Proxim Wireless Corporation

Tsunami MP.11 HS 245054_R, Tsunami MP.11 HS 245054_RC, and Tsunami MP.11 HS 245054_S

(Hardware Version: 2.0.0; Firmware Version: 1.0.0)

FIPS 140-2 Non-Proprietary Security Policy

Level 2 Validation

Document Version 1.1

Prepared for:

Proxim Wireless Corporation
1561 Buckeye Drive
Milpitas, CA 95035
Phone: (408) 383-7600
Fax: (408) 383-7680
http://www.proxim.com

Prepared by:

Corsec Security, Inc.
10340 Democracy Lane, Suite 201
Fairfax, VA 22030
Phone: (703) 267-6050
Fax: (703) 267-6810
http://www.corsec.com

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2008-05-21	Xiaoyu Ruan	Initial draft
0.2	2008-06-20	Xiaoyu Ruan	Addressed Lab comments
0.3	2008-06-23	Xiaoyu Ruan	Addressed Lab comments
0.4	2008-07-08	Xiaoyu Ruan	Addressed Lab comments
0.5	2008-07-08	Xiaoyu Ruan	More models
0.6	2008-07-09	Xiaoyu Ruan	Company new address
0.7	2008-07-22	Xiaoyu Ruan	Addressed Lab comments
0.8	2008-09-15	Darryl Johnson	Modified model names; addressed lab comments
0.9	2008-09-17	Darryl Johnson	Addressed lab comments
1.0	2008-09-19	Darryl Johnson	Corrected bit size for CRC
1.1	2009-01-29	Darryl Johnson	Addressed CMVP comments

Table of Contents

Table of Figures

List of Tables

1 Introduction

1.1 Purpose

This document is a non-proprietary Cryptographic Module Security Policy for the Tsunami MP.11 HS 245054_R, Tsunami MP.11 HS 245054_RC, and Tsunami MP.11 HS 245054_S (hardware version: 2.0.0; firmware version: 1.0.0) from Proxim Wireless Corporation. This Security Policy describes how the Tsunami MP.11 HS 245054_R, Tsunami MP.11 HS 245054_RC, and Tsunami MP.11 HS 245054_S meet the security requirements of FIPS 140-2 (Federal Information Processing Standards Publication 140-2 – *Security Requirements for Cryptographic Modules*) and how to run the devices in a secure FIPS 140-2 mode. This policy was prepared as part of the overall Level 2 FIPS 140-2 validation of the devices.

FIPS 140-2 details the U.S. and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website at: http://csrc.nist.gov/groups/STM/index.html.

In this document, the Tsunami MP.11 HS 245054 series is collectively referred to as “the module” or “the device”.

1.2 Document Organization

The Security Policy document is one document in a FIPS 140-2 submission package. In addition to this document, the submission package contains:

- Vendor evidence
- Finite state machine
- Crypto-Officer and User guidance
- Functional specification
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Corsec Security, Inc. under contract to Proxim. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Proxim and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Proxim.

2 Tsunami MP.11 HS Series

2.1 Overview

Proxim Wireless Corporation (Nasdaq: PRXM) is a leader in core-to-client solutions for broadband municipal wireless networks for private and government use. Proxim's systems enable a variety of wireless applications including security and surveillance systems, mobile workforce automation and machine-to-machine communications. Proxim has shipped more than 1.5 million wireless devices to more than 200,000 customers worldwide.

Proxim's Tsunami MP.11 product family offers fixed and mobile WiMAX (Worldwide Interoperability for Microwave Access) capabilities to distribute wireless broadband access supporting video, voice, and data applications. The Tsunami MP.11 HS 245054_R, Tsunami MP.11 HS 245054_RC, and Tsunami MP.11 HS 245054_S wireless products are additions to Proxim's family of point-to-multipoint broadband wireless access systems.

The Tsunami MP.11 HS 245054_R is an outdoor model, and includes an integrated antenna. The Tsunami MP.11 HS 245054_RC is also an outdoor model, but comes with exterior antenna connectors instead of an integrated antenna. The Tsunami MP.11 HS 245054_S is the indoor model. The outdoor models feature a ruggedized enclosure with active heating and cooling technology for outdoor deployment in extreme weather conditions. These products support a proprietary Wireless Outdoor Router Protocol (WORP) designed to optimize the performance of outdoor wireless point-to-point and point-to-multipoint links using 802.11b radios. All three models run identical firmware.

Each model can be operated in two different configurations: classic "base station unit" (BSU) functionality and "subscriber unit" (SU) functionality. The same firmware and hardware is used for SU and BSU operations. The BSU and SU features are roughly analogous to Wireless Access Point (WAP) and wireless client functionality in a traditional WAP setup. As shown on the right of Figure 1, the device is typically deployed in configurations where one or more SUs communicate wirelessly with a single BSU. Each unit must also communicate over a wired port. An SU and a BSU can be set up back-to-back using the wired port to extend wireless range as shown in Figure 1. Proxim offers a "Quick Bridge" shown in the left of Figure 1. The Quick Bridge offers a pre-configured BSU and SU that are licensed to connect only to each other with pre-set keys. The device acts as an Ethernet-to-wireless converter in both SU and BSU modes. In addition, the device includes an internal learning bridge, switching traffic based on Media Access Control (MAC) addresses and router functionality to manage Internet Protocol (IP) networking.

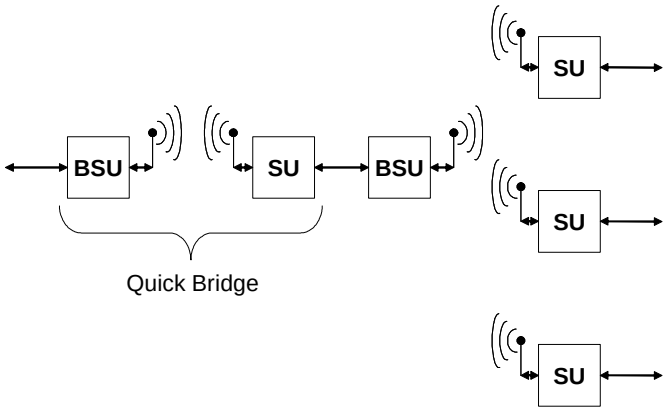

Figure 1 – Deployment of Tsunami MP.11 HS 245054 Series

The module supports an Approved mode of operation and a non-Approved mode of operation. In the Approved mode of operation, the module features Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) web

interface with Transport Layer Security (TLSv1), Secure Shell (SSH) version 2, Simple Network Management Protocol version 3 (SNMPv3), and serial port for configuration and management.

Although SNMPv3 can support AES encryption, it does not utilize a FIPS approved key generation method; therefore, the module firmware has been designed to block the ability to view or alter critical security parameters (CSPs) through this interface. Also note that the SNMP interface is a management interface for the Tsunami devices and that no CSPs or user data are transmitted over this interface. The serial port interface does not utilize encryption. A direct, physical connection between the Tsunami device and a management console or PC is required.

Underlying cryptographic algorithms for TLS and SSH include Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES or Triple DES), Rivest, Shamir, and Adleman (RSA), Digital Signature Algorithm (DSA), Secure Hash Algorithm (SHA), Keyed-Hash Message Authentication Code (HMAC), and Random Number Generator (RNG). In the Approved mode of operation, the module provides wireless data transfer functionality that is protected by AES in Cipher Block Chaining (CBC) mode.

The Cryptographic Algorithm Validation Program (CAVP) has issued certificates to the module for all FIPS-Approved cryptographic algorithms implemented in the Approved mode of operation.

(Implemented in firmware)

- AES – 128-bit and 256-bit encryption and decryption in CBC, ECB[1], and CFB[2] modes (certificate #830).
- Triple DES – 112-bit and 168-bit in CBC and ECB modes (certificate #695).
- RSA PKCS[3]#1 v1.5 – 1024-bit and 2048-bit signature verification (certificate #400).
- DSA – 1024-bit key generation and signature generation/verification (certificate #302).
- SHA-1 (certificate #826).
- HMAC-SHA-1 (certificate #461).
- ANSI[4] X9.31 Appendix A.2.4 RNG (certificate #477).

(Implemented in hardware)

- AES – 256-bit encryption and decryption in CBC mode (certificate #794).

The module implements the following non-Approved cryptographic algorithms in the Approved mode of operation.

(Implemented in firmware)

- A non-Approved RNG for seeding the ANSI X9.31 Appendix A.2.4 RNG.
- RSA PKCS#1 v1.5 key transport used in TLS – 1024-bit providing 80 bits of encryption strength.
- Diffie-Hellman key agreement used in SSH – 1024-bit providing 80 bits of encryption strength.

The cryptographic boundary is defined as the enclosure of the device. The power injector is not in the boundary. The Tsunami MP.11 HS series is validated at the following levels (when operating in the Approved mode of operation). In Table 1, N/A indicates “not applicable”.

Table 1 – Security Level per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2

[1] Electronic Codebook
[2] Cipher Feedback
[3] Public Key Cryptography Standards
[4] American National Standards Institute

Section	Section Title	Level
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference/ Electromagnetic Compatibility	2
9	Self-Tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Interfaces

The module supports the four logical interfaces defined in FIPS 140-2: data input interface, data output interface, control input interface, and status output interface. In addition, the device supports a power input interface.

2.2.1 Tsunami MP.11 HS 245054_R

The Tsunami MP.11 HS 245054_R is the outdoor model with integrated antenna. It features two ports and two Light-Emitting Diodes (LEDs). See Figure 2, Figure 3, Table 2, and Table 3 for photographs and descriptions.

Figure 2 – Tsunami MP.11 HS 245054_R Ports

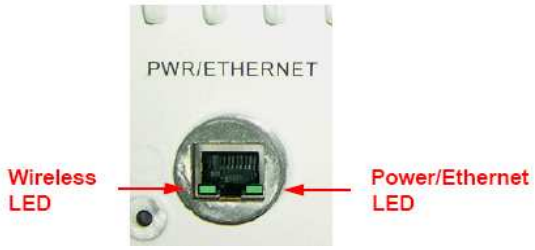

Figure 3 – Tsunami MP.11 HS 245054_R LEDs

Table 2 – Ports on Tsunami MP.11 HS 245054_R

Port	Description	Logical Interfaces
Power/Ethernet port	RJ-45 female	Data input, data output, control input, status output, power input
Serial port	RJ-11 female	Data input, data output, control input, status output
Antenna	Integrated antenna	Data input, data output

Table 3 – LEDs on Tsunami MP.11 HS 245054_R

LED / Status	Wireless	Power/Ethernet
Off	No wireless link established	Power is not present or the device is malfunctioning
Red	Power in on; unit is self-heating	N/A
Flashing green	Wireless link is being established	Power is on; Ethernet link is down
Solid green	Wireless link has been established	Power is on; Ethernet link is up

2.2.2 Tsunami MP.11 HS 245054_RC

The Tsunami MP.11 HS 245054_RC is the outdoor model without integrated antenna. It features four ports and two LEDs. See Figure 4, Figure 5, Table 4, and Table 5 for photographs and descriptions.

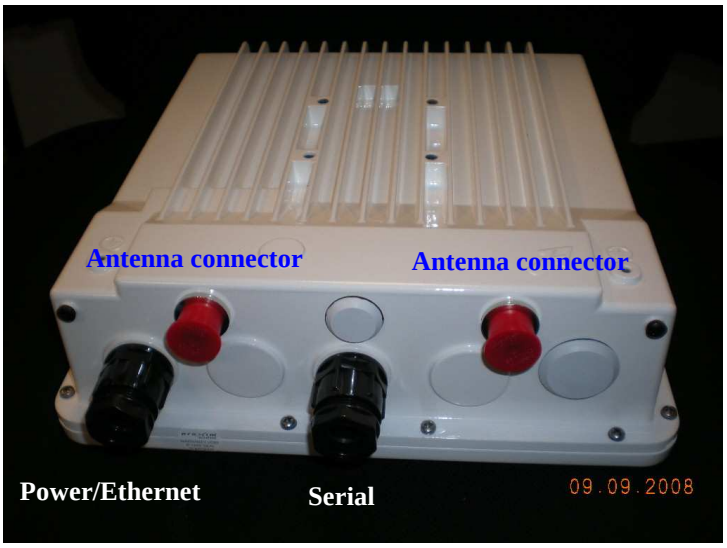

Figure 4 – Tsunami MP.11 HS 245054_RC Ports

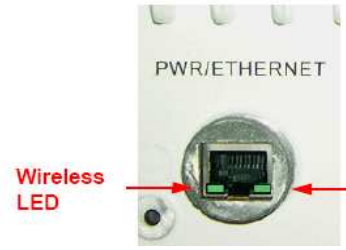

Figure 5 – Tsunami MP.11 HS 245054_RC LEDs

Table 4 – Ports on Tsunami MP.11 HS 245054_RC

Port	Description	Logical Interfaces
Power/Ethernet port	RJ-45 female	Data input, data output, control input, status output, power input
Serial port	RJ-11 female	Data input, data output, control input, status output
Two antenna connectors	Antenna connectors	Data input, data output

Table 5 – LEDs on Tsunami MP.11 HS 245054_RC

LED / Status	Wireless	Power/Ethernet
Off	No wireless link established	Power is not present or the device is malfunctioning
Red	Power in on; unit is self-heating	N/A

Flashing green	Wireless link is being established	Power is on; Ethernet link is down
Solid green	Wireless link has been established	Power is on; Ethernet link is up

2.2.3 Tsunami MP.11 HS 245054_S

Tsunami MP.11 HS 245054_S is the indoor model. It features five ports, two buttons, and four LEDs. See Figure 6, Figure 7, Table 6, and Table 7 for photographs and descriptions.

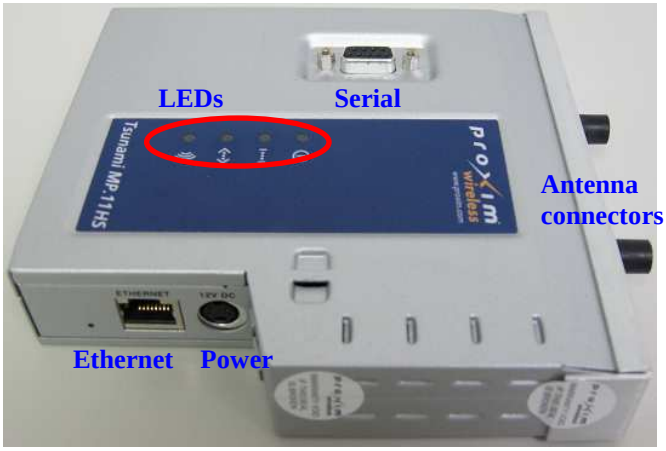

Figure 6 – Tsunami MP.11 HS 245054_S Ports and LEDs

Figure 7 – Tsunami MP.11 HS 245054_S Buttons

Table 6 – List of Ports and Buttons on Tsunami MP.11 HS 245054_S

Port/Button	Description	Logical Interfaces
Power port	12V DC[5] power input	Power input
Ethernet port	RJ-45 female	Data input, data output, control input, status output, power input
Serial port	DE-9 female	Data input, data output, control input, status output
Two antenna connectors	Antenna connectors	Data input, data output
Reset button	Reboot the device	Control input
Reload button	Reset the device to factory defaults	Control input

The four LEDs shown in Figure 6, from left to right, are dynamic frequency indicator, wireless link indicator, Ethernet indicator, and power indicator, respectively.

Table 7 – List of LEDs on Tsunami MP.11 HS 245054_S

LED / Status	Power	Ethernet Link	Wireless Link	Dynamic Frequency
Off	Power is not present or the device is malfunctioning	Not connected	Wireless interface is up but no wireless link established	N/A
Green	Power is present and the device is operational	Connected to 10 Mbps[6]	Immediately after connecting a wireless link	N/A
Blinking green	N/A	Data is being sent at 10 Mbps	Data is being sent or the wireless interface is initializing after reboot	Scanning for channel
Amber	The device is initializing after reboot (less than two minutes) or it cannot get a dynamic IP address (after two minutes)	Connected to 100 Mbps or the device is initializing after reboot (less than two minutes)	N/A	N/A
Blinking amber	N/A	Data is being sent at 100 Mbps	N/A	N/A
Red	A fatal error has occurred	An error in data transfer	A fatal error on the wireless interface has occurred	N/A

2.3 Roles and Services

The module supports two authorized roles: Crypto-Officer and User. A Crypto-Officer is a human being that manages and configures the module. The User is a peer device (SU or BSU) that uses the module's wireless data transfer functionality.

[5] Direct Current
[6] Megabits per second

2.3.1 Crypto-Officer Role

In the Approved mode of operation, a Crypto-Officer can access the module through one of the following four interfaces (protocols):

- HTTPS web interface with TLS
- SSH
- SNMP
- Serial console

The module implements role-based authentication. All four module interfaces require that the Crypto-Officer authenticate using a password. A password has to be at least six and at most 32 characters long. Passwords can be combinations of any lower- and upper-case letters, numbers, and special symbols. There are a total of 94 different characters on keyboard, hence there are $94^6+94^7+\ldots+94^{31}+94^{32} = 1.3955\times10^{63}$ possibilities for a password. FIPS 140-2 requires that, for multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur. Based upon the module's processor speed of 1.66×10^8 Hz, the probability of guessing the password in a one-minute period is much smaller than one in 100,000

Table 8 – Crypto-Officer Services lists services that belong to the Crypto-Officer role. The purpose of each service is shown in the first column ("Service"), and the corresponding function is described in the second column ("Description"). For more information about the (CSPs) listed in the rightmost column, see Table 10 – CSPs.

Table 8 – Crypto-Officer Services

Service	Description	Input	Output	CSPs and Access
Log in HTTPS	Crypto-Officer logs in the module through HTTPS	Username, WebPassword	Status	WebPassword – read TLSRSAkeys – read TLSMS – read, write, delete TLSAESkey – read, write, delete TLSHMACkey – read, write, delete
Log in SSH	Crypto-Officer logs in the module through SSH	Username, SSHpassword	Status	SSHpassword – read, write SSHDSAkeys – read SSHDHkeys – read, write, delete SSHAESkey – read, write, delete SSH3DESkey – read, write, delete
Log in SNMP	Crypto-Officer logs in the module through SNMP	Username, SNMPpassword	Status	None
Log in serial port	Crypto-Officer logs in the module through serial port	Username, SerialPassword	Status	SerialPassword – read, write
Upgrade	Download and upgrade firmware	New firmware image	Status	UpgradeRSAKey – read
Run self-tests	Initiate power-up self-tests	Reboot command	Status	None
View status	Get status output from the module	View log command	Event log	None

Service	Description	Input	Output	CSPs and Access
Configure security settings	Enable/disable "Secure Management Status"; set security parameters, including passwords, CBCkeys, etc.	Parameters (including keys and passwords) to be set	Status	SSHDSAkeys – write, delete WebPassword – write SSHpassword – write SerialPassword – write CBCkey – write
Configure system settings	Set non-security relevant parameters, including IP address, bandwidth, etc.	Parameters to be set	Status	None

2.3.2 User Role

The User is a peer device (SU or BSU) that uses the module's wireless data transmission functions. The User is authenticated to the Tsunami by virtue of possession of a valid CBCkey (See Table 10) and the use of it to encrypt data sent to the Tsunami. Since a CBCkey is 256 bits, there are 2^{256} possibilities. FIPS 140-2 requirements state that, for multiple attempts to use the authentication mechanism during a one-minute period, the probability shall be less than one in *100,000* that a random attempt will succeed or a false acceptance will occur. Based upon the module's processor speed of 1.66×10^8 Hz, the probability of guessing the password in a one-minute period is much smaller than one in 100,000.

Table 9 – User Services shows the services for the User role. Similar to Table 8 – Crypto-Officer Services, the purpose of each service is shown in the first column ("Service"), and the corresponding function is described in the second column ("Description"). For more information about the CBCkey in the rightmost column, see Table 10 – CSPs.

Table 9 – User Services

Service	Description	Input	Output	CSP and Access
Transmit wireless data	Transmit data for the User	Plaintext data to be transferred to the peer module	Encrypted data sent to the peer module	CBCkey – read
Receive wireless data	Receive data from a peer module	Encrypted data received from the peer module	Decrypted data received from the peer module	CBCkey – read

2.4 Physical Security

The Tsunami HP.11 HS 245054 series models are multi-chip standalone cryptographic modules. The entire contents of each module (including all hardware, firmware, and data) are enclosed in an opaque metal or metal/plastic case. The modules feature three different enclosures. The cases are sealed using warranty labels (tamper-evident labels) in order to prevent the covers from being removed without signs of tampering. All integrated circuits (ICs) in the modules are coated with commercial standard passivation.

2.5 Operational Environment

The operational environment requirements do not apply to the module. The module does not provide a general purpose Operating System (OS) and only allows the updating of image components after checking RSA signatures on new firmware images. Crypto-Officers can download and install new firmware images on a device. A firmware upgrade image is signed by Proxim with a RSA private key, which never enters the module. The module verifies the signature on the new firmware image using the associated RSA public key installed during manufacturing. The upgrade is allowed only if the verification passes. Otherwise the upgrade process fails and the old image is reused.

2.6 Cryptographic Key Management

The following table gives a list of all cryptographic keys and other CSPs used by the module in the Approved mode of operation.

Table 10 – CSPs

CSP	Type	Generation / Input	Output	Storage	Zeroization	Use
WebPassword	Password	Input in encrypted form (encrypted by TLSAESkey)	Never	Plaintext in non-volatile memory	When a new WebPassword is set	Web interface authentication
TLSRSAkeys	1024-bit RSA public and private keys	Installed during manufacturing	Public keys are output in plaintext; private keys are not output	Plaintext in non-volatile memory	Upon enforced reload[7]	Transport TLSMS
TLSMS	384-bit TLS master secret	Key transport with TLSRSAkeys	Never	Plaintext in volatile memory	Upon session termination	Derive TLSAESkey and TLSHMACkey
TLSAESkey	128-bit AES keys	Derived from TLSMS	Never	Plaintext in volatile memory	Upon session termination	Encrypt and decrypt TLS traffic
TLSHMACkey	160-bit HMAC keys	Derived from TLSMS	Never	Plaintext in volatile memory	Upon session termination	Authenticate TLS traffic
SSHpassword	Password	Input in encrypted form (encrypted by SSHAESkey or SSH3DESkey)	Never	Plaintext in non-volatile memory	When a new SSHpassword is set	SSH authentication
SSHDSAkeys	1024-bit DSA public and private keys	Generated by internal ANSI RNG when “Secure Management Status” is enabled	Public keys are output in plaintext; private keys are not output	Plaintext in non-volatile memory	Upon enforced reload	Authenticate SSH data sent by the module (SSH server)
SSHDHkeys	1024-bit Diffie-Hellman public key and private key	Generated by internal ANSI RNG	Public keys are output in plaintext; private keys are not output	Plaintext in volatile memory	Upon SSH session termination	Negotiate SSHAESkey or SSH3DESkey
SSHAESkey	128-bit AES key	1024-bit Diffie-Hellman key agreement	Never	Plaintext in volatile memory	Upon session termination or when a new SSHAESkey is generated (after a certain timeout)	Encrypt and decrypt SSH traffic

[7] To invoke an enforced reload, press and hold the module’s Reload button for at least 20 seconds. The Reload button on the outdoor variants is located on the side of the power injector.

CSP	Type	Generation / Input	Output	Storage	Zeroization	Use
SSH3DESkey	168-bit Triple DES key	1024-bit Diffie-Hellman key agreement	Never	Plaintext in volatile memory	Upon session termination or when a new SSH3DESkey is generated (after a certain timeout)	Encrypt and decrypt SSH traffic
SerialPassword	Password	Input in plaintext	Never	Plaintext in non-volatile memory	When a new SerialPassword is set	Serial port authentication
CBCkey	256-bit AES key	Input in plaintext (using serial console) or encrypted form (encrypted by SSHAESkey or SSH3DESkey)	Output in encrypted form over TLS (encrypted by TLSAESkey) or SSH (encrypted by SSHAESkey or SSH3DESkey)	Plaintext in non-volatile memory	Upon enforced reload	Encrypt and decrypt wireless data
UpgradeRSAkey	2048-bit RSA public key	Installed during manufacturing	Never	Plaintext in non-volatile memory	Upon enforced reload	Verify signatures on firmware upgrade
RNGseed	64-bit ANSI RNG seed	Generated by internal non-Approved RNG	Never	Plaintext in volatile memory	When a new RNGseed is fed	Generate random numbers

2.6.1 CSP Generation

The module uses ANSI X9.31 Appendix A.2.4 RNG to generate cryptographic keys. This RNG is FIPS-Approved as indicated by Annex C to FIPS PUB 140-2. The seeds of the ANSI X9.31 Appendix A.2.4 RNG are provided by a non-Approved RNG, which is a deterministic RNG in firmware and does not have an external interface. The DSA keypair generation follows the FIPS 186-2 standard.

2.6.2 CSP Input/Output

In TLS sessions, the module's RSA public key is exported to the Crypto-Officer's web browser in plaintext. The TLS master secret is imported into the module with 1024-bit RSA key wrap. In SSH sessions, the module's DSA public key and Diffie-Hellman public key are exported to the Crypto-Officer's SSH terminal in plaintext. The Crypto-Officer can configure passwords via HTTPS, SSH, and serial console interfaces. Likewise, Crypto-Officers can configure CBCkeys via HTTPS, SSH, and serial console interfaces. In the FIPS-Approved mode of operation, CBCkeys and passwords (except the SNMP password) cannot be set through SNMP. Passwords never leave the module. CBCkeys can be output in encrypted form over TLS (encrypted by TLSAESkey) or SSH (encrypted by SSHAESkey or SSH3DESkey). Firmware upgrade employs a 2048-bit RSA public key for signature verification. Installed during manufacturing, this RSA public key never leaves the module.

2.6.3 CSP Storage and Zeroization

Ephemeral keys, such as SSH and TLS session keys and TLS master secrets, reside only in volatile memory in plaintext. Their memory blocks are freed when their underlying sessions are over. All CSPs stored in the non-volatile memory are zeroized upon enforced reload.

2.7 Self-Tests

The module performs the following self-tests at power-up. Upon failure of a power-up self-test, the module will enter a fatal error state, crash, and reboot automatically.

- Firmware integrity test using 16-bit Cyclic Redundancy Check (CRC)
- Known Answer Test (KAT) on Triple DES encryption and decryption (firmware implementation)
- KAT on AES encryption and decryption (firmware implementation)
- KAT on HMAC-SHA-1 message authentication (firmware implementation)
- KAT on RSA encryption/decryption (firmware implementation)
- KAT on RSA signature generation/verification (firmware implementation)
- KAT on ANSI X9.31 Appendix A.2.4 RNG (firmware implementation)
- KAT on AES-CBC encryption and decryption (hardware implementation)
- Pairwise consistency test on DSA signature generation/verification (firmware implementation)

The module implements the following conditional self-tests:

- Continuous RNG test for the non-Approved RNG that seeds the ANSI X9.31 Appendix A.2.4 RNG
- Continuous RNG test for the ANSI X9.31 Appendix A.2.4 RNG
- Pairwise consistency test for new DSA keypair
- Firmware upgrade test using 2048-bit RSA signature verification

If one of the first three conditional self-tests fails, the module will enter a fatal error state and automatically reboot. Upon failure of a firmware upgrade test, the module will enter an error state where the new firmware will be rejected and will not replace the current firmware.

3 Secure Operation

This section describes how to configure the module such that it operates in the Approved mode of operation.

3.1 Initial Setup

The device should be unpacked and inspected according to the User's Guide. Installation and configuration instructions for the device can also be found in the Installation and Management Guide. The device comes pre-installed with default usernames and passwords for management interfaces. The passwords can be used by the operator to setup the device. After the initial setup, passwords should be changed to ensure privacy and security; it is the responsibility of the Crypto-Officer to ensure that these new passwords are kept secret.

3.2 Approved Mode of Operation

By default, the Secure Management Status is disabled. The following sections provide the steps required to enable Secure Management Status via the SNMPv3 and web interfaces.

3.2.1 Enabling Approved Mode of Operation via SNMPv3

To enable the Approved mode of operation using SNMPv3, perform the following steps (note that these steps should be applicable across various SNMP management tools).

- To enable Secure Management Status from a non-secure interface (SNMPv1/v2), go to oriSNMPSecureManagementStatus.0 and set its value to enable(1).
- Go to oriSystemReboot.0 and set its value to 1, then press the <ENTER> key to reboot the system. After three to four minutes, the device will come up with the Secure Management Status enabled, and the device will now not be accessible from SNMP v1 or SNMP v2c.

3.2.2 Enabling Approved Mode of Operation on Web Interface

To enable the Approved mode of operation via the web interface, perform the following steps:

- Go to *<IP address>/config/configure-management-services.html* and select "Enable" for "Secure Management Status". See Figure 8.

Figure 8 – Setting "Secure Management Status" on Web Interface

- Go to *<IP address>/config/commands-reboot.html* and click on "Reboot" to reboot the device. See Figure 9.

Figure 9 – Rebooting the Device on Web Interface

- Go to *<IP address>/config/configure-security-macauth.html* and select "AES" for "Encryption Option". See Figure 10. Then, enter four encryption keys, i.e., CBCkeys, as instructed. A CBCkey must be exactly 32 characters long.

  NOTE: Encryption keys should only be disclosed to authorized Crypto-Officers, and it is the responsibility of the Crypto-Officers to protect those keys.

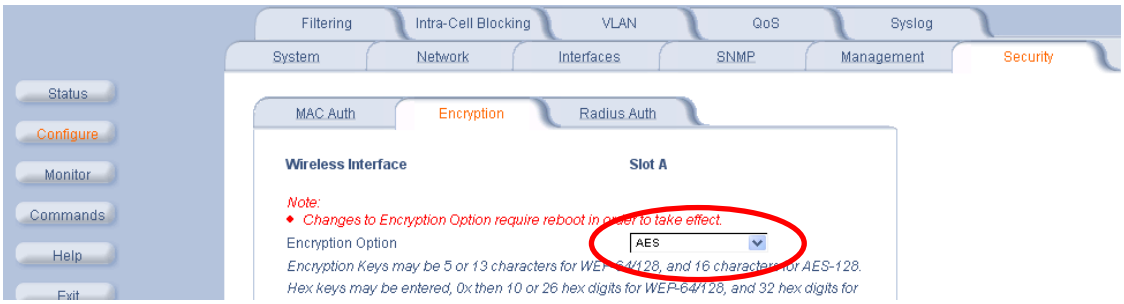

Figure 10 – Setting "Encryption Option" for Wireless Data Transfer on Web Interface

- Go to *<IP address>/config/commands-reboot.html* and click on "Reboot" to reboot the device. See Figure 9.

3.2.3 Enabling Approved Mode of Operation on Command Line Interface

To enable the Approved mode of operation via a command line interface, perform the following steps.

- Run "*set snmpv3enable enable*" command. See Figure 11. Despite the name of the parameter (*snmpv3enable*), it is configuring the secure management status.

```
[Tsunami MP.11 245054-S]> set snmpv3enable enable
set snmpv3enable enable
The following elements require reboot

snmpv3enable

[Tsunami MP.11 245054-S]> show snmpv3enable
show snmpv3enable

This parameter has been changed previously and will not take effect until the next reboot.


enable

[Tsunami MP.11 245054-S]>
```

Figure 11 – Setting "Secure Management Status" on Command Line Interface

- Run "*reboot <n>*" command where *n* is the number of seconds after which the device will be rebooted. In Figure 12, *n* is set to 30 for example. Notice that, after reboot, the device will not accept telnet connections.

```
[Tsunami MP.11 245054-S]> reboot 30
reboot 30
The device will reboot in 30 second(s).
This command line interface session is ending now.

[Tsunami MP.11 245054-S]>
[Tsunami MP.11 245054-S]>
```

Figure 12 – Rebooting the Device on Command Line Interface

- Run "*set wifsec 3 encryptoption aes*" command. See Figure 13.

```
[Tsunami MP.11 245054-S]> set wifsec 3 encryptoption aes
set wifsec 3 encryptoption aes
The following elements require reboot

encryptoption

[Tsunami MP.11 245054-S]> show wifsec
show wifsec

This parameter has been changed previously and will not take effect unil the next reboot.


Index                    :              3
EncryptionOption         :            AES
EncryptionKey1           :         ******
EncryptionKey2           :         ******
EncryptionKey3           :         ******
EncryptionKey4           :         ******
Encryption Key in Use    :              0


[Tsunami MP.11 245054-S]>
```

Figure 13 – Setting "Encryption Option" for Wireless Data Transfer on Command Line Interface

- Run "*cspclipasswdset wirifkey1 # <EncryptionKey1> <EncryptionKey1> 3*", "*cspclipasswdset wirifkey2 # <EncryptionKey2> <EncryptionKey2> 3*", "*cspclipasswdset wirifkey3 # <EncryptionKey3> <EncryptionKey3> 3*", and "*cspclipasswdset wirifkey4 # <EncryptionKey4> <EncryptionKey4> 3*" commands to configure four AES encryption keys (i.e., CBCkeys). Notice that the command requires that an encryption key be entered twice. Also notice that a CBCkey must be exactly 32 characters long. See Figure 14 for example of setting encryption key 1 to "11111111111111111111111111111111".

```
[Tsunami MP.11 245054-S]> cspclipasswdset wirifkey1 # 11111111111111111111111111111111 11111111111111111111111111111111 3
cspclipasswdset wirifkey1 * ******************************** ******************************** *

 Password changed successfully
[Tsunami MP.11 245054-S]>
```

Figure 14 – Setting Encryption Key 1 on Command Line Interface

- Run "*reboot <n>*" command where integer *n* is the number of seconds after which the device will be rebooted. See Figure 12 for example.

3.2.4 Physical Security Considerations

The warranty labels on the device enclosure also serve as tamper-evident labels. See Figure 15, Figure 16, and Figure 17 for sample labels on outdoor and indoor variants. The operator shall examine the enclosure regularly and see if there are signs of tamper attempts. If damage to tamper-evident labels is found, then the device is not

considered operating in the Approved mode of operation. The device must be returned to the factory for service before it can operate in the Approved mode of operation again.

Figure 15 – A Warranty Label on Tsunami MP.11 HS 245054_R

Figure 16 – A Warranty Label on Tsunami MP.11 HS 245054_RC

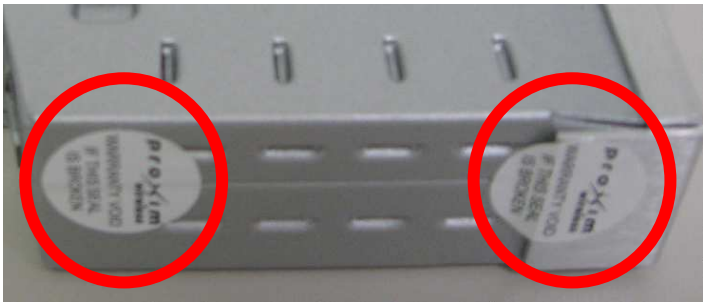

Figure 17 – Two Warranty Labels on Tsunami MP.11 HS 245054_S

3.3 Status

The module maintains a system event log that can be used to identify error states. The system log is accessible on the web interface at *<IP address>/status-eventlog.html* or a command line interface by running "*log dump*" command.

3.4 CSP Zeroization

See Section 2.6.3 for information on CSP zeroization. The firmware image and all CSPs will be zeroized upon enforced reload.

4 Acronyms

Table 11 – Acronyms

Acronym	Definition
3DES	Triple Data Encryption Standard
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BSU	Base Station Unit
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CMVP	Cryptographic Module Validation Program
CRC	Cyclic Redundancy Check
CSP	Critical Security Parameter
DC	Direct Current
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
HMAC	Keyed-Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Secure Sockets Layer
IC	Integrated Circuit
IP	Internet Protocol
KAT	Known Answer Test
LED	Light-Emitting Diode
MAC	Media Access Control
Mbps	Megabit per second
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OS	Operating System
PKCS	Public Key Cryptography Standards
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm

Acronym	Definition
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SU	Subscriber Unit
TLS	Transport Layer Security
WAP	Wireless Access Point
WiMAX	Worldwide Interoperability for Microwave Access
WORP	Wireless Outdoor Router Protocol