06.02		X	X	X
AS07.11	TE07.11.02		X	X	X
AS07.13	TE07.13.01			X	X
AS07.15	TE07.15.03			X	X
AS07.16	TE07.16.04			X	X
Section 8 - Cryptographic Key Management					
AS08.02	TE08.02.02	X	X	X	X
AS08.03	TE08.03.02	X	X	X	X
AS08.07	TE08.07.02	X	X	X	X
AS08.09	TE08.09.02	X	X	X	X
AS08.10	TE08.10.02	X	X	X	X
	TE08.10.03	X	X	X	X
AS08.12	TE08.12.02	X	X	X	X
AS08.13	TE08.13.02	X	X	X	X
AS08.15	TE08.15.03			X	X
AS08.18	TE08.18.02	X	X	X	X
AS08.19	TE08.19.02	X	X	X	X
Section 9 - Cryptographic Algorithms					
	None				
Section 10 - EMI / EMC					

Assertion	Test Evidence	Level 1	Level 2	Level 3	Level 4
	As required				
Section 11 - Self-Tests					
AS11.02	TE11.02.03	X	X	X	X
AS11.03	TE11.03.03	X	X	X	X
AS11.06	TE11.06.01	X	X	X	X
AS11.07	TE11.07.02	X	X	X	X
AS11.09	TE11.09.02	X	X	X	X
AS11.14	TE11.14.06	X	X	X	X
AS11.16	TE11.16.02			X	X
AS11.20	TE11.20.04	X	X	X	X
AS11.21	TE11.21.02	X	X	X	X

Section 1 - Cryptographic Module Design and Documentation

1.1 Non-validated security sub-elements

Applicable Levels:	ALL
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	General, AS01.01
Relevant Test Requirements:	TE01.01.01-.03
Relevant Vendor Requirements:	VE01.01.01

Question/Problem

Will a FIPS PUB 140-1 certificate be issued for a cryptographic module containing non-validated security sub-elements? Or must a vendor use only security-relevant components and sub-elements for which they have complete design information in order to receive FIPS PUB 140-1 validation?

Resolution

It is recognized that vendors may implement security-related cryptographic module sub-elements that are developed by another vendor (e.g., a DES chip). It is the testing laboratory's responsibility, however, to ensure that all security-related functions and elements contained in the cryptographic module meet test requirements. Even if a cryptographic module's sub-elements are proprietary or classified, the laboratory shall have access to the following information:

1. security functions performed by the cryptographic module;
2. the cryptographic module's interface commands;
3. how roles map to services within the cryptographic module; and
4. a finite state machine model for the cryptographic module.

Having access to these four items should be sufficient for determining if the cryptographic module passes particular validation tests, including cases where sub-elements may contain proprietary or classified information.

Additional Comments

1.2 Re-validation of sub-elements

Applicable Levels:	ALL
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	General, AS01.01
Relevant Test Requirements:	TE01.01.01-.03
Relevant Vendor Requirements:	VE01.01.01

Question/Problem

What is the position on the re-validation of sub-elements that have been validated previously by either the current testing laboratory or another laboratory?

Resolution

Currently, NIST and CSE do not have enough experience to *generalize* whether a sub-element validated in one FIPS PUB 140-1 cryptographic module validation can be re-used in another validation without being re-tested. If a laboratory wants to accept a cryptographic module sub-element that was tested in another cryptographic module validation, then this must be approved by NIST or CSE on a case-by-case basis. This applies to previous testing by the same lab or a different lab. Once NIST, CSE, and the laboratories have gained more experience regarding sub-element re-testing, then the determination of re-testing may be generalized for particular tests, areas, and/or security levels.

Additional Comments

At the present time, consistent with their quality systems, laboratories may sub-contract tests to non-CMT labs, and so the possibility of sub-contracting testing to another CMT lab exists. However, in both situations, there must be a single laboratory that takes responsibility for the validation.

1.3 Cryptographic boundary must be fixed

Applicable Levels:	ALL
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS01.02
Relevant Test Requirements:	TE01.02.03-.04
Relevant Vendor Requirements:	VE01.02.01

Question/Problem

Can the cryptographic boundary include different components at different times?

Resolution

No. The cryptographic boundary must be defined and must be static. FIPS PUB 140-1 states in section 4.1, and VE01.02.01 that "The cryptographic boundary shall be an explicitly defined, contiguous perimeter that establishes the physical bounds of the cryptographic module." There are many requirements throughout the standard that are specified based on the cryptographic boundary of the module. Requirements that are heavily dependent on the cryptographic boundary include (but are not limited to):

- Module Interfaces
- Roles and Services
- Physical Security

- Operating System Security
- Key Management

A defined cryptographic boundary that would allow for some components to be within the module at specific times, and not within it at other times would place a "time" factor on these requirements; some requirements would be applicable to different parts of the module depending on where the cryptographic boundary is at what time. This was not intended, and as a result may reduce the intended strength of the requirements.

Additional Comments

1.4 Limiting requirements on a sub-module within a cryptographic module

Applicable Levels:	ALL
Effective Dates:	9/16/96-
Last Modified:	
Relevant Assertions:	AS01.02, AS01.06, AS06.01
Relevant Test Requirements:	TE01.02.01, TE01.02.05, TE01.06.01-.02, TE06.01.01
Relevant Vendor Requirements:	VE01.02.01-.02, VE01.06.01-.02, VE06.01.01

Question/Problem

How does one determine if FIPS 140-1 requirements should apply to a sub-module within a cryptographic module?

Resolution

The following guidelines might be used with any type of sub-module (software, firmware, or hardware) in order to determine if particular FIPS 140-1 requirements apply. If a vendor indicates that a sub-module falls into one of the following three categories, then it is up to the testing laboratory to determine whether or not that is valid. If it is determined to be valid, then the lab shall indicate what requirements and tests are affected in the validation testing report. Certain requirements and tests might not apply if a sub-module can be placed in any of the three following categories:

I. The sub-module is isolated from the rest of the cryptographic module so that it cannot adversely affect the security of the cryptographic module. In this case, the sub-module performs no security related functions.

II. The sub-module performs one or more generic, basic functions which are used by a cryptographic function, and all of the following conditions hold:

   A. the sub-module is offered in a generic Commercial-Off-The-Shelf (COTS) product which has been widely distributed and tested;

   B. in general, the sub-module was not designed for security purposes;

   C. the vendor did not make any alterations to the sub-module and took steps to ensure that the sub-module was implemented without modification (i.e., shrink-wrapped software is used; source code is re-compiled but not modified; etc.);

   D. the cryptographic module performs known answer tests (if applicable) which verify the correct operations of the sub-module's security related functions (e.g., KAT's on basic math functions that were not specifically designed for implementing crypto, etc.).

III. The sub-module performs security related functions which are classified (e.g., SKIPJACK), and the implementation is vouched for by the U.S. and/or Canadian governments. In this case, the classified details need not be provided. However, requirements that do not conflict with the classified nature of the sub-module still apply (e.g., requirements pertaining to: known answer tests, finite state machine model, sub-module's interface commands, security functions that are performed by the sub-module, and mapping of roles to services provided by the sub-module, etc.).

Additional Comments

An example of such a sub-module might be a resistor, memory chip, power supply, or other component in a hardware cryptographic module. The vendor could argue that such components fall under category II, parts A, B, and C in the above guidance.

1.5 Cryptographic module security policy

Applicable Levels:	ALL
Effective Dates:	2/25/97-
Last Modified:	9/16/98
Relevant Assertions:	AS01.07, AS06.03, AS06.07, AS06.08
Relevant Test Requirements:	TE01.07.01, TE06.03.01, TE06.07.01, TE06.08.01
Relevant Vendor Requirements:	VE01.07.01, VE06.03.01, VE06.07.01, VE06.08.01

Question/Problem

At what level of detail shall the cryptographic module security policy be written? What types of services shall be addressed in the security policy?

Resolution

There is a distinction pertaining to two "types" of security policies which are needed (by the labs and validation authorities):

- First, a security policy of some type must be provided to a laboratory so that it can perform all tests which reference the security policy. There is no requirement that a policy be contained in a single document; it may in fact be embodied in multiple documents, so long as all of the necessary information is available to the laboratory during testing. This policy may perhaps contain proprietary information.
- Second, a NON-PROPRIETARY security policy must be submitted to the validation authorities (NIST and CSE) prior to issuance of a validation certificate. This document MAY be identical to the security policy originally provided to the laboratory, but it does not have to be. This document will be retained by NIST and CSE along with the validation report, so that it can be released to entities (presumably potential customers) which have an interest in the product, and wish to learn more about it by examining the security policy. This document shall incorporate the following features:
- It shall NOT include ANY proprietary information, and there shall be no markings on the document indicating that it contains any of such information.

    1. It shall list roles and services of the module (and how they are related), different types of critical security parameters (keys, key components), capabilities, protection, etc.

    2. It shall be relatively brief (on the order of 10 pages or LESS), and understandable to a user who is not necessarily familiar with the cryptographic module.

    (9/16/98)

3. It may be copyrighted, HOWEVER it SHALL be marked in such a way that NIST and CSE can copy/release it as necessary, without having to get special written permission from the vendor (e.g., the copyright statement might contain the words, "May be reproduced only in its entirety [without revision]".).

Additional Comments: (11/24/97)
Also see Guidance 4.1, regarding Security Policy consolidation and formatting

1.6 Cryptographic Module Designation

Applicable Levels:	ALL
Effective Dates:	6/18/01-
Last Modified:	
Relevant Assertions:	AS01.01
Relevant Test Requirements:	TE01.01.01-03
Relevant Vendor Requirements:	VE01.01.01, VE09.01.01

Introduction

The FIPS cryptographic algorithm or FIPS 140-1 cryptographic module validations require the identification or exact designation of the *object* that is undergoing test and subsequent validation. ISO 9000 and any configuration management methodology is dependent on knowing exactly what level, version, part number, etc. that represents the object. Without this knowledge, it is not possible to ascertain what has been tested, what is validated and what a user purchases and deploys. FIPS 140-1 cryptographic module validations also reference pertinent cryptographic algorithm validation certificates. There must be a correlation between the objects that the algorithm certificate represents and the cryptographic module under validation.

Question/Problem

What designation information (and at what granularity) must be provided for cryptographic algorithm/module validation? What is the correspondence between algorithm designations and FIPS 140-1 designations?

Resolution

- When a cryptographic object is submitted for FIPS algorithm validation, information must be provided that uniquely and precisely identifies the object under test. A cryptographic object is a collection of hardware, software and/or firmware that constitutes the embodiment of the cryptographic algorithm. A level, version, part number, etc must be provided for the object. For example, a software .DLL that implements SHA-1 would require a version or level identifier.

- When a cryptographic module is submitted for FIPS 140-1 validation, information must be provided that uniquely and precisely identifies the components undergoing validation. Components may be hardware, software and/or firmware. A level, version, part number, etc must be provided for each component, as applicable. This identifier must be provided to end users of the products so that an end user can ascertain that the product they have deployed is the same as the validated cryptographic module.

- In section VE09.01.01, FIPS Approved algorithms that are embodied in the cryptographic module must be referenced by their NIST algorithm certificate number. During the testing for conformance to FIPS 140-1 by the laboratory, the tester SHALL verify that the level, version, part number, etc. of the cryptographic object that is specified on the algorithm certificate matches the reference listed in the cryptographic module under test. Sub-components that are validated to

FIPS Approved algorithms may be referenced by their algorithm certificate number by more than one FIPS 140-1 cryptographic module if it is used in many embodiments.

Additional Comments:

Section 2 - Module Interfaces

2.1 Maintenance access interface on a general purpose PC at Level 1

Applicable Levels:	1
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS02.03
Relevant Test Requirements:	TE02.03.02
Relevant Vendor Requirements:	VE02.03.02

Question/Problem

If the cryptographic module is implemented as software running on a general purpose PC, does removal of the cover constitute a maintenance action and thus require that a maintenance role be present?

Resolution

No. The removal of a cover on a PC does not constitute a maintenance access for Level 1 (for module interface requirements). Since there is no maintenance access interface, no maintenance role is required (as per AS03.03), and AS03.04 (e.g., the cryptographic module shall clear all keys and other critical security parameters) need not be enforced.

Additional Comments

This resolution applies to Level 1 software cryptographic modules running on a PC only. This resolution does not currently apply to Level 1 hardware cryptographic modules that may reside within a general purpose PC, nor does it apply to Levels 2-4.

2.2 Zeroization requirements

Applicable Levels:	ALL
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS02.07
Relevant Test Requirements:	TE02.07.02
Relevant Vendor Requirements:	VE02.07.01

Question/Problem

Test TE02.07.02 says that "Zeroization techniques may include overwriting memory, or shorting memory to ground if the vendor shows that this drains off all charge within a few seconds." Given knowledge of a cryptographic module's design, along with some basic tools, a `few seconds' might be sufficient for an attacker to obtain keys from memory before they are zeroized. In addition, other parts of the DTR refer to the

`immediate' zeroization of keys when tampering is detected. Thus allowing for a `few seconds' would seem to contradict these other requirements.

Resolution

The ability for someone to open a module's cover and access keys in memory before they are zeroized depends heavily on the design and configuration of the cryptographic module. Depending on the design and configuration, the time between tamper detection and zeroization can be on the order of a few milliseconds to several seconds. But in essence, a person shall not be able to physically open the cryptographic module's cover and obtain the keys from memory, even given detailed knowledge of the module's design. If a tester can open a cryptographic module's maintenance access interface and access plaintext private and secret keys, or other critical security parameters in memory (e.g., by methods described in TE02.07.02) before they are zeroized, then this test (TE02.07.02) is failed.

The reference to `immediate' zeroization of keys (e.g., in VE05.10.01) means that upon detection of tampering, the cryptographic module shall `drop everything' and perform zeroization. When tamper detection occurs, the next action of the module is to enter the state where zeroization takes place. `Immediate' is not used in the sense of time, but rather it refers to states and functions of the cryptographic module.

Additional Comments

2.3 Input/output of public keys versus secret and private keys

Applicable Levels:	3, 4
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS02.13
Relevant Test Requirements:	TE02.13.01
Relevant Vendor Requirements:	VE02.13.01

Question/Problem

There is a requirement at levels 3 and 4 that "plaintext cryptographic keys, plaintext authentication data, and other unprotected critical security parameters" be input and output using ports that are physically separate from all other ports of the module. Do plaintext public keys (for use with a public key cryptographic algorithm) have to likewise be input/output using physically separate ports?

Resolution

No. In this assertion, "cryptographic keys" is referring to secret or private keys, which need to be protected from disclosure. Public keys would fall under the category of "other data" (which is not a critical security parameter). Public keys do not have to be encrypted before they are input/output to/from the module.

Additional Comments

2.4 Using the same physical port for input and output of plaintext crypto keys

Applicable Levels:	3, 4
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS02.13
Relevant Test Requirements:	TE02.13.01
Relevant Vendor Requirements:	VE02.13.01

Question/Problem

There is a requirement at levels 3 and 4 that "plaintext cryptographic keys, plaintext authentication data, and other unprotected critical security parameters" be input and output using ports that are physically separate from all other ports of the module. In addition to the physical separation of ports for critical security parameters and all other ports, must the input ports be physically separate from the output ports?

Resolution

No. Although the standard and DTR do not preclude the use of physically separate ports for the input of critical security parameters and the output of critical security parameters, this is *not* a requirement. The important distinction in this assertion is the separation of ports used for handling critical security parameters and all other ports.

Additional Comments

2.5 Logical interfaces for hardware modules

Applicable Levels:	ALL
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS02.02
Relevant Test Requirements:	TE02.02.01-.04
Relevant Vendor Requirements:	VE02.02.01-.04

Question/Problem

A module is required to have at least four logical interfaces, for: 1) data input, 2) data output, 3) control input, and 4) status output. If there are two buffers being used, one for input and another for output, can one interface be used for both data and control input, and another interface for data and status output?

Resolution

Yes. The standard does not preclude a module from using the same input interface for both data and control input - and the same holds for the output interface. However, there shall be some way for the module to distinguish between data and control (or data and status) information.

Additional Comments

Section 3 - Roles and Services

3.1 Maintenance role requirement for power-on self-tests

Applicable Levels:	ALL
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS03.01, AS11.01
Relevant Test Requirements:	TE03.01.01-.02
Relevant Vendor Requirements:	VE03.01.01

Question/Problem

Does the presence of power-on self-tests, or other self-tests, imply that a maintenance role is necessary to invoke them?

Resolution

Self-tests, as defined under section 4.11 of FIPS 140-1, whether defined as power-up self-tests, conditional self-tests, self-tests that are callable upon demand, or other self-tests as implemented by the vendor, are not to be considered as maintenance tests or actions; hence, a maintenance role is not implied.

Additional Comments

A vendor may choose to define self-tests as maintenance tests if the vendor decides this is necessary.

3.2 Delineation of services between roles

Applicable Levels:	ALL
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS03.01, AS03.02, AS03.07
Relevant Test Requirements:	TE03.01.01, TE03.02.01, TE03.07.01-.03
Relevant Vendor Requirements:	VE03.01.01, VE03.02.01, VE03.07.01-.02

Question/Problem

Does the presence of two or more roles imply that different services must be available for each role? Can all services be the same for all roles?

Resolution

More than one role can have the same set of services. If a cryptographic module does not delineate between the services accessible to any role (i.e., all services are available to all roles and no delineation of that role exists within the cryptographic module), then it is only necessary for the vendor to document the services offered in terms of two roles - User and Crypto-Officer. Both of these roles, at a minimum, must be supported by a cryptographic module (at any level - see AS03.02). Services need not be restricted in either role.

Additional Comments

3.3 Implementation of the "Show Status" service

Applicable Levels:	ALL
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS03.07, AS03.08
Relevant Test Requirements:	TE03.07.01, TE03.08.01-.02
Relevant Vendor Requirements:	VE03.07.01, VE03.08.01

Question/Problem

What types of status must be shown by the cryptographic module? Is a "Percentage Complete" status necessary during long operations such as key generation or encryption?

Resolution

For the "Show Status" service, a cryptographic module must, at a minimum, show the status, where practical, in terms of the Finite State Machine at a particular point in time (i.e., current state of the module). VE03.07.01 presents several possible functions to which the "Show Status" service might be applied. "Show Status" does not have to be applied to those functions which are listed, nor is this list exclusive; therefore it is possible to implement a "Percentage Complete" status, but it is not required.

Additional Comments

3.4 Authentication mechanisms

Applicable Levels:	3, 4
Effective Dates:	2/25/97-
Last Modified:	12/22/98
Relevant Assertions:	AS03.16
Relevant Test Requirements:	TE03.16.01
Relevant Vendor Requirements:	VE03.16.01

Question/Problem

Are the authentication mechanisms specified in TE03.16.01 listed in an order of increasing level of security? What types of authentication mechanisms shall be used at particular security levels?

Resolution

The authentication mechanisms listed in section 4.3.3 of FIPS PUB 140-1 are *examples* of how an operator can be authenticated. This list is not exhaustive. TE03.16.01 and FIPS PUB 140-1 do not imply a hierarchy of these methods (i.e., that one is more robust than the other), nor does FIPS PUB 140-1 require certain mechanisms to be applicable for a certain level. The requirements in FIPS PUB 140-1 (for Levels 3 and 4) is that the module be able to uniquely identify and verify the identity of the operator regardless of the identification and authentication technique used.

Additional Comments

More guidance on these authentication mechanisms can be found in:

- FIPS 112, *Password Usage*,
- FIPS 181, *Automated Password Generator*, and
- FIPS 190, *Guideline for the Use of Advanced Authentication Technology Alternatives*, and
- FIPS 196, *Entity Authentication Using Public Key Cryptography*.

3.5 Identity-based authentication requirements

Applicable Levels:	3, 4
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS03.20
Relevant Test Requirements:	TE03.20.01
Relevant Vendor Requirements:	VE03.20.01

Question/Problem

Can a single-user module meet the identity-based authentication requirements for Level 3 and 4?

Resolution

Yes. FIPS PUB 140-1 specifies identity-based authentication as the ability of a cryptographic module to "authenticate the identity of an operator and verify that the identified operator is authorized to assume a specific role (or set of roles). The module shall require that the operator be individually identified and that the specified identity be authenticated" [FIPS PUB 140-1, 4.3.3]. For modules that can support multiple users, the requirement for identity-based authentication does require that a user be identified and authenticated against the pool of other users of the module. However it is not the intent of FIPS PUB 140-1 to implicitly require that all modules at Level 3 (of roles & services requirements) have the capability to support multiple simultaneous users. A single-user module must be able to recognize and verify the identity of the one specified user, using an authentication mechanism that is capable of providing identity-based authentication.

Additional Comments

3.6 Maintenance role and zeroization of unprotected critical security parameters (CSPs)

Applicable Levels:	ALL
Effective Dates:	12/15/97-
Last Modified:	9/28/98
Relevant Assertions:	AS03.03, AS03.04, AS02.05, AS02.07
Relevant Test Requirements:	TE03.03.01, TE03.04.01-.02, TE02.05.01, TE02.07.01-.02
Relevant Vendor Requirements:	VE03.03.01, VE03.04.01, VE02.05.01, VE02.07.01

Question/Problem

What are the basic requirements concerning the maintenance role and zeroization of unprotected critical security parameters (CSPs) ?

Resolution

At **all** levels of Roles and Services, a maintenance role is required if the module has a maintenance access interface. When entering this role, the module shall zeroize all unprotected CSPs prior to performing any other maintenance services, whether or not the operator is authenticated. *(9/28/98 - clarified) "Zeroization" shall be enforced by the module when the maintenance role is entered.*

Level 1 physical security does not provide physical security mechanisms above and beyond the requirement that the module be "production quality". For modules which meet only level 1 in physical security, it is acceptable for zeroization upon entering the maintenance role to be performed **procedurally**. "Procedural zeroization" refers to zeroization that is *not* enforced by the module.

If zeroization is implemented procedurally in the module, then the procedure for zeroizing unprotected CSPs shall be clearly described in the module's security policy.

Additional Comments

3.7 Use of HMAC for user/operator authentication

Applicable Levels:	2, 3, 4
Effective Dates:	10/6/99-
Last Modified:	
Relevant Assertions:	AS03.14, AS03.16
Relevant Test Requirements:	TE03.14.01-.02, TE03.16.01-.03
Relevant Vendor Requirements:	VE03.14.01, VE03.16.01

Question/Problem

Can HMAC (Hash-based Message Authentication Code) be used to perform user/operator authentication?

Resolution

A cryptographic module may implement HMAC to meet the user/operator authentication requirements of FIPS 140-1. If HMAC is implemented, SHA-1 shall be used as the FIPS-approved hashing algorithm.

If HMAC is used as part of a public key based key exchange/distribution method, then the requirements of Section 4.8.2, Key Distribution, are applicable.

If the key used in the HMAC algorithm is generated by the cryptographic module, the requirements of Section 4.8.1, Key Generation, are applicable.

The key used in the HMAC algorithm shall meet the requirements of Section 4.8.5, Key Destruction.

Additional Comments

Section 4 - Finite State Machine Model

4.1 FSM and Security Policy consolidation and formatting

Applicable Levels:	ALL
Effective Dates:	11/24/97-
Last Modified:	4/28/00
Relevant Assertions:	AS04.01-.04, AS01.07
Relevant Test Requirements:	TE04.01(-.04).01, TE01.07.01
Relevant Vendor Requirements:	VE04.02.01, VE04.04.01, VE01.07.01

Question/Problem

May a CMT lab assemble the FSM and Security Policy from existing vendor documentation?
Resolution
A CMT lab may take existing vendor documentation for an existing cryptographic module (design phase completed) and consolidate or reformat the existing information (from multiple sources) into a set format. *(9/28/98)* If this occurs, NIST and CSE shall be notified of this when the validation report is submitted.
For the **FSM**, the vendor-provided documentation must readily provide 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).
For the **Security Policy** the vendor-provided documentation must readily provide a precise specification of the security rules under which a cryptographic module must operate, including the security rules derived from the requirements of FIPS 140-1 and the additional security rules imposed by the vendor.
In addition, a lab must be able to show a mapping from the consolidated or reformatted FSM and/or Security Policy back the original vendor source documentation. This mapping must be maintained by the lab as part of its validation records.

Additional Comments

The first paragraph under **Resolution** states that, "A CMT lab may take existing vendor documentation for an existing cryptographic module (design phase completed) and consolidate or reformat the existing information…" Consolidation is defined as follows:

- The original source documents were prepared by the vendor (or a subcontractor to the vendor) and submitted to the laboratory with the cryptographic module.
- The laboratory extracts applicable technical statements from the original source documentation to be used in the FSM and/or Security Policy. The technical statements may **only** be reformatted to improve readability of the FSM and/or Security Policy. The content of the technical statements must not be altered.
- The laboratory may develop transitional statements in the FSM and/or Security Policy to improve readability. These transitional statements shall be specified as developed by the laboratory in the mapping.

Also see Guidance G.4 for more information on what a CMT lab may and may not do.

Section 5 - Physical Security

5.1 Conformal coating features

Applicable Levels:	2, 3, 4 (multi-chip embedded)
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS05.09
Relevant Test Requirements:	TE05.09.01
Relevant Vendor Requirements:	VE05.09.01

Question/Problem

If the conformal coating used to encapsulate a multiple-chip, embedded cryptographic module can be scratched, without marking the cryptographic module, so that writing can be read off of an embedded feature (e.g., memory chip, processor, capacitor, etc.), does this meet the requirement for tamper evidence? This might be possible if the color of the coating is identical to (or close to) the color of the underlying feature.

Resolution

Since the conformal coating is supposed to be visibly opaque, no writing on an embedded feature shall be visible. Therefore if writing is visible, that in itself can be considered as evidence of tampering. One way that this might be more effective in providing tamper evidence, is if the color of the coating contrasts with the colors of underlying features on the encapsulated cryptographic module module.

Additional Comments

5.2 Tamper evidence requirements and logical module interfaces for PC-like modules

Applicable Levels:	2, 3, 4 (multi-chip standalone and embedded)
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS05.09, AS05.19, AS02.02
Relevant Test Requirements:	TE05.09.01, TE05.19.01, TE02.02.01-.04
Relevant Vendor Requirements:	VE05.09.01, VE05.19.01, VE02.02.01-.04

Question/Problem

If a personal computer is to be implemented as a cryptographic module with physical security of level 2 or higher, how does one treat the keyboard and other similar devices, with respect to tamper evidence?

Resolution

In a typical PC configuration consisting of a monitor, keyboard, and *system unit* (containing the motherboard, memory, microprocessor(s), circuitry that comes in contact with security-relevant data), one may define the enclosure containing the system unit as the cryptographic module boundary, with the monitor and keyboard existing outside of that boundary. As such, there are several ports that function as module interfaces:

a. Keyboard port - logical data input interface;

b. Disk drive and network "ports" - logical data input/output interfaces; and

c. Monitor and printer port - logical data output interfaces.

The standard defines a port ("a functional unit of a cryptographic module through which data or signals can enter or exit the module"[Section 2.1]), and makes a distinction between ports and covers ("Documentation shall include a complete specification of the interfaces of a cryptographic module, including any physical or logical ports, physical covers or doors..."[Section 4.2]). At level 2 and above, there are no requirements or tests for tamper evidence other than on removable covers and doors. *Thus, there are no requirements for tamper evidence on the various ports listed above* (e.g., there does not have to be a tamper evident seal on the keyboard jack where it plugs into the keyboard port, etc.)

Additional Comments

This guidance can also be applied to multi-chip embedded modules, such as a PC adapter, which has input/output ports.

5.3 Additional tamper evidence for embedded modules

Applicable Levels:	2, 3, 4 (multi-chip embedded)
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	related to AS05.09
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What kind of tamper evidence is provided if the cryptographic module is embedded inside a larger device (e.g., it is an adapter inside a computer?

Resolution

In the case where an embedded cryptographic module is used inside a larger embodiment, there are no tamper evidence requirements on that larger embodiment. For example, if the cryptoboundary is defined to only contain an adapter, and it is used inside a PC, there is no requirement in FIPS 140-1 to provide tamper evidence on the cover of the PC. The only place where place where tamper evidence is applicable (at level 2 and higher) is on the adapter itself.

Therefore, it may be desirable for the vendor or customer to use tamper evident measures (e.g., cover locks, tamper evident seals, etc.) on the larger embodiment that contains the embedded cryptographic module. However, this lies outside the scope of this standard.

Additional Comments

5.4 Tamper evidence for cryptographic modules with physical security at levels 3 and 4

Applicable Levels:	3, 4
Effective Dates:	2/25/97-
Last Modified:	
Relevant Assertions:	AS05.03, AS05.09, AS05.19
Relevant Test Requirements:	TE05.03.01, TE05.09.01, TE05.19.01
Relevant Vendor Requirements:	VE05.03.01, VE05.09.01, VE05.19.01

Question/Problem

For cryptographic modules that are targeting levels 3 and 4 for physical security, do they also have to meet tamper evidence requirements for modules with level 2 physical security?

Resolution

The entire rationale of FIPS 140-1 is to provide for increasing levels of security; thus each level adds new features, and builds upon the previous levels.

Tamper evidence and tamper detection/response are not necessarily mutually exclusive. The former warns the valid cryptographic module user that a tamper attempt has occurred, whether it has been successful or not, while the latter protects the cryptographic module from such tamper attempts. In addition, there may be cases where a failure in a module may cause it to be zeroized or disabled (e.g., a blown power supply). There may be cases where keys are zeroized, and without tamper evidence features, there would be no indication that tampering had occurred. The user is left to guess whether zeroization occurred because of tampering or some "natural" failure of the module. Awareness of such tampering would necessitate a more drastic course of action rather than just a simple maintenance procedure, which might be the response if the module simply indicates that keys were zeroized.

The standard and DTR are clear in the area of physical security, in that to meet a particular level, all requirements from lower levels must also be met for a particular type of implementation (e.g., single chip, multi-chip embedded, and multi-chip standalone).

Additional Comments

5.5 Physical security requirements (Level 2) for multi-chip standalone cryptographic modules

Applicable Levels:	**2** (for all three physical embodiments)
Effective Dates:	**4/28/2000-** (supersedes previous IG 5.5, now listed as E.2)
Last Modified:	
Relevant Assertions:	AS05.03, AS05.09, AS05.19
Relevant Test Requirements:	TE05.03.01, TE05.09.01, TE05.19.01
Relevant Vendor Requirements:	VE05.03.01, VE05.09.01, VE05.19.01

Question/Problem

What are the Level 2 security requirements pertaining to enclosures designed to be non-removable, but which may be removed by force?

Resolution

1. The fact that a cryptographic module's enclosure is designed to be non-removable does not imply that it is, in fact, non-removable. When testing a cryptographic module for Level 2 compliance that is housed in an enclosure, the tester shall attempt to remove the cryptographic module's enclosure, even in cases where the manufacturer claims that the enclosure is non-removable. The tester shall apply a level of effort necessary to remove the cover or enclosure.

2. When a tester opens and closes the enclosure, attempting not to leave evidence of tampering, the time taken to accomplish this shall NOT include the time (or estimated time) needed to tamper with the cryptographic module's internal electronic components. This time shall include the time required to remove any additional physical barriers (e.g., epoxy over the components or internal shields) such that the internal electronic components of the cryptographic module can be accessed, and the "drying time" necessary for any sealant that is used to close and reseal the enclosure.

3. The tester shall only use tools and materials that are readily available in places such as a hardware store or hobby shop. The use of extremely expensive tools (e.g., a laser) are excessive for Level 2 physical security testing.

4. In opening and closing the enclosure, a tester shall use only cryptographic module components that are part of the cryptographic module being tested. For example, a tester shall not use another enclosure, label, or seal in place of the original.

5. The tester shall have some experience attempting to open and close the cryptographic module; however, the tester is not assumed to be an expert at penetrating the cryptographic module being tested. Rather, the assumption is that the tester has experience with LESS THAN 10 instances of the cryptographic module being tested.

Additional Comments

1. The underlying assumption is that the attacker does not have unlimited time and resources to mount the attack. For example, if a tester needs less than 2 hours to open the enclosure, gain access to the internal electronic components, and close the enclosure on a cryptographic module WITHOUT leaving evidence of tampering, then the tamper evidence requirements are NOT met.

2. "Detectable signs" and "tamper evidence" shall include both inoperability and visual evidence on the cryptographic module itself. Inoperability may include situations where an attempt to operate the cryptographic module requires a significantly greater physical effort than normal (e.g., a PC Card or smart card that cannot be easily placed (or fits too loosely) in its slot or reader/writer.).

3. Smartcards are considered to have a partial enclosure where half or all of the chip is covered by the plastic card housing. In this case, the ability to remove and replace the chip without visible tamper evidence on the plastic card housing and/or the exposed chip surface results in a failure of the tamper evidence requirements. Unique situations where the plastic card housing is clear or the chip is mounted in such a way as to allow both surfaces of the chip to be viewed by the user may meet the tamper evidence requirements by use of tamper evident coatings on the chip. The underlying requirement is for the user to be able to easily observe signs of tampering.

5.6 Key loader physical security requirements at Level 3

Applicable Levels:	**3**
Effective Dates:	**2/25/97-**
Last Modified:	
Relevant Assertions:	AS05.10, AS05.20
Relevant Test Requirements:	TE05.10.04, TE05.20.04
Relevant Vendor Requirements:	VE05.10.01, VE05.20.01

Question/Problem

Do the physical requirements at Level 3 pertain to a key loader if it is included as part of the cryptographic module?

Resolution

If a key loader *is* defined within the cryptographic boundary, and the key loader contains plaintext cryptographic keys or other unprotected security parameters, then these must be zeroized under the conditions stated in TE05.20.04. If the key loader is *not* defined within the cryptographic boundary, then the key loader is beyond the scope of FIPS PUB 140-1; however, the key entry requirements place restrictions on how the key loader can present keys to and receive keys from the cryptographic module.

VE05.20.01 states that "the circuitry shall be operational whenever plaintext cryptographic key, or other unprotected critical security parameters, are contained within the module."; this is done even when the module is not powered up (e.g., circuitry operated using battery power).

Additional Comments

In typical cases, a key loader shall not be included within the defined cryptoboundary.

5.7 Tamper response/zeroization circuitry on removable covers and doors for embedded and standalone modules

Applicable Levels:	**3, 4**
Effective Dates:	**3/21/97-**
Last Modified:	11/21/97
Relevant Assertions:	AS05.10, AS05.20
Relevant Test Requirements:	TE05.10.04, TE05.20.04
Relevant Vendor Requirements:	VE05.10.01, VE05.20.01

Question/Problem

Assume an embedded or standalone module implements level 3 physical security by applying a tamper response and zeroization mechanism to a removable cover or door. How shall the tester remove the cover/door? What are some conditions under which the applicable test would have "failed" as a result?

Resolution

The tester shall remove the cover/door, where "remove" may consist of opening, prying, or disassembling (e.g., if screws are holding the cover in place, then the screws may be loosened or removed), using a sharp

object (e.g., screwdriver, x-acto knife, or other basic instrument). "Remove" shall NOT consist of drilling, milling, burning, melting, grinding or dissolving the cover/door/enclosure, in order to gain access to the circuitry or tamper response mechanism. These types of "attacks" are addressed by Level 4 physical security, where a tamper detection envelope is implemented. In order for the module to pass either TE05.10.04 or TE05.20.04, then the tester shall not be able to disable the tamper response mechanism before it zeroizes plaintext critical security parameters.

(11/21/97)
The tester must determine if Level 3 physical security requirements are met. If fasteners (e.g., rivets, press-fittings, etc.) are used to hold a cover/enclosure in place, and the fasteners are visible to the tester (clearly delineating a mechanism for removal), then it is acceptable for a tester to drill out these fasteners, in order to test the removal of the cover/enclosure for tamper response. Note that drilling can ***only*** be performed on the fasteners, and not on the enclosure itself.

In situations where a tester can disable the tamper response mechanism by "removing" the cover/door (as described above) and inserting a physical probe, then the applicable test is failed. If one can use a probe in this manner before zeroization takes place, then it is very likely that a probe could also be used to obtain plaintext critical security parameters. Assertions AS05.11 and AS05.21 address modules that have ventilation slits, and require that these slits be protected to prevent undetected probing. Likewise, the creation of any type of slit or hole during cover/door partial "removal" should also have a similar type of protection to prevent undetected probing (i.e., this protection is the tamper response mechanism).

(11/21/97)
Note that any existing opening revealed by the removal of a fastener may be probed by a tester.

Additional Comments

Note that TE05.10.04 and TE05.20.04 also describe how additional testing is to be done.

5.8 Testing of tamper-detection envelope for level 4 physical security (embedded/standalone)

Applicable Levels:	**4**
Effective Dates:	**12/7/98-**
Last Modified:	
Relevant Assertions:	AS05.12, AS05.22
Relevant Test Requirements:	TE05.12.01, TE05.22.01
Relevant Vendor Requirements:	VE05.12.01, VE05.22.01

Question/Problem

For multiple-chip embedded/standalone cryptographic modules at level 4 physical security, how does the testing laboratory determine the adequacy of the module's tamper-detection envelope (i.e., What constitutes a breach in the barrier/enclosure of the module's tamper-detection envelope?).

Resolution

The tamper-detection envelope of a level 4 (physical security) multiple-chip embedded/standalone module is considered breached and fails **TE05.12.01 / TE05.22.01** if the testing laboratory, using readily available/obtainable technology, is able to penetrate the module's barrier/enclosure and gain undetected physical access to critical security parameters.

Additional Comments

1. The Derived Test Requirements lists drilling, milling, grinding, or dissolving as examples of barrier/enclosure penetration. In addition, Implementation Guidance 5.7 states that "...drilling, milling, burning, melting, grinding, or dissolving the cover/door/enclosure, in order to gain access to the circuitry or tamper response mechanism. . .are addressed by Level 4 physical security, where a tamper-detection envelope is implemented."

2. When testing multiple-chip embedded/standalone cryptographic modules for level 4 physical security, the testing laboratory can assume that the attacker is highly motivated but does not have the technical resources of a major university or a government agency. In addition, the discussion of insider versus outsider attack is not relevant, since the tamper-detection envelope is active against all penetration (as described above).

3. Level 4 physical security does not protect the device itself against reverse engineering attacks, where the attacker is interested in the technology and not the critical security parameters. This type of attack is outside the scope of FIPS 140-1.

4. The phrase "readily available/obtainable" refers to technology in existence at the time the module is in the validation process. The following examples are provided for clarification and are current as of the guidance date:

X-ray Machine:	readily available/obtainable
Electron Tunneling Microscope:	NOT readily available/obtainable

5. In order to pass level 4 physical security, the module must first meet level 1-3 physical security requirements, as stated in the standard.

Section 6 - Software Security

There are currently no implementation guidance for this section.

Section 7 - Operating System Security

7.1 Authentication of cryptographic software within a cryptographic module

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	
Relevant Assertions:	AS07.02, AS11.14
Relevant Test Requirements:	TE07.02.01-.02, TE11.14.03-.04
Relevant Vendor Requirements:	VE07.02.01, VE11.14.01

Question/Problem

In cases where the cryptographic module is implemented as software running on a general-purpose computer, must a cryptographic authentication mechanism be applied to software on the computer other than the cryptographic software being validated?

Resolution

No. The requirements under assertion AS07.02 only apply to the cryptographic module software which is being developed and/or modified by the vendor. For example, operating system software such as DOS or Windows need not be authenticated.

Additional Comments

7.2 Level 2 O/S Requirements - Use of TCSEC, ITSEC, and CTCPEC Evaluations

Applicable Levels:	**2**
Effective Dates:	**7/30/97-**
Last Modified:	
Relevant Assertions:	AS07.05
Relevant Test Requirements:	TE07.05.01-.02
Relevant Vendor Requirements:	VE07.05.01

Question/Problem

For Level 2 operating system requirements, what C2 level operating systems can be used - just those with a TCSEC C2 rating, or do other evaluated O/S's qualify?

Resolution

For the purposes of meeting FIPS 140-1 Level 2 O/S requirements (i.e., C2 or equivalent), a cryptographic module may use an operating system which has been successfully evaluated against one or more of the following criteria:

CRITERIA	LEVEL
Trusted Computer Systems Evaluation Criteria (**TCSEC**)	**C2**
Canadian Trusted Computer Product Evaluation Criteria (**CTCPEC**)	**C2 Functionality Profile** (Functionality Level) **T1** (Assurance Criteria Level)
Information Technology Security Evaluation Criteria **(ITSEC)**	**F-C2** (Functionality Level) **E2** (Assurance Level)

An O/S can be considered as "evaluated" if it appears on the appropriate Evaluated Products List (EPL) from any one of the following countries: United States, Canada, United Kingdom, Germany, France, and The Netherlands. EPLs can be obtained as follows:

NATION	ORGANIZATION	CONTACT
United States (TCSEC)	National Security Agency INFOSEC Awareness Group Maryland, USA	TEL: (410) 766-8729
Canada (CTCPEC)	Communications Security Establishment ATTN: ITS Publications Administrator P.O. Box 9703, Terminal Ottawa, Canada K1G 3Z4	TEL: (613) 991-7409 FAX: (613) 991-7411 EMAIL: criteria@cse.dnd.ca
United Kingdom (ITSEC)	Certification Body Secretary UK IT Security and Certification Scheme P.O. Box 152 Cheltenham GL52 5UF, UK	TEL: +44 1242-238739 FAX: +44 1242-235233 EMAIL: cbsec@itsec.gov.uk UK ITSEC scheme
Germany (ITSEC)	Bundesamt fuer Sicherheit in der Informationstechnik Referat II2/II3 Postfach 20 03 63 D-53133 Bonn, Germany	TEL: +49 228-9582-111 FAX: +49 228-9582-455 EMAIL: zerti@bsi.de

France (ITSEC)	Service Central de la Securite des Systemes d'Information Centre de Certification de la Securite des TI 18 rue du docteur Zamenhof 92131 Issy les Moulineaux, France	TEL: +33 1-41463753 FAX: +33 1-41463701 EMAIL: 100565.1335@compuserve.com
The Netherlands (ITSEC)	Netherlands National Communications Security Agency P.O. Box 20061 2500 EB The Hague, The Netherlands	TEL: +31 70-3485637 FAX: +31 70-3486503 EMAIL: criteria@nlncsa.minbuza.nl

Additional Comments

7.3 Operating System Requirements

Applicable Levels:	**ALL**
Effective Dates:	**6/18/01-**
Last Modified:	
Relevant Assertions:	AS11.20
Relevant Test Requirements:	TE11.20.01
Relevant Vendor Requirements:	VE11.20.01-04

Introduction

As stated in FIPS 140-1, “The operating system requirements in this section shall apply to a cryptographic module only if the module provides a means whereby an operator can load and execute software or firmware that was not included as part of the validation of the module.”

Question/Problem

Untrusted software and/or firmware that may be loaded into a cryptographic module after FIPS 140-1 validation, requires the use of an evaluated operating system. If the software/firmware load test is applied when software/firmware is loaded after validation, is an evaluated operating system required?

Resolution

For a validated cryptographic module, the operating system requirements are not applicable (N/A) if ALL externally loaded software (and/or firmware) includes the software/firmware load test. In addition, the externally loaded software/firmware shall be validated by a FIPS 140-1 laboratory.

Additional Comments

Section 8 - Cryptographic Key Management

8.1 List of FIPS-approved key management methods

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	1/10/2002
Relevant Assertions:	AS08.04, AS08.08
Relevant Test Requirements:	TE08.04.01, TE08.08.01
Relevant Vendor Requirements:	VE08.04.01, VE08.08.01

Question/Problem

What methods for key management are currently FIPS-approved?

Resolution

FIPS 140-1 states that several aspects of key management must use FIPS-approved methods. Below is a list of currently acceptable FIPS-approved methods (as of the "Last Modified" date listed above):

- **Key generation:**
  - **Note:** *Whenever a module generates a key to be used with a FIPS-approved algorithm (e.g., for generating/verifying a signature, encrypting another key, encrypting data, etc.), then that key shall be generated using one of the methods listed below.*
  - Pseudorandom number generation:
    - American Bankers Association, *Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA),* **ANSI X9.31-1998** - Appendix A;
    - American Bankers Association, *Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA),* **ANSI X9.62-1998** - Annex A.4;
    - National Institute of Standards and Technology, *Digital Signature Standard (DSS),* **FIPS 186-2**, January 27, 2000 - Appendix 3.1;
    - National Institute of Standards and Technology, *Digital Signature Standard (DSS),* **FIPS 186-2**, January 27, 2000 - Appendix 3.2.
  - Random number generation: Currently, there is no FIPS-approved random number generator. *However,* **FIPS 186-2** *allows for such a random number generator to be used in generating values for x and k (provided that in the future there exists a FIPS for random number generation - 10/29/97).*

    (10/29/97)
    For key generation, **FIPS 186-2** *specifically states in Appendix 3 that "They (keys) shall be generated by the techniques given in this appendix, or using other FIPS approved security*

methods." This applies to the generation of any key used by a FIPS-approved algorithm, within a FIPS 140-1 cryptographic module. It is acceptable for the output of a random number generator to generate a seed value for one of the FIPS-approved pseudorandom number generators listed above, in order to generate keys.

- ***Key distribution:***
  - Secret key based:
    - **FIPS 171**, *Key Management Using ANSI X9.17*
  - Public key based: *Currently, there is no FIPS-approved public-key based key distribution technique. Until such time as one is available, commercially available public key methods may be used.*

Additional Comments

If there is a question concerning whether or not a particular public-key based key distribution method is acceptable or not, the vendor shall contact NIST either directly or through a CMT laboratory (if the vendor has a working relationship with such a lab) for a decision.

8.2 Using various public-key methods for key management/distribution

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	
Relevant Assertions:	AS08.08
Relevant Test Requirements:	TE08.08.01
Relevant Vendor Requirements:	VE08.08.01

Question/Problem

What public-key methods are acceptable to use in support of key management? Are there currently any FIPS-approved methods for this ?

Resolution

FIPS 140-1 states that "Until such time as a FIPS-approved public key-based key distribution technique is established, commercially available public key methods may be used." [FIPS 140-1, 4.8.2]. Currently, there are no FIPS-approved public-key methods for distributing keys.
There are implementations of such methods which use a combination of a public-key algorithm and a hashing algorithm. In this case, the hashing algorithm used shall be a FIPS-approved hashing algorithm (e.g., FIPS 180-1, Secure Hash Standard (SHS)); use of a non-FIPS approved hashing algorithm in this situation would NOT be acceptable.

Additional Comments

If there is a question concerning whether or not a particular public-key based key distribution method is acceptable or not, the vendor shall contact NIST either directly or through a CMT laboratory (if the vendor has a working relationship with such a lab) for a decision.

8.3 Use of key loaders and its implications

Applicable Levels:	**3, 4**
Effective Dates:	**2/25/97-**
Last Modified:	
Relevant Assertions:	AS08.15, AS08.16
Relevant Test Requirements:	TE08.15.01-.03, TE08.16.01-.03
Relevant Vendor Requirements:	VE08.15.01, VE08.16.01-.02

Question/Problem

Can a key loader be part of the cryptographic module, and if so, what are the requirements at Level 3?

Resolution

If a key loader is *not* included as part of the cryptographic module, then the secret or private keys must pass from the key loader to the cryptographic module in one of the two ways listed in AS08.15 (encrypted or using split knowledge procedures). If the key loader *is* included as part of the module, then the secret or private keys must pass *into the key loader* in one of the two ways listed in AS08.15. Note that at Level 3 there are additional restrictions placed on key entry and user identification (refer to AS08.16). Also, defining the key loader to be within the cryptoboundary has implications on physical security requirements, among other areas (see the guidance on "Key loader physical security requirements at Level 3").

The requirements for key entry at Levels 3 and 4 (requiring entry of encrypted keys or using split knowledge procedures) were specified to allow for environments where dual control of keys is desired. The implication is carried in the requirements that the cryptographic module must have the capability to support a key entry function that requires more than one user to have control during the key entry process.

Additional Comments

8.4 Use and testing of FIPS 171 key distribution techniques

Applicable Levels:	**ALL**
Effective Dates:	**6/1/97-**
Last Modified:	
Relevant Assertions:	AS08.08
Relevant Test Requirements:	TE08.08.01
Relevant Vendor Requirements:	VE08.08.01

Question/Problem

If a cryptographic module implements FIPS 171 key management, and it is not a validated implementation of FIPS171 (i.e., there is no validation certificate that can be presented to the lab), what is tested and what information must be provided by the vendor?

Resolution

Since NIST's validation test suite for FIPS 171 is no longer operational, some other method is needed to determine if FIPS 171 requirements have been met. (A full-blown validation of ANSI X9.17 and FIPS 171 are not expected.) Thus, the following process will be used during FIPS 140-1 testing, within the scope of Vendor Required Information and Testing Requirements for AS08.08:

1. The vendor provides the lab with written affirmation of compliance to FIPS 171. This affirmation shall include supporting statements which show how all 27 elements of FIPS 171 are addressed (particularly those X9.17 options which are specified as mandatory in FIPS 171), and shall identify exactly where these elements are addressed in the cryptographic module's source code. Some of the

optional elements may in fact not be implemented - in that case, the vendor should indicate that these options are not implemented.

2. Based on the vendor's written affirmation, the lab shall verify that the FIPS 171 elements affirmed to be implemented in the cryptographic module actually correspond with elements listed in FIPS 171. In addition, the lab shall verify that the mandatory elements in FIPS 171 are addressed in the written affirmation. (e.g., Vendor affirmation states that "Key notarization is implemented as required in element #10 of FIPS 171, and it occurs within the 'notarize_key()' function in the 'key_mgmt.c' file. This function is called from the following places within the source code: . . ."; the lab also verifies that key notarization is required by FIPS 171.)

3. The lab then compares the cryptographic module code with the appropriate FIPS 171 element, referencing the appropriate specification in ANSI X9.17 as necessary. (e.g., The lab compares the key notarization implementation with steps listed in section 7.5 of ANSI X9.17 to verify that notarization is being done correctly.) This is intended to verify the correct implementation of the particular FIPS 171 requirement, and NOT the verification of all elements of ANSI X9.17. Verification by the lab is especially important for the 16 elements in FIPS 171 which are identified as "mandatory" or "forbidden".

Additional Comments

8.5 Initialization Vector (IV) requirements

Applicable Levels:	**ALL**
Effective Dates:	**10/29/97-**
Last Modified:	9/28/98
Relevant Assertions:	AS08.05, AS09.01, AS11.16, AS11.22
Relevant Test Requirements:	TE08.05.01, TE11.16.01-03, TE11.22.01
Relevant Vendor Requirements:	VE08.05.01, VE11.16.01, VE11.22.01

Question/Problem

Are there any particular requirements regarding the generation of initialization vectors?

Resolution

Requirements for the size and generation of DES initialization vectors are derived from FIPS 74 and FIPS 81:

IV Size: The required IV length for the various modes of DES, based on FIPS 74 and 81, is as follows:

CBC	64 bits
CFB	48-64 bits
OFB	64 bits

IV Generation: There are several cases involving IV generation - one when the IV is generated externally, and then loaded into the module for use, and another when the IV is generated internally:

1. IVs generated ***outside*** a 140-1 cryptographic module:

   The randomness of externally generated IVs does not have to be checked by the module using that IV; however, the IV must be of the required minimum length for the appropriate DES mode (as indicated above).

In addition, if the IV is to be used with DES in the OFB mode, then it is **not** acceptable for the IV to remain fixed for multiple encryptions, if the same key is used for those encryptions.

2. IVs generated ***inside*** a 140-1 cryptographic module:

   - IVs generated within a module **shall** be pseudorandomly or randomly generated.

   - IVs **may** be generated with a FIPS-approved pseudorandom number generator (PRNG) or random number generator (RNG) (see Guidance 8.1). *(9/28/98 - clarified) Until such time as a FIPS-approved RNG is available, a non-FIPS approved RNG may be used for IV generation. Note that this is not true for key generation (see Guidance 8.1).* In addition, **FIPS 74** states that "The DES may be used as a pseudorandom number generator to generate the IV."

   (9/28/98 - clarified) In the case where a module generates IVs with *an RNG* method that is non-FIPS approved, then the lab **shall** 1) inform NIST/CSE of this fact, and 2) be able to demonstrate that the IV generator is capable of generating random data. This shall be accomplished by running one or more of the statistical random number generator tests from section 4.11.1 of FIPS 140-1, as required under TE08.05.01.

   Any RNG or PRNG that is used to generate IVs **shall** fulfill all relevant requirements in FIPS 140-1, including the Continuous RNG self-test (AS11.22). There may be other applicable tests. For example, if level 3 or 4 is desired, then a statistical RNG/PRNG self-test must be implemented internally by the module (AS11.16).

Additional Comments

8.6 Over-The-Air-Rekeying (OTAR) in radio communications cryptographic modules

Applicable Levels:	**ALL**
Effective Dates:	**6/4/1999-**
Last Modified:	
Relevant Assertions:	AS08.08
Relevant Test Requirements:	TE08.08.01
Relevant Vendor Requirements:	VE08.08.01

Question/Problem

May radio communications cryptographic modules use over-the-air rekeying, using a non-FIPS 171, secret-key based key distribution technique?

Resolution

In the absence of a FIPS-approved key distribution technique for Over-The-Air-Rekeying (OTAR), it is acceptable for radio communications cryptographic modules to implement OTAR as specified in the following standard:

- TIA/EIA Telecommunications Systems Bulletin, **APCO Project 25, *Over-The-Air-Rekeying (OTAR) Protocol***, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACA, January 1996, Telecommunications Industry Association.

An additional description of this protocol is located in:

- TIA/EIA Telecommunications Systems Bulletin, ***Over-The-Air-Rekeying (OTAR) Operational Description***, New Technology Standards Project, Digital Radio Technical Standards, TSB102.AACB, January 1997, Telecommunications Industry Association.

The following process shall be used during FIPS 140-1 testing, within the scope of Vendor Required Information and Testing Requirements for AS08.08:

1. The vendor provides the lab with written affirmation of compliance to the APCO Project 25 OTAR Protocol, in TSB102.AACA. This affirmation shall include supporting statements which show how all mandatory Key Management (KM) Procedures (identified in section 7.1.1 of TSB102.AACA) are met.

   In the cryptographic module's source code, the vendor shall identify exactly where these elements - and any other implemented optional KM procedures - are addressed. If particular optional KM procedures from section 7.1.2 are *not* implemented, the vendor shall indicate that these options are not implemented.

2. The lab shall verify that all of the APCO 25 mandatory KM Procedures are addressed in the vendor's written affirmation, and that the vendor indicates that all such procedures are all implemented within the cryptographic module.

3. The lab then compares the cryptographic module source code with the appropriate APCO 25 mandatory KM procedure, referring to the TSB102.AACA standard as necessary. (e.g., The lab compares the cryptographic module's key deletion implementation with 1) the Delete-Key Procedure listed in section A.5 of TSB102.AACA, and 2) the message formats for Delete-Key-Command, Delete-Key-Response, and Delayed Acknowledgment messages (in sections B.1.8, B.1.9, and B.1.7, respectively), to verify that key deletion is being done correctly.)

Additional Comments

The procedures listed above are necessary, due to the absence of a formal testing program for APCO Project 25 OTAR.

This guidance does *not* apply to non-radio communications cryptographic modules.

8.7 X9.17/X9.31 Pseudorandom Key and IV Generation

Applicable Levels:	**ALL**
Effective Dates:	**6/18/01-**
Last Modified:	
Relevant Assertions:	AS08.04, AS08.05
Relevant Test Requirements:	TE08.04.01, TE08.05.01
Relevant Vendor Requirements:	VE08.04.01, VE08.05.01

Introduction

If a cryptographic module implements a deterministic RNG, the RNG must be compliant with ANSI X9.17 Appendix C/ANSI X9.31 Appendix A[1] or FIPS 186-2. ANSI X9.31 specifies a seed, seed key and Date/Time vector. The method required to generate the initial seed and seed key values and provisions for the Date/Time vector are not specified.

[1] Because ANSI has withdrawn X9.17, the appropriate reference is to ANSI X9.31.

Question/Problem

ANSI X9.31, Appendix A references a DEA key pair (*K) and a 64-bit seed value (V) that are used in the generation of pseudorandom keys and IVs. A question has been raised about the source of these two parameters for the FIRST execution of the ANSI X9.31 deterministic generator. Specifically, may a nondeterministic random number generator (RNG) or any other non-Approved RNG be used to generate the initial seed key and seed values? This is important because there is no FIPS approved nondeterministic RNG. Also, what is considered a Date/Time vector parameter?

Resolution

The DTR does not specifically address the generation of the initial seed and seed key values. Therefore, in the FIPS mode of operation, a crypto module may implement a non-Approved RNG (deterministic or nondeterministic) that generates the initial seed and seed key values that are input to the ANSI X9.31 deterministic RNG. The seed and seed key may also be re-generated from the non-Approved RNG on each iteration of the ANSI X9.31 RNG. ANSI X9.31 defines that the Date/Time vector must be updated on each iteration. In lieu of a Date/Time vector, an incrementer may be used.

Additional Comments

8.8 Key Wrapping

Applicable Levels:	**ALL**
Effective Dates:	**6/18/01-**
Last Modified:	
Relevant Assertions:	AS08.10
Relevant Test Requirements:	TE08.10.01
Relevant Vendor Requirements:	VE08.10.01-03

Introduction

FIPS 140-1 requires that electronically distributed secret and private keys be entered and output in encrypted form. FIPS 140-1 also requires that encryption be performed using an Approved algorithm. This requirement is mandatory when the cryptographic module is operating in FIPS mode.

The process of encrypting keys is called key wrapping. Key wrapping is used to protect the confidentiality and integrity of the key for distribution outside the cryptographic module. The term “key wrapping” is used to distinguish between the encryption of keys and the encryption of data.

Question/Problem

May a cryptographic module implement a public key based algorithm to encrypt keys that are electronically distributed? Currently, there are no Approved public key based key distribution (key establishment in FIPS 140-2) algorithms.

Resolution

As stated in FIPS 140-1, “Until such time as a FIPS approved public key-based key distribution technique is established, commercially available public key methods may be used.” Therefore, a non-Approved public key based key distribution (key establishment in FIPS 140-2) algorithm may be used to encrypt keys for electronic distribution. In the validation report, public key-based keys that are used to encrypt keys shall be specified as key wrapping keys.

Additional Comments

8.9 FIPS 186-2, Appendix 3 Random Number Generation for the DSA

Applicable Levels:	**ALL**
Effective Dates:	**6/18/01-**
Last Modified:	
Relevant Assertions:	AS08.05
Relevant Test Requirements:	TE08.05.01
Relevant Vendor Requirements:	VE08.05.01

Introduction

Recently, Dr. Daniel Bleichenbacher of Bell Laboratories discovered an attack on the Digital Signature Algorithm (DSA) as specified in FIPS 186-2, *Digital Signature Standard* and ANSI X9.30 (Part 1), *Public Key Cryptography for the Financial Services Industry: Digital Signature Algorithm (DSA) (Revised).* The attack relies on the non-uniformity of the pseudorandom number generator (PRNG) and (in the best case for the attacker) requires 2^{64} time, 2^{41} memory, and 2^{22} known signatures. The non-uniformity also exists in the PRNG specified in ANSI X9.31-1998, *Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA).*

Question/Problem

When using the random number generator specified in FIPS 186-2, Appendix 3, is it acceptable to remove the "mod q" function from the formula?

Resolution

When using the RNG specified in Appendix 3 for *general purpose* random number generation (not for the DSA key generation and signature functions), it is acceptable to remove the "mod q" function from the formula. The "mod q" function must be used during the key generation and digital signature functions. This is a short-term solution. Currently, NIST and ANSI are reviewing the proposed alternatives to addressing this issue.

Additional Comments

Section 9 - Cryptographic Algorithms

NOTE: All cryptographic algorithms (both FIPS-approved and non-FIPS approved) implemented in the cryptographic module shall be listed in the validation report. This information will then be included in the validation certificate.

9.1 FIPS-approved algorithms

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	4/28/00
Relevant Assertions:	AS09.01
Relevant Test Requirements:	TE09.01.01
Relevant Vendor Requirements:	VE09.01.01

Question/Problem

What is the current set of FIPS-approved cryptographic algorithms ?

Resolution

Below is the current list of FIPS-approved cryptographic algorithms:

- **Encryption (Secret-key based):**
  - *Triple Data Encryption Algorithm ("**Triple DES**")*, in FIPS 46-3, *Data Encryption Standard (DES)*, using the various modes specified in ANSI X9.52-1998, *Triple Data Encryption Algorithm Modes of Operation*. **FIPS 46-3 states that Triple DES is "the FIPS-approved symmetric encryption algorithm of choice".** *(11/8/1999)*
  - *Data Encryption Algorithm ("**DES**")*, in FIPS 46-3, *Data Encryption Standard (DES)*, using the various modes specified in FIPS 81, *DES Modes of Operation*.
  - ***Skipjack** Algorithm*, referred to in FIPS 185, *Escrowed Encryption Standard (EES)* and specified in the R21 Technical Report entitled "SKIPJACK" (S) (R21-TECH-044-91), using the modes specified in FIPS 81. The SKIPJACK algorithm was made public in June 1998.
- **Electronic signatures (Secret-key based):**
  - *Data Authentication Algorithm* (a.k.a., Message Authentication Code (**MAC**)), in FIPS 113, *Computer Data Authentication*.
- **Digital signatures (Public-key based):**
  - *Digital Signature Algorithm (**DSA**)*, specified in FIPS 186-2, *Digital Signature Standard (DSS)*.
  - ***RSA*** signature algorithm, referenced in FIPS 186-2, *Digital Signature Standard (DSS)*, and specified in ANSI X9.31. *(12/22/98)*
  - *Elliptic Curve DSA (**ECDSA**)* signature algorithm, referenced in FIPS 186-2, *Digital Signature Standard (DSS)*, and specified in ANSI X9.62. *(4/28/2000)*

- ***Hash (message digest) generation:***
    - *Secure Hash Algorithm (**SHA-1**)*, in FIPS 180-1 (SHS).

Additional Comments

NOTE: See the guidance under section 8 in this document which lists the current FIPS-approved methods for:

- ***Key generation**, and*
- ***Key distribution.***

9.2 Cryptographic module with no FIPS-approved algorithms cannot be validated

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	
Relevant Assertions:	AS09.01
Relevant Test Requirements:	TE09.01.01
Relevant Vendor Requirements:	VE09.01.01

Question/Problem

Can a cryptographic module be validated even though it does not contain a FIPS approved cryptographic algorithm?

Resolution

No, a FIPS 140-1 cryptographic module must implement *at least one* FIPS-approved cryptographic algorithm in order to be a candidate for validation by NIST and CSE.

Additional Comments

9.3 SHA-1 granularity

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	
Relevant Assertions:	AS09.01
Relevant Test Requirements:	TE09.01.01
Relevant Vendor Requirements:	VE09.01.01

Question/Problem

Can an implementation of SHA-1 perform hashing only on byte-oriented data, or is it required to hash messages of any bit length?

Resolution

FIPS 180-1, the *Secure Hash Standard*, allows for the hashing of messages that are of any bit length ($< 2^{64}$ bits), and does not require that messages be of a byte length (equal to a multiple of 8 bits). However, some cryptographic modules, or interfaces to the cryptographic modules, are designed to hash data only on a byte-oriented basis. As long as this hashing is performed correctly (i.e., in accordance with specs in FIPS 180-1), then this is acceptable.

If an SHA-1 implementation successfully passes SHA-1 validation tests for byte-oriented messages only, then the SHS Validation Certificate shall indicate that the implementation has been validated only for the hashing of byte-ordered data.

Additional Comments

9.4 Expired 11/8/1999 - see E.1 Triple DES implementation within a 140-1 cryptographic module

9.5 PKCS #1 RSA Implementation

Applicable Levels:	**ALL**
Effective Dates:	**6/18/01-**
Last Modified:	
Relevant Assertions:	AS09.01
Relevant Test Requirements:	TE09.01.01
Relevant Vendor Requirements:	VE09.01.01

Introduction

FIPS 186-2, *Digital Signature Standard* was revised to include RSA implementations that are compliant with ANSI X9.31. The ANSI specification is different from the PKCS #1 document that also specifies RSA implementations.

Question/Problem

Will PKCS #1 compliant RSA implementations be allowed in FIPS mode?

Resolution

FIPS 186-2 references the ANSI X9.31 RSA specification. The acceptance of PKCS #1 RSA implementations is included in the Federal Register Notice that announced FIPS 186-2. Therefore, RSA implementations that are compliant with PKCS #1 (by vendor affirmation) are considered FIPS-approved and shall be listed as FIPS-approved cryptographic algorithms on the certificate.

Additional Comments

The following Federal Register Notice was published on 02/15/2000. The notice announces the approval of FIPS 186-2. This notice includes the reference to PKCS #1 implementations of RSA. (Note: this reference is NOT included in FIPS 186-2.) The applicable language is underlined.

DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
[Docket No._____]

Announcing Approval of Federal Information Processing Standard (FIPS) 186-2,

Digital Signature Standard

AGENCY: National Institute of Standards and Technology (NIST), Commerce.

ACTION: Notice.

SUMMARY: The Secretary of Commerce approved Federal Information Processing Standard 186-2, Digital Signature Standard (DSS), which supersedes Federal Information Processing Standard (FIPS) 186-1, Digital Signature Standard (DSS). FIPS 186-2 expands the Digital Signature Standard by specifying two voluntary industry standards for generating and verifying digital signatures. This action will enable Federal agencies to use the Digital Signature Algorithm (DSA), which was originally the single approved technique for digital signatures, as well as two American National Standards that were developed by the financial community. These latter standards are ANSI X9.31, Digital Signatures Using Reversible Public Key Cryptography, and ANSI X9.62, Elliptic Curve Digital Signature Algorithm (ECDSA).

SUPPLEMENTARY INFORMATION: Under Section 5131 of the Information Technology Management Reform Act of 1996 and the Computer Security Act of 1987, the Secretary of Commerce is authorized to approve standards and guidelines for the cost effective security and privacy of sensitive information processed by federal computer systems.

……

Therefore NIST recommended that the Secretary of Commerce approve FIPS 186-2 to include the Digital Signature Algorithm, the RSA technique (ANSI X9.31) and the elliptic curve digital signature technique, which has now been approved as a voluntary industry standard (ANSI X9.62, Elliptic Curve Digital Signature Algorithm). Other comments supported the continued use of another RSA signature algorithm that is specified by PKCS#1. FIPS 186-2 allows for the continued acquisition of implementations of PKCS#1 for a transition period of eighteen months. This transition period will enable federal agencies to plan for the acquisition of implementations of the algorithms promulgated by FIPS 186-2.

Section 10 - Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

10.1 FCC Testing and Certification Requirements

Applicable Levels:	**ALL**
Effective Dates:	**2/21/97-**
Last Modified:	
Relevant Assertions:	AS10.01-.03
Relevant Test Requirements:	TE10.01.01, TE10.02.01, TE10.03.01
Relevant Vendor Requirements:	VE10.01.01, VE10.02.01, VE10.03.01

Question/Problem

Is it true that the FCC allows self-certification of a device to FCC Part 15, Subpart J, Class A (for business use)? If so, is self-certification acceptable for meeting the requirements of section 10?

Resolution

Below is a list of the procedures required for various devices to be deemed as conforming to FCC requirements in 47 CFR Part 15 for

a. radio receivers, and

b. personal computers and peripherals designated for

   i. business use (Class A), and

   ii. home use (Class B)

This information was accurate at the time that this guidance was issued, and may change in the future as a result of FCC requirements changes.

[Part 15 applies to non-intentional emitters and low power transmitters. Low power transmitters (eg., garage door openers,

(Subpart J does not apply to non-intentional radiators - this was changed in 1992. Non-intentional emitter requirements now reside in Subpart B of FCC Part 15.)

High power radio transmitters, and transmitters providing certain classes of service (eg., land mobile, business use, etc.) must be "Type Accepted" according to the appropriate Rule Part, which is based on the designated band and service that the transmitter is to be used.]

**Note that these are procedures that the vendor should have already taken with an FCC-approved lab - these are not new requirements for CMT labs. In each of the cases below, information is listed which a CMT lab shall require from a vendor. The information provided to the CMT lab shall be reflected in the 140-1 validation report.*

I. **Radios (both transmitters and receivers)**

- *FCC Procedures:*

1. A "listed" lab tests a device for conformance to FCC requirements. ("Listed" means that the FCC has determined that a lab meets certain FCC criteria based on a filing of site description and site performance data--it does not imply accreditation by the FCC.)

2. The lab issues a test report, and either the lab or vendor submits that report to the FCC, along with a formal Application for "Certification", "Notification" or "Type Acceptance", as required by the type of device. The applicant submits a proposed FCC ID Number which is composed of the combination of an FCC Grantee Code prefix (a 3 alpha-character code assigned by the FCC) and a number of discretionary suffix digits that are the choice of the applicant.

3. If all is in order, the FCC Grants an Equipment Authorization; the vendor can then legally sell the equipment. The FCC ID number must be applied to the equipment with appropriate warning statements on the label and in the user's manual.

- ****CMT Lab Procedures (applicable to* AS10.01*):*
  - The CMT lab shall request the FCC ID number from the cryptographic module vendor.

II. **Personal Computers and Peripheral Equipment: non-intentional emitters (Class A - business use)**

- *FCC Procedures:*

0. A facility with equipment and a site that satisfies the FCC's requirements tests a device for conformance to FCC requirements.

1. The lab issues a test report to the vendor.

2. The vendor then puts a sticker bearing the proper warning statement on its equipment. However, this sticker does NOT bear an FCC ID number, since no such number is issued.

- ****CMT Lab Procedures (applicable to* AS10.02*):*
  - The CMT lab shall request the following information from the cryptographic module vendor:

1. the name of FCC testing laboratory,

2. the ID# of lab's test report, and

3. the test report date.

III. **PCs and Peripherals (Class B - home use)**

There are two types of procedures approved by the FCC which may be used by a vendor with a Class B product:

- *FCC Procedure #1:*
  - Procedure 1 is basically identical to the procedure used for radio equipment described in section I above.

- ****CMT Lab Procedures (applicable to* AS10.03*):*

- The CMT lab shall request the FCC ID Number from the cryptographic module vendor.

- *FCC Procedure #2:*

  - Procedure 2 (a.k.a. "Declaration of Conformity", adopted by the FCC on May 9, 1996, and announced in the FCC's Report and Order, "FCC-96-208"):

    1. An accredited lab (accredited by either NVLAP or A2LA to do FCC testing for Part 15) tests a device for conformance to FCC requirements, and issues a test report to the vendor.

    2. The vendor then makes a "Declaration of Conformity" (DoC). This document is kept on file by the vendor - it is not filed with the FCC, but it is a releasable document.

    3. The vendor places a label on the equipment with the FCC logo and appropriate warning statement.

- ****CMT Lab Procedures (applicable to* AS10.03*):*

  - The CMT lab shall request a copy of the DoC from the vendor, and identify this in the 140-1 validation report.

Additional Comments

- In order to obtain the proper information from the cryptographic module vendor, it is suggested that the CMT lab ask the vendor to "provide the status of FCC approval, and whether it is Class A or Class B (if it's a PC or peripheral)"

- The list of NVLAP-accredited FCC testing laboratories can be found at : http://ts.nist.gov/ts/htdocs/210/214/scopes/ect.htm

Note that the FCC also uses laboratories accredited by other bodies, including the American Association for Laboratory Accreditation (A2LA). The A2LA maintains a home page (http://www.a2la.org/), which contains a list of their accredited laboratories.

10.2 Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Applicable Levels:	**ALL**
Effective Dates:	**6/18/01-**
Last Modified:	
Relevant Assertions:	AS10.02-03
Relevant Test Requirements:	TE10.02.01, TE10.03.01
Relevant Vendor Requirements:	VE10.02.01, VE10.03.01

Introduction

During a cryptographic module revalidation, minor changes may be made to the hardware, software and/or firmware. IG G.8 specifies the criteria for a revalidation. Many of these changes may seem negligible in regard to EMI/EMC emissions and any need for recertification.

Question/Problem

Does the vendor need to provide a new FCC certificate as a result of hardware, software or firmware changes during a revalidation? How much of a change would require a new certificate? Can the vendor claim that the hardware change was insignificant?

Resolution

The DTR requires the laboratory to receive from the vendor an FCC certificate representing the new revalidated module. This would apply to any *hardware* change (firmware and software changes excluded). It is not the purview of the CMT laboratory or the vendor to claim any cryptographic module hardware changes are not relevant in regard to the EMI/EMC requirement. A letter from the FCC laboratory to the vendor and supplied to the CMT laboratory can be sufficient to state that the FCC laboratory has reviewed the change and that the change does not require additional testing.

Additional Comments

Section 11 - Self-Tests

11.1 Performing power-up and conditional self-tests

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	
Relevant Assertions:	AS11.09
Relevant Test Requirements:	TE11.09.01-.02
Relevant Vendor Requirements:	VE11.09.01

Question/Problem

Is resetting or rebooting an acceptable method of initiating power-up self-tests on demand? Is this also an acceptable method for initiating conditional self-tests?

Resolution

Yes, resetting and rebooting a cryptographic module are acceptable means for initiating BOTH power-up self-tests on demand as well as conditional self-tests.

Additional Comments

11.2 Known answer test for DSA

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	4/28/00
Relevant Assertions:	AS11.10, AS11.11, AS11.19
Relevant Test Requirements:	TE11.10.01, TE11.11.01, TE11.19.01, TE11.19.(
Relevant Vendor Requirements:	VE11.10.01, VE11.11.01, VE11.19.01

Question/Problem

How can a known answer test be implemented for the DSA algorithm?

Resolution

In order to perform a known answer test (KAT) for the DSA algorithm, the cryptographic module would have to be able to regenerate a known signature value each time the test is performed. Signature generation with the DSA involves the generation of a *k* value, which would have to be fixed in order to regenerate a particular signature value. However, FIPS 186-2 (DSS) requires that "Parameter *k* must be regenerated for each signature."

For the DSA known answer test, requiring an implementation to fix the *k* value for self-testing purposes may pose a greater risk than not implementing a known answer test at all, plus it contradicts the requirement in FIPS 186-2 quoted above. *Thus, it is acceptable for a cryptographic module to not implement a DSA KAT.*

HOWEVER, if a DSA KAT is not implemented, then there MUST be a pairwise consistency test for the DSA algorithm (see AS11.19). This test checks to see that signatures generated by the cryptographic module are verifiable, and it shall be implemented on each DSA key pair.

Additional Comments

The absence of a DSA known answer test in a cryptographic module will be noted in an accompanying implementation note.

11.3 Control of firmware or software loads

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	
Relevant Assertions:	AS11.20
Relevant Test Requirements:	TE11.20.01-.04
Relevant Vendor Requirements:	VE11.20.01

Question/Problem

Who may control the key for generating a DAC or digital signature on software or firmware to be loaded into the cryptographic module? May a user who is not the manufacturer of the module control the key, and if so, under what circumstances?

Resolution

FIPS PUB 140-1 does not, in fact, stipulate who is to control a cryptographic key used to sign software. The requirements regarding this test are (1) "a cryptographic mechanism using a FIPS approved authentication technique . . . shall be applied to all validated software and firmware that can be externally loaded into a cryptographic module", and (2) "software and firmware that has been validated by the FIPS 140-1 Validation Program is considered to be validated software and firmware." (FIPS 140-1, 4.11.2).
However, if the cryptographic module manufacturer wishes to continue labeling products as complying with FIPS 140-1, then the manufacturer must continue to use a validated version of the cryptographic module software/firmware. Therefore, the manufacturer's responsibility includes ensuring that additional software/firmware is validated before loading it into the cryptographic module. If the manufacturer provides another entity with the signature key, then the manufacturer must ensure that the signer of the software is acting on the manufacturer's behalf. Normally, the manufacturer would sign the software before it was sent to the laboratory for validation testing. Once validated, the signed software could be loaded by any designated party.

Additional Comments

11.4 Error Detection Code (EDC) requirements

Applicable Levels:	**ALL**
Effective Dates:	**2/25/97-**
Last Modified:	
Relevant Assertions:	AS11.14
Relevant Test Requirements:	TE11.14.01-.06
Relevant Vendor Requirements:	VE11.14.01

Question/Problem

AS11.14 indicates that an Error Detection Code (EDC) is an acceptable method for testing the integrity of the firmware. TE11.14.01 implies that the EDC must be FIPS-approved. What non-FIPS approved algorithms are acceptable for the calculation of EDCs that are used for software authentication? For example; is a Cyclical Redundancy Check (CRC) sufficient for an EDC?

Resolution

A FIPS-approved EDC is the Data Authentication Code (DAC) specified in FIPS 113, *Computer Data Authentication*.
The intent of TE11.14.01 is to have the tester verify which of two types of techniques, 1) a non-FIPS approved EDC or 2) a DAC, is used to verify the integrity of the software. Pursuant to the results of TE11.14.01, if the tester determines that an EDC is used, then test TE11.14.02 is to be performed; if a DAC is used, than test TE11.14.03 is to be performed. Test TE11.14.01 fails if the tester is unable to determine what authentication technique, if any, is being used to verify the integrity of the firmware or software.
Therefore, TE11.14.01 does *not* require the EDC to be FIPS-approved. A known technique such as the CRC may be used (or other common non-cryptographic firmware verification techniques); in which case TE11.14.02 applies if the tester can determine that this is the technique used. However, if a DAC is used that contains cryptographic operations such as hashing to a known value, a MAC, or a digital signature, then a FIPS-approved algorithm must be used (e.g., DSA), and either TE11.14.03 or TE11.14.04 is applicable.

Additional Comments

11.5 Use of Triple DES in the Calculation of a Data Authentication Code (DAC)

Applicable Levels:	**ALL**
Effective Dates:	**9/5/2000-**
Last Modified:	
Relevant Assertions:	AS11.14, AS11.20
Relevant Test Requirements:	TE11.14.01-.06, TE11.20.01-.04
Relevant Vendor Requirements:	VE11.14.01, VE11.20.01

Question/Problem

May the Triple DES algorithm be used in the calculation of a Data Authentication Code (DAC) to meet the requirements listed in the Self-Test section of FIPS 140-1? Furthermore, is the use of the Triple DES algorithm in the calculation of a DAC compliant with FIPS 113: Computer Data Authentication?

Resolution

Section 3 of FIPS 113 states that "The Data Authentication Algorithm (DAA) makes use of the Data Encryption Standard (DES) cryptographic algorithm specified in FIPS PUB 46." FIPS PUB 46-3, Data Encryption Standard, now includes the Triple DES algorithm and recommends migration to Triple DES. Therefore, Triple DES may be used to meet the requirements of FIPS 140-1 and is compliant with FIPS 113 provided that the Triple DES algorithm has been validated by the CMVP and is operated in the TCBC mode (one, two, or three key) as specified in FIPS 46-3. In addition, all input and output parameter requirements of the DAA defined in FIPS 113 must be met. Appendix 1 of FIPS 113 provides a diagram of the DAA where Triple DES would be substituted for the DES blocks and the Triple DES keys substituted for the DES key.

Additional Comments

Additional modes other than TCBC may be considered for use in the future.

Expired Implementation Guidance

E.1 Triple DES implementation within a 140-1 cryptographic module

Applicable Levels:	**ALL**
Effective Dates:	**4/9/98-11/8/1999** (formerly Implementation Guidance 9.4)
Last Modified:	
Relevant Assertions:	AS09.01
Relevant Test Requirements:	TE09.01.01
Relevant Vendor Requirements:	VE09.01.01

Question/Problem

What kind of testing must be done for a Triple DES implementation to be considered as part of the "FIPS-mode" of a validated cryptographic module, since there are currently no specific Triple DES validation tests? (Also see guidance G.6)

Resolution

If Triple DES is being implemented in a 140-1 module, then - until NIST has specific Triple DES conformance tests - in order for NIST to recognize that implementation, it must meet several critieria:

a. the DES engine(s) used within the Triple DES implementation must be validated as conforming to FIPS 46-2/81 as appropriate; and
b. it must implement one or more of the following modes of Triple DES (a.k.a. TDEA) listed in draft American National Standard X9.52, "Triple Data Encryption Algorithm" in section 3.3:

    1. TDEA Electronic Codebook Mode (TECB);
    2. TDEA Cipher Block Chaining Mode (TCBC);
    3. TDEA Cipher Block Chaining Mode - Interleaved (TCBC-I);
    4. TDEA Cipher Feedback Mode (TCFB);
    5. TDEA Cipher Feedback Mode - Pipelined (TCFB-P);
    6. TDEA Output Feedback Mode (TOFB);
    7. TDEA Output Feedback Mode - Pipelined (TOFB-P);

    ***** Note that modes 8) TDEA Cipher Block Chaining with Output Feedback Masking (TCBCM) and 9) TDEA Cipher Block Chaining with Output Feedback Masking - Interleaved (TCBCM-I) will ***NOT*** be recognized as being FIPS 140-1 compliant.

Additional Comments

E.2 Physical security requirements (Level 2) for multi-chip standalone cryptographic modules

Applicable Levels:	**2 (multi-chip standalone)**
Effective Dates:	**9/16/96-4/27/2000** (formerly Implementation Guidance 5.5 - superseded by new version)
Last Modified:	
Relevant Assertions:	AS05.19
Relevant Test Requirements:	TE05.19.01
Relevant Vendor Requirements:	VE05.19.01

Question/Problem

What are the Level 2 security requirements pertaining to enclosures designed to be non-removable, but which may be removed by force?

Resolution

1. The fact that a cryptographic module's enclosure is designed to be non-removable does not imply that it is, in fact, non-removable. When testing a multi-chip standalone module for Level 2 compliance, the tester shall attempt to remove the cryptographic module's enclosure, even in cases where the manufacturer claims that the enclosure is non-removable. The tester shall apply a level of effort necessary to remove the cover. ***(Note that the definition of a "removable cover" - as opposed to a non-removable enclosure - is being reviewed by NIST and CSE.)***

2. When a tester opens and closes the enclosure, attempting not to leave evidence of tampering, the time taken to accomplish this shall NOT include the time (or estimated time) needed to tamper with the cryptographic module's internal electronic components. This time shall include the time required to remove any additional physical barriers (e.g., epoxy over the components or internal shields) such that the internal electronic components of the cryptographic module can be accessed, and the "drying time" necessary for any sealant that is used to close and reseal the enclosure.

3. The tester shall only use tools and materials that are readily available in places such as a hardware store or hobby shop. The use of extremely expensive tools (e.g., a laser) are excessive for Level 2 physical security testing.

4. In opening and closing the enclosure, a tester shall use only cryptographic module components that are part of the cryptographic module being tested. For example, a tester shall not use another enclosure, label, or seal in place of the original.

5. The tester shall have some experience attempting to open and close the cryptographic module; however, the tester is not assumed to be an expert at penetrating the cryptographic module being tested. Rather, the assumption is that the tester has experience with LESS THAN 10 instances of the cryptographic module being tested.

Additional Comments

1. If a tester needs 2 hours or more to open the enclosure, gain access to the internal electronic components, and close the enclosure on a cryptographic module WITHOUT leaving evidence of tampering, then this is sufficient for passing test TE05.19.01.

2. "Detectable signs" and "tamper evidence" shall include both inoperability and visual evidence on the cryptographic module itself. Inoperability may include situations where an attempt to operate the

cryptographic module requires a significantly greater physical effort than normal (e.g., a PC Card or smart card that cannot be easily placed (or fits too loosely) in its slot or reader/writer.).