

FIPS 140-2 Security Policy

Tropos Wireless IP Mesh Router

Tropos Networks

555 Del Rey Ave

Sunnyvale CA 94085

USA

Dec. 3rd, 2009

Document *Version 3.8*

© Copyright 2009 Tropos Networks.

This document may be freely reproduced whole and intact including this Copyright Notice.

TABLE OF CONTENTS

1. MODULE OVERVIEW.....4

2. SECURITY LEVEL10

3. SECURE OPERATION AND SECURITY RULES.....10

4. PORTS AND INTERFACES.....11

5. IDENTIFICATION AND AUTHENTICATION POLICY13

6. ACCESS CONTROL POLICY.....15

 ROLES AND SERVICES.....15

 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPs).....16

 DEFINITION OF CSPs MODES OF ACCESS17

7. OPERATIONAL ENVIRONMENT18

8. SECURITY RULES19

9. CONFIGURATION IN FIPS MODE20

10. HOW TO DETERMINE THE MODULE IS IN FIPS MODE21

11. PHYSICAL SECURITY POLICY.....21

 PHYSICAL SECURITY MECHANISMS21

 OPERATOR REQUIRED ACTIONS21

12. MITIGATION OF OTHER ATTACKS POLICY29

FIGURES

Figure 1 – Image of 5320 Cryptographic Module 4

Figure 2– Image of 6310/6320 Cryptographic Module 5

Figure 3 - Image of 7320 Cryptographic Module 6

Figure 4 – Logical Cryptographic Boundary 9

Figure 5 – Bottom View: Tamper labels on 5320..... 22

Figure 6 – Top View: Tamper labels on 5320 23

Figure 7 – Side View: Tamper labels on 5320 23

Figure 8 – Bottom View: Tamper labels on 6310/6320 24

Figure 9 – Side View: Tamper labels on 6310/6320 25

Figure 10 – Side View: Tamper labels on 6310/6320 25

Figure 11 – Bottom View: Tamper labels on 7320..... 26

Figure 12 – Top View: Tamper labels on 7320 27

Figure 13 – Side View: Tamper labels on 7320 27

Figure 14 – Lid for AC units..... 28

1. Module Overview

The Tropos 5320/6310/6320/7320 Wireless IP Mesh router uses 802.11 a/b/g/n WiFi standards for communications, and 802.11i for security. The primary purpose of a Tropos router is to provide wireless data connectivity in a secure fashion. The device is a multi-chip standalone module whose cryptographic boundary is the perimeter of the hard opaque commercial grade metal casing. No components are to be excluded from FIPS 140-2 requirements.

Figure 1, Figure 2, and Figure 3 below illustrate the cryptographic boundary.

Figure 1 – Image of 5320 Cryptographic Module



Figure 2– Image of 6310/6320 Cryptographic Module



Figure 3 - Image of 7320 Cryptographic Module



For the Tropos Wireless IP Mesh Router, the support firmware version is 7.3. There are 15 hardware versions covered by this document and they are listed in the table below:

Hardware Version	Radio (Quantity)	Power Supply	Battery
6310-3030	2.4GHz (1)	DC	No
6320-2531	2.4GHz(1) 5.4GHz(1)	DC	No
6320-3030	2.4GHz(1) 5.8GHz(1)	DC	No
5320-2531	2.4GHz(1) 5.4GHz(1)	AC	No
5320-2631	2.4GHz(1) 5.4GHz(1)	AC	Yes
5320-3030	2.4GHz(1) 5.8GHz(1)	AC	No
5320-3130	2.4GHz(1) 5.8GHz(1)	AC	Yes
5320-6000	2.4GHz(1) 5.8GHz(1)	DC	No
5320-6060	2.4GHz(1) 5.4GHz(1)	DC	No
7320-2531	2.4GHz(1) 5.4GHz(1)	AC	No
7320-2631	2.4GHz(1) 5.4GHz(1)	AC	Yes
7320-3030	2.4GHz(1) 5.8GHz(1)	AC	No

7320-3130	2.4GHz(1) 5.8GHz(1)	AC	Yes
7320-6000	2.4GHz(1) 5.8GHz(1)	DC	No
7320-6060	2.4GHz(1) 5.4GHz(1)	DC	No

For any Tropos router with DC power supply, the attached metal cover has 3 holes with following possible configurations:

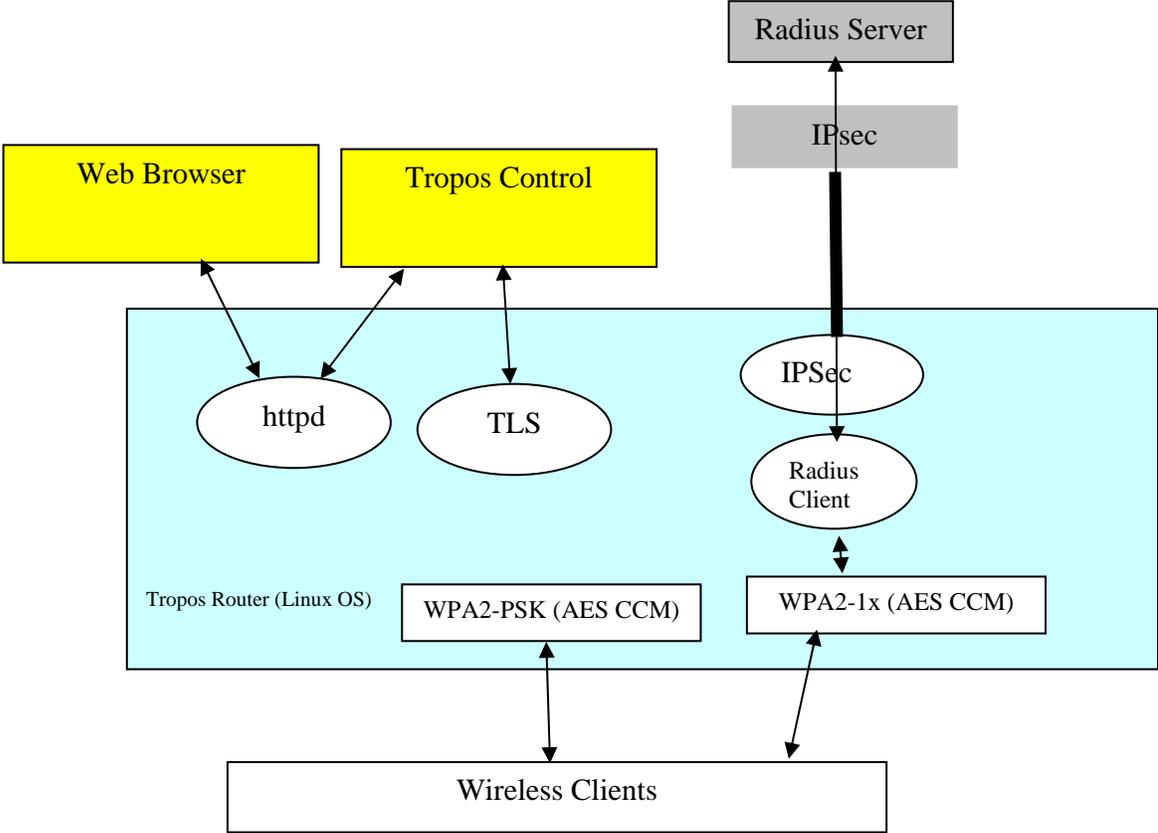
- 1- MGT port blocked, LAN port blocked, DC connected
- 2- MGT port blocked, LAN port connected, DC connected
- 3- MGT port connected, LAN port blocked, DC connected
- 4- MGT port connected, LAN port connected, DC connected.

For any Tropos router with AC power supply, the attached metal cover has either no hole or 2-holes, with the following possible configurations:

- 1- no hole cover
- 2- MGT port connected, LAN port blocked
- 3- MGT port blocked, LAN port connected
- 4- MGT port connected, LAN port connected

Figure 4 below is the logical cryptographic boundary of the Tropos module. Cryptographic officials manage the router via Web Browser or Tropos Control. Wireless clients must connect through WPA2-PSK or WPA2-1x protocols. IPsec is used to provide secure tunnel between the radius client inside the Tropos router and Radius Server.

Figure 4 – Logical Cryptographic Boundary



2. Security Level

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

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	2
Mitigation of Other Attacks	N/A

3. Secure Operation and Security Rules

In order to operate the Tropos Wireless IP Mesh Router securely, the operator should be aware of the security rules enforced by the module and should adhere to the physical security rules and secure operation rules required.

Approved mode of operation

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

1. Tropos Networks FIPS Crypto Library (OpenSSL) Algorithm Implementation:
 - AES CBC
 - HMAC SHA-1
 - SHA-1
 - DRNG – ANSI X9.31 with AES. This approved DRNG can be used, e.g., for generation of TLS secrets and IPsec keys
 - RSA – Signature Verification
 - Triple-DES CBC
2. Tropos Networks FIPS Crypto Library (IPsec) Algorithm Implementation:
 - AES CBC
 - HMAC SHA-1
 - SHA-1
3. Tropos Networks Atheros CCM Algorithm Implementation:
 - AES CCM

The cryptographic module supports the following non-FIPS approved algorithms and security functions that are allowed for use in FIPS mode:

- Diffie-Hellman (1024-bit modulus) allowed in FIPS mode for key agreement.
- RSA (1024-bit) allowed in FIPS mode for key exchange used by TLS. This key establishment method provides 80-bits of security.
- Hardware NDRNG. This is used only for seeding approved DRNG.

Non-FIPS mode of operation

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

- Blowcrypt
- RC4
- MD5 for hashing

4. Ports and Interfaces

The Wireless IP Mesh Router provides the following physical ports and logical interfaces:

5320 Tropos Mesh Router:

Physical Interface (Quantity)	Data Input	Data Output	Control Input	Status Output
Ethernet LAN/MGT Port (2)	Yes	Yes	Yes	Yes
Wireless Antenna Port (3)	Yes	Yes	Yes	Yes
IR Port (1)	Disabled in FIPS	Disabled in FIPS	Disabled in FIPS	Disabled in FIPS
LED (1)	No	No	No	Yes
Power Port	No	No	No	No

6310 Tropos Mesh Router:

Physical Interface (Quantity)	Data Input	Data Output	Control Input	Status Output
Ethernet LAN/MGT Port (2)	Yes	Yes	Yes	Yes
Wireless Antenna Port (3)	Yes	Yes	Yes	Yes
IR Port (1)	Disabled in FIPS	Disabled in FIPS	Disabled in FIPS	Disabled in FIPS
LED (1)	No	No	No	Yes
Power Port (POE-in via Ethernet LAN port)	No	No	No	No

6320 Tropos Mesh Router:

Physical Interface (Quantity)	Data Input	Data Output	Control Input	Status Output
Ethernet LAN/MGT Port (2)	Yes	Yes	Yes	Yes
Wireless Antenna Port (4)	Yes	Yes	Yes	Yes
IR Port (1)	Disabled in FIPS	Disabled in FIPS	Disabled in FIPS	Disabled in FIPS
LED (1)	No	No	No	Yes
Power Port (POE-in via Ethernet LAN port)	No	No	No	No

7320 Tropos Mesh Router:

Physical Interface (Quantity)	Data Input	Data Output	Control Input	Status Output
Ethernet LAN/MGT Port (2)	Yes	Yes	Yes	Yes
Wireless Antenna Port (4)	Yes	Yes	Yes	Yes
IR Port (1)	Disabled in FIPS	Disabled in FIPS	Disabled in FIPS	Disabled in FIPS
LED (1)	No	No	No	Yes
Power Port	No	No	No	No

5. Identification and Authentication Policy

Assumption of roles

The Tropos Wireless IP Mesh Router supports two distinct roles, a User and a Cryptographic Officer (CO). The CO performs all management and configuration responsibilities. The User is fulfilled by all wireless clients. The cryptographic module shall enforce the separation of roles using role-based operator authentication.

Table 2 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Role-based operator authentication	Shared Secret or RADIUS based authentication
Cryptographic-Officer	Role-based operator authentication	Password

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password (Web UI)	<p>All passwords in the cryptographic module must be a minimum of 8 characters chosen from a 72 character set. The probability that a random attempt will succeed or a false acceptance will occur is $1/72^8$ (1/722,204,136,308,736).</p> <p>To exceed a one in 100,000 probability of a successful random password guess in one minute, it would require more than 7 billion login attempts per minute, which far exceeds the operational capabilities of the cryptographic module to support.</p>
Pre-shared Key (802.11i, WPA-PSK)	<p>All pre-shared keys in the cryptographic module must be a minimum of 8 characters chosen from a 72 character set. The probability that a random attempt will succeed or a false acceptance will occur is $1/72^8$ (1/722,204,136,308,736).</p> <p>To exceed a one in 100,000 probability of a successful random key guess in one minute, it would require more than 7 billion authentication attempts per minute from the malicious client, which far exceeds the operational capabilities of the cryptographic module to support.</p>
EAP-TLS (802.11i, WPA-1X)	<p>With Radius authentication based on EAP-TLS via RSA 1024-bit certificates, which provides 80-bits of security strength. The probability that a random attempt will succeed or a false acceptance will occur is $1/2^80$.</p> <p>To exceed a one in 100,000 probability of a successful random key guess in one minute, it would require more than 10^{19} (10,000,000,000,000,000,000) authentication attempts per minute from the malicious client, which far exceeds the operational capabilities of the cryptographic module to support.</p>

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User:	<ul style="list-style-type: none"> • <u>Cryptographic operations – Encryption and Decryption of network data</u> • <u>Generation and use of 802.11i cryptographic keys</u>
Cryptographic-Officer:	<ul style="list-style-type: none"> • <u>Cryptographic Operations</u> • <u>Module Configuration</u> • <u>User Role Account and Authentication Management</u> • <u>Key Management</u> • <u>Self-Test</u> • <u>FIPS Mode Enable/Disable</u> • <u>IPsec Tunnel Establishment</u> • <u>Non-Security Related Module Parameters Configuration</u> • <u>System Upgrade and Downgrade</u> • <u>Restore factory defaults</u> • <u>Zeroization</u> • <u>Module Debugging</u> • <u>Logging</u> • <u>System Status</u>

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Show status: This service provides the current status of the cryptographic module through LED's. Note: The System Status service above is an authenticated service that provides

more specific information about the network.

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2 by power cycling the module.

Non-FIPS mode of operation

The following non-approved services cannot be used in FIPS mode of operation.

- SSH v2
- WEP
- WPA-TKIP
- SNMP
- TKIP

Definition of Critical Security Parameters (CSPs)

- Router-EMS Authentication Key
- Configurator (WebUI) password
- RADIUS Authentication Key
- RADIUS Accounting Shared Secret
- IPsec ISAKMP Shared Secret
- IKE session seed key (SKEYID)
- IKE session derivation key (SKEYID_D)
- IKE session encryption key (SKEYID_A)
- IKE session authentication key (SKEYID_E)
- IPSec authentication key
- IPSec encryption key
- 802.11i Pre-shared Key
- 802.11i Pairwise Master Key (PMK)
- 802.11i Group Master Key (GMK)
- 802.11i Group Temporal Key (GTK)
- 802.11i Pairwise Transient Key (PTK)
- 802.11i Key Confirmation Key (KCK)
- 802.11i Key Encryption Key (KEK)
- 802.11i Temporal Key (TK)
- TLS Master Secret
- TLS Session Keys
- TLS (HTTPS) RSA Private Key
- Manufacture Installed Router RSA Private Key
- Diffie-Hellman (DH) Shared Secret
- Diffie-Hellman (DH) Private Component
- Pseudo-random number generator (DRNG) Seed

- Pseudo-random number generator (DRNG) Seed Key

Definition of CSPs Modes of Access

Table 6 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

Table 5 – CSP Access Rights within Roles & Services

Roles

CO	User	Services	Cryptographic Keys and CSPs Access Operation
X	X	Cryptographic Operations	Use all 802.11i Keys
X	X	Generation and use of 802.11i cryptographic keys	Use all 802.11i Keys
X		Module Configuration	Use all TLS Keys
X		User Role Account and Authentication Management	Use all TLS Keys
X		Key Management	Generating, modifying, and entering pre-configured keys (passwords, keys entered during manufacturing)
X		Self-Test	SHA-1 checksum and DRNG
X		FIPS Mode Enable/Disable	Use all TLS Keys
X		IPsec Tunnel Establishment	Use all IKE and IPsec Keys and Diffie-Hellman Keys
X		Non-Security Related Module Parameters Configuration	Use all TLS Keys
X		System Upgrade and Downgrade	Use Manufacture Installed Router RSA Private Key
X		Restore factory defaults	Destroy all unprotected Keys and CSPs on FLASH.
X		Zeroization	Destroy all unprotected Keys and CSPs
X		Module Debugging	N/A
X		Logging	N/A
X		System Status	N/A

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the

Tropos Wireless IP Mesh Routers do not contain a modifiable operational environment. All software loaded into the module will be protected by digital signatures signed by Tropos.

8. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of Tropos Wireless IP Mesh Router.

1. The cryptographic module shall provide two distinct operator roles. These are the User role, and the Cryptographic-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 message traffic using the AES algorithm.
5. The cryptographic module shall perform the following tests:

A. Power up Self-Tests:

After power-up, the Tropos Router performs the “Cryptographic Algorithms Tests”, “Software Integrity Tests” and “Critical Functional Tests”, they are listed below.

The router will not output anything and provide any user services until all the Self Tests pass. If any of these tests fail, the router will restart automatically from this state. The Power Up Self Test will be re-run after the restart. If the router fails the Power Up Self Test 10 times consecutively, the router will zeroize itself, and all the CSPs on the router will be destroyed. Once the router enters this state, the Operator will need to contact Tropos Support to bring the router out of this state:

1. Cryptographic algorithm tests:
 - a. AES Known Answer Test for OpenSSL
 - b. AES Known Answer Test for IPsec
 - c. DRNG Known Answer Test
 - d. SHA-1 Known Answer Test for OpenSSL
 - e. SHA-1 Known Answer Test for IPsec
 - f. RSA Known Answer Test
 - g. HMAC Known Answer Test for OpenSSL
 - h. HMAC Known Answer Test for IPsec
 - i. Triple-DES Known Answer Test for OpenSSL
 - j. AES CCM Known Answer Test
2. Software Integrity Test (RSA signature validation and SHA-1 file integrity check)

B. Conditional Self-Tests:

1. Continuous Random Number Generator (CRNG) test – performed on NDRNG and DRNG

C. Firmware Upgrade Tests:

Upon firmware upgrade via Configurator or Tropos Control, the Tropos router performs SHA-1 integrity check and RSA signature verification on the loaded firmware. Note: To maintain validation, only FIPS validated firmware can be loaded during firmware upgrades. Otherwise, the module is in a non-Approved mode of operation.

6. At any time the cryptographic module is in a powered-on state, the operator shall be capable of commanding the module to perform the power-up self-test.
7. Prior to each use, the internal DRNG shall be tested using the conditional test specified in FIPS 140-2 §4.9.2.
8. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
9. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9. Configuration in FIPS Mode

During initialization, the CO must perform the following configuration steps in order to be in FIPS mode:

1. Enable “FIPS Mode”
2. Disable “Infrared Access Port”
3. SSH access must be kept disabled
4. Make sure both “Active Software Images” are FIPS validated images
5. Save “Last Known Good Profile”
6. Configure auth type for all ESSID’s with WPA2 AES-CCM only mode
7. Enable “IPsec for RADIUS” and configure IPsec related parameters
8. Set “Router-EMS Authentication Key”
9. “Configurator Password” must have minimum of 8 characters, and must be changed from the default CO password.
10. Set “Backward Compatibility” to “7.1 and later”

Mesh Service is allowed but mesh communication is considered plaintext for FIPS 140-2 purpose.

10. How to Determine the Module is in FIPS Mode

The operator can verify FIPS configuration via Configurator’s “Security and Password” page or via Tropos Control’s “Configuration View” page.

If the FIPS field is identified as “Enabled”, then the Module is in FIPS mode. Please also check other configuration options specified in Section 9 and make sure they are configured correctly.

11. Physical Security Policy

Physical Security Mechanisms

The Tropos 5320 Wireless IP Mesh Router multi-chip standalone cryptographic module includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with tamper evident seals.
- Tamper evident seals. Note: To operate in FIPS Approved mode the tamper evident seals shall be installed as indicated.
- Hard opaque metal enclosure.

Operator Required Actions

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test
Tamper Evident Seals	Once per week

Instructions to Apply Tamper Evident Seals

The following are the general instructions for applying tamper seals:

- Make sure the surface is clean with no accumulated dust
- Apply the label with no air bubbles inside or opening along the border

- When applying the label to secure a lid, make sure the label covers the lid surface as well as the surface on the box
- When applying the label for a connector or a blank plug on the lid, make sure the label covers the connector surface and the surface on the lid. Additionally, the blank plug or connector must be secured first before applying the label, such that the label does not twist or damage once applied to the flat surface of the connector or plug
- When applying the label along a edge on the box, make sure the label covers the top and bottom surfaces of the box

Figure 5 – Bottom View: Tamper labels on 5320 is a representative bottom view of 5320 hardware. The unit shows a lid with three holes and two connectors using two of the three openings. Two labels secure the connectors, one label covers the hole on the lid and two labels secure the lid. Any attempt to open the lid or the connectors should be evident on the seal.

Figure 6 – Top View: Tamper labels on 5320 is a representative top view of 5320 hardware. There are four labels securing all the four sides.

Figure 7 – Side View: Tamper labels on 5320 is a representative side view of 5320 hardware. It shows the label covering the top and bottom portion of the lid. Any attempt to lift the lid should break the seal on this label.

Figure 5 – Bottom View: Tamper labels on 5320



Figure 6 – Top View: Tamper labels on 5320



Figure 7 – Side View: Tamper labels on 5320



Figure 8 – Bottom View: Tamper labels on 6310/6320 shows the bottom view with four labels on the corners. Figure 9 – Side View: Tamper labels on 6310/6320 and Figure 10 – Side View: Tamper labels on 6310/6320 show the two side views. Note that the labels have to cover the grey base as well as the white cover so that any attempt to separate the two is evident on the labels.

Figure 8 – Bottom View: Tamper labels on 6310/6320



Figure 9 – Side View: Tamper labels on 6310/6320



Figure 10 – Side View: Tamper labels on 6310/6320



Figure 11 – Bottom View: Tamper labels on 7320



Figure 11 – Bottom View: Tamper labels on 7320 is a representative bottom view of 7320 hardware. The unit shows a lid with two holes and a connector using one of the openings. One label secures the connector, one label covers the hole on the lid and two labels secure the lid. Any attempt to open the lid or the connectors should be evident on the seals.

Figure 12 – Top View: Tamper labels on 7320 is a representative top view of 7320 hardware. There are four labels securing all the four sides.

Figure 13 – Side View: Tamper labels on 7320 is a representative side view of 7320 hardware. It shows the label covering the top and bottom portion of the lid. Any attempt to lift the lid should break the seal on this label.

Figure 14 – Lid for AC units shows the lid for the use on 5320 and 7320 AC units. The lid has no holes and hence only two labels would be required to secure the lid on the box.

Figure 12 – Top View: Tamper labels on 7320



Figure 13 – Side View: Tamper labels on 7320



Figure 14 – Lid for AC units



12. Mitigation of Other Attacks Policy

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