Cambium Networks, Ltd.

PTP 700 Point to Point Wireless Ethernet Bridge

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 000v018
Date: April 16, 2025

Table of Contents

1 – General 6
1.1 Overview 6
1.2 Security Levels 6
2 – Cryptographic Module Specification 7
2.1 Description 7
2.2 Tested and Vendor Affirmed Module Version and Identification 14
2.3 Excluded Components 19
2.4 Modes of Operation 19
2.5 Algorithms 21
2.6 Security Function Implementations 24
2.7 Algorithm Specific Information 26
2.8 RBG and Entropy 27
2.9 Key Generation 28
2.10 Key Establishment 28
2.11 Industry Protocols 28
3 Cryptographic Module Interfaces 29
3.1 Ports and Interfaces 29
4 Roles, Services, and Authentication 32
4.1 Authentication Methods 32
4.2 Roles 33
4.3 Approved Services 34
4.4 Non-Approved Services 48
4.5 External Software/Firmware Loaded 48
4.6 Bypass Actions and Status 48
4.7 Cryptographic Output Actions and Status 48
4.8 Additional Information 49
5 Software/Firmware Security 50
5.1 Integrity Techniques 50
5.2 Initiate on Demand 50
5.3 Open-Source Parameters 50
6 Operational Environment 51
6.1 Operational Environment Type and Requirements 51
7 Physical Security 52
7.1 Mechanisms and Actions Required 52
7.2 User Placed Tamper Seals 63

8 Non-Invasive Security 64
8.1 Mitigation Techniques 64
9 Sensitive Security Parameters Management 65
9.1 Storage Areas 65
9.2 SSP Input-Output Methods 65
9.3 SSP Zeroization Methods 65
9.4 SSPs 66
10 Self-Tests 76
10.1 Pre-Operational Self-Tests 76
10.2 Conditional Self-Tests 78
10.3 Periodic Self-Test Information 82
10.4 Error States 83
11 Life-Cycle Assurance 84
11.1 Installation, Initialization, and Startup Procedures 84
11.2 Administrator Guidance 84
11.3 Non-Administrator Guidance 85
11.4 Design and Rules 85
Rules of Operation 85
11.5 End of Life 85
12 Mitigation of Other Attacks 86
References and Definitions 86

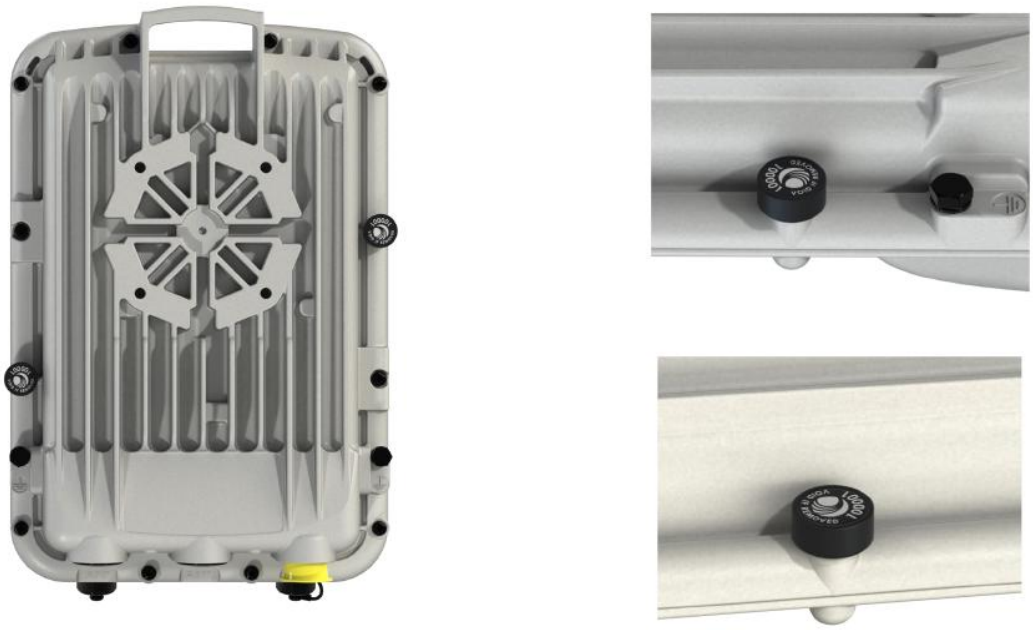
List of Tables

Table 1: Security Levels 6
Table 2 – Executable Code Sets 9
Table 3: Tested Module Identification – Hardware 19
Table 4: Modes List and Description 19
Table 5: Approved Algorithms 23
Table 6: Vendor-Affirmed Algorithms 23
Table 7: Non-Approved, Allowed Algorithms with No Security Claimed 23
Table 8: Security Function Implementations 26
Table 9: Ports and Interfaces 29
Table 10: Authentication Methods 32
Table 11: Roles 33
Table 12: Approved Services 47
Table 13: Mechanisms and Actions Required 52
Table 14: Storage Areas 65
Table 15: SSP Input-Output Methods 65
Table 16: SSP Zeroization Methods 65
Table 17: SSP Table 1 70
Table 18: SSP Table 2 75
Table 19: Pre-Operational Self-Tests 77
Table 20: Conditional Self-Tests 80
Table 21: Pre-Operational Periodic Information 82
Table 22: Conditional Periodic Information 83
Table 23: Error States 83
Table 24 – References 86
Table 25 – Acronyms and Definitions 87

List of Figures

Figure 1 – PTP 45700 Connectorized Hardware Variant – Front and Back (White) 10
Figure 2 – PTP 45700 Connectorized Hardware Variant – Front and Back (Green) 10
Figure 3 – PTP 45700 Connectorized Hardware Variant – Front and Back (Tan) 11
Figure 4 – PTP 45700 Connectorized+Integrated Hardware Variant–Back and Front (Green) 11
Figure 5 – PTP 45700 Beam Steering Hardware Variant–Back and Front (White) 12
Figure 6 – PTP 78700 Connectorized Hardware Variant–Back and Front (White) 12
Figure 7 – PTP 78700 Integrated Hardware Variant–Back and Front (Tan) 13
Figure 8 – Indication of the firmware image 20
Figure 9 – Global Indication of Approved Mode of operation 20
Figure 10 – Physical Ports and Interfaces on the PTP 45700 Connectorized Variant 30
Figure 11 – Physical Ports and Interfaces on the PTP 45700 Connectorized+Integrated Variant 30
Figure 12 – Physical Ports and Interfaces on the PTP 78700 Variant 31

Figure 13 – Tamper-Evident Barrel Locations on a Connectorized PTP 45700 Unit (White/Desert Tan/Green)



.....53
Figure 14 – Tamper-Evident Barrel Locations on a Connectorized+Integrated PTP 45700 Unit (White/Desert Tan/Green).....55
Figure 15 - Tamper-Evident Barrel Locations on a Beam Steering PTP 45700 Unit (White/Desert Tan/Green).....57
Figure 16 – Tamper-Evident Barrel Locations on a Connectorized PTP 78700 Unit (White/Desert Tan/Green).....59
Figure 17 – Tamper-Evident Barrel Locations on an Integrated PTP 78700 Unit (White/Desert Tan/Green).....61

1 – General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version700-04-10-FIPS of the PTP 700 Point-to-Point Wireless Ethernet Bridge. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 2 module.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are provided in the table below:

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	3
5	Software/Firmware security	2
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	2
10	Self-tests	2
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 – Cryptographic Module Specification

2.1 Description

Purpose and Use:

This Cambium Networks PTP 700 module, hereafter denoted as the Module, is a fixed point-to-point wireless Ethernet bridge operating in frequency bands 4400 MHz to 5875 MHz, or 7150 MHz to 8500 MHz.

The Module is intended for use by US Federal agencies or other markets that require a FIPS 140-3 validated wireless Ethernet bridge, deployed as two units in a fixed outdoor point-to-point wireless link, bridging between two Ethernet networks, or as a fixed outdoor point-to-multipoint wireless network with a minimum of three units and a maximum of nine units bridging between multiple Ethernet networks.

The Module is intended to be used in fixed infrastructure deployment (for example between communication towers or buildings) or as a temporary deployment (for example in tactical military or disaster recovery applications).

Module Type: Hardware

Module Embodiment: Multi-Chip Standalone

Module Characteristics:

PTP 700 is available in two frequency variants:

- PTP 45700
- PTP 78700

The PTP 45700 variant 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 PTP 78700 variant operates in licensed frequency bands between 7125 MHz and 8500 MHz, in channel bandwidths up to 45 MHz, providing aggregate data rates up to 503 Mbit/s.

The Module transmits and receives Ethernet frames at wired interfaces 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 45700 has three physical formats or platform variants as follows:

- Connectorized: Uses an external antenna.
- Connectorized+Integrated: Configurable to use a separately mounted external antenna or an integrated 22 dBi flat plate antenna.

- Beam Steering: Uses an electrically steerable integrated 21 dBi flat plate antenna to provide automatic alignment during installation.

PTP 78700 has two physical formats or platform variants as follows:

- Connectorized: Uses an external antenna.
- Integrated: Uses an integrated 26 dBi flat plate antenna

Color variants

The PTP 45700 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 colored paint finish, and the white units have a white powder-coat finish.
- The connectors and fixings in the white PTP 45700 units have a reflective plated finish, and the green and tan units have connectors and fixings with a black surface finish.

The PTP 78700 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 colored paint finish, and the white units have a powder-coat finish.

Modules were initially available with a Chemical Agent Resistant Coating (CARC) finish. Current production of Green and Tan modules uses a standard painted finish.

Capacity variants

Some of the PTP 45700 and PTP 78700 platform variants are available in a choice of two capacity variants:

- Full
- Lite 150

The Lite 150 variant provides the same set of features and performance as the Full variant except that:

- The maximum channel bandwidth in a Lite 150 ODU is restricted to 20 MHz
- The maximum modulation mode in a Lite 150 ODU is restricted to 64QAM 0.92.

A PTP 700 unit with the Lite 150 license can be converted to the Full license by purchase and application of an upgrade.

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 1 to Figure 7. The Module is a multi-chip standalone embodiment. The cryptographic boundary is the same as the physical perimeter, defined by the external housing of the outdoor unit (ODU).

Executable Code List

The PTP 700 cryptographic module has the following executable code set in Table 1.

Table 2 – Executable Code Sets

#	Package Name_*	Firmware Version	Integrity Test Implemented
1	Main Application	PTP 700-04-10-FIPS	CRC-32
2	Recovery	RECOVERY-02-00	CRC-32

At a power cycle or restart, the CPU automatically executes the Boot Monitor image. The Boot Monitor expands the compressed image for Recovery or Main Application, checks its integrity using CRC-32, copies the image to RAM and passes control to the loaded Recovery or Main Application image.

The Boot Monitor loads the Recovery image in the event of an integrity failure of the Main Application image, or following a short power cycle. Boot Monitor does not execute thereafter until a subsequent power cycle or restart occurs.

Recovery and Main Application are mutually exclusive and never loaded at the same time.
The Boot Loader does not implement any cryptographic functions.

The Recovery and Main Application images contain embedded programming information for a Altera Cyclone V GXC7 FPGA.

The Recovery image provides a basic web management interface with the following utilities:

- Upgrade Application image
- Erase configuration
- Zeroize CSPs
- Erase IP interface configuration
- Reboot

Recovery does not provide any cryptographic functions apart from checking the digital signature of replacement Application firmware. Recovery does not allow use of the wireless interface.

Figure 1 – PTP 45700 Connectorized Hardware Variant – Front and Back (White)

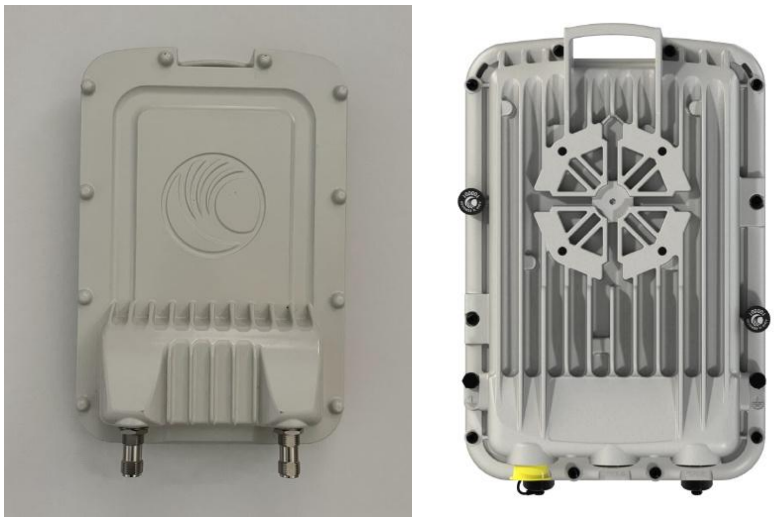


Figure 2 – PTP 45700 Connectorized Hardware Variant – Front and Back (Green)



Figure 3 – PTP 45700 Connectorized Hardware Variant – Front and Back (Tan)



Figure 4 – PTP 45700 Connectorized+Integrated Hardware Variant–Back and Front (Green)



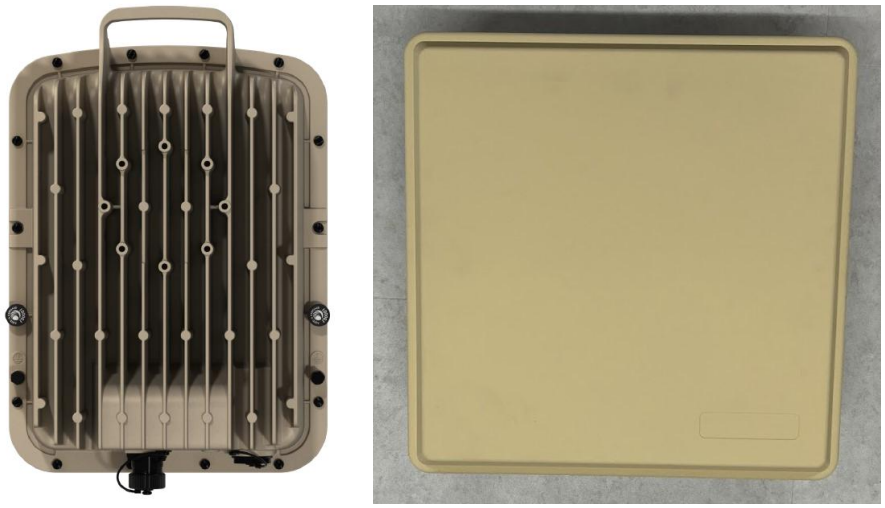
Figure 5 – PTP 45700 Beam Steering Hardware Variant–Back and Front (White)



Figure 6 – PTP 78700 Connectorized Hardware Variant–Back and Front (White)



Figure 7 – PTP 78700 Integrated Hardware Variant–Back and Front (Tan)



2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

The PTP 700 Wireless Ethernet Bridge cryptographic module is tested on the following operational environment.

All of the supported hardware platforms include the following processors:

- Texas Instruments TMS320C6657, Multicore Fixed and Floating-Point DSP
- Altera Cyclone V GXC7 FPGA

Hardware Version is indicated by the suffix in the Part Number.

Surface Finish: “Powder” indicates powder coat; “CARC” indicates spray painted finish with Chemical Agent Resistant Coating; “Non-CARC” indicates spray painted finish with conventional paint.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PTP 45700 Connectorized Models	C045070B003B, C045070B003A, C045070B003C, C045070B003D, C045070B034A, C045070B034B, C045070B034C, C045070B034D, C045070B034E, C045070B034F, C045070B039A, C045070B039B, C045070B039C, C045070B039D,	45700-04-10-FIPS	TI TMS320C6657, Altera GXC7	Connectorized, Capacity = Full/Lite 150, Frequency = 45700, Finish = Powder/CARC/Non-CARC

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
	C045070B039E, C045070B039F, C045070B044A, C045070B044B, C045070B044C, C045070B046A, C045070B046B, C045070B046C, C045070B046D, C045070B046E, C045070B046F, C045070B048A, C045070B048B, C045070B048C, C045070B048D, C045070B048E, C045070B048F			
PTP 45700 Connectorized+Integrated Models	C045070B004A, C045070B004B, C045070B004C, C045070B038A, C045070B038B, C045070B038C, C045070B038D,	45700-04-10-FIPS	TI TMS320C6657, Altera GXC7	Connectorized+Integrated, Capacity = Full/Lite 150, Frequency = 45700, Finish = Powder/CARC/Non-CARC

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
	C045070B038E, C045070B038F, C045070B040A, C045070B040B, C045070B040C, C045070B040D, C045070B040E, C045070B040F, C045070B045A, C045070B045B, C045070B045C, C045070B047A, C045070B047B, C045070B047C, C045070B047D, C045070B047E, C045070B047F, C045070B049A, C045070B049B, C045070B049C, C045070B049D, C045070B049E, C045070B049F			

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
PTP 45700 Beam Steering Models	C045070B041A, C045070B041B, C045070B041C, C045070B042A, C045070B042B, C045070B042C, C045070B043A, C045070B043B, C045070B043C	45700-04-10-FIPS	TI TMS320C6657, Altera GXC7	Beam Steer, Capacity = Full, Frequency = 45700, Finish = Powder/CARC/Non-CARC
PTP 78700 Connectorized Models/PTP 78700 Integrated Models	C070070B001A, C070070B001B, C070070B003A, C070070B003B, C070070B003C, C070070B003D, C070070B005A, C070070B005B, C070070B005C, C070070B005D, C070070B007A, C070070B007B, C070070B009A, C070070B009B, C070070B009	78700-04-10-FIPS	TI TMS320C6657, Altera GXC7	Connectorized/Integrated, Capacity = Full/Lite 150, Frequency = 78700, Finish = Powder/CARC/Non-CARC

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
	C, C070070B009D, C070070B011A, C070070B011B, C070070B011C, C070070B011D, C070070B002A, C070070B002B, C070070B004A, C070070B004B, C070070B004C, C070070B004D, C070070B006A, C070070B006B, C070070B006C, C070070B006D, C070070B008A, C070070B008B, C070070B010A, C070070B010B, C070070B010C, C070070B010D, C070070B012A, C070070B012B,			

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
	C070070B012C, C070070B012D			

Table 3: Tested Module Identification – Hardware

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

NOTE: Module has a Hardware Operational Environment.

Tested Module Identification – Hybrid Disjoint Hardware:

NOTE: Module has a Hardware Operational Environment.

Tested Operational Environments - Software, Firmware, Hybrid:

NOTE: Module has a Hardware Operational Environment.

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

NOTE: The module is not claiming any Vendor Affirmed Operational Environments.

N/A for this module.

2.3 Excluded Components

No components are excluded from the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved Mode	Approved mode of operation	Approved	See Figure 9

Table 4: Modes List and Description

Any ODU in the PTP 700 series can be used in the Approved Mode, and there are no special “FIPS hardware” variants. However, the approved mode firmware cannot be installed unless the PTP 700 ODU has a license key that 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 firmware image is indicated by the display of a white “FIPS 140-3” graphic in the navigation bar of the web-based management interface as shown in Figure 8.

The Approved mode is indicated by the display of a green “FIPS 140-3” graphic in the navigation bar of the web-based management interface as shown in Figure 9. This serves as the global indicator for the module that only supports approved services in an approved manner.

Figure 8 – Indication of the firmware image

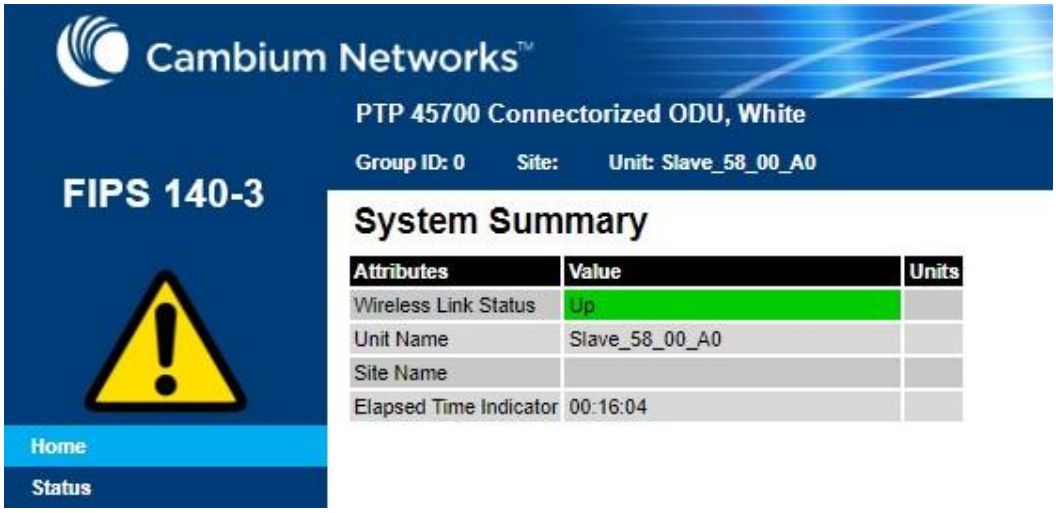
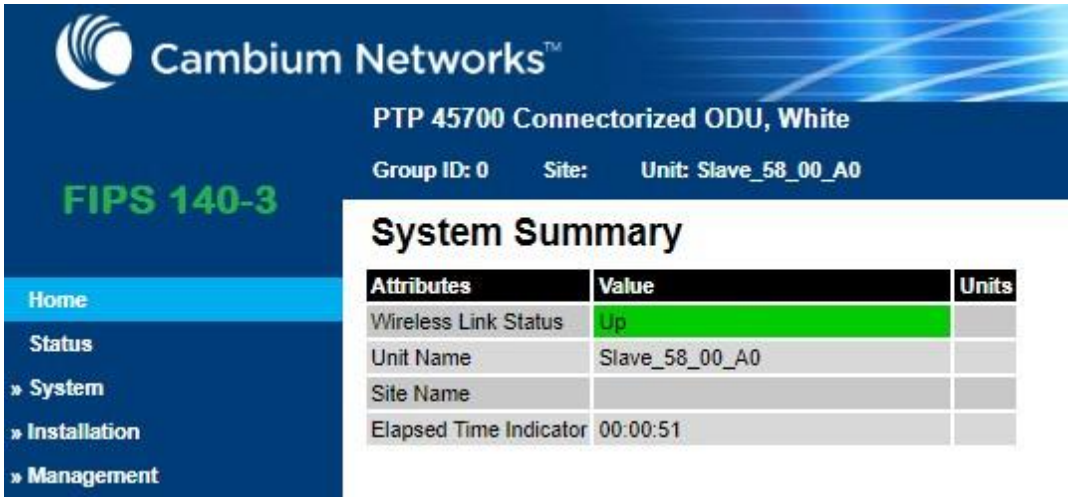


Figure 9 – Global Indication of Approved Mode of operation



2.5 Algorithms

Approved Algorithms:

The Module implements the Approved cryptographic algorithms listed the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CFB128	A4740	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
AES-CFB128	AES2594	Direction - Decrypt, Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-ECB	A4740	Direction - Decrypt, Encrypt Key Length - 128, 256	SP 800-38A
AES-GCM	A4740	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 128, 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 0-65536 Increment 8 AAD Length - AAD Length: 0-128 Increment 8	SP 800-38D
Counter DRBG	A4741	Prediction Resistance - No Supports Reseed - Yes Mode - AES-128 Derivation Function Enabled - Yes Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 1024 Nonce - Nonce: 64 Personalization String Length - Personalization String Length: 0-128 Increment 8 Returned Bits - 2048	SP 800-90A Rev. 1
DSA SigVer (FIPS186-4)	A4740	L - 1024, 2048 N - 160, 256 Hash Algorithm - SHA-1, SHA2-256	FIPS 186-4
ECDSA KeyGen (FIPS186-5)	A4740	Curve - P-256, P-384 Secret Generation Mode - testing candidates	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A4740	Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A4740	Component - No Curve - P-256, P-384 Hash Algorithm - SHA2-256, SHA2-384	FIPS 186-5

Algorithm	CAVP Cert	Properties	Reference
EDDSA SigVer	A4740	Curve - ED-25519 PreHash - No Pure - Yes	FIPS 186-5
HMAC-SHA-1	A4740	MAC - MAC: 160 Key Length - Key Length: 8-512 Increment 8	FIPS 198-1
HMAC-SHA2-256	A4740	MAC - MAC: 256 Key Length - Key Length: 8-512 Increment 8	FIPS 198-1
HMAC-SHA2-384	A4740	MAC - MAC: 384 Key Length - Key Length: 8-1024 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A4740	Domain Parameter Generation Methods - P-256, P-384 Hash Function Z - SHA2-256, SHA2-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
KDF SNMP (CVL)	A4742	Password Length - Password Length: 64, 256 Engine ID - 53616D706C65205465787420537472696E672031323334353637 38, 80004531010A829F2C	SP 800-135 Rev. 1
RSA SigGen (FIPS186-4)	A4740	Signature Type - PKCSPSS Modulo - 2048 Hash Pair - Hash Algorithm - SHA2-256 Salt Length - 32	FIPS 186-4
RSA SigVer (FIPS186-2)	A4740	Public Exponent Mode - Fixed Fixed Public Exponent - 010001 Signature Type - PKCS 1.5 Modulo - 2048 Hash Pair - Hash Algorithm - SHA2-256	FIPS 186-4
RSA SigVer (FIPS186-4)	A4740	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048 Hash Pair - Hash Algorithm - SHA2-256 Salt Length - 32 Public Exponent Mode - Fixed Fixed Public Exponent - 010001	FIPS 186-4
SHA-1	A4740	Message Length - Message Length: 160, 0-65536 Increment 8	FIPS 180-4
SHA2-256	A4740	Message Length - Message Length: 256, 0-65536 Increment 8	FIPS 180-4
SHA2-384	A4740	Message Length - Message Length: 384, 0-65536 Increment 8	FIPS 180-4
SHA2-512	A4740	Message Length - Message Length: 512, 0-65536 Increment 8	FIPS 180-4

Algorithm	CAVP Cert	Properties	Reference
TLS v1.3 KDF (CVL)	A4740	HMAC Algorithm - SHA2-256, SHA2-384 KDF Running Modes - DHE, PSK-DHE	SP 800-135 Rev. 1

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

The Module implements the Vendor Affirmed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
CKG	Symmetric: AES-256-CBC, AES-128-CFB128, AES-256-GCM, AES-256-CCM, HMAC SHA-1, HMAC SHA2-256, HMAC SHA2-384, HMAC SHA2-512: :	N/A	SP800-133rev2 Sections 4 Example 1 and IG D.H
CKG-Asym	Asymmetric: ECC P-256, ECC P-384:	N/A	SP800-133rev2 Section 4 Example 1 and IG D.H

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The module does not implement any Non-Approved, but Allowed Algorithms in the Approved Mode of Operation.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The Module implements the following Non-Approved but Allowed cryptographic Algorithm with No Security Claimed.

Name	Caveat	Use and Function
DES	No security claimed.	Obfuscation of configuration and performance data for remote customer support and obfuscation of configuration management data. Configuration data does not include SSPs.

Table 7: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

The module does not implement any Non-Approved Algorithms, Not Allowed in the Approved Mode of Operation.

N/A for this module.

2.6 Security Function Implementations

The table below shows the Security Function Implementations that the module implements:

Name	Type	Description	Properties	Algorithms
AES-CFB-WLS-D (SFI#1)	BC-UnAuth	Block cipher Decryption		AES-CFB128: (AES 2594) CFB128 128-bit, 256-bit Decryption:
AES-CFB-WLS-E (SFI#2)	BC-UnAuth	Block cipher Encryption		AES-CFB128: (AES 2594) CFB128 128-bit, 256-bit Encryption:
AES-CFB-SNMP-D(SFI#3)	BC-UnAuth	Block cipher Decryption		AES-CFB128: (A4740)
AES-CFB-SNMP-E (SFI#4)	BC-UnAuth	Block cipher Encryption		AES-CFB128: (A4740)
AES-ECB-D (SFI#5)	BC-UnAuth	Block cipher Decryption		AES-ECB: (A4740)
AES-ECB-E (SFI#6)	BC-UnAuth	Block cipher Encryption		AES-ECB: (A4740)
AES-GCM-D (SFI#7)	BC-Auth	Block cipher Decryption		AES-GCM: (A4740)
AES-GCM-E (SFI#8)	BC-Auth	Block cipher Encryption		AES-GCM: (A4740)
CKG (SFI#9)	CKG	Symmetric Key Generation	IG [D,H]:	Counter DRBG: (A4741) AES-ECB: (A4740) CKG: ()
DSA (SFI#10)	DigSig-SigVer	Digital signature verification.		DSA SigVer (FIPS186-4): (A4740) SHA2-256: (A4740) SHA-1: (A4740)
EDDSA (SFI#11)	DigSig-SigVer	Digital signature verification.		EDDSA SigVer: (A4740) SHA2-512: (A4740)
HMAC-SHA1 (SFI#12)	MAC	Message Authentication		HMAC-SHA-1: (A4740) SHA-1: (A4740)

Name	Type	Description	Properties	Algorithms
HMAC-SHA2-256 (SFI#13)	MAC	Message Authentication		HMAC-SHA2-256: (A4740) SHA2-256: (A4740)
HMAC-SHA2-384 (SFI#14)	MAC	Message Authentication		HMAC-SHA2-384: (A4740) SHA2-384: (A4740)
KAS1 (SFI#15)	KAS-Full	SSP Agreement with TLS v1.3	IG [D.F]: SSP establishment methodology provides between 128 and 192 bits of encryption strength:	KAS-ECC-SSC Sp800-56Ar3: (A4740) TLS v1.3 KDF: (A4740)
KAS-SSC (SFI#16)	KAS-SSC	Shared Secret Calculation	IG [D.F]:	KAS-ECC-SSC Sp800-56Ar3: (A4740)
KDF-TLS (SFI#17)	KAS-135KDF	Key Derivation	IG [D.F]:	TLS v1.3 KDF: (A4740)
KDF-SNMP (SFI#18)	KAS-135KDF	Key Derivation		KDF SNMP: (A4742)
RBG (SF#19)	DRBG	Randon Number Generation		Counter DRBG: (A4741) AES-ECB: (A4740)
RSA-PSS-GEN (SFI#20)	DigSig-SigGen	Digital Signature generation		RSA SigGen (FIPS186-4): (A4740) SHA2-256: (A4740) SHA2-384: (A4740)
RSA-PSS-VER (SFI#21)	DigSig-SigVer	Digital Signature verification		RSA SigVer (FIPS186-4): (A4740) SHA2-256: (A4740) SHA2-384: (A4740)
RSA-PKCS (SFI#22)	DigSig-SigVer	Digital Signature verification		RSA SigVer (FIPS186-2): (A4740) SHA2-256: (A4740)
SHA-1 (SFI#23)	SHA	Secure Hash Standard		SHA-1: (A4740)
SHA2-256 (SFI#24)	SHA	Secure Hash Standard		SHA2-256: (A4740)
SHA2-384 (SFI#25)	SHA	Secure Hash Standard		SHA2-384: (A4740)

Name	Type	Description	Properties	Algorithms
ECDSA (SFI#26)	DigSig-SigGen	Digital signature generation		ECDSA SigGen (FIPS186-5): (A4740) SHA2-256: (A4740) SHA2-384: (A4740)
ECDSA (SFI#27)	DigSig-SigVer	Digital signature verification		ECDSA SigVer (FIPS186-5): (A4740) SHA2-256: (A4740) SHA2-384: (A4740)
ECDSA (SFI#28)	AsymKeyPair-KeyGen	ECDSA Key Pair Generation		ECDSA KeyGen (FIPS186-5): (A4740) CKG-Asym: () Asymmetric: ECC P-256, ECC P-384: SHA2-256: (A4740) SHA2-384: (A4740)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

AES GCM IV Uniqueness

FIPS140-3 IG C.H, Option 5

TLS v1.3: TLS v1.3 is specified in IETF RFC 8446. In the TLS v1.3 implementation, a shared master secret is established as part of each TLS negotiation using key agreement with ECDHE. The private key used in ECDHE is generated within the implementation using the approved DRBG.

Traffic keying material is then derived from the master secret at TLS server and client, using the specified HMAC-based KDF (HKDF), as described in Sections 7.1 and 7.3 of RFC 8446, providing:

- client_write_key
- client_write_iv
- server_write_key
- server_write_iv

The appropriate write_key value is used directly as the secret key K for AES-GCM encryption and decryption. The IV for AES-GCM encryption and decryption is generated using the appropriate write_iv value as described in Section 5.3 of RFC 8446. IV generation consists of the following steps: The 64-bit TLS sequence number is padded with zeros to 96 bits

The padded sequence number is XORed with the appropriate 96-bit write_iv to create the IV

The TLS sequence number increments for every record transmitted, ensuring that a different IV is used each time the authenticated encryption/decryption function is invoked.

Note that in TLS v1.3 terminology the SP 800-38D IV is referred to as the Nonce (N).

The nonce explicit part of the IV is incremented each time an AES GCM computation is performed. The Module establishes a new session key when the nonce explicit part of the IV exhausts the maximum number of possible values (2^{32}-1). This meets the SP 800-38D collision probability requirement.

Note: KDF-TLS is used in TLS 1.3. No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

Note: KAS-SSC [56Ar3] - Per [IG] D.F Scenario 2 path (2), compliant with the derivation of a shared secret Z in one or more of the key agreement schemes in Section 6 of SP 800-56Arev3.

Note: KDF-SNMP is used in SNMPv3. No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

KAS [56Ar3] - Per [IG] D.F Scenario 2 path (2), compliant key agreement scheme where testing is performed it is split into (i) testing the computation of the shared secret, (ii) testing the key derivation function used in deriving the keying material comply to IG 2.4.B.

Legacy Use

RSA SigVer [FIPS 186-2] and DSA SigVer [FIPS 186-4] are approved for legacy use only: Algorithms designated as “Legacy” can only be used on data that was generated prior to the Legacy Date specified in FIPS 140-3 IG C.M

SHA-1 Transition:

As per NIST announcement, usage of SHA-1 for all applications will be transitioned away, and will be deemed as non-approved usage by December 31, 2030.

2.8 RBG and Entropy

N/A for this module.

The module does not implement any entropy sources.

The entropy for seeding the SP 800-90Ar1 DRBG is determined by the user of the module, which is outside of the module’s cryptographic boundary. To be compliant, the target application shall supply

at least 256 bits of entropy in order to meet the security strength required for the random number generation mechanism. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated SSPs (e.g., keys).

N/A for this module.

2.9 Key Generation

For Key Generation methods, see Section 2.6 Security Function Implementations above.

2.10 Key Establishment

For Key Establishment methods, see Section 2.6 Security Function Implementations above.

Key Transport Information

The module does not implement any Key Transport functions.

2.11 Industry Protocols

For Industry Protocols, see Section 2.6 Security Function Implementations above.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below.

Physical Port	Logical Interface(s)	Data That Passes
Main PSU Port	Data Input Data Output Control Input Status Output Power	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.
Aux Port	Data Input Data Output Control Input Status Output	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.
SFP (Fiber) Port	Data Input Data Output Control Input Status Output	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.
RF Horizontal	Data Input Data Output Control Input Status Output	RF input and output for connection to an external horizontally polarized 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.
RF Vertical	Data Input Data Output Control Input Status Output	RF input and output for connection to an external vertically polarized 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.
Ground terminal	Power	Used for safety and lightning protection.

Table 9: Ports and Interfaces

Note: The Module does not have any control output interface.

Figure 10 – Physical Ports and Interfaces on the PTP 45700 Connectorized Variant

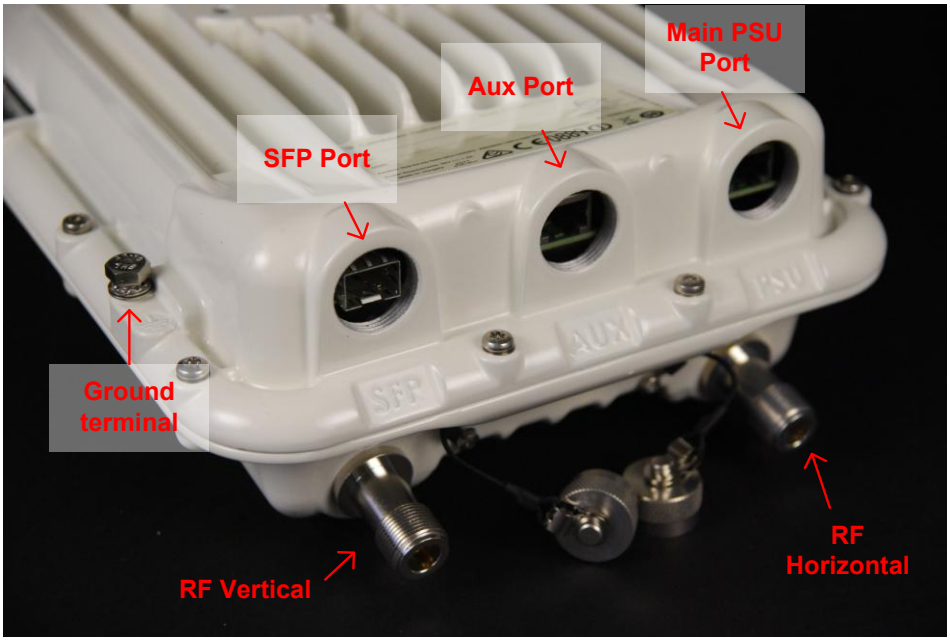


Figure 11 – Physical Ports and Interfaces on the PTP 45700 Connectorized+Integrated Variant

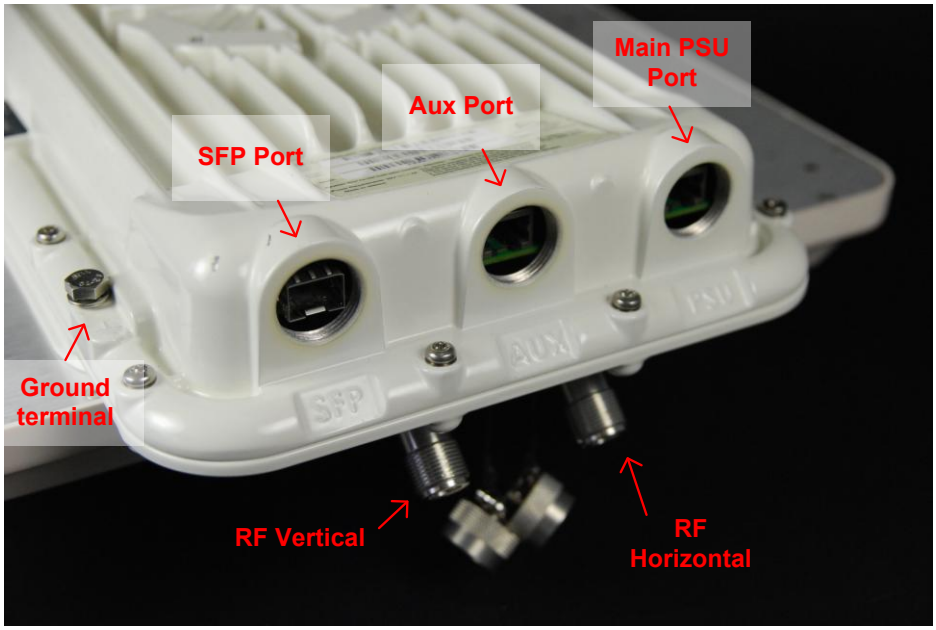


Figure 12 – Physical Ports and Interfaces on the PTP 78700 Variant



4 Roles, Services, and Authentication

4.1 Authentication Methods

The Module's authentication methods are listed in the table below:

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Local User Accounts	An identity-based Security Officer (SO) account is created at first use. Other identity-based accounts are created by a SO user. Authentication is by username and password with minimum password length of 15 ASCII characters.	Password Based	1 in 3.95 × 10^29	1 in 1.32 × 10^28
Single Sign-On	A local identity-based Security Officer (SO) configures for single sign-on where the authentication is provided by the Identity Provider (IdP)	RSA SigVer (FIPS186-4) (A4740)	1 in 2^112	1 in 2^112

Table 10: Authentication Methods

Local User Accounts

The default minimum password length is 15 characters. The SO can change minimum password length between 15 and 31 characters inclusive.

Passwords can contain:

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

The character set contains 94 characters.

A user account is locked following three unsuccessful authentication attempts.

The minimum number of unique passwords is 94^15 = 3.95 × 10^29.

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. These 30 attempts could conceivably be made within one minute.

Password strength per minute = (94^15)/30 = 1.32 × 10^28

Single Sign-On

The Single Sign-On authentication is provided by the redirected external Identity Provider (IdP) based on the 2048-bit RSA certificate. The users are authenticated using passwords with a minimum of 8 characters, but the IUT's authentication of the signature returned by the IdP is performed using the 2048-bit RSA certificate.

RSA 2048 has a minimum equivalent computational resistance to attack of 2^112 (2048 bits). The probability of a successful random attempt is 1/ (2^112), which is less than 1/1,000,000 (million). Due to limitations, it is conceivable that the redirect to the IdP would be one attempt per minute; the per minute strength is equivalent to 1 in 2^112 which is less than 1/100,000.

4.2 Roles

The Module supports four distinct operator roles, Security Officer (SO), System Administrator (SA), Installer (IN) and Read Only (RO). PTP 700 enforces the separation of roles using identity-based authentication, where each user is assigned one of the roles.

The Security Officer role is equivalent to the Cryptographic Officer identified in [FIPS140-3]. The SO role is permitted to configure SSPs.

The System Administrator is equivalent to the User identified in [FIPS140-3]. The SA role is not permitted to configure SSPs.

The Module does not support a maintenance role.

The Module 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 the same or lower permissions.

The Roles Table below lists all operator roles supported by the Module.

Name	Type	Operator Type	Authentication Methods
Security Officer (SO)	Identity	CO	Local User Accounts Single Sign-On
System Administrator (SA)	Identity	User	Local User Accounts Single Sign-On
Installer (IN)	Identity	User	Local User Accounts Single Sign-On
Read Only (RO)	Identity	User	Local User Accounts Single Sign-On

Table 11: Roles

Security Officer: A system administrator with read/write access to general and cryptographic configuration.

System Administrator: A system administrator with read/write access to general configuration but no access to cryptographic configuration.

Installer: A non-expert user with limited read/write access but no access to cryptographic configuration.

Read Only: An operator with read-only access to general configuration but no access to cryptographic configuration.

Firmware Update: An operator responsible for updating the firmware on the PTP 700.

In the Approved Services table, under “Roles” column “U” stands for unauthenticated services.

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:

The SSPs modes of access shown in the table below are defined as:

- G = Generate: The Module generates or derives the SSP.
- R = Read: The SSP is read from the Module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the Module (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.
- Z = Zeroize: The Module zeroizes the SSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Self-Test	Known answer tests for all the supported cryptographic algorithms	Successful completion of self tests is implied by the restart of the module. On failure, module restarts and sets error code in Restart Reason.	Power	Error status: Module restarts and sets error code in restart reason Success: Module restarts normal operation	None	Unauthenticated
Web interface network connection	Establish a secure connection using HTTPS from module to web	Web browser indicates secure connection. For example, padlock	-	-	AES-GCM-D (SFI#7) AES-GCM-E (SFI#8) CKG (SFI#9)	Unauthenticated - RSA WEB PRIV: E - RSA WEB PUB: W - ECDHE WEB PRIV: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	browser on an external general purpose computer (GPC)	symbol in Site Information in Google Chrome.			HMAC-SHA2-256 (SFI#13) HMAC-SHA2-384 (SFI#14) KAS1 (SFI#15) KAS-SSC (SFI#16) KDF-TLS (SFI#17) RBG (SF#19) RSA-PSS-GEN (SFI#20) RSA-PKCS (SFI#22) SHA2-256 (SFI#24) SHA2-384 (SFI#25) ECDSA (SFI#26) ECDSA (SFI#27	- ECDHE WEB PUB1: G - ECDHE WEB PUB2: W - TLS WEB MS: G - TLS WEB SK: G - CTR DRBG SEED: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					) ECDSA (SFI#28)	
Web interface login	Operator accesses the module by authenticating username and password.	Module displays the login dialog in the web interface and provides access when user is authenticated.	Username Password	-	HMAC-SHA2-256 (SFI#13) SHA2-256 (SFI#24)	Security Officer (SO) - PW DIGEST: E - HMAC KEY: E System Administrator (SA) - PW DIGEST: E - HMAC KEY: E Installer (IN) - PW DIGEST: E - HMAC KEY: E Read Only (RO) - PW DIGEST: E - HMAC KEY: E
Web interface logout	Operator logs out from the module	Module displays logout dialogue in the web interface.	Command	-	None	Security Officer (SO) System Administrator (SA) Installer (IN) Read Only (RO)
Web interface SSO	Operator accesses the module using single sign on with SAML security assertion.	Module displays the login dialog in the web interface and provides access when user is	-	-	RSA-PSS-VER (SFI#21)	Security Officer (SO) - RSA SSO PUB: System Administrator (SA) - RSA SSO PUB: E Installer (IN)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		authenticated to identity provider.				- RSA SSO PUB: E Read Only (RO) - RSA SSO PUB: E
Web interface module status (Show Status/Show Version)	Show module status and versioning information including the module identifier (model number)	Module displays status information in the web interface.	N/A	Module Identifier: PTP 45700 Connectorized+Integrated ODU, PTP 45700 Connectorized ODU, PTP 47500 Beam Steering ODU, PTP 78700 Connectorized ODU. Approved mode status: FIPS 140-3 text highlighted in Green, on the web interface. Hardware Version: All versions listed in Table Tested Module Identification - Hardware. Firmware Version: 45700-40-10-FIPS and 78700-04-10-FIPS	None	Security Officer (SO) System Administrator (SA) Installer (IN) Read Only (RO)
Web interface security configuration	Operator configures security operation of the module, including License Key, excluding SSPs.	Module accepts configuration data in the web interface.	-	-	DSA (SFI#10) EDDSA (SFI#11)	Security Officer (SO) - DSA LIC PUB: E - EDDSA LIC PUB: E
Web interface general	Operator configures wireless	Module accepts configurati	-	-	None	Security Officer (SO) System

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
configuration	and networking operation of the module.	on data in the web interface.				Administrator (SA)
Web interface wireless security configuration	Operator configures wireless security configuration like encryption keys and certificates	Module accepts configuration data in the web interface.	-	-	None	Security Officer (SO)
Web interface cnMaestro configuration	Operator configures cnMaestro connection parameters of the module.	Module accepts configuration data in the web interface.	-	-	None	Security Officer (SO)
Web interface installation	Operator selects a predefined configuration for wireless and networking operation.	Module accepts configuration data in the web interface.	-	-	None	Installer (IN)
Reboot by command at the web interface	Reboot the module.	Module requests confirmation in the web interface and restarts.	Command	-	None	Security Officer (SO) - ECDHE WEB PRIV: Z - ECDHE WEB PUB1: Z - ECDHE WEB PUB2: Z - TLS WEB

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						MS: Z - TLS WEB SK: Z - RSA MAES PUB: Z - ECDHE MAES PRIV: Z - ECDHE MAES PUB1: Z - ECDHE MAES PUB2: Z - TLS MAES MS: Z - TLS MAES SK: Z - RSA WLS PUB2: Z - ECDHE WLS PRIV: Z - ECDHE WLS PUB1: Z - ECDHE WLS PUB2: Z - TLS WLS MS: Z - TLS WLS SK1: Z - TLS WLS SK2: Z - SNMP AUTHPRIV PP: Z - HMAC KEY: Z - DRBG STATE: Z System Administrator (SA) - ECDHE WEB PRIV: Z - ECDHE WEB PUB1:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Z - ECDHE WEB PUB2: Z - TLS WEB MS: Z - TLS WEB SK: Z - RSA MAES PUB: Z - ECDHE MAES PRIV: Z - ECDHE MAES PUB1: Z - ECDHE MAES PUB2: Z - TLS MAES MS: Z - TLS MAES SK: Z - RSA WLS PUB2: Z - ECDHE WLS PRIV: Z - ECDHE WLS PUB1: Z - ECDHE WLS PUB2: Z - TLS WLS MS: Z - TLS WLS SK1: Z - TLS WLS SK2: Z - SNMP AUTHPRIV PP: Z - HMAC KEY: Z - DRBG STATE: Z
Administer web	Create new user	Module allows	Password	-	SHA2-256	Security Officer (SO)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
interface user accounts	accounts, update or reset passwords.	configuration changes in the Local User Accounts page in the web interface.			(SFI#24)	- PW DIGEST: G
Update web interface password	Operator updates his/her own password for the web-based interface.	Module displays change password dialog in the web interface.	Password	-	SHA2-256 (SFI#24)	Security Officer (SO) - PW DIGEST: G System Administrator (SA) - PW DIGEST: G Installer (IN) - PW DIGEST: G Read Only (RO) - PW DIGEST: G
cnMaestro network connection	Establish a secure tunnel with HTTPS from module to cnMaestro server	Module displays status indicator in the web interface.	-	-	AES-GCM-D (SFI#7) AES-GCM-E (SFI#8) CKG (SFI#9) HMAC-SHA2-256 (SFI#13) HMAC-SHA2-384 (SFI#14) KAS1 (SFI#15) KAS-	Unauthenticated - RSA MAES PUB: W - RSA MAES ROOT: E - ECDHE MAES PRIV: G - ECDHE MAES PUB1: G - ECDHE MAES PUB2: W - TLS MAES MS: G - TLS MAES SK: G - CTR DRBG SEED: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SSC (SFI#16) KDF-TLS (SFI#17) RBG (SF#19) RSA-PSS-GEN (SFI#20) RSA-PSS-VER (SFI#21) RSA-PKCS (SFI#22) SHA2-256 (SFI#24) SHA2-384 (SFI#25) ECDSA (SFI#26) ECDSA (SFI#27) ECDSA (SFI#28)	
Establish secure wireless link	Module establishes an authenticated and	Module displays Wireless Link Status and	-	-	AES-GCM-D (SFI#7) AES-GCM-E	Unauthenticated - RSA WLS PRIV: E - RSA WLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	encrypted wireless link to a remote module using TLS 1.3 for key agreement.	Wireless Encryption attributes in the System Status page of the web interface.			(SFI#8) CKG (SFI#9) HMAC-SHA2-256 (SFI#13) HMAC-SHA2-384 (SFI#14) KAS1 (SFI#15) KAS-SSC (SFI#16) KDF-TLS (SFI#17) RBG (SF#19) RSA-PSS-GEN (SFI#20) RSA-PSS-VER (SFI#21) RSA-PKCS (SFI#22) SHA2-256 (SFI#24) SHA2-	PUB1: W - RSA WLS PUB2: W - ECDHE WLS PRIV: G - ECDHE WLS PUB1: G - ECDHE WLS PUB2: W - TLS WLS MS: G - TLS WLS SK1: G - TLS WLS SK2: G - CTR DRBG SEED: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					384 (SFI#25) ECDSA (SFI#26) ECDSA (SFI#27) ECDSA (SFI#28)	
Wireless encryption	Encrypt and decrypt end-user's data for transmission across the wireless link	Module displays negotiated wireless encryption algorithm in the Wireless Encryption attribute in the System Status page of the web interface.	Plain text Ethernet, Encrypted wireless	Encrypted wireless, Plain text Ethernet	AES-CFB-WLS-D (SFI#1) AES-CFB-WLS-E (SFI#2)	Unauthenticated - TLS WLS SK2: E - AES GCM IV: E
Update firmware with zeroization	Verify digital signature of replacement firmware. Write firmware to non-volatile memory. SSPs are always zeroized upon firmware upgrade.	Operator selects replacement firmware using the web interface. Web interface provides progress tracker and requests confirmation, including zeroization, before restarting. Module restarts.	Command	-	DSA (SFI#10) EDDSA (SFI#11)	Security Officer (SO) - EDDSA FW PUB: E - KoK: Z - DRBG ENT: Z - RSA WEB PRIV: Z - RSA WEB PUB: Z - RSA WLS PRIV: Z - RSA WLS PUB1: Z - RSA WLS ROOT: Z - PSK WLS: Z - SNMP AUTHPRIV

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						LOC: Z - SNTP KEY: Z - PW DIGEST: Z - RSA SSO PUB: Z - DSA LIC PUB: E
Zeroise SSPs	Protect encrypted SSPs in non-volatile memory by erasing the key of keys. Remove SSPs from volatile memory by reboot.	Operator triggers zeroization action using the web interface with confirmation. Module restarts.	Command	-	None	Security Officer (SO) - ECDHE WEB PRIV: Z - ECDHE WEB PUB1: Z - ECDHE WEB PUB2: Z - TLS WEB MS: Z - TLS WEB SK: Z - RSA MAES PUB: Z - ECDHE MAES PRIV: Z - ECDHE MAES PUB1: Z - ECDHE MAES PUB2: Z - TLS MAES MS: Z - TLS MAES SK: Z - RSA WLS PUB2: Z - ECDHE WLS PRIV: Z - ECDHE WLS PUB1: Z - ECDHE WLS PUB2: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TLS WLS MS: Z - TLS WLS SK1: Z - TLS WLS SK2: Z - SNMP AUTHPRIV PP: Z - HMAC KEY: Z - DRBG STATE: Z - KoK: Z - DRBG ENT: Z - RSA WEB PRIV: Z - RSA WEB PUB: Z - RSA WLS PRIV: Z - RSA WLS PUB1: Z - RSA WLS ROOT: Z - PSK WLS: Z - SNMP AUTHPRIV LOC: Z - SNTP KEY: Z - PW DIGEST: Z - RSA SSO PUB: Z
Configure SSPs	Configure SSPs for HTTPS, wireless encryption, authenticated NTP, SNMPv3	Operator configures SSPs in the web interface, submits changes. Module restarts.	SSPs	-	AES-ECB-D (SFI#5) AES-ECB-E (SFI#6) KDF-SNMP (SFI#18)	Security Officer (SO) - KoK: W - DRBG ENT: W - RSA WEB PRIV: W - RSA WEB PUB: W - RSA WLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PRIV: W - RSA WLS PUB1: W - RSA WLS ROOT: W - PSK WLS: W - SNMP AUTHPRIV PP: W - SNTP KEY: W - PW DIGEST: G - RSA SSO PUB: W
SNMPv3 general configuration	Operator configures wireless and networking operation of the module using SNMPv3. SNMP does not allow input or output of SSPs.	SNMP manager modifies MIB objects in the module with indication of successful operation.	-	-	AES-CFB-SNMP-D(SFI#3) AES-CFB-SNMP-E (SFI#4) HMAC-SHA1 (SFI#12) SHA-1 (SFI#23)	Security Officer (SO) - SNMP AUTHPRIV LOC: E
Synchronize Real Time Clock	Synchronize RTC with authenticated NTP server	Module indicates RTC synchronization status in the web interface	NTP messages with authentication	Updated date and time	SHA-1 (SFI#23)	Unauthenticated - SNTP KEY: E

Table 12: Approved Services

4.4 Non-Approved Services

NOTE: There are no Non-Approved services available.

4.5 External Software/Firmware Loaded

The module supports loading of replacement firmware from an external source as a means to deliver additional features or to rectify defects in the existing firmware. Replacement firmware is available from the module manufacturer and is digitally signed using the EdDSA algorithm. The firmware load test ensures that only authorized firmware can be loaded.

The module will not accept firmware from other publishers and will not accept general purpose application software.

4.6 Bypass Actions and Status

The module does not support a bypass action.

4.7 Cryptographic Output Actions and Status

Self-initiated wireless connection

A suitably-configured module will establish an authenticated and encrypted wireless connection to a remote module following power cycle or reboot, without operator intervention. This is a necessary characteristic to ensure high availability in equipment deployed within network infrastructure.
To achieve self-initiated use of approved services in the wireless interface, Security Officer must first complete the following steps::

- Configure Encryption Algorithm = TLS RSA, TLS PSK 128-bit, or TLS PSK 256-bit
- For TLS RSA, configure Device Root CA certificate, Device Private Key, Device Public Certificate
- For TLS PSK, configure 128-bit or 256-bit Pre-Shared Key
- Submit changes in the Security Wizard

The module indicates use of a self-initiated wireless connection by means of the Wireless Link Status attribute in the System Status page of the web interface. The wireless connection is authenticated and encrypted unless the Wireless Encryption attribute in the System Status page is set to “None”.

Transmission and reception of encrypted data at the wireless interface

If the module is suitably configured for a secure wireless connection, as described above, it receives plaintext Ethernet frames at wired Ethernet ports and encrypts this data for transmission over the wireless link. Similarly, encrypted data received at the wireless ports is decrypted within the module and transmitted as plaintext Ethernet frames at the wired Ethernet ports. Bridging of network traffic does not require further operator intervention.

Self-initiated cnMaestro network management connection

A suitably-configured module will establish an authenticated and encrypted web-socket (HTTPS) connection to a cnMaestro server following power cycle or reboot, without operator intervention. This is a necessary characteristic to ensure continuity of the network management capability.
To achieve self-initiated use of approved services in the wireless interface, Security Officer must first complete the following steps::

- Configure cnMaestro = Enabled
- Configure cnMaestro Server Internet Address
- Optionally, configure Cambium ID and Onboarding Key
- Submit changes in the Installation Wizard

4.8 Additional Information

Direct Connection for Initial Configuration
PTP 700 zeroizes CSPs on transition into the 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.

5 Software/Firmware Security

5.1 Integrity Techniques

The module performs the Firmware Integrity test by using an EDC (32-bit CRC) KAT during the Pre-Operational Self-Test. In addition, the module also conducts the firmware load test by using EDDSA (Cert. #A4740) for a validated firmware to be loaded into the module.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by power cycle or reboot.

5.3 Open-Source Parameters

The module uses the following open source packages:

- OpenSSL
- net-snmp

OpenSSL

OpenSSL software has been modified to compile on the TI DSP TMS320C6657processor along with changes to use a dedicated heap, NIST DRBG implementation for generating random bytes and compile only the algorithms used by the module.

Further OpenSSL is statically linked to the module software.

NET-SNMP

Simple Network Management Protocol (SNMP) is a standardized protocol that allows network administrators to monitor and manage the module. Security parameters are not allowed to be configured or queried by SNMP.

Net-snmp module also uses a dedicated heap to control the memory used by the package and isolate any memory issues to only this package.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The Module has a limited operational environment at Level 2 under the FIPS 140-3 definitions therefore per the FIPS 140-3 Management Manual Section 7.5 Partial validations and non-applicable areas this section in not applicable.

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Appropriate module enclosure screws covered with tamper-evident barrels.	30 days	Inspect screw heads for chipped/missing barrels. If found remove module from service.

Table 13: Mechanisms and Actions Required

Inspection Guidance

If damage to the tamper-evident barrel on screw heads are chipped/damaged/missing or damage to the enclosure is observed, the unit should be removed from service and inspected more closely. If tampering is suspected or confirmed, return the module to the manufacturer.

The correct location of the tamper-evident barrels is shown in the following figures: Figure 13 through Figure 17.

Figure 13 – Tamper-Evident Barrel Locations on a Connectorized PTP 45700 Unit (White/Desert Tan/Green)









Figure 14 – Tamper-Evident Barrel Locations on a Connectorized+Integrated PTP 45700 Unit (White/Desert Tan/Green)

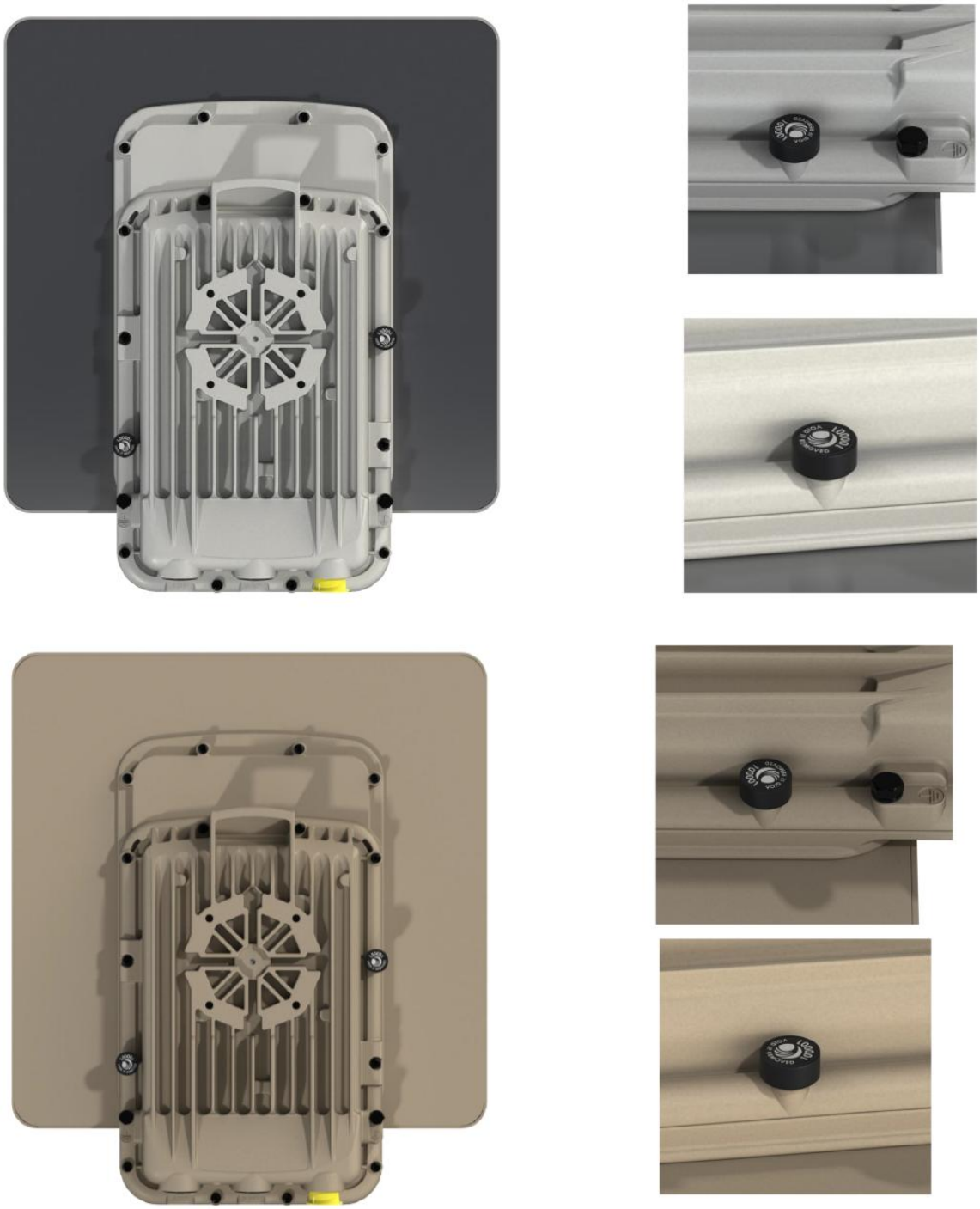
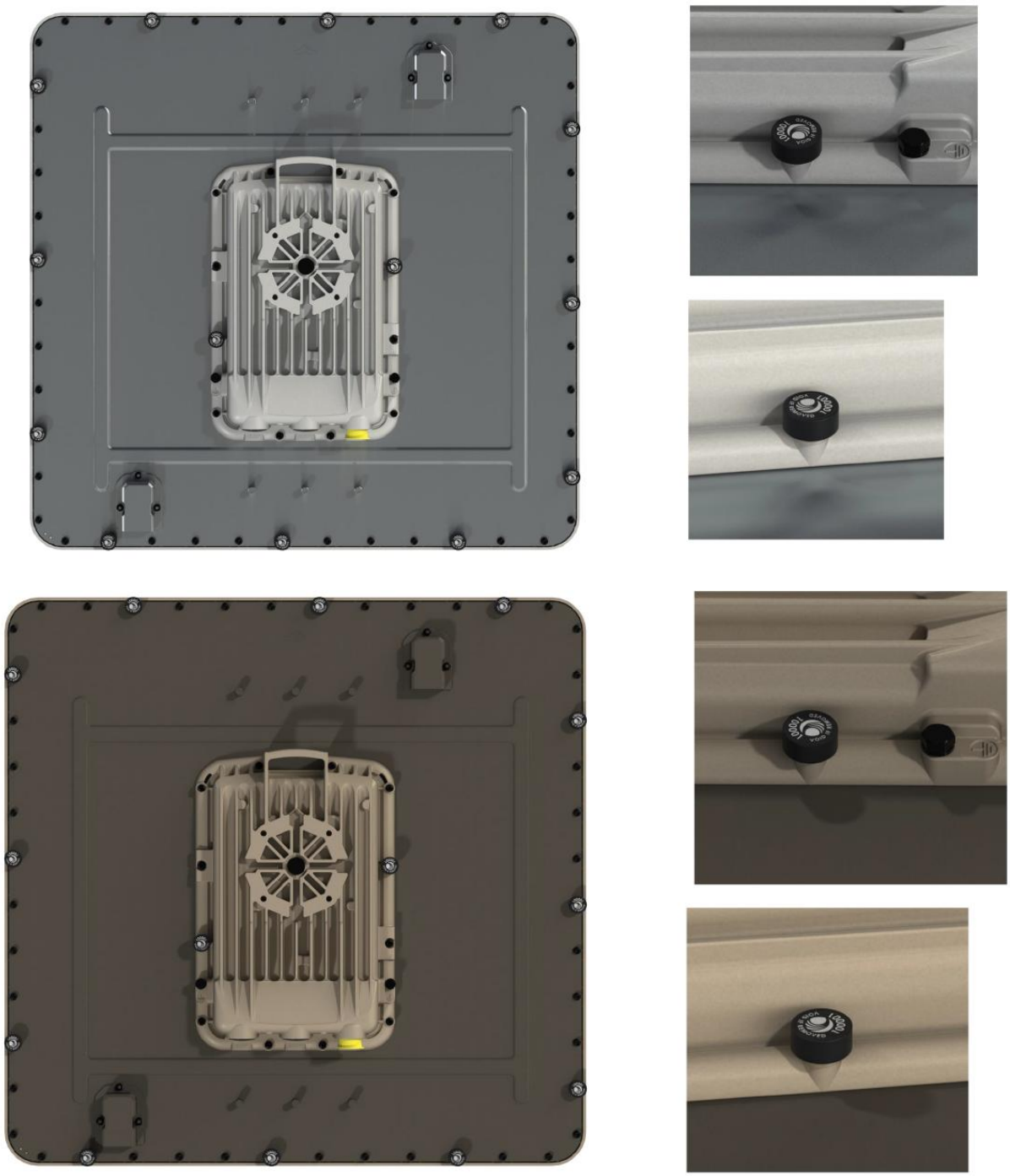


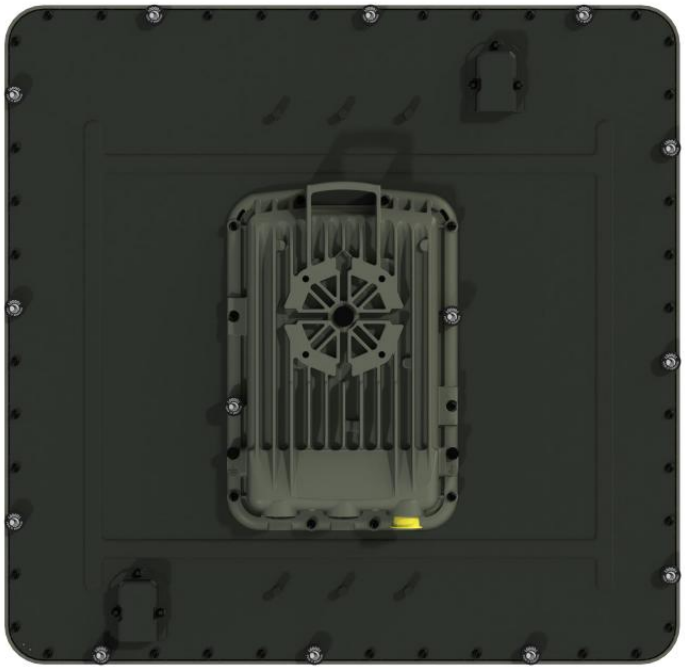






Figure 15 - Tamper-Evident Barrel Locations on a Beam Steering PTP 45700 Unit (White/Desert Tan/Green)





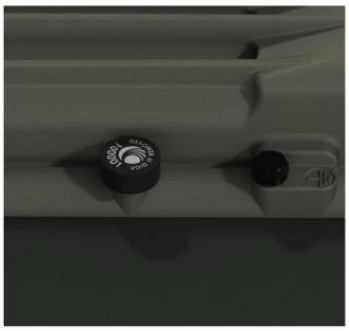




Figure 16 – Tamper-Evident Barrel Locations on a Connectorized PTP 78700 Unit (White/Desert Tan/Green)

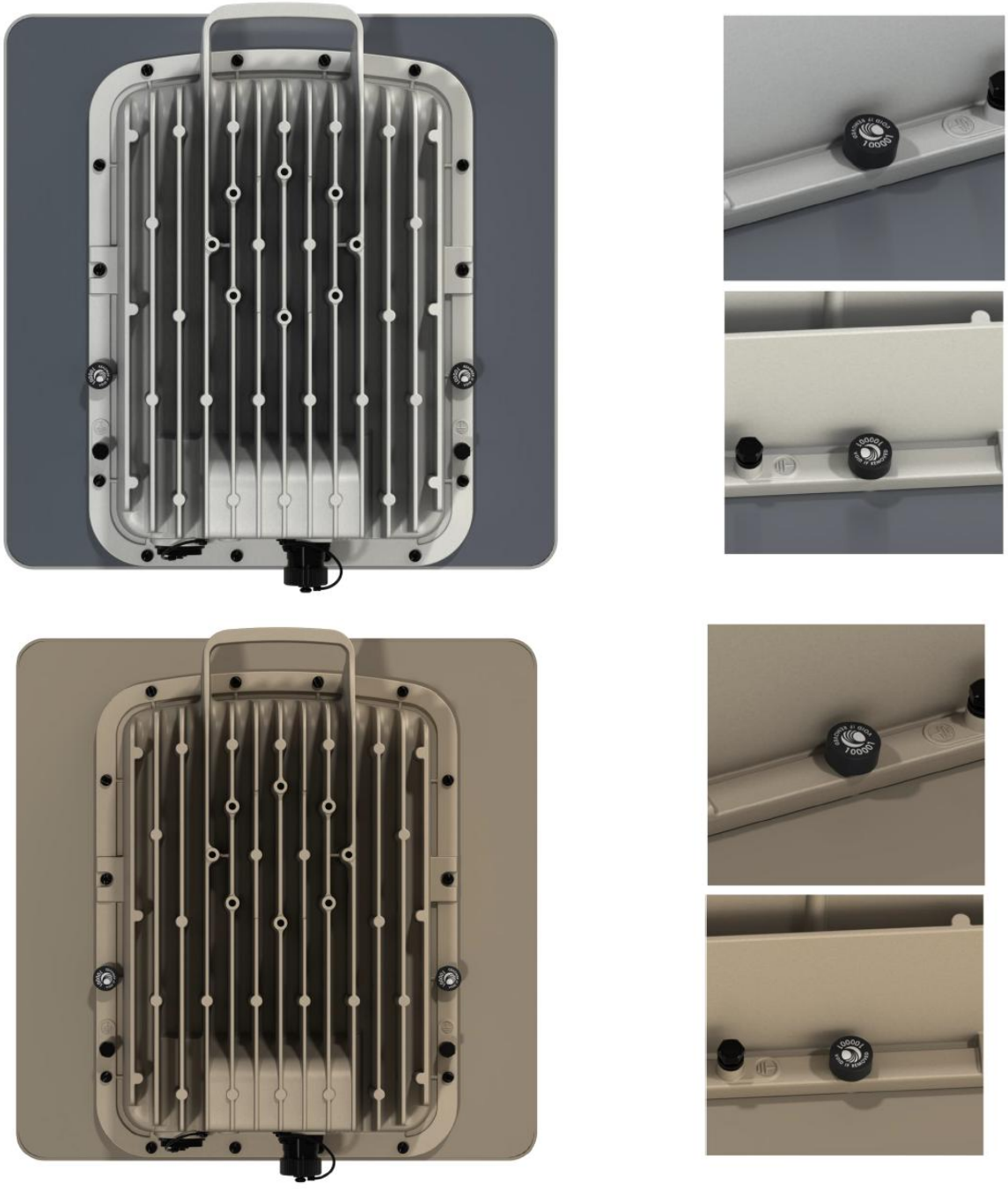








Figure 17 – Tamper-Evident Barrel Locations on an Integrated PTP 78700 Unit (White/Desert Tan/Green)









7.2 User Placed Tamper Seals

The module uses tamper-evident barrels made from aluminum with a hard black anodized finish over enclosure screws instead of tamper seals. The module will be shipped from the manufacturer with tamper-evident barrels as shown in Figure 13 to Figure 17.

8 Non-Invasive Security

8.1 Mitigation Techniques

The Module does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Volatile (S1)	Stored in volatile memory (RAM)	Dynamic
Non-volatile (S2)	Stored in non-volatile memory, encrypted with the Key of Keys.	Static
Key of Keys (S3)	Stored in non-volatile memory as plain text.	Static
Embedded (S4)	Embedded in the operating firmware as plain text.	Static

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input with Direct configuration from directly connected GPC (I1)	General purpose computer (GPC) (outside)	Module (S2)	Plaintext	Manual	Direct	
Input with Electronic configuration from directly connected GPC (I2)	GPC (outside)	Module (S2)	Plaintext	Manual	Electronic	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Erase Key of Keys	A dedicated flash memory bank is erased to zeroize the Instantiate (KoK) CSP. Erased flash memory has a default value of "1".	Triggered by a SO user from Main Application, or Recovery.
Z2	Overwrite volatile SSPs	Overwritten in RAM with a fixed pattern of zeros.	Triggered by a SO user from Main Application, or Recovery by a reboot of the module.

Table 16: SSP Zeroization Methods

Non-volatile SSPs are stored encrypted with the Key of Keys (KoK). The KoK is stored in plaintext in a dedicated flash memory area. SSPs can be accessed by the application firmware by decrypting with the KoK. The Zeroize function erases the KoK. Following zeroization, the encrypted SSPs remain in non-volatile memory, but are protected because the KoK is not available for decryption.

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in Section 4.3

Entropy Caveat: *No assurance of the minimum strength of generated SSPs (e.g., keys)*

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KoK	Key of Keys encrypts SSPs for non-volatile storage.	128, 256 - 128, 256	Symmetric key - CSP			AES-ECB-D (SFI#5) AES-ECB-E (SFI#6)
DRBG ENT	CTR DRBG entropy input used to seed the DRBG.	512 - 512	N/A - CSP			RBG (SF#19)
CTR DRBG SEED	Seed for the CTR DRBG	256 - 256	N/A - CSP	RBG (SF#19)		RBG (SF#19)
RSA WEB PUB	RSA public key certificate used to authenticate the HTTPS server.	2048 - 112	Asymmetric public key - CSP			RSA-PSS-VER (SFI#21) RSA-PKCS (SFI#22)
RSA WEB PRIV	RSA private key used to authenticate the HTTPS server to web browser.	2048 - 112	Asymmetric private key - CSP			RSA-PSS-GEN (SFI#20) RSA-PKCS (SFI#22)
ECDHE WEB PRIV	Private key used with ECDHE for key agreement within HTTPS with TLS 1.3.	256, 384 - 128, 192	Asymmetric private key - CSP	ECDSA (SFI#28)		KAS1 (SFI#15)
ECDHE WEB PUB1	Public key used with ECDHE for key agreement within HTTPS with TLS 1.3.	256, 384 - 128, 192	Asymmetric public key - PSP	ECDSA (SFI#28)		KAS1 (SFI#15)
ECDHE WEB PUB2	Public key used with ECDHE supplied by web browser.	256, 384 - 128, 192	Asymmetric public key - PSP	KDF-TLS (SFI#17)	KAS1 (SFI#15) KAS-SSC (SFI#16)	KAS-SSC (SFI#16)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS WEB MS	Master secret generated by KAS in HTTPS using ECDHE.	128, 256 - 128, 256	Shared secret - CSP	KDF-TLS (SFI#17)	KAS1 (SFI#15) KAS-SSC (SFI#16)	KDF-TLS (SFI#17)
TLS WEB SK	Encryption session key derived in HTTPS from TLS 1.3 master secret.	128, 256 - 128, 256	Symmetric key - CSP	KDF-TLS (SFI#17)		AES-GCM-D (SFI#7) AES-GCM-E (SFI#8)
RSA MAES PUB	RSA public key certificate used to authenticate the cnMaestro server using HTTPS. Externally generated and embedded in firmware image.	2048 - 112	Asymmetric public key - PSP			RSA-PSS-VER (SFI#21) RSA-PKCS (SFI#22)
RSA MAES ROOT	RSA root certificate used to authenticate the cnMaestro server using HTTPS. Externally generated and embedded in firmware image.	2048 - 112	Asymmetric public key - PSP			RSA-PKCS (SFI#22)
ECDHE MAES PRIV	Private key used with ECDHE for key agreement within HTTPS with TLS 1.3.	256, 384 - 128, 192	Asymmetric private key - CSP	ECDSA (SFI#28)		KAS1 (SFI#15)
ECDHE MAES PUB1	Public key used with ECDHE for key agreement within HTTPS with TLS 1.3.	256, 384 - 128, 192	Asymmetric public key - PSP	ECDSA (SFI#28)		KAS1 (SFI#15)
ECDHE MAES PUB2	Public key used with ECDHE supplied by cnMaestro.	256, 384 - 128, 192	Asymmetric public key - PSP	KDF-TLS (SFI#17)	KAS1 (SFI#15) KAS-SSC (SFI#16)	KAS1 (SFI#15)
TLS MAES MS	Master secret generated by KAS using ECDHE for cnMaestro interface.	128, 256 - 128, 256	Shared secret - CSP	KDF-TLS (SFI#17)	KAS1 (SFI#15) KAS-SSC (SFI#16)	KAS1 (SFI#15)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
TLS MAES SK	Encryption session key derived in HTTPS from TLS 1.3 master secret.	128, 256 - 128, 256	Symmetric key - CSP	KDF-TLS (SFI#17)		AES-GCM-D (SFI#7) AES-GCM-E (SFI#8)
AES GCM IV	IV needed for TLS WEB SK, TLS MAES MS and TLS MAES SK	96 - 96	N/A - CSP	RBG (SF#19)		AES-GCM-D (SFI#7) AES-GCM-E (SFI#8)
RSA WLS PRIV	RSA private key used to authenticate the wireless link using TLS 1.3.	2048 - 112	Asymmetric private key - CSP			RSA-PSS-VER (SFI#21)
RSA WLS PUB1	RSA public key certificate identifying the module, used authenticate the wireless interface using TLS 1.3	2048 - 112	Asymmetric public key - PSP			RSA-PSS-VER (SFI#21)
RSA WLS PUB2	RSA public key certificate identifying the remote device in the wireless interface.	2048 - 112	Asymmetric public key - PSP	KDF-TLS (SFI#17)	KAS1 (SFI#15) KAS-SSC (SFI#16)	RSA-PKCS (SFI#22)
RSA WLS ROOT	RSA root certificate used to verify RSA WLS2.	2048 - 112	Asymmetric public key - PSP			RSA-PKCS (SFI#22)
PSK WLS	Pre-shared key used to authenticate the wireless interface.	128, 256 - 128, 256	Shared secret - CSP			KAS-SSC (SFI#16)
ECDHE WLS PRIV	Private key used with ECDHE for key agreement at wireless interface with TLS 1.3.	256, 384 - 128, 192	Asymmetric private key - CSP	ECDSA (SFI#28)		KAS1 (SFI#15)
ECDHE WLS PUB1	Public key used with ECDHE for key agreement at wireless interface with TLS 1.3	256, 384 - 128, 192	Asymmetric public key - PSP	ECDSA (SFI#28)		KAS1 (SFI#15)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ECDHE WLS PUB2	Public key used with ECDHE supplied by remote wireless device.	256, 384 - 128, 192	Asymmetric public key - PSP	KDF-TLS (SFI#17)	KAS1 (SFI#15) KAS-SSC (SFI#16)	KAS1 (SFI#15)
TLS WLS MS	Master secret generated by KAS using ECDHE in TLS 1.3 at wireless interface.	128, 256 - 128, 256	Shared secret - CSP	KDF-TLS (SFI#17)	KAS1 (SFI#15) KAS-SSC (SFI#16)	KAS1 (SFI#15)
TLS WLS SK1	Wireless interface encryption session key for TLS 1.3 derived from TLS WLS MS.	128, 256 - 128, 256	Symmetric key - CSP	KDF-TLS (SFI#17)		AES-GCM-D (SFI#7) AES-GCM-E (SFI#8)
TLS WLS SK2	AES encryption key for wireless link, exported from TLS 1.3	128, 256 - 128, 256	Symmetric key - CSP	KDF-TLS (SFI#17)		AES-CFB-WLS-D (SFI#1) AES-CFB-WLS-E (SFI#2)
SNMP AUTHPRIV LOC	Localized privacy key for SNMPv3 in to ten user accounts.	128 - 128	Symmetric key - CSP	KDF-SNMP (SFI#18)		AES-CFB-SNMP-D(SFI#3) AES-CFB-SNMP-E (SFI#4) HMAC-SHA1 (SFI#12) SHA-1 (SFI#23)
SNMP AUTHPRIV PP	Passphrases used to derive localized keys LOC SNMP AUTHPRIV using the standard SNMPv3 KDF.	- - -	- - CSP			KDF-SNMP (SFI#18)
SNTP KEY	Symmetric keys used with SHA-1 to authenticate time messages from NTP servers.	128 - 128	Symmetric key - CSP			SHA-1 (SFI#23)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PW DIGEST	SHA2-256 digest of user passwords for ten identity-based user accounts in the web interface.	- - -	- - CSP	SHA2-256 (SFI#24)		SHA2-256 (SFI#24)
HMAC KEY	SHA2-256 used with HMAC to sign and verify authentication cookies.	256 - 256	Symmetric key - CSP	CKG (SFI#9)		HMAC-SHA2-256 (SFI#13) SHA2-256 (SFI#24)
RSA SSO PUB	Public key certificate used to authenticate SAML assertion from external IdP in web interface single sign on.	2048 - 112	- - PSP			RSA-PSS-VER (SFI#21)
DRBG STATE	The DRBG state (V and Key) stored in volatile memory.	256 - 256	- - CSP	RBG (SF#19)		RBG (SF#19)
EDDSA FW PUB	EdDSA public key used to authenticate replacement firmware. Externally generated and embedded in firmware image.	256 - 128	Asymmetric public key - PSP			EDDSA (SFI#11)
EDDSA LIC PUB	EdDSA public key used to authenticate License Keys. Externally generated and embedded in firmware image.	256 - 128	Asymmetric public key - PSP			EDDSA (SFI#11)
DSA LIC PUB	DSA public key used to authenticate legacy License Keys. Externally generated and embedded in firmware image.	1024, 2048 - 80, 112	Asymmetric public key - PSP			DSA (SFI#10)

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KoK	Input with Direct configuration from directly connected GPC (I1)	Key of Keys (S3):Plaintext		Z1	DRBG ENT:Encrypts RSA WEB PUB:Encrypts RSA WEB PRIV:Encrypts RSA WLS PRIV:Encrypts RSA WLS PUB1:Encrypts RSA WLS ROOT:Encrypts PSK WLS:Encrypts SNMP AUTHPRIV LOC:Encrypts SNTP KEY:Encrypts PW DIGEST:Encrypts RSA SSO PUB:Encrypts
DRBG ENT	Input with Direct configuration from directly connected GPC (I1)	Non-volatile (S2):Encrypted		Z1	CTR DRBG SEED:Used to derive KoK:Encrypted by
CTR DRBG SEED		Volatile (S1):Plaintext		Z2	DRBG STATE:Used to derive DRBG ENT:Derived From
RSA WEB PUB	Input with Electronic configuration from directly connected GPC (I2)	Non-volatile (S2):Encrypted		Z1	RSA WEB PRIV:Paired With KoK:Encrypted by
RSA WEB PRIV	Input with Electronic configuration from directly connected GPC (I2)	Non-volatile (S2):Encrypted		Z1	RSA WEB PUB:Paired With KoK:Encrypted by
ECDHE WEB PRIV		Volatile (S1):Plaintext	HTTPS TLS session	Z2	ECDHE WEB PUB1:Paired With TLS WEB MS:Used

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					to establish ECDHE WEB PUB2:Used With
ECDHE WEB PUB1		Volatile (S1):Plaintext	HTTPS TLS session	Z2	ECDHE WEB PRIV:Paired With TLS WEB MS:Used to establish ECDHE WEB PUB2:Used With
ECDHE WEB PUB2		Volatile (S1):Plaintext	HTTPS TLS session	Z2	TLS WEB MS:Used to establish ECDHE WEB PUB1:Used With ECDHE WEB PRIV:Used With
TLS WEB MS		Volatile (S1):Plaintext	HTTPS TLS session	Z2	TLS WEB SK:Used to derive ECDHE WEB PRIV:Established from ECDHE WEB PUB1:Established from ECDHE WEB PUB2:Established from
TLS WEB SK		Volatile (S1):Plaintext	HTTPS TLS session	Z2	TLS WEB MS:Derived From AES GCM IV:Used With
RSA MAES PUB		Volatile (S1):Plaintext	cnMaestro TLS session	Z2	RSA MAES ROOT:Verified by
RSA MAES ROOT		Embedded (S4):Plaintext		N/A	RSA MAES PUB:Used to verify
ECDHE MAES PRIV		Volatile (S1):Plaintext	cnMaestro TLS session	Z2	ECDHE MAES PUB1:Paired With TLS MAES MS:Used to establish ECDHE MAES PUB2:Used With
ECDHE MAES PUB1		Volatile (S1):Plaintext	cnMaestro TLS session	Z2	ECDHE MAES PRIV:Paired With TLS MAES MS:Used to establish ECDHE MAES PUB2:Used With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ECDHE MAES PUB2		Volatile (S1):Plaintext	cnMaestro TLS session	Z2	TLS MAES MS:Used to establish ECDHE MAES PRIV:Used With ECDHE MAES PUB1:Used With
TLS MAES MS		Volatile (S1):Plaintext	cnMaestro TLS session	Z2	TLS MAES SK:Used to derive AES GCM IV:Used With ECDHE MAES PRIV:Established from ECDHE MAES PUB1:Established from ECDHE MAES PUB2:Established from
TLS MAES SK		Volatile (S1):Plaintext	cnMaestro TLS session	Z2	TLS MAES MS:Derived From AES GCM IV:Used With
AES GCM IV		Volatile (S1):Plaintext		Z2	TLS WEB SK:Used With TLS MAES MS:Used With TLS MAES SK:Used With
RSA WLS PRIV	Input with Electronic configuration from directly connected GPC (I2)	Non-volatile (S2):Encrypted		Z1	RSA WLS PUB1:Paired With KoK:Encrypted by
RSA WLS PUB1	Input with Electronic configuration from directly connected GPC (I2)	Non-volatile (S2):Encrypted		Z1	RSA WLS PRIV:Paired With KoK:Encrypted by
RSA WLS PUB2		Volatile (S1):Plaintext	Wireless TLS session	Z2	RSA WLS ROOT:Verified by
RSA WLS ROOT	Input with Electronic configuration from directly	Non-volatile (S2):Encrypted		Z1	RSA WLS PUB2:Used to verify KoK:Encrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	connected GPC (I2)				
PSK WLS	Input with Electronic configuration from directly connected GPC (I2)	Non-volatile (S2):Encrypted		Z1	KoK:Encrypted by
ECDHE WLS PRIV		Volatile (S1):Plaintext	Wireless TLS session	Z2	ECDHE WLS PUB1:Paired With TLS WLS MS:Used to establish ECDHE WLS PUB2:Used With
ECDHE WLS PUB1		Volatile (S1):Plaintext	Wireless TLS session	Z2	ECDHE WLS PRIV:Paired With TLS WLS MS:Used to establish ECDHE WLS PUB2:Used With
ECDHE WLS PUB2		Volatile (S1):Plaintext	Wireless TLS session	Z2	TLS WLS MS:Used to establish ECDHE WLS PRIV:Used With ECDHE WLS PUB1:Used With
TLS WLS MS		Volatile (S1):Plaintext	Wireless TLS session	Z2	TLS WLS SK1:Used to derive ECDHE WLS PRIV:Established from ECDHE WLS PUB1:Established from ECDHE WLS PUB2:Established from
TLS WLS SK1		Volatile (S1):Plaintext	Wireless TLS session	Z2	TLS WLS MS:Derived From TLS WLS SK2:Used to derive
TLS WLS SK2		Volatile (S1):Plaintext	Wireless TLS session	Z2	TLS WLS SK1:Derived From
SNMP AUTHPRIV LOC		Non-volatile (S2):Encrypted		Z1	SNMP AUTHPRIV PP:Derived From KoK:Encrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
SNMP AUTHPRIV PP	Input with Direct configuration from directly connected GPC (I1)	Volatile (S1):Plaintext	Until reboot	Z2	SNMP AUTHPRIV LOC:Used to derive
SNTP KEY	Input with Direct configuration from directly connected GPC (I1)	Non-volatile (S2):Encrypted		Z1	KoK:Encrypted by
PW DIGEST	Input with Electronic configuration from directly connected GPC (I2)	Non-volatile (S2):Encrypted		Z1	KoK:Encrypted by
HMAC KEY		Volatile (S1):Plaintext	Until user logs out	Z2	
RSA SSO PUB	Input with Electronic configuration from directly connected GPC (I2)	Non-volatile (S2):Encrypted		Z1	KoK:Encrypted by
DRBG STATE		Volatile (S1):Plaintext	Until next DRBG operation	Z2	CTR DRBG SEED:Derived From
EDDSA FW PUB			-	N/A	
EDDSA LIC PUB		Embedded (S4):Plaintext		N/A	
DSA LIC PUB		Embedded (S4):Plaintext		N/A	

Table 18: SSP Table 2

Note: No SSPs are entered into or output from the module in encrypted form.

10 Self-Tests

10.1 Pre-Operational Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

Pre-operational self–tests are available on demand by power cycling the Module.

The Module performs the following pre-operational self-tests in the table below

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity	32-bit CRC	KAT	SW/FW Integrity	Success: Module starts normally Failure: Module restarts in Recovery	32 bit CRC computed over firmware image for Main Application or Recovery.

Table 19: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The Module performs the following conditional self-tests in the table below

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CFB128 Encrypt (AES 2594)	AES-128, AES-192, AES-256	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Encrypt	Restart
AES-CFB128 Decrypt (AES 2594)	AES-128, AES-192, AES-256	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Decrypt	Restart
AES-CFB128 Encrypt (A4740)	AES-128	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Encrypt	Restart
AES-CFB128 Decrypt (A4740)	AES-128	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Decrypt	Restart
AES-ECB Encrypt (A4740)	AES-128, AES-256	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Encrypt	Restart
AES-ECB Encrypt (A4740)	AES-128, AES-256	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Decrypt	Restart
AES-GCM Encrypt (A4740)	AES-128, AES-256	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Encrypt	Restart
AES-GCM Decrypt (A4740)	AES-128, AES-256	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Decrypt	Restart

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
CSP entry	-	Duplicate entries	Manual Entry	Success: Module submits web page or navigates to next web page in Wizard interface. Failure: Module displays error message in dialog box and will not allow user to proceed until the error is resolved.	-	CSP entry for Key of Keys Entropy Wireless PSK SNTP key SNMP authentication SNMP privacy
CSP integrity	32-bit CRC	KAT	Critical Function	Module restarts Failure code	CRC checked before CSP is decrypted	Reading CSPs from non-volatile storage.
Counter DRBG (A4741)	AES ECB 128-bit	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Instantiate, Generate, and Reseed critical function tests are implemented in accordance with section 11.3 of [90A] as part of this Known Answer Test (KAT)	Restart
DSA SigVer (FIPS186-4) (A4740)	1024-bit 2048-bit	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Signature verification	Restart
ECDH	EC P-256 EC P-384	KAT	PCT	Success: Module operates normally Failure: Module restarts with failure code	Pair-wise consistency test upon key generation	Before generating EC key pair
ECDSA SigGen (FIPS186-5) (A4740)	EC P-256 EC P-384	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Signature generation	Restart
ECDSA SigVer (FIPS186-5) (A4740)	EC P-256 EC P-384	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Signature verification	Restart
EDDSA SigVer (A4740)	Ed25519	KAT	SW/FW Load	Web interface	Signature verification	Before writing replacement firmware to flash

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC SHA-1 (A4740) HMAC SHA2-256 (A4740) HMAC SHA2-384 (A4740)	SHA-1 SHA2-256 SHA2-384	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Message authentication	Restart
KAS-ECC-SSC Sp800-56Ar3 (A4740)	SHA2-256 SHA2-384	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Shared secret establishment	Restart
RSA SigVer (FIPS186-2) (A4740)	2048-bit	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Signature verification	Restart
RSA SigGen (FIPS186-4) (A4740)	2048-bit	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Signature generation	Restart
RSA SigVer (FIPS186-4) (A4740)	2048-bit	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Signature verification	Restart
SHA-1 SHA2-256 SHA2-384 SHA2-512	SHA-1 SHA2-256 SHA2-384 SHA2-512	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Digest generation	Restart
KDF SNMP (A4742)	HMAC SHA-1	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Key Derivation Algorithm using HMAC	Restart
TLS v1.3 KDF (A4740)	HMAC SHA2-256, HMAC SHA2-384	KAT	CAST	Success: Module starts normally Failure: Module restarts with failure code	Key derivation using TLS 1.3	Restart

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware integrity	KAT	SW/FW Integrity	On demand	Manually

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CFB128 Encrypt (AES 2594)	KAT	CAST	On Demand	Manually
AES-CFB128 Decrypt (AES 2594)	KAT	CAST	On Demand	Manually
AES-CFB128 Encrypt (A4740)	KAT	CAST	On Demand	Manually
AES-CFB128 Decrypt (A4740)	KAT	CAST	On Demand	Manually
AES-ECB Encrypt (A4740)	KAT	CAST	On Demand	Manually
AES-ECB Encrypt (A4740)	KAT	CAST	On Demand	Manually
AES-GCM Encrypt (A4740)	KAT	CAST	On Demand	Manually
AES-GCM Decrypt (A4740)	KAT	CAST	On Demand	Manually
CSP entry	Duplicate entries	Manual Entry	On Demand	Manually
CSP integrity	KAT	Critical Function	On Demand	Manually
Counter DRBG (A4741)	KAT	CAST	On Demand	Manually
DSA SigVer (FIPS186-4) (A4740)	KAT	CAST	On Demand	Manually
ECDH	KAT	PCT	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A4740)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A4740)	KAT	CAST	On Demand	Manually
EDDSA SigVer (A4740)	KAT	SW/FW Load	On Demand	Manually
HMAC SHA-1 (A4740) HMAC SHA2-256 (A4740) HMAC SHA2-384 (A4740)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A4740)	KAT	CAST	On Demand	Manually
RSA SigVer (FIPS186-2) (A4740)	KAT	CAST	On Demand	Manually
RSA SigGen (FIPS186-4) (A4740)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (A4740)	KAT	CAST	On Demand	Manually
SHA-1 SHA2-256 SHA2-384 SHA2-512	KAT	CAST	On Demand	Manually
KDF SNMP (A4742)	KAT	CAST	On Demand	Manually
TLS v1.3 KDF (A4740)	KAT	CAST	On Demand	Manually

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ES1	The module fails CAST, PCT, firmware integrity	The module enters the failure state	Reboot/Power cycle the module	The module restarts with a failure reset reason
ES2	The module fails firmware load test	The module returns to normal operation	None	The module rejects image upgrade with failure message
ES3	The module fails manual entry of CSPs	The module returns to normal operation	None	The module rejects the manual CSP entry with a web-dialog error message
ES4	The module fails CSP integrity check	The module enters the failure state	Reboot/Power cycle the module	The module zeroizes SSPs and restarts with a failure reset reason

Table 23: Error States

Failure of a pre-operational self-test or conditional self-test causes the module to reboot and subsequently repeat pre-operational self-tests. This could conceivably result in a continuous cycle of reboots; in which case an operator should use the Recovery mode to install alternative firmware. The error code is displayed as the reboot reason following successful restart.

Data output ports are disabled during self-tests.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The PTP 700 module operates exclusively in the Approved mode when the following procedures are followed.

Installation and Initialization:

The following steps must be performed in order to securely install, initialize, and start up the PTP 700 Point to Point Wireless Ethernet Bridge cryptographic module in the Approved mode of operation:

- Power up the module using an approved power supply referenced in the PTP 700 User Guide.
- Connect a general-purpose computer (GPC) to the Main PSU port of the module using a direct copper Ethernet connection.
- Configure the GPC to connect to the web management interface of the module in the 169.254.X.X network as described in the PTP 700 User Guide. The module has a default IP address of 169.254.1.1.
- At first use, the module is configured for identity-based authentication and requires the user to set a System Admin password of not less than fifteen characters.
- Install a License Key that includes the AES and FIPS licenses. This requires purchase of the upgrades and application of the resulting entitlement in the License Key Generator in Cambium Network Customer Support.
- Upgrade firmware to the latest FIPS validated release and reboot the module.
- On restart, the module zeroizes SSPs, configures identity-based authentication, and requires the user to specify a Security Officer username and password of not less than 15 characters. The initial Security Officer user can then create additional user accounts for other users as required. Configure the Key of Keys, Entropy, the HTTPS interface for secure web management, Wireless encryption and disable HTTP, using the direct cabled connection before connecting the module to a data network.

Once configured, the module operates in approved mode following power cycle or restart without further operator intervention.

Delivery:

The following steps must be performed in order to securely deliver the PTP 700 Point to Point Wireless Ethernet Bridge cryptographic module to the authorized operator:

- Check that the module is undamaged, and that tamper-evident barrels are intact, using the procedure provided in Section 7.1.

11.2 Administrator Guidance

Refer to the PTP 700 User Guide available for download from the Cambium Networks Customer Support web site.

11.3 Non-Administrator Guidance

Refer to the *PTP 700 User Guide* available for download from the Cambium Networks Customer Support web site.

11.4 Design and Rules

Rules of Operation

1. The Module provides five distinct roles: Security Officer (SO), System Administrator (SA), Installer (IN),Read Only (RO) and unauthenticated (U)..
2. The Module provides identity-based authentication.
3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate pre-operational self-tests by power cycling power or resetting the Module.
6. All self-tests do not require any operator action.
7. Data output is inhibited during manual SSP entry, pre-operational self-tests, software/firmware loading, zeroization and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module supports manual SSP establishment method for initial configuration, by direct connection of the management device.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module does not output plaintext CSPs. The Module allows input of plaintext CSPs as part of initial configuration, by direct connection of the management device.
15. The Module does not output intermediate key values.
16. The Module does not provide bypass services or ports/interfaces.

11.5 End of Life

Use the Zeroize CSPs function whenever the module is removed from service, redeployed, or retired. At End of Life, the module can be recycled using any recognized electronic equipment recycling method.

12 Mitigation of Other Attacks

The Module does not implement any mitigation method against other attacks.

References and Definitions

The following standards are referred to in this Security Policy.

Table 24 – References

Abbreviation_*	Full Specification Name
[FIPS140-3]	Security Requirements for Cryptographic Modules, March 22, 2019
[ISO19790]	International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017
[ISO24759]	International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015
[IG]	Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, February 26, 2025.
[131A]	Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019
[133]	NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020
[135]	National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.
[186]	National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.
[197]	National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197-upt1, May 9, 2023
[38A]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001
[38D]	National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007
[56Ar3]	NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018

Abbreviation_*	Full Specification Name
[90A]	National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.

Table 25 – Acronyms and Definitions

Acronym_*	Definition
APT	Adaptative Proportion Test
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
IN	Installer
KAT	Known Answer Test
KDF	Key Derivation Function
PCT	Pairwise Consistency Test
PTP	Point to Point
RCT	Repetitive Count Test
SA	System Administrator
SNMP	Simple Network Management Protocol
SO	Security Officer
SSO	Single Sign-On
SSP	Sensitive Security Parameter
TLS	Transport Layer Security