

Cambium Networks
PTP 800 Compact Modem
Unit (CMU)
FIPS 140-2 Security Policy
System Release 800-05-02-FIPS



Cambium Networks

CONTENTS

| | |
|--|----|
| 1 Introduction..... | 5 |
| 1.1 Purpose..... | 5 |
| 1.2 Port Identification | 6 |
| 1.3 The PTP 800 Series Part Numbers..... | 6 |
| 1.4 References..... | 6 |
| 1.5 Acronyms | 7 |
| 2 Security Level | 8 |
| 3 Mode of Operation..... | 8 |
| 3.1 Prerequisites for the Approved Mode of Operation..... | 8 |
| 3.2 Configuring the Approved Mode of Operation..... | 9 |
| 3.3 Checking that the unit is in the Approved Mode of Operation..... | 11 |
| 3.4 Approved and non-approved modes of operation | 12 |
| 4 Ports and Interfaces | 13 |
| 5 Identification and Authentication Policy | 14 |
| 5.1 Assumption of Roles | 14 |
| 6 Access Control Policy | 15 |
| 6.1 Authentication Strength | 15 |
| 6.2 Roles and Services..... | 15 |
| 6.3 Unauthenticated Services: | 18 |
| 6.4 Service I/O Specification | 19 |
| 6.5 Definition of Critical Security Parameters..... | 21 |
| 6.6 Definition of Public Keys..... | 22 |
| 7 Operational environment | 24 |
| 8 Security Rules | 24 |
| 8.1 Self-Tests | 24 |
| 8.2 Firmware Self-Tests | 25 |
| 8.3 FIPS Integrity Test Error Indicators..... | 25 |
| 9 Identification of FIPS Mode of Operation | 25 |
| 10 Physical Security Policy..... | 25 |

11 Mitigation of Other Attacks Policy..... 25

TABLES

Table 1 – The Cambium PTP 800 Series CMU..... 6
Table 2 – Module Security Level Specification 8
Table 3 – FIPS Approved and allowed algorithms 12
Table 4 – Management protocols in FIPS mode 13
Table 5 – Ports and Interfaces..... 13
Table 6 – Roles and Authentication 14
Table 7 – Password strength 15
Table 8 – Services and CSP Access 17
Table 9 – Authenticated Services 18
Table 10 – Unauthenticated Services 18
Table 11 – Specification of Service Inputs & Outputs..... 19

FIGURES

Figure 1 – PTP 800 CMU 5
Figure 2 – PTP 800 CMU Front Panel 6
Figure 3 – Indication of FIPS 140-2 capability 9

1 INTRODUCTION

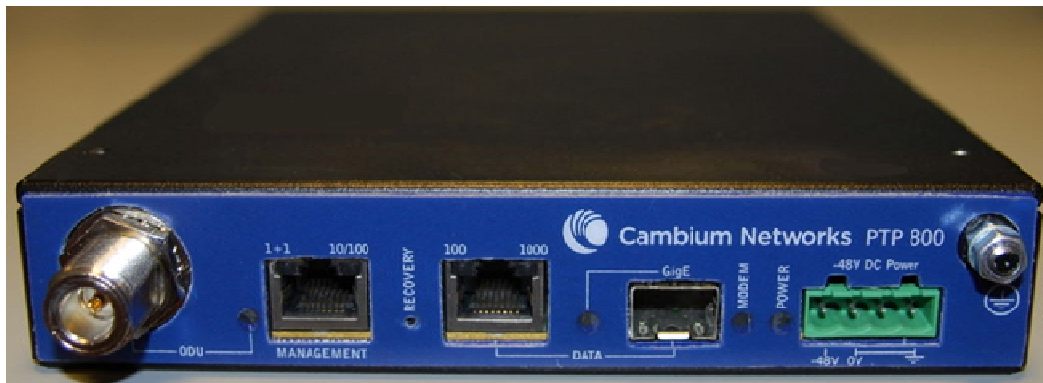
1.1 Purpose

This document describes the security policy for the Cambium Networks PTP 800 Compact Modem Unit (CMU). The primary purpose for this device is to provide data security for Internet Protocol (IP) traffic. The CMU device is a multi-chip standalone cryptographic module encased in hard opaque commercial grade metal cases. The CMU case is the cryptographic boundary of the PTP 800 product.

The CMU is a component of the Cambium Networks PTP 800 Series Point to Point Licensed Ethernet Microwave Bridges (hereafter the PTP 800 or PTP 800 Series). PTP 800 products operate in the 6 to 38 GHz RF bands, with user-configured channel bandwidths from 7 to 56 MHz, and provide a transparent point to point Ethernet service at up to 368 Mbps throughput (full duplex).

A PTP 800 link consists of the CMU together with a Radio Frequency Unit (RFU) designed to operate in the appropriate microwave frequency band. The CMU and RFU are interconnected by a single co-axial cable carrying IF signals, DC power, and control signals.

Figure 1 – PTP 800 CMU



The purpose of this security policy is to validate the Cambium PTP 800 Series software Version PTP 800-05-02 submitted for FIPS 140-2 Level 1 validation.

Three hardware revisions of the CMU are in use: Version 5.2, Version 5.3, and Version 6.6. The differences between these hardware revisions are minor, and unrelated to the cryptographic operation of the unit. The specific differences are as follows:

Version 5.3: Removed PCB test points; changed the SFP cage.

Version 6.6: Removed unused front panel LEDs; changed several resistors to reduce individual power dissipation; changed lightning protection diodes; added circuit traces to support synchronous Ethernet and IEEE 1588v2; modified IF matching network; changed the component type for several decoupling capacitors.

All PTP 800 series products share a common CMU which is FIPS validated.

1.2 Port Identification

Image showing PTP 800 CMU port identification /annotations:

Figure 2 – PTP 800 CMU Front Panel



1.3 The PTP 800 Series Part Numbers

Table 1 – The Cambium PTP 800 Series CMU

| Product Name | HW Part Number |
|--------------|-----------------------------------|
| PTP 800 CMU | WB3517, Versions 5.2, 5.3 and 6.6 |

1.4 References

- (a) FIPS PUB 186-2, Federal Information Processing Standards Publication 186-2, Feb 2000.
- (b) FIPS PUB 180-3, Federal Information Processing Standards Publication 180-3, October 2008.
- (c) FIPS PUB 140-2, Federal Information Processing Standards Publication 140-2, 25th May 2001.
- (d) FIPS PUB 197, Federal Information Processing Standards Publication 192, 26th November 2001.
- (e) DSAVS, Digital Signature Algorithm Validation Suite, 10th March 2004.
- (f) PTP 800 Series User Guide. phn-0896 007v001, Monday 30th June 2008
- (g) X.680, ASN.1 Encoding Rules: specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), (07/02)
- (h) PKCS #8: Private-Key Information Syntax Standard, Version 1.2, November 1, 1993
- (i) PKCS #1: Public Key Cryptography Standards (PKCS), Version 2,1, June 14, 2001
- (j) RFC 4346, The Transport Layer Security Protocol version 1.0, April 2006.
- (k) NIST SP 800-90 Recommendation for Random Number Generators Using Deterministic Random Bit Generators. March 2007.

1.5 Acronyms

| | |
|------|---|
| CA | Certification Authority |
| CMU | Compact Modem Unit |
| CO | Cryptographic Officer |
| CSP | Critical Security Parameter |
| DER | Distinguished Encoding Rules |
| DES | Data Encryption Standard |
| DSA | Digital Signature Algorithm |
| FIPS | Federal Information Processing Standard |
| HMAC | Hashed Message Authentication Code |
| KAT | Known Answer Test |
| PTP | Point to Point |
| SA | System Administrator |
| SNMP | Simple Network Management Protocol |
| TLS | Transport Layer Security |

2 SECURITY LEVEL

The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2.

Table 2 – Module Security Level Specification

| Security Requirements Section | FIPS 140-2 Level |
|-------------------------------------|------------------|
| Cryptographic Module Specification | 3 |
| Module Ports and Interfaces | 1 |
| Roles, Services, and Authentication | 3 |
| Finite State Model | 1 |
| Physical Security | 1 |
| Operational Environment | N/A |
| Cryptographic Key Management | 1 |
| EMI/EMC | 1 |
| Self-Tests | 1 |
| Design Assurance | 3 |
| Mitigation of Other Attacks | N/A |

3 MODE OF OPERATION

3.1 Prerequisites for the Approved Mode of Operation

A user can verify that the wireless unit is capable of operating in FIPS mode by visually inspecting any management webpage and looking for the FIPS logo:

Figure 3 – Indication of FIPS 140-2 capability

The FIPS logo on its own is not an indicator of correct FIPS configuration. The logo is present when the operator has a correct hardware, software, and license line-up to allow FIPS mode. The operator must follow the procedure outlined in Section 3.2 to enter approved mode. When in approved mode, the FIPS logo will be displayed and the Secure Mode Alarm that is used to indicate incorrect configuration will not be asserted.

If the FIPS logo is not displayed, proceed as follows:

- (a) Check the capability summary in the Software License Key page to ensure that the current license key supports AES and FIPS 140-2. If necessary, obtain an access key and generate a new license key.
- (b) Check the installed software version in the System Status page to ensure that the software image is FIPS validated. If necessary, upgrade to the latest FIPS validated image.

3.2 Configuring the Approved Mode of Operation

If the FIPS logo is displayed, the approved mode of operation can be configured using the Security Configuration Wizard.

3.2.1 Obtaining cryptographic material

Before starting the Security Configuration Wizard, ensure that the following cryptographic material has been generated using a FIPS-approved cryptographic generator:

- Key Of Keys
- TLS Private Key and Public Certificates
- Entropy Input
- Wireless Link Encryption Key for AES

3.2.2 Starting Security Configuration Wizard

To start the wizard, proceed as follows:

- (a) Select menu option **Security**. The Security Configuration Wizard page is displayed.
- (b) Review the summary of HTTPS/TLS security related parameters.
- (c) If any updates are required, select **Continue to Security Wizard**.

3.2.3 Step 1: Enter Key of Keys

To enter the Key Of Keys via the Security Wizard, proceed as follows:

- (a) The Step 1: Enter Key of Keys page is displayed.
- (b) Enter the generated key of keys in both the Key Of Keys and Confirm Key Of Keys fields.
- (c) Select **Next**.

3.2.4 Step 2: TLS Private Key and Public Certificate

To enter the TLS Private Key and Public Certificate via the Security Wizard, proceed as follows:

- (a) The Step 2: TLS Private Key and Public Certificate page is displayed.
- (b) If a valid TLS private key exists, then an SHA-256 thumbprint of the key is displayed. If this key is correct, then take no action. Otherwise, select **Browse** and select the generated private key file (.der).
- (c) If a valid TLS public certificate exists, then an SHA-256 thumbprint of the certificate is displayed. If this certificate is correct, then take no action. Otherwise, select **Browse** and select the generated certificate file (.der).
- (d) Select **Next**.

3.2.5 Step 3: User Security Banner

To enter the user security banner via the Security Wizard, proceed as follows:

- (a) The Step 3: User Security Banner page is displayed.
- (b) Update the User Defined Security Banner field.
- (c) Select **Next**.

3.2.6 Step 4: Random Number Entropy Input

To enter the Entropy Input via the Security Wizard, proceed as follows:

- (a) The Step 4: Random Number Entropy Input page is displayed.
- (b) If valid entropy input exists, then an SHA-256 thumbprint of the input is displayed. If this input is correct, then take no action. Otherwise, enter the generated input in the Entropy Input and Confirm Entropy Input fields. If the two values are not identical, an error message is displayed.
- (c) Select **Next**.

3.2.7 Step 5: Enter the Wireless Link Encryption Key

To enter the wireless link encryption key via the Security Wizard, proceed as follows:

- (a) The Step 5: Enter The Wireless Link Encryption Key page is displayed.
- (b) Select the applicable value in the Encryption Algorithm field.
- (c) If a valid encryption key exists, then an SHA-256 thumbprint of the key is displayed. If this key is correct, then take no action. Otherwise, enter the generated key in the Wireless Link Encryption Key and Confirm Wireless Link Encryption Key fields. If the two values are not identical, an error message is displayed.
- (d) Select **Next**.

3.2.8 Step 6: HTTP and Telnet Settings

To configure HTTP and Telnet via the Security Wizard, proceed as follows:

- (a) The Step 6: HTTP and Telnet Settings page is displayed.
- (b) Review and update the HTTP and Telnet attributes. If the unit is required to operate in FIPS 140-2 secure mode, HTTP, Telnet and SNMP Control must all be disabled.
- (c) Select **Next**.

3.2.9 Step 7: Commit Security Configuration

Review all changes that have been made in the Security Wizard. To ensure that the changes take effect, select **Commit Security Configuration**. The unit reboots and the changes take effect.

3.3 Checking that the unit is in the Approved Mode of Operation

The unit is ready to operate in FIPS 140-2 secure mode when both of the following conditions apply:

- (a) The FIPS 140-2 capability logo is displayed in the navigation bar.
- (b) The Secure Mode Alarm is not present in the Home page.

If the FIPS 140-2 capability logo is not displayed in the navigation bar, then return to 3.1 Prerequisites for the Approved Mode of Operation and check that all prerequisites are fulfilled.

If the FIPS 140-2 Operational Mode Alarm is present in the Home page, take action depending upon the alarm setting as follows:

- (a) If the alarm is 'FIPS mode is not configured', then return to 3.2 Configuring the Approved Mode of Operation and check that all Security Wizard settings are correct for FIPS 140-2.
- (b) If the alarm is 'FIPS mode is configured, but not active', then return to 3.2.8 Step 6: HTTP and Telnet Settings and set the following attributes to 'No':
 - HTTP Access Enabled
 - Telnet Access Enabled
 - SNMP Control of HTTP And Telnet

3.4 Approved and non-approved modes of operation

3.4.1 Approved mode of operation

In the non-approved non-FIPS mode of operation, it is possible to use all the approved algorithms of FIPS mode and also to use in the clear management protocols. No CSPs are shared between these modes of operation. A zeroise CSPs is forced if a user causes the unit to transition between modes.

In FIPS mode, the cryptographic module only supports FIPS Approved and allowed algorithms as follows:

Table 3 – FIPS Approved and allowed algorithms

| Algorithm | NIST Certificate Number |
|---|-------------------------|
| SHA-1 and SHA-256 for hashing (b) | 1557 |
| DSA 2048/256 for digital signature verification of uploaded firmware images. The DSA algorithm conforms to FIPS 186-3 (e). | 556 |
| AES 128 & 256-bit firmware library DSP CBC, CTR and ECB modes used in TLS, SNMP, and DRBG. | 1776 |
| AES 128 & 256-bit keys for wireless link encryption engine implemented in FPGA ECB mode only. | 1526 |
| SP800-90 DRBG, CTR_DRBG see (k) section 10.2.1 | 123 |
| Triple-DES 3-key used with TLS cipher suite | 1149 |
| HMAC-SHA-1 used within TLS for key establishment | 1041 |
| RSA 2048-bit for key unwrapping during TLS Handshake (key wrapping; key establishment methodology provides 112 bits of encryption strength) | N/A |

Note that the AES certificate 1526 lists operation with 128-bit, 192-bit, and 256-bit keys, based on the underlying capabilities of the FPGA core used within the PTP 800 CMU. The PTP 800 CMU application software allows a user to select only 128-bit or 256-bit operation.

Table 4 – Management protocols in FIPS mode

| Protocol | Cipher Suites supported by the module | Notes |
|----------------------------------|---|---|
| TLS v1.0 & HTTP over TLS (HTTPS) | TLS_RSA_WITH_3DES_EDE_CBC_SHA TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA | The module acts as the server endpoint in the TLS communication. The clients are authenticated at the application layer using passwords |

3.4.2 Non-FIPS modes of operation

The following algorithms and protocols are available in the Non-FIPS mode of operation:

- (a) Custom RNG¹
- (b) HTTP
- (c) Unencrypted Wireless
- (d) MD5
- (e) RADIUS

The Custom RNG is used only when the CMU has no TLS private key. A TLS private key will always be available when the CMU is in the FIPS approved mode of operation.

MD5 is used as part of SNMPv3 and in the TLS protocol.

RADIUS is used to provide remote authentication for users of the web (HTTP and HTTPS) interface. RADIUS must be disabled in the FIPS approved mode of operation.

4 PORTS AND INTERFACES

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

Table 5 – Ports and Interfaces

| Port | Data Input | Data Output | Status Output | Control Input | Power Input |
|---------------|------------|-------------|---------------|---------------|-------------|
| Gigabit/Fiber | ✓ | ✓ | ✓ | ✓ | |

¹ A custom RNG is included in the operational code. This RNG is not utilised in FIPS mode.

| | | | | | |
|--------------------|---|---|---|---|---|
| Gigabit Management | ✓ | ✓ | ✓ | ✓ | |
| IF | ✓ | ✓ | ✓ | ✓ | |
| Power / Earthing | | | | | ✓ |
| LEDs | | | ✓ | | |
| Recovery Button | | | | ✓ | |

5 IDENTIFICATION AND AUTHENTICATION POLICY

5.1 Assumption of Roles

Table 6 – Roles and Authentication

| Role | Type of Authentication | Authentication Mechanism |
|-----------------------------------|------------------------------------|---|
| Security Officer (Crypto-Officer) | Username and password verification | Username and password entered over a TLS socket to the HTTPS server and verified by CMU. |
| System Administrator | Username and password verification | Username and password entered over a TLS socket to the HTTPS server and verified by CMU. |
| Read-only user | Username and password verification | Username and password entered over a TLS socket to the HTTPS server and verified by wireless unit |

6 ACCESS CONTROL POLICY

6.1 Authentication Strength

In FIPS mode password complexity is enforced:

The complexity rules are:

The password must contain at least two characters for each of the four groups:

- (a) lowercase letter
- (b) uppercase letter
- (c) decimal numerals
- (d) special characters²

The password must have a minimum length of 10 characters

The passwords must not contain the user's username.

The maximum number of repeated characters in a password is 2.

When passwords are changed at least four distinct character must change

Password must not be reused for the next 10 passwords.

Only three authentication attempts are permitted for any user within any one minute period.

A password with minimum complexity can be constructed by selecting, 2 lowercase, 2 uppercase, 2 special characters, and 4 numeric characters. The strength of this combination is calculated as follows:

$$p = \frac{1}{26^2} \cdot \frac{1}{26^2} \cdot \frac{1}{32^2} \cdot \frac{1}{10^4} = \frac{1}{4.7 \times 10^{12}}$$

Table 7 – Password strength

| Test | Strength |
|-------------------------------|--|
| 1 in 100,000 in any minute | Pass strength is 1 in 4.7 x 10 ¹² |
| 1 in 1,000,000 at any attempt | Pass strength is 1 in 1.5 x 10 ¹² |

6.2 Roles and Services

The services available to authenticated users are summarised in Table 8 and Table 9.

² Allowable special characters are: !"#%&'()*+,-./:;<=>@[\\]^_`{|}~

Table 8 also identifies the CSP access type for each CSP in braces after each CSP. {R}ead, {W}rite, {Z}eroize and {U}se internally but don't output.

RO – Read Only User

SA – System Administrator

CO - Cryptographic Officer

Table 8 – Services and CSP Access

| Role | Service | CSPs |
|-------------|------------------------------|--|
| RO, SA, CO | Authentication | Authenticate, password {R,W}, key of keys {U} The CO has R and W access to all user passwords, CO password, SA password, and RO password. Users with the SA or RO role only has R and W access to their associated passwords |
| SA, CO | Firmware Upgrade | DSA Public key {U, W} |
| CO | Encrypt | Encrypt / Decrypt wireless traffic using wireless encryption key {U} , key of keys {U} |
| RO, SA, CO | TLS | Authenticate and key exchange using TLS private key {U}, entropy seed {U}, key of keys {U} TLS pre-master secret {U, W}, TLS master secret {U} and TLS keyset {U} |
| RO, SA, CO | Zerose | Key of keys {Z} |
| | Self-Test | N/A |
| CO | Cryptographic Key Management | Key of keys {U}, TLS X509 private key {W}, wireless link encryption key {W}, entropy seed {W} |
| CO, SA | Module Configuration | N/A |
| CO, SA | Reboot | N/A |
| CO, SA, RO | View Status | N/A |
| CO, SA, RO | View Configuration | N/A |
| CO, SA, RO | Logout | N/A |

Table 9 – Authenticated Services

| Service | Role | Purpose |
|------------------------------|------------|---|
| Authentication | CO, SA, RO | Authenticate user logins |
| Firmware Upgrade | CO, SA | Upgrade operational firmware |
| Encrypt | CO | Encrypt / Decrypt wireless traffic |
| Zeroise | CO, SA, RO | Zeroise all CSPs |
| Cryptographic Key management | CO | Cryptographic key data entry and CSP zeroisation |
| Module Configuration | CO, SA | A selection of standard wireless unit configuration settings |
| Reboot | CO, SA | Reboot the wireless unit |
| View Status | SA, CO, RO | View module status including hardware and firmware versions |
| View Configuration | RO, SA, CO | View all system administrative configuration |
| Logout | RO, SA, CO | Logs out the authenticated operator |
| TLS | RO, SA, CO | Establish a secure TLS session to support secure authentication |

6.3 Unauthenticated Services:

The services available to unauthenticated users are summarised in Table 10.

Table 10 – Unauthenticated Services

| Service | Role | Purpose |
|-----------|------|--|
| Self-Test | - | This service executes a suite of cryptographic self- |

| | | |
|--------------------------|---|--|
| | | tests as required by FIPS 140-2 level 2. This service is initiated via module power cycle |
| Recovery | - | Enter recovery mode |
| SNMP | - | View status and configuration using the SNMP management protocol. It is important to note that no CSPs are transported using the SNMP protocol |
| Visual Status Indication | - | View module status using LEDs |

6.4 Service I/O Specification

Table 11 – Specification of Service Inputs & Outputs

| Service | Control Input | Data Input | Data Output | Status Output |
|------------------|------------------------|---|-----------------------------|---|
| Authentication | Authentication request | Username & password | None | Status OK if username and password match plain text username and password CSP |
| Firmware Upgrade | Upgrade request | Plaintext header + BZIP2 compressed image | DSA verification 'v' vector | Status OK if 'v' = 'r' |
| Zeroise | Zeroise Request | None | None | True if key of keys removed from non-volatile storage and system reboot |
| Self-Test | System reboot | None | None | True if algorithm self-test successful. Otherwise false |
| Cryptographic | Data Entry | Key of Keys, TLS | None | True if key |

| Service | Control Input | Data Input | Data Output | Status Output |
|----------------------|----------------------------|--|------------------------------------|--|
| Key Management | | X509 Private key, TLS public certificate, RNG entropy, passwords | | correctly validated. Otherwise false |
| Module Configuration | Data Entry | Wireless Configuration | None | True if configuration parameters correctly validated. Otherwise false |
| Reboot | Data Entry | None | None | None |
| View Status | View Status Request | None | Status information | None |
| View Configuration | View Configuration Request | None | Configuration Information | None |
| Logout | Logout Request | None | None | OK |
| SNMP | PDU request | PDU data | PDU response data | PDU Status |
| TLS | Session Requests | Authentication & payload data | Session & payload data responses | Session status |
| Recovery | Data Entry | Reset | None | None |
| Encrypt | None | Ethernet bridged packets | Encrypted Ethernet bridged packets | None |

6.5 Definition of Critical Security Parameters

The following CSPs and public keys are contained in the modules FLASH memory. These are NOT read into SDRAM by the FIPS module.

6.5.1 Key of Keys

The key of keys is stored as a 128/256-bit AES key and is stored in the CSP FLASH bank. The key of keys is read during the DMGR initialisation procedure and the key expansion is stored in SDRAM. All DMGR attributes that are marked as CSPs are encrypted/decrypted as they are written/read from the configuration FLASH banks using the key expansion.

The integrity of the key of keys is validated by the user with a CRC32.

The key of keys can be configured or erased by a user with the security officer role.

6.5.2 TLS X509 Private Key

TLS private key is used by the HTTPS server. The private key is designated as a DMGR CSP and is encrypted using the key of keys.

A key size of 2048-bits is supported

Entered via a secure webpage upload

Generated by a FIPS approved algorithm outside the module

Validity checked by performing a modulus check on private and associated public certificate.

The X.509 private key can be configured or erased by a user with the security officer role.

6.5.3 RNG Entropy

SP800-90 DRBG entropy string is used by the TLS stack and other random processes. The entropy string is designated as a DMGR CSP and is encrypted using the key of keys.

A key size of 512-bits is supported

Entered via a secure webpage upload

Generated by a FIPS approved algorithm outside the module

The entropy string can be configured by the security office.

6.5.4 RNG Internal State Variables

SP800-90 DRBG algorithm internal state variable V.

SP800-90 DRBG algorithm 128-bit AES key.

6.5.5 Wireless Encryption Key

The wireless encryption key (AES 128 or 256) is used to encrypt/decrypt all control and data sent over the wireless MAC layer.

The wireless encryption key can be configured by the security officer role.

6.5.6 TLS Key Set

The TLS keyset comprises of the session keys. The TLS service is used for authenticity and privacy when transporting CSPs from the user's browser to PTP 800 module.

The TLS keyset is generated by TLS "Approved" PRF with the help of TLS Master secret and server and client random.

The server random is generated using the approved DRBG. The client random is generated by the operator's browser.

6.5.7 TLS pre-master secret and TLS master secret

The 46 byte pre-master secret is generated by the operator's browser, PKCS#1 v1.5 encoded, wrapped with RSA 2048.

The master-secret is generated using TLS PRF:

`master_secret = PRF(pre_master_secret, "master secret", ClientHello.random + ServerHello.random)`

6.5.8 Passwords

The PTP 800 has 10 configurable user accounts. Each user account has an associated password. All passwords are designated as DMGR CSPs and are encrypted using the key of keys.

A user with the security officer role can reset all user account passwords. Users with system administrator or read only user roles can reset their own passwords

6.5.9 CSP Encrypted by Key of Keys

The following CSPs are AES encrypted (i) using a key of keys approach and are not zeroised:

- (a) Wireless Encryption Key – This key is used for the Encryption/Decryption of all traffic over the wireless link.
- (b) System passwords
- (c) TLS X.509 private key
- (d) DRBG Entropy seed

6.6 Definition of Public Keys

The following are the public keys contained in the module:

- (a) **TLS X509 Public Certificate** (located in the configuration FLASH bank). The certificate can be modified by a user uploading a new valid certificate. The longevity of the key is encoded in the X509 certificate expiry time.
- (b) **Firmware DSA 2048-bit public key** (p, q, g, and y vectors) (located in the FIPS module code and defined as static const unsigned char arrays). The DSA public key cannot be erased and can only be replaced by upgrading the firmware.
- (c) **TLS Public Certificate**

7 OPERATIONAL ENVIRONMENT

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the PTP 800 device does not contain a modifiable operational environment.

8 SECURITY RULES

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

- (a) The cryptographic module shall provide four roles. Security administrator, system administrator, read-only user, SNMP user.
- (b) The cryptographic module shall provide identity based authentication.
- (c) The module supports no bypass states and no maintenance roles.
- (d) The cryptographic module shall perform the following power up self-tests listed in Section 8.1.
- (e) Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- (f) The module does not output CSPs.

8.1 Self-Tests

The operator shall be capable of commanding the module to perform the power-up self-test by power cycling the module.

Data output shall be inhibited during power up self-tests, and error states.

After FIPS configuration the module performs a reboot and subsequent FIPS self-test.

The image will perform the following tests:

8.1.1 Cryptographic Power-up Self-Tests

- (a) SHA-1 and SHA-256 known answer test
- (b) DSA signature verification known answer test
- (c) AES (FPGA used for wireless link encryption). Encryption and Decryption KAT
- (d) AES (DSP TLS and SNMPv3). Encryption and Decryption KAT
- (e) Triple-DES Encryption / Decrypt KAT
- (f) DRBG. Known answer test
- (g) HMAC-SHA-1. Known answer test
- (h) RSA decrypt

8.1.2 Firmware Integrity Test (CRC32)

A firmware integrity test is performed before booting the FIPS module.

8.2 Firmware Self-Tests

- (a) Firmware Load Test: DSA 2048 signature verification
- (b) DRBG Continuous Test comparing greater than 64 bits
- (c) RSA decrypt
- (d) Firmware non-volatile storage integrity check
- (e) CSP integrity self-test is performed when reading CSPS from non-volatile storage.

8.3 FIPS Integrity Test Error Indicators

All FIPS integrity test failures will result in a watchdog reset of the module. The integrity test failure messages are:

- (a) FIPS Cryptographic Self-Test Failure
- (b) FIPS DRBG Failure
- (c) FIPS RSA Decrypt Self-Test Failure
- (d) DSA Pair Wise Consistency FIPS Self-Test Failure
- (e) Bootcode Integrity Check Failure

9 IDENTIFICATION OF FIPS MODE OF OPERATION

Correct configuration of the module can be confirmed by observing the FIPS 140-2 label on the webpage navigation frame and that the Secure Mode Alarm is not present in the Home page.

10 PHYSICAL SECURITY POLICY

The PTP 800 is a multi-chip standalone cryptographic module and includes production-grade components and production-grade opaque enclosure.

11 MITIGATION OF OTHER ATTACKS POLICY

No other attacks have been identified.

Cambium Networks

Cambium Networks provides professional grade fixed wireless broadband and microwave solutions for customers around the world. Our solutions are deployed in thousands of networks in over 153 countries, with our innovative technologies providing reliable, secure, cost-effective connectivity that's easy to deploy and proven to deliver outstanding metrics.

Our award-winning Point to Point (PTP) radio solutions operate in licensed, unlicensed and defined use frequency bands including specific FIPS 140-2 solutions for the U.S. Federal market. Ruggedized for 99.999% availability, our PTP solutions have an impeccable track record for delivering reliable high-speed backhaul connectivity even in the most challenging non-line-of-sight RF environments.

Our flexible Point-to-Multipoint (PMP) solutions operate in the licensed, unlicensed and federal frequency bands, providing reliable, secure, cost effective access networks. With more than three million modules deployed in networks around the world, our PMP access network solutions prove themselves day-in and day-out in residential access, leased line replacement, video surveillance and smart grid infrastructure applications.

Cambium Networks solutions are proven, respected leaders in the wireless broadband industry. We design, deploy and deliver innovative data, voice and video connectivity solutions that enable and ensure the communications of life, empowering personal, commercial and community growth virtually everywhere in the world.



www.cambiumnetworks.com

Cambium Networks and the stylized circular logo are trademarks of Cambium Networks, Ltd. All other trademarks are the property of their respective owners.

© Copyright 2013 Cambium Networks, Ltd. This document may be freely reproduced and distributed in its entirety without modification.