Cambium Networks Ltd

PTP 700 Point to Point Wireless Ethernet Bridge

Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

System Release 700-01-00-FIPS

Contents

Tables

Figures

1 INTRODUCTION

1.1 Purpose

This document is the Security Policy for the Cambium Networks PTP 700 Point to Point Wireless Ethernet Bridge Outdoor Unit (ODU). The ODU meets the requirements for a Cryptographic Module validated to FIPS 140-2 at Level 2. In this Security Policy, we refer to the PTP 700 ODU as "the Module".

1.2 Supported hardware variants

The Module is available in 20 different hardware variants as detailed in Table 1.

Table 1 – Cryptographic module hardware configurations

	Module	HW P/N and Version
1	PTP 700 Connectorized ODU (FCC)-White	C045070B001A
2	PTP 700 Connectorized+Integrated ODU (FCC)-White	C045070B002A
3	PTP 700 Connectorized ODU (Global)-White	C045070B003A
4	PTP 700 Connectorized+Integrated ODU (Global)-White	C045070B004A
5	PTP 700 Connectorized ODU (EU)-White	C045070B005A
6	PTP 700 Connectorized+Integrated ODU (EU)-White	C045070B006A
7	PTP 700 Lite Connectorized ODU (FCC)-White	C045070B007A
8	PTP 700 Lite Connectorized+Integrated ODU (FCC)-White	C045070B008A
9	PTP 700 Lite Connectorized ODU (Global)-White	C045070B009A
10	PTP 700 Lite Connectorized+Integrated ODU (Global)-White	C045070B010A
11	PTP 700 Lite Connectorized ODU (EU)-White	C045070B011A
12	PTP 700 Lite Connectorized+Integrated ODU (EU)-White	C045070B012A
13	PTP 700 Connectorized ODU (IC)-White	C045070B025A
14	PTP 700 Connectorized+Integrated ODU (IC)-White	C045070B026A
15	PTP 700 Lite Connectorized ODU (IC)-White	C045070B027A

	Module	HW P/N and Version
16	PTP 700 Lite Connectorized+Integrated ODU (IC)-White	C045070B028A
17	PTP 700 Connectorized ODU (Global)-Green	C045070B034A
18	PTP 700 Connectorized+Integrated ODU (Global)-Green	C045070B038A
19	PTP 700 Connectorized ODU (Global)-Desert Tan	C045070B039A
20	PTP 700 Connectorized+Integrated ODU (Global)-Desert Tan	C045070B040A

1.3 Supported firmware versions

The Module supports one firmware version as listed in Table 2.

Table 2 – Cryptographic module firmware versions

	Modules supported	Firmware Version
1	See 1 to 20 in Table 1.	700-01-00-FIPS

1.4 Module description

The Module is deployed in pairs to create a wireless bridge between two Ethernet networks. The PTP 700 product operates in licensed, lightly-licensed, and unlicensed frequency bands between 4400 MHz and 5875 MHz, in channel bandwidths up to 45 MHz, providing aggregate data rates up to 450 Mbit/s. The Module transmits and receives Ethernet frames as plaintext, and transmits and receives encrypted wireless signals.

The Module is available in 20 different variants, listed in Table 1.

The 20 variants consist of combinations of physical format, regional variants, capacity variants and surface finishes.

PTP 700 has two physical formats or platform variants as follows:

(a) Connectorized

(b) Connectorized+Integrated

The Connectorized variants are intended to be connected to an external antenna. The Connectorized+Integrated variants include an integrated flat panel antenna and additionally provide connectors for an external antenna that can be used in place of the integrated antenna.

The Module is available in four regional variants:

(a) FCC. This variant supports only the FCC rules for the USA and associated territories.

(b) EU. This variant supports countries of the European Union.

(c) IC. This variant supports the Industry Canada rules for operation in Canada.

(d) Global. This variant supports operation in any country.

The sale and distribution of the regional variants are restricted; for example, only the FCC variant is available for purchase by customers in the USA, and only the EU variant is available in the EU.

The Module is available in two capacity tiers: the capacity of the Lite variant provides 50% of the capacity of the Full variant. The features and general capabilities of the Lite and Full variants are otherwise identical.

The green and desert tan units are identical in performance and construction to the equivalent white units, except that:

- The green and desert tan units have a coloured paint finish, where the white units have a powder-coat finish.
- The tamper-evident seals on the green and desert tan units have a matt black background, where the tamper-evident seals on the white units have a silver metallic background.
- The connectors and fixings in the green and desert tan units have a black surface finish, where the connectors and fixings on the white units have a reflective plated finish.

1.5 Hardware and physical cryptographic boundary

The Module is a multi-chip standalone device, where the cryptographic boundary is the external housing of the ODU.

The physical form of the two hardware platform variants is shown in Figure 1 and Figure 2. In each case, the physical boundary of the ODU is the physical cryptographic boundary.

A unit with the green surface finish is shown in Figure 3. A unit with the desert tan surface finish is shown in Figure 4.

Figure 1 – PTP 700 Connectorized Hardware Variant (White)

Figure 2 – PTP 700 Connectorized+Integrated Hardware Variant (White)

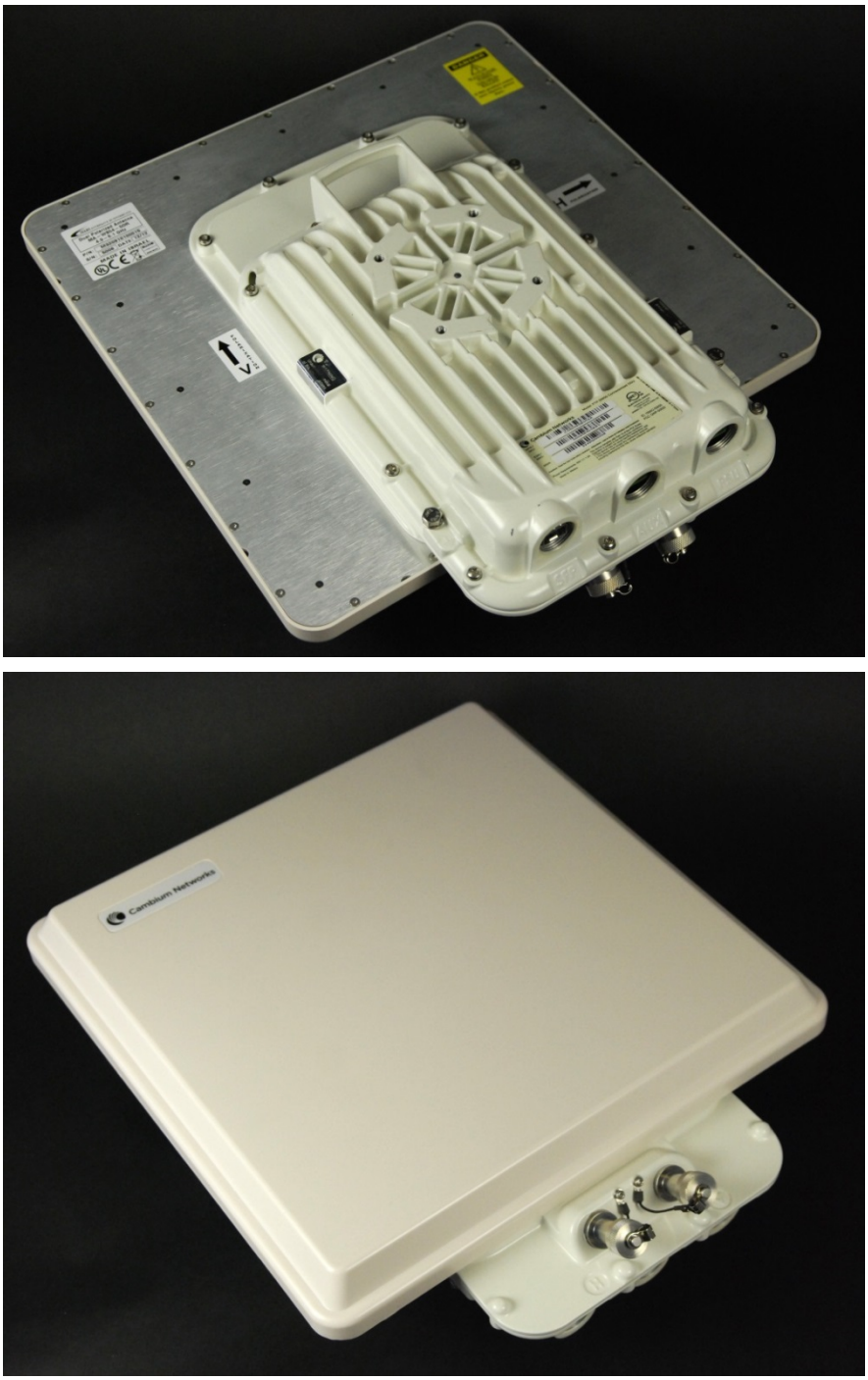


Figure 3 – PTP 700 Connectorized Hardware Variant (Green)

Figure 4 – PTP 700 Connectorized+Integrated Hardware Variant (Desert Tan)

1.6 Ports and interfaces

The Module provides the ports and interfaces listed in Table 3

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
Main PSU Port	Transports plaintext data in and out when configured as a logical data port. Transports control in and status out when configured as a logical management port. Provides power to the module using power over Ethernet.	Power, Control in, Data in, Data out, Status out
Aux Port	Transports plaintext data in and out when configured as a logical data port. Transports control in and status out when configured as a logical management port.	Control in, Data in, Data out, Status out
SFP (Fiber) Port	Transports plaintext data in and out when configured as a logical data port. Transports control in and status out when configured as a logical management port.	Control in, Data in, Data out, Status out
RF Horizontal	RF input and output for connection to an external horizontally polarised antenna. Exchanges encrypted control in, data in, data out and status out with another ODU. For connectorized operation, input and output are via an N type connector. For integrated operation, input and output are via the antenna.	Control in, Data in, Data out, Status out
RF Vertical	RF input and output for connection to an external vertically polarised antenna. Exchanges encrypted control in, data in, data out and status out with another ODU. For connectorized operation, input and output are via an N type connector. For integrated operation, input and output are via the antenna.	Control in, Data in, Data out, Status out
Ground terminal	Used for safety and lightning protection.	Power

The location of the ports is identified in Figure 5 and Figure 6.

Figure 5 – Location of ports and interfaces on the Connectorized platform variant

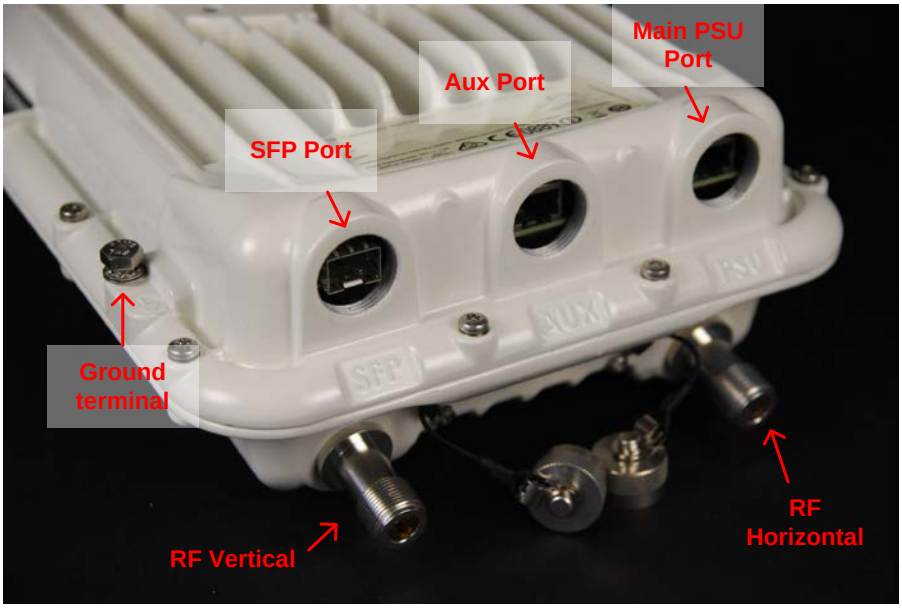
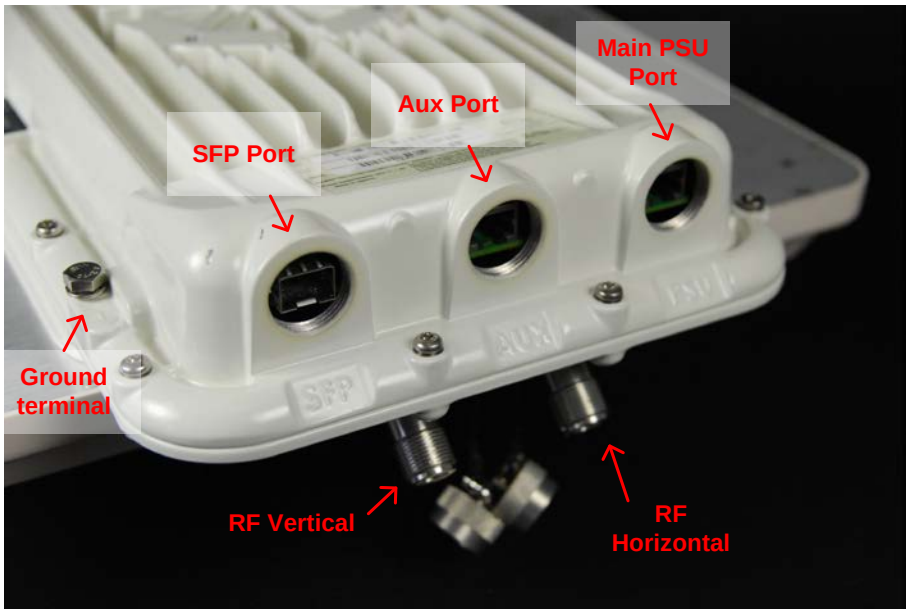


Figure 6 – Location of ports and interfaces on the Connectorized+Integrated platform variant



1.7 Firmware and logical cryptographic boundary

The Module executes a single firmware image protected by a 2048-bit DSA signature. The firmware includes an embedded real time operating system (RTOS). The module will not load or execute software supplied by the user or by third parties. The module does not have a general-purpose operating environment, and does not provide any direct access for users to the operating system.

1.8 Security level

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

Table 4 – Security Level of Security Requirements

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

1.9 Modes of operation

Cambium Networks provides distinct firmware images for standard (non-FIPS) and FIPS operation. The standard image always operates in the standard (non-FIPS) mode, and the FIPS image operates in the FIPS Approved mode when:

(a) A minimum 10 character password is used for all authorized roles. If a password shorter than 10 characters is used with the FIPS image, the module is in the non-Approved mode.

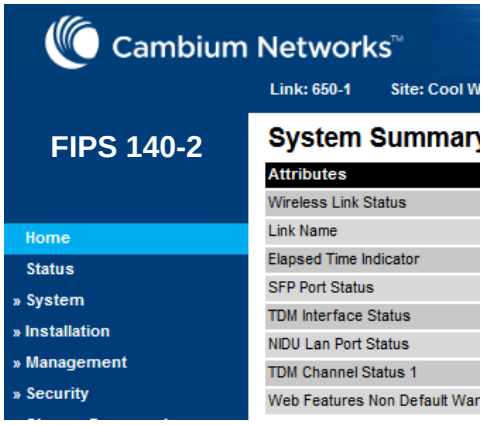
(b) Remote authentication using RADIUS is disabled.

Any ODU in the PTP 700 series can be used in the FIPS approved mode, and there are no special "FIPS hardware" variants. However, the FIPS firmware cannot be installed unless the PTP 700 unit has a license key that includes the FIPS license. The license is sold as an optional upgrade. A new license key can be generated at the Cambium Networks web site, binding the purchased upgrade to a specific hardware serial number.

The presence of the FIPS firmware image is indicated by the display of a "FIPS 140-2" graphic in the navigation bar of the web-based management interface as shown in Figure 7.

To change from the Approved mode to the non-Approved by setting a password shorter than 10 characters or enabling RADIUS, the operator shall zeroize all keys using the zeroization service, then power cycle the module.

Figure 7 – Indication of FIPS firmware



2 CRYPTOGRAPHIC FUNCTIONALITY

2.1 Cryptographic functions

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: Encryption, Decryption Modes: CFB128 Key sizes: 128, 256 bits Used for stream encryption and decryption over the wireless link.	2594
AES	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC, CTR Key sizes: 128, 256 bits Used for SNMP, TLS and DRBG in the management agent.	2754
KTS	[SP 800-38F] Key Transport within TLS Key sizes: AES 128 or 256 bits HMAC-SHA-1 used for authentication Security Strengths: 128 or 256 bits	AES 2754, HMAC 1728
DRBG	[SP 800-90A] Functions: CTR DRBG Security Strengths: 128 bits	465
DSA	[FIPS 186-4] Functions: Signature Verification Key sizes: 1024 bits and 2048 bits (DSA 1024 is not used as part of the module's security services)	842
HMAC	[FIPS 198-1] Functions: Generation, Verification SHA sizes: HMAC-SHA1, HMAC-SHA256	1728
SHA	[FIPS 180-4] Functions: Digital Signature Verification, SNMP KDF SHA sizes: SHA-1, SHA-256	2323

Algorithm	Description	Cert #
SNMP KDF	[SP 800-135] Functions: Key Derivation Function	202
TLS KDF	[SP 800-135] Functions: Key Derivation Function	203

Table 6 – Protocols Allowed in FIPS Mode

Note that these protocols have not been reviewed or tested by the CAVP or CVMP.

Protocol	Description	Cert #
TLS v1.0/v1.1	[IG D.8 and SP 800-135] Cipher Suites: TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_AES_256_CBC_SHA Key Derivation Function in uses HMAC-SHA-1 and MD5. TLS Message uses HMAC-SHA1	TLS KDF: 203 HMAC:1728
SNMPv3	[IG D.8 and SP 800-135]	SNMP KDF: CVL 202 AES: 2594

Table 7 – Non-Approved Algorithms Allowed in FIPS Mode

Algorithm	Description
RSA	Functions: Key wrapping Key size: 2048-bit (provides 112 bits of strength)
MD5	Allowed only for use in TLS

Table 8 – Non-Approved Algorithms for use in Standard (non-FIPS) Mode only

Algorithm/Protocol	Description
Custom RNG	The Custom RNG is used as part of a challenge-response scheme that protects a debug mode. Debug mode allows the manufacturer to investigate problems in equipment deployed by customers. Debug access is disabled in the ODU as a default, and must be enabled by the operator of the equipment. In the FIPS approved mode, debug access is permanently disabled, and cannot be enabled by the operator or manufacturer.
RADIUS	RADIUS is used for remote authentication of username and password credentials for access to the web-based management interface. Remote authentication must be disabled in the FIPS approved mode.
MD5	MD5 is used to authenticate NTP messages for synchronization.

2.2 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
Key of keys	128 or 256-bit AES key stored in the dedicated CSP flash bank. The key of keys is read during the data manager initialisation procedure and the key expansion is stored in RAM. The integrity of the key of keys is validated by a CRC32. The key of keys CSP may be configured or erased by a user with the CO role. The key of keys attribute is used to encrypt the remaining CSPs for storage in general purpose flash memory banks, and to decrypt CSPs as they are read from flash memory. The key of keys must be generated by a FIPS-approved algorithm outside the module.
TLS private key	2048-bit private key used in RSA-2048 by the HTTPS server. Encrypted and decrypted for non-volatile storage using the key of keys. Validity of the private key is checked by performing a modulus check on private and associated public certificate. The TLS private key may be configured by a user with the CO role, and erased by a CO using the Zeroise CSPs service. The TLS private key must be generated by a FIPS-approved algorithm outside the module.
RNG entropy	SP800-90 DRBG entropy string with key size of 512 bits, used by the TLS interface and other random processes. Encrypted and decrypted for non-volatile storage using the key of keys. The RNG entropy may be configured by a user with the CO role, and erased by a CO using the

CSP	Description / Usage
	Zeroise CSPs service. The RNG entropy must be generated by a FIPS-approved algorithm outside the module. RNG entropy input into the module must have a minimum of 512 bits of entropy.
HMAC session key	256-bits generated using the FIPS-approved DRBG. Used by the authentication process to sign and verify HMAC signed web authentication cookies. Overwritten every time a user successfully authenticates to the Module. The authentication cookie is used by the Module to create and store session information. Each time a webpage is clicked by an authenticated user the session cookie is replayed by the browser. After receiving the cookie, the Module uses the HMAC session key and arguments extracted from the cookie to regenerate the HMAC. If the HMAC is successfully regenerated the user is allowed access to the Module otherwise the user is forced to re-authenticate.
Wireless encryption key	128 or 256 bit AES key used to encrypt and decrypt all control and data sent over the wireless link. Encrypted and decrypted for non-volatile storage using the key of keys. The wireless encryption key may be configured by a user with the CO role, and erased by a CO using the Zeroise CSPs service. The wireless encryption key must be generated by a FIPS-approved algorithm outside the module.
TLS key set	Consists of the session keys. The TLS keyset is generated by TLS approved PRF with the help of TLS master secret and server and client random. The TLS service is used for authenticity and privacy when transporting CSPs from the user's browser to the Module. The server random is generated using the approved DRBG. The client random is generated by the operator's browser.
TLS master secret and pre-master secret	The 46-byte pre-master secret is generated by the user's browser, PCKS#1 v1.5 encoded, wrapped with RSA 2048. The 48-byte master-secret is generated using TLS PRF: master_secret = PRF(pre_master_secret, "master secret", ClientHello.random + ServerHello.random). The TLS Pre-Master Secret and TLS Master Secret are zeroized after use.
DRBG internal state	The DRBG state (V and Key) are stored in volatile memory. The DRBG internal state is zeroized after use.
Passwords	The Module has 10 configurable user accounts for the web-based (HTTPS) interface. Each user account has an associated password. All passwords are designated as CSPs and are encrypted using the key of keys. A user with the CO role can reset all user account passwords. Users with SA or RO roles can reset their own passwords.
SNMP session key	When using SNMP version 3 a session key is negotiated between the client and server. SNMP is used for general configuration and status reporting. CSPs are not accessible via SNMP.

2.3 Public Keys

Table 10 – Public Keys

Key	Description / Usage
TLS public certificate	Public component of a 2048-bit RSA key pair with the TLS private key. The certificate can be configured by a user with the CO role, and erased by a CO using the Zeroise CSPs service. The longevity of the key is encoded in the X509 certificate expiry time.
Firmware DSA public key	DSA 2048-bit public key (p, q, g and y vectors) used to authenticate replacement firmware. The DSA public key cannot be erased and can only be replaced by upgrading the firmware.

3 ROLES, AUTHENTICATION AND SERVICES

3.1 Assumption of Roles

The Module supports four distinct operator roles, Security Officer (SO), System Administrator (SA), Read Only (RO) and Firmware Update (FU). The permissions of the SO role are a superset of the permissions of the SA role, and the permissions of the SA role are a superset of the permissions of the RO role. The cryptographic module enforces the separation of roles using identity-based authentication, where each user is assigned one of the roles. A user is never required to change roles. Table 11 lists the operator roles supported by the Module.

The Security Officer role is equivalent to the Cryptographic Officer identified in [FIPS140-2].

The System Administrator is equivalent to the User identified in [FIPS140-2].

The Module does not support a maintenance role and/or bypass capability.

The Module does not support concurrent operators. An authenticated operator may be logged out by the Module following a configurable period of inactivity, or when another user with higher permissions seeks to log in.

Authentication data is entered at a web page, and is protected during entry by HTTPS/TLS. Authentication data is authenticated by comparison with data stored locally in the Module. Passwords are stored as a cryptographic hash value derived from the configured password string. The cryptographic hash value is further encrypted for non-volatile storage using the key of keys.

Table 11 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
Security officer	A system administrator with read/write access to general and cryptographic configuration.	Identity-based	Username and password
System Administrator	A system administrator with read/write access to general configuration but no access to cryptographic configuration.	Identity-based	Username and password
Read Only	An operator with read-only access to general configuration but no access to cryptographic configuration.	Identity-based	Username and password
Firmware Update	An operator responsible for updating the firmware on the module	Identity-based	Digital signature

3.2 Authentication Method

Password authentication

The Module does not enforce a minimum password complexity or length. On order for the module to be in the FIPS Approved Mode, the following password requirements shall be followed. The password must contain at least:

(a) Two characters for each of the four groups:

- lowercase letter
- uppercase letter
- decimal numerals
- special characters

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

(b) A minimum of 10 characters

(c) No more than two repeated characters.

A user account is locked following three unsuccessful authentication attempts.

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

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

The maximum number of sequential attempts to guess a password before management action is needed to restore access is three attempts for each of ten user accounts, making a total of 30 attempts. There is a possibility that these 30 attempts could be made within one minute.

Table 12 – Password strength

Requirement	Strength
1 in 10^6 at any attempt	Pass strength is 1 in 4.7 x 10^{12}
1 in 10^5 in any minute	Pass strength is 1 in 1.5 x 10^{11}

In addition to the password complexity listed above, when passwords are changed at least four distinct characters must change. A password must not be reused for the next 10 passwords.

Digital signature authentication

Firmware updates are authenticated by a DSA 2048 digital signature, which provides 112 bits of security. The probability of a random attempt succeeding is 2^{-112} . Approximately four firmware update attempts can be performed in a one minute period. The probability of a random attempt succeeding in a one minute period is 4×2^{-112}.

3.3 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service.

Table 13 – Authenticated Services

Service	Role	Purpose
Zeroise CSPs	SO	Zeroizes CSPs stored in non-volatile memory by erasing the flash bank containing the key of keys. Removes CSPs from volatile memory by reboot.
Configure CSPs	SO	Allows a SO user to install key of keys, TLS private key, RNG entropy, and wireless encryption key. RNG entropy input into the module must have a minimum of 512

Service	Role	Purpose
		bits of entropy.
Create and administer user accounts	SO	Allows a SO user to create user accounts for users of the web-based interface. Allows a SO user to reset the passwords for web-users.
Login	SO, SA, RO	Permits access to the management agent for a user of the web-based management interface by authenticating username and password. Automatically logs out any existing user of the same or lower privileges.
Update password	SO, SA, RO	Allows a user of the web-based interface to update his or her own password.
Reboot by command	SO, SA	Allows a SO or SA user to reboot the Module by means of a command in the web-based interface.
Upgrade firmware	SO, SA, FU	Allows a SO, SA or FU operator to upgrade the operational firmware in the Module. CSPs are zeroized if standard firmware is upgraded to FIPS firmware, or FIPS firmware is upgraded to standard firmware.
Logout	SO, SA, RO	Invalidates any previously HMAC signed cookies by regenerating the HMAC session key
Encrypt/decrypt	SO	Allows a SO operator to configure AES encryption keys for the wireless port.
General configuration	SO, SA	Allows a SO or SA operator to configure wireless and networking operation of the module, excluding configuration of CSPs.

Note that all CSPs stored in non-volatile memory are first encrypted using AES with a Key of Keys. The Key of Keys is stored in a dedicated flash bank. The Zeroize CSPs service erases the Key of Keys bank and thereby denies access to other CSPs. This approach ensures that all CSPs are zeroized as a consequence of a single action, and ensures that general configuration attributes are not affected by the Zeroize CSPs action.

Table 14 – Unauthenticated Services

Service	Description
Encrypt/decrypt	The module encrypts traffic for transmission at the wireless port, and decrypts traffic received at the wireless port.

Service	Description
Reboot by power cycle	The module automatically reboots on a power cycle
Establish HTTPS/TLS session	The TLS secure communications protocol for the web interface using the TLS private key, TLS master secret and pre-master secret, and the TLS key set, is used before the user is authenticated. The user must subsequently be authenticated by username and password for access to authenticated services.
Power-on self-test	The module executes a suite of cryptographic self-tests on power-up.
General configuration	Some aspects of wireless and networking operation can be configured via the SNMP interface. CSPs are not accessible via this interface.
View Status	Users can view status of PTP 700 wireless unit in the web-based (HTTP) interface, and via the SNMP interface
Zeroize CSPs	An unauthenticated operator can zeroize CSPs by booting the module in recovery mode. Recovery mode is selected by a short power cycle.
Reset network configuration	An unauthenticated operator can reset the Ethernet and IP configuration from recovery mode. This is useful if, for example, the operator has forgotten the IP address of the unit.
Reset all configuration data	An unauthenticated operator can reset all configuration data, including CSPs and network configuration, from recovery mode.
Reboot from recovery	Recovery mode provides an option to reboot the unit.

Table 15 – CSP Access Rights within Services

Service	Key of keys	TLS private key	RNG entropy	HMAC session key	Wireless encryption key	TLS key set	TLS master secret and pre-master secret	Passwords
Authenticated services								
Zeroise CSPs	Z	Z	Z	Z	Z	Z	Z	Z
Configure CSPs	W	W	W		W			
Create and administer user accounts	R							W

Service	Key of keys	TLS private key	RNG entropy	HMAC session key	Wireless encryption key	TLS key set	TLS master secret and pre-master secret	Passwords
Login	R							R
Update password	R							W
Reboot by command								
Upgrade firmware (see Note)	Z	Z	Z	Z	Z	Z	Z	Z
Logout								
General configuration								
Unauthenticated services								
Encrypt/decrypt					R			
Reboot by power cycle								
Establish HTTPS/TLS session	R	R	R	R		R	R	
Power-on self-test								
General configuration								
View Status								
Zeroize CSPs	Z	Z	Z	Z	Z	Z	Z	Z
Reset network configuration								
Reset all configuration data	Z	Z	Z	Z	Z	Z	Z	Z
Reboot from recovery								

Note: The Upgrade Firmware service zeroises all CSPs when firmware is upgraded from standard (non-FIPS) to FIPs, or from FIPS to standard firmware. The FIPS firmware is upgraded to a later version of FIPS firmware, the CSPs are retained.

4 SELF-TESTS

Each time the Module is powered up it tests that the cryptographic algorithms 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 cryptography by the Module. If one of the KATs fails, the Module reboots and repeats the self-tests.

The Firmware Integrity Test sends the module into recovery mode if it fails.

Table 16 – Power Up Self-tests

Test Target	Description
Firmware Integrity	32 bit CRC performed over all code in EEPROM.
AES	KATs: Encryption, Decryption Modes: CFB128 Key sizes: 128 bits Stream-based encryption used for data transferred over the wireless link
AES	KATs: Encryption, Decryption Modes: ECB, CBC Key sizes: 128 bits Used for TLS
DRBG	KATs: CTR DRBG Security Strengths: 128 bits
DSA	KAT: Signature Verification Key sizes: 2048 bits
HMAC	KATs: Generation, Verification SHA sizes: HMAC-SHA1, HMAC-SHA256
RSA	KATs: RSA Decrypt Key sizes: 2048 bits
SHA	KATs: SHA-1, SHA-256

RSA is used only as part of HTTPS.

Possible test failure messages are as follows:

(a) FIPS Cryptographic Self Test Failure

(b) FIPS DRBG Failure

(c) FIPS RSA Decrypt Self Test Failure

(d) DSA Signature Verification FIPS Self Test Failure

(e) Bootcode Integrity Check Failure (32-bit CRC)

Table 17 – Conditional Self-tests

Test Target	Description
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG. DRBG health tests as described in SP800-90A, Section 11.3.
Firmware Load	DSA 2048 signature verification performed when firmware is loaded.

The module does not have a hardware RNG.

Table 18 – Critical Function Self-tests

Test Target	Description
CSP Integrity Check	Performed when reading CSPs from non-volatile storage.

5 PHYSICAL SECURITY POLICY

The PTP700 is a multi-chip standalone cryptographic module and includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with two tamper evident labels.
- Protected, opaque vent.

Tamper-evident labels

The tamper-evident labels on the module enclosure must be checked every 30 days. If damage to the label or the enclosure is observed, the module should be removed from service and inspected more closely. The correct location of the tamper evident labels is shown in Figure 8 to Figure 11.

Figure 8 – Detail of the tamper-evident label on a white Connectorized+Integrated unit

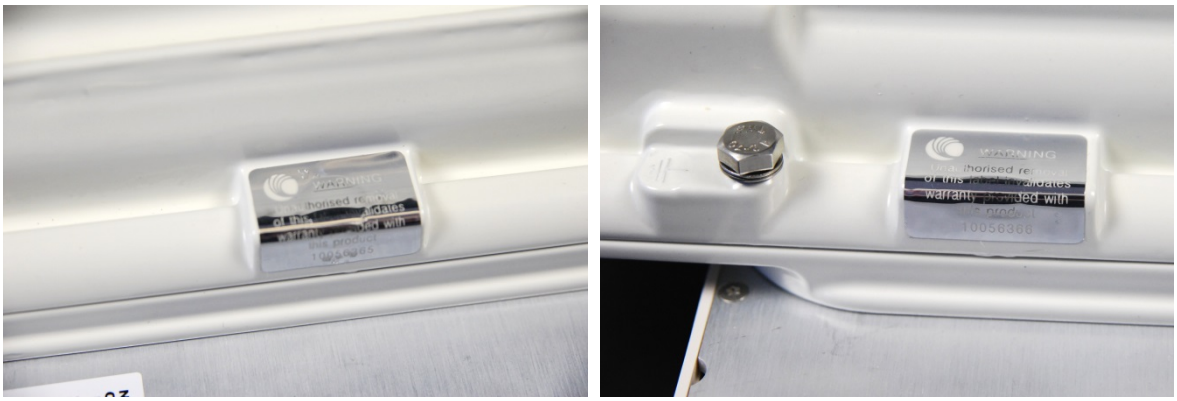


Figure 9 – Detail of the tamper evident label on a white connectorized unit

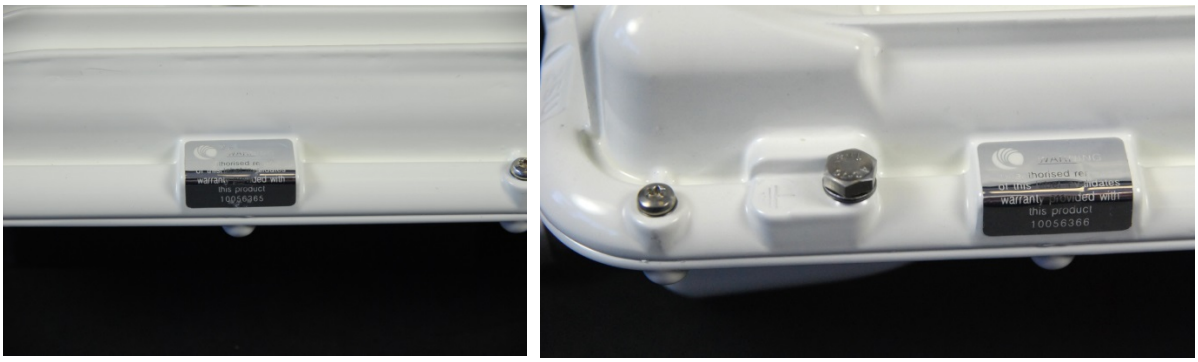


Figure 10 – Detail of the tamper-evident label on a tan Connectorized+Integrated unit

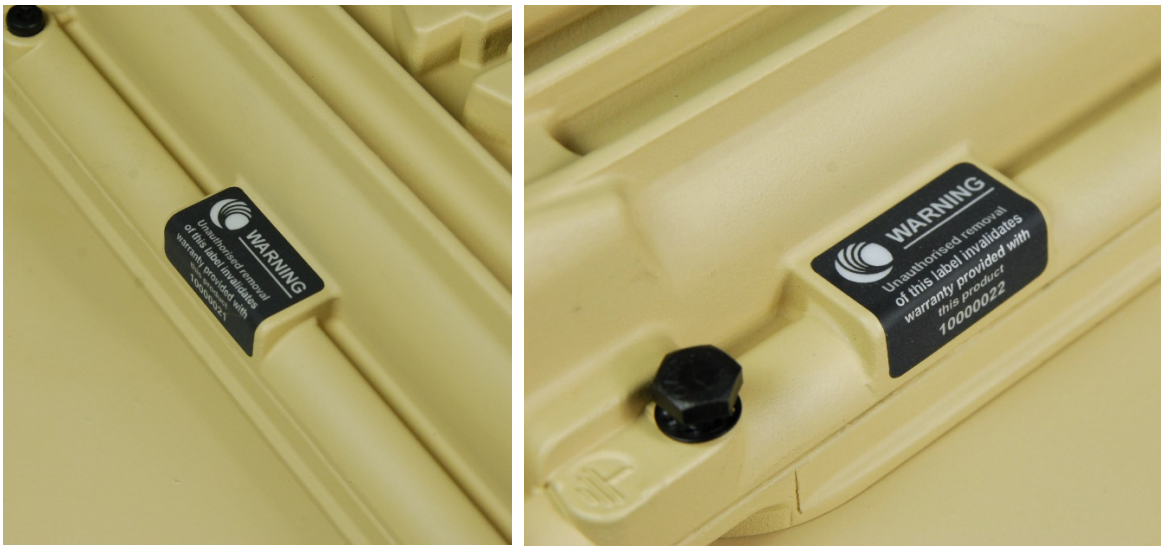


Figure 11 – Detail of the tamper evident label on a green connectorized unit

Tamper-evident labels are applied to the PTP 700 ODU as part of the manufacturing process.

If labels are damaged, return ODUs to Cambium Networks using the RMA process to request replacement labels. Spare labels are not available to operators.

Inspection of the tamper-evident labels

PTP 700 ODUs with White finish are fitted with silver-coloured tamper-evident labels. The labels consist of a thin foil layer protected by a clear plastic layer. When the label is removed, the foil layer is perforated, as shown in Figure 12. Any visible damage to the foil layer indicates that the label may have been removed by an attacker.

PTP 700 ODUs with Green or Dessert Tan finish are fitted with black labels. The labels consist of a thin foil layer protected by an opaque plastic layer printed in white on a black background. When the label is removed, the foil layer delaminates to show a characteristic diagonal pattern consisting of the repeated word "VOID". This is visible across the label but is particularly visible in the white graphics and text, as shown in Figure 12. Any appearance of the "VOID" indicator shows that the label may have been removed by an attacker.

Figure 12 – Example of label tampering

6 OPERATIONAL ENVIRONMENT

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the PTP 700 device does not contain a modifiable operational environment.

7 MITIGATION OF OTHER ATTACKS POLICY

No other attacks have been identified.

8 SECURITY RULES AND GUIDANCE

Operator roles

The Module supports three operator roles for access to the management agent of the unit, but only the Security Officer role has access to the security configuration of the Module. The other two roles are provided for general administration of non-security-related aspects of the PTP 700 product.

Plaintext/Ethernet frames received at the wired Ethernet ports are encrypted within the Module for transmission at the wireless ports. Similarly, encrypted data received at the wireless ports is decrypted within the Module and transmitted as plaintext Ethernet frames at the wired Ethernet ports. These frames are simply processed data and as data (i.e. not a User), authentication does not apply.

Direct connection for initial configuration

The Module zeroizes CSPs on transition into the FIPS Approved Mode. As a consequence, the initial security configuration will be completed using an unprotected HTTP session. Security Officers must ensure that the initial security configuration of the Module is completed in a restricted environment using a direct cabled Ethernet connection from a standalone PC or other management workstation. Subsequent management actions can use the HTTPS interface, and in this case the connection between the management workstation and the Module can be via a LAN or other data network.

FIPS-approved generation for cryptographic material

The Module requires that the cryptographic material used must be generated outside the module using FIPS-approved random generation algorithms.

9 REFERENCES AND DEFINITIONS

The following standards are referred to in this Security Policy.

Table 19 – References

Abbreviation	Full Specification Name
[DSA2VS]	Digital Signature Algorithm Validation System, May 2014.
[FIPS140-2]	Security Requirements for Cryptographic Modules, December 2002.
[FIPS180-4]	Secure Hash Standard, March 2012
[FIPS186-4]	Digital Signature Standard, July 2013
[FIPS197]	Advanced Encryption Standard, November 2001
[PKCS#1]	Public Key Cryptography Standards (PKCS), Version 2.2, October 2012
[PKCS#8]	Private-Key Information Syntax Standard, Version 1.2, May 2008
[phn-4148]	Cambium Networks PTP 700 Series User Guide
[RFC4346]	The Transport Layer Security Protocol version 1.0, April 2006.
[SP800-90A]	Recommendation for Random Number Generators Using Deterministic Random Bit Generators, January 2012.
[SP800-131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011
[SP800-131B]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, February 2011
[X.680]	Abstract Syntax Notation One (ASN.1): Specification of basic notation, August 2015.

Table 20 – Acronyms and Definitions

Acronym	Definition
CA	Certification Authority
CO	Cryptographic Officer
CSP	Critical Security Parameter
DER	Distinguished Encoding Rules
DSA	Digital Signature Algorithm
FIPS	Federal Information Processing Standard

Acronym	Definition
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
KDF	Key Derivation Function
PTP	Point to Point
SA	System Administrator
SNMP	Simple Network Management Protocol
TLS	Transport Layer Security

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.

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

© Copyright 2018 Cambium Networks, Ltd. May be reproduced only in its original entirety [without revision].