Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program

National Institute of Standards and Technology
Communications Security Establishment

Initial Release: March 28, 2003

Last Update: May 22, 2008

Table of Contents

 New Guidance and Modified Guidance

New Guidance

- 01/24/08: 7.7 Key Establishment and Key Entry and Output
- 12/18/07: 1.13 CAVP Requirements for Vendor Affirmation of NIST SP 800-38D
- 11/16/07: 7.6 RNGs: Seeds, Seed Keys and Date/Time Vectors
- 07/03/07: 14.3 Logical Diagram for Software, Firmware and Hybrid Modules
- 06/28/07: G.13 Instructions for completing a FIPS 140-2 Validation Certificate
- 06/21/07: 1.11 CAVP Requirements for Vendor Affirmation of NIST SP 800-56A
- 06/21/07: 1.12 CAVP Requirements for Vendor Affirmation of NIST SP 800-90
- 01/26/07: G.12 Post-Validation Inquiries
- 01/25/07: 1.10 Vendor Affirmation of Cryptographic Security Methods

Modified Guidance

- 05/22/08: G.13 Instructions for completing a FIPS 140-2 Validation Certificate – Updated reference for symmetric key wrapping annotation
- 02/07/08: 7.1 Acceptable Key Establishment Protocols – Updated AES Key Wrap URL.
- 01/24/08: G.2 Completion of a test report: Information that must be provided to NIST and CSE – Added reference to CMVP comments document.
- 01/24/08 G.8 Revalidation Requirements – Added reference to the CMVP FAQ in change scenario 1.
- 01/16/08: G.13 Instructions for completing a FIPS 140-2 Validation Certificate – Added reference for listing multiple operating systems, and reference for symmetric key wrapping annotation.
- 01/16/08: 1.8 Listing of DES Implementations – Updated to reflect the ending of the DES transition period.
- 01/16/08: 7.1 Acceptable Key Establishment Protocols
- 01/16/08: 9.4 Cryptographic Algorithm Tests for SHS Algorithms and Higher Cryptographic Algorithms Using SHS Algorithms – Added RSA KAT requirements regarding the relationship of the exponents.
- 11/08/07: G.2 Completion of a test report: Information that must be provided to NIST and CSE – Added clarification on output type of draft certificate.
- 10/18/07: Updated links
- 07/26/07: Minor editorial updates.

- 06/26/07: 7.1 Acceptable Key Establishment Protocols – Updated to reflect the publishing of NIST SP 800-56A.
- 06/26/07: G.8 Revalidation Requirements – Additional guidelines for determining <30% change for Scenario 3.
- 06/22/07: G.2 Completion of a test report: Information that must be provided to NIST and CSE - editorial changes for clarification.
- 06/22/07: G.8 Revalidation Requirements - editorial changes for clarification.
- 06/14/07: 3.1 Authorized Roles
- 03/19/07: Updated references to revision of NIST SP 800-57
- 02/26/07: 1.6 Use of Non-NIST-Recommended Asymmetric Key Sizes and Elliptic Curves
- 02/23/07: 7.4 Zeroization of Power-Up Test Keys
- 01/25/07: G.8 Revalidation Requirements
- 01/25/07: 7.5 Strength of Key Establishment Methods

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) 140-2, *Security Requirements for Cryptographic Modules*. In addition, this program covers the testing of Approved security functions, including the Advanced Encryption Standard, 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 140-2* (DTR), which is used by CMT laboratories to test for a cryptographic module's conformance to FIPS 140-2. 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 140-2, 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 140-1 and 140-2:

- Cryptographic Module Validation List

General Issues

G.1 Request for Guidance from the CMVP

Applicable Levels:	*All*
Original Publishing Date:	*02/25/1997*
Effective Date:	
Last Modified Date:	*09/12/2005*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

The Cryptographic Module Validation Program (CMVP) and the Cryptographic Algorithm Validation Program (CAVP) defines two types of questions: *Programmatic Questions* and *Test-specific Questions*. The CMVP and CAVP define two types of requests: *Informal Requests* and *Official Requests*.

Question/Problem

What is the difference between *Informal Requests* verses *Official Requests*? To whom should these questions be directed? If an official reply is requested for a question, is there a defined format for these types of requests?

Resolution

Programmatic Questions: These are questions pertaining to the general operation of the Cryptographic Module Validation Program or the Cryptographic Algorithm Validation Program. The CMVP and CAVP suggest reviewing the CMVP Frequently Asked Questions (FAQ), and the CAVP Frequently Asked Questions (FAQ), CMVP Announcements and CMVP Notices posted on the CMVP web site first as the answer may be readily available. The information found on the CMVP web site provides the official position of the CMVP and CAVP.

Test-specific Questions: These are questions concerning specific test issues of the Cryptographic Module Validation Program or the Cryptographic Algorithm Validation Program. These issues may be technology related or related to areas of the standard that may appear to be open to interpretation.

General Guidance: Programmatic questions regarding the CMVP or the CAVP can be directed to either NIST or CSE by contacting the appropriate points of contact listed below. The complete list of NIST and CSE points of contacts shall be included on copy for all questions.

Vendors who are under contract with a CMT laboratory for FIPS 140-2 or algorithm testing of a particular implementation(s) must contact the contracted CMT laboratory for any questions concerning the test requirements and how they affect the testing of the implementation(s).

CMT Laboratories must submit all *test-specific questions* in the RFG format described below. These questions must be submitted to all points of contact.

Federal agencies and departments, and vendors not under contract with a CMT laboratory who have specific questions about a FIPS 140-2 test requirements or any aspect of the CMVP or CAVP should contact the appropriate NIST and CSE points of contact listed below.

Questions can either be submitted by e-mail, telephone, and facsimile or written (if electronic document, Microsoft Word document format is preferred).

Informal Request: Informal requests are considered as *ad hoc* questions aimed at clarifying issues about the FIPS 140-2 and other aspects of the CMVP and CAVP. Replies to informal requests by the CMVP are non-binding and subject to change. It is recommended that informal requests be submitted to all points of contact. Every attempt is made to reply to informal request with accurate, consistent, clear replies on a very timely basis.

Official Request: If an official response is requested, then an official request must be submitted to the CMVP and/or CAVP written in the Request for Guidance (RFG) format described below. An official response requires internal review by both NIST and CSE, as well as with others as necessary, and may require follow-up questions from the CMVP and/or CAVP. Therefore such requests, while time sensitive, may not be immediate.

Request for Guidance Format: Questions submitted in this format will result in an official response from the CMVP and CAVP that will state current policy or interpretations. This format provides the CMVP and CAVP a clear understanding of the question. A RFG shall have the following items:

1. Clear indication of whether the RFG is **PROPRIETARY** or **NON-PROPRIETARY**,
2. A descriptive title,
3. Applicable statement(s) from FIPS 140-2,
4. Applicable assertion(s) from the FIPS 140-2 DTR,
5. Applicable required test procedure(s) from the FIPS 140-2 DTR,
6. Applicable statements from FIPS 140-2 Implementation Guidance,
7. Applicable statements from algorithmic standards,
8. Background information if applicable, including any previous CMVP or CAVP official rulings or guidance,
9. A concise statement of the problem, followed by a clear and unambiguous question regarding the problem, and
10. A suggested statement of the resolution that is being sought.

All questions should be presented in a detailed and implementation-specific format, rather than an academic or hypothetical format. This information should also include a brief non-proprietary description of the implementation and the FIPS 140-2 target security level. All of this will enable a more efficient and timely resolution of FIPS 140-2 related questions by the CMVP and CAVP. The statement of resolution shall be stated in a manner which the CMVP and CAVP can either answer "YES" or "NO". The CMVP may optionally provide rationale if the answer is not in line with the suggested statement of resolution.

When appropriate, the CMVP and CAVP 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.

Preferably, questions should be non-proprietary, as their response will be distributed to ALL CMT laboratories. Distribution may be restricted on a case-by-case basis.

NIST and CSE Points of Contact:

- **National Institute of Standards and Technology – CMVP**

Randall J. Easter reaster@nist.gov
(301) 975-4641

Allen Roginsky allen.roginsky@nist.gov
(301) 975-3603

National Institute of Standards and Technology – CAVP

Sharon Keller skeller@nist.gov
(301) 975-2910

- **Communications Security Establishment – CMVP**
(of the Government of Canada)

Ken Lu ken.lu@cse-cst.gc.ca
(613) 991-8122

Jean Campbell jean.campbell@cse-cst.gc.ca
(613) 991-8121

Additional Comments

G.2 Completion of a test report: Information that must be provided to NIST and CSE

Applicable Levels:	*All*
Original Publishing Date:	*02/25/1997*
Effective Date:	
Last Modified Date:	*01/24/2008*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What information should be provided to NIST and CSE upon completion of the CMT laboratory conformance testing in order for NIST and CSE to perform a validation review? Are there any other additional requirements during report COORDINATION?

Resolution

The following test report information shall be provided to both NIST and CSE by the CMT laboratory upon report submission. The ZIP file and files within the ZIP file shall follow all programmatic naming conventions.

1. **Non-proprietary Security Policy** <PDF>
   Reference FIPS 140-2 DTR and IG 14.1 for requirements. The non-proprietary security policy shall not be marked as proprietary or copyright without a statement allowing copying or distribution.

2. **CRYPTIK v5.5 (or higher) Reports**
   The validation report submission must be output from the NIST provided Cryptik tool.

   a. **Signature page** <insert PDF of signed signature page>

   b. **General Information** <PDF>

   c. **Billing for Cost Recovery** <PDF – do not include if not applicable>

   d. **Report Overview with Assessments** <PDF>

   e. **Full Report with Assessments** <PDF>

   f. **Certificate** <DOC>

      1. The RTF output from CRYPTIK shall be renamed to a DOC file.
      2. Shall include PIV Card Application certificate number reference as applicable.

   g. **Vendor Text File** <TXT>
      Export the validation data and include the <name>_vendor.txt file.

   h. **Definitions / References** <PDF - optional>

3. **Physical Test Report** <PDF – mandatory at Levels 2, 3 and 4>
   The laboratory's physical testing report with photos, drawing, etc. as applicable.

4. **Revalidation change summary** <PDF – if applicable>

5. **Section Summaries** < PDF – optional>
   Briefly describe how the requirements in each section are met.

The CMT laboratory has the option to additionally provide *Notes* and *Proprietary* output with the Full Report with Assessments, but this is not required by NIST and CSE. The Report Overview with Assessments shall not include proprietary information. The PDF files shall not be locked. All Cryptik PDF submission output, scanned signature page, physical test report, revalidation change summary and optional section summaries shall be merged into a single PDF document.

The submission documents shall be ZIP'ed into a single file, encrypted and sent to the following NIST and CSE points of contact:

- **NIST:** CMVP@nist.gov
- **CSE:** CMVP@cse-cst.gc.ca

Once a report is received by the CMVP and moves to IN REVIEW, comments may be generated for the laboratory to resolve. The CMVP comments are returned to the laboratory and the report will move to COORDINATION.

The laboratory will address each comment and update any applicable files as necessary in addition to providing a response and additional clarification as necessary in the CMVP comments document. The laboratory will re-submit the report in its entirety as above (original report submission) and also include the updated CMVP comments file.

6. **CMVP Comments** <DOC>

Additional Comments

Reception of the electronic submission documents will determine position in the CMVP validation review queue. Those reports marked to be listed, will appear in the weekly published Modules-In-Process listing posted on the CMVP web site: http://csrc.nist.gov/groups/STM/cmvp/inprocess.html

An Initial Review will not be performed on the submission documents. The received report will only be opened to gather information necessary for the pre-validation data base and for NIST cost recovery billing.

G.3 Partial Validations and Not Applicable Areas of FIPS 140-2

Applicable Levels:	*All*
Original Publishing Date:	*02/25/1997*
Effective Date:	
Last Modified Date:	*01/21/2005*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

Can a cryptographic module be validated only for selected areas of Section 4 of FIPS 140-2? Which areas of Section 4 of FIPS 140-2 can be marked *Not Applicable*?

Resolution

NIST and CSE will not issue a validation certificate unless the cryptographic module meets at least the Security Level 1 requirements for each area in Section 4 of FIPS 140-2 that cannot be designated as *Not Applicable* according to the following:

- **Section 4.5**, Physical Security may be designated as *Not Applicable* if the cryptographic module is a software-only module and thus has no physical protection mechanisms;
- **Section 4.6**, Operational Environment may be designated as *Not Applicable* depending on the module implementation (e.g. if the operational environment for the cryptographic module is a limited operational environment); and
- **Section 4.11**, Mitigation of Other Attacks may be designated as *Not Applicable* if the vendor has made no claim that the cryptographic module provides such protection mechanisms.

The CMT laboratory must provide in the validation test report the rationale for marking sections as *Not Applicable*.

Additional Comments

If a section is *Not Applicable*, it will be marked N/A on the module validation certificate. If Section 4.6 is N/A, depending on the module implementation, configuration information may still be required on the module validation certificate (e.g. a *firmware* module must provide the tested configuration)

G.4 Design and testing of cryptographic modules

Applicable Levels:	*All*
Original Publishing Date:	*11/12/1997*
Effective Date:	
Last Modified Date:	*04/28/2000*
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 140-2, 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 140-2, *Security Requirements for Cryptographic Modules*.

Also see IG G.9, regarding FSM and Security Policy consolidation and formatting.

G.5 Maintaining validation compliance of software or firmware cryptographic modules

Applicable Levels:	*All*
Original Publishing Date:	*11/21/1997*
Effective Date:	
Last Modified Date:	*03/23/2006*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

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

Resolution

The tested/validated module version, operational environment upon which it was tested, and the originating vendor are stated on the validation certificate. The certificate serves as the benchmark for the module-compliant configuration.

This guidance addresses two separate scenarios: actions a vendor can affirm or change to maintain a modules validation, and actions a user can affirm to maintain a modules validation.

This guidance is *not applicable* for validated modules when **Section 4.5 Physical Security** has been validated at Levels 2 or higher.

Vendor

1. A vendor may perform post-validation recompilations of a software or firmware module and affirm the modules continued validation compliance provided the following is maintained:

    a) Software modules that do not require any source code modifications (e.g., changes, additions, or deletions of code) to be recompiled and ported to another operational environment must:

        i) For **Level 1 Operational Environment**, a software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any general purpose computer (GPC) provided that the GPC uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and

        ii) For **Level 2 Operational Environment**, a software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any GPC provided that the GPC incorporates the specified CC evaluated EAL2 (or equivalent) operating system/mode/operational settings or another compatible CC evaluated EAL2 (or equivalent) operating system with like mode and operational settings.

    b) Firmware modules (i.e. Operational Environment is *not applicable)* modules that do not require any source code modifications (e.g., changes, additions, or deletions of code) to be recompiled and its identified unchanged tested operating system (i.e. same version or revision number) may be ported together from one GPC or platform to another GPC or platform while maintaining the module's validation.

The CMVP allows vendor porting and re-compilation of a validated software and firmware cryptographic module from the OS(s) and/or GPC(s) specified on the validation certificate to an OS(s) and/or GPC(s) which were not included as part of the validation testing. The validation status is maintained on the new OS(s) and/or GPC without re-testing the cryptographic module on the new OS(s) and/or GPC(s). However, the CMVP makes no statement as to the correct operation of the module when ported to an OS(s) and/or GPC(s) not listed on the validation certificate.

The vendor may provide a new security policy per which would affirm and include references to the new operational environment(s), GPC(s) or platform(s).

2. Software or firmware modules that require non-security relevant source code modifications (e.g., changes, additions, or deletions of code) to be recompiled and ported to another hardware or operational environment must be reviewed by a CMT laboratory and revalidated per **FIPS 140-2 IG G.8 (1)** to ensure that the module does not contain any operational environment-specific or hardware environment-specific code dependencies.

3. If the new operational environment and/or platform is requested to be updated on the validation certificate, the CMT laboratory shall follow the requirements for non-security relevant changes in **FIPS 140-2 IG G.8 (1)** and in addition, perform the regression test suite of operational tests included in **FIPS 140-2 IG G.8** Table G.8.1 – Regression Test Suite. Underlying algorithm validations must meet requirements specified in **FIPS 140-2 IG 1.4** *Binding of Cryptographic Algorithm Validation Certificates.*

   Upon re-testing and validation, the CMVP provides the same assurance as the original operational environment(s) and platform(s) as to the correct operation of the module when ported to the newly listed OS(s) and/or platform(s) operational environments which would be added to the modules validation web entry.

The vendor must meet all applicable requirements in **FIPS 140-2 Section 4.10**.

This policy only addresses the operational environment under which a software or firmware module executes and does not affect requirements of the other sections of FIPS 140-2. A module must meet all requirements of the level stated.

FIPS 140-2 IG 1.3 *Firmware Designation* describes the difference in terminology between a *software* and a *firmware* module.

User

A user may not modify a validated module. Any user modifications invalidate a modules validation. [Note 1]

A user may perform post-validation porting of a module and affirm the modules continued validation compliance provided the following is maintained:

1. For **Level 1 Operational Environment**, a software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any general purpose computer (GPC) provided that the GPC uses the specified single user operating system/mode specified on the validation certificate, or another compatible single user operating system, and

2. For **Level 2 Operational Environment**, a software cryptographic module will remain compliant with the FIPS 140-2 validation when operating on any GPC provided that the GPC incorporates the specified CC evaluated EAL2 (or equivalent) operating system/mode/operational settings or another compatible CC evaluated EAL2 (or equivalent) operating system with like mode and operational settings.

The CMVP allows user porting of a validated software cryptographic module on an OS(s) and/or GPC(s) which were not included as part of the validation testing. The validation status is maintained on the new OS(s) and/or GPC without re-testing the cryptographic module on the new OS(s) and/or GPC(s). However, the

CMVP makes no statement as to the correct operation of the module when executed on an OS(s) and/or GPC(s) not listed on the validation certificate.

Additional Comments

Users include third party integrators or any entity that is the not originating vendor as specified on the validation certificate.

Note 1: A user may post-validation recompile a module if the unmodified source code is available and the modules Security Policy provides specific guidance on acceptable recompilation methods to be followed as a specific exception to this guidance. The methods in the Security Policy must be followed without modification to maintain validation under this guidance.

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

Applicable Levels:	*All*
Original Publishing Date:	*03/11/1998*
Effective Date:	
Last Modified Date:	*04/02/1998*
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

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 140-2 compliant.

The FIPS 140-2 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

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

Applicable Levels:	*All*
Original Publishing Date:	*04/14/1998*
Effective Date:	
Last Modified Date:	
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?

Resolution

The CMT laboratories are accredited by NVLAP to perform cryptographic module validation testing to determine compliance with FIPS 140-2. 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 140-2, 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 irresolvable 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*
Original Publishing Date:	*08/17/2001*
Effective Date:	
Last Modified Date:	*01/24/2008*
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?

Resolution

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.)

A cryptographic module that is changed under change scenarios 1, 2 and 4 below, must meet ALL standards, implementation guidance and algorithm testing that were met at the time of original validation. A module does not need to continue to meet requirements that were removed or added since the time of original validation.

A cryptographic module that is changed under change scenarios 3 and 5 below, must meet ALL standards, implementation guidance and algorithm testing in effect at the time of module report submission to the CMVP. 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 and 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 under scenarios 3 and 5, this Triple-DES implementation must be tested and validated against FIPS 46-3, and the cryptographic module must meet the applicable FIPS 140-2 requirements, e.g., self-tests.

There are five possible **change** scenarios:

1. Modifications are made to hardware, software or firmware components **that do not affect any FIPS 140-1 or FIPS 140-2 security relevant items**. The vendor is responsible for providing the applicable documentation to the CMT laboratory, which identifies the modification(s). Documentation may include a previous validation report, design documentation, source code, etc. The CMT laboratory shall review the vendor-supplied documentation and identify any additional documentation requirements. The CMT laboratory shall also determine additional testing as required to confirm that FIPS 140-1 or FIPS 140-2 security relevant items have not been affected by the modification.

   Upon successful review and applicable testing as required, the CMT laboratory shall submit a signed explanatory letter (sent to the CMVP electronically in PDF format) to NIST and CSE that contains a description of the modification(s) and lists the affected TEs and their associated laboratory assessment. The assessment shall include the analysis performed by the laboratory that confirms that no security relevant items were affected. The letter shall also indicate whether the modified cryptographic module replaces the previously validated module or adds to the latter. If new algorithm certificates were obtained, they shall be listed.

   Upon a satisfactory review by NIST and CSE, the updated version or release information will be posted on the *Validated FIPS 140-1 and FIPS 140-2 Cryptographic Module List* web site entry associated with the original cryptographic module. No new certificate will be issued.

   It is strongly encouraged that a new security policy be provided for posting that updates the module version number with the new version number.

   Please refer to CMVP FAQ Section 5.8 for other non-security relevant change requests.

2. No modifications are made to any hardware, software or firmware components of the cryptographic module. All version information is unchanged. Post validation, Approved security relevant functions or services for which testing was available at the time of validation, or security relevant functions or services that were not tested during the original validation, are now tested and are being submitted for inclusion as a FIPS Approved function or service. The CMT laboratory is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient and the vendor is responsible for submitting the requested documentation to the CMT laboratory. Documentation may

include a previous validation report and applicable NIST and CSE rulings, design documentation, source code, etc.

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

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

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

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

3. Modifications are made to hardware, software or firmware components **that affect some of the FIPS 140-2 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 modules security relevant features[1]. The CMT laboratory is responsible for identifying the documentation that is needed to determine whether a revalidation is sufficient and the vendor is responsible for submitting the requested documentation to the CMT laboratory. Documentation may include a previous validation report and applicable NIST and CSE rulings, design documentation, source code, etc.

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

   a. Review the COMPLETE list of assertions for the module embodiment and security level,
   b. Identify, from the previous validation report, the assertions that have been affected by the modification,
   c. Identify additional assertions that were NOT previously tested but should now be tested due to the modification, and
   d. 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 Table G.8.1 – Regression Test Suite.

[1] For example, security relevant features may include addition/deletion/change of minor components and their composition, addition/deletion of ports and interfaces, addition/delete/modification of security functions, modification of the physical boundary and protection mechanisms. These changes may affect many TE's yet be considered a minor change (<30%), or affect few TE's yet be a gross change (>30%).

When a cryptographic module is tested for revalidation from FIPS 140-1 to FIPS 140-2, the CMT laboratory may re-use information contained in the FIPS 140-1 test report for the preparation of the FIPS 140-2 test report. The table found in Mapping FIPS 140-2 to FIPS 140-1 can be used to guide the tester.

Note: Included in the table are the ASs, TEs, VEs (AS2 for FIPS 140-2 and AS1 for FIPS 140-1, etc.), security level(s), single chip (S), multi chip embedded (ME), multi chip standalone (MS), operational test (Op - x is used for the operational tests, r is used for regression test), applicable to FIPS 140-2 (M - match), and comment (describes the applicability of FIPS 140-1 results to FIPS 140-2, and may include info on the FIPS 140-2 requirement). The CMT laboratory shall perform all the operational tests (TEs labeled with an x and an r in the Op field).

The CMTL must provide a summary of the changes and rationale of why this meets the <30% guideline. The CMVP upon review, may determine that the changes are >30% and shall be submitted as a full report. The CMT laboratory shall document the test results in the associated assessments and all affected TEs shall be annotated as "re-tested." The CMT laboratory shall submit a test report as specified in G.2 describing the modification and highlighting those assertions that have been modified and retested (selecting the re-tested option in CRYPTIK). Upon a satisfactory review by NIST and CSE, the updated version will be revalidated to FIPS 140-2 and a new certificate will be issued.

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

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

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

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

5. 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 a CMT laboratory. The CMT laboratory shall submit a test report as specified in G.2.

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 a CMT laboratory.

Table G.8.1 – Regression Test Suite

Regression Testing Table		
AS	**TE**	**Security Level**

		1	2	3	4
Section 1 - Cryptographic Module Specification					
AS01.03	TE.01.03.02	x	x	x	x
Section 2 - Cryptographic Module Ports and Interfaces					
AS02.06	TE02.06.02	x	x	x	x
	TE02.06.04	x	x	x	x
AS02.13	TE02.13.03	x	x	x	x
AS02.14	TE02.14.02	x	x	x	x
AS02.16	TE02.16.02			x	x
AS02.17	TE02.17.02			x	x
Section 3 - Roles, Services and Authentication					
AS03.02	TE03.02.02	x	x	x	x
	TE03.02.03	x	x	x	x
AS03.12	TE03.12.03	x	x	x	x
AS03.13	TE03.13.02	x	x	x	x
AS03.14	TE03.14.02	x	x	x	x
AS03.15	TE03.15.02	x	x	x	x
AS03.17	TE03.17.02		x		
AS03.18	TE03.18.02		x		
AS03.19	TE03.19.02			x	x
	TE03.19.03			x	x
AS03.21	TE03.21.02	x	x	x	x
AS03.22	TE03.22.02		x	x	x
AS03.23	TE03.23.02	x	x	x	x
Section 4 - Finite State Model					
AS04.03	TE.04.03.01	x	x	x	x
AS04.05	TE04.05.08	x	x	x	x
Section 5 - Physical Security					
	NONE				
Section 6 - Operational Environment					
AS06.05	TE06.05.01	x			
AS06.06	TE06.06.01	x			
AS06.07	TE06.07.01	x	x	x	x
AS06.08	TE06.08.02	x	x	x	x
AS06.11	TE06.11.02		x	x	x
	TE06.11.03		x	x	x
AS06.12	TE06.12.02		x	x	x
	TE06.12.03		x	x	x
AS06.13	TE06.13.02		x	x	x
	TE06.13.03		x	x	x
AS06.14	TE06.14.02		x	x	x
	TE06.14.03		x	x	x
AS06.15	TE06.15.02		x	x	x
AS06.16	TE06.16.02		x	x	x
AS06.17	TE06.17.02		x	x	x

AS06.22	TE06.22.02			x	x
	TE06.22.03			x	x
AS06.24	TE06.24.02			x	x
	TE06.24.03			x	x
AS06.25	TE06.25.02			x	x
Section 7 - Cryptographic Key Management					
AS07.01	TE07.01.02	x	x	x	x
AS07.02	TE07.02.02	x	x	x	x
AS07.15	TE07.15.02	x	x	x	x
	TE07.15.03	x	x	x	x
	TE07.15.04	x	x	x	x
AS07.25	TE07.25.02	x	x	x	x
AS07.27	TE07.27.02	x	x	x	x
AS07.28	TE07.28.02	x	x	x	x
AS07.29	TE07.29.02	x	x	x	x
AS07.31	TE07.31.04			x	x
AS07.39	TE07.39.02	x	x	x	x
AS07.41	TE07.41.02	x	x	x	x
Section 8 - EMI / EMC					
	As Required				
Section 9 - Self Tests					
AS09.04	TE09.04.03	x	x	x	x
AS09.05	TE09.05.03	x	x	x	x
AS09.09	TE09.09.02	x	x	x	x
AS09.10	TE09.10.02	x	x	x	x
AS09.12	TE09.12.02	x	x	x	x
AS09.22	TE09.22.07	x	x	x	x
AS09.35	TE09.35.05	x	x	x	x
AS09.40	TE09.40.03	x	x	x	x
	TE09.40.04	x	x	x	x
AS09.45	TE09.45.03	x	x	x	x
AS09.46	TE09.46.03	x	x	x	x
Section 10 - Design Assurance					
AS10.03	TE10.03.02	x	x	x	x
Section 11 - Mitigation of Other Attacks					
	NONE				
Appendix C - Cryptographic Module Security Policy					
	As Required				

Additional Comments

G.9 FSM, Security Policy, User Guidance and Security Officer Guidance Documentation

Applicable Levels:	*All*
Original Publishing Date:	*05/29/2002*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

May a CMT lab create original documentation specified in FIPS 140-2? The specific documents in question are the FSM, Security Policy, User Guidance and Security Officer Guidance.

Resolution

FSM and Security Policy:

A CMT lab may take existing vendor documentation for an existing cryptographic module (post-design and post-development) and consolidate or reformat the existing information (from multiple sources) into a set format. If this occurs, NIST and CSE shall be notified of this when the validation report is submitted. Additional details for the individual documents are provided below.

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).

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 140-2 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. The mapping(s) must be maintained by the lab as part of the validation records.

Consolidating and reforming are 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.

User Guidance and Security Officer Guidance:

A CMT lab may create User Guidance, Security Officer Guidance and other non-design related documentation for an existing cryptographic module (post-design and post-development). If this occurs, NIST and CSE shall be notified of this when the validation report is submitted.

Additional Comments

G.10 Physical Security Testing for Re-validation from FIPS 140-1 to FIPS 140-2

Applicable Levels:	*All*
Original Publishing Date:	*03/29/2004*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

FIPS 140-2 IG G.2 specifies that all report submissions must include a separate physical security test report section for Levels 2, 3 or 4.

Question/Problem

Questions have been asked regarding re-validation test reports where a previous separate physical security test report may not have existed or evidence such as images, etc. had not been provided with the original validation test report. What should the CMT laboratory provide if the physical security requirements have not changed?

Resolution

If a previous *separate* physical security test report did not exist for the module undergoing re-validation testing and the physical security features of the module have not changed, the CMT Laboratory must compile the physical security test evidence that has been maintained from their records from the original tested module and create and submit a new *separate* physical security test report. If the records no longer exist because they were generated outside the period of the CMT Laboratories record retention period specified in the quality manual, then re-testing shall be required to provide such evidence. It is not required that a CMT laboratory perform re-testing simply to create new photographic images that may not have been saved or generated during the original testing

Additional Comments

If the CMT Laboratory was not the original testing laboratory and therefore does not have access to the previous test records, then the module shall be re-tested to be able to provide such evidence. Without the prior records, the new CMT Laboratory cannot make a determination that the physical security has or has not changed.

G.11 Testing using Emulators and Simulators

Applicable Levels:	*All*
Original Publishing Date:	*09/12/2005*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

Vendors of cryptographic modules use independent, accredited Cryptographic Module Testing (CMT) Laboratories to have their modules tested for conformance to the requirements of FIPS 140-2. Organizations wishing to have testing performed would contract with the laboratories for the required services. The Derived Test Requirements (DTR) document describes the methods that will be used by accredited laboratories to test whether the cryptographic module conforms to the requirements of FIPS 140-2. It includes detailed procedures, inspections, documentation and code reviews, and operational and physical tests that the tester must follow, and the expected results that must be achieved for the cryptographic module to satisfy its conformance to the FIPS PUB 140-2 requirements. These detailed methods are intended to provide a high degree of objectivity during the testing process and to ensure consistency across the accredited testing laboratories.

Definitions:

An **emulator** attempts to "model" or "mimic" the behavior of a cryptographic module. The correctness of the emulators' behavior is dependant on the inputs to the emulator and how the emulator was designed. It is not guaranteed that the actual behavior of the cryptographic module is identical, as many other variables may not be modeled correctly or with certainty.

A **simulator** exercises the actual module source code (e.g., VHDL code) prior to physical entry into the module (e.g., an FPGA or custom ASIC). From a behavioral perspective, the behavior of the source code within the simulator may be logically identical when placed into the module or instantiated into logic gates. However, many other variables exist that may alter the actual behavior (e.g. path delays, transformation errors, noise, environmental, etc). It is not guaranteed that the actual behavior of the cryptographic module is identical, as many other variables may not be identified with certainty.

Question/Problem

May a CMT Laboratory tester use module emulation and/or simulation methods to perform cryptographic module testing?

Resolution

There are three broad areas of focus during the testing of a cryptographic module: operational testing of the module at the defined boundary of the module, algorithm testing and operational fault induction error testing.

1. Operational Testing

   Emulation or simulation is prohibited for the operational testing of a cryptographic module. Actual

testing of the cryptographic module must be performed utilizing the defined ports and interfaces and services that a module provides.

2. Operational Fault Induction

   An emulator or simulator may be utilized for fault induction to test a cryptographic module's transition to error states as a complement to the already allowed source code review. Rationale must be provided for the applicable TE why a method does not exist to induce the actual module into the error state for testing.

3. Algorithm Testing

   Algorithm testing utilizing the defined ports and interfaces and services that a module provides is the preferred method. This method most clearly meets the requirements of FIPS 140-2 IG 1.4.

   If this preferred method is not possible where the module's defined set of ports and interfaces and services do not allow access to internal algorithmic engines, two alternative methods may be utilized:

   a. A module may be modified by the CMT Laboratory for testing purposes to allow access to the algorithmic engines (e.g. test jig, test API), or

   b. A module simulator may be utilized.

   When submitting the algorithm test results to the CAVP, the actual operational environment on which the testing was performed must be specified (e.g. including modified module identification or simulation environment). When submitting the module test report to the CMVP, AS01.12 must include rationale explaining why the algorithm testing was not conducted on the actual cryptographic module.

   An emulator may not be used for algorithm testing.

Additional Comments

G.12 Post-Validation Inquiries

Applicable Levels:	*All*
Original Publishing Date:	*01/26/2007*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

FIPS 140-2 conformance testing that is performed by the accredited Cryptographic Module Testing Laboratories (CMTL) and validation of those test results by NIST and CSE provide a level of assurance that a module conforms to the requirements of FIPS 140-2 and other underlying standards.

Once a module is validated and posted on the NIST CMVP web site, many parties review and scrutinize the merits of the validation. These parties may be potential procurers of the module, competitors, academics or others.

If a party performing a post-validation review believes that a conformance requirement of FIPS 140-2 has not been met and was not determined during testing or subsequent validation review, the party may submit a inquiry to the CMVP for review.

Question/Problem

What is the procedure and process for submitting an inquiry for review and how is the review performed? If a review is determined to have merit, what actions may be taken regarding the module's validation status?

Resolution

An *Official Request* must be submitted to the CMVP in writing with signature following the guidelines in FIPS 140-2 IG G.1. If the requestor represents an organization, the official request must be on the organization's letterhead. The assertions must be objective and not subjective. The module must be identified by reference to the validation certificate number(s). The specific technical details must be identified and the relationship to the specific FIPS 140-2 Derived Test Requirements assertions must be identified. The request must be non-proprietary and not prevent further distribution by the CMVP.

The CMVP will distribute the unmodified official request to the CMTL that performed the conformance testing of the identified module. The CMTL may choose to include participation of the vendor of the identified module during its determination of the merits of the inquiry. Once the CMTL has completed its review, it will provide to the CMVP a response with rationale on the technical validity regarding the merits of the official request. The CMTL will state its position whether its review of the official request regarding the module:

1. is without merit and the validation of the module is unchanged.
2. has merit and the validation of the module is affected. The CMTL will further state its recommendations regarding the impact to the validation.

The CMVP will review the CMTLs position and rationale supporting its conclusion.

If the CMVP concurs that the official request is without merit, no further action is taken.

If the CMVP concurs that the official request has merit, a security risk assessment will be performed regarding the non-conformance issue.

Additional Comments

G.13 Instructions for completing a FIPS 140-2 Validation Certificate

Applicable Levels:	*All*
Original Publishing Date:	*06/28/2007*
Effective Date:	
Last Modified Date:	*05/22/2008*
Relevant Assertions:	*General*
Relevant Test Requirements:	

Relevant Vendor Requirements:	

Question/Problem

How are the various fields on a FIPS 140-2 validation certificate presented and provided to the CMVP for validation?

Resolution

During the pre-validation testing by an accredited cryptographic module testing laboratory, the CMVP supplied CRYPTIK tool is used to create the pre-validation draft certificate. The information to be presented on the validation certificate is entered through the Module Description screen. This draft certificate is presented to the CMVP for review and validation along with the other report components identified in G.2.

These instructions describe the presentation of the information on the certificate via entry in CRYPTIK.

File Naming: The name of the file, which contains the draft validation certificate, must be re-named from the CRYPTIK output (certificate.rtf) to the following format:

TID_nn[2]_nnnn[3]_nnnn[4]-140crtxxxx[5].doc

Front of the Validation Certificate

1. [**CRYPTO MODULE NAME**] - the complete name of the cryptographic module. Do not include the version number with the name. The name of the cryptographic module shall be consistent with IG 1.1 and the name found in the security policy. Include all necessary ™, ® and © symbols. CRYPTIK may not accept or pass the special symbols and therefore they may need to be added manually into the .doc file.

   Examples: **Crypto Acceleration Token**
   Secure Cryptographic ToolKit™
   Best Crypto©

   If the test report represents multiple modules, list all module names. If this requires the use of the word "and", then the word "and" shall be italicized. CRYPTIK cannot output italicized fonts, so this must be performed manually into the exported .doc file.

   Examples: **Crypto Sensor AM-5000 *and* AM-5010**
   Crypto 8000 PCI, Crypto 9000 PCI *and* Crypto Plus++ PCI

2. [***by* Vendor Name**] - the name of the vendor (including Corp., Inc., Ltd., etc) that developed the cryptographic module.

   Examples: ***by* AcmeSecurity, Inc.**
   ***by* Acmeproducts, Ltd.**

   Note the italicized word "by" in front of the vendor name. CRYPTIK cannot output italicized fonts, so this must be performed manually after exporting from CRYPTIK.

[2] nn is the 2-digit CMTL lab code
[3] nnnn is the CMTL assigned TID
[4] nnnn is the CSE TID
[5] xxxx is the assigned certificate number (if available)

3. [**(applicable caveat)**] - This caveat may be modified or expanded by the CMVP during the validation process.

   Cryptographic modules may not have a caveat if the module only has a single FIPS Approved mode of operation.

   Examples: **When operated in FIPS mode**
   Added if the module can also operate in a non-FIPS mode.

   When operated in FIPS mode with module [module name] validated to FIPS 140-2 under Cert. #nnn operating in FIPS mode
   Added if the module's validation is dependent on an underlying validation.

   For services provided by the FIPS-approved algorithms listed on the reverse

   When operated in FIPS mode and using FIPS Approved algorithms and processes as listed on reverse

   When operated in FIPS mode and initialized to Overall Level 2 per Security Policy
   Added if the module can be initialized to different overall levels.

   This module contains the embedded module [module name] validated to FIPS 140-2 under Cert. #nnn operating in FIPS mode
   Added if the module implements another embedded validated cryptographic module.

Back of the Validation Certificate

4. [**CRYPTO MODULE NAME *by* Vendor Name**] - the name of the cryptographic module and the vendor that developed the module. The complete name of the vendor shall be used (e.g., Corp., Inc., LTD.) This information shall match the information listed in items 1 and 2 above. Note the italic font between the module name and the vendor name. If there is more than one module name on the certificate that requires the use of the word "and", then the word "and" is also italicized. CRYPTIK cannot output italicized fonts, so this must be performed manually after exporting from CRYPTIK.

5. [**(*Version No. nnn;***] - the version number of the crypto module. This number shall be of sufficient level such that updates/upgrades/changes shall be reflected in a version change. For example, version 4 may not be sufficient if the releases are numbered 4.0, 4.1, 4.2, etc. The version number may also include letters, for example, 4.0a, 4.0b, 4.0c, etc. This shall include the version numbers for each element; hardware, software, and firmware, if applicable. Each elements version number (e.g. hardware, firmware, software) shall be separated by a semi-colon. If a module does not include an element, leave the field blank; do not enter "NA". The version numbers shall be the same as the ones found in the security policy. For example, hardware version: 4.2; software version: 4.0a. If there are several version numbers, the word "version" shall be pluralized. Note the italic font for the version numbers in the examples found in section 6 below. CRYPTIK cannot output italicized fonts, so this must be performed manually after exporting from CRYPTIK.

6. [**module type)**] - the module type is one of the following: **Software**, **Firmware, Hybrid** or **Hardware**. If a module is hardware with embedded software and/or firmware, the modules type is simply labeled Hardware. Note the non-italicized font of the module type.

   Examples: **(*Hardware Version: 4.2; Software Version: 4.0a*; Hardware)**
   (*Hardware Versions: 5.2 and 5.3, Build 3; Firmware Version: 2.45*; Hardware)

   Note the use of the comas, semi-colons and colons.

7. [**(applicable NPIVP Cert. #)**] When a module implements a validated PIV application, the application

validation certificate type and number shall be indicated under the module version number and module type line as either:

(PIV Card Application: Cert. #nnn)

(PIV Middleware: Cert. #mmm)
or
(PIV Card Application: Cert. #nnn; PIV Middleware: Cert. #mmm)

8. [***Lab Name,***] - the name of the CMT Laboratory.

9. ***NVLAP LAB CODE*** [***999999-9***] - the code assigned by NVLAP to the CMT laboratory

10. **CRYPTIK Version** [**x.xx**] - the version of the CRYPTIK tool used to create the report

11. **Level [n]** - for each of the 11 areas, include the specific level. For FIPS 140-2, the Operating System Security Level, the Physical Security level and Mitigation of Other Attacks level may not be applicable and if so, shall be marked as N/A.

    If a module meets Level 3 Physical Security and also has been tested for EFP and/or EFT, this shall be annotated on the certificate as: **Level 3 +EFP** or **+EFT** or **+EFP/EFT**

12. [***(embodiment type)***] - the cryptographic module shall be specified as one of the three types: **Multi-chip Standalone**, **Multi-chip Embedded**, or **Single-chip**, in this format.

13. **tested in the following configuration(s)**: - the specific configuration(s) that was(were) used during testing by the lab. This shall match the information in the test report in AS01.08.

    For a *software* cryptographic module at Security Level 1, the test platform does not need to be specified but the caveat "(single-user mode) must be included. For a *software* cryptographic module at Security Level 2, the test platform needs to be specified. For Java applets, the Java environment (JRE, JVM) version needs to be specified for all Security Levels. For multiple operating environment entries, separate each with a semi-colon; do not use "and".

    Examples: **Microsoft Windows XP with SP2 (single-user mode)**
    Sun Solaris Version 2.6SE running on a Sun Ultra SPARC-1 workstation
    Microsoft Windows XP with SP2; HP-UX 11.23 (single user mode)

    For a *firmware* cryptographic module, the certificate shall specify the hardware platform and operating system that was used for testing.

    Example: **BlackBerry® 7230 with BlackBerry OS® Versions 3.8, 4.0 and 4.1**

    If this field is not applicable, mark the field as N/A.

14. **The following FIPS approved Cryptographic Algorithms are used**: - the Approved security functions included in the cryptographic module and utilized by the modules callable services or internal functions. The security function is listed and then the applicable algorithm Certificate number in parentheses. Do NOT include the modes or key lengths, e.g., ECB, CBC; 128 bits. All algorithm entries must be separated by semi-colons.

    If a module contains within it an already validated embedded cryptographic module, all Approved security functions that are used by the modules callable services and internal functions shall be annotated on the certificate (both those within the embedded module and in addition to the embedded module). Algorithms

that are either in "dead code" or in the embedded module that are never called shall not be listed on the certificate.

The algorithm must meet all three (3) conditions to be listed as FIPS Approved:

1. Must be an Approved security function as specified in FIPS 140-2 Annex A;
2. Must meet all requirements of FIPS 140-2 (KAT, etc); and
3. Must be used in at least one FIPS Approved cryptographic function for that cryptographic algorithm.

Examples: **Triple-DES (Certs. #78 and #122); Triple-DES MAC (Triple-DES Cert. #78, vendor affirmed); SHS (Cert. #23); HMAC (Cert. #23); RSA (Cert. #133); CCM (Cert. #3); RNG (SP 800-90, vendor affirmed); KAS[6] (SP 800-56A, vendor affirmed)**

For MAC, the certificate number must specify the underlying algorithm certificate and the "vendor affirmed" caveat.

For multiple certificate entries, the term "Cert" shall be pluralized (i.e., Certs), an "and" shall be placed between the last two certificate numbers and there shall be an "#" in front of each number.

Examples: **AES (Cert. #11); Triple-DES (Certs. #118 and #133); DSA (Cert. #132); SHS (Certs. #103, #115 and #119); RSA (Cert. #24); HMAC (Cert. #52); RNG (Cert. #33)**

15. **non-FIPS approved algorithms**: - the non-FIPS approved cryptographic algorithms implemented in the cryptographic module.

For DES and DES MAC, after May 19, 2007, these shall be listed as non-Approved without any additional caveat.

Examples: **DES; MD5; RC4; Blowfish; EC Diffie-Hellman (key agreement)**

For algorithms that are used both Approved and non-Approved (e.g. RSA), then it only needs to be listed once on the FIPS Approved line. The Security Policy shall indicate all uses of the algorithm. Exceptions are cases where there are caveats highlighting weaknesses in the use of algorithms.

Examples: **RSA (encrypt/decrypt)**
In this example, RSA is implemented and *only* used for encryption/decryption.

AES (Cert. nnn; non-compliant)
In this example, AES is implemented, has an algorithm certificate, but the KAT was not implemented and fails the FIPS 140-2 requirements.

AS.07.19 requires that the wrapping key used in key transport be equal or of greater strength than the wrapped key. If the strength of the largest key that can be established by a cryptographic module is greater than the comparable strength of the implemented key establishment method, then the module certificate and security policy shall be annotated with, in addition to the other required caveats, the caveat "**(key establishment methodology provides xx bits of encryption strength)**" for that key establishment method as allowed in IG 7.5 – *Strength of Key Establishment Methods*.

If the module supports, for a particular key establishment method, a single strength, then the caveat shall state the strength provided by the keys.

[6] Key Agreement Scheme

Examples: **Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength)**

RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength)

Triple-DES (Cert. #114, key wrapping; key establishment methodology provides 80 bits of encryption strength)

AES (Cert. #300, key wrapping; key establishment methodology provides 192 bits of encryption strength)

If a module *only* implements the 1024-bit and 2048-bit Diffie-Hellman then:

Diffie-Hellman (key agreement; key establishment methodology provides 80 or 112 bits of encryption strength)

If a module implements several key sizes between 1024-bit and 15,360-bit Diffie-Hellman, then only the range end points are indicated:

Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength)

If a module implements several key sizes between 1024-bit and 15,360-bit Diffie-Hellman, and also less than 80-bits of strength, then only the range end points are indicated and a caveat regarding the strength less than 80-bits:

Diffie-Hellman (key agreement; key establishment methodology provides between 80 and 256 bits of encryption strength; non-compliant less than 80-bits of encryption strength)

If a module implements only a key size less than 80-bits of strength (for example 56-bits), then only the caveat regarding the non-compliant strength less than 80-bits is provided:

Diffie-Hellman (non-compliant key agreement; key establishment methodology provides 56 bits of encryption strength)

If AES MAC is implemented for OTAR, it shall be specified as:

AES MAC (AES Cert. #2, vendor affirmed; P25 AES OTAR)

If AES MAC is implemented and not used for OTAR, it shall be specified as:

AES MAC (AES Cert. #2; non-compliant)

Note: In all cases, the CMVP report reviewer must ascertain the correctness of the added caveat(s) and the most accurate wording and the best interpretation to give to the Federal users.

If this field is not applicable, mark the field as N/A.

For non-Approved algorithms that have names similar to Approved security functions, the caveat "(non-compliant)" must be appended to alleviate misinterpretation.

Example: **AES (non-compliant)**
In this example, AES stands for Accelerated Encryption Software

16. ***Overall Level Achieved*: [n]** – the overall level of the crypto module. This value is the *lowest* value of the individual levels.

Additional Comments

Section 1 - Cryptographic Module Specification

1.1 Cryptographic Module Name

Applicable Levels:	*All*
Original Publishing Date:	*02/27/2004*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.05, AS01.08 and AS01.09*
Relevant Test Requirements:	*TE01.08.03,04 and 05 and TE01.09.01 and 02*
Relevant Vendor Requirements:	*VE01.08.03 and VE01.09.01*

Question/Problem

How shall the name of a cryptographic module relate to the defined cryptographic boundary?

Resolution

The provided name of the cryptographic module (which will be on the validation certificate) shall be consistent with the defined cryptographic boundary as defined in the test report.

It is not acceptable to provide a module name that represents a module that has more components than the modules defined boundary. If it is desired to have a name that does represent a larger entity, then the cryptographic boundary must be consistent. All components residing within the cryptographic boundary must either be included (**AS.01.08**) or excluded (**AS.01.09**) in the test report.

Additional Comments

Example: The provided name of a cryptographic module is the *Crypto Card*. However, the defined cryptographic boundary in the test report is a small black encapsulated component placed in one corner of the card. The named card also has additional components that were not referenced (e.g. batteries, connectors). If the defined boundary in the test report specifies *ONLY* the black encapsulated component, it is clearly NOT the *Crypto Card*. A unique different name shall be provided to be consistent with the defined boundary. To represent the entire card, the boundary must be redefined and must include all the components and address them properly (include/exclude).

1.2 FIPS Approved Mode of Operation

Applicable Levels:	*All*
Original Publishing Date:	*03/15/2004*
Effective Date:	
Last Modified Date:	*09/12/2005*
Relevant Assertions:	*AS01.02, AS01.03 and AS01.04*
Relevant Test Requirements:	*TE01.03.01-02 and TE01.04.01-12*
Relevant Vendor Requirements:	*VE01.03.01-02 and VE01.04.01-02*

Definition

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

Question/Problem

Are there any operational requirements when switching between modes of operation, either from an Approved mode of operation to a non-Approved mode of operation, or vice versa?

Resolution

In addition to the requirements specified in AS01.02, AS.01.03 and AS.01.04, a module shall not share CSPs between an Approved mode of operation and a non-Approved mode of operation.

Additional Comments

This separation mitigates the risk of untrusted handling of CSPs generated in an Approved mode of operation. Examples:

- a module may not generate keys in a non-Approved mode of operation and then switch to an Approved mode of operation and use the generated keys for Approved services. The keys may have been generated using non-Approved methods and their integrity and protection cannot be assured.
- a module shall not electronically import keys in plain text in a non-Approved mode of operation and then switch to an Approved mode of operation and use those keys for Approved services.
- a module may not generate keys in an Approved mode of operation and then switch to a non-Approved mode of operation and use the generated keys for non-Approved services. The integrity and the protection of the Approved keys cannot be assured in the non-Approved mode of operation.

1.3 Firmware Designation

Applicable Levels:	*All*
Original Publishing Date:	*04/28/2004*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.01*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

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

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

The *operational environment* of a cryptographic module refers to the management of the software, firmware, and/or hardware components required for the module to operate. The operational environment can be non-modifiable (e.g., firmware contained in ROM, or software contained in a computer with I/O devices disabled), or modifiable (e.g., firmware contained in RAM or software executed by a general purpose computer).

A *limited operational environment* refers to a static non-modifiable virtual operational environment (e.g., JAVA virtual machine on a non-programmable PC card) with no underlying general purpose operating system upon which the operational environment uniquely resides.

If the operational environment is a limited operational environment, the operating system requirements in Section 4.6.1 do not apply.

Question/Problem

How shall a *software* cryptographic module running on a limited operational environment be designated as?

Resolution

If the Operational Environment is a limited operational environment, and is indicated as NA on the certificate, then the cryptographic module shall be designated as a ***firmware*** module.

Additional Notes

- The reference tested OS must be indicated on the validation certificate for all software and firmware cryptographic modules. It will be referenced on the CMVP validation list web page as follows:
  - If the Operational Environment is applicable: -*Operational Environment: Tested as meeting Level x with ...*
  - If the Operational Environment is NA: -*Tested: ...*
- For a Level 2 module, the reference hardware platform used during operational testing must also be listed.
- For JAVA applets, the tested JAVA environment (JRE, JVM) and operating system need to be specified for all Security Levels.

Per FIPS 140-2 IG G.5, porting of software modules is only applicable to modules operating on a General Purpose Computer (GPC) and when the Operational Environment is applicable. The module's validation will be maintained if no changes are made to underlying source code.

If the operational environment is not applicable, a firmware module and its identified tested OS together may be ported from one platform to another platform while maintaining the module's validation For firmware module's that are JAVA applets, the firmware module, its identified tested OS, and the tested JAVA environment (JRE, JVM) must be moved together when porting from one platform to another platform in order to maintain the module's validation.

All other cases, the validation of the cryptographic module is not maintained.

1.4 Binding of Cryptographic Algorithm Validation Certificates

Applicable Levels:	*All*
Original Publishing Date:	*01/21/2005*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE01.12.01*

Background

Cryptographic algorithm implementations are tested and validated under the Cryptographic Algorithm Validation Program (CAVP). The cryptographic algorithm validation certificate states the name and version

number of the validated implementation, and the tested operational environment.

Cryptographic modules are tested and validated under the Cryptographic Module Validation Program (CMVP). The cryptographic module validation certificate states the name and version number of the validated cryptographic module, and the tested operational environment.

The validation certificate serves as a benchmark for the configuration and operational environment used during the validation testing.

Question/Problem

What are the configuration control and operational environment requirements for the cryptographic algorithm implementation(s) embedded within a cryptographic module when the latter is undergoing testing for compliance to FIPS 140-2?

Resolution

For a validated cryptographic algorithm implementation to be embedded within a software, firmware or hardware cryptographic module that undergoes testing for compliance to FIPS 140-2, the following requirements must be met:

1. the implementation of the validated cryptographic algorithm has not been modified upon integration into the cryptographic module undergoing testing; and

2. the operational environment under which the validated cryptographic algorithm implementation was tested by CAVS must be identical to the operational environment that the cryptographic module is being tested under by the CMT laboratory.

Additional Comments

1.5 Validation Testing of SHS Algorithms and Higher Cryptographic Algorithm Using SHS Algorithms

Applicable Levels:	*All*
Original Publishing Date:	*08/19/2004*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE01.12.01*

Background

The Cryptographic Algorithm Validation Program (CAVP) validates every SHS algorithm implementation: SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512. Several higher cryptographic algorithms use those SHS hashing algorithms in their operation.

Question/Problem

What are validation testing requirements for the SHS algorithms and higher cryptographic algorithms implementing SHS algorithms for their use in FIPS Approved mode of operation?

Resolution

To be used in a FIPS Approved mode of operation:

- every SHS algorithm implementation must be tested and validated on the appropriate OS.
- for DSA, RSA, ECDSA and HMAC, every implemented combination must be tested and validated on the appropriate OS.

The algorithmic validation certificate annotates all the tested implementations that may be used in a FIPS Approved mode of operation.

Any algorithm implementation incorporated within a FIPS 140-2 cryptographic module that is not tested may not be used in a FIPS Approved mode of operation. If there is an untested subset of a FIPS Approved algorithm, it would be listed as non-Approved and non-compliant on the FIPS 140-2 validation certificate.

Additional Comments

1.6 Use of Non-NIST-Recommended Asymmetric Key Sizes and Elliptic Curves

Applicable Levels:	*All*
Original Publishing Date:	*09/12/2005*
Effective Date:	
Last Modified Date:	*02/26/2007*
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE01.12.01*

Background

The Cryptographic Algorithm Validation Program (CAVP) validates implementations of DSA, RSA and ECDSA but only for the NIST-Recommended asymmetric key sizes and elliptic curves. The algorithm standards allow the use of other non-NIST-Recommended key sizes and curves. The Cryptographic Algorithm Validation System (CAVS) provided by the CAVP to the Cryptographic Module Testing (CMT) Laboratories does not test for all the possible key sizes and curves that a module may implement.

Question/Problem

Does the CMVP allow the use of non-NIST-Recommended DSA and RSA key sizes and ECDSA curves in a FIPS Approved mode of operation? If so, what are the requirements for those to be used in FIPS mode?

Resolution

The CMVP allows the use of non-NIST-Recommended DSA and RSA key sizes and ECDSA curves in a FIPS Approved mode of operation providing:

- an algorithm implementation must have been tested and validated for at least one NIST-Recommended key size (DSA and RSA) and one NIST-Recommended curve (ECDSA) as applicable,
- the security policy must list all non-NIST-Recommended curves and associated key strengths that are implemented, and,

– the algorithm implementation MUST use an Approved message digest algorithms.

Additional Comments

All NIST-recommended curves, key and modulus sizes must be tested to be used in a FIPS Approved mode of operation.

For NIST-Recommended elliptic curves, the value of f is commonly considered to be the size of the private key (Table 2, NIST SP 800-57). From this value the strength can be determined.

Refer to IG 1.4 *Use of Cryptographic Algorithm Validation Certificates* for guidance on operational environment requirements.

This guidance *may* be affected by the approval of FIPS 186-3 and the release of NIST Draft Special Publication 800-56 – *Recommendation for Key Establishment Schemes Using Discrete Logarithm Cryptography* and if so, would be replaced by the requirements stated in those documents.

1.7 Multiple *Approved* Modes of Operation

Applicable Levels:	*All*
Original Publishing Date:	*09/12/2005*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.03 and AS01.04*
Relevant Test Requirements:	*TE01.03.01-02 and TE01.04.01-02*
Relevant Vendor Requirements:	*VE01.03.01-02 and VE01.04.01-02*

Background

Section 4.1 of FIPS PUB 140-2 does not preclude a vendor from implementing more than one Approved mode of operation in a cryptographic module. An example of multiple Approved modes of operation may be a module where all modes may not have the same set of services.

Question/Problem

May a module implement more than one Approved mode of operation? What are the requirements for a module to implement more than one Approved mode of operation?

Resolution

A cryptographic module may be designed to support multiple Approved modes of operation.

For a cryptographic module to implement more than one Approved mode of operation, the following shall apply:

- the overall security level can not be changed when configured for different Approved modes of operation;
- the security policy shall describe each Approved mode of operation implemented in the cryptographic module and how each one is configured;
- upon re-configuration from one Approved mode of operation to another, the cryptographic module shall reinitialize and perform a power on self-test;

- power on self-tests shall be performed for all Approved security functions used in the selected Approved mode of operation; and

- if re-configuration changes the physical security level of the module, upon re-configuration the cryptographic module shall perform a zeroization of all CSPs within the module.

To confirm the correct operation of the several modes of operation, the tester shall:

- verify the documentation describing each Approved mode of operation;

- use the vendor provided instructions described in the non-proprietary security policy to invoke each Approved mode of operation;

- verify that, for each Approved mode of operation, only the security functions implemented for that mode are accessible and that security functions not implemented for that mode are not;

- verify that the aforementioned requirements are met for each Approved mode of operation;

- verify that the requirements of AS.01.03 and/or AS.01.04 are met for each Approved mode of operation; and

- verify that CSPs are not shared between the multiple Approved modes of operation.

Additional Comments

1.8 Listing of DES Implementations

Applicable Levels:	*All*
Original Publishing Date:	*11/23/2005*
Effective Date:	*05/19/2007*
Last Modified Date:	*01/16/2008*
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE01.12.01*

Background

DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
[Docket No. 040602169-5002-02]

Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation.

Question/Problem

With the withdrawal of the DES cryptographic algorithm, how does the DES and DES MAC algorithms get listed on the FIPS 140-2 validation certificate?

Resolution

The DES transition period ended on May 19, 2007. DES and DES MAC are no longer Approved security functions and shall be listed on the FIPS 140-2 certificate as non-Approved algorithms.

Additional Comments

1.9 Definition and Requirements of an Hybrid Cryptographic Module

Applicable Levels:	*Level 1*
Original Publishing Date:	*10/05/2006*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.01 and AS01.08*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

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

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

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

Question/Problem

Define what a ***hybrid*** cryptographic module is and specify the requirements applicable to this module type?

Resolution

A ***hybrid*** cryptographic module is a special type of software cryptographic module that, as part of its operation, utilizes special purpose hardware[7] and, if applicable, firmware components, installed within the physical boundary of the GPC.

In addition to the requirements applicable to a software cryptographic module, the following requirements are also applicable to the additional hardware and, if applicable, firmware components of the ***hybrid*** cryptographic module:

- Cryptographic Module Specification: All the components of the ***hybrid*** cryptographic module must be fully specified by type, part numbers and version numbers;
    - Manufacturer and model of the special purpose hardware component(s) and platform(s) on which testing was performed;
    - Operating system(s) on which testing was performed; and

[7] e.g. installed hardware accelerator cards, cryptographic hardware chips, unique firmware either incorporated within the special purpose hardware or as a compliment to the GPC base platform, etc.

- All additional special purpose hardware and firmware components

- Cryptographic Module Ports and Interfaces: By policy, all inputs and outputs of the hybrid cryptographic module must be directed through the software component;

- Roles, Services and Authentication: All the services and sub-services provided by each component of the ***hybrid*** cryptographic module must be specified;

- Physical Security: Section 5 – Physical Security is applicable for a ***hybrid*** module.
  - The module is not completely implemented as software; therefore this section is not optional.

- Cryptographic Key Management: Key exchanged within the boundary of the GPC and between two or more components of the ***hybrid*** cryptographic module may be transferred in plaintext;

- Self-Tests: Self-tests requirements are applicable to all components of the ***hybrid*** cryptographic module;
  - A strong integrity test shall be performed on the software component,
  - A firmware integrity test (AS09.22) shall be performed on any applicable special purpose firmware component, and
  - All other applicable power-up or conditional tests are applicable to all components as required.

- Security Policy: The security policy must specify all the components of the ***hybrid*** cryptographic module by type, part numbers and version numbers. The security policy must contain a picture of the hardware components of the module. The security policy must specify all the services and sub-services provided by each component of the ***hybrid*** cryptographic module.

- Operational Environment: Section 6 – The operating system requirements are applicable for a ***hybrid*** module.
  - The module is a software module; therefore this section is not optional.

Additional Comments

Hybrid cryptographic modules shall be only applicable at FIPS 140-2 Level 1.

The hybrid cryptographic module may be ported to other compatible GPCs per IG G.5.

Changes to *any* components of the ***hybrid*** cryptographic module require the re-validation of the complete module as per IG G.8 – *Revalidation Requirements*.

The firmware and hardware components of the ***hybrid*** module are considered an extension of the software component to perform or accelerate cryptographic operations. In a ***hybrid*** module, the firmware and hardware components can only exchange data and CSPs with the controlling software component of the module.

1.10 Vendor Affirmation of Cryptographic Security Methods

Applicable Levels:	*All*

Original Publishing Date:	*01/25/2007*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE01.12.01*

Background

A cryptographic module shall implement at least one Approved security function used in an Approved mode of operation. Non-Approved security functions may also be included for use in non-Approved modes of operation or allowed for use in an Approved mode of operation. Documentation shall list all security functions, both Approved and non-Approved, that are employed by the cryptographic module and shall specify all modes of operation, both Approved and non-Approved. The vendor shall provide a validation certificate for all Approved cryptographic algorithms. The tester shall verify that the vendor has provided validated certificate(s) as described above.

Questions/Problems

For Approved security functions, Approved random number generators or Approved key establishment techniques specified in FIPS 140-2 Annexes A, C, and D, if CAVP testing is not available, can the Approved methods be used in FIPS mode, and if so, how shall it be tested and annotated on the module validation certificate and security policy?

Resolution

As new methods are published and Approved, they will be added to the relevant FIPS 140-2 Annexes. The annexes may reference FIPS 140-2 Implementation Guidance for methods *allowed* in lieu of Approved methods.

1. If a new Approved methods (e.g. NIST FIPS, Special Publication, etc) are added to the Annexes which provides a new method that did not exist before (e.g. key establishment), until such time that CAVP testing is available for the new method, the CMVP would continue to:

   – allow methods as provided by guidance (untested and listed as non-Approved but *allowed* in FIPS mode); and
   – allow the vendor to implement the new Approved method (untested, listed as Approved and allowed in FIPS mode with the caveat *vendor affirmed*).

   Once testing is deployed by the CAVP to the testing laboratories:

   a. a transition period (e.g. n months) would be provided for new test reports received by the CMVP:

      - during the transition period, a new Approved method would either be listed as Approved with a reference to a CAVP validation certificate, or as *vendor affirmed* if testing was not performed; and
      - allow continued implementation of methods as provided by guidance (untested and listed as non-Approved but *allowed* in FIPS mode).

   b. when the transition period ends, for newly received test reports:

      - only Approved methods that have been tested and received a CAVP validation certificate would be allowed. All other methods would be listed as non-Approved and not allowed in an Approved FIPS mode of operation.

c. the vendor could optionally follow up with testing of un-tested vendor affirmed methods and if so, the reference to *vendor affirmed* would be removed and replaced by reference to the algorithm certificate. If there are no changes to the module, this change can be submitted under FIPS 140-2 IG G.8 Scenario 1[8]. If the module is changed, this change can be submitted under FIPS 140-2 IG G.8 Scenarios 1, 3 or 5 as applicable [2].

2. If a new Approved methods (e.g. NIST FIPS, Special Publication, etc) are added to Annexes which provides a new method commensurate with those that currently exist (e.g. an new symmetric key algorithm, RNG, hash, digital signature, etc), until such time that CAVP testing is available for the new method, the CMVP would:

   – allow prior Approved methods (tested and listed as Approved); and
   – allow the vendor to implement the new Approved method (untested, listed as Approved and allowed in FIPS mode with the caveat *vendor affirmed*)

   Once testing is deployed by the CAVP to the testing laboratories:

   a. a transition period (e.g. n months) would be provided for new test reports received by the CMVP:

      - during the transition period, a new Approved method would either be listed as Approved with a reference to a CAVP validation certificate, or as *vendor affirmed* if testing was not performed.

   b. when the transition period ends, for newly received test reports:

      - only Approved methods that have been tested and received a CAVP validation certificate would be allowed. All other methods would be listed as non-Approved and not allowed in an Approved FIPS mode of operation.

   c. the vendor could optionally follow up with testing of prior un-tested vendor affirmed methods and if so, the reference to *vendor affirmed* removed and replaced by reference to the algorithm certificate. If there are no changes to the module, this change can be submitted under FIPS 140-2 IG G.8 Scenario 1[1]. If the module is changed, this change can be submitted under FIPS 140-2 IG G.8 Scenarios 1, 3 or 5 as applicable [9].

3. The Security Technology Group at NIST may determine that prior methods may be retroactively disallowed and moved to non-Approved and not allowed in a FIPS mode of operation (e.g. DES). A Federal Register notice would be published with a transition period to allow migration from the no longer Approved or allowed method.

4. For all Approved methods, all applicable FIPS 140-2 requirements shall be met (e.g., key management, self-tests, etc.)

Additional Comments

***Vendor Affirmed*:** a security method reference that is listed with this caveat has not been tested by the CAVP, and the CMVP or CAVP provide no assurance regarding its correct implementation or operation. Only the vendor of the module affirms that the method or algorithm was implemented correctly.

[8] This is a special case where FIPS 140-2 IG G.8 Scenario 2 would not apply.
[9] If the change is security relevant either to the module or the method, then FIPS 140-2 IG Scenarios 3 or 5 would be applicable depending on the extent of the changes. If for example there was a non-security relevant change to the module not associated with the security method implementation, FIPS 140-2 Scenario 1 could be applicable.

The users of cryptographic modules implementing vendor affirmed security functions must consider the risks associated with the use of un-tested and un-validated security functions.

Test Requirements

Until the FIPS 140-2 DTR and Cryptik tool are updated and released, please provide the following information under VE and TE 01.12.01.

Required Vendor Information

VE01.12.03: The vendor shall provide a list of all vendor affirmed security methods.

VE01.12.04: The vendor provided nonproprietary security policy shall include reference to all vendor affirmed security methods.

Required Test Procedures

TE01.12.03: The tester shall verify that the vendor has provided the list of vendor affirmed security methods as described above.

TE01.12.04: The tester shall verify that the vendor provided documentation specifies how the implemented vendor affirmed security methods conform to the relevant standards.

Required Use of "Vendor Affirmed" Caveat

All cryptographic methods that are Approved and *vendor affirmed* shall be specified on the certificate and in the security policy, and be annotated with, in addition to the other required caveats as applicable, the caveat (vendor affirmed: *FIPS or NIST Special Publication #*).

Caveat Annotation Examples

The only Approved RNG implemented is vendor affirmed:
RNG (vendor affirmed: SP 800-90)

Multiple Approved RNGs are implemented, both tested and vendor affirmed:
RNG (Cert.# nnn and vendor affirmed: SP 800-90)

Key Establishment Schemes:
KES (vendor affirmed: SP 800-56A)

1.11 CAVP Requirements for Vendor Affirmation of NIST SP 800-56A

Applicable Levels:	*All*
Original Publishing Date:	*06/21/2007*
Effective Date:	
Transition End Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE01.12.01*

Background

NIST Special Publication 800-56A was added to FIPS 140-2 Annex D on January 24, 2007. FIPS 140-2 Implementation Guidance, IG 1.10, was added January 25, 2007. Until CAVP testing for NIST SP 800-56A is available, IG 1.10 is applicable. NIST SP 800-56A includes information beyond the specifications of the key agreement algorithm itself; i.e. Instructions to the implementer to aid in the implementation of the algorithm.

Question/Problem

To claim *vendor affirmation* to NIST SP 800-56A, what sections of the publication need to be addressed?

Resolution

Validation testing for NIST SP 800-56A, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* includes validation testing for the key agreement schemes and key confirmation. To claim *vendor affirmation* to SP 800-56A, information contained in the following sections that are supported by the implementation under test (IUT) shall be implemented:

Section 5.6.2.4	FFC Full Public Key Validation Routine (if implement FFC)
Section 5.6.2.5	ECC Full Public Key Validation Routine (if implement ECC)
Section 5.7	DLC Primitives
Section 5.8	Key Derivation Functions for Key Agreement Schemes
Section 6	Key Agreement

If key confirmation is supported by the implementation, the applicable information contained in the following section must be implemented:

Section 8	Key Confirmation

Additional Comments

1. The components in SP 800-56A shall only be used within the SP 800-56A protocol. This includes the full public key validation routines, the DLC primitives, the key derivation functions, the key agreement functions, and the key confirmation functions.
2. The requirements specified in NIST SP 800-56A depend on several NIST Approved security functions, for example, SHA, DSA, ECDSA, etc. While validation testing for NIST SP 800-56A concentrates on the key agreement and key confirmation components, other supporting security functions are not thoroughly tested by the testing in NIST SP 800-56A. The validation testing for these supporting security functions are found in the validation test suite for this specific function. Therefore, these supporting security functions shall be validated as a prerequisite to NIST SP 800-56A vendor affirmation.

   To claim vendor affirmation to NIST SP 800-56A, the underlying security functions used by this IUT shall be tested and validated prior to claiming vendor affirmation. These include:

   - Supported hash algorithms (SHA1, SHA224, SHA256, SHA384, and/or SHA512)
   - Supported Message Authentication Code (MAC) algorithms (CMAC, CCM, and/or HMAC)
   - Supported Random Number Generators (RNG)
   - If Finite Field Cryptography (FFC) is supported,
     - If the IUT generates domain parameters the DSA PQG generation and/or verification tests.
     - If the IUT generates key pairs, the DSA key pair generation tests.
   - If Elliptic Curve Cryptography (ECC) is supported,
     - If the IUT generates key pairs, the ECDSA key pair generation test and/or the Public Key Validation (PKV) test.

3. The SP 800-56 self tests required in cryptographic module implementations must consist of a known answer test that validates the correctness of the implemented DLC primitives and key derivation functions for each key agreement scheme implemented.

Derived Test Requirements

Required Vendor Information

The vendor shall provide evidence that their implementation implements the sections outlined above completely and accurately. This shall be accomplished by documentation and code review.

Required Test Procedures

The tester shall review the vendor's evidence demonstrating that their implementation conforms to the specifications specified above. This shall be accomplished by documentation and code review. The tester shall verify the rationale provided by the vendor.

1.12 CAVP Requirements for Vendor Affirmation of NIST SP 800-90

Applicable Levels:	*All*
Original Publishing Date:	*06/21/2007*
Effective Date:	
Transition End Date:	*02/15/2008*
Last Modified Date:	
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE01.12.01*

Background

NIST Special Publication 800-90 was added to FIPS 140-2 Annex C on January 24, 2007. FIPS 140-2 Implementation Guidance, IG 1.10, was added January 25, 2007. Until CAVP testing for NIST SP 800-90 is available, IG 1.10 is applicable. NIST SP 800-90 includes information beyond the specifications of the deterministic random bit generation (DRBG) algorithms themselves, e.g., stricter entropy requirements, and assurance.

Question/Problem

To claim *vendor affirmation* to NIST SP 800-90, what sections of the publication need to be addressed?

Resolution

To claim *vendor affirmation*, the vendor shall affirm compliance with the following three sections of NIST SP 800-90, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators*:

Section 9 DRBG Mechanism Functions
Section 10 DRBG Algorithm Specifications
Section 11 Assurance

The vendor is not required to meet the requirements in Section 8, including the entropy requirements in Section 8.6. Entropy requirements are addressed in FIPS 140-2 DTR AS.07.13.

Additional Comments

The requirements of NIST SP 800-90 depend on several NIST Approved security functions, for example, SHA, AES, and three-key Triple-DES. The validation testing for these supporting security functions is found in their corresponding validation test suites and, therefore, they shall be validated as a prerequisite to NIST SP 800-90 vendor affirmation.

To claim vendor affirmation to NIST SP 800-90, the following supporting security functions, if used, shall be tested and validated:

- Supported hash algorithms (SHA224, SHA256, SHA384, and/or SHA512)
- Supported Message Authentication Code (MAC) algorithm (HMAC)
- Advanced Encryption Standard (AES)
- Three key Triple-DES

Derived Test Requirements

Required Vendor Information

The vendor shall provide evidence that their implementation implements the sections outlined above completely and accurately. This shall be accomplished by documentation and code review.

Required Test Procedures

The tester shall review the vendor's evidence demonstrating that their implementation conforms to the specifications specified above. This shall be accomplished by documentation and code review. The tester shall verify the rationale provided by the vendor.

1.13 CAVP Requirements for Vendor Affirmation of NIST SP 800-38D

Applicable Levels:	*All*
Original Publishing Date:	*12/18/2007*
Effective Date:	
Transition End Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.12*
Relevant Test Requirements:	*TE01.12.01*
Relevant Vendor Requirements:	*VE01.12.01*

Background

NIST SP 800-38D was added to FIPS 140-2 Annex A on December 18, 2007. FIPS 140-2 Implementation Guidance, IG 1.10 was added January 25, 2007. Until CAVP testing for NIST SP 800-38D is available, IG 1.10 is applicable. NIST SP 800-38D includes information beyond the specifications of the Galois/Counter Mode itself; i.e., uniqueness requirements on IVs and keys.

Question/Problem

To claim *vendor affirmation* to NIST SP 800-38D, what sections of the standard need to be addressed?

Resolution

Validation testing for NIST SP 800-38D, *Recommendation for Block cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC* includes validation testing for the authenticated encryption function and the authenticated decryption function.. To claim *vendor affirmation* to SP 800-38D, information contained in the following sections that are supported by the implementation under test (IUT) shall be implemented:

Section 5	Elements of GCM
Section 6	Mathematical Components of GCM
Section 7	GCM Specifications

Additional Comments

1. The GCM functions in NIST SP 800-38D require the forward direction of an approved symmetric key block cipher with a block size of 128 bits. Currently, the only NIST-approved 128-bit block cipher is the Advanced Encryption Standard (AES) algorithm specified in Federal Information Processing Standard (FIPS) Pub. 197. The validation testing for the forward direction of this supporting algorithm, the AES Cipher (Encrypt) function, is found in its corresponding validation test suite and, therefore, shall be validated as a prerequisite to NIST SP 800-38D vendor affirmation.

2. The SP800-38D Self Tests required in cryptographic module implementations shall consist of a known answer that validates the correctness of the GCM elements, GCM mathematical components and GCM specifications of the two GCM functions, namely, the authenticated encryption function and the authenticated decryption function.

3. Section 8, *Uniqueness Requirement on IVs and Keys*, and Section 9, *Practical Considerations for Validating Implementations*, contain requirements for module validation, which is conducted by the CMVP. Therefore, Section 8 and Section 9 are outside of the scope of algorithm validation.

Derived Test Requirements

Required Vendor Information

The vendor shall provide evidence that their implementation implements the sections outlined above completely and accurately. This shall be accomplished by documentation and code review.

Required Test Procedures

The tester shall review the vendor's evidence demonstrating that their implementation conforms to the specifications specified above. This shall be accomplished by documentation and code review. The tester shall verify the rationale provided by the vendor.

Section 2 – Cryptographic Module Ports and Interfaces

Section 3 – Roles, Services, and Authentication

3.1 Authorized Roles

Applicable Levels:	*All*
Original Publishing Date:	*05/29/2002*
Effective Date:	
Last Modified Date:	*06/14/2007*
Relevant Assertions:	
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

An operator is not required to assume an authorized role to perform services where cryptographic keys and CSPs are not modified, disclosed, or substituted (e.g., show status, self-tests, or other services that do not affect the security of the module).

Authentication mechanisms may be required within a cryptographic module to authenticate an operator accessing the module, and to verify that the operator is authorized to assume the requested role and perform the services within the role.

Resolution

An operator shall assume an authorized role for all services utilizing Approved security functions with the following exceptions if cryptographic keys and CSPs are not created, modified, disclosed, or substituted:

- The Secure Hash Algorithms (SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512) which are specified in *Secure Hash Standard*, FIPS 180-2 with Change Notice 1 dated February 25, 2004;
- The deterministic Random Number Generators which are specified in National Institute of Standards and Technology, *Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised)*, NIST Special Publication 800-90, March 2007. If the RNG service is provided to an operator who is not required to assume an authorized role, the entropy source and seeding of the RNG shall be completely contained within the boundary of the cryptographic module and not subject to manipulation by any operator or service of the module;
- Processes used for authentication (e.g., symmetric algorithm secret sharing, asymmetric algorithms for authentication). The completion of the authentication mechanism shall be enforced (e.g., the module will cease to function, even after power up) until the authentication is completed before any generalized authenticated role for any services utilizing Approved security functions is allowed; and
- Show status, self-tests, zeroization or other services that do not affect the security of the module.

Additional Comments

Section 4 - Finite State Model

Section 5 - Physical Security

5.1 Opacity and Probing of Cryptographic Modules with Fans, Ventilation Holes or Slits at Level 2

Applicable Levels:	*Level 2*
Original Publishing Date:	*02/10/2004*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS05.49*
Relevant Test Requirements:	*TE05.49.01*
Relevant Vendor Requirements:	*VE05.49.01*

Background

Cryptographic modules typically require the use of heat dissipation techniques that can include the use of fans, ventilation holes or slits. The size of these openings in the modules' enclosure, or the spacing between fan blades, may allow the viewing or possible probing of internal components and structures within the cryptographic module.

Question/Problem

How do the opacity requirements of FIPS 140-2 affect the design of the heat dissipation techniques on those cryptographic modules at Security Level 2? Should the cryptographic module prevent probing through the ventilation holes or slits at Security Level 2?

Resolution

The following are the physical security requirements for multi-chip stand-alone module at Security Level 2 pertaining to opacity and probing:

- the embodiments that are entirely contained within a metal or hard plastic production-grade enclosure that may include doors or removable covers (Security Level 1 requirement); and
- the enclosure of the cryptographic module shall be opaque within the visible spectrum.

Probing Requirements

Probing is not addressed at Security Level 2. Probing through ventilation holes or slits is addressed at Security Level 3 (AS.05.21).

Opacity Requirements

The purpose of the opacity requirement is to deter direct observation of the cryptographic module's internal components and design information to prevent a determination of the composition or implementation of the module.

A module is considered "opaque" only if it cannot be determined by visual inspection within the visible spectrum using artificial light sources shining through the enclosure openings or translucent surfaces, the manufacturer and/or model numbers of internal components (such as specific IC types) and/or design and composition information (such as wire traces and interconnections).

Component outlines may be visible from the enclosure openings or translucent surfaces as long as the component's manufacturer and/or model numbers, and/or composition and information about the module's design cannot be determined.

All components within the boundary of the cryptographic module must meet the opacity requirements of the standard. Excluded non-security relevant components do not have to meet these requirements.

Additional Comments

Note: Visible light is defined as light within a wavelength range of 400nm to 750nm.

5.2 Testing Tamper Evident Seals

Applicable Levels:	*Levels 2, 3 and 4*
Original Publishing Date:	*09/12/2005*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS.05.16, AS.05.35, AS.05.36, AS.05.37, AS.05.48, AS.05.50*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

What level of testing and scope of testing should be applied when testing tamper evident seals?

Resolution

If a module uses tamper evident labels, it shall not be possible to remove or reapply a label without tamper evidence. For example, if the label can be removed without tamper evidence, and the same label can be re-applied without tamper evidence, the assertion fails.

Conversely, if any attempt to remove the label leaves evidence, or removal and re-application leaves evidence, or the label is destroyed during removal, the assertion passes. This means that the CMT lab shall have to use creative ways (e.g. chemically, mechanically, thermally) to remove a label without evidence and without destroying the original label, and be able to re-apply the removed label in a manner that does not leave evidence.

Additional Comments

It is out-of-scope for an attacker to introduce new materials to cover up evidence of the attack.

Section 6 – Operational Environment

6.1 Single Operator Mode and Concurrent Operators

Applicable Levels:	*All*
Original Publishing Date:	*03/10/2003*
Effective Date:	
Last Modified Date:	*04/24/2003*
Relevant Assertions:	*AS06.04*
Relevant Test Requirements:	*TE06.04*
Relevant Vendor Requirements:	*VE06.04*

Background

Historically, for a FIPS 140-1 and FIPS 140-2 validated software cryptographic module on a server to meet the single user requirement of Security Level 1, the server had to be configured so that only *one* user at a time could access the server. This meant configuring the server Operating System (OS) so that only a single user at a time could execute processes (including cryptographic processes) on the server. Consequently, servers were not being used as intended.

Question/Problem

AS06.04 states: "(Level 1 Only) The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded)". What is the definition of concurrent operators in this context? Specifically, may Level 1 software modules be implemented on a server and achieve FIPS 140-2 validation? (Note: this question is also applicable to VPN, firewalls, etc.)

Resolution

Software cryptographic modules implemented in client/server architecture are intended to be used on both the client and the server. The cryptographic module will be used to provide cryptographic functions to the client and server applications. When a crypto module is implemented in a server environment, the server application is the user of the cryptographic module. The server application makes the calls to the cryptographic module. Therefore, the server application is the single user of the cryptographic module, even when the server application is serving multiple clients

Additional Comments

This information must be included in the non-proprietary security policy.

6.2 Applicability of Operational Environment Requirements to JAVA Smart Cards

Applicable Levels:	*All*
Original Publishing Date:	*04/08/2003*
Effective Date:	
Last Modified Date:	*09/11/2003*
Relevant Assertions:	*AS06.01*

Relevant Test Requirements:	
Relevant Vendor Requirements:	

Background

FIPS 140-2 states (Section 4.6 Operational Environment) "A limited operational environment refers to a static non-modifiable virtual environment (e.g., a JAVA virtual machine on a non-programmable PC card) with no underlying general purpose operating system upon which the operational environment uniquely resides."

Question

Does the FIPS 140-2 statement mean that a smart card implementing a non-modifiable operating system (e.g., like the ones currently used today in most smart cards) that accept and run JAVA applets (whether validated or not) is a limited operational environment?

Resolution

The CMVP cannot issue a general statement that applies to all JAVA card modules since functionality and design can vary greatly from module to module. The determination is left to the CMT laboratories, which have the complete module documentation available to them. In general**,** however, a JAVA smart card module with the ability to load unvalidated applets post-validation is considered to have a ***modifiable*** operational environment and the Operational Environment requirements of FIPS 140-2 are applicable.

A JAVA smart card module having a modifiable operational environment which either:

a) is configured such that the loading of any applets is not possible, or

b) loads only applets that have been tested and validated to either FIPS 140-1 or FIPS 140-2,

could be considered to have a ***limited*** operational environment and have the FIPS 140-2 Operational Environment requirements section of the module test report marked as *Not Applicable*.

The validated JAVA smart card cryptographic module must use an Approved authentication technique on all loaded applets. The module shall also meet, at a minimum, the requirements of AS09.34, AS09.35, AS10.03 and AS10.04, as well as any other applicable assertions. Validation of the cryptographic module is maintained through the loading of applets that have either been tested and validated during the validation effort of the smart card itself or through an independent validation effort (i.e., the applet itself has its own validation certificate number).

The security policy of the validated smart card module must state whether:

- The module can load applets post-validation, validated or not (Note: if the module can load non-validated applets post-validation, the security policy must clearly indicate that the module's validation to FIPS 140-1 or FIPS 140-2 is no longer valid once a non-validated applet is loaded);

- Any applets are contained within the validated cryptographic module and, if so, must list their name(s) and version number(s).

Additional Comments

The name(s) and version number(s) of all applets contained within a validated cryptographic module shall be listed on the module's certificate and CMVP website entry.

6.3 Correction to Common Criteria Requirements on Operating System

Applicable Levels:	*All*
Original Publishing Date:	*03/29/2004*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS06.10, AS06.21 and AS06.27*
Relevant Test Requirements:	*TE06.10, TE06.21 and TE06.27*
Relevant Vendor Requirements:	*VE06.10, VE06.21 and VE06.27*

Background

Depending on how assertions AS.06.10, AS.06.21 and AS.06.27 are read, they could be interpreted as the OS upon which the module is running on has to meet ALL of the listed PPs in Annex B at EAL2, EAL3 and EAL4 respectively. This is because of the plural at the end of the "Protection Profile**s**".

Question/Problem

Must the OS upon which the module is running on has to meet ALL of the listed PPs in Annex B at EAL2, EAL3 and EAL4 respectively?

Resolution

No, the requirements should be interpreted to read as follows:

- For **AS.06.10**:

  an operating system that meets the functional requirements specified in **a** Protection Profile listed in Annex B and is evaluated at the CC evaluation assurance level EAL2

- For **AS.06.21**, the first sentence:

  an operating system that meets the functional requirements specified in **a** Protection Profile listed in Annex B.

- For **AS.06.27**, the first sentence:

  an operating system that meets the functional requirements specified in **a** Protection Profile listed in Annex B.

Additional Notes

6.4 Approved Integrity Techniques

Applicable Levels:	*All*
Original Publishing Date:	*01/21/2005*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS06.08*
Relevant Test Requirements:	*TE06.01.01-02*

Relevant Vendor Requirements:	*VE06.08.01*

Background

Section 4.6.1 of FIPS 140-2 states that "A cryptographic mechanism using an Approved integrity technique (e.g. Approved message authentication code or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the cryptographic module."

Question/Problem

What is an *Approved integrity technique*, as specified in AS06.08, and when must be it performed?

Resolution

An *Approved integrity technique* is a keyed cryptographic mechanism that uses an Approved and validated cryptographic security function. This includes a digital signature scheme, an HMAC or a MAC. Approved security functions are listed in FIPS 140-2 Annex A.

The Approved integrity technique is considered a *Power-Up Test* and shall meet all power-up test requirements.

Additional Comments

Section 7 – Cryptographic Key Management

7.1 Acceptable Key Establishment Protocols

Applicable Levels:	*All*
Original Publishing Date:	*02/10/2004*
Effective Date:	
Last Modified Date:	*02/07/2008*
Relevant Assertions:	*AS07.21*
Relevant Test Requirements:	*TE07.21.01*
Relevant Vendor Requirements:	*VE07.21.01-02*

Background

Cryptographic modules may use various symmetric and asymmetric key establishment schemes within protocols to establish and maintain secure communication links between modules. FIPS 140-2 Annex D provides a list of the Approved key establishment techniques for establishing keying material that are applicable to FIPS 140-2.

Question/Problem

FIPS 140-2 Annex D states that SP 800-56A provides approved asymmetric key establishment schemes to establish keying material. Annex D also states that additional symmetric and asymmetric key establishment schemes are allowed in a FIPS Approved mode of operation. What are these additional schemes?

Resolution

Key establishment is the process by which secret keying material is securely established between two or more entities. Keying material is data that is necessary to establish and maintain a cryptographic keying relationship[10]. Secret keying material includes keys, secret initialization vectors and other secret information. Symmetric and asymmetric key establishment may be accomplished using either key agreement or key transport schemes.

Key agreement is a method of key establishment where the resulting keying material is a function of information contributed by two or more participants, so that no party can predetermine the value of the secret keying material independently from the contribution of any other party. Key agreement is performed using key agreement schemes. At this time, NIST has specified key agreement schemes in SP 800-56A using Discrete Logarithm Cryptography (DLC). Key agreement schemes for Integer Factorization Cryptography (e.g., RSA) will be specified in a subsequent document. Each scheme in SP 800-56A consists of several elements:

- A primitive (i.e., an algorithm) that is used to generate a shared secret from the public and/or private keys of the initiator and responder in a key agreement transaction. The shared secret is an intermediate value that is used as input to a key derivation function.

[10] The state existing between two entities in which they share at least one cryptographic key.

- A key derivation function (KDF) that uses the shared secret and other information to derive keying material[11].
- An optional message authentication code (MAC) that is used for key confirmation or implementation validation. Key confirmation is a procedure that provides assurance to one party (the key confirmation recipient) that another party (the key confirmation provider) actually possesses the correct secret keying material and/or shared secret.
- The rules for using the scheme securely. The rules specified in SP 800-56A include criteria for generating the domain parameters and asymmetric key pairs used during key agreement, methods for obtaining the required assurances, and specifications for performing key confirmation.

Several of the currently used implementations of DLC key agreement schemes do not comply with all requirements of SP 800-56A. In many cases, the KDF used to generate the keying material from the shared secret is different than a KDF specified in SP 800-56A.

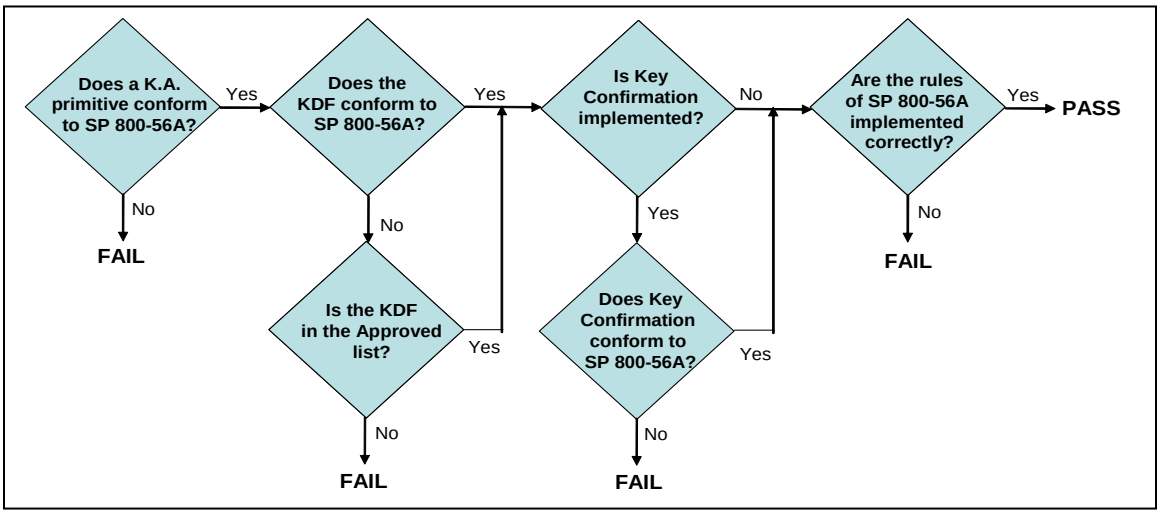


Figure 7.1-1: DLC Key Agreement Validation

Figure 7.1-1 depicts the DLC key agreement validation process. All implementations of DLC key agreement schemes to be submitted for FIPS 140-2 validation **shall** include:

1. One or more of the key agreement primitives specified in SP 800-56A. Domain parameters and key sizes **shall** conform to SP 800-56A.

2. KDFs **shall** conform to:

   - One of the KDFs in SP 800-56,
   - The KDF specified in IKEv2 (IETF RFC 4306), which is allowed only for the purpose of establishing keying material for security associations managed by IKEv2. The PRF used in IKEv2 **shall** employ the HMAC as specified in FIPS 198 (based on an Approved hash function).
   - Until December 31, 2010, **shall** conform to one of the following:

     a. One of the KDFs specified in American National Standard (ANS) X9.42-2001, *Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography*. An example of a protocol that uses ANS X9.42 is

[11] The keying material may be used directly (e.g., as a key), or the keying material may be used to derive (other) keys. The use of the keying material is outside the scope of SP 800-56A.

specified in RFC 2631, *Diffie-Hellman Key Agreement Method.* For the KDFs specified in ANS X9.42:

1) The *OtherInfo* field of the key derivation function **should** be defined and used as specified in SP 800-56.
2) The *counter* in the ASN.1 key derivation function **should** be represented as a 32-bit, big-endian bit string.

b. The KDFs specified in American National Standard (ANS) X9.63-2001, *Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography*. An example of a protocol that uses ANS X9.63 is specified in RFC 3278, *Use of Elliptic Curve Cryptography* (*ECC*) *Algorithms in Cryptographic Message Syntax* (*CMS*). For the KDFs specified in ANS X9.63, the *OtherInfo* field of the key derivation function **should** be defined and used as specified in SP 800-56.

c. The KDF specified in IKEv1 (IETF RFC 2409) is allowed only for the purpose of establishing keying material for security associations managed by IKEv1. The PRF used in IKEv1 **shall** employ the HMAC specified in FIPS 198 (based on an Approved hash function).

d. The KDF specified in SSH (IETF RFC 4253) is allowed only for the purpose of establishing SSH sessions, and

e. The KDF in TLS is allowed only for the purpose of establishing keying material (in particular, the *master secret*) for a TLS session with the following restrictions, even though the use of the SHA-1 and MD5 hash functions are not consistent with in Table 1 or Table 2 of SP 800-56A:

1) The use of MD5 is allowed in the TLS protocol only; MD5 **shall not** be used as a general hash function.

2) The maximum number of blocks of secret keying material that can be produced by repeated use of the pseudorandom function during a single call to the TLS key derivation function **shall** be 2^{32}-1.

3. If key confirmation is claimed for a key agreement scheme, one or more of the key confirmation methods in SP 800-56A **shall** be used.

4. An implementation **shall** conform to the key agreement rules specified in SP 800-56A, with the possible exception of the format of the KDF (see above).

Key transport is a method of key establishment whereby one party (the sender) selects a value for the secret keying material and then securely distributes that value to another party (the receiver). Key transport may be accomplished by:

- Wrapping the key using a secret symmetric key and a symmetric encryption algorithm. Key transport by wrapping a key obtained from DLC-based key agreement is addressed in SP 800-56A.
- In the absence of applicable standards, the CMVP will allow the wrapping of keys to be transported using the AES or the Triple DES symmetric key algorithms. The wrapping **shall** be performed in compliance with AES Key Wrap Specification (Draft), published by the National Institute of Standards and Technology on 16 November 2001. If the Triple DES is used, then it **shall** be used in exactly the same way that is defined for AES in the aforementioned draft standard. Both the 2-key and the 3-key Triple DES can be used for key wrapping.

  The symmetric key algorithm used for key wrapping **shall** be tested, even if the algorithm is not

otherwise used by the cryptographic module, and the algorithm's certificate number **shall** be shown on the module's certificate. The use of this algorithm for key wrapping **shall** be documented on the Non-Approved line of the cryptographic module's certificate. If the security strength of the key wrapping key and algorithm combination can be lower than that of the (potential) security strength of the wrapped key, then the resulting security strength of the wrapped key is the security strength of the key wrapping key and algorithm, and **should** be shown on the module's certificate in accordance with IG G.13.

- Encrypting the keying material using a public key and an asymmetric algorithm. At the present time, no FIPS or NIST Recommendation specifies schemes for this method of key transport.

Note: Until such time as a key agreement recommendation is available using RSA, all key establishment schemes that use RSA are interpreted as providing key transport.

The allowable key sizes for key transport are specified in SP 800-57, Recommendation for Key Management, Part 1.

Any key transport scheme using an RSA-based key transport methodology that uses the allowable key sizes specified in SP 800-57 is acceptable until NIST provides further guidance.

Key transport schemes in the following protocols using asymmetric algorithms will be allowed for validation in FIPS mode to establish keying material until such time as Approved key transport schemes are determined:

1. The key transport scheme in SSL v3.1 is acceptable for use in the FIPS mode.

2. The key transport schemes in TLS and EAP-TLS may be used in the FIPS mode. While the protocols use the same cryptographic algorithms as the versions of SSL prior to version 3.1, the manner in which the algorithms are used makes them acceptable to be used in FIPS mode.

The following key establishment methods are ***unacceptable***:

- SSL: all versions of SSL, except SSL v3.1[12], are not to be used in the FIPS mode. The manner in which the method uses approved and non-approved cryptographic algorithms for its operation prohibits its usage.[13]

- Password-Based Key Establishment Methods: all password-based key establishment methods such as PKCS#5 are not to be used in the FIPS mode.

The CMVP *may* allow other techniques and/or methods for use in a FIPS mode but they **shall** meet all the following requirements:

- are industry accepted;
- are commercially available;

[12] SSL v3.1 is allowed, as it is equivalent to TLS v1.0.
[13] The problem with SSL 3.0 is the key derivation process that applies to all SSL 3.0 cipher suites: half of the master key that is set up during the SSL key exchange depends entirely on the MD5 hash function. MD5 is not a FIPS approved algorithm, and its collision resistance property has recently been broken by Antoine Joux.

TLS also uses MD5 in the key derivation process, but in a different manner, so that all of the master key depends on both MD5 and SHA-1, and nothing in TLS actually depends on MD5 for its security.

Therefore, TLS implementations can be validated under FIPS 140-2, while SSL 3.0 implementations cannot. TLS is version 3.1 of SSL, and most current servers and clients are capable of doing both SSL 3.0 and TLS.

William Burr, NIST Security Technology Group

- are widely used by government and industry; and
- are known in the public domain.

The **final determination** of an allowed method for use in a FIPS mode is made by the NIST Security Technology Group.

Additional Comments

This IG does not address key establishment for use in authentication techniques.

The key establishment method(s) used by the cryptographic module must be listed under AS.07.21.

7.2 Use of IEEE 802.11i Key Derivation Protocols

Applicable Levels:	*All*
Original Publishing Date:	*01/21/2005*
Effective Date:	
Last Modified Date:	*09/12/2005*
Relevant Assertions:	*AS07.17*
Relevant Test Requirements:	*TE07.17.01-02*
Relevant Vendor Requirements:	*VE07.17.01*

Background

FIPS 140-2 Annex D provides a list of the FIPS Approved key establishment techniques applicable to FIPS PUB 140-2.

The commercially available schemes referred to in FIPS 140-2 Annex D are concerned with the derivation of a shared secret, or, as it is sometimes called, "the keying material." The IEEE 802.11i standard describes how to derive keys from a secret shared between two parties. It does not specify how to establish this commonly shared secret.

Question/Problem

Assuming that the shared secret is established using a key establishment technique specified in Annex D, can a cryptographic module use the 802.11i key derivation techniques to derive a data protection key, a key encryption key and other keys for use in a FIPS Approved mode of operation?

Resolution

Until such a time that a FIPS or NIST recommendation exists specifying methods for key derivation from established keying material, the key derivation function specified in IEEE 802.11i used to derive keys from a shared common secret is allowed in a FIPS mode of operations within the IEEE 802.11i protocol..

Additional Notes and Conditions

NIST will be releasing a draft of Special Publication 800-56 for public comment. This document, when finalized, will provide Approved methods to derive keying material.

Implementations of the IEEE 802.11i protocol operating in a FIPS approved mode of operation must meet the following requirements:

1. If a key is derived from a shared secret then:

   a) the shared secret (the keying material) is established using a FIPS Approved method specified in FIPS 140-2 Annex D; AND

   b) the key derivation function as defined in IEEE 802.11i.

2. If 802.11i protocols are used for data protection, then the data protection method shall be AES CCM, which is an Approved security function for use in a FIPS Approved mode of operation as specified in FIPS 140-2 Annex A.

3. The keying material may be established via manual methods as specified in FIPS 140-2. The key derivation function as defined in IEEE 802.11i may then be applied.

References

Amendment 6: IEEE 802.11Medium Access Control (MAC) Security Enhancements, IEEE P802.11i/D10.0, April 2004. Section 8.5.1.2. Pairwise Key Hierarchy.

7.3 Use of other Core Symmetric Algorithms in ANSI X9.31 RNG

Applicable Levels:	*All*
Original Publishing Date:	*01/21/2005*
Effective Date:	*01/28/2005*
Last Modified Date:	
Relevant Assertions:	*AS07.10*
Relevant Test Requirements:	*TE07.10.01*
Relevant Vendor Requirements:	*VE07.10.01*

Background

ANSI X9.31 Appendix A.2.4 specifies 2-key Triple-DES as the core symmetric algorithm in its deterministic random number generator.

Question/Problem

Is it acceptable to use other FIPS Approved symmetric algorithms as the ANSI X9.31 Appendix A.2.4 RNG core algorithm?

Resolution

In addition to 2-key Triple-DES, it is acceptable to use the following FIPS Approved symmetric algorithms as the ANSI X9.31 RNG core algorithm:

- AES
- 3-key Triple-DES
- SKIPJACK

CAVS testing is available for the 2-key Triple-DES, 3-key Triple-DES and AES. Until such time as CAVS testing is available for RNG testing using SKIPJACK, for module testing purposes, the core cryptographic algorithm SKIPJACK shall be validated and the RNG implementation will be marked as "vendor affirmed".

Additional Comments

FIPS 140-2 Annex C has been updated to include reference to the NIST RNG specification for implementing 3-key Triple-DES and AES with ANSI X9.31 Appendix A.2.4.

7.4 Zeroization of Power-Up Test Keys

Applicable Levels:	*All*
Original Publishing Date:	*09/12/2005*
Effective Date:	
Last Modified Date:	*02/23/2007*
Relevant Assertions:	*AS07.41*
Relevant Test Requirements:	*TE07.41.01-04*
Relevant Vendor Requirements:	*VE07.41.01*

Background

Section 4.7.6 of FIPS 140-2 states that "*The cryptographic module shall provide methods to zeroize all Plaintext secret and private cryptographic keys and CSPs within the module*."

Question/Problem

Are cryptographic keys used by a module ONLY to perform Section 4.9.1 Power-Up Tests (e.g. cryptographic algorithm Known Answer Tests (KAT) or software/firmware integrity tests) considered CSPs and is zeroization required under Section 4.7.6?

Resolution

Cryptographic keys used by a cryptographic module ONLY to perform Section 4.9.1 Power-Up Tests are not considered CSPs and therefore do not need to meet the Section 4.7.6 zeroization requirements.

Additional Comments

7.5 Strength of Key Establishment Methods

Applicable Levels:	*All*
Original Publishing Date:	*11/23/2005*
Effective Date:	*06/29/2005*
Last Modified Date:	*01/25/2007*
Relevant Assertions:	*AS07.19*
Relevant Test Requirements:	*TE07.19.01-02*
Relevant Vendor Requirements:	*VE07.19.01*

Background

FIPS 140-2 AS.07.19 states that "Compromising the security of the key establishment method (e.g., compromising the security of the algorithm used for key establishment) shall require as many operations as determining the value of the cryptographic key being transported or agreed upon. "

NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General (Revised)* (March 2007), Section 5, Sub-Section 5.6.1, Comparable Algorithm Strength, contains Table 2, which provides comparable security strengths for the Approved algorithms.

Table 2: Comparable strengths

Bits of security	Symmetric key algorithms	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
80	2TDEA[18]	$L = 1024$ $N = 160$	$k = 1024$	$f = 160\text{-}223$
112	3TDEA	$L = 2048$ $N = 224$	$k = 2048$	$f = 224\text{-}255$
128	AES-128	$L = 3072$ $N = 256$	$k = 3072$	$f = 256\text{-}383$
192	AES-192	$L = 7680$ $N = 384$	$k = 7680$	$f = 384\text{-}511$
256	AES-256	$L = 15{,}360$ $N = 512$	$k = 15{,}360$	$f = 512+$

[18] The 80-bit security of 2TDEA is based on the availability of 2^{40} matched plaintext and ciphertext blocks to an attacker (see [ANSX9.52], Annex B).

1. Column 1 indicates the number of bits of security provided by the algorithms and key sizes in a particular row. Note that the bits of security is not necessarily the same as the key sizes for the algorithms in the other columns, due to attacks on those algorithms that provide computational advantages.
2. Column 2 identifies the symmetric key algorithms that provide the indicated level of security (at a minimum), where 2TDEA and 3TDEA are specified in [SP800-67], and AES is specified in [FIPS197]. 2TDEA is TDEA with two different keys; 3TDEA is TDEA with three different keys.
3. Column 3 indicates the minimum size of the parameters associated with the standards that use finite field cryptography (FFC). Examples of such algorithms include DSA as defined in [FIPS186-3] for digital signatures, and Diffie-Hellman (DH) and MQV key agreement as defined in [ANSX9.42] and [SP800-56]), where L is the size of the public key, and N is the size of the private key.
4. Column 4 indicates the value for k (the size of the modulus n) for algorithms based on integer factorization cryptography (IFC). The predominant algorithm of this type is the RSA algorithm. RSA is specified in [ANSX9.31] and [PKCS#1]. These specifications are referenced in [FIPS186-3] for digital signatures. The value of k is commonly considered to be the key size.
5. Column 5 indicates the range of f (the size of n, where n is the order of the base point G) for algorithms based on elliptic curve cryptography (ECC) that are specified for digital signatures in [ANSX9.62] and adopted in [FIPS186-3], and for key establishment as specified in [ANSX9.63] and [SP800-56]. The value of f is commonly considered to be the key size.

For example, if a 256-bit AES is to be transported utilizing RSA, then k=15,360 for the RSA key pair. A 256-bit AES key transport key could be used to wrap a 256-bit AES key.

For key strengths not listed in Table 2 above, the correspondence between the length of an RSA or a Diffie-Hellman key and the length of a symmetric key of an identical strength can be computed as:

> If the length of an RSA key L (this is the value of k in the fourth column of Table 2 above), then the length x of a symmetric key of approximately the same strength can be computed as:

$$x = \frac{1.923 \times \sqrt[3]{L \times \ln(2)} \times \sqrt[3]{[\ln(L \times \ln(2))]^2} - 4.69}{\ln(2)} \qquad (1)$$

If the lengths of the Diffie-Hellman public and private keys are L and N, correspondingly, then the length y of a symmetric key of approximately the same strength can be computed as:

$$y = \min(x, N/2), \qquad (2)$$

where x is computed as in formula (1) above.

Question/Problem

What does FIPS 140-2 assertion AS.07.19 mean in the context of NIST Special Publication 800-57?

Resolution

The requirement applies to the key establishment methods found in Section 4.7.

If a key is established via a key agreement or key transport method, the transport key or key agreement method shall be of equal or greater strength than the key being transported or established. For example, it is acceptable to have a two-key Triple-DES key (80-bit strength) transported using a 2048-bit RSA key (112-bit strength).

If the apparent strength of the largest key (taken at face value) that can be established by a cryptographic module is greater or equal than the largest comparable strength of the implemented key establishment method, then the module certificate and security policy will be annotated with, in addition to the other required caveats, the caveat "(Key establishment methodology provides xx bits of encryption strength)" for that key establishment method. For example, if a 256-bit AES is to be transported utilizing RSA with a value of k=1024 for the RSA key pair, the caveat would state "RSA (PKCS#1, key wrapping, key establishment methodology provides 80 bits of encryption strength)".

Furthermore, if the module supports, for a particular key establishment method, several key strengths, then the caveat will state either the choice of strengths provided by the keys while operated in FIPS mode, if there are only two possible effective strengths, or a range of strengths if there are more than two possible strengths. For example, if a module implements 512 and 1024-bit public key Diffie-Hellman with the private keys of 112 and 160 bits then the caveat would state “Diffie-Hellman (key agreement; key establishment methodology provides 56 or 80 bits of encryption strength)". If, on the other hand, a module implements, in support of a key wrapping protocol, the RSA encryption/decryption with the RSA keys of 1024, 2048, 4096 and 15360 bits, then the caveat would say “RSA (key wrapping; key establishment methodology provides between 80 and 256 bits of encryption strength)”. These caveats provide clarification to Federal users on the actual strength the module is providing even though Table 4 below states that the strength is sufficient.

Additional Comments

NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General (Revised)* (March 2007) also provides the following information in Section 5.6.2:

Table 4 provides recommendations that may be used to select an appropriate suite of algorithms and key sizes for Federal Government unclassified applications. A minimum of eighty bits of security **shall** be provided until 2010. Between 2011 and 2030, a minimum of 112 bits of security **shall** be provided. Thereafter, at least 128 bits of security **shall** be provided.

1. Column 1 indicates the estimated time periods during which data protected by specific cryptographic algorithms remains secure. (i.e., the algorithm security lifetimes).

2. Column 2 identifies appropriate symmetric key algorithms and key sizes: 2TDEA and 3TDEA are specified in [SP800-67], the AES algorithm is specified in [FIPS197], and the computation of Message Authentication Codes (MACs) using block ciphers is specified in [SP800-38].
3. Column 3 indicates the minimum size of the parameters associated with FFC, such as DSA as defined in [FIPS186-3].
4. Column 4 indicates the minimum size of the modulus for IFC, such as the RSA algorithm specified in [ANSX9.31] and [PKCS#1] and adopted in [FIPS186-3] for digital signatures.
5. Column 5 indicates the value of *f* (the size of *n*, where *n* is the order of the base point *G*) for algorithms based on elliptic curve cryptography (ECC) that are specified for digital signatures in [ANSX9.62] and adopted in [FIPS186-3], and for key establishment as specified in [ANSX9.63] and [SP800-56]. The value of *f* is commonly considered to be the key size.

Table 4: Recommended algorithms and minimum key sizes

Algorithm security lifetimes	Symmetric key Algorithms (Encryption & MAC)	FFC (e.g., DSA, D-H)	IFC (e.g., RSA)	ECC (e.g., ECDSA)
Through 2010 (min. of 80 bits of strength)	2TDEA[21] 3TDEA AES-128 AES-192 AES-256	Min.: L = 1024; N =160	Min.: k=1024	Min.: f=160
Through 2030 (min. of 112 bits of strength)	3TDEA AES-128 AES-192 AES-256	Min.: L = 2048 N = 224	Min.: k=2048	Min.: f=224
Beyond 2030 (min. of 128 bits of strength)	AES-128 AES-192 AES-256	Min.: L = 3072 N = 256	Min.: k=3072	Min.: f=256

[21] The 80-bit security of 2TDEA is based on the availability of 2^{40} matched plaintext and ciphertext blocks to an attacker (see [ANSX9.52], Annex B).

The algorithms and key sizes in the table are considered appropriate for the protection of data during the given time periods. Algorithms or key sizes not indicated for a given range of years **shall not** be used to protect information during that time period. If the security life of information extends beyond one time period specified in the table into the next time period (the later time period), the algorithms and key sizes specified for the later time **shall** be used. The following examples are provided to clarify the use of the table:

a. If information is encrypted in 2005 and the maximum expected security life of that data is only five years, any of the algorithms or key sizes in the table may be used. But if the information is protected in 2005 and the expected security life of the data is six years, then 2TDEA would not be appropriate.
b. If a CA signature key and all certificates issued under that key will expire in 2005, then the signature and hash algorithm used to sign the certificate needs to be secure for at least five years. A certificate issued in 2005 using 1024 bit DSA and SHA-1 would be acceptable.
c. If information is initially signed in 2009 and needs to remain secure for a maximum of ten years (i.e., from 2009 to 2019), a 1024 bit RSA key would not provide sufficient protection between 2011 and 2019 and, therefore, it is not recommended that 1024-bit RSA be used in this case. It is recommended that the algorithms and key sizes in the "Through 2030" row (e.g., 2048-bit RSA) should be used to provide the cryptographic protection. In addition, the signature must be generated using a hash algorithm of comparable or greater strength, such as SHA-224 or SHA-256.

The CMVP will be providing additional guidance and transition periods in regard to the information in Table 4.

7.6 RNGs: Seeds, Seed Keys and Date/Time Vectors

Applicable Levels:	*All*
Original Publishing Date:	*11/16/2007*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS07.09*
Relevant Test Requirements:	*TE07.09.01*
Relevant Vendor Requirements:	*VE07.09.01*

Background

An RNG may employ a seed and seed key and a Date/Time vector for its operation. FIPS 140-1 IG **8.7** provides a basis for the requirements related to the ANSI X9.31 RNG **seed**, **seed key** and Date/Time vector. The document titled *NIST Recommended Random Number Generator based on ANSI X9.31 Appendix A.2.4 using the 3-Key Triple DES and AES Algorithms* allows for the use of Triple-DES and AES.

Questions/Problems

1. In the case where an RNG employs a **seed** and **seed key**, how does AS07.09 apply?

2. In the case where an RNG employs a Date/Time vector, what, if any, additional attributes apply?

Resolution

1. **AS.07.09** of FIPS 140-2 specifies that the seed and seed key shall not have the same value.

   During initialization of the **seed** or **seed key**, the initialization data provided for one, shall not be provided as initialization data to the other. The **seed** or **seed key** or both may be re-initialized prior to each call for a random data value.

2. The Date/Time vector shall be updated on each iteration or call to the RNG. In lieu of a Date/Time vector, an incrementer may be used. The Date/Time vector or incrementer shall be a non-repeating value during each instance of the module's power-on state.

Additional Comments

ANSI X9.31 specifies that the **seed** shall also be kept secret. As such, the **seed** is considered a CSP and shall meet all the requirements pertaining to CSPs.

FIPS 140-2 AS07.14 and AS07.23 are applicable to the **seed key**.

The seed key is sometimes referred as the RNG key; the key used by the underlining encryption algorithm(s) implemented by the RNG.

7.7 Key Establishment and Key Entry and Output

Applicable Levels:	*All*
Original Publishing Date:	*01/24/2008*
Effective Date:	

Last Modified Date:	*01/24/2008*
Relevant Assertions:	*General*
Relevant Test Requirements:	
Relevant Vendor Requirements:	

Question/Problem

Given different configurations of cryptographic modules, how can a modules key establishment and key entry and output states be easily mapped to the FIPS 140-2 requirements for Cryptographic Module Ports and Interfaces (Section 4.2), Key Establishment (Section 4.7.3) and Key Entry and Output (Section 4.7.4)?

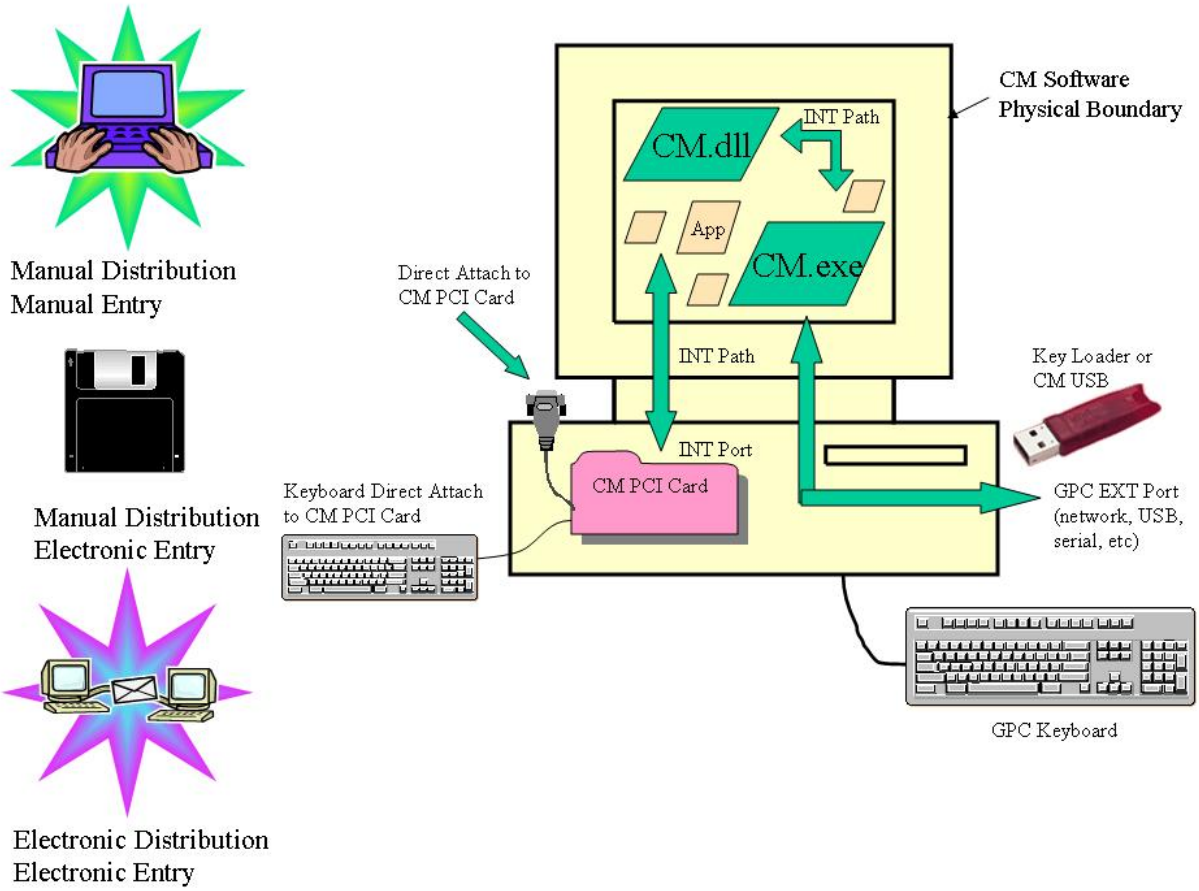
Resolution

Using the following guidelines, first determine how keys are established to a module. Once the establishment method is determined, the Key Entry format table will indicate the requirements on how keys shall be entered or output. The following is based on the requirements found in FIPS 140-2 in Sections 4.2 and 4.7.

CM: a FIPS 140-1 or FIPS 140-2 *validated* Cryptographic Module
GPC: General Purpose Computer
EXT: a *validated* Cryptographic Module which lies *External* or outside of the boundary in regard to the reference diagrams CM software physical boundary. This also includes a standalone CM.
INT: a *validated* Cryptographic Module which lies *Internal* or inside of the boundary in regard to the reference diagrams CM software physical boundary.
App: a non-validated non-crypto general purpose software application operating inside of the boundary in regard to the reference diagrams CM software physical boundary.

Key Establishment – Table 1	
MD: Manual Distribution	**ME: Manual Entry (Input / Output)**
ED: Electronic Distribution	**EE: Electronic Entry (Input / Output)**
CM Software[1] from GPC Keyboard	**MD / ME**
CM Software[1] to/from GPC Key Loader (e.g., diskette, USB token, etc)	**MD / EE**
CM Software[1] to/from GPC EXT Ports (e.g., network port)	**ED / EE**
CM Software[1] to/from CM Software[1] via GPC INT Path	NA
CM Software[1] to/from App Software via GPC INT Path	**NA**
CM Software[1] to/from INT CM Hardware via GPC INT Path	**NA**
CM Software[1] to/from EXT CM Hardware running on a non-networked GPC (key loader)	**MD / EE**
CM Software[1] to/from EXT CM Hardware running on a networked GPC	**ED / EE**
INT CM Hardware to/from App Software via GPC INT Path	**ED / EE**
INT CM Hardware to/from GPC EXT Ports via GPC INT Path	**ED / EE**
INT CM Hardware from GPC Keyboard via GPC INT Path	**ED / EE**
INT CM Hardware to/from direct attach key loader	**MD / EE**
INT CM Hardware from direct attach keyboard	**MD / ME**
EXT CM Hardware to/from networked GPC	**ED / EE**
EXT CM Hardware to/from directly attached key loader (a non-networked GPC could be considered and used as a key loader)	**MD / EE**
EXT CM Hardware from direct attach keyboard	**MD / ME**
[1] **Must meet requirements of AS.06.04, AS.06.05 and AS.06.06**	

The following illustration provides reference to the above Key Establishment table.



Key Entry Format – Table 2

		Distribution (Establishment)							
		Manual				Electronic			
Entry (Input / Output)	Manual	Keyboard, Thumbwheel, Switch, Dial							
		1	2	3	4				
		P/E	P/E	E/SK	E/SK				
	Electronic	Smart Cards, Token, Diskettes and Key Loaders				Key Transport or Key Agreement			
		1	2	3	4	1	2	3	4
		P/E	P/E	E/SK	E/SK	E	E	E	E

Legend:
P/E: May be Plaintext or Encrypted

E: Encrypted
E/SK: Encrypted or Plaintext Split Knowledge (via separated physical ports or via trusted path)

At Levels 3 and 4, plaintext key components may be entered either via separate physical ports or logically separated ports using a trusted path. Manual entry of plaintext keys must be entered using split knowledge procedures. Keys may also be entered encrypted manually. If automated methods, they must be encrypted.

Additional Comments

This IG reaffirms that keys established using *manual transport methods* and *electronically input or output* to a cryptographic module may be input or output in plaintext at Levels 1 and 2.

Level 1 Software – General Purpose Operational Environment

AS06.04: (Level 1 Only) The operating system shall be restricted to a single operator mode of operation (i.e., concurrent operators are explicitly excluded).

AS06.05: (Level 1 Only) The cryptographic module shall prevent access by other processes to plaintext private and secret keys, CSPs, and intermediate key generation values during the time the cryptographic module is executing/operational. Processes that are spawned by the cryptographic module are owned by the module and are not owned by external processes/operators.

AS06.06: (Leve1 1 Only) Non-cryptographic processes shall not interrupt the cryptographic module during execution.

A Software Cryptographic Module (SCM) requires the use of an underlying General Purpose Computer (GPC) and Operational Environment (OE) to execute/operate. A SCM is conceptually comprised of two sub-elements: a Physical Cryptographic Module (PCM) and the Logical Cryptographic Module (LCM) boundary. The LCM is executes/operates within the PCM. The LCM is the collection of executable code that encompasses the cryptographic functionality of the SCM (e.g., .dll's, .exe's). Other general-purpose application software (App) (e.g., word processors, network interfaces, etc) may reside within the PCM. Therefore the PCM encompasses the following elements: GPC, OE, LCM and App. The LCM relies on the OE and GPC for memory management, access to ports and interfaces, and other services such as the requirements of AS06.04, AS06.05 and AS06.06. The LCM has no operational control over other App elements within the PCM of the SCM. The SCM, which is comprised of all the various sub-elements (GPC, OE, LCM and App), is restricted to a single operator mode of operation, such that the single operator has a level of confidence in the SCM environment as a whole. The CMVP views the non-LCM elements (GPC, OE and App) as implicitly excluded.

Example: If the LCM generates keys, it must use a FIPS Approved RNG. That key may be stored within the PCM but must meet **AS06.05** unless the LCM wishes the key to be exported. If exported, refer to Table 1 for the key establishment and key entry requirements. If a key is generated outside of the LCM, then the generation method is out-of-scope but the key must be imported per Table 1 requirements.

It is the burden of the operator of the SCM to understand the environment the SCM is running. If that environment is not acceptable, then there are alternative solutions (hardware cryptographic modules and/or Level 2, 3 or 4 software cryptographic modules) that should be considered.

If the operating system requirements of AS06.04, AS06.05 and AS06.06 cannot be met, then the SCM cannot be validated at Level 1. The vendor provided documentation shall indicate how these requirements are met (AS14.02).

Section 8 – Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Section 9 – Self-Tests

9.1 Known Answer Test for Keyed Hashing Algorithm

Applicable Levels:	*All*
Original Publishing Date:	*02/10/2004*
Effective Date:	
Last Modified Date:	*09/22/2004*
Relevant Assertions:	*AS09.07*
Relevant Test Requirements:	*TE09.07.01*
Relevant Vendor Requirements:	*VE09.07.01*

Background

Several keyed hashing algorithms are FIPS-approved (e.g. DES MAC, HMAC-SHA-1) and have different levels of complexity that determine the power-on Know-Answer-Test (KAT) requirements.

Question/Problem

What are the KAT requirements when implementing keyed hashing algorithms in FIPS mode?

Resolution

The following table summarizes the minimal KAT requirements:

KAT Requirements	Keyed Hashing algorithm	Underlying algorithm
DES MAC / Triple-DES MAC	No	Yes
HMAC-SHA-1	Yes	No
HMAC-SHA-224	Yes	No
HMAC-SHA-256	Yes	No
HMAC-SHA-384	Yes	No
HMAC-SHA-512	Yes	No

Rationale

DES MAC and the Triple-DES MAC algorithms do not include much additional complexity over the underlying algorithmic engine (e.g. DES and Triple-DES). However, keyed hashing algorithms such as HMAC-SHA-1 have additional complexity over the underlying algorithmic engine (e.g. SHA-1). A KAT performed on the DES or Triple-DES algorithms adequately verifies their associated hashing algorithm. This is not the case for the keyed hashing algorithm using a SHS algorithm which implements several other functions in addition to the underlying SHS algorithm.

Additional Comments

As discussed in FIPS 140-2 IG 9.3, if HMAC-SHA-1 is used as the Approved integrity technique to verify the software or firmware components as specified in AS.06.08, a KAT is not required for either the HMAC-SHA-1 or the underlying SHA-1 algorithm.

9.2 Known Answer Test for Embedded Cryptographic Algorithms

Applicable Levels:	*All*
Original Publishing Date:	*02/10/2004*
Effective Date:	
Last Modified Date:	*08/19/2004*
Relevant Assertions:	*AS09.19*
Relevant Test Requirements:	*TE09.19.01-03*
Relevant Vendor Requirements:	*VE09.19.01-02*

Background

Core cryptographic algorithms are often embedded into other higher cryptographic algorithms for their operation in FIPS mode (e.g. SHA-1 algorithm embedded into HMAC-SHA-1 and DSA, DES or Triple-DES into RNGs). FIPS 140-2 requires that cryptographic modules that implement FIPS-approved algorithms used in FIPS mode perform a Known-Answer-Test (KAT) as part of their power-up self-tests. This requirement is also valid for the core cryptographic algorithm implementation. However, when the cryptographic module performs the KAT on the higher cryptographic algorithm, the embedded core cryptographic algorithm may also be self-tested.

Question/Problem

If an embedded core cryptographic algorithm is self-tested during the higher cryptographic algorithm KAT, is it necessary for the cryptographic module to implement a KAT for the already self-tested core cryptographic algorithm implementation?

Resolution

It is acceptable for the cryptographic module not to perform a KAT on the embedded core cryptographic algorithm implementation if;

1. the higher cryptographic algorithm uses that implementation,
2. the higher cryptographic algorithm performs a KAT at power-up and,
3. all cryptographic functions within the core cryptographic algorithm are tested (e.g. encryption and decryption for DES and Triple-DES).

Additional Comments

If the cryptographic module contains several core cryptographic algorithm implementations (e.g., several different implementations of SHA-1 algorithm) and some are not used by other higher FIPS-approved cryptographic algorithms (and are therefore not self-tested), then the cryptographic module must perform a KAT at power-up for each of those implementations.

Implementation of DES or Triple-DES within an RNG such as ANSI X9.31 does not meet bullet #3 above since not all the DES or Triple-DES cryptographic functions are tested (e.g. encrypt is performed in the RNG generation, not decrypt)

Implementation of SHA-1 within the FIPS 186-2 random number generation algorithms does not meet bullet #3 above since the hashing function is not completely performed

9.3 KAT for Algorithms used in an Integrity Test Technique

Applicable Levels:	*All*
Original Publishing Date:	*02/10/2004*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS06.08 and AS09.16*
Relevant Test Requirements:	*TE06.08.01-02 and TE09.16.01-02*
Relevant Vendor Requirements:	*VE06.08.01 and VE09.16.01*

Background

AS06.08 requires that a cryptographic mechanism using an Approved integrity technique shall be applied to all cryptographic software and firmware components within the cryptographic module. AS09.16 requires that a cryptographic algorithm test using a Known-Answer-Test (KAT) shall be conducted for all cryptographic functions of each Approved cryptographic algorithm implemented by the cryptographic module and used in FIPS mode of operation.

Question/Problem

Must a cryptographic module implement a separate KAT for the underlying cryptographic algorithm used in the Approved integrity technique?

Resolution

A cryptographic module may not implement a separate KAT for the underlying cryptographic algorithm used for the Approved integrity technique if all the cryptographic functions of the underlying cryptographic algorithm are tested (e.g. encryption and decryption for Triple-DES).

Rationale

The software/firmware integrity check using an Approved integrity technique is considered a KAT since the cryptographic module uses itself as an input to the algorithm and a known answer as the expected output.

EX: If HMAC-SHA-1 is used as the Approved integrity technique to verify the software or firmware components, a KAT is not required for either the HMAC-SHA-1 or the underlying SHA-1 algorithm.

EX: If Triple-DES MAC is used as the Approved integrity technique to verify the software or firmware components, a KAT is still required for the underlying Triple-DES as the integrity checking may not use both the Triple-DES encrypt and decrypt functions.

EX: If RSA is used to verify the signature of the software or firmware components, a KAT is still required for the underlying RSA as the integrity checking would not use the RSA signature generation function. However, a KAT for the underlying SHA-1 hashing function is not required.

Additional Comments

9.4 Cryptographic Algorithm Tests for SHS Algorithms and Higher Cryptographic Algorithms Using SHS Algorithms

Applicable Levels:	*All*
Original Publishing Date:	*08/19/2004*
Effective Date:	
Last Modified Date:	*01/16/2008*
Relevant Assertions:	*AS09.16*
Relevant Test Requirements:	*TE09.16.01*
Relevant Vendor Requirements:	*VE09.16.01*

Background

Cryptographic algorithm test. A cryptographic algorithm test using a known answer shall be conducted for all cryptographic functions (e.g., encryption, decryption, authentication, and random number generation) of each Approved cryptographic algorithm implemented by a cryptographic module. A known-answer test involves operating the cryptographic algorithm on data for which the correct output is already known and comparing the calculated output with the previously generated output (the known answer). If the calculated output does not equal the known answer, the known-answer test shall fail.

Cryptographic algorithms whose outputs vary for a given set of inputs (e.g., the Digital Signature Algorithm) shall be tested using a known-answer test or shall be tested using a pair-wise consistency test (specified below).

Each algorithm implementation to be used in a FIPS Approved mode of operation must implement a cryptographic algorithm test. The cryptographic algorithm test is a *health check* of the algorithm implementation performed at power-up or on demand.

Question/Problem

What are the minimum requirements placed on Known Answer Tests (KATs) for SHS algorithms and higher cryptographic algorithms implementing SHS algorithms so that they can be used in FIPS Approved mode of operation? What are the minimum requirements placed on a pair-wise consistency test (for public and private keys) if performed at power-up or on demand?

Resolution

Following is a subset of algorithm KAT specific implementation guidance:

- the following are minimal requirements for SHS algorithms:
  - a KAT for SHA-1 (if applicable) is required;
  - a KAT for SHA-256 (if applicable) is required;
  - a KAT for SHA-224 (if applicable) is required if SHA-224 is implemented without SHA-256;
  - a KAT for SHA-512 (if applicable) is required; and,
  - a KAT for SHA-384 (if applicable) is required if SHA-384 is implemented without SHA-512.

- a KAT or pair-wise consistency for DSA and RSA (if applicable) is required and shall be performed on:
  - at minimum, the smallest NIST-Recommended modulus size or DSA prime that is supported by the module; and,
  - at minimum, any one of the implemented underlying SHS algorithms used by the higher cryptographic algorithm.

- an RSA KAT shall be performed using both the public and private exponents (*e* and *d*) and the two exponents shall correspond [that is, $d * e = 1 \pmod{(p-1)(q-1)}$].

- a KAT or pair-wise consistency for ECDSA (if applicable) is required and shall be performed at a minimum, on:
  - any one of the implemented curves in each of the implemented two types of fields (i.e., prime field where *GF(p)*, and binary field where $GF(2^m)$); and
  - any one of the implemented underlying SHS algorithms used by the higher cryptographic algorithm.

- a KAT for HMAC (if applicable) is required and shall be performed at minimum, on any one of the implemented underlying SHS algorithms.

Additional Comments

FIPS 140-2 IG 9.2 *Known Answer Test for Embedded Crypto Algorithms* applies.

This IG is consistent with FIPS 140-2 IG 9.1 *Known Answer Test For Keyed Hashing Algorithm*.

Rationale: The purpose of a KAT is to perform a health-check of the cryptographic module to identify catastrophic failures or alterations of the module between power cycles and not that the implementation is correct. The implementation verification is performed during the cryptographic algorithmic testing and validation.

Section 10 – Design Assurance

Section 11 – Mitigation of Other Attacks

Section 12 – Appendix A: Summary of Documentation Requirements

Section 13 – Appendix B: Recommended Software Development Practices

Section 14 – Appendix C: Cryptographic Module Security Policy

14.1 Level of Detail When Reporting Cryptographic Services

Applicable Levels:	*All*
Original Publishing Date:	*11/15/2001*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS01.02, AS01.03, AS01.12, AS01.16, AS03.14, AS10.06, AS14.02, AS14.03, AS14.04, AS14.06, AS14.07*
Relevant Test Requirements:	*TE01.03.01, TE01.03.02, TE01.16.01, TE03.14.01, TE10.06.01, TE14.07.01, TE14.07.02*
Relevant Vendor Requirements:	*VE01.03.01, VE01.03.02, VE01.16.01, VE03.14.01, VE03.14.02, VE10.06.01, VE14.07.01, VE14.07.02, VE14.07.03*

Question/Problem

What is the level of detail that the non-proprietary security policy must contain in order to describe the cryptographic service(s) implemented by a cryptographic module?

Resolution

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

- The service name
- A concise description of the service purpose and/or use (the service name alone may, in some instances, provide this information)
- A list of Approved security functions (algorithm(s), key management technique(s) or authentication technique) used by, or implemented through, the invocation of the service.
- A list of the cryptographic keys and/or CSPs associated with the service or with the Approved security function(s) it uses.
- For each operator role authorized to use the service:
    - Information describing the individual access rights to all keys and/or CSPs
    - Information describing the method used to authenticate each role.

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

Additional Comments

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

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

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

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

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

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

See also the definitions of ***Approved mode of operation*** and ***Approved security function*** in FIPS 140-2.

14.2 Level of Detail When Reporting Mitigation Of Attacks

Applicable Levels:	*All*
Original Publishing Date:	*11/15/2001*
Effective Date:	
Last Modified Date:	
Relevant Assertions:	*AS14.09*
Relevant Test Requirements:	*TE14.09.01*
Relevant Vendor Requirements:	*VE14.09.01*

Question/Problem

What is the level of detail that the non-proprietary security policy must contain that describes the security mechanism(s) implemented by the cryptographic module to mitigate other attacks?

Resolution

The level of detail describing the security mechanism(s) implemented by the cryptographic module to mitigate other attacks required to be contained in the security policy must be similar to what is found on advertisement documentation (product glossies).

Additional Comments

14.3 Logical Diagram for Software, Firmware and Hybrid Modules

Applicable Levels:	*All*
Original Publishing Date:	*07/03/2007*
Effective Date:	

Last Modified Date:	
Relevant Assertions:	*AS14.01*
Relevant Test Requirements:	*TE14.01.01*
Relevant Vendor Requirements:	*VE14.01.01*

Background

FIPS 140-2 DTR VE.14.01.01 specifies the requirement for the vendor to provide in the security policy a diagram or image of the physical cryptographic module.

While the requirement is vague when applied to a software, firmware or hybrid cryptographic module, it is intended as well to clearly illustrate the *logical boundary* of the module as well as the other logical objects and the operating environment with which the module executes with.

Question/Problem

For a software, firmware or hybrid cryptographic module, what are the requirements of the *logical diagram* contained in the security policy as specified in VE.14.01.01?

Resolution

The *logical diagram* must illustrate:

- the logical relationship of the software, firmware or hybrid module with respect to the operating environment. This shall include, as applicable, references to any operating system, hardware components (i.e. hybrid) other supporting applications, and illustrate the physical boundary of the platform. All the logical and physical layers between the logical object and the physical boundary shall be clearly defined.

Additional Comments

The *logical diagram* must convey basic information to the operator of the cryptographic module about its relationship respective to the operating environment.

The *logical diagram* could be a subset of the block diagram specified in AS.01.13.

Expired Implementation Guidance

End of Document