

**Cambium Networks Ltd**  
**PTP 700 Point to Point**  
**Wireless Ethernet Bridge**  
**Non-Proprietary FIPS 140-2**  
**Cryptographic Module**  
**Security Policy**  
**System Release 700-02-65-FIPS**

# Contents

- 1 Introduction ..... 5
  - 1.1 Purpose ..... 5
  - 1.2 Supported Hardware Variants ..... 5
  - 1.3 Supported Firmware Versions ..... 6
  - 1.4 Module Description ..... 6
  - 1.5 Hardware and Physical Cryptographic Boundary ..... 7
  - 1.6 Ports and Interfaces ..... 12
  - 1.7 Firmware and Logical Cryptographic Boundary ..... 14
  - 1.8 Security Level ..... 14
  - 1.9 FIPS Approved Mode ..... 14
  - 1.10 Configuration and Operation States ..... 15
- 2 Cryptographic Functionality ..... 16
  - 2.1 Cryptographic Functions ..... 16
  - 2.2 Critical Security Parameters ..... 21
  - 2.3 Public Keys ..... 24
- 3 Roles, Authentication and Services ..... 24
  - 3.1 Assumption of Roles ..... 24
  - 3.2 Authentication Method ..... 25
  - 3.3 Services ..... 26
- 4 Self-tests ..... 32
- 5 Physical Security Policy ..... 34
- 6 Operational Environment ..... 36
- 7 Mitigation of Other Attacks Policy ..... 37
- 8 Security Rules and Guidance ..... 37
- 9 References and Definitions ..... 37

## Tables

Table 1 – PTP 700 Hardware Configurations..... 5

Table 2 – Ports and Interfaces ..... 12

Table 3 – Security Level of Security Requirements ..... 14

Table 4 – Approved and CAVP Validated Cryptographic Functions..... 16

Table 5 – Protocols Allowed in FIPS Mode ..... 20

Table 6 – Non-Approved Algorithms Allowed in FIPS Mode..... 21

Table 7 – Non-Approved Algorithms with No Security Claimed [IG 1.23] ..... 21

Table 8 – Critical Security Parameters (CSPs)..... 21

Table 9 – Public Keys..... 24

Table 10 – Roles Description ..... 25

Table 11 – Password Strength..... 26

Table 12 – Authenticated Services ..... 26

Table 13 – Unauthenticated Services ..... 28

Table 14 – CSP Access Rights within Authenticated Services ..... 29

Table 15 – CSP Access Rights within Unauthenticated Services ..... 30

Table 16 – Power Up Self-Tests..... 32

Table 17 – Conditional Self-Tests ..... 33

Table 18 – Critical Function Self-Tests ..... 33

Table 19 – References ..... 37

Table 20 – Acronyms and Definitions..... 38

## Figures

Figure 1 – PTP 700 Connectorized Hardware Variant – Front and Back (White)..... 8

Figure 2 – PTP 700 Connectorized+Integrated Hardware Variant–Back and Front (White)..... 9

Figure 3 – PTP 700 Connectorized Hardware Variant–Back and Front (Green)..... 10

Figure 4 – PTP 700 Connectorized+Integrated Hardware Variant–Back and Front (Desert Tan) ..... 11

Figure 5 – Location of Ports and Interfaces on the Connectorized Platform Variant..... 13

Figure 6 – Location of Ports and Interfaces on the Connectorized+Integrated Platform Variant ..... 13

Figure 7 – Indication of FIPS-Approved Mode ..... 15

Figure 8 – Tamper-Evident Seal Locations on a White Connectorized+Integrated Unit..... 34

Figure 9 – Tamper-Evident Seal Locations on a White Connectorized Unit ..... 35

Figure 10 – Tamper-Evident Seal Locations on a Tan Connectorized+Integrated Unit..... 35

Figure 11 – Tamper-Evident Seal Locations on a Green Connectorized Unit ..... 36

Figure 12 – Example of Tampered Seals ..... 36

# 1 INTRODUCTION

## 1.1 Purpose

This document is the Security Policy for the Cambium Networks PTP 700 Point to Point Wireless Ethernet Bridge module, hereafter denoted as the “Module” or PTP 700. PTP 700 meets the requirements for a Cryptographic Module validated to FIPS 140-2 at Level 2.

## 1.2 Supported Hardware Variants

PTP 700 is available in 16 different variants as detailed in Table 1.

**Table 1 – PTP 700 Hardware Configurations**

Platform Variant	Region	Color	Capacity Tier	Part Number
Connectorized	Global	White	Full	C045070B003A, C045070B003B
			Lite	C045070B009A, C045070B009B
		Green	Full	C045070B034A
		Desert Tan	Full	C045070B039A
Connectorized + Integrated	Global	White	Full	C045070B004A
			Lite	C045070B010A
		Green	Full	C045070B038A
		Desert Tan	Full	C045070B040A
	FCC	White	Full	C045070B002A
			Lite	C045070B008A
	EU	White	Full	C045070B006A
			Lite	C045070B012A
IC	White	Full	C045070B026A	
		Lite	C045070B028A	

## 1.3 Supported Firmware Versions

PTP 700 supports firmware version 700-02-65-FIPS.

## 1.4 Module Description

PTP 700 is deployed to create a point-to-point wireless bridge joining two Ethernet networks, or a point-to-multipoint wireless bridge joining between two and nine Ethernet networks. The Module 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. Variants of the module are available with different physical format, regulatory compliance, capacity, and color.

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.

PTP 700 is available in four variants for regulatory compliance:

- (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.

PTP 700 is available in two capacity tiers: The Lite variant provides 50% of the maximum data rate 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**

PTP 700 is a multi-chip standalone device, where the cryptographic boundary is the external housing of the outdoor unit (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 – Front and Back (White)



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



Figure 3 – PTP 700 Connectorized Hardware Variant–Back and Front (Green)



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



## 1.6 Ports and Interfaces

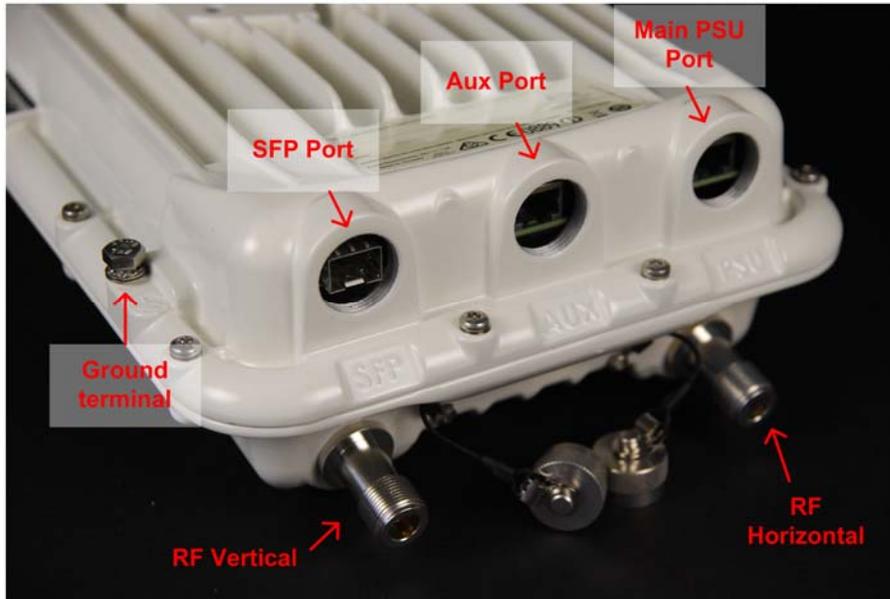
PTP 700 provides the ports and interfaces listed in Table 2

**Table 2 – Ports and Interfaces**

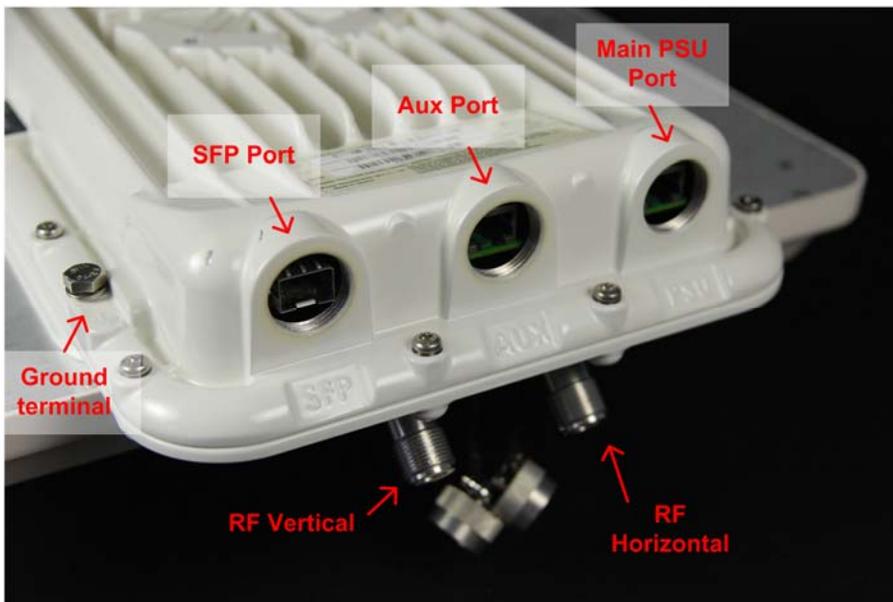
Port	Description	Logical Interface Type
Main PSU Port	Transports plaintext data in and out when configured as a logical data port. Transports control in and status out when configured as a logical management port. Provides power to the PTP 700 ODU using power over Ethernet.	Power, Control in, Data in, 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 internal 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 internal 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

PTP 700 executes a single firmware image protected by a 2048-bit DSA signature with a SHA-256 hash. The firmware includes an embedded real time operating system (RTOS). PTP 700 will not load or execute software supplied by the user or by third parties. PTP 700 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 PTP 700 are as follows:

**Table 3 – Security Level of Security Requirements**

Security Requirement	Security Level
Cryptographic Module Specification	3
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 FIPS Approved Mode

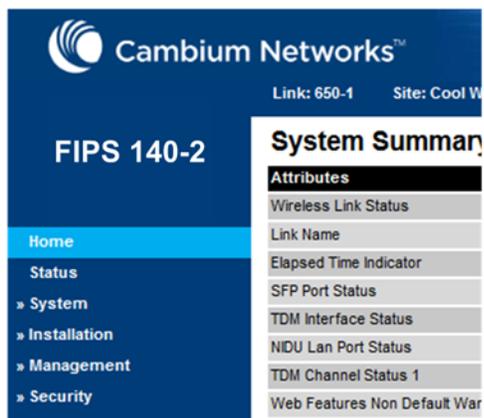
Cambium Networks provides a distinct firmware image for FIPS operation. The FIPS firmware image always operates in the FIPS Approved mode.

Any ODU in the PTP 700 series can be used in the FIPS Approved Mode, as there are no special “FIPS hardware” variants. Installing the FIPS firmware requires that the PTP 700 ODU has a license key installed which includes the FIPS license and the 128-bit or 256-bit AES license. The licenses are sold as optional upgrades. A new license key can be generated at the Cambium Networks web site, binding the purchased upgrade entitlements 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.

Any other firmware is outside of the scope of this FIPS 140-2 validation.

**Figure 7 – Indication of FIPS-Approved Mode**



## 1.10 Configuration and Operation States

### Configuration State

A PTP 700 unit is in the Configuration state while it is being configured for secure operation using approved algorithms.

The Configuration state is indicated by the presence of the Secure Mode Alarm displayed in the web-based management interface.

The configuration steps to configure the PTP 700 for secure operation are as follows:

- The Key of Keys is configured
- The DBRG Entropy is configured
- The HTTPS/TLS management interface is configured and enabled, with private key and public key certificate installed.
- The HTTP management interface is disabled
- Web-interface passwords for enabled accounts are not less than eight characters
- The wireless link is encrypted using either:
  - TLS-RSA, with user-provided public key, device certificate and root CA installed, or
  - TLS-PSK, with pre-shared key installed

## Operation State

A PTP 700 unit is in the Operation state once it has been correctly configured for secure operation using approved algorithms, as listed above.

The Operation state is indicated when the Secure Mode Alarm is absent in the web-based management interface.

The web interface and wireless interface are secure when the PTP 700 is in the Operation state.

## 2 CRYPTOGRAPHIC FUNCTIONALITY

### 2.1 Cryptographic Functions

PTP 700 implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below. Any algorithm variants not identified in the Security Policy but listed in the CAVP certificate were tested but not used.

**Table 4 – Approved and CAVP Validated Cryptographic Functions**

Algorithm	Implementation	Description	Cert #
AES	Helion Fast AES Core IP 120918	[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. *192 key size was tested but not used	AES 2594
AES	PTP700-OpenSSL 01.00	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB, CBC Key sizes: 128, 256 bits Mode: CFB 128 Key size: 128 bits Used for: DRBG, CSP protection, SNMPv3 data confidentiality or privacy protection as per RFC 3826	AES 5648

Algorithm	Implementation	Description	Cert #
AES	PTP700- MatrixSSL 01.00	[FIPS 197, SP 800-38A] Functions: Encryption, Decryption Modes: ECB*, CBC Key sizes: 128, 256 bits Used for: TLS tunnel using HTTPS and EAP-TLS. *ECB is tested but not used.	AES 5647
CKG	PTP700- MatrixSSL 01.00	[SP 800-133] Functions: Symmetric Key Generation Used for: <ul style="list-style-type: none"> <li>• TLS server random generation in HTTPS.</li> <li>• TLS client and server random generation, TLS pre-master secret in EAP-TLS.</li> <li>• Random EAP REQ/RESP message ID in EAP-TLS.</li> <li>• HTTPS web cookie.</li> </ul> Uses: NIST_CTR_DRBG	Vendor Affirmed
DRBG	NIST_CTR_DRBG 20070927	[SP 800-90A] Functions: CTR DRBG Security Strength: 128 bits Used in Cryptographic Key Generation. Uses: OpenSSL AES. Note: All entropy is loaded into the module. There is no assurance of the minimum strength of generated keys and the strength of these keys are modified by available entropy.	DRBG 2279
DSA	PTP700-OpenSSL 01.00	[FIPS 186-4] Functions: Signature Verification Key sizes: 2048 bits (with SHA-256). Used for: Signature verification of replacement firmware images and license keys.	DSA 1448
KTS	PTP700- MatrixSSL 01.00	[IG D.9] AES-CBC: 128, 256 bits HMAC: HMAC-SHA1, HMAC-SHA256. Used for: HTTPS updating for CSPs when the management station is not directly connected.	AES 5647 and HMAC 3761

Algorithm	Implementation	Description	Cert #
HMAC	PTP700-OpenSSL 01.00	[FIPS 198-1] Functions: HMAC generation, verification SHA sizes: HMAC-SHA1, HMAC-SHA256. Used for: <ul style="list-style-type: none"> <li>• SNMPv3 KDF (HMAC-SHA1)</li> <li>• HTTP and HTTPS web cookie (HMAC-SHA256)</li> <li>• SNMPv3 authentication (HMAC-SHA1)</li> </ul>	HMAC 3762
HMAC	PTP700- MatrixSSL 01.00	[FIPS 198-1] Functions: HMAC generation, verification SHA sizes: HMAC-SHA1, HMAC-SHA256, HMAC-SHA384 Used for HTTPS: <ul style="list-style-type: none"> <li>• TLS PRF in TLS v1.1 (HMAC-SHA1)</li> <li>• TLS PRF for TLS v1.2 (HMAC-SHA256)</li> <li>• HMAC for TLS v1.1/1.2 (HMAC-SHA1, 256)</li> </ul> Used for EAP-TLS: <ul style="list-style-type: none"> <li>• TLS PRF for TLS v1.2 (HMAC-SHA256, 384)</li> <li>• HMAC for TLS v1.2 (HMAC-SHA256, 384)</li> </ul>	HMAC 3761
SHS	PTP700-OpenSSL 01.00	[FIPS 180-4] Functions: Generation, verification SHA sizes: SHA-1, SHA-256 Used for: <ul style="list-style-type: none"> <li>• Digital thumbprint generation during data entry of CSPs (SHA-1)</li> <li>• SNTP server authentication (SHA-1)</li> <li>• SNMPv3 KDF (SHA-1)</li> <li>• User password storage (SHA-256)</li> <li>• DSA (SHA-256)</li> <li>• HMAC-SHA1 (SHA-1)</li> <li>• HMAC-SHA256 (SHA-256)</li> </ul>	SHA 4529

Algorithm	Implementation	Description	Cert #
SHS	PTP700- MatrixSSL 01.00	[FIPS 180-4] Functions: Generation, verification SHA sizes: SHA-1, SHA-256, SHA-384, SHA-512* Used for: <ul style="list-style-type: none"> <li>• RSA certificate signature verification (SHA-256)</li> <li>• RSA signature generation and verification for TLS Certificate Verify message (SHA-256)</li> <li>• HMAC-SHA1 (SHA-1)</li> <li>• HMAC-SHA256 (SHA-256)</li> <li>• HMAC-SHA384 (SHA-384)</li> </ul> *SHA-512 tested but not used.	SHA 4528
SNMP KDF	Net-SNMP 5.7.1	[SP 800-135] Functions: Key Derivation Function for localized passwords.	CVL 2041
TLS KDF	PTP700- MatrixSSL 01.00	[SP 800-135] Functions: Key Derivation Function TLS 1.1 and TLS 1.2	CVL 2040
RSA	PTP700- MatrixSSL 01.00	[PKCS #1 v2.2, PKCS #1 v1.5] Functions: Signature generation, signature verification Key size: 2048-bit SHA size: SHA-256.	RSA 3038

**Table 5 – Protocols Allowed in FIPS Mode**

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

Protocol	Description
<p>TLS</p>	<p>[IG D.8 and SP 800-135]</p> <p>Cipher Suites, HTTPS/TLS web interface, TLS 1.1/1.2</p> <ul style="list-style-type: none"> <li>• TLS_RSA_WITH_AES_128_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA</li> <li>• TLS_RSA_WITH_AES_128_CBC_SHA256</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA256</li> </ul> <p>Cipher suites, no wireless security, TLS 1.2</p> <ul style="list-style-type: none"> <li>• *TLS_PSK_WITH_NULL_SHA</li> </ul> <p>Cipher suites, wireless security with TLS-RSA, TLS 1.2</p> <ul style="list-style-type: none"> <li>• *SSL_RSA_WITH_NULL_SHA</li> <li>• TLS_RSA_WITH_AES_128_CBC_SHA256</li> <li>• TLS_RSA_WITH_AES_256_CBC_SHA256</li> </ul> <p>Cipher suites, wireless security with TLS-PSK, TLS 1.2</p> <ul style="list-style-type: none"> <li>• TLS_PSK_WITH_AES_128_CBC_SHA256</li> <li>• TLS_PSK_WITH_AES_256_CBC_SHA384</li> </ul> <p>TLS v1.1 KDF uses HMAC-SHA-1 and MD5.</p> <p>TLS v1.2 KDF uses HMAC-SHA-256 and HMAC-SHA-384.</p> <p>TLS v1.1 Message uses HMAC-SHA-1.</p> <p>TLS v1.2 Message uses HMAC-SHA-256 and HMAC-SHA-384.</p> <p>*Note: Cipher suites TLS_PSK_WITH_NULL_SHA and SSL_RSA_WITH_NULL_SHA are used only in the Configuration state. These cipher suites are not available after the PTP 700 is configured for secure operation in the Operation state.</p> <p>Note: SSL_RSA_WITH_NULL_SHA is always used with TLS v1.2, and the “SSL” in the label simply reflects the early point in the evolution of SSL/TLS when this cipher suite was defined.</p>
<p>SNMPv3</p>	<p>[IG D.8 and SP 800-135]</p> <p>Corresponding FIPS Algorithms: HMAC-SHA-256 (Cert. #3762), SHS (Cert. #4529), AES (Cert. #5648)</p>

**Table 6 – Non-Approved Algorithms Allowed in FIPS Mode**

Algorithm	Description
RSA	Key transfer in TLS with a 2048-bit modulus. Key establishment methodology provides 112 bits of encryption strength.
MD5	Allowed only for use in TLS 1.1

**Table 7 – Non-Approved Algorithms with No Security Claimed [IG 1.23]**

Algorithm	Description
DES (no security claimed)	Used with data files for field diagnostics, and configuration save and restore. The data files do not contain CSPs.

## 2.2 Critical Security Parameters

All CSPs used by the PTP 700 are described in this section. All usage of these CSPs (including all CSP lifecycle states) is described in the services detailed in Section 4.

**Table 8 – Critical Security Parameters (CSPs)**

CSP	Description / Usage
Key of Keys	<p>The Key of Keys is an operator-configured 128-bit or 256-bit AES key stored unencrypted in a dedicated non-volatile memory area.</p> <p>The Key of Keys is used to encrypt the remaining CSPs as they are written to non-volatile storage in the ODU, and to decrypt these same CSPs as they are read from non-volatile storage in the ODU.</p> <p>The Key of Keys must be generated by a FIPS-approved algorithm outside the PTP 700 unit.</p>
DRBG entropy	<p>DRBG entropy is an operator-configured 512-bit key used as an entropy source in the TLS stack and other random processes.</p> <p>The DRBG entropy must be generated by a FIPS-approved algorithm outside the PTP 700 unit. DRBG entropy input into PTP 700 must have a minimum of 512 bits of entropy.</p>
RSA private key for HTTPS interface	<p>The operator-configured RSA private key for HTTPS is used in RSA-2048 by the HTTPS/TLS server of the web-based management interface. PTP 700 supports the 2048-bit key size for TLS certificates and private key.</p> <p>Validity of the private key is checked by performing a modulus check on private and associated public certificate.</p>

CSP	Description / Usage
	<p>The TLS private key must be generated by a FIPS-approved algorithm outside the PTP 700 unit.</p>
<p>RSA private key for wireless encryption</p>	<p>The operator-configured RSA private key wireless encryption is used in RSA-2048 by wireless encryption when the TLS-RSA option has been selected. PTP 700 supports the 2048-bit key size for TLS certificates and private key.</p> <p>Validity of the private key is checked by performing a modulus check on private and associated public certificate.</p> <p>The TLS private key must be generated by a FIPS-approved algorithm outside the PTP 700 unit.</p>
<p>Wireless encryption pre-shared key</p>	<p>The operator-configured 128-bit or 256-bit pre-shared key (PSK) is used in the PSK option for wireless encryption key as the pre-master secret in the standard TLS conversation for wireless encryption.</p> <p>The TLS private key must be generated by a FIPS-approved algorithm outside the PTP 700 unit.</p>
<p>Localized authentication and privacy keys for SNMPv3</p>	<p>Localized authentication and privacy keys are used with HMAC-SHA1 and AES-256 respectively in the SNMPv3 interface. Each account (up to ten accounts) has different keys.</p> <p>Each localized key is derived from an operator-configured passphrase using the standard SNMPv3 KDF. The passphrases are not stored in non-volatile storage.</p>
<p>Authentication keys for SNTP</p>	<p>The operator-configured authentication keys are used with SHA-1 to authenticate time messages from NTP servers. Up to two servers (and thus two keys) can be configured.</p>
<p>HMAC session key</p>	<p>The HMAC session key is used by the authentication process to sign and verify HMAC signed web authentication cookies. The HMAC session key is generated using the FIPS approved DRBG. The session key is overwritten every time a user successfully authenticates to the PTP 700.</p> <p>The authentication cookie is used by PTP 700 to create and store session information. Each time a webpage is clicked by an authenticated user, the session cookie is replayed by the browser to PTP 700. After receiving the cookie the ODU 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 PTP 700 unit otherwise the user is forced to re-authenticate.</p>
<p>TLS master secret and session keys for HTTPS</p>	<p>PTP 700 generates the TLS master secret from the TLS pre-master secret using the standard TLS PRF. TLS session keys are generated by the standard TLS PRF using the TLS master secret and server and client random.</p> <p>HTTPS/TLS is used for authentication and privacy when transporting CSPs from the user's browser to the PTP 700 ODU. The server random is generated using the approved DRBG. The client random is generated by the user's browser.</p> <p>AES sizes: 128-bit, 256-bit.</p> <p>HMAC sizes: HMAC-SHA-1, HMAC-SHA-256</p>

CSP	Description / Usage
TLS master secret and session keys for EAP-TLS	<p>PTP 700 generates the TLS master secret from the TLS pre-master secret using the standard TLS PRF. TLS session keys are generated by the standard TLS PRF using the TLS master secret and server and client random.</p> <p>Encryption is used in EAP-TLS for secure authentication of the remote wireless device. The server random and client random are generated by the Master ODU and Slave ODU respectively using the approved DRBG.</p> <p>The EAP-TLS master secret is used to export keying material for stream cipher wireless encryption.</p> <p>AES sizes: 128-bit, 256-bit.</p> <p>HMAC sizes: HMAC-SHA-256, HMAC-SHA-384.</p>
Passphrases for SNMPv3 authentication and privacy	<p>The user-configured SNMPv3 security passphrases for authentication and (optionally) privacy are associated with up to ten SNMP user accounts. The passphrases are used to derive localized keys with the standard SNMPv3 KDF. The passphrases are not stored in non-volatile storage.</p>
DRBG internal state	<p>The DRBG state (V and Key) are stored in volatile memory.</p> <p>The DRBG internal state is updated after use.</p>
Passwords	<p>PTP 700 has ten configurable web-based user accounts. Each user account has an associated password.</p> <p>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.</p> <p>An unauthenticated user can also zeroize CSP's through the unauthenticated services Zeroize CSPs and Reset ALL Configuration described in Table 13.</p>

## 2.3 Public Keys

Table 9 – Public Keys

Key	Description / Usage
TLS public certificate for HTTPS	Public component of a 2048-bit RSA key pair with the TLS private key. The certificate must be signed using SHA-256. 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.
TLS public certificate for EAP-TLS device authentication	Public component of a 2048-bit RSA key pair with the TLS private key. The certificate must be signed using SHA-256. 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.
TLS public certificate for EAP-TLS from remote device.	Public component of a 2048-bit RSA key pair, received from a remote PTP 700 device using the TLS protocol. The certificate must be signed using RSA with SHA-256. The longevity of the key is encoded in the X509 certificate expiry time. The public key of the remote device is not stored in non-volatile storage.
Root CA public certificate for device authentication	Public component of a 2048-bit RSA key pair in a self-signed CA certificate. The public key is used to verify the public key certificate provided by the remote device. 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.
License key DSA public key	DSA 2048-bit public key (p, q, g and y vectors) used to authenticate License Keys. 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

PTP 700 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. PTP 700 enforces the separation of roles using identity-based authentication, where each user is assigned one of the roles. Table 10 lists the operator roles supported.

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].

PTP 700 does not support a maintenance role.

PTP 700 does not support concurrent operators. An authenticated operator may be logged out automatically following a configurable period of inactivity. A new operator seeking to log in will automatically log out an existing operator with lower permissions.

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 PTP 700 unit. 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 10 – 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	Password
System Administrator	A system administrator with read/write access to general configuration but no access to cryptographic configuration.	Identity-based	Password
Read Only	An operator with read-only access to general configuration but no access to cryptographic configuration.	Identity-based	Password
Firmware Update	An operator responsible for updating the firmware on the PTP 700.	Role-based	Digital signature

### 3.2 Authentication Method

#### Password Authentication

The default minimum password length is eight (8) characters. The SO can change minimum password length between eight (8) and thirty-one (31) characters inclusive.

Passwords can contain:

- (a) Lowercase letter
- (b) Uppercase letter
- (c) Decimal numerals
- (d) Special characters: !"#%&'()\*+,-./:;<=>?@[\_\]^\_`{|}~

The character set contains 94 characters.

A user account is locked following three (3) unsuccessful authentication attempts.

The minimum number of unique passwords is  $94^8 = 6.10 \times 10^{15}$ .

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 11 – Password Strength**

Requirement	Strength
1 in $10^6$ at any attempt	Password strength is 1 in $6.10 \times 10^{15}$
1 in $10^5$ in any minute	Password strength is 1 in $2.03 \times 10^{14}$

### 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  $1/2^{112}$ . Approximately four (4) firmware update attempts can be performed in a one minute period. The probability of a random attempt succeeding in a one minute period is  $4 \times 1/2^{112}$ .

### 3.3 Services

All services implemented by PTP 700 are listed in the tables below. Each service description also describes all usage of CSPs by the service.

**Table 12 – Authenticated Services**

Service	Role	Purpose
Zeroize 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.
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.
Update password	SO, SA, RO	Allows a user of the web-based interface to update his or her own password.

Service	Role	Purpose
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.
Logout	SO, SA, RO	Invalidates any previously HMAC authenticated cookies by regenerating the HMAC session key
Reboot by command	SO, SA	Allows a SO or SA user to reboot the PTP 700 by means of a command in the web-based interface.
Update firmware	SO, SA, FU	Allows a SO, SA or FU operator to update the operational firmware in the PTP 700. CSPs are zeroized if standard firmware is updated to FIPS firmware, or FIPS firmware is updated to standard firmware.
General configuration	SO, SA	Allows a SO or SA operator to configure wireless and networking operation of the PTP 700, excluding configuration of CSPs. This includes SNMPv3.
Configure CSPs	SO	Allows a SO user to install key of keys and DRBG entropy.
Configure HTTPS	SO	Allows a SO user to install TLS private keys and TLS public key certificate for HTTPS.
Configure wireless link encryption	SO	Allows a SO operator to install private keys, public key certificates and pre-shared keys for encryption at the wireless port.
Configure authenticated NTP	SO	Allows a SO operator to install authentication keys for NTP.
Configure SNMPv3	SO	Allows a SO user to install authentication and privacy keys for SNMPv3.

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 13 – Unauthenticated Services**

Service	Description
Reboot by power cycle	PTP 700 automatically reboots on a power cycle
Power-on self-test	PTP 700 executes a suite of cryptographic self-tests on power-up.
View Status	Users can view status of PTP 700 unit in the web-based (HTTP) interface, and via the SNMP interface
Network configuration using SNMP v1 or SNMP v2c.	Some aspects of wireless and networking operation can be configured via the SNMP interface. CSPs are not accessible via this interface.
Zeroize CSPs	An unauthenticated operator can zeroize CSPs by booting the PTP 700 unit 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 PTP 700 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 14 – CSP Access Rights within Authenticated Services**

Z = Zeroize, I = Input, S = Store, U = Use, O = Output.

Service	Passwords	Key of Keys	DRBG entropy	DRBG internal state	RSA private key for HTTPS	TLS key set HTTPS	HMAC session key	RSA private key for wireless	Wireless PSK	TLS key set wireless	Wireless session keys	SNTP authentication keys	SNMPv3 passphrases	Localized SNMPv3 keys
Zeroise CSPs	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Create and administer user accounts	I, S	U												
Update password	I, S	U												
Login	U	U					G							
Logout														
Reboot by command				Z		Z	Z			Z	Z		Z	
Update firmware (see Note)	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
General configuration			U	U	U	U	U							U
Configure CSPs		I, S	I, S	U	U	U	U							
Configure HTTPS		U	U	U	I, S	G	U							
Configure wireless encryption		U	U	U	U	U	U	I, S	I, S	G	G			

Service	Passwords	Key of Keys	DRBG entropy	DRBG internal state	RSA private key for HTTPS	TLS key set HTTPS	HMAC session key	RSA private key for wireless	Wireless PSK	TLS key set wireless	Wireless session keys	SNTP authentication keys	SNMPv3 passphrases	Localized SNMPv3 keys
Configure authenticated NTP		U	U	U	U	U	U					I, S		
Configure SNMPv3		U	U	U	U	U	U						I	S

**Table 15 – CSP Access Rights within Unauthenticated Services**

Service	Passwords	Key of Keys	DRBG entropy	DRBG internal state	RSA private key for HTTPS	TLS key set HTTPS	HMAC session key	RSA private key for wireless	Wireless PSK	TLS key set wireless	Wireless session keys	SNTP authentication keys	SNMPv3 passphrases	Localized SNMPv3 keys
Reboot by power cycle				Z		Z	Z			Z	Z		Z	
Power-on self-test			U	U										
View Status							U							
Network configuration using SNMP v1 or SNMP v2c.														
Zeroize CSPs	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Reset network configuration														

Service	Passwords	Key of Keys	DRBG entropy	DRBG internal state	RSA private key for HTTPS	TLS key set HTTPS	HMAC session key	RSA private key for wireless	Wireless PSK	TLS key set wireless	Wireless session keys	SNTP authentication keys	SNMPv3 passphrases	Localized SNMPv3 keys
Reset all configuration data	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Reboot from recovery				Z		Z	Z			Z	Z		Z	

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

## 4 SELF-TESTS

Each time the PTP 700 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 PTP 700.

On power up or reset, PTP 700 performs the self-tests described in Table 16 below. All KATs must be completed successfully prior to any other use of cryptography by PTP 700. If one of the KATs fails, the unit reboots and repeats the self-tests.

Data output ports are disabled during self-tests.

The Firmware Integrity Test sends the PTP 700 into recovery mode if it fails.

**Table 16 – Power Up Self-Tests**

Test Target	Implementation	Description
Firmware Integrity		32 bit CRC performed over all code in EEPROM. DSA-2048 with SHA-256 over boot code image.
AES	Helion FPGA	KATs: Encryption, Decryption Modes: CFB128 Key sizes: 128 bits
AES	OpenSSL	KATs: Encryption, Decryption Modes: ECB, CBC, CFB128 Key sizes: 128 bits
AES	MatrixSSL	KATs: Encryption, Decryption Modes: ECB, CBC Key sizes: 128 bits
DRBG	NIST_CTR_DRBG	KATs: CTR DRBG Security Strengths: 128 bits This includes DRBG health tests as described in SP800-90A, Section 11.3.
DSA	OpenSSL	KAT: Signature Verification Key sizes: 2048 bits
HMAC	OpenSSL	KATs: Generation, Verification SHA sizes: HMAC-SHA1, HMAC-SHA256
HMAC	MatrixSSL	KATs: Generation, Verification SHA sizes: HMAC-SHA1, HMAC-SHA256, HMAC-SHA384
RSA	MatrixSSL	KATs: RSA Signature Generation, RSA Signature Verification. Key sizes: 2048 bits

Test Target	Implementation	Description
SHA	OpenSSL	KATs: SHA-1, SHA-256
SHA	MatrixSSL	KATs: SHA-1, SHA-256, SHA-384, SHA-512
SNMP KDF	Net-SNMP	KAT: SNMPv3 KDF
TLS KDF	MatrixSSL	KATs: TLS 1.1, TLS 1.2 KDF's

RSA is used only as part of HTTPS and wireless TLS.

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 or DSA 2048)

**Table 17 – Conditional Self-Tests**

Test Target	Description
DRBG	DRBG Continuous Test performed when a random value is requested from the DRBG.
Firmware Load	DSA 2048 signature verification performed when firmware is loaded.

PTP 700 does not have a NDRBG.

**Table 18 – Critical Function Self-Tests**

Test Target	Description
CSP Integrity Check (CRC-32)	Performed when reading CSPs from non-volatile storage.

## 5 PHYSICAL SECURITY POLICY

PTP 700 is a multi-chip standalone cryptographic module and includes the following physical security mechanisms:

- Production-grade components and production-grade opaque enclosure with two (2) tamper evident seals applied during the manufacturing process.
- Protected, opaque vent.

### Tamper-Evident Seals

The tamper evident seals on the PTP 700 enclosure must be checked every 30 days. If damage to the seal or the enclosure is observed, the unit should be removed from service and inspected more closely. The correct location of the tamper evident seals is shown in Figure 8 through Figure 11.

**Figure 8 – Tamper-Evident Seal Locations on a White Connectorized+Integrated Unit**



Figure 9 – Tamper-Evident Seal Locations on a White Connectorized Unit



Figure 10 – Tamper-Evident Seal Locations on a Tan Connectorized+Integrated Unit



**Figure 11 – Tamper-Evident Seal Locations on a Green Connectorized Unit**



## Inspection of the Tamper-Evident Seals

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

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

**Figure 12 – Example of Tampered Seals**



## 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

PTP 700 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 PTP 700 unit. 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 PTP 700 for transmission at the wireless ports. Similarly, encrypted data received at the wireless ports is decrypted within the PTP 700 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

PTP 700 zeroizes CSPs on transition into the FIPS Approved Mode. As a consequence, the initial security configuration (Configuration State) will be completed using an unprotected HTTP session. Security Officers must ensure that the initial security configuration of the PTP 700 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 PTP 700 can be via a LAN or other data network.

### FIPS-Approved Generation for Cryptographic Material

PTP 700 requires that the cryptographic material used must be generated outside the ODU 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

Abbreviation	Full Specification Name
[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 Rev 1.]	Recommendation for Random Number Generators Using Deterministic Random Bit Generators, January 2015.
[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
[SP800-133]	Recommendation for Cryptographic Key Generation December 2012
[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
HMAC	Hashed Message Authentication Code
KAT	Known Answer Test
KDF	Key Derivation Function

Acronym	Definition
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.



[www.cambiumnetworks.com](http://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 2018 Cambium Networks, Ltd. May be reproduced only in its original entirety [without revision].