Non-Proprietary Security Policy

MPM-1000

17 May 2007

Table of Contents

List of Figures

List of Tables

1. Introduction

1.1 Scope

This Security Policy specifies the security rules under which the L-3 Linkabit MPM-1000 must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by L-3 Linkabit. These rules, in total, define the interrelationship between the:

- module operators,
- module services,
- and critical security parameters (CSPs)

1.2 Module Overview

The MPM-1000 supports full duplex Single Channel Per Carrier (SCPC) Frequency Division Multiple Access (FDMA) and network-centric Multiple Frequency -Time Division Multiple Access (MF-TDMA) satellite terminal communications. When operated in the network-centric mode, the MPM-1000 implements the Network-Centric Waveform (NCW) specified by MIL-STD-188-EEE.

The modem provides Intermediate Frequency (IF) modulation and demodulation, Forward Error Correction (FEC) encoding/decoding, AES encryption/decryption, and a variety of I/O interfaces in a standard rack mountable package. The MPM-1000 is controlled by an external computer connected to the control (CDU) Ethernet interface. It can provide Control, Monitoring, & Alarm (CMA) services to the entire satellite terminal including upconverter, downconverter, antenna control processor, GPS, and power amplifier.

Figure 1. MPM-1000 IP Modem

1.3 FIPS 140-2 Security Level

The MPM-1000 has been tested to an overall FIPS 140-2 Level 2. Security levels achieved for each FIPS 140-2 subsection is given in Table 1.

TABLE 1. FIPS 140-2 Security Levels

FIPS 140-2 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

1.4 Crypto Module Physical Embodiment

The MPM-1000 is implemented as a multiple-chip standalone cryptographic module as defined by FIPS 140-2.

1.5 Crypto Module Cryptographic Boundary

The cryptographic boundary of the MPM-1000 is the whole chassis excluding the reference generator, power supply, and fans. These components are excluded from the cryptographic boundary because the malfunction of these components do not compromise the security of the module.

1.5.1 Security Related Components

The MPM-1000 components that are involved in the security function are:

- Modem Controller (MC) Circuit Card Assembly (CCA)
- Multi-Purpose Modem (MPM) CCA
- Alea I USB True Random Number Generator (Hardware RNG)
- Backplane
- Chassis
- Tamper-evident labels

1.5.2 Non-Security Related Components

The MPM-1000 components that are not involved in the security function and therefore excluded from FIPS 140-2 requirements are:

- Reference generator
- Power supply
- Fans

1.6 Hardware/Firmware Version Numbers

TABLE 2. MPM-1000 Part/Version Numbers

Module Name	Hardware Part Number	Firmware Version Number
MPM-1000	119811-1	120435-03 (Modem Controller CCA) 119881-05 (Multi-Purpose Modem CCA)

2. FIPS 140-2 Operational Modes

The MPM-1000 operates in two primary communication modes: Network-Centric and Spoke mode. At any point in time the MPM-1000 is either actively communicating in one of these two modes, or the terminal is off-line. The operating mode of the MPM-1000 is set using the Select Mode pull-down menu at the operator Human-Computer-Interface (HCI) window on the external control computer.

The MPM-1000 employs a third communication function, which operates when the terminal is off-line or concurrently with active Network-Centric mode communication. This function is referred to as the Secure Voice Orderwire (SVOW).

Only the Network-Centric mode utilizes FIPS-approved cryptography and security functions. The MPM-1000 is operating in the FIPS-approved mode when configured for Network-Centric mode or the terminal is offline. No cryptographic or security functions are used in the Spoke mode, nor are they used by the SVOW function. The MPM-1000 is operating in a non-FIPS mode when configured for Spoke mode. Note that all stored keys and other Critical Security Parameters (CSP) are automatically zeroized when the MPM-1000 is switched to the Spoke mode.

The MPM-1000 powers up into the off-line state. The operator must enter a command at the external control computer in order to enter one of the active communication modes or utilize the SVOW function.

The MPM-1000 exits both communication modes on command from the operator, returning to the off-line state. The SVOW function is enabled and disabled by an appropriate operator command. The SVOW cannot be enabled if the MPM-1000 is actively communicating in the Spoke mode.

2.1 Approved Security Algorithms and Functions

TABLE 3. Approved Security Functions – NCW Waveform Support

AES-256 (FPGA)	Traffic encryption/decryption algorithm (user data packets and NCW orderwire messages)

TABLE 4. Approved Security Functions – Secure Control Link (SSHv2)

AES-256 (Software)	SSHv2 symmetric encryption/decryption algorithm.
HMAC-SHA-1	SSHv2 data authentication algorithm.
SHA-1	SSHv2 data authentication algorithm.
DSA	SSHv2 entity authentication signature and software signature verification
DRNG	Digital Signature Standard Appendix 3.1/SHA-1 used to generate DSA keys and Diffie-Hellman parameters required for SSHv2 protocol. This DRNG is also used to derive operational AES keys from an externally supplied seed key in support of the NCW waveform.

2.2 Non-Approved Security Algorithms and Functions

TABLE 5. Non-Approved Security Functions

Diffie-Hellman	Key agreement algorithm used by SSHv2 to establish symmetric keys (AES and HMAC/SHA-1). Key establishment methodology provides 80 bits of encryption strength.
Hardware RNG	USB hardware randomizer used to seed the SSHv2 DRNG. This USB hardware RNG is installed within the cryptographic boundary during manufacturing.

3. Module Interfaces

TABLE 6. Physical & Logical Interface Summary

MPM-1000 Physical Interface	FIPS 140-2 Logical Port	Description
CDU ETHERNET	Control Input Status Output	Control of MPM-1000 in all modes; transport of encrypted CSPs associated with Network-Centric mode.
DATA ETHERNET	Data Input Data Output	Used in Network-Centric mode only. Plaintext input and output.
TX IF	Data Output	Interface to the RF transmission channel. Used in all modes. Ciphertext output in Network-Centric mode.
RX IF	Data Input	Interface to the RF transmission channel. Used in all modes. Ciphertext input in Network-Centric mode.
AC INPUT	Power Interface	Used in all modes.
5/10 MHZ REF IN	Control Input	Used in all modes. Externally generated analog sinusoid signal used as a time base by the MPM-1000.
10 MHZ REF OUT	Status Output	Used in all modes. Internally generated analog sinusoid signal used as a time base by the MPM-1000.
BASEBAND	Data Input Data Output	Used in Spoke mode only. Unmodulated digital data (no cryptography).
VOICE	Data Input Data Output	Used for SVOW (no cryptography). Unmodulated digital voice signal. Encryption of voice provided by external cryptographic equipment.
TERMINAL DEVICES	Data Input Data Output	Used in all modes. Control and status signals exchanged between the internal SNMP agent and satellite terminal elements external to the MPM-1000.
MIL-STD-165A MODEM CONTROL	Control Input Status Output	Used in Spoke mode only (no cryptography). Control and status signals exchanged between the internal MIL-STD-165A modem and external controller.
Modem Status LED	Status Output	Red when in FIPS error state; Green otherwise.
Power LED	Status Output	Indicates presence of power.

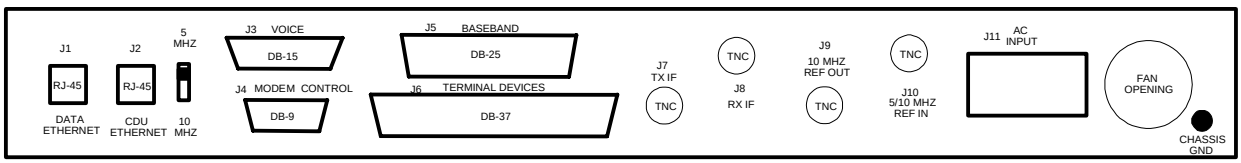

Figure 2. MPM-1000 Rear Panel Connectors

4. Access Control Policy

The MPM-1000 implements two authenticated operator roles: *Crypto-Officer* and *User*.

The Crypto-Officer and User roles are authenticated and assumed by successfully establishing an SSHv2 connection to the MPM-1000 at the control network interface.

All other control accesses to the MPM-1000 are via SNMPv2. Access through SNMP provides no security relevant functionality and as such does not require the assumption of a role or operator authentication.

The Crypto-Officer and User roles are authorized to perform the following services:

- Input TRANSEC keying parameters: seed keys (MSK) and Seeds
- Initiate a network over-the-air Reseeding sequence
- Initiate an over-the-air zeroization of another terminal(s)
- Install software updates

Unauthenticated SNMP has access to all services and functions provided by the MPM-1000 except those described above for Crypto-Officer and User roles.

The Crypto-Officer and User roles have access to all services and functions provided by the MPM-1000. Both roles are authorized to invoke all services and functions.

4.1 Concurrent Operator Access

The MPM-1000 permits simultaneous access of a single operator authenticated into the role of Crypto-Officer or User, and any number of operators accessing the MPM-1000 via SNMP.

4.2 MPM-1000 Services

TABLE 7. MPM-1000 Services[1]

Service	Unauthenticated Access	Crypto-Officer/ User
Load Current TRANSEC Seed Key		X
Load Current TRANSEC Seed		X
Load Future TRANSEC Seed Key		X
Load Future TRANSEC Seed		X
Initiate over-the-air network reseed		X
Initiate over-the-air-zeroize		X
Load software update		X
Secure control (SSHv2)		X
Non-secure control (SNMPv2)	X	X
Initiate self tests (non-FIPS)	X	X
Initiate self tests (FIPS)	X	X
Request status	X	X
Set terminal configuration	X	X
Initiate Network-Centric Mode communications		X
Terminate Network-Centric Mode communications		X
Initiate Spoke Mode communications	X	X
Terminate Spoke Mode communications	X	X
Secure Voice Orderwire (SVOW)	X	X
Request over-the-air terminal reseed		X
Zeroize local terminal	X	X
Shutdown Terminal	X	X
Change SSHv2 client authentication key		X
Delete SSHv2 client authentication key		X

Note: All services are invoked by operator selections made at the control computer GUI.

4.2.1 Load Current TRANSEC Seed Key

This operation transfers a TRANSEC Seed Key into the MPM-1000's "Current TRANSEC Seed Key" storage location. The MPM-1000 stores only one current seed key at any one time. The Current TRANSEC Seed Key is used (in conjunction with the Current TRANSEC Seed) to generate operational NCW keys (MEKs) when the operator activates the terminal for Network-Centric mode operation.

4.2.2 Load Current TRANSEC Seed

This operation transfers a TRANSEC Seed into the MPM-1000's "Current TRANSEC Seed" storage location. The MPM-1000 stores only one current Seed at any one time. The Current

TRANSEC Seed is used (in conjunction with the Current TRANSEC Seed Key) to generate operational NCW keys (MEKs) when the operator activates the terminal for Network-Centric mode operation.

4.2.3 Load Future TRANSEC Seed Key

This operation transfers a TRANSEC Seed Key into the MPM-1000's "Future TRANSEC Seed Key" storage location. The MPM-1000 stores only one future seed key at any one time. The Future TRANSEC Seed Key is used (in conjunction with the Future TRANSEC Seed) to generate operational NCW keys (MEKs) when the network executes a "changeover" to the next seed key cryptoperiod.

4.2.4 Load Future TRANSEC Seed

This operation transfers a TRANSEC Seed into the MPM-1000's "Future TRANSEC Seed" storage location. The MPM-1000 stores only one future Seed at any one time. The Future TRANSEC Seed is used (in conjunction with the Future TRANSEC Seed Key) to generate operational NCW keys (MEKs) when the network executes a "changeover" to the next seed key cryptoperiod.

4.2.5 Initiate Over-The-Air Network Reseed

This service, initiated by a command entered by the operator, results in the network distribution of a Future Seed Key and changeover schedule. The changeover time parameter is entered by the operator as part of the command entry sequence. The Future Seed Key distributed to the network is the one stored in the initiating terminal at the time the command is entered. If the command is entered at a Network Member terminal, the Future Seed Key and changeover schedule is first transferred to the Network Controller Terminal (via ROW message). The Network Controller Terminal then distributes the Future Seed Key and changeover schedule to the network (via broadcast FOW message). Note that the Future Seed Key, as is all data transmitted by the terminal, is encrypted with the current MEK.

4.2.6 Initiate Over-The-Air Zeroize

This service, initiated by a command entered by the operator, causes a zeroize message to be transmitted to a targeted network terminal. The terminal address of the targeted terminal is entered by the operator as part of the command entry sequence. All secret keys, private keys, and CSPs are zeroized upon invoking the OTAZ command.

4.2.7 Load Software Update

This service is used to load new software to the MPM-1000. All software downloads are cryptographically authenticated by digital signature verification.

4.2.8 Secure Control

The secure control service refers to any control activity that requires an SSHv2 connection to the MPM-1000 control Ethernet port.

4.2.9 Non-Secure Control

The non-secure control service refers to any control activity that does not require an SSHv2 connection to the MPM-1000 control Ethernet port. Non-secure control connections are SNMPv2 connections and can't be used to access any security relevant functionality.

4.2.10 Initiate Self-Tests (Non-FIPS)

This service is the standard terminal Built-In-Test (BIT) function. Standard terminal BIT does not include FIPS-required testing, and is initiated by the operator as required.

4.2.11 Initiate Self-Tests (FIPS)

This service represents the FIPS-required security testing, and is initiated automatically upon power up without intervention by the operator.

4.2.12 Request Status

This service returns various status indicators to the operator HCI upon request.

4.2.13 Set Terminal Configuration

This service allows the operator to set various terminal parameters via the HCI. The operator configurable settings are summarized in Table 8.

TABLE 8. Terminal Configuration Settings Summary

Operator Configurable Items	Functions
Alarms Settings	The operator can change the priority of non-security related alarms and whether or not it will sound the audible indicator.
Satellite Data	The operator can enter information about the satellites that will be used for the network.
Network Centric Waveform Setup	The operator can set the configuration of detailed aspects of the Network Centric Waveform mode such as the Forwarding Table Age Limit.
System Settings	The operator can configure various satellite terminal system parameters such as Location, Up/Down Converter frequencies and Frequency Reference settings.
IP Address Settings	The operator can change the IP addresses of the MPM-1000's Control Ethernet and Data Ethernet ports. The Net Mask and Default Gateway of the Data Ethernet port can also be changed.

4.2.14 Initiate Network-Centric Mode Communications

This service invokes Network-Centric mode traffic data encryption and decryption (AES). However, the service is not available to unauthenticated accesses (SNMP) unless and until it is enabled by an authenticated Crypto Officer or User. The service is enabled by the loading of a TRANSEC Seed.

4.2.15 Terminate Network-Centric Mode Communications

This service causes the MPM-1000 to log out of the NCW network and cease Network-Centric mode communications.

4.2.16 Initiate Spoke Mode Communications

This service invokes Spoke operation. Spoke mode operation does not utilize any cryptographic functionality. All stored keys and other Critical Security Parameters (CSP) are automatically zeroized when the MPM-1000 is switched to the Spoke mode.

4.2.17 Terminate Spoke Mode Communications

This service causes the MPM-1000 to cease Spoke mode communications.

4.2.18 Shut Down Terminal

This service represents the removal of power from the MPM-1000.

4.2.19 Secure Voice Orderwire (SVOW)

This service allows the operator to conduct Secure Voice Orderwire communication concurrently with Network-Centric operation or when the terminal is in the off-line state. The SVOW function does not utilize any cryptographic functionality.

4.2.20 Request Over-The-Air Terminal Reseed

This service allows the operator of a Member Terminal to request a Future Seed Key from the Network Control Terminal. The request is initiated by operator command at the HCI. The Future Seed Key is transferred to the Member Terminal over-the-air within a directed FOW message. Note that this message, along with all FOW and ROW messages, is encrypted using the current operational key.

4.2.21 Zeroize Local Terminal

This service allows the operator to zeroize all CSPs stored in the terminal. Local zeroize is initiated by operator command at the HCI.

4.2.22 Change SSHv2 Client Authentication key

This service overwrites an existing SSHv2 client ID key with a new one. This is done via secure SFTP, which requires the operator be authenticated.

4.2.23 Delete SSHv2 Client Authentication key

This service deletes the SSHv2 client ID public key in the MPM-1000. This requires internal access to the module (see Section 11.3). Operator authentication is achieved by external controls on equipment tamper labels.

4.3 MPM-1000 Critical Security Parameters (CSPs)

TABLE 9. MPM-1000 CSPs

CSP	Definition
Current Message Seed Key (MSK)	Seed key used to derive operational keys (MEKs)
Current Seed	Variable that modifies MEK generation
Future MSK	Seed key used to derive operational keys (MEKs)
Future Seed	Variable that modifies MEK generation
Message Encryption Key (MEK)	Operational AES keys; used to encrypt/decrypt NCW network data
SSHv2 Server ID key pair	DSA key pair used to authenticate MPM-1000 to the control computer (SSHv2 client)
SSHv2 Server Ephemeral Diffie-Hellman Key	Private part of DH key pair used to establish a shared secret with the control computer (SSHv2 client)
SSHv2 Symmetric Encryption Key (AES)	Derived from the DH shared secret; used to encrypt the CDU Ethernet link
SSHv2 Symmetric MAC key (HMAC)	Derived from the DH shared secret; used to authenticate the CDU Ethernet link data

TABLE 10. MPM-1000 Public Keys

Public Keys	Definition
CO/User DSA Public Key	The public key that is used to authenticate the CO and User roles.
SSHv2 Server ID Public Key	The public key component of the SSHv2 Server ID key pair.
Titan Public Key	This public key is used for signature verification of firmware updates in order to protect against unauthorized modification.
SSHv2 Server Ephemeral Diffie-Hellman Key	Public part of DH key pair used to establish a shared secret with the control computer (SSHv2 client)

TABLE 11. CSP Access – Crypto-Officer/User

Service	CSP	CSP Access Description
Load Current TRANSEC Seed Key	Current MSK	Load to terminal [1]
Load Current TRANSEC Seed	Current Seed	Load to terminal [1]
Load Future TRANSEC Seed Key	Future MSK	Load to terminal
Load Future TRANSEC Seed	Future Seed	Load to terminal
Initiate over-the-air network reseed	Future MSK	Distribute to network via over-the-air network reseed[2]
Initiate over-the-air-zeroize	All CSPs in remote terminal	Zeroize all CSPs in targeted remote terminal
Load Software Update	SSHv2 CSPs	Software loaded via SFTP
Initiate self tests (non-FIPS)	N/A	N/A
Initiate self tests (FIPS)	N/A	N/A
Request status	N/A	Monitor presence
Set terminal configuration	N/A	N/A
Initiate Network-Centric Mode Communications	MEKs	Encrypt/decrypt RF network data
Terminate Network-Centric Mode Communications	N/A	N/A
Initiate Spoke Mode Communications (non-cryptographic)	All CSPs	Zeroize
Terminate Spoke Mode Communications (non-cryptographic)	N/A	N/A
Secure Voice Orderwire (SVOW)	N/A	N/A
Request over-the-air terminal reseed	Future MSK	Request via orderwire and store
Zeroize local terminal	All CSPs	Zeroize
Non-secure control (SNMP)	N/A	N/A
Secure control (SSHv2)	SSHv2 CSPs	Negotiate SSHv2 protocol
Shutdown terminal	MEKs, Current/Future Seed, ephemeral SSHv2 CSPs	Zeroize (RAM power loss)
Install SSHv2 client authentication key	SSHv2 Client Public Key	Store in uninitialized module (FTP)
Change SSHv2 client authentication key	SSHv2 Client Public Key	Overwrite existing key in module (SFTP)
Delete SSHv2 client authentication key	SSHv2 Client Public Key	Manually delete from module memory (physical switch inside security boundary)

1. MEKs are automatically generated when both Current MSK and Seed are loaded
2. New MEKs are automatically generated at designated changeover time

5. Identification and Authentication Policy

The MPM-1000 utilizes the SSHv2 "public key" authentication method to authenticate the Crypto Officer and User, wherein the external controlling computer (operator) is required to cryptographically prove it owns the private key that matches the public key that has been pre-stored in the MPM-1000. This proof is provided in the form of a digital signature.

The SSHv2 identity key pair is a DSA 1024 key. The strength of the authentication is cryptographically equivalent to an 80-bit symmetric key. Therefore, the operator authentication mechanism employed by the MPM-1000 associates a false acceptance or random access rate of one in 2^{80} or 1.2×10^{24}. During each access attempt, the Client (candidate operator) posts its 1024-bit public key to the SSH Server in the MPM-1000. Assuming for the purpose of calculation that posting of the client key was the only data transmitted during an attempted SSH access, then 5,859,375 accesses could be attempted every minute on the 100 Mbps MPM-1000 Control Ethernet port. Since the probability of a fortuitous authentication success using random data is one in 1.2×10^{24} (or 8.3×10^{-25}), the probability of a fortuitous authentication success in one minute is one in 2.1×10^{17} (or 4.86×10^{-18}). This is less than the one in 100,000 (or 1×10^{-5}) probability required by FIPS 140-2.

TABLE 12. MPM-1000 Authentication

Role	Authentication Type	Auth. Data Required
Crypto-Officer	Role-based	Identity Key Pair (DSA 1024)
User	Role-based	Identity Key Pair (DSA 1024)

6. Key Associations

The MPM-1000 utilizes keys in two domains:

- Keys required for Network-Centric Waveform (NCW) communication
- Keys required for the secure local CDU Ethernet connection (SSHv2)

The MPM-1000 uses a public/private key pair to authenticate software downloads (only the public component is stored in the MPM-1000).

6.1 NCW Keys

NCW operational keys are internally generated using the DSS Appendix 3.1/SHA-1 DRNG with externally supplied seed key and seed. The MPM-1000 stores only one current seed key and seed, and may store one future seed key and one future Seed. The nominal crypto period of a seed key is six months. During a seed key changeover, the future seed key and seed overwrite the current parameters, becoming the new current values.

The MPM-1000 generates thirty-two operational keys from the seed key and seed. The operational keys are labeled 0 through 31. The particular operational key to be used by the NCW network at any point in time (current operational key) is determined by a mapping of the current week-of-year to a key number. In an NCW network, only one terminal operates as the Network Controller Terminal (NCT). It is the NCT that determines the current operational key, which is referenced by key number within an unencrypted field in each Reference Forward Orderwire message transmitted by the NCT. All other terminals in the network, Network Terminals (NTs), determine the current operational key by reading the key number field in the Reference FOW.

The cryptoperiod of an NCW operational key is one week. The NCT also drives the rollover from one operational key to the next. The NCT does this by transmitting a rollover command message sequence in the Reference FOW when the network frame count equals a value that corresponds to one week in elapsed time. The rollover message sequence directs the NTs to begin encrypting/decrypting network traffic using the next operational key number.

MSKs are associated with the calendar date, as indicated in the Effective Date field that is logically bound (by CRC) to the random seed data. MEKs are derived from the combination of MSK and TRANSEC Seed. MEKs are therefore associated with both time, via the Effective Date of the parent MSK, and the User or Crypto Officer who enters (possesses) the seed.

6.2 SSHv2 Keys

The SSHv2 protocol, as implemented by the MPM-1000, uses static client/server ID key pairs for entity authentication and ephemeral keys for data encryption and data authentication (MAC). The MPM-1000 functions as the SSHv2 server and the external controlling computer (connected to the CDU Ethernet port) functions as the SSHv2 client.

The public component of the client ID key pair must be installed in the MPM-1000 file system prior to the establishment of a secure connection (see Crypto Officer and User Guidance). The MPM-1000 automatically generates the server ID key pair during initialization using an approved RNG. The public component of the server ID key pair is posted to the client during the SSHv2 connection establishment phase.

The SSHv2 protocol produces symmetric keys for data encryption and authentication from a shared secret value created by Diffie-Hellman key agreement. The Diffie-Hellman public keys are generated ephemerally using an approved RNG.

7. Module Self Tests

7.1 Power Up Self Tests

The MPM-1000 performs self-tests of all FIPS-approved algorithms and security functions during terminal initialization. Terminal initialization is performed at power up and after a terminal reset. The specific tests included are listed below.

- Software Integrity Test (32 and 128-bit EDC)
- SSHv2 DRNG Known Answer Test
- SSHv2 AES-256 Known Answer Test
- SSHv2 HMAC/SHA-1 Known Answer Test — Encrypt/Decrypt
- SSHv2 SHA-1 Known Answer Test
- SSHv2 DSA (1024 bit) Pairwise Consistency test
- NCW TRANSEC AES-256 (FPGA) Known Answer Test — Encrypt/Decrypt
- Other Critical Functions (see 7.3)

The MPM-1000 inhibits all data output from the data output ports when performing FIPS testing. The data output ports include the Data Ethernet and TX IF interface. The front panel Modem Status LED will remain GREEN if power up self testing completes without a failure. The LED is illuminated RED if a failure is detected during any of the self tests.

7.2 Conditional Self Tests

The MPM-1000 performs certain self tests of FIPS-approved algorithms and security functions prior to each use of the function. These conditional FIPS tests are listed below.

- SSHv2 RNG Continuous RNG Test
- Hardware RNG Continuous RNG Test
- SSHv2 Server ID Key Pairwise Consistency Test
- Software Load Test (DSA signature verification)
- Other Critical Functions (see below).

7.3 Other Critical Functions

In addition to the approved algorithm and security function testing cited above, the MPM-1000 employs two critical functions that are unique to the MPM-1000 application. The first of these functions is called the Seed Key/Seed Comparison Test. This test insures that the MSK seed key and Seed parameters applied to the MEK generation process are not equivalent. This test is applied whenever the MEK generation function is called.

The other critical function is called the Seed Format Test. This test insures that the Seed entered by the operator meets the size and character content requirements of a Seed. This test is applied whenever the operator enters a Seed. .

During power up self testing, a MSK and Seed, with identical bit content, are passed to the MEK generation function. The Seed Key/Seed Comparison Test must detect the illegal condition or the test will fail.

During power up self testing, a Seed with illegal format is passed to the Seed Format Test, which must detect the illegal format or the test will fail.

7.4 Self Test Failures

The MPM-1000 enters a FIPS error state if any FIPS-required power up or conditional test fails. The front panel "Modem Status" LED is illuminated red to indicate that the module is in the FIPS error state. The FIPS error state can only be exited by cycling the power to the MPM-1000 or initiating a terminal reset. The MPM-1000 inhibits all output from the data output ports when in the FIPS error state. The data output ports include the Data Ethernet, TX IF, Voice (SVOW), and Terminal Devices interfaces. The paths used to output data at these interfaces are also logically disconnected from the processes performing key generation and zeroization of cryptographic keys and CSPs using globally visible software state flags. The processes that output data will not do so if the MPM-1000 state condition flags indicate that the security critical processes listed above are in progress.

8. Physical Security

The security boundary of the MPM-1000 exists at the outer perimeter of the chassis. Tamper evidence is provided by four tamper-evident labels applied on the outer surface of the chassis.

The MPM-1000 chassis consists of three separable components as shown in Figure 4. The labels must be installed as shown in Figure 5. This ensures that the integrity of at least one of the tamper labels will be breached if any of the chassis components are dislocated.

Figure 3. Tamper Label

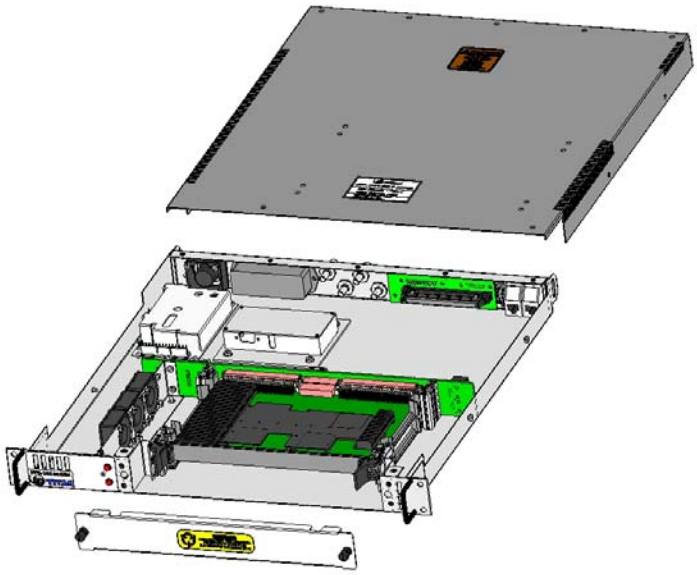

Figure 4. MPM-1000 Chassis Components

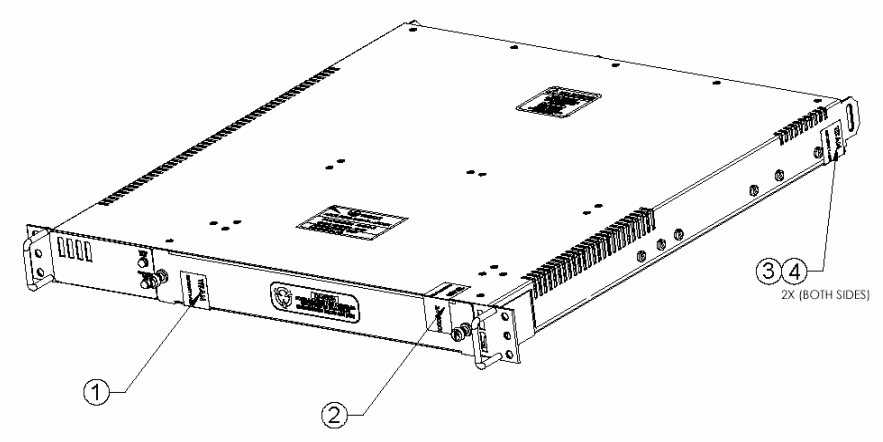

Figure 5. Tamper Label Placement

8.1 Tamper Label Inspection & Handling

The tamper labels should be inspected for evidence of tamper prior to each use of the system, particularly when the MPM-1000 has been stored unattended or has otherwise been accessible to untrusted personnel. Evidence of tamper should be reported to the local manager responsible for communications and/or facility security.

Replacement tamper evident labels should be obtained from L3 Linkabit or other sources that have been approved by L3 Linkabit. Unused labels are security-sensitive items and should be handled accordingly. They should be stored under lock and managed by security personnel. Tamper labels are each marked with a unique serial number. A record of the label serial numbers affixed to each MPM-1000 unit should be maintained and stored securely.

9. Delivery & Operation

This section contains a procedure to insure that MPM-1000 units are safely shipped, installed, and initialized at the user's facility. The procedure addresses the following threats:

- Malicious modification of internal MPM-1000 components while in transit
- Installation of a malicious SSHv2 client public ID key prior to initialization at the user's facility

9.1 L3 Linkabit Production Facility

Unit production testing will be performed prior to applying the MPM-1000 tamper labels, using a test SSHv2 client ID key. After testing, the test key will be deleted by activating the MC INIT button on the MPM-1000 internal backplane. The chassis will be closed and the tamper labels applied immediately after clearing the test key.

9.2 MPM-1000 Units In Transit

No special handling of MPM-1000 units is required while in transit.

9.3 Receipt and Inspection at the User's Installation Facility

The MPM-1000 user should carefully inspect the tamper labels for evidence of tampering once it has arrived at the installation site. The user should contact L3 Linkabit if tampering is suspected. The MPM-1000 should only be physically installed if no evidence of tampering exists.

After completing the tamper label inspection and physical installation of the MPM-1000, the initialization procedure provided below should be performed (see Crypto Officer and User Guidance).

10. Mitigation of Other Attacks

The MPM-1000 is not designed to provide protection against attacks beyond those required by FIPS 140-2.

11. Crypto-Officer/User Guidance

Secure control of the MPM-1000 is afforded to operators authenticated in the role of Crypto–Officer or User. Authentication is achieved by virtue of the entity authentication phase of the SSHv2 connection protocol, which is based on the verification of ID key pairs stored in the MPM-1000 (SSHv2 server) and the designated control computer (SSHv2 client).

The MPM-1000 generates its SSHv2 ID key automatically upon initial power up and upon subsequent power ups after the unit has been zeroized. The MPM-1000 Operator's Manual should be consulted for instructions on obtaining and installing an SSHv2 ID key in the designated controller. The Operator's Manual also provides instructions for transferring the public component of the client key in the MPM-1000.

The first time a secure connection to the MPM-1000 is attempted, the operator will be prompted to accept the MPM-1000's server ID key. This prompt will not occur during subsequent connections, as long as the server key does not change. The operator should accept the key at the prompt only if the prompt is expected. ***If the prompt is not expected, it may be indicative of a malicious attempt to violate the security of the system.***

11.1 MPM-1000 Initialization at the User Facility

After completing the tamper label inspection and physical installation of the MPM-1000, the designated controller should be connected to the MPM-1000 CDU Ethernet port. Using the procedure provided in the MPM-1000 Operator's Manual, the operator should transfer the public component of the SSHv2 client ID key to the MPM-1000.

After installing the client public key in the MPM-1000, the operator should establish a secure connection between the designated controller and the MPM-1000. This can be accomplished by entering a Network-Centric mode seed key or Seed.

In response to the attempt to enter the TRANSEC parameter, the designated controller will display a key "fingerprint" to the operator. This fingerprint is a hash of the MPM-1000's server ID public key. The operator will be prompted to accept or reject the key. The operator should accept the key to complete the initialization process.

The MPM-1000 Operator's Manual should be consulted if the TRANSEC parameter is not accepted by the MPM-1000, or any other step in this initialization procedure does not produce the expected result.

11.2 Changing the Client ID Key

Whenever the client ID key in the designated controller changes, the public key stored in the MPM-1000 must be updated. If the control computer still owns the original client private key, the public key can be changed by writing a new authorized_keys file via SFTP. This method can be used if the original controller needs to update its ID key or transfer control to another computer. It is important to note that the original private key can no longer be used to establish an SSHv2 connection after the public key is changed. Changing the client public key via SFTP can only be done by an operator authenticated into the role of Crypto-Officer or User.

12. References

AES National Institute of Standards and Technology, *Advanced Encryption Standard (AES)*, Federal Information Processing Standards Publication 197, November 26, 2001.

Diffie-Hellman RFC 2631 – Diffie-Hellman Key Agreement Method E. Rescorla June 1999.

DRNG National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2 with Change Notice 1, October 05, 2001, Appendix 3.1.

DSA National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-2 with Change Notice 1, October 05, 2001.

HMAC National Institute of Standards and Technology, *The Keyed-Hash Message Authentication Code (HMAC)*, Federal Information Processing Standards Publication 198, March 06, 2002.

SHA-1 National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standards Publication 180-2 with Change Notice 1, February 25, 2004.