Demystifying FIPS 140 Series Compliance

Understanding its Importance, Validation, and Certification

Ken Foster
August 7, 2016

Table of Contents

What is FIPS 140 Series Compliance?

The Federal Information Processing Standard (FIPS) is a series of requirements intended to standardize the secure implementation and execution of cryptographic modules used in the protection of information. The standard is maintained by the National Institute of Standards and Technology (NIST). These standard address the "cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks" [1].

What is the difference between FIPS 140-1 and 140-2?

FIPS 140-1, originally established in March 1995, provided the initial set of guidelines for the secure implementation of cryptographic modules. Prior to these guidelines, individual vendors were free to use various crypto libraries or implement home-grown algorithms without regard for compatibility or secure implementation. These original guidelines are still available for review from NIST [2]. This standard was retired on May 25, 2002 and is only provided for legacy devices whom are incompatible with the new standard and are in midst of transition. In 2016, any device still using the FIPS 140-1 standard would be considered non-compliant and in an at-risk of configuration. In May 2001, NIST updated the standards to address new cryptographic risks with the release of FIPS 140-2 [1]. The rigor of FIPS 140-2 includes four graduated security levels dependent on the sensitivity of the information under protection. The publication also directs the Independent Validation (Derived Test) of the implemented cryptographic modules by an accredited laboratory [3].

Why is it important to Protecting Government Information?

"FIPS 140-2 precludes the use of unvalidated cryptography for the cryptographic protection of sensitive or valuable data within Federal systems. Unvalidated cryptography is viewed by NIST as providing no protection to the information or data - in effect the data would be considered unprotected plaintext. If the agency specifies that the information or data be cryptographically protected, then FIPS 140-2 is applicable. In essence, if cryptography is required, then it must be validated" [4]. This standard is an evaluated condition for organizations measured under PCI-DSS, HIPPA, and NIST 800-53 compliant requirements. In California, Attorney General Kamala Harris has defined expected measures required to protect citizen data [5]. Organizations that to not comply are in effect failing to implement "Reasonable Security" measures. A breach resulting from a compliance failure could result in a breach of trust with our citizens, penalties, costs associated with post-incident protection services, and civil liability.

Determining Device Operational Modes?

Step 1: Associating Compliance Controls with Cryptographic Measures?

Compliance standards are continually updated, so users should always consult the current materials for the best information on this topic. This guide favors the NIST compliance regiment throughout the publication. However, because many government entities are required to comply with multiple standards, where appropriate, those standards are addressed. With regards to NIST within this guide, the level of compliance protection is assumed at the "Moderate" level. Based on this standard, the following minimum controls (Table 1) are encumbered by cryptographic requirements:

Table 1. NIST Controls Impacted by Cryptographic Protections

Control	Title
AC-17(2)	Remote Access | Protection of Confidentiality and Integrity
AC-18(1)	Wireless Access | Authentication and Encryption
AC-19(5)	Access Control for Mobile Devices | Full Device / Container Encryption
SC-7(21)	Boundary Protection | Isolation of System Components
SC-8	Transmission Confidentiality and Integrity
SC-12(1)	Cryptographic Key Establishment and Management | Availability
SC-28(1)	Protection of Information At-Rest | Cryptographic Protection

For entities whom have PCI-DSS implications for processed and stored information [6], related controls are provided (Table 2).

Table 2. PCI-DSS Version 3.2 Controls Impacted by Cryptographic Protections

2.1.1(a)	Wireless Environments | Encryption Key Change
2.1.1.(d)	Wireless Environments | Firmware Support for Strong Encryption
2.3(a)	Non-Console Administrative Access | Encrypted with Strong Encryption
3.4.1	Primary Account Number Unreadable When Stored | Disk Encryption of Information
3.6(a)	Cryptographic Key Mgt | Process and Procedure Documentation
3.6.5(c)	Cryptographic Key Mgt |Retired or Replaced Retained Keys use only for decryption / verification operations
4.1(d)	Strong Cryptographic Protocols in Use | Proper Strength implemented
4.1.1	Strong Cryptographic Protocols in Use | Industry Best Practice for Strong Encryption Implementation for Wireless transmission in use

Finally, for entities whom have HIPPA implications for processed and stored information [7], related controls are provided (Table 2).

Table 3. Health Insurance Portability and Accountability Act (HIPPA) Controls Impacted by Cryptographic Protections

4.14(8)	Access Control | Automatic Logoff and Encryption / Decryption
4.16(2)	Integrity | Identify Any Possible Unauthorized Sources for Intercept / Modification
4.17(3)	Person / Entity Authentication | Select / Implement Authentication Option
4.18(4)	Transmission Security | Implement Encryption

Step 2: Determine Devices impacted by Step 1 Controls:

Next, we must determine what devices should be operating in FIPS mode. Based on the controls and their focus, we can narrow down the devices impacted by FIPS 140-2. There are generally four common areas most entities should consideration. However, a thorough review of your network and business process architecture should be conducted to identify unique requirements. For this guide, minimally consider the following areas:

1. Remote Network Access providers (e.g. VPN and External Remote Access Tools)
2. Cloud Repositories and Remote Compute Environments (e.g. FEDRAMP, Amazon, State Data Centers, etc…)
3. Data In-Transit Devices (e.g. Site-to-Site Tunnels, MPLS Mesh Networks, Wireless Access Points, etc…)
4. Data At-Rest Repositories (e.g. Data Stores, Document Repositories, File Servers, workstations, Mobile Devices, Removable Storage Devices, etc…)

Step 3: Determine the Current FIPS Operational Mode:

This is a complex process where the phrase “Trust, but Verify” [8] is best adopted. It’s not uncommon for vendors to unintentionally misrepresent their FIPS compliance based on a generally accepted algorithm instead of an independently validated implementation. At the end of the day you are the one whom must perform the due diligence to verify their claims. Begin this process by determining how your vendor represents their FIPS compliance within their provided Appliance / Application / or Operating System. This should be documented in their technical guidance. If you are unable to locate this information, open a support ticket and ask for the appropriate steps. Always defer to the vendor directions for this procedure. A list of common perimeter checks is provided (Appendix A). It’s important to remember, FIPS is often a separately licensed option on appliances and devices. If your device is not in FIPS mode, then you are not FIPS compliant for that device(s) even if the vendor supports that configuration. Entering FIPS mode can have impacts on performance and intra-lata communications. Always understand those impacts on the configuration is prior to implementation within production environments. For new implementations, attempting this within a test environment is always the best course of action.

Step 4: Does My Vendor Have a FIPS Certificate of Compliance?

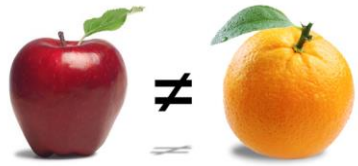
If your device is in FIPS mode, then next step is to verify vendor implementation compliance. Certificates of Compliance are issued to vendors whom have successfully undergone a rigorous independent validation testing regiment. The certificate attests to a specific firmware / software version(s) and configuration(s). Deviation from any of these caveats invalidates your compliance. Often in hardware, additional physical and application security measures are required in addition to the encryption implementation. Vendors often provide a FIPS Configuration guide to assist users in understanding the steps and impacts of these deployments. Because certification is version specific, remember that upgrading to the most current firmware or build could render the device non-compliant.

Verifying Certification of Vendor Hardware / Software:

To check if the vendor is compliant, go to: http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm and search for the vendor in question. This list is continuously updated but honestly omissions can happen. If you can't find your vendor and device listed, all is not lost. Call your vendors technical support team and ask for a copy of the certificate. An example certificate is provided (Appendix B). If the certificate is for a different entity, its likely not going to apply to your device. This is because compliance is based on two generate considerations. The trustworthiness and leak protections implemented in the algorithm and the vendors' implementation within the software / hardware and including additional configured protections. If you are not sure, call the Cryptographic Module Validation Program team and they can assist you in determining if the provided certificate covers the implementation in question [9].

Is a Common Criteria (CC) Certification and FIPS 140-2 the Same?

No, it's a common mistake to assume that a Common Criteria certification is a substitute for a FIP 140-2 certificate of compliance. "The Common Criteria (CC) and FIPS 140-2 are different in the abstractness and focus of tests. FIPS 140-2 testing is against a defined cryptographic module and provides a suite of conformance tests to four security levels. FIPS 140-2 describes the requirements for cryptographic modules and includes such areas as physical security, key management, self-tests, roles and services, etc. The standard was initially developed in 1994 - prior to the development of the CC. CC is an evaluation against a created protection profile (PP) or security target (ST). Typically, a PP covers a broad range of products. A CC evaluation does not supersede or replace a validation to either FIPS 140-1 or FIPS 140-2. The four security levels in FIPS 140-1 and FIPS 140-2 do not map directly to specific CC EALs or to CC functional requirements. A CC certificate cannot be a substitute for a FIPS 140-1 or FIPS 140-2 certificate" [3].



Enforcing FIPS in Operating Systems

Windows Operating Systems:

In Microsoft Windows © operating Systems, the term "FIPS Mode" refers to implementing a series of security policies and forced use of approved modules. Microsoft provides a step-by step guide for implementation of stand-alone and Domain Joined hosts [10] for meeting FIPS compliance.

Linux Operating Systems:

Red Hat Linux (RHL) / CentOS ©

Versions 6 [11] and 7 [12] have implementation instructions provided by the vendor; see the references provided.

Other Linux Operating Systems

A search didn't render a mature document for other Operating Systems. In most cases, only references to Apache Open SSL modifications were detected. Other components under consideration include SSH daemons, and shadow file encryption algorithms used.

AIX © Operating Systems:

IBM AIX procedures are provided [13], although a call to technical support is likely a better option since there are a number issues to deal with based on your implemented version.

What can I do if My Device / Hardware / Software is Non-Compliant?

If you have determined the solution currently implemented is non-compliant, you need to ask the following questions:

- Can I upgrade or license an approved module from this current vendor?
    - Did my original Statement of Work (SOW) require FIPS compliance?
    - Do I have contractual recourse?
- Do I need to find a new vendor; if so what is the operational impact on back-end business processes?
    - Do I need a consultant to evaluate impact and make vendor recommendations?
    - Does the current back-end impacted vendor have a list of known integrating solutions that work with their product?
        - Are those certified?
- Do I need to suspend remote access or access from untrusted network segments until a solution can be implemented?
- Does this finding require reporting to a Federal or State regulatory agency?
    - How does this impact my current Risk Assessment?

- Do I need to disclose this issue to peer entities as part of an existing agreement?

Once you have answered these questions, this will drive your next steps within the remediation process. This begins with documenting your findings in writing to management. This ensures that the appropriate decision makers are formally notified and the process of remediation can be documented. Mistakes happen and mature organizations work to resolve them. If an entity were to not take remediation steps to solve the issue, they would be failing to meet the definition of "Reasonable Security", thus potentially liable under the law. That's will result in a "lose lose" scenario for management, the technical staff, and most importantly the citizens whom the entity is charged to support.

Works Cited

[1] National Institute of Standards and Technology (b), "Security Requirements for Cryptographic Modules (FIPS 140-2)," 25 May 2001. [Online]. Available: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf. [Accessed 16 March 2013].

[2] National Institute of Standards and Technology (a), "FIPS Publication 140-1," March 1995. [Online]. Available: http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-1/1401test.pdf. [Accessed 7 August 2016].

[3] National Institute of Standards and Technology (c), "Derived Test Requirements for FIPS Publication 140-2," 4 January 2011. [Online]. Available: http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402DTR.pdf. [Accessed 7 August 2016].

[4] National Institute of Standards and Technology (d), "Cryptographic Module Validation Program (CMVP)," 1 February 2016. [Online]. Available: http://csrc.nist.gov/groups/STM/cmvp/. [Accessed 7 August 2016].

[5] State of Calfornia Attorney Generals Office, "California Data Breach Report 2016 - Security-based Standards - Recommendation 1," February 2016. [Online]. Available: https://oag.ca.gov/breachreport2016. [Accessed 7 August 2016].

[6] PCI Security Standards Council, "Self-Assessment Questionnaire D, Version 3.2," April 2016. [Online]. Available: https://www.pcisecuritystandards.org/documents/PCI-DSS-v3_2-SAQ-D_Merchant.pdf?agreement=true&time=1470587716193. [Accessed 7 August 2016].

[7] National Institute of Standards and Technology (e), "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule," October 2008. [Online]. Available: http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/nist80066.pdf. [Accessed 7 August 2016].

[8] N. Porzucki, "Suzanne Massie taught President Ronald Reagan this important Russian phrase: 'Trust, but verify'," 7 March 2014. [Online]. Available: http://www.pri.org/stories/2014-03-07/suzanne-massie-taught-president-ronald-reagan-important-russian-phrase-trust. [Accessed 7 August 2016].

[9] National Institute of Standards and Technology (f), "Contacts," 28 July 2015. [Online]. Available: http://csrc.nist.gov/groups/STM/cmvp/contacts.html. [Accessed 7 August 2016].

[10] Microsoft Incorporated, "FIPS 140 Validation," May 2014. [Online]. Available: https://technet.microsoft.com/en-us/library/security/cc750357.aspx. [Accessed 7 August 2016].

[11] Red Hat Incorporated (b), "Chapter 9.2 Federal Information Processing Standard (RHL 6.8)," nd. [Online]. Available: https://access.redhat.com/documentation/en-

US/Red_Hat_Enterprise_Linux/6/html/Security_Guide/sect-Security_Guide-Federal_Standards_And_Regulations-Federal_Information_Processing_Standard.html. [Accessed 7 August 2016].

[12] Red Hat Incorporated (a), "Chapter 7. Federal Standards and Regulations (RHL 7)," nd. [Online]. Available: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/Security_Guide/chap-Federal_Standards_and_Regulations.html. [Accessed 7 August 2016].

[13] International Business Machines Incorporated, "The db2ssh tool and FIPS," nd. [Online]. Available: http://www-01.ibm.com/support/docview.wss?uid=swg21617590. [Accessed 7 August 2016].

Appendix A – Common Perimeter Devices – Determining FIPS Operational Configuration Status

Juniper (Pulse) Netscreen: In CLI: get system

BlueCoat VPN: In CLI: show version

Cisco Products: show running-config fips

Palo Alto Appliances: *FIPS-CC* will display at all times in the status bar at the bottom of the web interface

McAfee Sidewinder Firewalls: cf -T fips query

Dell Sonicwall Appliances: *In GUI: System* | *Settings* | *Locate FIPS Mode* | *validate status setting*

F5 Appliances: In CLI: tmsh | run util fips-util info

Citrix Netscaler: In CLI: show ssl fips

** Note: Always consult the appropriate vendor prior to using these steps to ensure they are appropriate for your device and build version. Use these steps at your own risk.

Appendix B – FIPS Example Certification Certificate

FIPS 140-2 Consolidated Validation Certificate

The National Institute of Standards and Technology of the United States of America

The Communications Security Establishment of the Government of Canada

Consolidated Certificate No. 0005

The National Institute of Standards and Technology, as the United States FIPS 140-2 Cryptographic Module Validation Authority; and the Communications Security Establishment Canada, as the Canadian FIPS 140-2 Cryptographic Module Validation Authority; hereby validate the FIPS 140-2 testing results of the cryptographic modules listed below in accordance with the Derived Test Requirements for FIPS 140-2, Security Requirements for Cryptographic Modules. FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting Sensitive Information (United States) or Protected Information (Canada) within computer and telecommunications systems (including voice systems).

Products which use a cryptographic module identified below may be labeled as complying with the requirements of FIPS 140-2 so long as the product, throughout its life-cycle, continues to use the validated version of the cryptographic module as specified in this consolidated certificate. The validation report contains additional details concerning test results. No reliability test has been performed and no warranty of the products by both agencies is either expressed or implied.

FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range and potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of a cryptographic module.

The scope of conformance achieved by the cryptographic modules as tested are identified and listed on the Cryptographic Module Validation Program website. The website listing is the official list of validated cryptographic modules. Each validation entry corresponds to a uniquely assigned certificate number. Associated with each certificate number is the module name(s), module versioning information, applicable caveats, module type, date of initial validation and applicable revisions, Overall Level, individual Levels if different than the Overall Level, FIPS-approved and other algorithms, vendor contact information, a vendor provided description and the accredited Cryptographic Module Testing laboratory which performed the testing.

Signed on behalf of the Government of the United States

Signature: _____

Dated: 6/20/2011

Chief, Computer Security Division
National Institute of Standards and Technology

Signed on behalf of the Government of Canada

Signature: _____

Dated: 23 June, 2011

Director, Architecture & Technology Assurance Group
Communications Security Establishment Canada

Page 1 of 4 5/16/2011

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm

Certificate Number	Validation / Posting Date	Module Name(s)	Vendor Name	Version Information
1498	04/01/2011	DataSecure Appliance i150 and i450	SafeNet, Inc.	Hardware Versions: P/Ns 947-00150-001 and 947-000031-001; Firmware Version: 4.9.0
1508	03/02/2011	ASTRO CDEM Motorola Advanced Crypto Engine (MACE)	Motorola, Inc.	Hardware Version: P/N 5185912Y01; Firmware Version: R01.01.01
1523	04/05/2011	Athena IDProtect	Athena Smartcard, Inc.	Hardware Version: P/N AT90SC28872RCU Revision G; Firmware Version: 010B.9288.0303
1525	04/01/2011	Xirrus Wi-Fi Array XS4 and XS8	Xirrus, Inc.	Hardware Versions: P/Ns: 190-0092-002 Rev D1 [XS4] and 190-0091-005 Rev A1 [XS8]; Firmware Version: 3.5
1527	03/28/2011	LOK-IT™ 10 KEY (Series SDG003FM) and LOK-IT™ 5 KEY (Series SDG004FP)	Systematic Development Group, LLC	Hardware Versions: 100-SDG003-33LF REV:1 (10 Key) and 100-SDG004-00LF REV:1 (5 Key); Firmware Version: USB Controller Firmware Revision V01.12A09-F01 (10 Key and 5 Key); Security Controller Firmware Revisions SDG003FM-008 (10 Key) and SDG004FP-008 (5 Key)
1528	03/30/2011			
1529	04/01/2011	Cisco 881, Cisco 881G and Cisco 891 Integrated Services Routers (ISRs)	Cisco Systems, Inc.	Hardware Versions: 881, 881G, 891 and [FIPS Kit (CISCO-FIPS-KIT=), Revision -B0]; Firmware Version: 15.1(2)T2A
1530	04/04/2011			
1531	04/12/2011	RFS7000 RF Switch	Motorola, Inc.	Hardware Version: RFS7000; Firmware Version: 4.1.0.0-040GR
1532	04/12/2011	NetLib® Encryptionizer® DE/FIPS	NetLib®	Software Versions: 2010.201.10.0 and 2010.501.10.0

Page 2 of 4 5/16/2011