National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

Cryptographic Module Validation Program

New Implementation Guidance

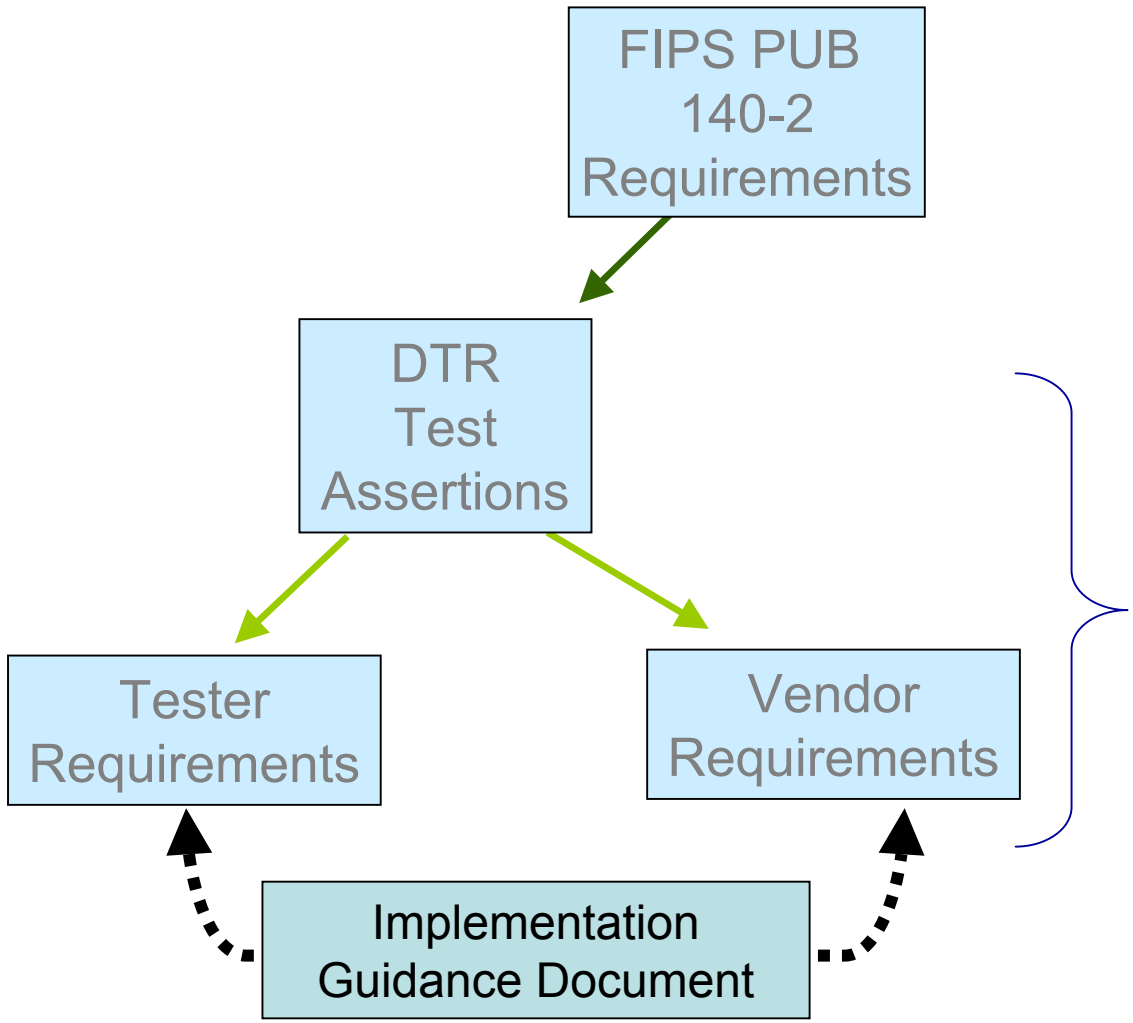
Randall J. Easter

Director, NIST CMVP

September 14, 2004

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada



Derived Test Requirements

Implementation Guidance

- Provide additional clarity or explanation of *shall* requirements in FIPS 140-2
- Address new technologies or methods
- Provide programmatic guidance

New Implementation Guidance

- G.10 Physical Security Testing for Re-validation from FIPS 140-1 to FIPS 140-2
- 1.1 Cryptographic Module Name
- 1.2 FIPS Approved Mode of Operation
- 1.3 Firmware Designation
- 1.4 Use of Cryptographic Algorithm Validation Certificates
- 1.5 Validation Testing of SHS Algorithms and Higher Cryptographic Algorithm Using SHS Algorithms
- 5.1 Opacity and Probing of Cryptographic Modules with Fans, Ventilation Holes or Slits at Level 2
- 6.3 Correction to Common Criteria Requirements on Operating System
- 7.1 Acceptable Key Establishment Protocols
- 9.1 Known Answer Test for Keyed Hashing Algorithm
- 9.2 Known Answer Test for Embedded Cryptographic Algorithms
- 9.3 KAT for Algorithms used in an Integrity Test Technique
- 9.4 Cryptographic Algorithm Tests for SHS Algorithms and Higher Cryptographic Algorithms Using SHS Algorithms

Updated Implementation Guidance

- **G.1 Implementation guidance requests to NIST and CSE**
- **G.2 Completion of a test report**
- **G.5 Maintaining validation compliance of software or firmware cryptographic modules**
- **G.8 Revalidation Requirements**
- **6.2 Applicability of Operational Environment Requirements to JAVA Smart Cards**

Proposed Implementation Guidance

- G.11 - Approval of Non Security Relevant Applications
- 2.x - Output Status Indication
- 3.x - Bypass Capabilities in Routers
- 5.x - Physical Security Guidance
- 7.x – Key Entry and Key Establishment
- 7.x – Approved Key Generation Methods
- 9.x - Software/Firmware Integrity Test – ECC Memory
- x.x - Pair-Wise Consistency Test for Key Pairs Used by Various rDSA Algorithms
- x.x – Error Recovery
- x.x – Emulation vs Simulation in Testing

G.1 Implementation guidance requests to NIST and CSE

- All programmatic and technical questions to be submitted to NIST/CSE in this format
- Official CMVP guidance will be distributed to all CMT Laboratories
- FIPS 140-2 IG Updated if possible

G.2 Completion of a test report

- New CMVP point of contacts
- At Levels 2, 3 and 4 – the CMT Laboratory must submit a detailed physical test report.
- Reception of the electronic submission documents will determine position in the CMVP validation review queue.

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

- For Level 1 Operational Environment, the 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
  - the source code of the software cryptographic module does not require modification prior to recompilation to allow porting to another compatible single user operating system.
- Software or firmware modules that require any source code modifications to be recompiled and ported to another GPC or operational environment must be reviewed by a CMT laboratory and revalidated per IG G.8 (1) [non-security relevant changes].
- If the Operational Environment is not applicable, a firmware module 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. Furthermore, except for GPCs, the tested platform must also be specified on the validation certificate.
- The CMVP allows the porting of a validated software 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 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.

G.8 Revalidation Requirements

- Modifications are made only to the physical enclosure of the cryptographic module that provides its protection and involves no operational changes to the module.
  - Each request will be handled on a case-by-case basis.

    An example of such a change could be a Level 2 tokens plastic encapsulation that has been reformulated or colored.

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

- 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.

- 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.

1.1 Cryptographic Module Name

- 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.

1.2 FIPS Approved Mode of Operation

- A module shall not share CSPs between modes of operation, (i.e., Approved mode of operation and a non-Approved mode of operation).

1.3 Firmware Designation

- 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.

1.4 Use of Cryptographic Algorithm Validation Certificates

- 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:
  - the source code or implementation of the validated cryptographic algorithm implementation has not been modified upon integration into the cryptographic module undergoing testing; and
  - the operational environment under which the validated cryptographic algorithm implementation was tested must be identical to the operational environment that the cryptographic module is being tested under.

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

- 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.

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

- 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.

6.3 Correction to Common Criteria Requirements on Operating System

- 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

7.1 Acceptable Key Establishment Protocols

- The following paragraphs describe the status of each protocol with reference to its usage in FIPS Approved mode of operation to establish keys to be used for data encryption and decryption:
  - SSL : all versions of the SSL protocol are not to be used in FIPS mode. The manner in which the protocol uses approved and non-approved cryptographic algorithms for its operation prohibits its usage.
  - TLS : the TLS protocol can be used in FIPS mode. While the protocol uses the same cryptographic algorithms as the SSL protocol, the manner in which the algorithms are used makes it acceptable to be used in FIPS mode.
  - IPSEC : the IPSEC protocol can be used in FIPS mode so long as the cryptographic algorithms used by the implementation are FIPS Approved.
  - Password-Based Key Establishment protocols : all password-based key establishment protocols such as PKCS#5 are not to be used in FIPS mode.

9.1 Known Answer Test for Keyed Hashing Algorithm

- 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

9.2 Known Answer Test for Embedded Cryptographic Algorithms

- It is acceptable for the cryptographic module not to perform a KAT on the embedded core cryptographic algorithm implementation if;
  - the higher cryptographic algorithm uses that implementation,
  - the higher cryptographic algorithm performs a KAT at power-up and,
  - all cryptographic functions within the core cryptographic algorithm are tested (e.g. encryption and decryption for DES and Triple-DES).

9.3 KAT for Algorithms used in an Integrity Test Technique

- 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).

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

- A KAT for each implemented SHS algorithm
  - efficiencies allowed when hash truncation occurs
- 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 that is supported by the module; and,
  - at minimum, any one of the implemented underlying SHS algorithms used by the higher cryptographic algorithm.
- 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(2m)*); 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.

NIST

- **Randall J. Easter** – Director, CMVP, NIST
  reaster@nist.gov

CSE

- **Jean Campbell** – Technical Authority, CMVP, CSE
  jean.campbell@CSE-CST.GC.CA