INTRODUCTION TO FIPS 140-2

Steve Weingart

Public Sector Certifications

Contents

- Rationale
- Explaining the Crypto Module Validation Program
- What is a Cryptographic Module?
- FIPS 140-2: an introduction
  - –Brief run through of the standard
- Testing!–The Derived Test Requirements
- Cryptographic Algorithm Validation

FIPS: An Overview

- **FIPS are a series of U.S. Federal Information Processing Standards.**
- **FIPS are mandatory to Federal agencies, e.g., NSA, CSI, NIST.**
- **They are not mandatory to individual US states, but are often used by them.**
- **They are often adopted by non-government agencies, other countries and other standards (such as Common Criteria).**

Mandate

With the passage of the Federal Information Security Management Act (FISMA) of 2002, there is no longer a statutory provision to allow for agencies to waive mandatory Federal Information Processing Standards (FIPS). The waiver provision had been included in the Computer Security Act of 1987; however, FISMA supersedes that Act. Therefore, the references to the "waiver process" contained in many of the FIPS are no longer operative.

FIPS 140-2 is therefore mandatory for US Government use.

Mandatory for Federal Cryptography

The FIPS 140-2 standard:

- **Is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems).**
- **Shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract.**
- **Precludes the use of unvalidated cryptography for the cryptographic protection of sensitive or valuable data within Federal systems.**

Mandatory for Federal Cryptography

- **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.**

THE CRYPTOGRAPHIC MODULE VALIDATION PROGRAM

What is the Program?

- **Cryptographic Module Validation Program (CMVP)**

- **A joint program between:**
  - **The U.S. NIST (National Institute for Standards and Technology)**
  - **The C.S.E. (Communications Security Establishment) of the Government of Canada**

Accredited Laboratories

- **ISO/IEC 17025**
- **In the US: Handbook 150 and HB 150-17**
- **Accredited by National Voluntary Laboratory Scheme (NVLAP) as an IT Security Laboratory**
- **Approved by the CMVP**
- **Laboratories are not allowed to perform consulting on the design of the cryptographic module.**

Conformance Testing

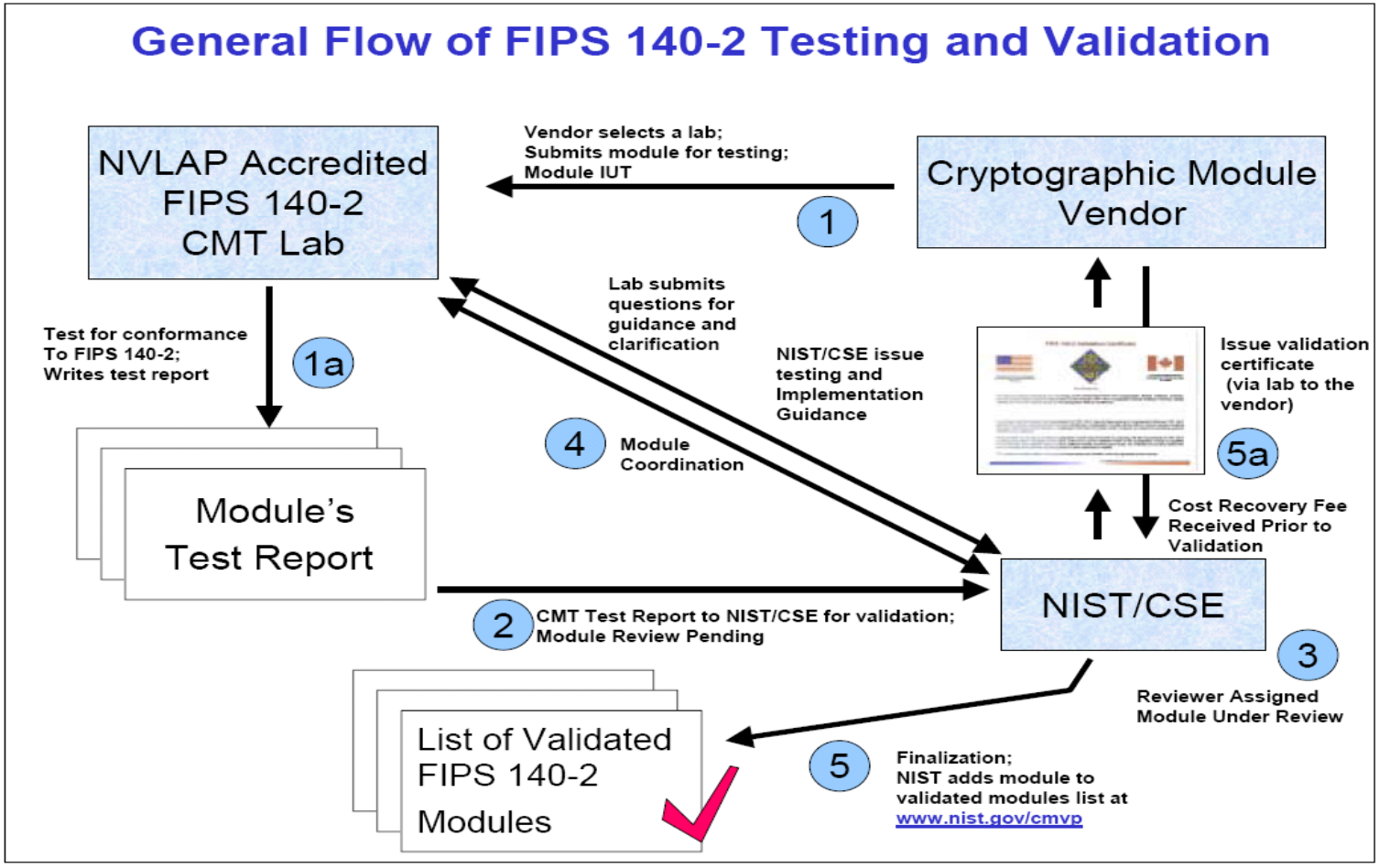
This validation program is about testing a product for

CONFORMANCE

to a standard specification:

FIPS 140-2

The Validation Process



WHAT IS A CRYPTOGRAPHIC MODULE?

What is a Cryptographic Module?

- **A cryptographic module is defined by its:**
  - Security Functionality
  - Boundaries
- **A cryptographic module can be embodied in:**
  - Hardware
  - Software
  - Firmware
  - Or a Hybrid

Security Functionality of a Cryptographic Module

- Symmetric Key Cryptography
- Asymmetric Key Cryptography
- Hashing
- Message Authentication (Keyed Hashes)
- Random Number Generators
- Key Management

The Cryptographic Boundaries

- **Physical**
  - Must be contiguous.
  - Is often a hard case.
  - (Some cryptographic modules have cryptographic modules within them.)
- **Logical**
  - Describes the boundary of the software components.

Security Objectives

- **To employ and correctly implement the Approved security functions for the protection of sensitive information.**
- **To protect a cryptographic module from unauthorized operation or use.**
- **To prevent the unauthorized disclosure of the contents of the cryptographic module, including plaintext cryptographic keys and CSPs.**
- **To prevent the unauthorized and undetected modification of the cryptographic module and cryptographic algorithms, including the unauthorized modification, substitution, insertion, and deletion of cryptographic keys and CSPs.**

Security Objectives

- **To provide indications of the operational state of the cryptographic module.**
- **To ensure that the cryptographic module performs properly when functioning in an Approved mode of operation.**
- **To detect errors in the operation of the cryptographic module and to prevent the compromise of sensitive data and CSPs resulting from these errors.**

FIPS 140-2: AN INTRODUCTION

History and Evolution

ISO/IEC 19790	ISO/IEC 19790 2nd Ed
2006	2012

Federal Standard 1027	FIPS 140 (Fed Std 1027)	FIPS 140-1	FIPS 140-2	FIPS 140-2 Change Notices
1982	Not Used	1994	2001	2002

FIPS 140-3
Est. 2013

Today

FIPS 140-2: an Overview

- **FIPS 140-2 was published in 2001.**
- **Change notes were added in 2002.**
- **FIPS 140-2 has recently been reviewed and FIPS 140-3 is currently in the decision stage, Using ISO 19790 is the more likely scenario going forward.**

The Key Documents

FIPS 140-2
Security Requirements for Crytographic Modules

Appendix "A" Summary of documentation Requirements
Appendix "B" Recommended Software Development Practices

Appendix "C" Crytographic Module Security Policy

Appendix "D" Selected Bibliography

Annex "A"
Approved Security Functions for FIPS PUB 140-2. (draft)

Annex "B"
Approved Protection Profiles for FIPS PUB 140-2. (draft)

Annex "C"
Approved Random Number Generators for FIPS PUB 140-2. (draft)

Annex "D"
Approved Key Establishment Techniques for FIPS PUB 140-2. (draft)

Derived Test Requirements (DTR)

Implementation Guidance

FIPS 140-2: Functional Areas

- **FIPS 140-2 is divided into 11 functional areas.**
- **Each area is awarded a Security Level between 1 and 4 depending on the requirements that it meets.**
- **The module as a whole is awarded an "Overall Security Level," which is the lowest level awarded in any of the levels.**

FIPS 140-2: Functional Areas

Cryptographic Module Specification

Cryptographic Module Ports and Interfaces

Roles Services and Authentication

Finite State Model

Physical Security

Operational Environment

Cryptographic Key Management

FIPS 140-2: Functional Areas (cont)

EMI/EMC

Self Tests

Design Assurance

Mitigation of Other Attacks

Security Levels

	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 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.			
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.			

Crypto Module Specification

- **Ensure the boundaries are described Security Policy document**
  - Physical
  - Logical

Ports & Interfaces

- All entry and exit points must be defined
- 4 logically distinct interfaces
  - Data Input
  - Data Output
  - Control Input
  - Status Output
- And, optionally
  - Separate external power interface
  - Key Loader
- At security level 3 and 4 physical ports must be physically separate

Roles, Services and Authentication

A cryptographic module shall support authorized roles for operators and corresponding services within each role.

- Multiple roles may be assumed by a single operator.
- If a cryptographic module supports concurrent operators, then the module shall internally maintain the separation of the roles and the corresponding services:
  - User Role
  - Crypto Officer Role
  - Maintenance Role (if applicable)
  - Optional Additional Roles

Roles, Services and Authentication

- **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.**

Access Control

- **Level 1: no access control required**
- **Level 2: role based access control**
- **Levels 3 and 4: identity based access control**

Finite State Model

- **The operation of a cryptographic module is specified using a finite state model (a state transition diagram and/or a state transition table):**
  - **all operational and error states of a cryptographic module**
  - **the corresponding transitions from one state to another**
  - **the input events that cause transitions from one state to another**
  - **the output events resulting from transitions from one state to another**

Note: The module must be in only one state at a time!

Finite State Model

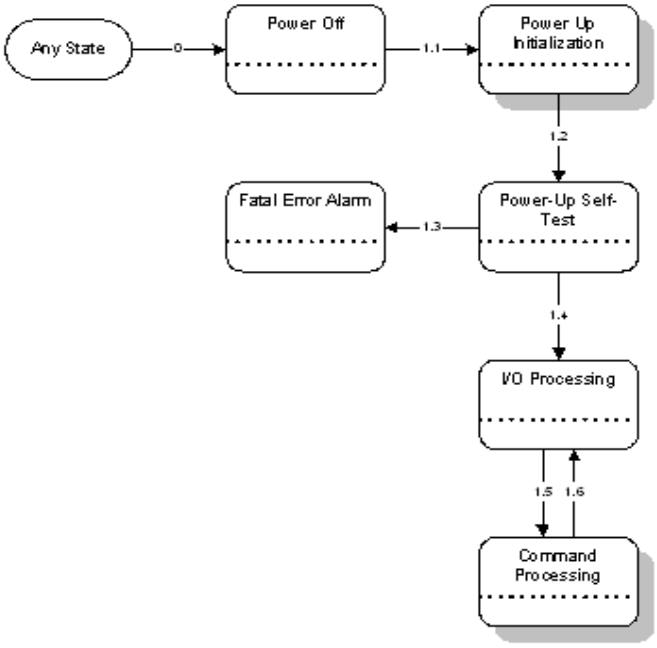


Figure 1. Top Level Finite State Diagram

Finite State Transition Table

Transition	Starting State	Ending State	Reason for Transition	Control / Data Input	Data / Status output
0	Power Off	Power On	Power on	Environment Init	No Data Output
1.1	Power On	Self Test	Initialization in FIPS 140-2 approved mode	Due to power up	No Data Output
1.2	Power On	Power off	Crypto module unloaded	shutdown	No Data Output
2.1	Self Test	Operational	Successful completion of self tests	do_test, do_integrity_check	Operational mode status
2.2	Self Test	Error	Self Test Failure	do_test, do_integrity_check	Operational mode status
3.1	Operational	Error	Conditional tests failed	get_prng_bytes	Operational mode status
3.2	Operational	Power Off	Shut down module	shutdown	No Data Output
4.1	Error	Power Off	Shut down module	shutdown	No Data Output

Physical Security

- **Single Chip**
  - **Single IC Chips, USB Tokens Or Smart Cards With A Single IC Chip**
- **Multiple Chip embedded**
  - **Adapters And Expansion Boards**
- **Multiple Chip standalone**
  - **Encrypting Routers/Network Equipment (us!) Or Secure Radios**

Physical Security

	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.

Table 2: *Summary of physical security requirements*

Operational Environment

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.

Operational Environment

- **The operational environment can be:**
  - Non-modifiable (e.g., firmware contained in ROM, or software contained in a computer with I/O devices disabled),
  - Modifiable (e.g., firmware contained in RAM or software executed by a general purpose computer).
- **The operating system is a critical component of the operating environment of a cryptographic module.**

Cryptographic Key Management

- **The security requirements for cryptographic key management encompass the entire lifecycle of cryptographic keys, cryptographic key components, and CSPs employed by the cryptographic module.**
- **Key management includes random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.**
- **A cryptographic module may also employ the key management mechanisms of another cryptographic module.**

EMI/EMC compliance

- **EMI: Electromagnetic Interference**
  - **Does the module interfere with other equipment?**
  - **EMI is caused by undesirable radiated electromagnetic fields or conducted voltages and currents.**

- **EMC: Electromagnetic Compatibility**
  - **Does other equipment interfere with the module?**
  - **EMC is the ability of electrical or electronic equipment/ systems to function in the intended operating environment without causing or experiencing performance degradation due to unintentional EMI.**
  - **In General, an FCC part 15 class A or B certificate is needed**

Self Tests

- **A cryptographic module shall perform power-up self-tests and conditional self-tests to ensure that the module is functioning properly.**
  - *Power-up self-tests* are performed when the cryptographic module is powered up (including integrity tests).
  - *Conditional self-tests* are performed when an applicable security function or operation is invoked.
- **If a cryptographic module fails a self-test, the module must enter an error state and output an error indicator via the status output interface.**
  - The cryptographic module shall not perform any cryptographic operations while in an error state. All data output via the data output interface shall be inhibited when an error state exists.

Design Assurance

- ***Design assurance* refers to the use of best practices by the developer of a cryptographic module during the design, deployment, and operation of a cryptographic module, providing assurance that the module is developed properly.**
  - –configuration management
  - –delivery and operation
  - –development
  - –guidance documents

Mitigation of Other Attacks

- **Sometimes developers/sponsors claim mitigation of attacks outside the scope of FIPS 140-2 (e.g., SPA, DPA, Light Attacks, Timing Attacks).**
  - If these are claimed in the security policy then they must be verified by the lab or a disclaimer placed in the security policy.

LABORATORY TESTING

THE DERIVED TEST REQUIREMENTS (DTR)

What are the DTR

- **Derived Test Requirements:**
  - –Derived directly from FIPS 140-2
  - –Offers a repeatable and testable basis for conformance tests

What are the DTR

First an assertion: a direct quote from FIPS 140-2.

The assertions are denoted by the form:

AS<requirement_number>.<assertion_sequence_number>.

For example, “AS01.03: (Levels 1, 2, 3, and 4) The operator shall be able to determine when an Approved mode of operation is selected.”

What are the DTR

Next, a set of requirements levied on the vendor. These requirements describe the types of documentation or explicit information that the vendor must provide in order for the tester to determine conformance to the given assertion. These requirements are denoted by the form:

VE<requirement_number>.<assertion_sequence_number>.<sequence_number>.

For example, “VE01.03.01: The vendor-provided nonproprietary security policy shall provide a description of the Approved mode of operation. VE01.03.02: The vendor-provided non-proprietary security policy shall provide instructions for invoking the Approved mode of operation.”

What are the DTR

Finally a set of requirements levied on the tester of the cryptographic module. These requirements instruct the tester as to what he or she must do in order to test the cryptographic module with respect to the given assertion. These requirements are denoted by the form:

- TE<requirement_number>.<assertion_sequence_number>.<sequence_number>

For example, "TE01.03.01: The tester shall verify that the vendor-provided nonproprietary security policy contains a description of the Approved mode of operation."

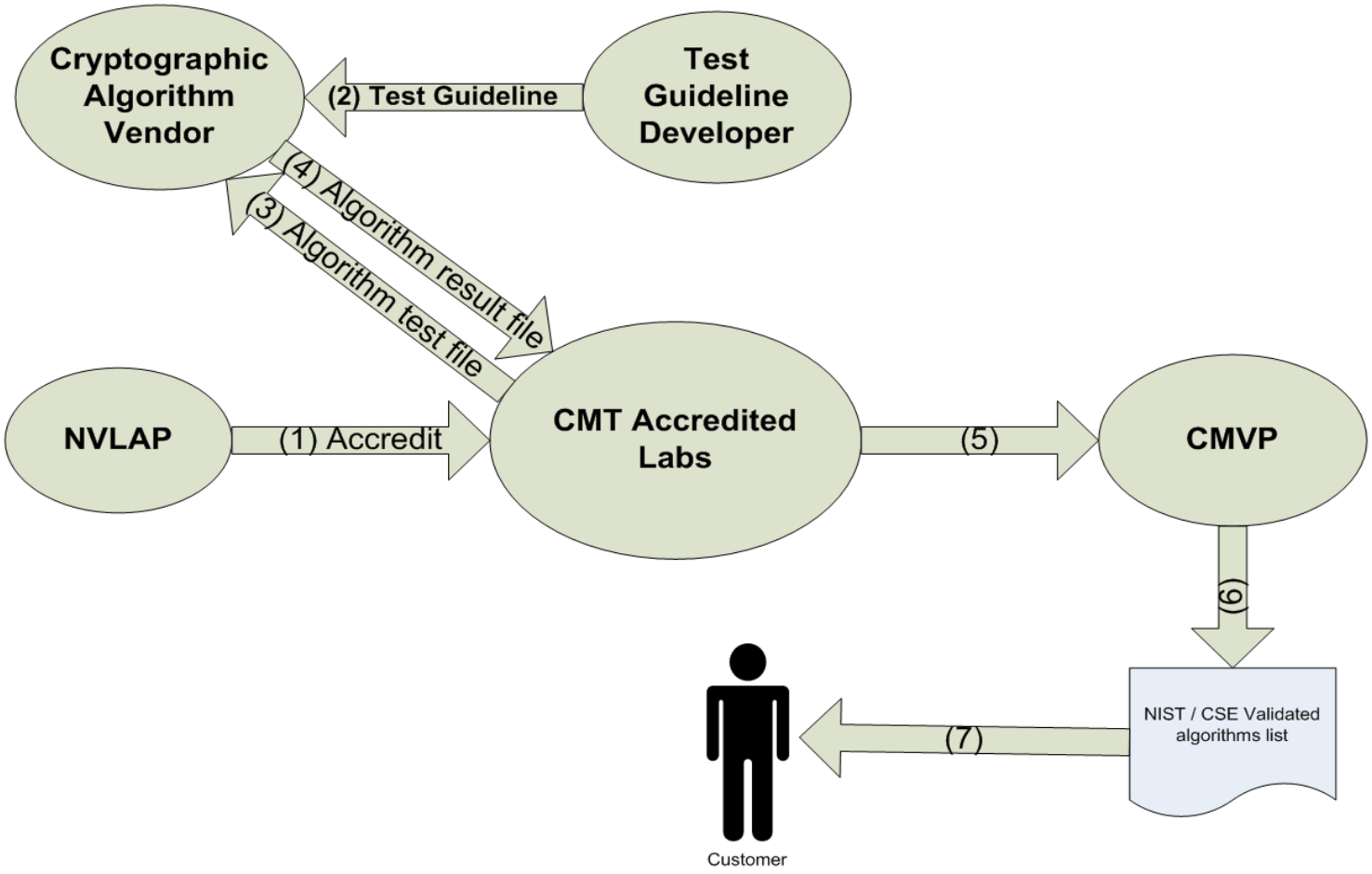
CRYPTOGRAPHIC ALGORITHM VALIDATION

Cryptographic Algorithm Validation

- **Algorithms used in Approved mode must be Validated by the CAVP (cryptographic algorithm validation program)**
- **To prove that they are Implemented correctly.**
- **They are published on a list given at**

http://csrc.nist.gov/cryptval/vallists.htm.

Crypto Algorithm Validation Process



Algorithms

- **Algorithms are validated independently**
- **The currently tested cryptographic algorithm types include**
  - symmetric encryption
  - asymmetric encryption
  - hashing
  - message authentication
  - random number generation

Algorithms

Algorithms are Validated Using the NIST CAVS tool

The Test tool is Provided to the Labs by the CAVP

1. **The Lab Generates Test Samples and Sends them to the Customer**
2. **The Customer Uses the Samples as Input and Generates the Cryptographic Output**
3. **The Customer Returns the Results to the Lab**
4. **The Lab Checks the Results and if They Match, Submits the Results to the CAVP for the Certificate**

Algorithms

- **Important Things to Remember**
- **Encryption and Decryption are Tested Separately**
- **In Counter Mode, the Test is Performed on ECB Mode and then the Counter Design is Examined Separately. It Must be Shown That a Particular Count can Only be Used Once with a Key.**
- **For newer counter modes such as GCM, there are additional requirements as to how the counter and IV are formed**
- **Make Sure That You Can Access the Input and Output of Each Algorithm Directly.**


FIPS
VALIDATED
140-2
™

QUESTIONS/DISCUSSION

Required Documentation (FIPS 140-2 Appendix A)

1) Security Policy
2) Finite State Model
2) Software
3) Hardware
5) Physical security
6) Design Assurance
7) EMI/EMC
8) Mitigation of other attacks (optional)

NOTE: Appendix A can be a difficult read until you understand the terms and intentions

Required Documentation: Security Policy

- Required Elements:
- The requirements for the Security Policy are laid out in FIPS 140-2 Appendix C
- It is primarily a specification for the purpose of the customer and/or user gaining understanding of the module, its function and the correct operation of the module
- Unless the product is ITAR, the security policy will be a public document available from the CMPV website
- The main FIPS 140-2 functions and descriptions must be in the security policy

Required Documentation: Security Policy (cont)

- For the most part, the SP maps the 11 requirements sections
- The module description in terms of implementation functions, security level and block diagrams (HW and SW)
- The list of approved and non-approved functions, ports, roles, services, I & A and access control of each service by role
- Self Tests (this is a big part of FIPS 140-2, it is important to understand the requirements)
- Operational Environment
- Design Assurance

Required Documentation: Security Policy (cont)

- CSP life cycle for all CSPs
- Description of Physical security
- Administrator and user guidance for installation, configuration and setup.
- Mitigation of any other attacks not listed in FIPS 140-2

Required Documentation: Finite State Model

- The module must be depicted and actually operate as a finite state machine
- The module may only be in one state at a time*
- Each state and transition must be described
- There must be a proven match between the model and the implementation (usually code XREF)

* This requirement is not well understood and often ignored

Required Documentation: Finite State Model

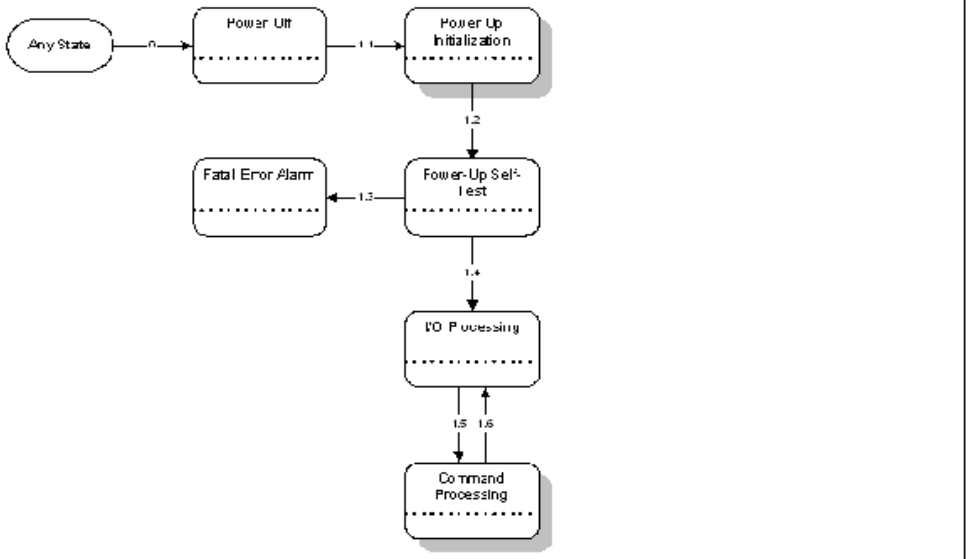


Figure 1. Tcp Level Finite State Diagram

Required Documentation: Finite State Model

TABLE 1 - TRANSITION TABLE FOR TOP LEVEL FINITE STATE DIAGRAM

Trans #	Current State	Next State	Cause of Transition (*Includes internal conditions, data inputs, and control inputs*)	Status Output (*Includes data outputs and final conditions*)	Source Code Reference
0	(Any State)	Power-Off	Removal of Power	None	
1.1	Power-Off	Power-up Initialization	Application of Power		
1.2	Power-up Initialization	Power-up Self-Test	Completion of Power-up Initialization (Module Operational State is set)		
1.3	Power-up Self-Test	Fatal Error Alarm	At least one self-test has failed.		
1.4	Power-up Self-Test	I/O Processing	Successful completion of the Power-up Self-Test		
1.5	I/O Processing	I/O Processing	Completion or termination of the last Command in the chain		
1.6	I/O Processing	Command Processing	Command received		
1.7	Command Processing	I/O Processing	Completion or termination of command		

Required Documentation: Software

- All source code
- A master component list (bill of materials) of all files in the software package
- Ideally there is a ‘theory of operation’ document

Required Documentation: Physical Security

- First the hardware components (same as before)
  - All schematics
  - All drawings (circuit card, mechanical)
  - A master component list (bill of materials) of all files and components in the hardware package
  - Data sheets for all components (passives too)
- Then the physical security specific items
  - Ideally there is a ‘theory of operation’ document
  - How it works, and how it meets the level requirements

Required Documentation:
Design Assurance

- Describe the configuration management system (source code control) for all source (HW & SW)
- Describe manufacturing and shipping security and controls.
- Many of the Design Assurance requirements are covered in other sections here, for the complete list see FIPS 140-2 Appendix A

Required Documentation: EMI/EMC

- For Levels 1 and 2, an FCC part 15 class A certification is required
- For Levels 3 and 4, an FCC part 15 class B certification is required
- A certificate or an FCC accredited test lab report is required
- For level 1 SW modules, the certificate(s) or evidence of the certificate(s) for the general purpose computing platform(s) used is(are) required.

Required Documentation: Mitigation of Other Attacks

- If the module defends against attacks outside if the scope of FIPS 140-2, the vendor may claim protection in this section.
- Examples include prevention of timing attacks on RSA, detection of ionizing radiation, etc.
- Documentation and test data supporting the claim of mitigation at the security level claimed is required.

QUESTIONS/DISCUSSION