FIPS 140-2 and You!

Josh Michaels, 2012-07-06

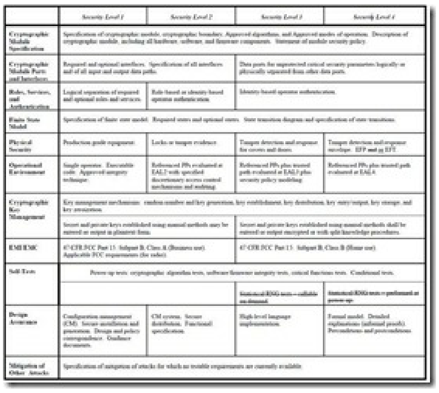
FIPS 140-2 and you?

FIPS.. the final frontier. These are the voyages of the Business Enterprise. To boldly send traffic where no one has sent before. To much? Perhaps, FIPS! The eternal pain in the butt? Whatever your opinion of FIPS 140-2, it’s here and it is not going anywhere soon.

FIPS stands for Federal Information Processing Standard. It is a collection of standards that the United States Federal government uses as requirements within government agencies. The standards are often used in the private sector as well to establish a baseline of requirements.

WARNING! This document is not a comprehensive FIPS guide. It’s a humanized version. Even so, grab a cup of coffee before you begin reading… or put the beer on ice.

The FIPS document we are looking at today is the infamous 140-2 “Security Requirements for Cryptographic Modules”. It’s an engaging 61 pages of wonderful, enamoring tales of encryption glory. That might be a bit of a stretch. It actually took 2 espressos and a 2 hour plane ride to force myself through it the first time. There are 11 separate disciplines with four levels of security. So, let me save you the lost sleep and show you the summary:



	Security Level 1	Security Level 2	Security Level 3	Security Level 4
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP and or EFT.
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
			Statistical RNG tests – callable on demand.	Statistical RNG tests – performed at power-up.
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and postconditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

Understand? Good, let’s go get some nachos!
No? Well here are some details

1: Cryptographic Module Specification:

Essentially this part defines the documentation and implementation that is required for a crypto module. It defines modes of operation (Approved security functions vs non approved as defined by ANNEX A (http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf). Example would be AES is approved, DES is not)

The documentation is fairly extensive including requirements of all security functions, approved and not, block diagrams, hardware design, and any security information

“whose disclosure or modification can compromise the security of the cryptographic module.”

Which seems to translate to

“ Any way someone can get into the module, get data from the module, admin the module”

2: Cryptographic Module Ports and Interfaces

This can be summed up as “how things get in and out of the module”. It defines 4 distinct interfaces (can be logical or physical depending on security level):

Data Input Interface: All data coming in, except for control data.
Data Output Interface: All data leaving, except for status output.
Control Input Interface: Input commands, switching and control data.
Status Output Interface: Signals, indicators, and status data that includes LED light signals, etc.

For level 1 and 2 security, you can have the input and output share physical and logical ports with other ports on the module.

At Level 3 and 4, the input and output of crypto components must be on a separate physical port or logically separated on a trusted path. And entries into the module must be made directly into the cryptographic module.

3: Roles, Services, and Authentication

-Roles-
They want all Crypto modules to have at least the following roles:
User Role: General security services, crypto operations and Approved Security Functions (remember appendix A?)

Crypto Officer role: Perform crypto initialization and management (Examples: putting keys in and out, auditing, etc)

And, if the module has a maintenance service, there has to be a:

Maintenance Role: For physical and logical maintenance/diagnostics. If you enter this role, all secrets, private keys, and unprotected CSPs (Critical Security Parameters) have to be zero’d out when entering or exiting the role.

-Services-
The standard requires that a module support at least 3 services:
Show status: How’s the module doing/what’s going on?
Perform Self Test: Run a self test on the unit (which they go on to specify later in the standard, how nice of them)
Perform Approved Security Function: Do some crypto.

Of course, they again require thorough documentation of the services provided.

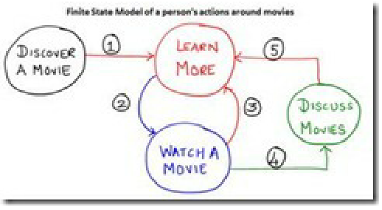
Operator Authentication
Role-based versus Identity based:
Identity based is basically equated to “You can prove who you are, you get certain rights” whereas role-based is “Select what you role you want, and I’ll give you that power, and I’ll authenticate the role has rights.”

Security Level 1: Does not require authentication. If you don’t use any authentication, you must require roles be chosen by the operator.

Security Level 2: Employ Role-Based authentication

Security Level 3/4: Employ Identity-based authentication

4: Finite State Model

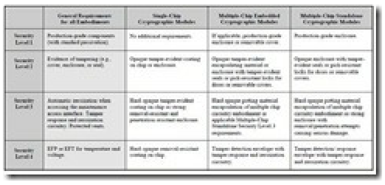


Essentially… have one that if fully defined.

5: Physical Security

They defined 3 specific instances for physical security:

Single Chip (IE: soldered on motherboard)
Multi-chip embedded (Expansion Cards)
Multi-chip Stand alone (separate boxes)



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

There are some specific examples as you go up the chain, but the easiest way to think about it:

Security Level 1: The cash box you used at the bake sale, the one with the single wafer lock.

Security Level 4: Fort Knox, suspended over a lava pit by a single rope guarded by a caffeinated monkey wielding a machete to cut the rope.

6: Operational Environment

Fancy words for “the stuff needed for the module to work”. Does it need special firmware, flash, or is it built into an OS? No matter the environment, it has to be documented and meet requirements for each security level.

Security level 1:
OS must be single user mode. All processes started by the module must remain owned by it. No other processes can access the keys, CSP, or the key generation values while the module is operational. The software/firmware must have protections against unauthorized disclosure and modification (vague eh?)

The crypto software/firmware must make use of Approve Integrity Techniques. (Message auth code or DSA).

Security Level 2:
All of level 1 plus:

OS must meet functional requirements of Common Criteria evaluation assurance level 2 (http://www.niap-ccevs.org/pp/pp_gpospp_v1.0.pdf)

Meet a slew of specific access requirements and implement an auditing trail.

Security Level 3:
All of 1 and 2, plus:

Adding in the OS requirement of Trusted Path and Informal TOW security policy model.

It reiterates the requirement for trusted path usage for all input and output of cryptographically important information.

Security Level 4:
All of 1,2, and 3 plus required to meet an EAL4 common criteria.

Coffee Break! Now's a good time to grab a fresh cup or a nice pour of Macallan 30 year.

7: Cryptographic Key Management

This covers the entire lifetime of the keys, from generation to disposal. All secrets must be protected from disclosure, modification and substitution. All public keys must be protected from modification and substitution.

-Random Number Generators-
Must use an approved generator and still pass the cryptographic algorithm checks (thankfully defined later in the doc)

Oh look.. another appendix Approved Random Number Generators (http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf)

-Key Generation-
Essentially, figuring out how the keys were made should be just as hard as figuring out the key. And if you let someone put in the seed for a key, they have to do it securely.

-Key Establishment-
Man, this is a tough one. If only I had an appendix to help… well lookie here! Appendix D: Approved Key Establishment techniques (http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf) . This one actually leads you down a rabbit hole all the way to: SP800-56A "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" http://csrc.nist.gov/publications/nistpubs/800-56A/SP800-56A_Revision1_Mar08-2007.pdf

-Key Entry and Output-
Completed securely and completely documented in how keys come in and out. They must be encrypted using an Approve Algorithm.

Security Level 1&2: secrets and private keys created automatically must be entered and output in encrypted form. If they are established via manual methods, they can come in and out in plaintext form.

Security Level 3&4: Manual Method secrets should be input and output encrypted or it can use a “split knowledge” procedure. The key comes out in two pieces, via a trusted path, to an authenticated operator.

-Key Storage-

You can store keys in plaintext or encrypted, it just should be locked down so that no unauthorized access can get at them. Also need to be sure the keys are associated with an entity.

-Key Zeroization-

I like that word.. Zeroization. Has a nice ring to it. Basically, the module has to have a way to erase the secrets, CSPs, etc.

8: Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)

Security level 1&2:
Must conform to “47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).”

Security level 3&4:
Must conform to “47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).”

Well, that makes me feel a little safer…

9: Self-Tests

Ya, the system should be able to check and make sure its working.

Power-up tests:
Happen every time the module comes up. They call out specifically a

Cryptographic Algorithm Test: Take a known answer for each crypto function and run a test to be sure the function gives you that answer. If it doesn’t, fail. (Or at security level 5, self destruct!)

Software Integrity Test: Check and make sure the software hasn’t changed (MAC, DSA).

Critical Functions Test: Anything else required for the module to work.

And of course, everything must be fully documented (what is tested, how it’s tested, where it’s tested, etc)

10: Design Assurance

If you build it, they will break it… so build it right. The design assurance requirements all revolve around making sure that modules are developed securely and documented thoroughly (and they mean thoroughly). It also goes on to talk about what the user manual should contain for both the crypto officer and standard operator. Basically, the crypto officer guide needs to cover all tasks in depth, while the user guide can be limited to approved security functions and user responsibilities.

11: Mitigation of Other Attacks

Leave it to NIST to save the best section for last. This brief portion speaks to a few of the known attacks on crypto modules, including “TEMPEST”. Sounds cool right? Tempest refers to collecting electromagnetic signals emitted from a module, then using those signals to try obtaining keystrokes, images, etc.

Congratulations, you’ve successfully made it through a humanized version of the NIST 140-2 document. Hopefully you found this a bit softer read.

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com