FIPS 140-2 Security Policy

Tropos Wireless IP Mobile Router

Tropos Networks
555 Del Rey Ave
Sunnyvale CA 94085
USA

Dec. 3rd, 2009

Document *Version 3.8*

TABLE OF CONTENTS

FIGURES

1. Module Overview

The Tropos 4210 Wireless IP Mobile router uses 802.11 b/g 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 below illustrates the cryptographic boundary.

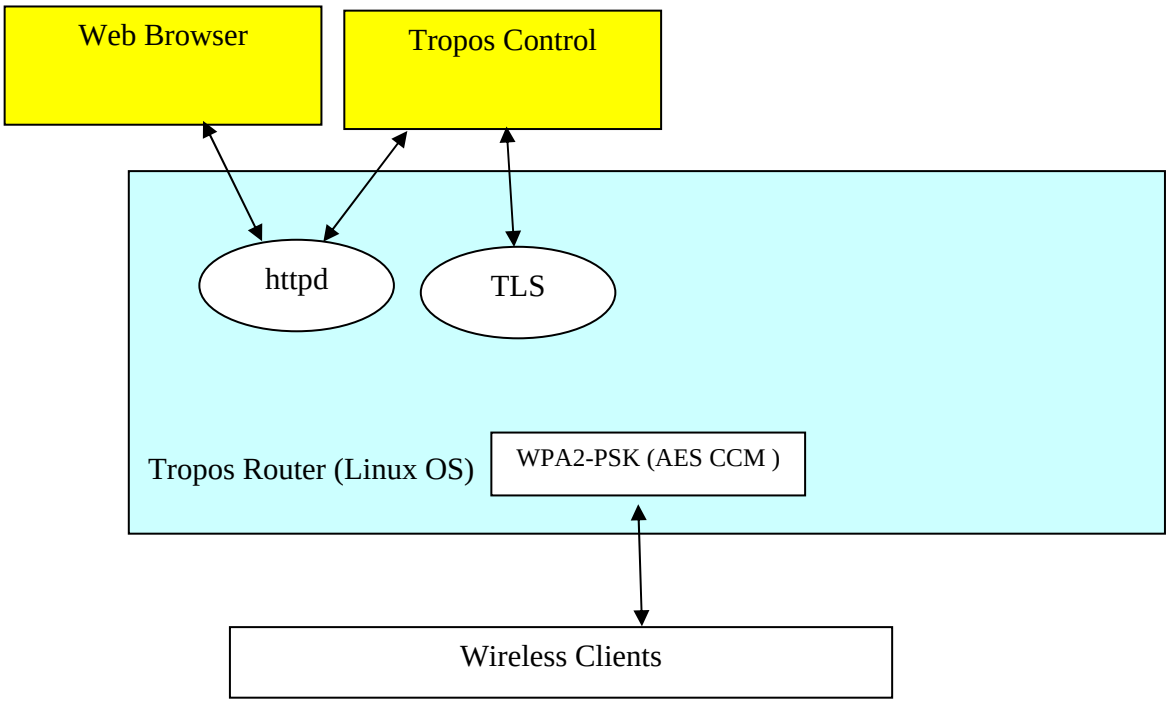
Figure 1 – Image of the 4210 Cryptographic Module

For the Tropos Wireless IP Mobile Router, the support firmware version is 7.3. There is only 1 hardware version covered by this document and it is listed in the table below:

Hardware Version	Radio (Quantity)	Power Supply	Battery
4210-2100	2.4GHz (1)	DC	No

Figure 2 below is the logical cryptographic boundary of the Tropos module. Cryptographic officials manage the router via Web Brower or Tropos Control. Wireless clients must connect through WPA2-PSK protocols.

Figure 2 – 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 Mobile 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 for generation of TLS secrets and IPsec Keys
    - RSA – Signature Verification
    - Triple-DES CBC
2. 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:

- 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 Mobile Router provides the following physical ports and logical interfaces:

4210 Tropos Mobile Router:

Physical Interface (Quantity)	Data Input	Data Output	Control Input	Status Output
Ethernet LAN/MGT Port (2)	Yes	Yes	Yes	Yes
Wireless Antenna Port (2)	Yes	Yes	Yes	Yes
USB Port (2) Only one is used	Yes	No	No	No
Console Port (2)	Disabled and Sealed in FIPS mode	Disabled and Sealed in FIPS mode	Disabled and Sealed in FIPS mode	Disabled and Sealed in FIPS mode
LED (1)	No	No	No	Yes
Power Port	No	No	No	No

5. Identification and Authentication Policy

Assumption of roles

The Tropos Wireless IP Mobile 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
Cryptographic-Officer	Role-based operator authentication	Password

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Password (Web UI)	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). 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.
Pre-shared Key (802.11i, WPA-PSK)	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). 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.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
User:	• Cryptographic operations – Encryption and Decryption of network data • Generation and use of 802.11i cryptographic keys
Cryptographic-Officer:	• Cryptographic Operations • Module Configuration • User Role Account and Authentication Management • Key Management • Self-Test • FIPS Mode Enable/Disable • Non-Security Related Module Parameters Configuration • System Upgrade and Downgrade • Restore factory defaults • Zeroization • Module Debugging • Logging • System Status

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-approved Services for FIPS:

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 Accounting Shared Secret
- 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
- 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		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 Mobile 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 Mobile 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. DRNG Known Answer Test
   c. SHA-1 Known Answer Test for OpenSSL
   d. RSA Known Answer Test
   e. HMAC Known Answer Test OpenSSL
   f. AES CCM Known Answer Test
   g. Triple-DES Known Answer Test for OpenSSL

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. SSH access must be kept disabled
3. Make sure both “Active Software Images” are release FIPS validated images
4. Save “Last Known Good Profile”
5. Configure auth type for all ESSID’s with WPA2 AES-CCM only mode
6. Set “Router-EMS Authentication Key”
7. “Configurator Password” must have minimum of 8 characters, and must be changed from the default CO password.
8. 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 4210 Wireless IP Mobile 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

Figure 3 – Side View: Tamper label on 4210 is a side view of the 4210 hardware. A single label secures the “GPS out” port and “Factory use” serial ports.

Figure 4 –Tamper labels on 4210 plate shows the bottom plate of the 4210 hardware. There are four labels securing the four screws.

Figure 3 – Side View: Tamper label on 4210

Figure 4 –Tamper labels on 4210 plate

12. Mitigation of Other Attacks Policy

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