The Xirrus Wi-Fi Array
XN4, XN8, XN12, XN16
Security Policy

Document *Version 1.0*

Xirrus, Inc.

February 15, 2011

TABLE OF CONTENTS

1. Module Overview

The Xirrus Wi-Fi Array (Models XN4, XN8, XN12 and XN16) are multi-chip standalone cryptographic modules. The primary purpose for this device is to provide data security for wireless Internet Protocol (IP) traffic.

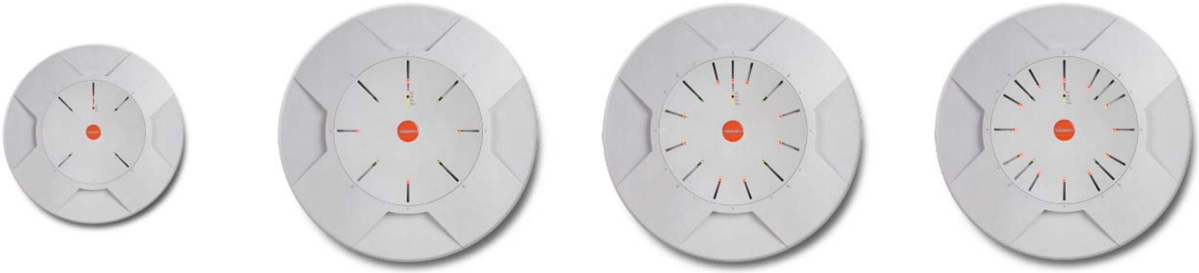


Figure 1 – Image of the Xirrus Wi-Fi Array

The Xirrus Wi-Fi Arrays all use the same basic design. There are two form factors, a small one for 4 radio arrays and a larger one for eight to sixteen radio arrays. The XN16 models use 16 radios, the XN12 models use 12 radios, the XN8 models use 8 radios and the XN4 models use 4 radios. The XN8, XN12 and XN16 all use the same PCB's with different build options for number of radios.   The same firmware is used in all models.

Table 1 – Part Number Table

Model	Part Number	Version	Firmware
XN16	190-0111-001	D	4.1 and 5.0
XN12	190-0128-001	D	4.1 and 5.0
XN8	190-0110-002	B	4.1 and 5.0
XN4	190-0109-001	D	4.1 and 5.0

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS-140-2.

Table 2 - 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	2
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

In FIPS mode, the cryptographic module only supports FIPS Approved algorithms as follows:

- AES (Cert. #1508; ECB and CBC 128-bit; encryption)
- AES (Cert. #1508; CCM mode)
- AES (Cert. #1515; CBC 128 and 256 bit)
- TDES (Cert. #1009)
- HMAC-SHA-1 (Cert. #860)
- SHA-1 (Cert. #1325)
- RSA (Cert. #715)
- RNG based on ANSI X9.31 Appendix A.2.4 using AES Algorithm (Cert. #800)

The module implements the following Non-Approved algorithms allowed for use in the FIPS Approved Mode of Operation:

- Non-Approved RNG (/dev/urandom)
- MD5 for TLS session key derivation
- RSA for key establishment (Key wrapping; Key establishment methodology provides 80 bits of encryption strength)
- Diffie-Hellman for SSH key establishment (Key agreement; key establishment methodology provides 80 bits or 112 bits of encryption strength)

- RC4 (considered plaintext)

Non-FIPS mode of operation

In non-FIPS mode, the cryptographic module provides non-FIPS Approved algorithms as follows:

- RC4 for encryption/decryption in TKIP and WEP
- MD5
- Software RNG(/dev/urandom)

4. Implementing FIPS Security

Wi-Fi Arrays may be configured to satisfy the requirements for Level 2 of Federal Information Processing Standard (FIPS) Publication 140-2. The procedure in this section lists simple steps that must be followed exactly to implement FIPS 140-2, Level 2. The procedure includes physical actions, and parameters that must be set in Web Management Interface (WMI) windows in the Security section and in other sections.

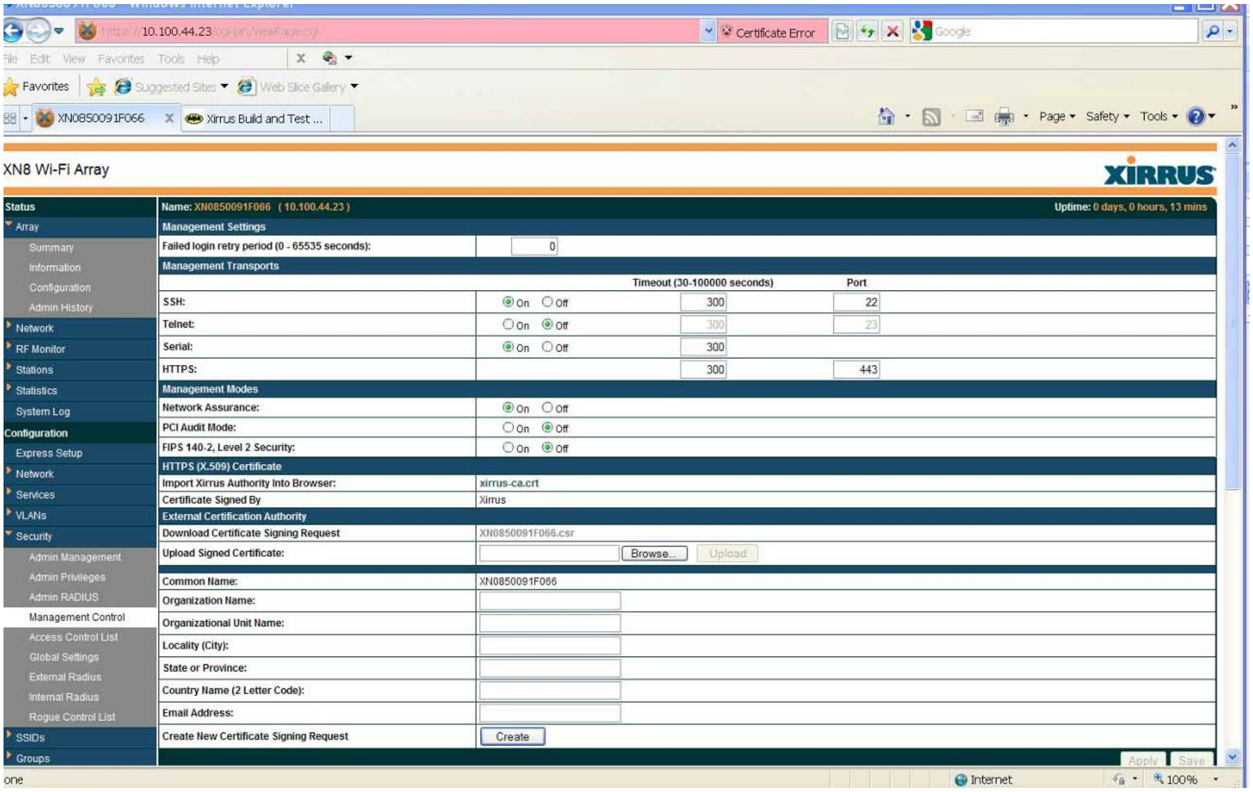
To implement FIPS 140-2, Level 2 using WMI (5.0 version)

1. Enable HTTPS using the CLI if it is not already enabled, using the following command:

   ```
   Xirrus_Wi-Fi_Array(config)# https on
   ```

   This allows the Web Management Interface to be used for the rest of this procedure. HTTPS is enabled on Arrays by default.

2. Select the Management Control from the Security window.



Name: XN0850091F066 (10.100.44.23)

Uptime: 0 days, 0 hours, 13 mins

Management Settings

Failed login retry period (0 - 65535 seconds): 0

Management Transports

		Timeout (30-100000 seconds)	Port
SSH:	● On ○ Off	300	22
Telnet:	○ On ● Off	300	23
Serial:	● On ○ Off	300	
HTTPS:		300	443

Management Modes

Network Assurance:	● On ○ Off
PCI Audit Mode:	○ On ● Off
FIPS 140-2, Level 2 Security:	○ On ● Off

HTTPS (X.509) Certificate

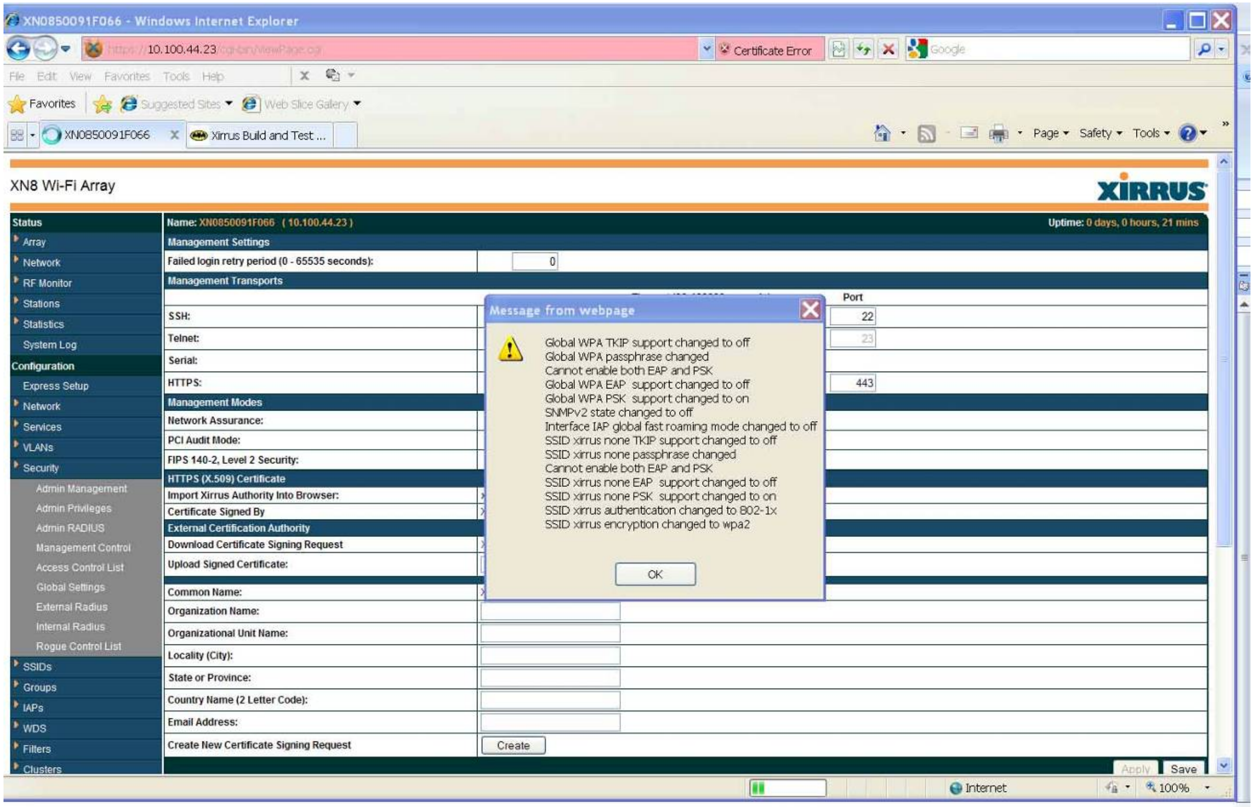
Import Xirrus Authority Into Browser:	xirrus-ca.crt
Certificate Signed By	Xirrus

External Certification Authority

Download Certificate Signing Request	XN0850091F066.csr
Upload Signed Certificate:	
Common Name:	XN0850091F066
Organization Name:	
Organizational Unit Name:	
Locality (City):	
State or Province:	
Country Name (2 Letter Code):	
Email Address:	
Create New Certificate Signing Request	

Figure 10 – Security Management Control Window

3. Set FIPS **140-2, Level 2 Security** to **On** (Figure 11). Click **Apply** and then **OK**



Name: XN0850091F066 (10.100.44.23)

Uptime: 0 days, 0 hours, 21 mins

Management Settings

Failed login retry period (0 - 65535 seconds): 0

Management Transports

	Port
SSH:	22
Telnet:	23
Serial:	
HTTPS:	443

Management Modes

Network Assurance:

PCI Audit Mode:

FIPS 140-2, Level 2 Security:

HTTPS (X.509) Certificate

Import Xirrus Authority Into Browser:

Certificate Signed By

External Certification Authority

Download Certificate Signing Request

Upload Signed Certificate:

Common Name:

Organization Name:

Organizational Unit Name:

Locality (City):

State or Province:

Country Name (2 Letter Code):

Email Address:

Create New Certificate Signing Request Create

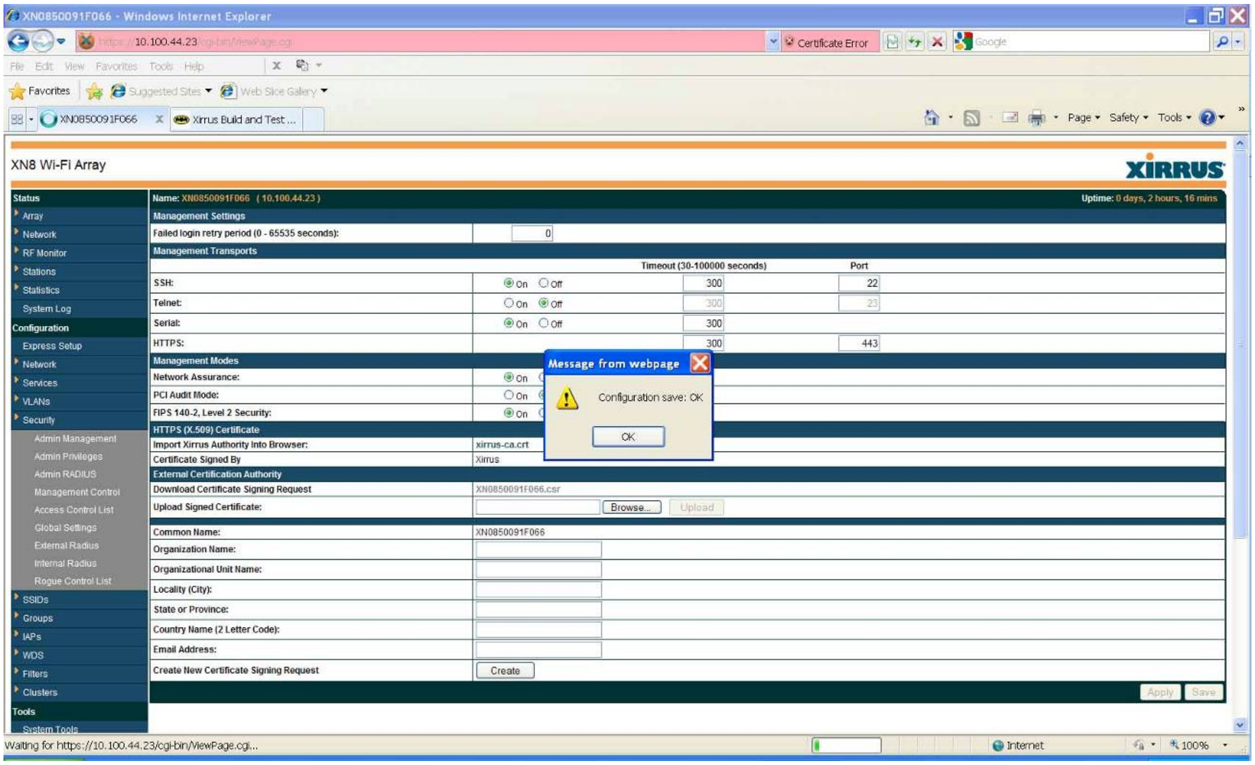
Message from webpage

```
Global WPA TKIP support changed to off
Global WPA passphrase changed
Cannot enable both EAP and PSK
Global WPA EAP  support changed to off
Global WPA PSK  support changed to on
SNMPv2 state changed to off
Interface IAP global fast roaming mode changed to off
SSID xirrus none TKIP support changed to off
SSID xirrus none passphrase changed
Cannot enable both EAP and PSK
SSID xirrus none EAP  support changed to off
SSID xirrus none PSK  support changed to on
SSID xirrus authentication changed to 802-1x
SSID xirrus encryption changed to wpa2
```

OK

Figure 11 – Setting FIPs mode On

4. Click **Save** then **OK**.



Name: XN0850091F066 (10.100.44.23)

Uptime: 0 days, 2 hours, 16 mins

Management Settings

Failed login retry period (0 - 65535 seconds): 0

Management Transports

		Timeout (30-100000 seconds)	Port
SSH:	● On ○ Off	300	22
Telnet:	○ On ● Off	300	23
Serial:	● On ○ Off	300	
HTTPS:		300	443

Management Modes

Network Assurance: ● On

PCI Audit Mode: ○ On

FIPS 140-2, Level 2 Security: ● On

HTTPS (X.509) Certificate

Import Xirrus Authority Into Browser: xirrus-ca.crt

Certificate Signed By: Xirrus

External Certification Authority

Download Certificate Signing Request: XN0850091F066.csr

Upload Signed Certificate: Browse... Upload

Common Name: XN0850091F066

Organization Name:

Organizational Unit Name:

Locality (City):

State or Province:

Country Name (2 Letter Code):

Email Address:

Create New Certificate Signing Request: Create

Message from webpage

Configuration save: OK

OK

Waiting for https://10.100.44.23/cgi-bin/ViewPage.cgi...

Figure 12 – Save configuration

To check if an Array is in FIPS mode:

You may determine whether or not the Array is running in FIPS mode by verifying that the settings described in the previous procedure are in effect.

To implement FIPS 140-2, Level 2 using CLI (4.1 and 5.0 version):

1. The following CLI command will perform all of the settings required to put the Array in FIPS mode:

   ```
   Xirrus_Wi-Fi_Array(config)# fips on
   ```

   This command remembers your previous settings for FIPS-related attributes. They will be restored if you use the **fips off** command.

   Use the **save** command to save these changes to flash memory.

2. Use the **fips off** command if you would like to revert the FIPS settings back to the values they had before you entered the **fips on** command.

   ```
   Xirrus_Wi-Fi_Array(config)# fips off
   ```

   Use the **save** command to save these changes to flash memory.

5. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

Model	10/100 Ethernet Port	Gigabit Ethernet Port	Serial Port (RS232)	TX/RX Radio Port	Status LEDs
XN16	1	2	1	16	20
XN12	1	2	1	12	16
XN12	1	2	1	8	12
XN4	N/A	1	1	4	6

10/100 Ethernet Port: data input, data output, control input, status output
Gigabit Ethernet Port: data input, data output, control input, status output
Serial Port (RS232): data input, data output, control input, status output
TX/RX Radio Port: data input, data output
LEDs: status output (Ethernet status, Integrated access point status, Array status)
Power: Power Input
Power: Power provided by POE

6. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support two distinct operator roles (User and Crypto Officer). The Crypto Officer role shall be performed by the Administrator managing the device, and the User role shall be performed by the wireless client using the device to send and receive data.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Crypto Officer	Identity-based operator authentication	Username and Password
User	Role based operator authentication	PSK

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Username and Password	Passwords are at least 5 characters long, with 94 characters available. Therefore, the probability that a random attempt will succeed or a false acceptance will occur is 1/7,339,040,224 which is less than 1/1,000,000. To exceed 1 in 100,000 probability of a successful random attempt during a 1-minute period, 73391 (1233 per second) attempts would have to be executed. This is not feasible from a standpoint of device capabilities.
PSK	802.11i Pre-Shared Key (PSK) is 32 bytes (256 bits) long, therefore there are 2^{256} possibilities for a PSK. This means that exceeding 1 in 100, 000 probability of a successful random attempt during a 1-minute period is not feasible from a device capabilities standpoint.

7. Access Control Policy

Roles and Services

Table 5 – Services Authorized for Roles

Role	Authorized Services
User: This role shall provide all of the services necessary for the secure transport of data over Wi-Fi.	• <u>802.11i with PSK</u>: This service allows a user to authenticate and send/receive data in a secure manner using 802.11i PSK mode.
Crypto Officer (CO): This role manages the cryptographic module in a secure fashion over the CLI or WMI.	• <u>Manage Configuration</u>: This service allows an administrator to change configuration settings within the module such as establishing SSIDs, modifying usage of power, turning radios on/off, and adding new users. Additionally, it allows an administrator to perform the zeroization process, to load new firmware into the

	module and to display the module's current configuration and status.
Unauthenticated Role(UA)	• Read LED status: Status is provided by the LEDs for interpretation. • Initiate self-test: Performed by power cycling the array.

Table 6 - Specification of Service Inputs & Outputs

Service	Control Input	Data Input	Data Output	Status Output
802.11i with PSK	Header info.	Data	Data	None
LED Status	None	None	None	Radio and Array power and condition status
Manage Configuration	Instructions	Configuration Data	Configuration Data	Configuration Status
Initiate Self-Tests	Power	None	None	Success/fail Failure will cause reboot

Definition of Critical Security Parameters (CSPs)

CSP	Description
Crypto Officer Password	This is an operator defined password (at least 5 characters long) that allows an administrator to log into the module. The password is stored on EEPROM as MD5 one-way hash. Destroyed via manage configuration service.
802.11i Pre-Shared Key (PSK) and Derived AES Session Key:	These are keys used for 802.11i encryption and integrity as well as User authentication. The PSK is entered directly by operator via SSH or HTTPS and is stored on EEPROM in RC4 encrypted form (considered plaintext). Destroyed via manage configuration service.
TLS Session Keys	These are AES (128 or 256 bits) or TDES (128 bits) keys and HMAC-SHA-1 keys used to support HTTPS. These are derived from the Pre-Master Secret. Destroyed via manage configuration service.
TLS Pre-Master Secret	This Key is used to derive TLS Session keys. It is established by RSA transport during the TLS handshake. Destroyed via manage configuration service.
TLS Private Key	RSA private key is used to decrypt TLS pre-Master Secret. Destroyed via manage configuration service.
SSH2 Session Keys	These are AES (128 or 256 bits) or TDES (128 bits) keys and HMAC-SHA-1 keys used to support SSH2 Sessions. These are derived from the

	SSH2 Shared Secret. Destroyed via manage configuration service.
SSH2 Shared Secret	This Key is used to derive SSH2 Session keys. It is established by Diffie-Hellman Key Agreement during the SSH2 negotiation. Destroyed via manage configuration service.
SSH2 Private Key	Ephemeral Diffie Hellman private keys used to establish the SSH2 Shared Secret. Destroyed via manage configuration service.
RNG State	Random number generator seed and seed key. Destroyed via manage configuration service.

Public Keys	**Description**
SSH2 Public Keys	Ephemeral Diffie-Hellman public keys used to establish the SSH2 Shared Secret .
RSA Public key	Public key used to establish TLS session.

Table 7 – CSP Access Rights within Roles & Services

Roles			Service	Cryptographic Keys and CSPs Access
CO	**User**	**UA**		
	X		802.11i with PSK	Derive 802.11i AES Session Key using 802.11i PSK. Encrypt/decrypt data traffic using 802.11i AES Session Key.
X			Manage Configuration	Login using Crypto Officer's password Enter 802.11i PSK Enter/Change Crypto Officer password values. 'Zeroize' all plaintext CSPs. Use TLS Private Key, Pre-Master Secret and Session Keys Use SSH2 Private Key, Shared Secret and Session Keys
		X	Initiate Self-tests	None
		X	LED Status	None

8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the Xirrus Access Point does not contain a modifiable operational environment.

9. Security Rules

The Xirrus Access Point's design corresponds to the cryptographic 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 two distinct operator roles. These are the User role and the Crypto Officer role.
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 encrypt/decrypt data using the AES algorithm.

5. The cryptographic module shall perform the following tests:

   A. <u>Power up Self-Tests:</u>

      1. Cryptographic algorithm tests:

         i. AES Known Answer Test

         ii. TDES Known Answer Tests

         iii. RSA Known Answer Test

         iv. RNG Known Answer Test

      2. Firmware Integrity Test (HMAC-SHA1)

   B. <u>Conditional Self-Tests:</u>

      i. Continuous tests for RNG and Non-Approved RNG.

      ii. Firmware Load Test (HMAC-SHA1)

6. Upon successful completion of self tests the system status led will be lit solid green. If a Self-test should fail, the module shall enter an error state and provide a status output via the system LED blinking red and system messaging.

7. 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.

8. All Data output shall be inhibited during power-up self tests and error states.

9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

10. The module shall support the use of Approved and specifically Allowed algorithms in the Approved mode of operation.

11. The module shall not share CSPs between modes of operation. CSPs shall not be maintained when entering and exiting the FIPS Approved Mode of Operation.

12. The following shall not be supported in the FIPS Approved Mode of Operation

    i. Management over IAPs
    ii. SNMP v1, v2 and v3
    iii. SSH1
    iv. SSL 2.0 and 3.0
    v. RADIUS (Internal and external)
    vi. Telnet
    vii. FTP, TFTP
    viii. HTTP
    ix. WEP
    x. WPA TKIP
    xi. WPA EAP
    xii. Entry of PSK as passphrase

13. The module shall be configured as defined in the Physical security section of this Security Policy. The tamper evident seals and security strap shall be installed for the

module to operate in a FIPS Approved mode of operation.

10. Physical Security Policy

Physical Security Mechanisms

The multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure
- Tamper evident seals.

Operator Required Actions

The operator is recommended to periodically inspect tamper evident seals.

Table 8 – Inspection/Testing of Physical Security Mechanisms

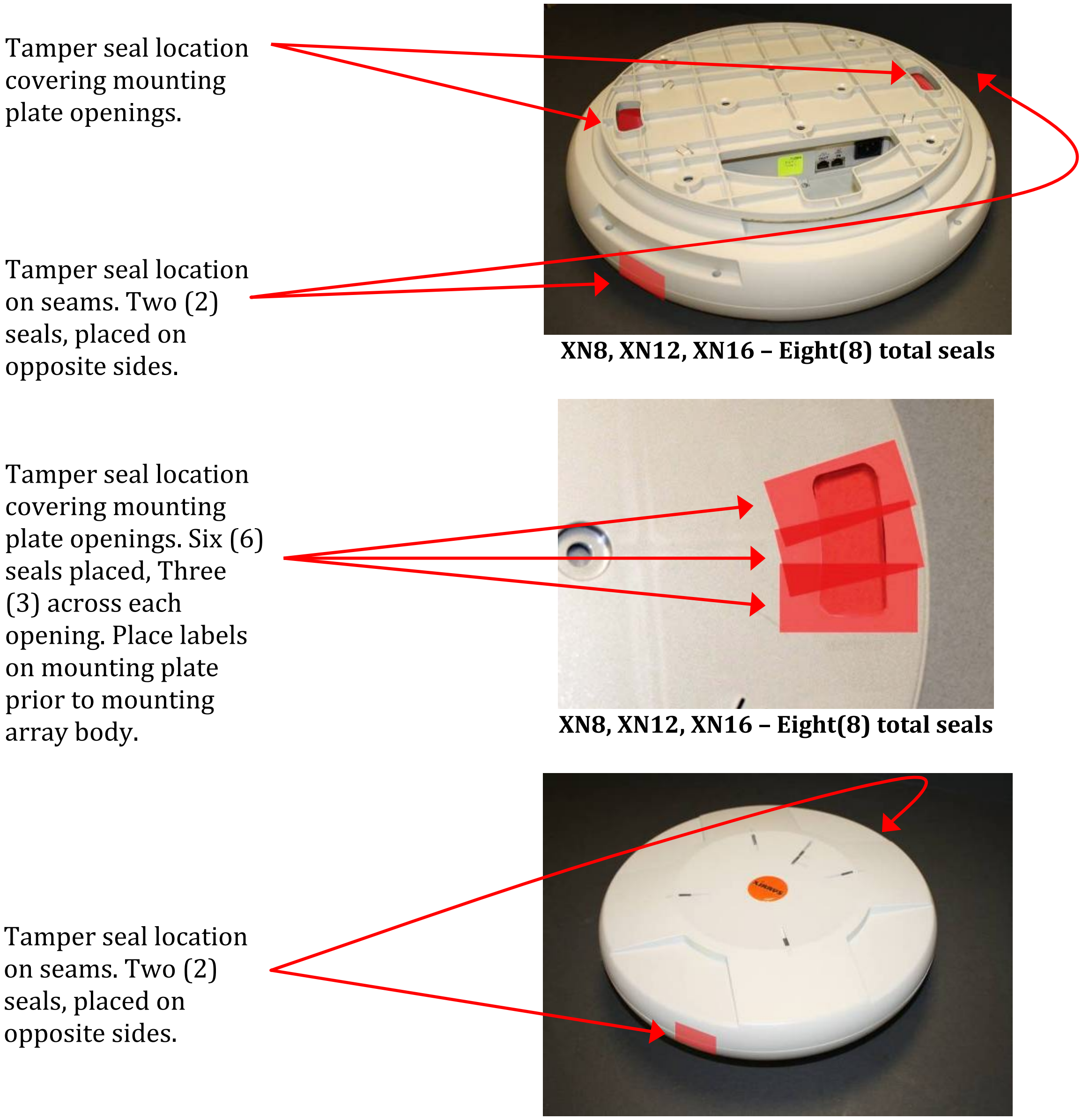
Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals	1 months	Instructions for the recommended inspections are located in the operator's manual.

Operator Required Actions

The Cryptographic Officer is required to configure and periodically inspect the cryptographic module. Tamper evident seals and security straps shall be in control of the Cryptographic Officer at all times.

1. Apply two seals, one on either side of the Array about 180° apart from each other, as indicated in the figures below.
   - **IMPORTANT:**
     - **Before you apply the tamper-evident seal, clean the surface area of any grease, dirt, or oil. We recommend using alcohol-based cleaning pads for this. Each seal must be applied to straddle both sides of an opening so that it will show if an attempt has been made to open the Array.**

     - **Make sure that each seal straddles a seam.**



Tamper seal location covering mounting plate openings.

Tamper seal location on seams. Two (2) seals, placed on opposite sides.

XN8, XN12, XN16 – Eight(8) total seals

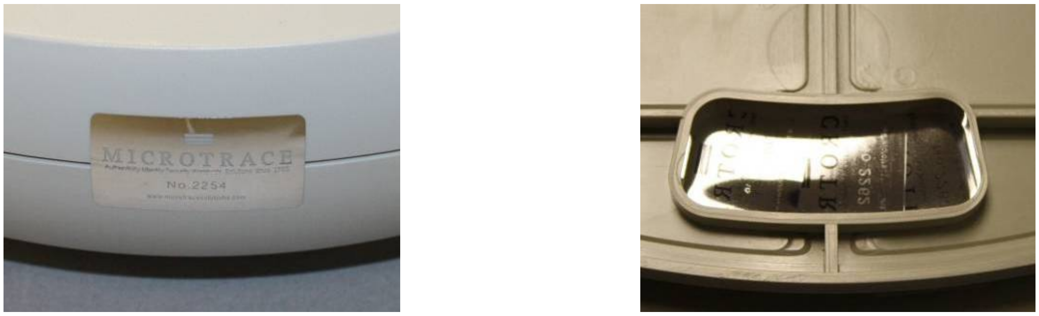
Tamper seal location covering mounting plate openings. Six (6) seals placed, Three (3) across each opening. Place labels on mounting plate prior to mounting array body.

XN8, XN12, XN16 – Eight(8) total seals

Tamper seal location on seams. Two (2) seals, placed on opposite sides.

XN4 – Two (2) total seals

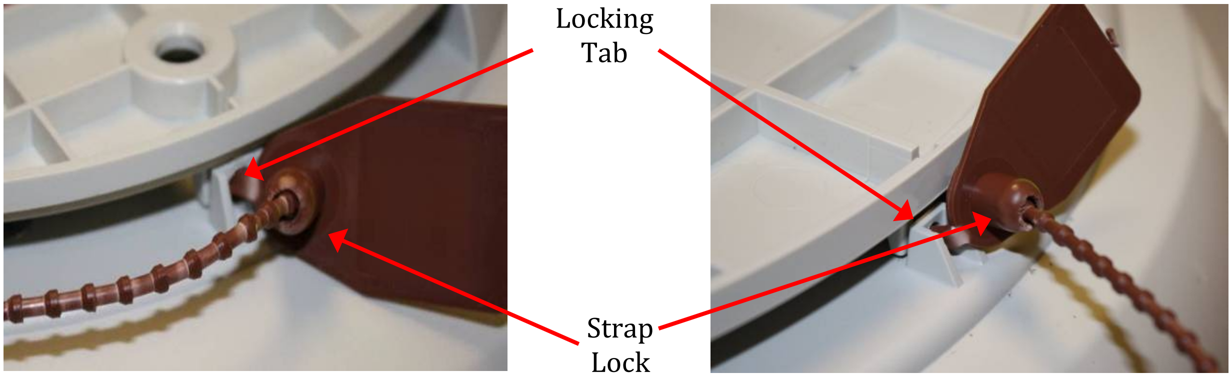
Figure 7 – Tamper-evident seal locations.
Location indicated by arrows and colored blocks



XN4 and XN8, XN12, XN16 - seam location **XN8, XN12, XN16 Mounting plate openings**

Figure 8 – Tamper-evident seal appearance

2. Apply the supplied tamper-evident security strap to the unit as indicated in the figure below. Each mounting plate and array body contains a single locking tab. The Array body is mounted to the mounting plate and rotated until the mounting plate clicks into place and the locking tabs are aligned. The security strap is threaded through the aligned locking tabs and then pulled through the strap lock until firmly affixed. The security strap should be pulled tight to disallow turning of the mounting plate. Tamper evidence may be indicated by a broken strap or cracked locking tab.



XN4 **XN8, XN12, XN16**

Figure 9 – Apply the security strap as shown through locking tab

11. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks that are outside of the scope of FIPS 140-2.

Table 9 – Mitigation of Other Attacks

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

12. Definitions and Acronyms

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CRC	Cyclic Redundancy Check
ECB	Electronic Code-Book
FIPS	Federal Information Processing Standards
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transfer Protocol
IAP	Integrated Access Points
LED	Light Emitting Diode
MAC	Message Authentication Code
MD5	Message-Digest #5
PSK	Pre-Shared Key
RADIUS	Remote Authentication Dial In User Service
RC4	ARCFOUR
RNG	Random Number Generator
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TDES	Triple – Data Encryption Standard
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TX/RX	Transmit / Receive
WEP	Wired Equivalent Privacy
Wi-Fi	IEEE 802.11 Wireless Networks
WMI	Web Management Interface
WPA	Wi-Fi Protected Access