Microwave Networks Incorporated
Proteus MX Licensed Band Radio Cryptographic Module

FIPS 140-2 Non-Proprietary Security Policy

Version: 06 Rev B

Date: January 6, 2017

Microwave Networks, Inc.
4000 Greenbriar Dr #100A
Stafford, TX 77477
281.263.6500
www.microwavenetworks.com

Revision	Date	By	Description
Version 4	March 2, 2016	Hammock	Create Version 4 Document
Version 4 Rev A	May 31,2016	Hammock	Updates to Physical Security – add photos
Version 4 Rev B	June 10, 2016	Liveris	Comments and updates to reflect the latest module capabilities
Version 4 Rev B	June 10, 2016	Hammock	Update Table 1 with correct Module part numbers
Version 4 Rev B	June 24,2016	Hammock	Incorporate CP suggestions
Version 5 Rev A	July 6, 2016	Hammock	Update list of certified modules.
Version 5 Rev B	July 11, 2016	Hammock	Correction MXD FW version in Table 1
Version 5 Rev C	July 18, 2016	Hammock	Terminology changes for consistency with other documents.
Version 5 Rev D	July 19, 2016	Hammock	Add notes from AL
Version 5 Rev E	July 19, 2016	Liveris	• Updated firmware kit part numbers • AES ECB mode usage details • Updated the services information • Added statements about module functionality.
Version 5 Rev F	July 22, 2016	Liveris	• Added reset module to crypto officer services and firmware download to unauthenticated services. • Added explanation to SPU shelf statement that SPU shelf is the only I/O device.
Version 5 Rev G			Accepted previous changes. Deleted reference to Logical Boundary (Para 1.3); add text regarding transient states (Para 1.4). Add NOTE (Para 1.4, Item 5)
Version 5 Rev H	Sept 9, 2016	Hammock	Add detail to Table 13 – Authenticated Services. Update Revisions in Table 1.
Version 5 Rev J	Sept 9, 2016	Hammock	Update Table 16 – add inspection of opaque coating.
Version 6, Rev A	Oct 20,2016	Liveris	Update Table 12 – corrected probability of random attempts Section 4, add text regarding display of error message Accept all changes for final
Version 6, Rev B	Jan 6, 2017		Add note to Table 6 Removed Firmware Authentication Key from Table 15

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Proteus MX Licensed Band Radio Cryptographic Module, hereafter denoted as “the Module” or the “Channel Unit”. The Module provides mux/demux and mod/demod functions along with an optional payload encryption feature for a line of license band point-to-point radios. The Module meets FIPS 140-2 overall Level 2 requirements.

The Module is a multi-chip embedded embodiment; the cryptographic boundary includes all of the MX channel unit, terminating at the front and rear panel connectors. The Module’s enclosure, also known as “Channel Unit Chassis” (not to be confused with the SPU Chassis, see §1.1), is included in the boundary, providing Level 2 physical security protection.

Several versions of the Module are covered under this FIPS 140-2 validation. The Modules differ in which non-security relevant options are installed (i.e., which of 3 available DC power supplies is installed), and which application code is installed. There are two variants of application code:

- MX application (FW Version 8746006-02 Rev A02)
  - The MX application is optimized to provide circuit redundancy when two MX Channel Units (modules) are installed in the same MX SPU Chassis (one is active, and the other is in standby mode). There is only a single set of external MX SPU connectors, which are only connected to the online unit and disconnected from the offline unit.
  - In the MX application, the external MOSCAD/SCE interface is on the front panel of the MX SPU Chassis connecting to the MX Channel Unit through the backplane connector.
- MXD application (FW Version 8746007-02 Rev A02)
  - In the MXD application, two independent MXD Channel Units share a single MXD SPU Chassis, but each of the MXD units has its own set of external MXD SPU Chassis connectors.
  - In the MXD application, the external MOSCAD/SCE interface is the serial connector on the front panel of the MXD Channel Unit.

The above differences are handled by the MUX FPGA code and the application code. The MX and MXD Channel Unit hardware and the rest of the MX and MXD firmware components are identical.

Table 1 – List of Cryptographic Modules

	Module	HW P/N and Version*	FW Version*
1	CHNL UNIT,MX,FIPS,NO µBUS,NO FUSE	8209361-10 Rev A03	8746006-02 Rev A02
2	CHNL UNIT,MX,FIPS, NO µBUS,UNIV PS	8209361-12 Rev A03	8746006-02 Rev A02
3	CHNL UNIT,MX,FIPS, NO µBUS,W/ FUSE	8209361-14 Rev A03	8746006-02 Rev A02
4	CHNL UNIT,MXD,FIPS,NO µBUS,NO FUSE	8209363-10 Rev A03	8746007-02 Rev A02
5	CHNL UNIT,MXD,FIPS, NO µBUS,UNIV PS	8209363-12 Rev A03	8746007-02 Rev A02
6	CHNL UNIT,MXD,FIPS, NO µBUS,W/ FUSE	8209363-14 Rev A03	8746007-02 Rev A02

* In addition to the stated P/Ns and versions, Version/Revision levels will be preceded with the characters “E” for Engineering, “P” for Prototype or “R” for Released representing MNI’s internal process for releasing items for general availability. This prefix does not correspond to any change in the Module.

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 Level 2 validation.

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	3
Cryptographic 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

The Module implementation is based on proprietary hardware/firmware specifications generated by Microwave Networks Inc., and is compliant with requirements of NIST and the Cryptographic Module Validation Program (CMVP). For more information on Microwave Networks Proteus MX, please visit http://www.microwavenetworks.com/products/proteus-mx.html. For more information on NIST and CMVP, please visit http://csrc.nist.gov/groups/STM/cmvp/ .

1.1 Proteus MX Overview

The Proteus MX is a mission critical Point-to-Point radio designed for speeds up to 363 Mbps. It is designed with 100% redundancy of all traffic and overhead channels and with automatic switchover, although it can be configured for non-protected use also. This makes it the perfect choice for Public Safety, Government, Utility, and Critical Infrastructure networks.

The core component of the Proteus MX radio is a Signal Processing Unit (SPU). The SPU is comprised of one or two Channel Units (the Module) and a proprietary SPU Chassis in 2RU format. The SPU Chassis hosts all user input/output connections and the majority of management connections to the Module. It provides two slots with mating connectors into which the Module(s) are plugged. The Module can be installed singly in an SPU, or two Modules can be installed to provide circuit redundancy (MX SPU Chassis) or repeater functionality (MXD SPU Chassis). When two Modules are installed in an SPU, each Module operates independently of the other. Figure 1 illustrates an installation scenario of the Proteus MX SPU where one of the Modules is fully installed in the top slot while the other Module partially installed in the bottom slot.

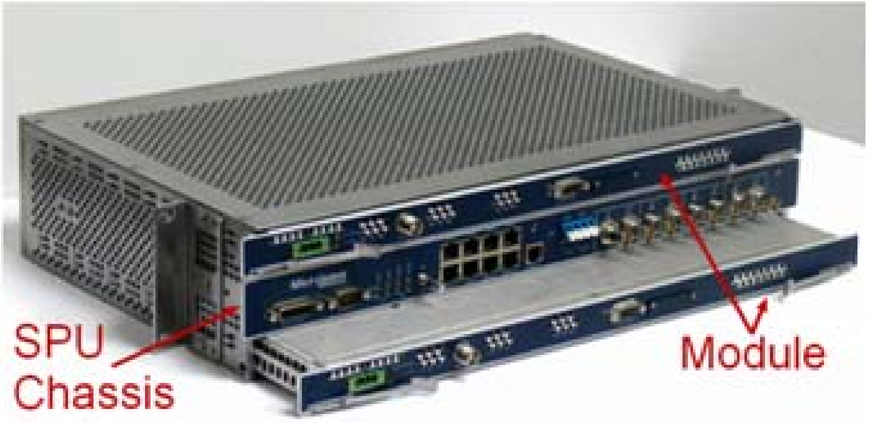


Figure 1 – Proteus MX SPU

The Module provides multiplexing and de-multiplexing function for user signals input to the SPU Chassis. It also provides the digital modulation/demodulation function and generates Intermediate Frequency (IF) signals sent and received from an external RF transceiver.

1.2 Hardware and Physical Cryptographic Boundary

The physical cryptographic boundary of the Module is the entire physical Module as depicted in Figure 2. In Figure 3 the top cover has been removed to show the two installed PCB assemblies: an internal DC-DC power supply and the mainboard. The mainboard includes a connector for a plug-in card for optional user interface signals; however, no plug-in cards are available for the FIPS validated module and this connector is not used. The DC-DC power supply is included within the Cryptographic Boundary but is not integral to the Critical Security Parameters (CSPs) and may be replaced or substituted without effect on the cryptographic process. The complete module includes a top cover and tamper evident seals providing Level 2 security.

Although the Module hosts all signal processing components needed for the complete set of radio functions, it is not able to act as a standalone entity since it relies on the SPU Chassis as an input/output device. For that reason, the Module is deemed as a multi-chip embedded embodiment.

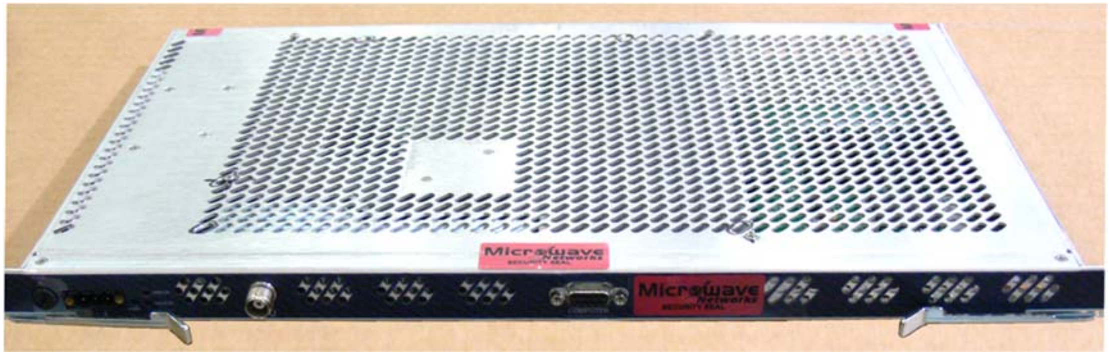


Figure 2 – The Cryptographic Module – Complete with Top Cover and Security Labels Installed

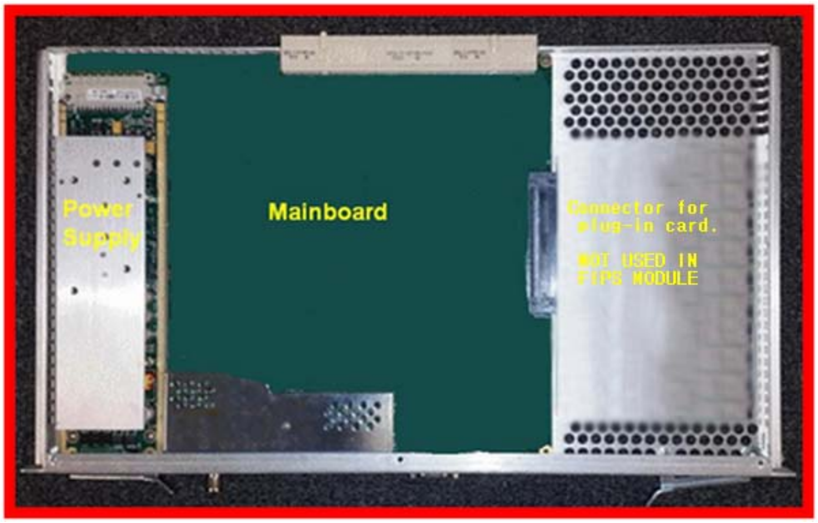


Figure 3 – The Cryptographic Module – Top Cover Removed

The Module is a plug-in shelf with limited I/O connections on its front panel. The rear panel connector plugs into a mating connector in the SPU Chassis. Table 3 lists all physical ports and interfaces of the Module.

Table 3 – Ports and Interfaces

Port or Interface (See Figure 4)	Description	Logical Interface Type
1	DC Power Input Connector	Power
2	LED Status indicators: Power Status; Major Alarm; Minor Alarm	Status out
3	IF connector, carrying aggregated signals over-the-air, control to the connected RF unit, and status from the connected RF unit. The aggregated signals include data transport, control through SNMPv3 or from the remote module, and status through SNMP or to the remote module.	Control in | Data in | Data out |Status out
4	Serial RS-232 port for management Command Line Interface (CLI) and Graphical User Interface (GUI), manual key distribution through serially connected computer, and key output.	Control in | Data in | Data out | Status out

Port or Interface (See Figure 4)	Description	Logical Interface Type
5	System Identification and Memory (SIM) card slot accepting MMC/SD card to store radio configuration data and event/status log. Physically protected by tamper evidence mechanism in FIPS mode	Maintenance Interface
6	SPU Chassis connector, 350-pin Hard Metric socket, MNI proprietary pin definition include connections of all traffic and overhead signals, all management interface (except TLI & SIM card) signals, and internally used power and signal necessary to perform functions of the radio	Power | Control in | Data in | Data out | Status out

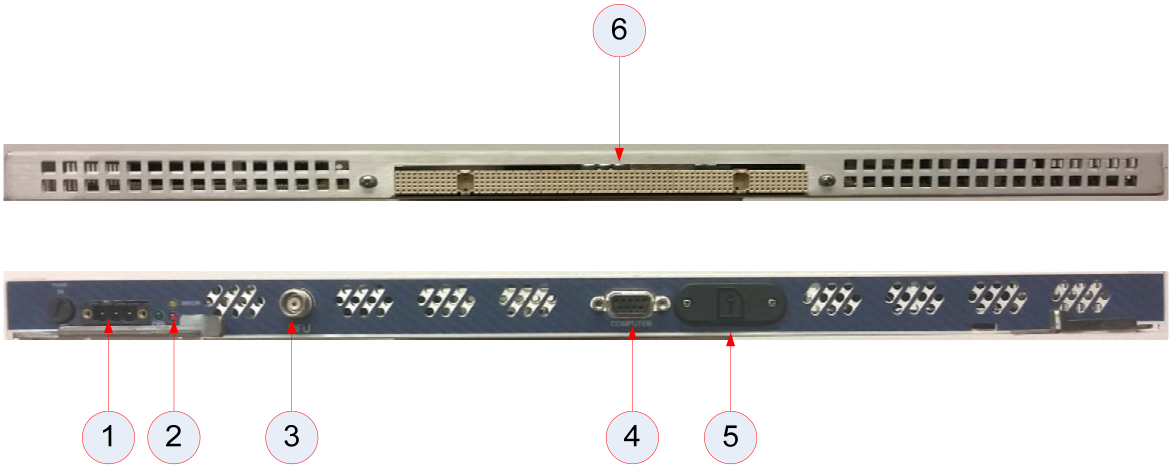


Figure 4 – MX Module Physical Ports and Interfaces (Back View on Top, Front View on Bottom)

1.3 Firmware and Logical Cryptographic Boundary

The Module is a hardware module with firmware running on the motherboard within the physical boundary. The firmware kit includes all firmware components needed for the Module hardware to function according to specification. Almost all components of the Module's firmware are persistently stored in a non volatile memory device (NOR Flash) within the physical boundary; only one component is stored in the SIM card. When the firmware has been executed by the Microprocessor and FPGA, the firmware will be stored in these devices' local RAM.

Figure 5 highlights the components and services within the Module which include cryptographic services. These include the Microprocessor, NOR Flash, RAM, AES FPGA, Serial CLI port, and the SIM card. The optional payload encryption and decryption service of the Module is provided by the AES FPGA, while the Microprocessor, with its peripheral memory and management ports, handles transactions involving cryptographic keys, such as manual key distribution, network management and control with SNMPv3, verification of signed code downloads, and other FIPS 140-2 relevant processing.

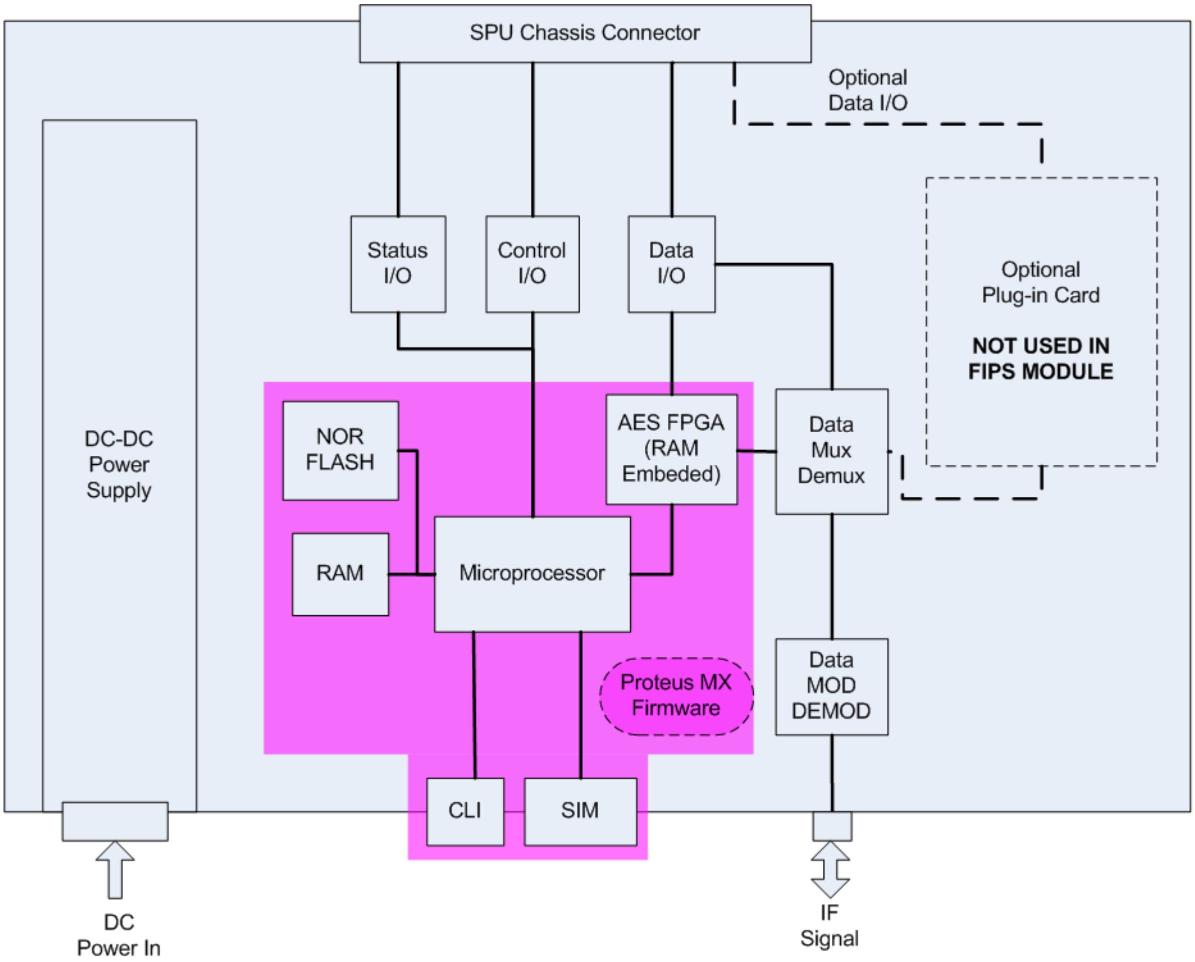


Figure 5 – Module CSP Components/Services

1.4 Mode of Operation

The Module has one approved mode, which is referred to as “FIPS-140 mode” or "FIPS mode" in the Module and product documentation, and one non-approved mode of operation referred to as non-FIPS mode. Although the Modules will be shipped from the factory with physical protection measures applied as described in Section 5, it is not set to the approved mode of operation until the following steps have been performed to have the Module commissioned to “FIPS-140 mode”. Upon enabling or disabling FIPS-140 mode, all CSPs will be zeroized and the Module will reboot. All traffic ingress and egress to and from the Module is stopped while enabling or disabling FIPS-140 mode; no transient states exist where traffic can be output during this process. After the reboot the CO will login using the default password, then will immediately be instructed to install a new authorization CO password.

Overview of enabling FIPS approved mode:

1. Inspect the Module for physical integrity of its packaging and tamper evident seals. Since the module operates while installed in the SPU Chassis (and in most cases is shipped installed in the SPU Chassis), the Module needs to be taken out of the SPU Chassis to be inspected.
2. For first-time use: Normally, the Module will be shipped with the SIM card installed and tamper evident seals applied to the SIM cover. If the SIM card is shipped separately, install the SIM card and tamper evident seal per the SIM Installation Maintenance Procedure. Refer to FIPS 140-2 Maintenance Procedures (FIPS 0012).

3. Install the Module in the SPU Chassis and power up.
4. Turn on "FIPS-140 mode" according to instructions in the Proteus MX FIPS 140-2 User Guide (or see Appendix A of this document).
5. Enabling (or disabling) FIPS-140 mode automatically zeroizes all CSPs in flash and RAM memory and reboots the Module.
   NOTE: The encryption key, if one had previously been installed, will be zeroized in RAM and flash memory, but will persist in the encryption FPGA; however, in this state no data input to or output from the encryption FPGA is allowed. A new encryption key must be installed by the CO, which overwrites the old key in the FPGA, before encryption can be enabled, once again allowing data to and from the encryption FPGA.
6. Wait for the Module reboot and finish all self-test and integrity checks successfully.
7. Log in with the default Crypto Officer (Admin) credentials.
8. The Module will immediately prompt the Crypto Officer to enter a new Admin (CO) authorization password.
9. Because all CSPs were zeroized upon enabling FIPS mode, the CO should next configure the User (guest) authentication password, SNMPv3 privacy passwords, and payload AES key if encryption will be enabled. If not changed by the CO, the default User password "guest" will remain, and the Admin authentication password will be used as the SNMPv3 privacy password. The only default password that can be used for authentication is the default User password and the only default keys that can be used for authentication/privacy are the corresponding User SNMPv3 keys.
10. Perform any other payload relevant configurations.
11. Enable payload encryption if applicable.

To verify that a module is in the approved mode of operation, log into the Module via the CLI or GUI, and check the status of the "FIPS mode" parameter in the Security menu (this is part of the "Show Status" service; refer to MX FIPS 140-2 User Guide for instructions).

For more details, please see the Proteus MX FIPS 140-2 User Guide (FIPS 0008). Excerpts from the FIPS 140-2 User Guide related to installing passwords are included in Appendix A.

Table 4 – Approved/Non-Approved Modes of Operation

Functions Available	Non-Approved Mode	FIPS-140 Mode	Notes
FW Download	No downloads allowed	Yes	Only signed FW downloads allowed
Automatic FPGA AES Key distribution	Yes	No	
Manual FPGA AES key distribution	No	Yes	
Radio management over non-secure network protocols (telnet, SNMPv1/2, etc.)	Yes	No	
Secure SNMPv3 access (SHA-1 and AES)	Yes	Yes	
Support of other protocols with non-approved algorithms, such as PPP, RADIUS, SSH	Yes	No	

2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 5 – Approved and CAVP Validated Cryptographic Functions

Algorithm	Description	Cert #
AES	[FIPS 197, SP 800-38A] Functions: Payload Encryption and Decryption Modes: OFB Key sizes: 128, 192, 256 bits	4080, 4081*
AES	[FIPS 197, SP 800-38A] Functions: SNMPv3 Message Encryption and Decryption Modes: ECB (encrypt only; for AES-CFB128 IV generation), CFB128 Key sizes: 128 bits	4082
DSA	[FIPS 186-4] Functions: Firmware Download Signature Verification Key sizes: 2048 bits (with SHA-256)	1107
HMAC	[FIPS 198-1] Functions: SNMPv3 Message Authentication SHA sizes: SHA-1	2664
KDF, Existing Application-Specific	[SP 800-135] Functions: SNMPv3 KDF	900 (CVL)
SHA	[FIPS 180-4] Functions: Firmware Download Digital Signature Verification (SHA-256), SNMPv3 Message Authentication and Key Derivation (SHA-1) SHA sizes: SHA-1, SHA-256	3360

* The Proteus MX variants (Table 1, #1-3) use AES Cert. #4080 while the Proteus MXD variants (#4-6) use AES Cert. #4081.

Table 6 – Protocols Allowed in FIPS Mode

Protocol	Description
SNMPv3	[IG A.8], [IG D.8], and [SP 800-135] With *SP 800-135* SNMP KDF, HMAC-SHA-1-96 authentication, and AES encryption/decryption (RFC 3826) Note: This protocol has not been reviewed or tested by the CAVP and CMVP.

Table 7 – Non-Approved Algorithms Allowed in FIPS Mode

Algorithm	Description
HMAC-SHA-1-96	[IG A.8] Based on the approved HMAC-SHA-1 algorithm (Cert. #2664); only used for SNMPv3

Table 8 – Non-Approved Cryptographic Functions for Use in Non-FIPS Mode Only

Non-Approved Algorithm	Corresponding Protocol(s)
DES	SNMPv3
Diffie-Hellman	SSH*
DSA (not tested, non-compliant): Key Pair Generation and Signature Generation	SSH
HMAC (not tested, non-compliant): HMAC-SHA-1	SSH
HMAC-MD5	SSH
MD5	RADIUS, SNMPv3, SSH, PPP
RC4	SSH
RNG	SSH
SHA-1 for signature generation (not tested, non-compliant)	SSH
Triple-DES CBC (not tested, non-compliant)	SSH

*Secure Shell (SSH) allows secure CLI access to the Module from remote locations only when the Module is in non-FIPS mode. Through SSH the CLI allows all normal radio related configuration actions such as setting the transmitter frequency or adjusting the transmitter power. The Admin user is allowed to change log-in passwords in non-FIPS mode, however all non-FIPS passwords will be replaced by the default log-in passwords when the Module is switched to FIPS mode. The CLI is restricted from downloading firmware when connected via SSH.

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 9 – Critical Security Parameters (CSPs)

CSP	Description / Usage
Crypto-Officer (Admin) Authentication Password	8- to 32-character long string (combination of any of 10 numbers, 52 letters, and 32 special characters) used to authenticate the Crypto-Officer role. (This is used for CLI and SNMPv3 authentication.)
User (Guest) Authentication Password	8- to 32-character long string (combination of any of 10 numbers, 52 letters, and 32 special characters) used to authenticate the User role. (This is used for CLI and SNMPv3 authentication.)
Payload Encryption Key	128-, 192-, or 256-bit long AES secret key used to encrypt and decrypt the payload.
SNMPv3 Privacy Password(s)	8- to 32-character long string (combination of any of 10 numbers, 52 letters, and 32 special characters) used to generate AES encryption key for SNMPv3 messages. Separate privacy passwords are used for the Admin (CO) and User

CSP	Description / Usage
	roles. If no privacy password is entered the Module will use the associated role authentication password as a privacy password.
SNMPv3 Authentication Key(s)	128-bit long HMAC-SHA-1 key(s) generated from the corresponding role authentication password used to authenticate SNMPv3 messages.
SNMPv3 Privacy Key(s)	128-bit long AES key(s) generated from the SNMPv3 privacy password used to encrypt and decrypt SNMPv3 messages.

2.2 Public Keys

Table 10 – Public Keys

Key	Description / Usage
Firmware Authentication Key	2048-bit long public component of a DSA key pair, used for signature verification of externally downloaded firmware.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The Module supports three operator roles, User, Cryptographic Officer (CO), and Maintenance:

- User role: Using the username "guest" and a password, the User role can gain "read-only" access to the status and the configuration parameters of the Module. The User role cannot view the values of any CSPs and is not allowed to change any module configuration or security settings. The User role can access the radio through the serial interface or through the network using the SNMPv3 protocol.
- CO role: Using the username "admin" and a password, the CO role can gain "read/write" access to all configuration and security parameters of the Module. The CO role handles the Module initialization and administration. The CO role can access the radio through the serial interface or through the network using the SNMPv3 protocol.
- Maintenance roles: A maintenance role exists solely for the purpose of adding, removing or replacing cards in the Module. Maintenance is performed only in a powered down mode. CO support is required to perform Maintenance services.

Table 11 lists all operator roles supported by the Module. The Module enforces separation of roles after successful authentication with a login user name and password for each specific role. The only way to change roles is by logging out and then logging in under the different role.

The Module supports a maintenance role and a bypass capability.

The Module supports concurrent operators. Only one operator session is supported through the serial CLI interface but SNMPv3 messages corresponding to different operators may be processed in parallel to the serial CLI session. Each serial session request or SNMPv3 message request is associated with the operator making the request and in this way separation between concurrent operators is achieved.

When power cycling or rebooting the Module, any active authenticated Admin or Guest session is terminated. Upon restart, the Module is reinitialized and a new authenticated session must be initiated. Configuration changes that have not been activated (saved in flash memory) are discarded.

When entering the authentication password at the login prompt or when the CO changes any of the role passwords, the characters are not displayed; a "*" character is displayed instead for every typed password character. The passwords are never output from the Module. The authentication passwords are used to generate the SNMPv3 authentication keys according to the SNMP standard documents (IETF RFC 3414 and NIST SP 800-135).

Table 11 – Role Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – "admin" username with read/write access to all module configuration and security settings Password based authentication through the serial CLI or serial GUI password prompt or the SNMPv3 authentication password	Role-based	Admin password
User	User – "guest" username with read-only access to all module status and settings Password based authentication through the serial CLI or serial GUI password prompt or the SNMPv3 authentication password	Role-based	Guest password
Maintenance	Maintenance consists of inserting, removing or replacing non-crypto relevant plug-in cards while the Module is powered down. The Crypto Officer must perform the Zeroize service and then power down the Module. The Module must remain powered down during maintenance and then the Crypto Officer must power up the Module and perform the Zeroize service to complete the maintenance.	N/A: The Module must remain powered down during maintenance. (The maintenance role & interface are protected by tamper seals.)	

3.2 Authentication Methods

The module supports password based authentication. Each password can be a string of 8 to 32 characters and can include any combination of the following characters:

- numbers (10 different ones: 0-9)
- letters (52 different ones: A-Z and a-z)
- special characters (32 different ones: ~`!@#$%^&*()_-+=|\{[}]:;"'<,>.?/).

Thus, the number of all possible passwords is (10+52+32)^{8}=94^{8}=6.1x10^{15}, i.e., the probability of a random password attempt being successful is one in 6.1x10^{15}, which is much lower than the one in 1,000,000 probability that the FIPS-140-2 standard requires.

The Module will allow only 3 incorrect entries per interface over a one minute period. Once three incorrect entries have been received that interface is blocked from additional login attempts until one minute after the first failed attempt.

The login interfaces in the Approved mode of operation are Serial and SNMPv3, which means that a total of six unsuccessful attempts are allowed per minute. Given that the number of all passwords is $6.1x10^{15}$, the probability of success for one of the six random attempts within a minute is equivalent to six in $6.1x10^{15}$, i.e., about one in 10^{15}, which is much less than the one in 100,000 probability that the FIPS-140-2 standard requires.

Additionally, after blocking has occurred, the system will set minor alarms as alerts (on the LED Status Indicator and the CLI) for bad password attempts.

Table 12 – Authentication Description

Authentication Method	Probability	Justification
Password-based	For one random attempt: $1/(10+52+32)^8=1.6x10^{-16}$	Minimum password length 8 characters, 10+52+32 possibilities per character
	For multiple attempts in one-minute period: $6/(10+52+32)^8=9.8x10^{-16}$	Minimum password length 8 characters, 10+52+32 possibilities per character, limited to 3 serial and 3 SNMPv3 attempts in the same minute.

3.3 Services

All services implemented by the Module are listed in the tables below.

Table 13 – Authenticated Services

Service	Description	CO	U
Role Authentication	Crypto Officer and User authenticated by the Module either through the serial interface or through SNMPv3.	X	X
Module Reset (Power-up self-test)	Reset the Module by using the reboot command in the CLI menu or through SNMPv3. Active Admin and Guests login sessions are discontinued.	X	
Enable/Disable Payload Encryption	The only bypass mode available in the Module is when FIPS mode is active but encryption is disabled. This service is used to enable or disable encryption.	X	
Payload Encryption Key Entry	Entered through a general purpose computer through a serial connection (CLI/GUI).	X	
Payload Encryption Key Output	Only possible through a serial CLI connection. The CO must issue the command to output the key, then separately confirm the command.	X	
Change Authentication Passwords	The CO may change the Admin or Guest privacy password.	X	
Change SNMPv3 Privacy Passwords	The CO may change the SNMPv3 privacy passwords. If no privacy password is set, the operation will use the authentication password as the privacy password.	X	

Service	Description	CO	U
Firmware Download	The CO may initiate a firmware download only when in FIPS mode. Downloaded firmware must include approved signature.	X	
Module Configuration	CO may change module configurations, including updating CSPs, using CLI or through SNMPv3.	X	
SNMPv3	SNMPv3 is used to monitor and configure the Module. Only the CO role can configure the Module through SNMPv3.	X	X
Show Status	Browsing through all the current values of configuration parameters (apart from CSPs) and viewing logs and statistics. Current encryption status (enabled or disabled) is shown.	X	X

Table 14 – Unauthenticated Services

Service	Description
Module Reset (Power-up self-test)	Reset the Module by disconnecting the power connector and then reconnecting it or by using an unauthenticated reboot command through the inter-module communication channel.
Zeroize	Sets all CSPs to default values, except for the public key used for verifying the signature in externally downloaded code.
Over-the-air and same chassis inter-module configuration	Modules operating in the same SPU Chassis or at the end of the same microwave link can read the other twin or far end module's status and change radio function related configuration parameters such as TX Power, Modulation, etc. No CSPs or secret/private keys are involved in this communication and no changes to security settings can be made.
Firmware Download	Through over-the-air or same-chassis inter-module communication a firmware download can be initiated. The module will still authenticate the signature in the downloaded firmware.
Show LED Status	LEDs on Module's front panel show current status.
Payload Encryption/Decryption	Encrypts data sent to the microwave link and decrypts data received from the microwave link.
SCE (MOSCAD)	The Status and Control Extender (SCE) allows reading some status parameters and performs limited configuration changes from the PPP/SCE interface.
SNMP traps	SNMPv1 traps with status information are transmitted from the Module over the network.
Networking services	The Module acts as a layer-2 network switch between all its network ports. The Module also offers auxiliary service channel transport, orderwire voice channel transport or bridging, and control of external relays based on its state.

Table 15 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- R = Read: The module reads the CSP and outputs it from the module.
- E = Execute: The Module executes using the CSP.
- W = Write: The Module writes the CSP. The write access is typically performed after a CSP is imported into the Module, when the Module generates a CSP, or when the Module overwrites an existing CSP.
- Z = Zeroize: The Module zeroizes the CSP.
- ZW = Zeroize to default value: Overwrites the CSP to a default value.

Table 15 – CSP Access Rights within Services

Service	CSPs					
	Crypto Officer Password	User Password	Payload Encryption Key	SNMPv3 Privacy Passwords	SNMPv3 Authentication Key(s)	SNMPv3 Privacy Key(s)
Role Authentication	E*	E*				
Module Reset (Self-test)						
Enable/Disable Payload Encryption			E			
Payload Encryption Key Entry			W			
Payload Encryption Key Output			R			
Change Authentication Passwords	W	W			W	W if no privacy password is set
Change SNMPv3 Privacy Passwords				W		W
Firmware Download						
Module Configuration						
SNMPv3	W	W		W	E/W	E/W
Show Status						
Zeroize	ZW	ZW	Z	Z	ZW	ZW
Over-the-air and same chassis inter-module configuration						
Show LED Status						
Payload Encryption/Decryption			E			
SCE (MOSCAD)						
SNMP traps						
Networking services						

* The User or Crypto Officer password is also entered during these operations, but only for comparison rather than "loading" a new value into the CSP slot.

4 Self-tests

Each time the Module is powered up it tests the cryptographic algorithms to assure they still operate correctly and that sensitive data have not been damaged. Power up self–tests are available on demand by power cycling the Module.

On power up or reset, the Module performs the self tests described in Table 16 below. All KATs must be completed successfully prior to any other use of the Module. If any of the KATs fail, the Module enters the error state and an error message is displayed in the serial CLI to alert the user. The module then reboots.

Table 16 – Power Up Self-tests

Test Target	Description
Firmware Integrity	16 bit CRC performed over firmware in flash.
AES (Cert. #4080 or #4081*)	KATs: Encryption, Decryption Modes: OFB Key sizes: 128 bits, 192 bits, 256 bits
AES (Cert. #4082)	KATs: Encryption, Decryption Modes: ECB (Encryption only), CFB128 (Encryption and Decryption) Key sizes: 128 bits
DSA (Cert. #1107)	KAT: Signature Verification with SHA-256 Key sizes: 2048 bits
HMAC (Cert. #2664)	KAT: Generation SHA sizes: SHA-1
SHA (Cert. #3360)	KATs: SHA-1, SHA-256
KDF, Existing Application-Specific (CVL Cert. #900)	KAT: SP 800-135 SNMP KDF

* The Proteus MX variants (Table 1, #1-3) use AES Cert. #4080 while the Proteus MXD variants (#4-6) use AES Cert. #4081.

Table 17 – Conditional Self-tests

Test Target	Description
Firmware Load	DSA 2048 Signature Verification performed when firmware is loaded.
Bypass Test	Bypass Test performed when the service Enable Payload Encryption is called, when the key length is changed, or when a new key is activated.

5 Physical Security Policy

All components of the Module are housed within an aluminum chassis with a separable top cover. Physical access to the Module components requires removing the top cover. The top cover is held in place with several screws. Three tamper evident seals placed around the perimeter of the top cover provide a visual indication if the top cover has been removed from the unit.

Additionally, the Module has a SIM card that stores device specific configuration information. The SIM card stores no CSPs; however, it is within the Module boundary. The SIM card can be removed from the front panel of the Module following the appropriate maintenance procedure. For physical security, the SIM card has a protective cover screwed to the chassis of Module. One additional tamper evident seal is applied over the cover to provide Level 2 physical protection for the SIM card.

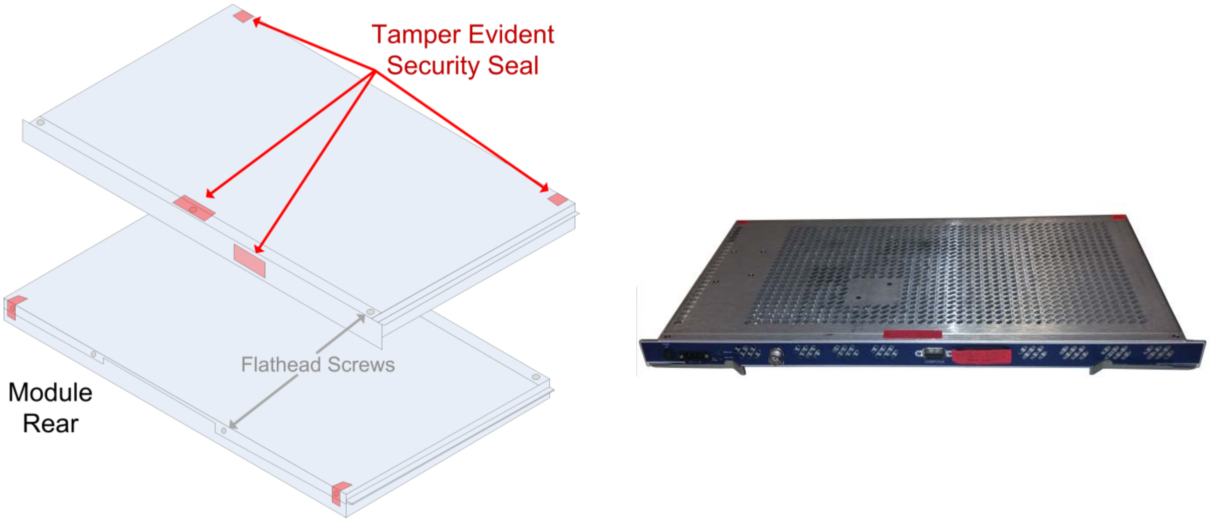


Figure 6 – Tamper Evident Label Placement

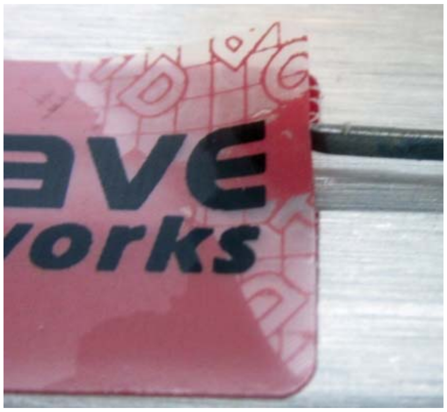


Figure 7 – Example of a Label Showing Evidence of Tamper

Table 18 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seals on channel unit cover	Inspect at least once each 12 months during normal preventive maintenance	Inspect for evidence of removal or tampering
Tamper Evident Seals on SIM slot protective cover	Inspect at least once each 12 months during normal preventive maintenance	Inspect for evidence of removal or tampering

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Opaque coating on Motherboard	Inspect at least once each 12 months during normal preventive maintenance	Using a flashlight, look through the vent holes in the top cover and inspect the coating on the motherboard for evidence of tampering such as gouges in the coating or newly exposed components or traces.

The Module meets the requirement of opacity for Level 2 Physical Security with a conformal coating on the motherboard. The coating hides all identifying marks and signal traces on the board from external viewing. As this motherboard is installed inside the Channel Unit Chassis, it is not possible to identify by sight the type or function of any components on the motherboard. Individual devices which are not coated are covered either by heat sinks or, in the case of connectors, with a plug. The conformal coating also protects the board from being probed from the outside.

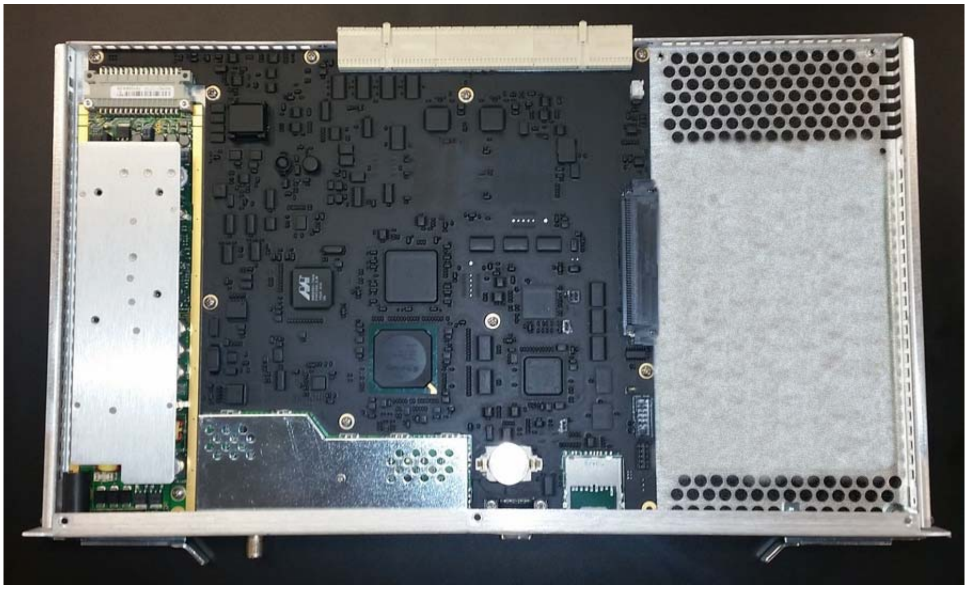


Figure 8 – Conformal Coated Motherboard

The following table describes components within physical boundary that are excluded from the opacity requirement along with the justifications for exclusion.

Table 19 – Components Excluded from Opacity Requirement

Reference	Description	Justification
1	SD card cage	Some pins are visible, but only connect to ground.
2	Power supply board and power supply connector	Power supply does not contain sensitive information and is generally not relevant to security.

Reference	Description	Justification
3	Battery	Internal 3V battery does not contain sensitive information and is only used to run the Real Time Clock (RTC). The module does not implement any functionality which can be compromised by a disrupted RTC. (e.g. Public Key Infrastructure)
4	CPLD jumper	This jumper connects to the onboard Altera CPLD, however the CPLD is configured so that the jumper has no effect on behavior.
5	Fan jumper	The module does not actually have a fan, so this jumper has no effect on module behavior.

5.1 Maintenance

Maintenance may consist of replacing the Power Supply inside the Module, or removing or replacing the front panel accessible SIM card. The Crypto Officer must zeroize all CSP and then power down the Module prior to performing maintenance. The module must remain powered down during the maintenance. Upon completion of maintenance the CO must power up the Module and log in with the default password. The CO will immediately be prompted to change the default password. The CO will also change the guest password, and if encryption is being used re-enter the encryption key and enable encryption.

Maintenance that requires removing the Module top cover, or removing the front panel SIM, will disturb the tamper evident seals. The tamper evident seals must be replaced to return the Module to FIPS compliance. When replacing a tamper evident seal any residue from the previous seal must be completely removed before a new seal is applied.

Refer to Proteus MX FIPS 140-2 User Guide (FIPS 0008) for additional details.

6 Operational Environment

The Module is designated as a *limited operational environment* under the FIPS 140-2 definitions. The Operational Environment requirements are not applicable.

The Module’s operational environment has been adapted from a version of embedded operating system such that there is no general purpose operating system functionality available to an operator.

The Module includes a firmware load service to support necessary updates. This firmware upgrade service requires the validation of a digital signature. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

The Module does not mitigate any other attacks.

8 Security Rules and Guidance

The Module design corresponds to the Module 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 module shall provide two distinct operator roles: User and Cryptographic Officer.
2. The module shall provide role-based authentication.
3. The module shall clear previous authentications on power cycle.
4. When the Module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
5. The operator shall be capable of commanding the Module to perform the power up self-tests by cycling power or resetting the Module.
6. Power up self-tests do not require any operator action.
7. Data output shall be inhibited during self-tests and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which secret keys or CSPs are zeroized by the zeroization service.
10. The firmware authentication public key can only be overwritten by new firmware.
11. The module supports a single operator via the serial port and concurrent operators via SNMPv3. It is also possible for the serial port and SNMPv3 to be used concurrently.
12. The module supports a maintenance role which requires CO role support.
13. The module does not support manual key entry.
14. The module cannot be used as a standalone device. It must be installed in a SPU shelf which provides many of the physical input/output ports for both data and control signals. The two SPU shelf variations, one for the MX application and one for the MXD application, are the only I/O devices used with the Module.
15. The module can be commanded by the CO to output the secret payload encryption key in plaintext, but no other CSPs can be output. Outputting the encryption key requires two steps – issuing the command and confirming the command.
16. All CSPs are entered in plaintext to the Module.
17. The module uses production-grade components.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 20 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[SP800-131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, January 2011

Table 21 – Acronyms and Definitions

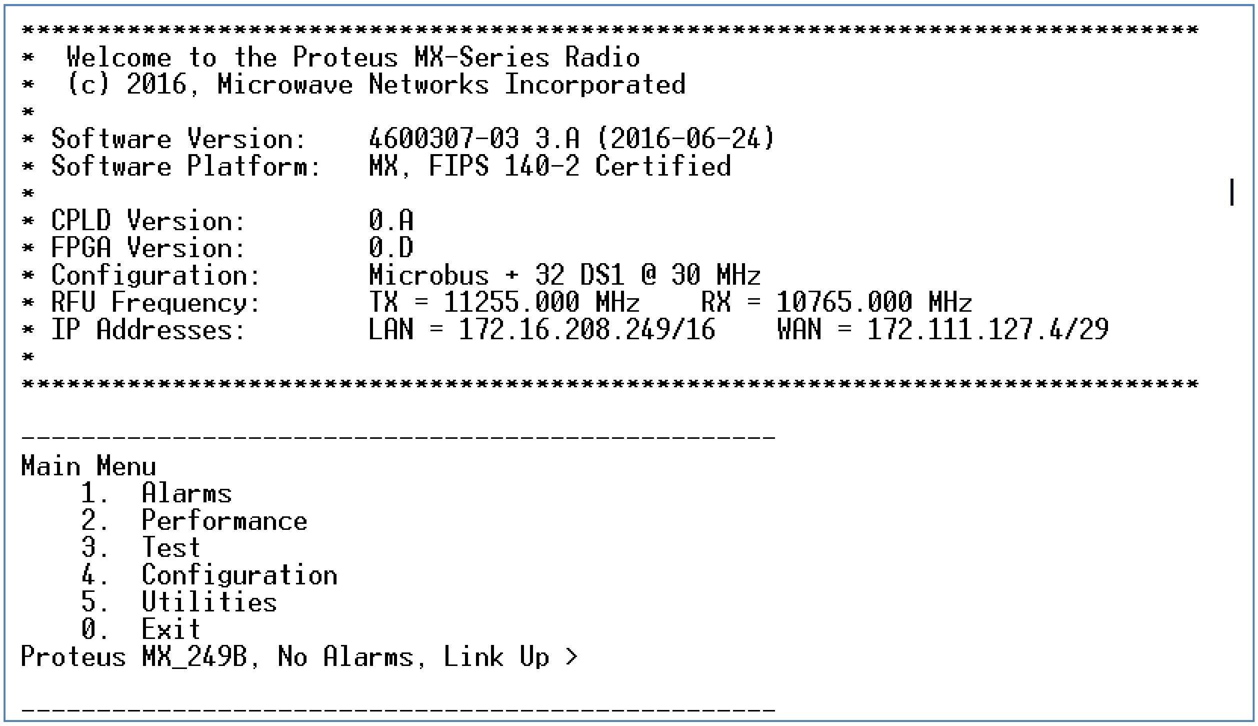
Acronym	Definition
CU	Channel Unit – Acronym is specific to this product

Acronym	Definition
SPU	Signal Processing Unit – Acronym is specific to this product
TLI	Transport Line Interface – Acronym is specific to this product
SIM	System Identification and Memory– Acronym is specific to this product
CO	Crypto Officer

Appendix A

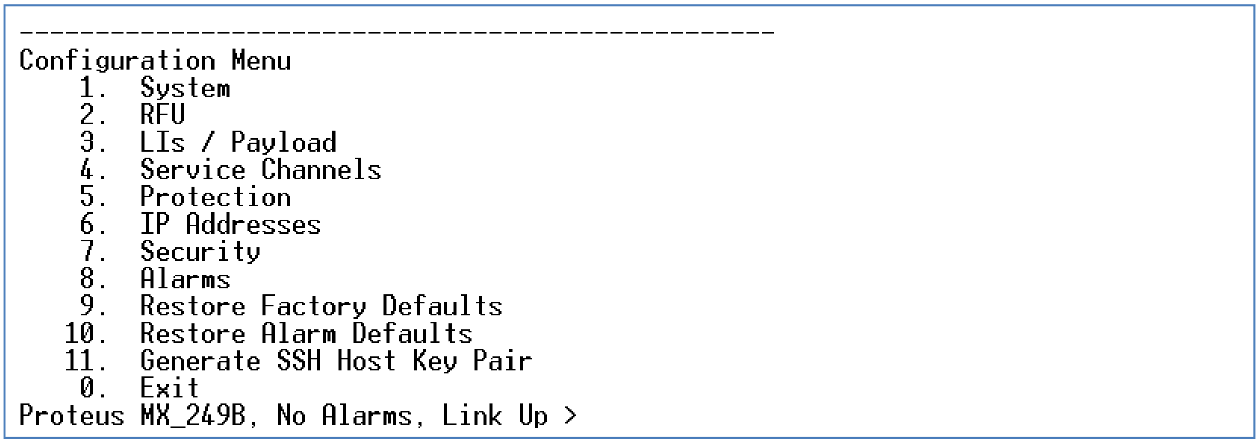
Excerpts from the Proteus MX FIPS 140-2 User Guide (FIPS 0008), Section 6.1 showing the steps check if FIPS mode is enabled, and steps required to enable/disable FIPS mode in the Proteus MX.

… log in as Admin using the password assigned during the previous session.



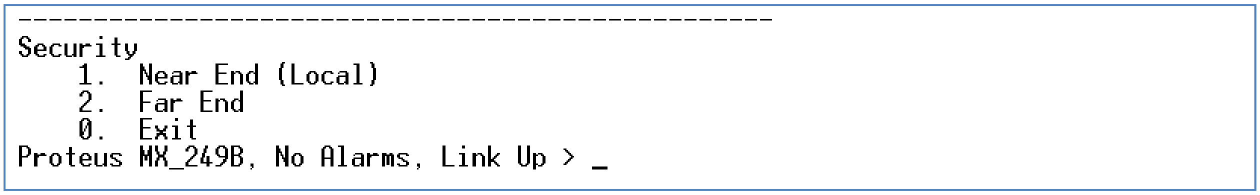
```
******************************************************************************
*  Welcome to the Proteus MX-Series Radio
*  (c) 2016, Microwave Networks Incorporated
*
* Software Version:    4600307-03 3.A (2016-06-24)
* Software Platform:   MX, FIPS 140-2 Certified
*
* CPLD Version:        0.A
* FPGA Version:        0.D
* Configuration:       Microbus + 32 DS1 @ 30 MHz
* RFU Frequency:       TX = 11255.000 MHz    RX = 10765.000 MHz
* IP Addresses:        LAN = 172.16.208.249/16    WAN = 172.111.127.4/29
*
******************************************************************************

--------------------------------------------------
Main Menu
    1.  Alarms
    2.  Performance
    3.  Test
    4.  Configuration
    5.  Utilities
    0.  Exit
Proteus MX_249B, No Alarms, Link Up >

--------------------------------------------------
```

From the Main Menu select option *4. Configuration*. The Configuration menu will open.



```
--------------------------------------------------
Configuration Menu
    1.  System
    2.  RFU
    3.  LIs / Payload
    4.  Service Channels
    5.  Protection
    6.  IP Addresses
    7.  Security
    8.  Alarms
    9.  Restore Factory Defaults
   10.  Restore Alarm Defaults
   11.  Generate SSH Host Key Pair
    0.  Exit
Proteus MX_249B, No Alarms, Link Up >
```

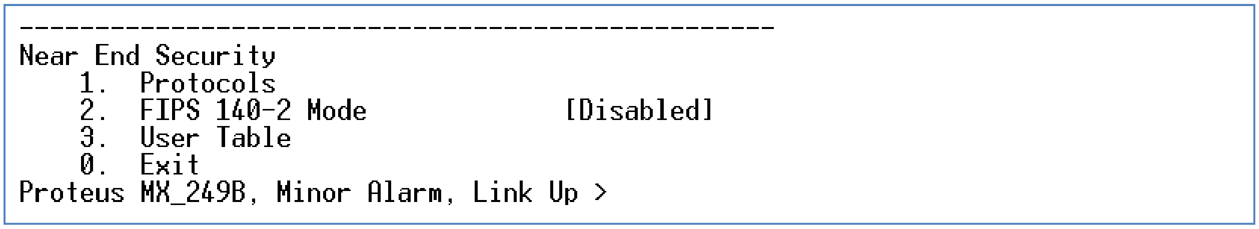
From the Configuration menu select Option *7. Security*



```
--------------------------------------------------
Security
    1.  Near End (Local)
    2.  Far End
    0.  Exit
Proteus MX_249B, No Alarms, Link Up > _
```

From the Security menu select Option *1. Near End (Local)*.

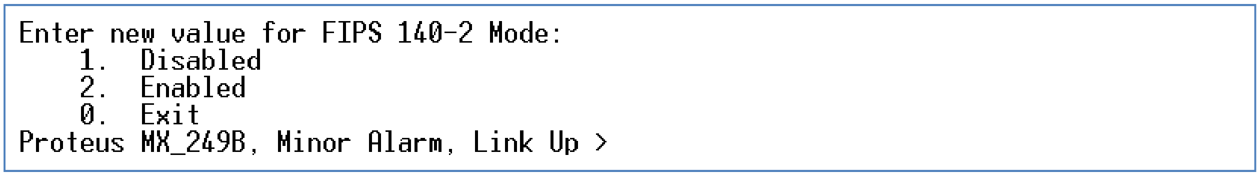
> **NOTE**: The CTI screens add the (Local) label to indicate which unit you are plugged into. Select the unit indicated as (Local). In a Protected Signal Processing Unit both Primary and Secondary units will be shown on the menu. In a protected SPU, the upper Channel Unit is considered the primary Channel Unit and the lower one is the secondary Channel Unit.



```
--------------------------------------------------
Near End Security
    1.  Protocols
    2.  FIPS 140-2 Mode             [Disabled]
    3.  User Table
    0.  Exit
Proteus MX_249B, Minor Alarm, Link Up >
```

If FIPS 140-2 Mode is indicated as Enabled, Exit back to Security menu.

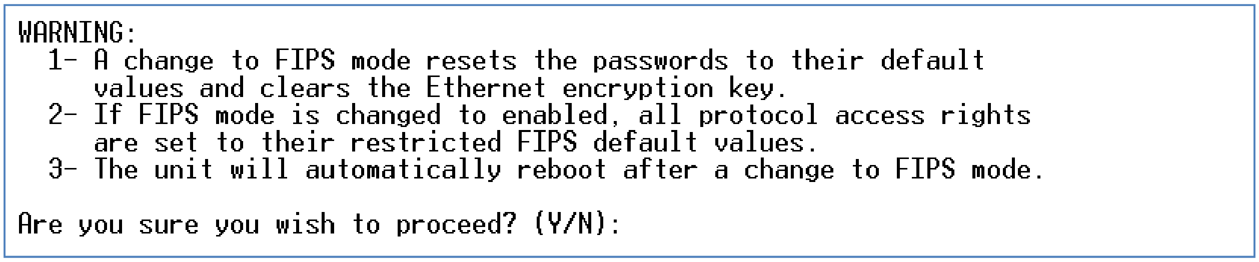
If FIPS 140-2 Mode is indicated as Disabled, select option *2. FIPS 140-2 Mode*



```
Enter new value for FIPS 140-2 Mode:
    1.  Disabled
    2.  Enabled
    0.  Exit
Proteus MX_249B, Minor Alarm, Link Up >
```

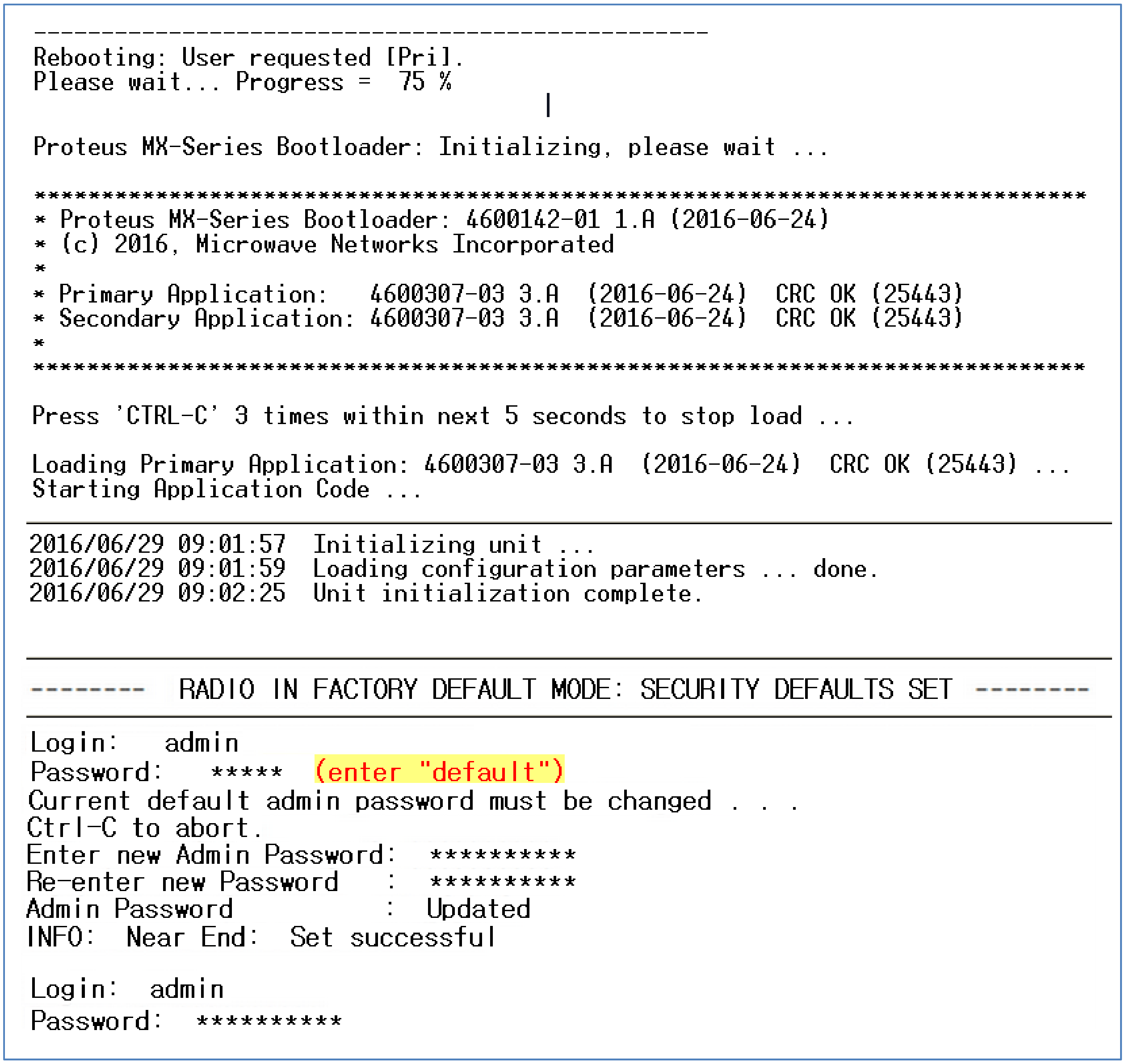
Select option *2. Enable.* A warning message will appear. Enabling or disabling FIPS mode will reboot the Channel Unit. During the reboot traffic will be blocked. Also, when Enabling FIPS mode, the Channel Unit will perform all required FIPS start-up tests which may take several minutes.

> **NOTE**: Enabling or disabling FIPS 140-2 Mode will always reboot the Channel Unit; all Security Parameters, including login passwords and encryption keys, will be zeroized



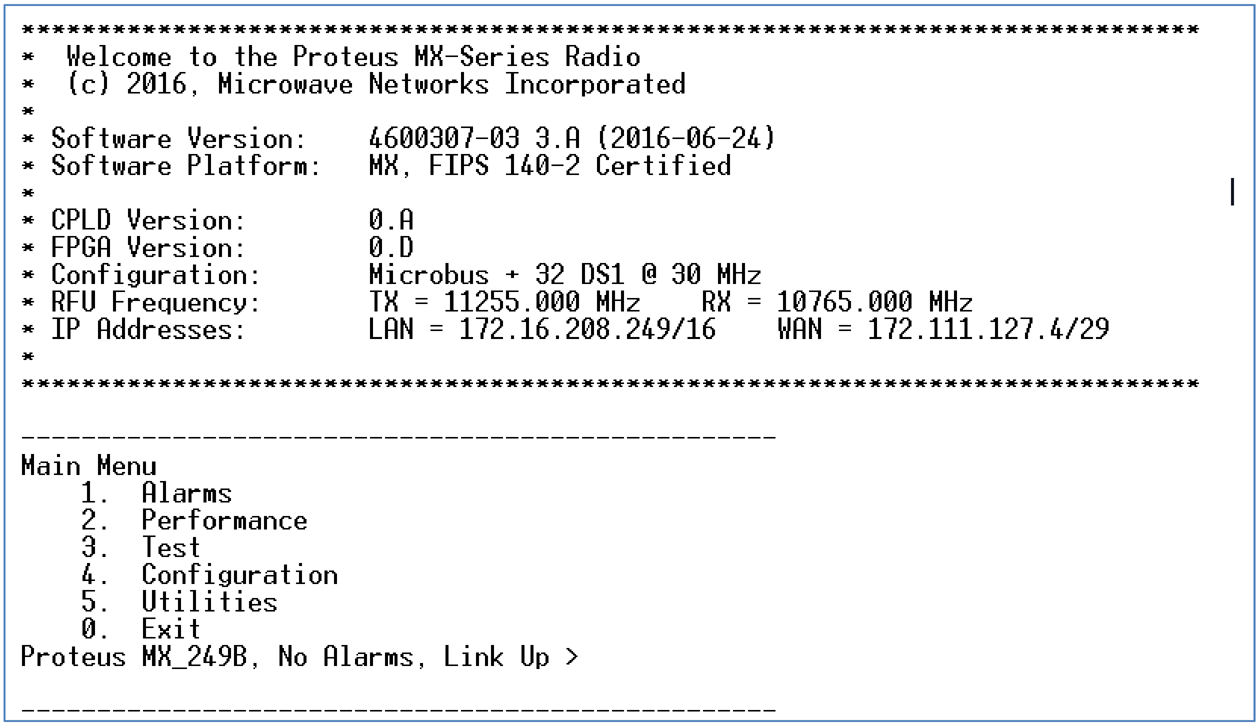
```
WARNING:
  1- A change to FIPS mode resets the passwords to their default
     values and clears the Ethernet encryption key.
  2- If FIPS mode is changed to enabled, all protocol access rights
     are set to their restricted FIPS default values.
  3- The unit will automatically reboot after a change to FIPS mode.

Are you sure you wish to proceed? (Y/N):
```

The Module will reboot and run through its FIPS self test routine. After rebooting you will have to reconnect and log back into the Channel Unit. Because you have enabled FIPS mode, the previous non-FIPS passwords are no longer valid. Upon initial login as Admin with FIPS mode enabled, you will use the factory ship default password “default”. You will immediately be prompted to install a new admin password.



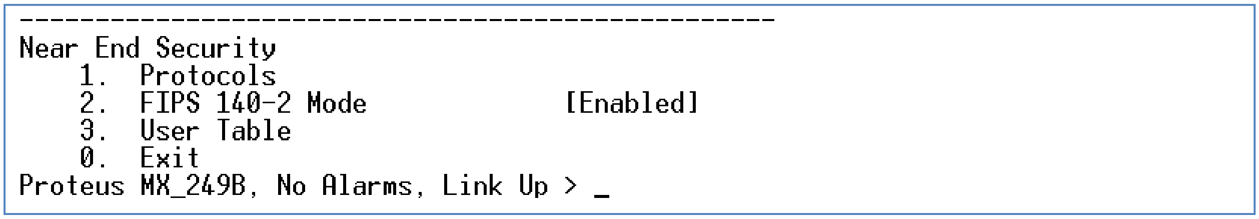
```
--------------------------------------------------
Rebooting: User requested [Pri].
Please wait... Progress =  75 %
                                      |

Proteus MX-Series Bootloader: Initializing, please wait ...

******************************************************************************
* Proteus MX-Series Bootloader: 4600142-01 1.A (2016-06-24)
* (c) 2016, Microwave Networks Incorporated
*
* Primary Application:   4600307-03 3.A  (2016-06-24)  CRC OK (25443)
* Secondary Application: 4600307-03 3.A  (2016-06-24)  CRC OK (25443)
*
******************************************************************************

Press 'CTRL-C' 3 times within next 5 seconds to stop load ...

Loading Primary Application: 4600307-03 3.A  (2016-06-24)  CRC OK (25443) ...
Starting Application Code ...

2016/06/29 09:01:57  Initializing unit ...
2016/06/29 09:01:59  Loading configuration parameters ... done.
2016/06/29 09:02:25  Unit initialization complete.


--------  RADIO IN FACTORY DEFAULT MODE: SECURITY DEFAULTS SET  --------

Login:   admin
Password:   *****  (enter "default")
Current default admin password must be changed . . .
Ctrl-C to abort.
Enter new Admin Password:  **********
Re-enter new Password   :  **********
Admin Password          :  Updated
INFO:  Near End:  Set successful

Login:  admin
Password:  **********
```

After inputting new Admin passwords you will return to the Welcome menu:



```
******************************************************************************
*  Welcome to the Proteus MX-Series Radio
*  (c) 2016, Microwave Networks Incorporated
*
* Software Version:    4600307-03 3.A (2016-06-24)
* Software Platform:   MX, FIPS 140-2 Certified
*
* CPLD Version:        0.A
* FPGA Version:        0.D
* Configuration:       Microbus + 32 DS1 @ 30 MHz
* RFU Frequency:       TX = 11255.000 MHz    RX = 10765.000 MHz
* IP Addresses:        LAN = 172.16.208.249/16    WAN = 172.111.127.4/29
*
******************************************************************************

--------------------------------------------------
Main Menu
    1.  Alarms
    2.  Performance
    3.  Test
    4.  Configuration
    5.  Utilities
    0.  Exit
Proteus MX_249B, No Alarms, Link Up >

--------------------------------------------------
```

If you now look at the *Configuration/Security/Near End Security* menu you will see FIPS is enabled.



```
--------------------------------------------------
Near End Security
    1.  Protocols
    2.  FIPS 140-2 Mode             [Enabled]
    3.  User Table
    0.  Exit
Proteus MX_249B, No Alarms, Link Up > _
```