MP-422F Mobility Point

Security Policy

Trapeze Networks

October 16, 2008

Copyright Trapeze Networks 2007. May be reproduced only in its original entirety [without revision].

TABLE OF CONTENTS

1. Module Overview

The Trapeze Networks MP-422F Mobility Point (access point) HW P/N MP-422F Rev. A, FW Version MSS 6.1.0.3 and 6.1.0.4 is a multi-chip standalone cryptographic module, whose primary purpose is to provide secure network communication to and from wireless users and connect them to an MX switch. The cryptographic boundary is defined as being the outer perimeter of the enclosure; the diagram below illustrates the cryptographic boundary.

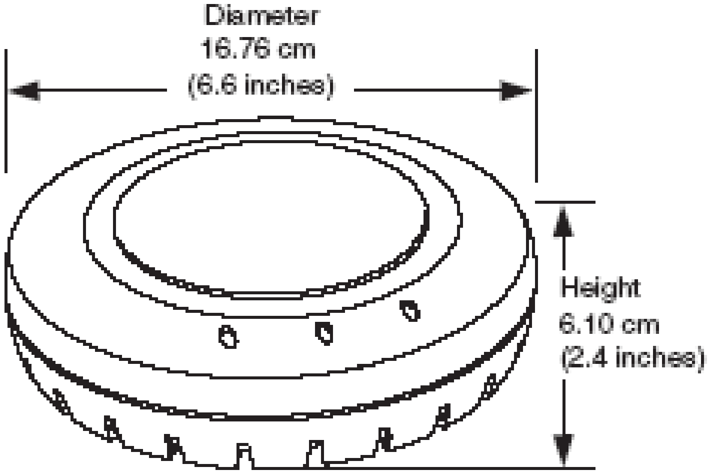

Figure 1 – Image of the Cryptographic Module (Top)

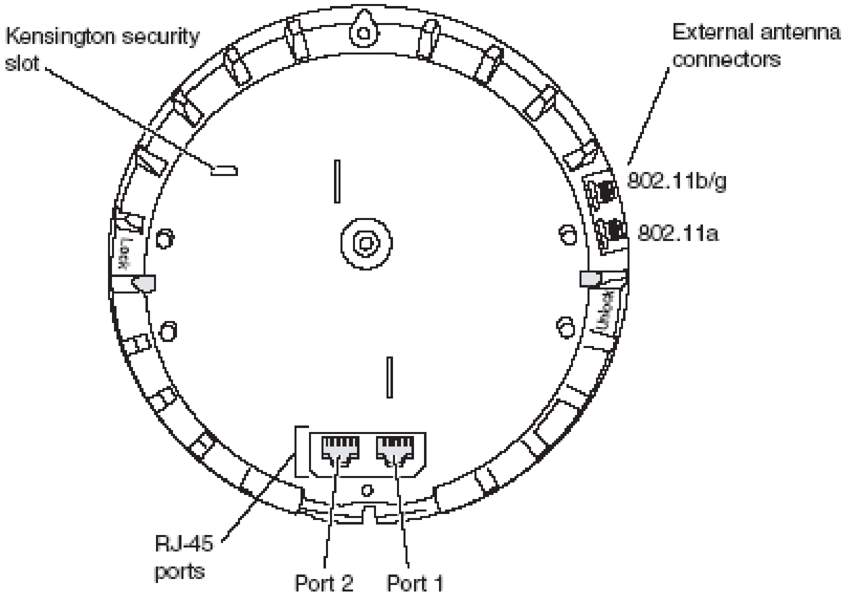

Figure 2 – Image of the Cryptographic Module (Bottom)

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. Modes of Operation

Approved mode of operation

The cryptographic module only supports an Approved mode and supports the following Approved algorithms:

- AES CCM (Cert. #641)
- SHA-1 (Cert. #676)
- HMAC SHA-1 (Cert. #330)

The module also supports the following non-Approved algorithms:

- RSA Key Wrapping (1024-bit keys provide an effective strength of 80-bits)
- MD5
- RNG (non-compliant)

The Approved software may be determined by verifying the software version is the Approved version via execution of the "Show Version Details" service from an attached MX switch.

4. Ports and Interfaces

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

10/100 Mbps Ethernet (Qty. 2):	Control In, Data In/Out, Status Out, Power In
External RF Antenna (Qty. 2):	Control In, Data In/Out, Status Out
LEDs:	Status Out

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module shall support two distinct operator roles (User and Cryptographic-Officer).

Table 2 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Role-based operator authentication	Knowledge of a Shared Secret (TK)
Cryptographic-Officer	Role-based operator authentication	Knowledge of a Shared Secret (MX Secret)

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Knowledge of a Shared Secret	The shared secret is at least 32-bits and at most 256-bits in length. The probability that a random attempt will succeed or a false acceptance will occur is at least 1/2^32 which is less than 1/1,000,000. Network latency and processor performance prevent a brute force attack from being successful within a given minute. The probability of a random attempt successfully authenticating to the module within one minute is less than 1/100,000 as a result of these resource restrictions.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services	
User	Secure Wireless Access:	Allows the User to browse the network through an encrypted channel.
Cryptographic-Officer:	Establish Secure Session:	Set-up an encrypted communication channel between the access point and the MX switch.
	Configure:	Specify the non-security relevant operational settings for the access point.
	Monitor:	Shows the status and statistics of the module.
	Session Management:	Install the User Transient Key or remove a User from the network.
	Access Point Management:	Reset/Zeroize the access point or Update the MX Secret.

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 and is invoked by power cycling the module.
- Show Status: Status information is available through the LEDs.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- MX Secret: Used to authenticate the CO to the module
- AP-MX Master Key: Used to encrypt traffic between the access point and MX
- AP-MX RSA Private Key: Used to unwrap the AP-MX Master Key
- Software Integrity Key: Used to verify the software integrity
- Transient Key: Used to provide data confidentiality for network traffic and authenticate the User.
- Group Transient Key: Used to provide data confidentiality for a network group

Definition of Public Keys

The following public key is contained in the module:

- AP-MX RSA Public Key: Used by an MX switch to wrap the AP-MX Master Key

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Use
- Import
- Export: N/A
- Zeroize

Table 5 – CSP Access Rights within Roles & Services

Role		**Service**	**Cryptographic Keys and CSPs Access Operation**
C.O.	**User**		
	X	Secure Wireless Access	Use Transient Key or Group Transient Key
X		Establish Secure Session	Use MX Secret Import AP-MX Master Key Use AP-MX RSA Private Key
X		Configure	Use AP-MX Master Key
X		Monitor	Use AP-MX Master Key
X		Session Management	Use AP-MX Master Key Import Transient Key or Group Transient Key
X		Access Point Management	Use AP-MX Master Key Import MX-Secret Import AP-MX RSA Private Key Zeroize All CSPs
X	X	Show Status	N/A
X	X	Self-tests	Use Software Integrity Key

7. Operational Environment

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

8. Security Rules

The cryptographic module'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 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 perform the following tests:

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

   1. Cryptographic algorithm tests:

   - AES CCM Known Answer Test
   - HMAC SHA-1 Known Answer Test
   - RSA Encrypt/Decrypt Known Answer Test

   2. Software Integrity Test (HMAC SHA-1 Verification)

   3. Critical Functions Tests: N/A.

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

   1. Continuous Random Number Generator Test (DRNG)

   2. Software Load Test (HMAC SHA-1 Verification)
5. Data output shall be inhibited during self-tests, zeroization, and error states.
6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9. Physical Security Policy

Physical Security Mechanisms

The cryptographic modules include the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with tamper evident seals.

Operator Required Actions

The operator is required to periodically inspect tamper evident seals.

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	**Application Guidance Details**
Tamper Evident Seals Tamper evident seals are provided to help indicate any attempt to transfer or remove the label in order to gain access inside the module. Operators should periodically inspect tamper evident seals. If you should detect any evidence of tampering, you should inform your management and security office immediately.	The module includes two tamper labels, which should be applied on opposing sides, bridging the gap between the two halves of the enclosure. *Upon placement of the seals, allow 24 hours for the adhesive seal to cure.* *Each TEL's position and corresponding serial no. should be recorded and logged for future reference.*

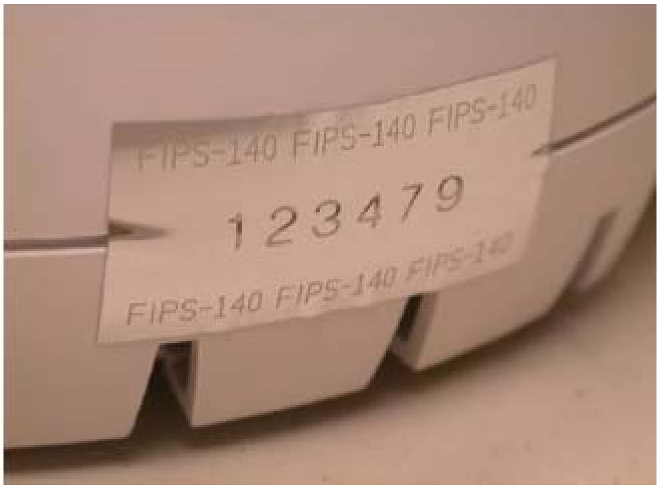

Figure 3 – Tamper Label Placement

10. Mitigation of Other Attacks Policy

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

11. Definitions and Acronyms

AES CCM	Advanced Encryption Standard Counter with CBC-MAC
SHA	Secure Hash Algorithm
MAC	Keyed Hash Message Authentication Code
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
MD5	Message Digest Algorithm 5
DRNG	Deterministic Random Number Generator