Wireless for the Outdoor Enterprise™

MD4000-FIPS Structured Mesh™ Module FIPS 140-2 Security Policy

Nov 2009

Corporate Headquarters
Meshdynamics, Inc.
2953 Bunker Hill Lane Ste 400
Santa Clara, CA 95054
USA
http://www.meshdynamics.com
Tel: 408 282 3574
Fax: 408 516 8987

Table Of Contents

Overview

This is a non-proprietary Cryptographic Module Security Policy for the **MD4000-FIPS Structured Mesh™ Module** from Meshdynamics, Inc, referred to in this document as the module.

The module contains 4 radio interfaces and complies with applicable FCC requirement for radios.

Note: This document may be copied in its entirety and without modification. All copies must include the copyright notice and statements on every page.

The validated firmware version is 2.5.72.

This security policy describes how the module meets the security requirements for FIPS 140-2 and how to run the module in a FIPS 140-2 mode of operation.

This policy was prepared as part of the Level 2 FIPS 140-2 validation of the **MD4000-FIPS Structured Mesh™ Module**.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2 –Security Requirements for Cryptographic Modules) details the U.S Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the **NIST** website at http://csrc.nist.gov/groups/STM/cmvp/

The document includes the following sections:

- **Security Levels**
  -describes the FIPS 140-2 security levels.
- **Physical Security**
  -describes how the module is physically secured using tamper evident seals.
- **Communication Ports and Interfaces**
  -describes the communication interfaces used by the module.
- **Secure Configuration**
  -describes processes for using the module in FIPS 140-2 approved mode.
- **Authentication**
  -describes how the module provides authentication of roles and services.
- **Cryptographic Key Management**
  -describes the various cryptographic security parameters used by the module.
- **Key Zeroization**
  -describes the procedure for clearing all security parameters on the module.
- **Self tests**
  -describes all the self-tests conducted by the module to ensure integrity.

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

Tamper Evidence

All Critical Security Parameters are stored and protected within each module's tamper evident enclosure. The Crypto Officer is responsible for properly placing all tamper evident labels. These security labels are fragile and cannot be removed without clear signs of damage to the labels.

The Crypto Officer should inspect the tamper evident seals periodically to verify they are intact.

Label Placement

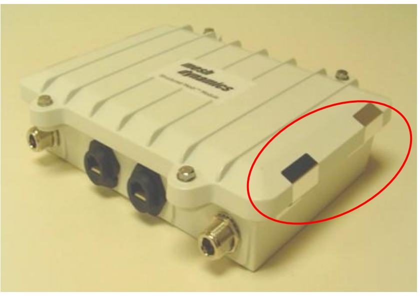


Fig. 1

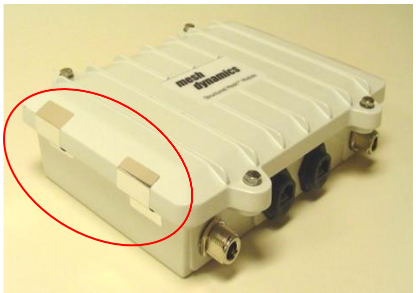


Fig. 2

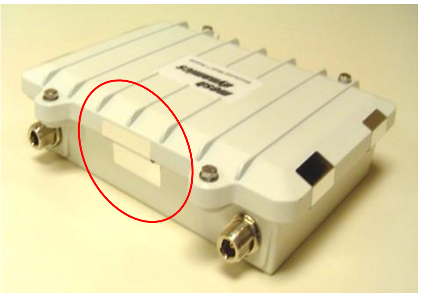


Fig. 3

Two tamper evident labels must be placed on the right-hand and left-hand sides of the module as shown in Figures 1 and 2.

One tamper evident label must be placed on the top edge of the lid.

The following procedure should be followed when placing the labels:

1. Turn off and unplug the module
2. Clean the module's enclosure of any grease, dirt or oil. Alcohol-based cleaning pads are recommended for this purpose.
3. Affix the label such that it secures the lid to the module's enclosure.

Physical Ports

Cryptographic Boundary

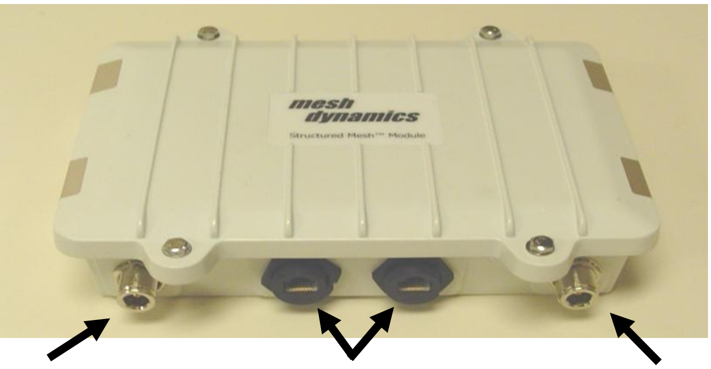
The cryptographic boundary is defined as the module’s enclosure.

The cryptographic boundary includes the following:

• 4 (Four) N-Female antenna ports

• 2 (Two) RJ-45 Ethernet ports, with only one port functional in FIPS 140-2 mode. The functional port in FIPS 140-2 mode is the left-hand Ethernet port.

Physical Ports



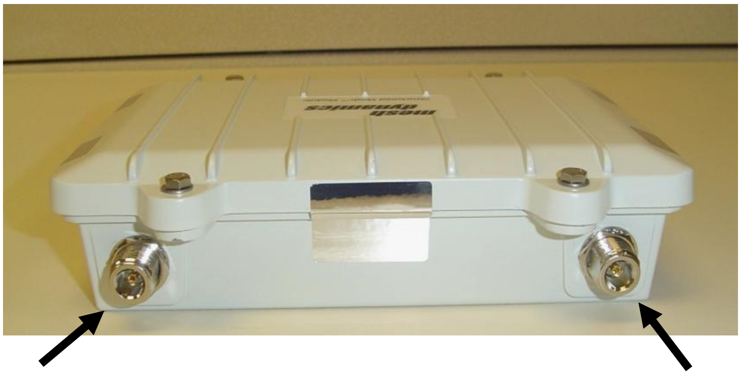
ANTENNA PORT

ETHERNET PORTS
LEFT PORT FUNCTIONAL

ANTENNA PORT

The MD4000-FIPS module has the following physical communication ports :

- 4 (Four) N-Female antenna ports
- 2 (Two) RJ-45 Ethernet ports, only one of which is functional in approved mode of operation.



ANTENNA PORT

ANTENNA PORT

FIPS 140-2 Logical Interfaces

Physical Port, Logical interface mapping

Physical Port	FIPS 140-2 Logical Interfaces
Left Ethernet	Data Input, Data Output, Control Input, Status Output
4 Antenna ports	Data Input, Data Output, Control Input, Status Output

Description

FIPS 140-2 Logical Interfaces	Description
Data Input	Data Input consists of ETHERNET packets entering the module via the Left Ethernet port. Data Input also consists of encrypted (128-bit AES-CCM/AES-KEYWRAP) packets entering the module via the 4 antenna ports.
Data Output	Data Output consists of ETHERNET packets exiting the module via the Left Ethernet port. Data Output also consists of encrypted (128-bit AES-CCM/AES-KEYWRAP) packets exiting the module via the 4 antenna ports.
Control Input	Control Input consists of 128-bit AES-ECB encrypted packets entering the module via the Left Ethernet or the 4 antenna ports.
Status Output	Status Output consists of 128-bit AES-ECB encrypted packets exiting the module via the Left Ethernet or the 4 antenna ports.

Overview

The MD4000-FIPS module meets the FIPS 140-2 Level 2 requirements. This section describes how to place and keep the module in a FIPS-approved mode of operation.

Operating the module without maintaining the following settings will remove the module from the FIPS-approved mode of operation.

NOTE: For FIPS 140-2 applications firmware upgrade can only be performed at the Meshdynamics facilities.

Approved Mode of Operation

The Crypto Officer must configure the following initialization procedures:

1. Using the Meshdynamics Network Viewer software, create a new FIPS 140-2 mode mesh network providing the following:
   - A unique mesh network community name
   - A random 128-bit AES encryption key
   - Check on the “FIPS 140-2 compliant” check box

2. Connect the personal computer directly to the module’s left ETHERNET port

3. Power-on the module and wait for about 60 seconds for the NMS software to detect the module.

4. Start the FIPS 140-2 Wizard tool from the Tools->Advanced Tools menu

5. Select the community created in Step 1

6. From the list of detected modules add the desired module to working list by selecting and pressing the ‘+’ button.

7. Configure the security settings for the module by pressing the Security button
   1. For each communication interface, set the Security Configuration to WPA Personal **(Only pre-shared key is allowed for authentication in FIPS mode of operation)**.
      1. Set the mode to WPA2/802.11i
      2. Set a random 256-bit pre-shared key
   2. For each Virtual-LAN, set the security configuration to WPA Personal **(Only pre-shared key allowed for authentication in FIPS mode of operation)**.
      1. Set the mode to WPA2/802.11i
      2. Set a random 256-bit pre-shared key

8. Press the update button to update the module with the security configuration.

9. Reboot the module by re-cycling power.

10. **If successful the NMS software shall indicate FIPS 140-2 approved mode of operation in the ‘Properties’ section.**

Approved Cryptographic Algorithms

The module supports many different cryptographic algorithms; however only the following FIPS approved algorithms may be used while in FIPS approved mode of operation:

- 128-bit AES-ECB encryption for securing the management of the module. (Certificate #728).
- 128-bit AES-CCM encryption for securing all packets transmitted between two modules and between the module and 802.11i authenticated clients over the wireless medium. (Certificate #728).
- ANSI X9.31 RNG using AES algorithm. (Certificate #425). Used for key generation.
- HMAC-SHA-1 for hashed message authentication of the WPA2/802.11i 4-way handshake. (Certificate #394) .
- SHA-1 for secure hashing. (Certificate #746).

Non-FIPS approved Algorithms

The module implements the following non-FIPS approved cryptographic algorithms:

- WEP-40, WEP-104 (RC4)
- 128-bit AES-KEYWRAP encryption for transferring 128-bit AES-CCM pair-wise and group keys generated using ANSI X9.31 algorithm between two modules. It uses the 128-bit key used for AES-ECB. (Certificate # 728). AES-KEYWRAP is not a FIPS-approved algorithm, however it is allowed in FIPS mode of operation.
- WPA/WPA2/802.11i using TKIP (RC4) cipher
- MD5
- HMAC-MD5 used for WPA/WPA2 TKIP
- Atheros 5414 hardware based RC4/CCM

Non-FIPS approved algorithms, except for AES-KEYWRAP cannot be used in FIPS mode of operation

Meshdynamics Network Viewer Software

For more information on using the Meshdynamics Network Viewer software please refer to the following documents:

- Network Viewer User Guide (MD4000_NMSGUIDE.pdf)

Services

SERVICE	DESCRIPTION
Management Service	Allows a crypto-officer to configure and manage a module, including installation and de-installation of the module.
Network Service	Allows authenticated wireless users to access the network using a 802.11 client.
Mesh Service	Allows multiple MD4000-FIPS modules to connect and relay packets.
Self Test	Triggers the power-on self test procedure by rebooting the module.
Zeroization Service	Allows a crypto-officer to zeroize the CSPs in the module.
Show Status	Allows crypto-officer to view the status of the module.

Roles

ROLE	DESCRIPTION	SERVICES
Crypto-Officer	Manages and configures modules.	Management, Network, Self Test, Zeroization, Show Status
User	Connects, authenticates, and access data on network.	Network, Self Test
Module User	Connects to other modules for relaying packets.	Mesh

NOTE: The Module allows multiple concurrent operators to use the module.

Crypto Officer Role Authentication

The module is managed using the Mesh Viewer NMS software.

The module uses a proprietary 128-bit AES-ECB encrypted protocol with 80-bit authentication.

The probability of a successful random attempt is ($1/2^{80}$).

The per-minute probability is 6.8×10^{-20}, which is less than the required 10^{-5}.

User Role Authentication

All wireless users authenticate using the IEEE 802.11i 4-way handshake protocol.

The protocol uses a 256-bit pre-shared key to generate a session specific 128-bit AES-CCM temporal key.

The key generation uses a 4-way handshake with a 128-bit HMAC-SHA1 based authentication.

The probability of a successful random attempt is ($1/2^{128}$).

The per-minute probability is 2.4×10^{-34}, which is less than the required 10^{-5}.

Module Role Authentication

Two modules authenticate using a Meshdynamics proprietary protocol.

The protocol uses a 128-bit AES-KEYWRAP with 80-bit authentication.

The probability of a successful random attempt is ($1/2^{80}$).

The per-minute probability is 6.8×10^{-20}, which is less than the required 10^{-5}.

The per-minute probability is based on 100 Mbps network speed with standard inter-frame gap of 9.6 micro-seconds between packets. The average frame size of 500 bytes is considered.

The module uses a variety of Critical Security Parameters during operation.

The following table includes a complete list of CSPs used by various services and protocols.

NOTE: All CSP's are stored in un-encrypted form.

NAME	ALGORITHM	STORAGE	SERVICE ACCESS MODES	DESCRIPTION
RNG seed (128-bits)	X9.31	SDRAM	Mesh Service: Module User – Execute Zeroization Service: Crypto-Officer – Delete	128-bit Seed for X9.31 RNG. It is initialized at startup.
RNG seed key (128-bits)	X9.31	SDRAM	Mesh Service: Module User – Execute Zeroization Service: Crypto-Officer – Delete	128-bit Seed key for X9.31 RNG.
PSK (256-bits)	Shared secret	Flash and SDRAM	Management Service: Crypto-Officer - Read/Write Network Service: User – Execute Zeroization Service: Crypto-Officer – Delete	The 256-bit 802.11i pre-shared key.
802.11i KCK for clients (128-bits)	HMAC-SHA1	SDRAM	Network Service: User – Execute Zeroization Service: Crypto-Officer – Delete	The KCK is used by 802.11i to authenticate 4-way and Group key handshake packets.
802.11i KEK for clients (128-bits).	AES	SDRAM	Network Service: User – Execute Zeroization Service: Crypto-Officer – Delete	The KEK is used by 802.11i to provide confidentiality for 4-way and group key handshake packets.
802.11i PTK for modules (128-bits)	AES-CCM	SDRAM	Mesh Service: Module User - Write, Execute Zeroization Service: Crypto-Officer – Delete	The PTK is the 802.11i session key for unicast communications
802.11i PTK for clients (128-bits)	AES-CCM	SDRAM	Network Service: User - Execute Zeroization Service: Crypto-Officer – Delete	The PTK is the 802.11i session key for unicast communications.
802.11i GTK for clients and modules (128-bits)	AES-CCM	SDRAM	Network Service: User - Execute Mesh Service: Module User - Write, Execute Zeroization Service: Crypto-Officer – Delete	The GTK is the 802.11i session key for broadcast and multicast communications.
IMCP key (128-bits)	AES-ECB	FLASH and SDRAM	Management Service: Crypto-Officer - Write, Execute Mesh Service: Module User - Execute Zeroization Service: Crypto-Officer – Delete	The IMCP key is used for encrypting and authenticating packets between modules and for management.

The Crypto Officer can zeroize and clear all cryptographic key information used by the module using the following initialization procedure:

1. Using the Meshdynamics MeshViewer Network Management System (NMS) software, open the FIPS 140-2 mode mesh network providing the following:
   - The mesh network community name
   - The 128-bit AES encryption key

2. Connect the personal computer directly to the module’s left ETHERNET port

3. Power-on the module and wait for about 60 seconds for the NMS software to detect the module.

4. Right-click on the icon representing the module and select ‘Restore Default Settings’

5. The module zeroizes and clears all cryptographic key information and sets itself in non-FIPS approved mode of operation, after it is rebooted.

NOTE: After a module is zeroized and rebooted, it does not operate in FIPS 140-2 approved mode of operation.

To use the module in FIPS 140-2 approved mode again, please refer to the ‘Secure Operation’ section.

Self Tests

The module includes an array of self-tests that are run during startup and periodically during operations to ensure all components are functioning correctly.

The following is the list of power-on self tests conducted by the module:

1. Firmware integrity test
2. AES-ECB known answer test
3. AES-CCM known answer test
4. HMAC-SHA1 known answer test
5. ANSI X9.31 RNG known answer test

In addition to the power-on self-tests, the module conducts the Continuous Random Number Generator test for the FIPS-approved ANSI X9.31 RNG

Error Indication

If any one of the self-tests fails, the module immediately reboots and the loss of the Ethernet link could be detected by the Ethernet hub to which the module is connected.
The Ethernet hub LED goes off and on as the module reboots and the self-tests are conducted again. If the failure continues the module reboots indefinitely.