McAfee, Inc.
Network Security Platform Sensor
M-8000 P

Security Policy

Version 1.12

November 28, 2011

TABLE OF CONTENTS

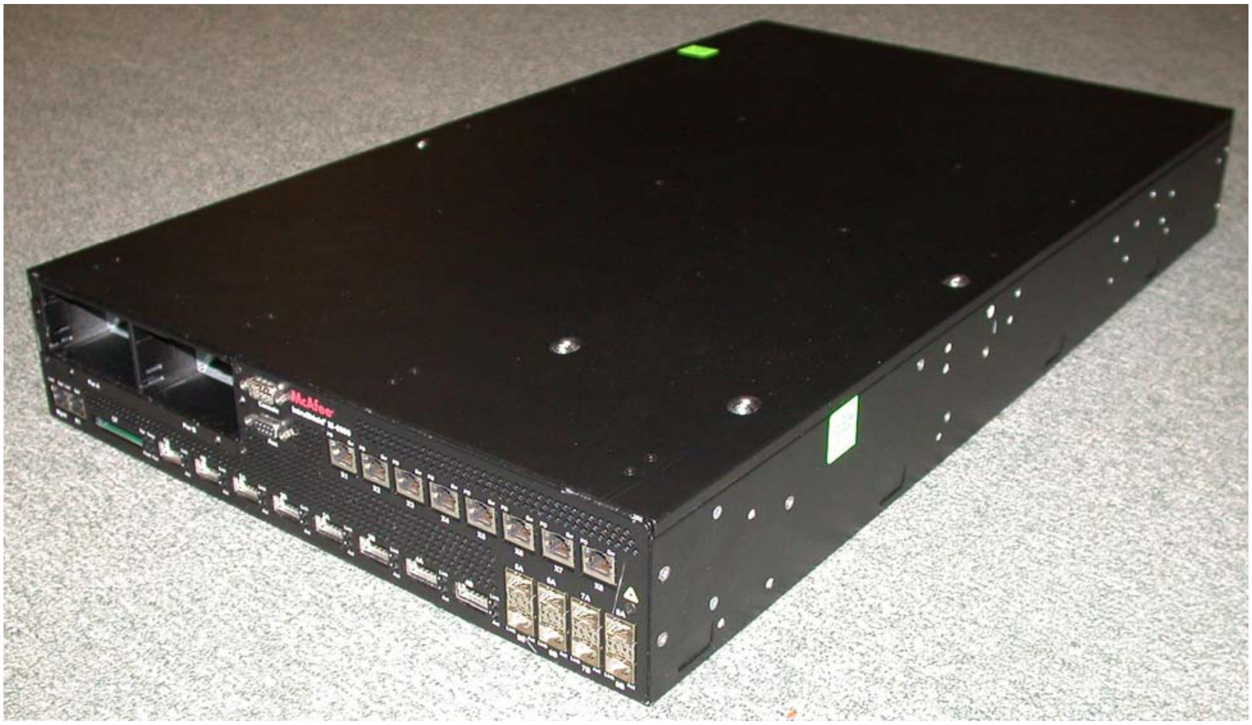
1 Module Overview

The Network Security Platform (NSP) Sensor M-8000 P (HW P/N M-8000 P, Version 1.40; FW Version 6.1.15.35; FIPS Kit P/N IAC-FIPS-KT8) is a multi-chip standalone cryptographic module as defined by FIPS 140-2. It is an Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) designed for network protection against zero-day, DoS/DDoS, encrypted and SYN Flood attacks, and real-time prevention of threats like spyware, malware, VoIP vulnerabilities, phishing, botnets, network worms, Trojans, and peer-to-peer applications. The cryptographic boundary is the outer perimeter of the enclosure, including the removable power supplies and fan trays. (The power supplies and fan trays are excluded from FIPS 140-2 requirements, as they are not security relevant.)

The McAfee M-8000 product consists of the M-8000 P cryptographic module physically connected with the M-8000 S cryptographic module. This security policy describes the M-8000 P only.

Figure 1 shows the module and its cryptographic boundary.

Figure 1 – Image of the Cryptographic Module



2 Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2. Table 1 specifies the levels met for specific FIPS 140-2 areas.

Table 1 - Module Security Level Specification

Security Requirements Section	**Level**
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3 Modes of Operation

The module only supports a FIPS Approved mode of operation. An operator can obtain the FIPS mode indicator by executing the “show” or “status” CLI command which returns the module’s firmware version, HW version, etc. The firmware and hardware versions must match the FIPS validated versions located on the CMVP website.

3.1 FIPS Approved Mode of Operation

The module supports the following FIPS Approved algorithms:

- AES CBC mode with 128 bits for encryption and decryption (Cert. #880)
- Triple-DES CBC mode with 2 and 3 keys for encryption and decryption (Cert. #781)

  (Note: 2-key Triple-DES encryption is Restricted per SP 800-131A and will be Disallowed in 2016. 2-key Triple-DES decryption will continue to be acceptable for Legacy-use.)

- RSA with 1024 and 2048 bit keys for signature generation/verification (Cert. #425)

  (Note: RSA signature generation with 1024 bit keys and 2048 bit keys with SHA-1 is Deprecated per SP 800-131A and will be Disallowed in 2014. RSA signature verification with 1024 bit keys and 2048 bit keys with SHA-1 will continue to be acceptable for Legacy-use.)

- DSA with 1024 bit keys for key generation, signature generation/verification (Cert. #345)

  (Note: DSA key and signature generation with 1024 bit keys is Deprecated per SP 800-131A and will be Disallowed in 2014. DSA signature verification with 1024 bit keys will continue to be acceptable for Legacy-use.)

- SHA-1 and SHA-256 for hashing (Cert. #871)
- ANSI X9.31 RNG with 2-Key Triple-DES (Cert. #505)

  (Note: ANSI X9.31 RNG is Deprecated per SP 800-131A and will be Disallowed in 2016.)

- HMAC-SHA-1 and HMAC-SHA-256 for message authentication (Cert. #971)
- XYSSL RSA with 2048 bit keys for signature verification (Cert. #830)

  (Note: RSA signature verification with 2048 bit keys and SHA-1 will continue to be allowed for Legacy use per SP 800-131A.)

- XYSSL SHA-1 for hashing and for use with image verification (Cert. #970)

The module supports the following FIPS allowed algorithms and protocols:

- RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength)

  (Note: Non SP 800-56B Key Transport Schemes providing < 112 bits of strength are Deprecated per SP 800-131A and will be Disallowed in 2014.)

- Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength)

  (Note: Non SP 800-56A Key Agreement Schemes providing < 112 bits of strength are Deprecated per SP 800-131A and will be Disallowed in 2014.)

- NDRNG for seeding the ANSI X9.31 RNG
- TLS v1.0 with the following cipher suites:
  - TLS_RSA_WITH_AES_128_CBC_SHA for communication with Network Security Platform (NSP) Manager
- SSH v2 with the following cipher suites:
  - Key Exchange methods (i.e., key establishment methods): Diffie-hellman-group-exchange-SHAl, Diffie-hellman-group1-SHAl, Diffie-hellman-group14-SHAl
  - Public Key methods (i.e., authentication methods): SSH-DSS, SSH-RSA
  - Encryption methods: 3DES-CBC, AES128-CBC
  - MAC methods: HMAC-SHA1, HMAC-SHAl-96
- MD5 used to identify “fingerprint” of potential malware using Artemis database (no security claimed)

4 Ports and Interfaces

Table 2 provides the cryptographic module's ports and interfaces.

Table 2 – Ports and Interfaces

Physical Ports	Logical Interfaces	Qty.
10-Gig Monitoring Ports	Data Input/Output	8
1-GigE Monitoring Ports	Data Input/Output	8
GigE Management Port	Control Input, Data Output, Status Output	1
GigE Response Port	Data Output	1
RS232 Console/Aux Ports	Control Input, Status Output	2
Compact Flash	Data Input	1
Power Ports	Power Input	2
RJ11 Control Port	Data Input, Power Output	8
LEDs	Status Output	many

Notes:

1. Two 10-GigE ports (out of eight) are used to connect to the peer M-8000 S unit. The other six are used to monitor external traffic.
2. The GigE Response Port is connected directly to the peer M-8000 S unit's GigE Management Port.

The module supports the following communication channels with the Network Security Platform (NSP) Manager (aka ISM):

- Install channel: Only used to associate a Sensor with the ISM (i.e., NSP Manager, see Table 3). They use a "shared secret". ISM listening on port 8501.
- Trusted Alert/Control channel (TLS): ISM listening on port 8502
- Trusted Packet log channel (TLS): ISM listening on port 8503
- Command channel (SNMP, plaintext): Sensor listening to 3rd Party SNMP Clients on port 8500
- Bulk transfer channel (All output is encrypted): ISM listening on port 8504

5 Identification and Authentication Policy

The cryptographic module shall support four distinct “User” roles (Admin, Sensor Operator(s), M-8000 S, and 3rd Party SNMP Client(s)) and one “Cryptographic Officer” (CO) role (Network Security Platform Manager). Table 3 lists the supported operator roles along with their required identification and authentication techniques. Table 4 outlines each authentication mechanism and the associated strengths.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Admin	Role-based authentication	Username and Password
Sensor Operator(s)	Role-based authentication	Username and Password
Network Security Platform Manager (CO)	Role-based authentication	Digital Signature
M-8000 S	Role-based authentication	Username and Password
3rd Party SNMP Client(s)	Role-based authentication	Username, Privacy and Authentication key

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password (Admin and Sensor Operator(s))	The password is an alphanumeric string of a minimum of fifteen (15) characters chosen from the set of ninety (90) printable and human-readable characters. The probability that a random attempt will succeed or a false acceptance will occur is 1/90^15 which is less than 1/1,000,000. After three (3) consecutive failed authentication attempts, the module will enforce a one (1) minute delay prior to allowing retry. The probability of successfully authenticating to the module within one minute is 3/90^15 which is less than 1/100,000. The module only supports five (5) concurrent SSH sessions. Thus, with the one-minute timing delay after three consecutive failed authentication attempts, the probability of successfully authenticating to the module within one minute through random attempts is 15/90^15, which is less than 1/100,000.

Authentication Mechanism	Strength of Mechanism
Username and Password (M-8000 S)	The password is an alphanumeric string of a minimum of eight (8) characters chosen from the set of ninety (90) printable and human-readable characters. The probability that a random attempt will succeed or a false acceptance will occur is 1/90^8 which is less than 1/1,000,000. After one (1) failed authentication attempt, the module requires a reboot prior to allowing retry which takes longer than one minute. The probability of successfully authenticating to the module within one minute is 1/90^8 which is less than 1/100,000.
Digital Signature and RSA Key Wrap	RSA 1024 and 2048-bit keys are used for the signing (in isolated McAfee laboratory) and verification (by sensor) of digital signatures. The probability that a random attempt will succeed or a false acceptance will occur is 1/2^80 which is less than 1/1,000,000. The module can only perform a single digital signature verification per second. The probability of successfully authenticating to the module within one minute is 60/2^80 which is less than 1/100,000.
Username, Privacy and Authentication Key	The privacy key and authentication key together make an alphanumeric string of a minimum of sixteen (16) characters chosen from the set of sixty-two (62) numbers, lower case, and upper case letters. The probability that a random attempt will succeed or a false acceptance will occur is 1/62^16 which is less than 1/1,000,000. The module will allow approximately one attempt per millisecond, meaning that 60,000 attempts can be made per minute. The probability of successfully authenticating to the module within one minute is 60,000/62^16 which is less than 1/100,000.

6 Access Control Policy

6.1 Roles and Services

Table 5 lists each operator role and the services authorized for each role. Following Table 5, all unauthenticated services are listed.

Table 5 – Services Authorized for Roles

Role					**Authorized Services**
Admin	Sensor Operator(s)	NSP Manager	M-8000 S	3rd Party SNMP Client(s)	
X	X	X	X		**Show Status**: Provides module status, usage statistics, log data, and alerts.
X					**Sensor Operator Management:** Allows Admin to add/delete Sensor Operators, set their session timeout limit, and unlock them if needed.
X	X	X			**Network Configuration**: Establish network settings for the module or set them back to default values.
X	X	X			**Administrative Configuration:** Other various services provided for admin, private, and support levels.
X	X	X			**Firmware Update**: Install an external firmware image through TFTP or compact flash.
X	X				**Install with ISM**: Configures module for use. This step includes establishing trust between the module and the associated management station.
		X			**Install with 3rd Party SNMP Client:** Configures module for 3rd Party SNMP use. This step includes establishing trust between the module and the associated 3rd Party SNMP Client. Trust is provided by ISM.
X	X				**Change Passwords**: Allows Admin and Sensor Operators to change their associated passwords. Admin can also change/reset Sensor Operators passwords.
X	X				**Zeroize**: Destroys all plaintext secrets contained within the module.

Role					Authorized Services
Admin	Sensor Operator(s)	NSP Manager	M-8000 S	3rd Party SNMP Client(s)	
		X			**Intrusion Detection/Prevention Management**: Management of intrusion detection/prevention policies and configurations through SNMPv3 and TLS.
				X	**Intrusion Detection/Prevention Monitoring:** Limited monitoring of Intrusion Detection/Prevention configuration, status, and statistics through SNMPv3.
X	X				**Disable SSH/Console Access:** Disables SSH and Console access.

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- **Self-Tests**: This service executes the suite of self-tests required by FIPS 140-2.
- **Intrusion Prevention Services**: Offers protection against zero-day, DoS/DDoS, encrypted and SYN Flood attacks, and real-time prevention of threats like spyware, malware, VoIP vulnerabilities, phishing, botnets, network worms, Trojans, and peer-to-peer applications. *Note:* The only cryptography performed during this service is an MD5 hash to identify the "fingerprint" of malware.

6.2 Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- **Administrator Passwords**: Password used for authentication of the "admin" role through console and SSH login. Extended permissions are given to the "admin" role by using the "support" or "private" passwords.
- **Sensor Operator Passwords**: Passwords used for authentication of "user" accounts through console and SSH login. Extended permissions are given to the "user" account by using the "support" or "private" passwords.
- **3rd Party SNMP Client Privacy and Authentication Keys**: Passwords used for authentication of 3rd Party SNMP Clients.
- **M-8000 Password:** Password used for authentication of M-8000 S.

- **ISM Initialization Secret (i.e., ISM Shared Secret)**: Password used for mutual authentication of the sensor and ISM during initialization.
- **Bulk Transfer Channel Session Key**: AES 128 bit key used to encrypt data packages across the bulk transfer channel.
- **SSH Host Private Keys**: DSA or RSA 1024 bit key used for authentication of sensor to remote terminal for CLI access.
- **SSH Session Keys**: Set of ephemeral Diffie-Hellman, Triple-DES or AES, and HMAC keys created for each SSH session.
- **TLS Sensor Private Key (for ISM)**: RSA 1024 bit key used for authentication of the sensor to ISM.
- **TLS Session Keys (for ISM)**: Set of ephemeral AES and HMAC keys created for each TLS session with the ISM.
- **Seed for RNG**: Seed created by NDRNG and used to seed the ANSI X9.31 RNG.
- **Seed Key for RNG**: Seed created by NDRNG and used as the Triple DES key used in the ANSI X9.31 RNG.

6.3 Definition of Public Keys:

The following are the public keys contained in the module:

- **McAfee FW Verification Key**: RSA 2048 bit key used to authenticate firmware images loaded into the module.
- **SSH Host Public Key**: DSA or RSA 1024 bit key used to authenticate the sensor to the remote client during SSH.
- **SSH Remote Client Public Key**: DSA or RSA 1024 bit key used to authenticate the remote client to the sensor during SSH.
- **TLS Sensor Public Key (for ISM):** RSA 1024 bit key used to authenticate the sensor to ISM during TLS connections.
- **TLS ISM Public Key**: RSA 1024 bit key used to authenticate ISM to sensor during TLS connections.

6.4 Definition of CSPs Modes of Access

Table 6 defines the relationship between access to keys/CSPs and the different module services. The types of access used in the table are Read (R), Write (W), and Zeroize (Z). Z* is used to denote that only the plaintext portion of the CSP is zeroized (i.e., the CSP is also stored using an Approved algorithm, but that portion is not zeroized).

Table 6 – Key/CSP Access Rights within Services

	Administrator Passwords	Sensor Operator Passwords	M-8000 Password	3rd Party SNMP Client P and A Keys	ISM Initialization Secret	Bulk Transfer Channel Session Key	SSH Host Private Keys	SSH Session Keys	TLS Sensor Private Key (for ISM)	TLS Session Keys (for ISM)	Seed for RNG	Seed Key for RNG	McAfee FW Verification Key	SSH Host Public Key	SSH Remote Client Public Key	TLS Sensor Public Key (for ISM)	TLS ISM Public Key
Show Status	R				R	R	R		R	R				R	R	R	R
Sensor Operator Management		R W															
Network Configuration					R		R		R	R				R	R	R	R
Administrative Configuration					R		R		R	R				R	R	R	R
Firmware Update					R		R		R	R				R	R	R	R
Install with ISM							R		R W	R W	R W	R W		R	R	R W	R W
Install with 3rd Party SNMP Client				R W													
Change Passwords	R W		R W				R							R	R		
Zeroize	Z*	Z*	Z	Z	Z	Z	R Z	Z	Z	Z	Z	Z	Z	R	R		
Intrusion Detection/Prevention Management						R			R	R						R	R
Intrusion Detection/Prevention Monitoring				R													
Disable SSH/Console Access																	
Self Tests																	
Intrusion Prevention Services																	

7 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the device supports a limited operational environment.

8 Security Rules

The cryptographic module's design corresponds to the module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide five distinct operator roles: Admin, Sensor Operator(s), Network Security Platform Manager, M-8000 S, and 3rd Party SNMP Client(s).

2. The cryptographic module shall provide role-based authentication.

3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.

4. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

      1. Cryptographic algorithm known answer tests:
         a. AES CBC 128 encryption/decryption Known Answer Tests
         b. Triple-DES CBC encryption/decryption Known Answer Tests
         c. RSA 1024 and 2048 Sign/Verify Known Answer Test
         d. DSA 1024 Sign/Verify Known Answer Test
         e. SHA-1 Known Answer Test
         f. SHA-256 Known Answer Test
         g. ANSI X9.31 RNG Known Answer Test
         h. RSA 1024 Decrypt Known Answer Test
         i. HMAC SHA-1 Known Answer Test
         j. HMAC SHA-256 Known Answer Test
         k. XYSSL RSA 2048 Verify Known Answer Test
         l. XYSSL SHA-1 Known Answer Test

      2. Firmware Integrity Test: XYSSL RSA 2048 used

      3. Critical Functions Tests: N/A

   B. Conditional Self-Tests:

      1. ANSI X9.31 RNG Continuous Test
      2. NDRNG Continuous Test
      3. RSA Sign/Verify Pairwise Consistency Test
      4. DSA Sign/Verify Pairwise Consistency Test
      5. External Firmware Load Test – XYSSL RSA 2048 used

5. At any time the cryptographic module is in an idle state, the operator shall be capable of commanding the module to perform the power up self-test by power cycling.

6. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.
9. The module shall only support five concurrent SSH operators when SSH is enabled.
10. The use of the Console Port/Aux port shall be restricted to the initialization of the cryptographic module.
11. The use of the Compact Flash Port shall be restricted to loading McAfee signed firmware.
12. The “SSL Decryption” service shall be disabled.

9 Physical Security Policy

9.1 Physical Security Mechanisms

The cryptographic module includes the following physical security mechanisms:

- Production-grade components
- Production-grade opaque enclosure with tamper evident seals. Tamper evident seals and further instructions are obtained in the FIPS Kit with the part number: IAC-FIPS-KT8.

9.2 Operator Required Actions

For the module to operate in a FIPS Approved mode, the tamper seals shall be placed by the Admin role as specified below. The Admin must clean the chassis of any dirt before applying the labels. Per FIPS 140-2 Implementation Guidance (IG) 14.4, the Admin role is also responsible for the following:

- Securing and having control at all times of any unused seals
- Direct control and observation of any changes to the module, such as reconfigurations, where the tamper evident seals or security appliances are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to a FIPS Approved state.

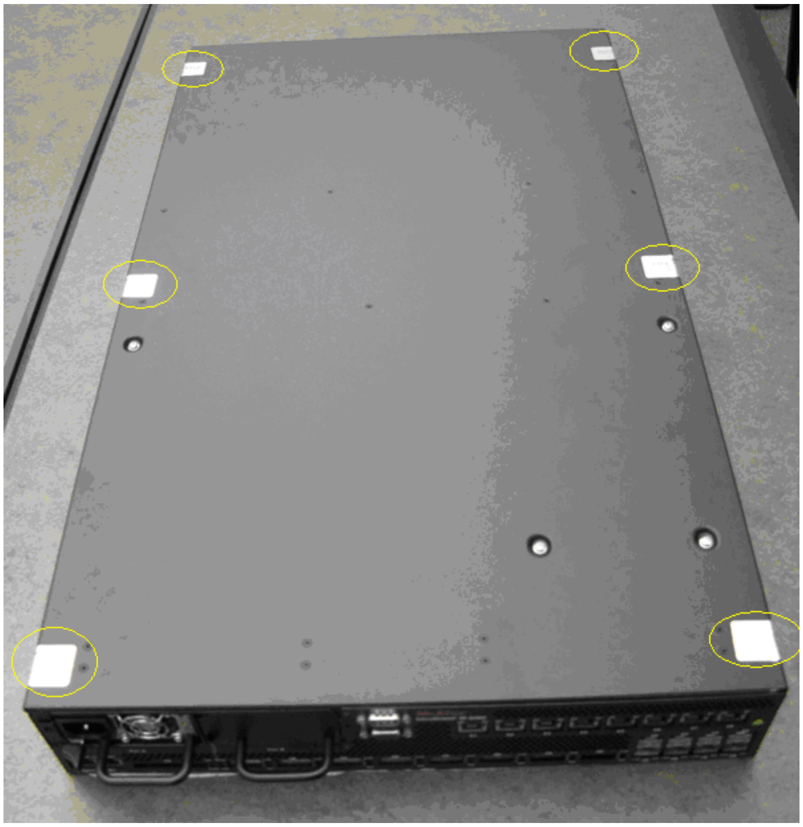
The Admin is also required to periodically inspect tamper evident seals. Table 7 outlines the recommendations for inspecting/testing physical security mechanisms of the module. If evidence of tamper is found during the periodic inspection, the operator should zeroize the module and modify Administrator Passwords upon start up. The operator should contact McAfee for new tamper labels, if necessary.

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	As specified per end user policy	Visually inspect the labels for tears, rips, dissolved adhesive, and other signs of malice.
Opaque Enclosure	As specified per end user policy	Visually inspect the enclosure for broken screws, bent casing, scratches, and other questionable markings.

Figure 2 depicts the tamper label locations on the cryptographic module. There are 6 tamper labels and they are circled in yellow.

Figure 2 – Tamper Label Placement



10 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.