FIPS 140-3

Status and Schedules

Allen Roginsky
CMVP NIST

September 28, 2005

Agenda

- History of FIPS 140
- Motivation for change
- Areas of change
- What will not change
- Schedules
- Previous validations

History of FIPS 140

- Federal Standard 1027
  - General Security Requirements for Equipment using DES
- FIPS 140
- FIPS 140-1 (11 January 1994)
- FIPS 140-2 (25 May 2001)
  - Security Requirements for Cryptographic Modules

History of FIPS 140

➡ Federal Standard 1027

FIPS 140

FIPS 140-1

FIPS 140-2

General Security Requirements
<u>for Equipment using DES</u>

- Very hardware oriented
- Restrictive

History of FIPS 140

Federal Standard 1027

⇨ FIPS 140

FIPS 140-1

FIPS 140-2

Security Requirements for **<u>Cryptographic Modules</u>**

- Cover change for the FED STD 1027

History of FIPS 140

Federal Standard 1027

FIPS 140

➡ FIPS 140-1

FIPS 140-2

Security Requirements for Cryptographic Modules

- Start giving flexibility to the vendors
- Still hardware oriented
- Start recognizing software modules

History of FIPS 140

Federal Standard 1027

FIPS 140

FIPS 140-1

→ FIPS 140-2

Security Requirements for Cryptographic Modules

- Re-organized FIPS 140-1
- Clarified some requirements
- Incorporation of refinements contained in Implementation Guidance
- Introduction of Design Assurance

Motivation for Change

- U.S. Federal Requirement
  - Must be reviewed every 5 years
- Tremendous technology advances
  - Standard is becoming out of date
  - Difficult to generically apply to new technologies
- Protection for more sensitive information
- Requirement improvements and strengthening
- Refinements and corrections

Areas of Change

- New security levels
- Special attention to software cryptographic modules
- Roles and services, authentication
  - No maintenance role
- Cryptographic key life cycle
  - key establishment and distribution: new standards
  - random number generator requirements

Areas of Change

- Physical security
- Self-tests
  - Power-up, module integrity checks
  - Conditional tests
- Security policy
  - Realign with what users need

FIPS 140-2 and FIPS 140-3

- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Authentication, and Services
- Finite State Module
- Physical Security
- Operational Environment
- Cryptographic Key Management
- EMI/EMC
- Self Tests
- Implementation Assurance
- Mitigation of Other Attacks

- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Authentication, and Services
- Software Security
- Physical Security
- Operational Environment
- Sensitive Security Parameter (SSP) Management
-
- Self Tests
- Implementation Assurance
- Mitigation of Other Attacks

Highlights

- Two New Security Levels
- SPA at Level 3
- Software Security Section
- EMI at Level 5
- Detached from CC
- SSPs, CSPs and PSPs
- Key Management Clarified
- Pre-operational tests
- Significant Changes to Almost Every Section

<table>
<tr><th></th><th><em>Security Level 1</em></th><th><em>Security Level 2</em></th><th><em>Security Level 3</em></th><th><em>Security Level 4</em></th><th><em>Security Level 5</em></th><th><em>Security Level 6</em></th></tr>
<tr><td><strong>Cryptographic Module Specification</strong></td><td colspan="6">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.</td></tr>
<tr><td><strong>Cryptographic Module Ports and Interfaces</strong></td><td colspan="2">Required and optional interfaces. Specification of all interfaces and of all input and output data paths.</td><td colspan="4">Input and output of critical security parameters either physically separated or logically separated using trusted path from other data ports and interfaces.</td></tr>
<tr><td><strong>Roles, Services, and Authentication</strong></td><td>Definition of module's services.</td><td>Role-based or identity-based operator authentication.</td><td colspan="4">Identity-based operator authentication.</td></tr>
<tr><td><strong>Software Security</strong></td><td colspan="3">Logical security mechanisms. Protected boundary. Approved authentication technique applied to all validated software.</td><td colspan="3">Logical temper detection and response capabilities.</td></tr>
<tr><td><strong>Physical Security</strong></td><td>Production-grade components</td><td>Evidence of tempering. Opaque covering.</td><td>Temper response and zeroization circuitry. Vents protected from probing. Simple power analysis.</td><td>Hard opaque removal-resistant coating or tamper detection envelope.</td><td>EFT or EFP for temperature and voltage. EMI protection.</td><td>Differential power analysis protection.</td></tr>
<tr><td><strong>Operational Environment (Modifiable Only)</strong></td><td>Single Operator.</td><td>Discretionary access control mechanisms.</td><td colspan="4">Trusted Path.</td></tr>
<tr><td rowspan="2"><strong>Cryptographic Key Management</strong></td><td colspan="6">Key management mechanisms: random bit and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.</td></tr>
<tr><td colspan="2">Secret and private keys established using manual methods may be entered or output in plaintext form.</td><td colspan="4">Secret and private keys established using manual methods are entered or output encrypted or with split knowledge procedures.</td></tr>
<tr><td><strong>Self-Tests</strong></td><td colspan="6">Pre-operational tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.</td></tr>
<tr><td rowspan="2"><strong>Design Assurance Including the Finite State Machine</strong></td><td colspan="6">Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions. Correspondence of design security policy and FSM.</td></tr>
<tr><td>Specification of components and testing. Start-up procedures.</td><td>Functional specification. High-level language. Secure distribution procedures.</td><td>Low-level design. Low-level testing. Preconditions and postconditions. Vendor data authentication.</td><td>Informal proof of correspondence between module design and functional specification.</td><td colspan="2">Formal model.</td></tr>
<tr><td><strong>Mitigation of Other Attacks</strong></td><td colspan="6">Specification of mitigation of attacks for which no testable requirements are currently available.</td></tr>
</table>

Milestones

	Start Date	Length
• Public Comment on FIPS 140-2	Jan 05	3 months
– Federal Registry Notice		
• CMVP Prepares Draft #0 FIPS 140-3	Apr 05	4 months
– Use received comments		
– Incorporate new requirements		
• Draft #0 Sent to Testing Labs	Sep 05	

Milestones

	Start Date	Length
• CMVP Publishes FIPS 140-3 Draft #1 for Public Comment	Nov 05	
– Use received comments	Feb 06	3 months
• FIPS 140-3 Approval process	May 06	
• FIPS 140-3 Approved !	**Sept 06**	
• FIPS 140-3 in effect (+ 6 mo)	**Mar 06**	
• FIPS 140-2 retires	**Sep 07**	

Concurrent Activities

- Implementation Guidance for FIPS 140-3 and Derived Test Requirements for FIPS 140-3 should be issued
- Vendor and Lab education
- NVLAP Publication 150-17

Status of Previous Validations

- Validations to FIPS 140-1 and FIPS 140-2 will still be recognized
- Migration path from previous validations to FIPS 140-3 will be defined
  - similar to (FIPS 140-1 to FIPS 140-2)

Conclusion

- FIPS 140-3 development is on the way
- Public is involved in the development process
- Watch the CMVP website
  - WWW.NIST.GOV/CMVP