Cambium
PTP 820 FIPS 140-2 Security Policy

PTP 820C

PTP 820C-HP

PTP 820C 2E2SX

PTP 820S

PTP 820N

PTP 820A

PTP 820G

PTP 820GX

Firmware:

PTP820 Release 10.9.6b74

Hardware:

PTP 820N, PTP 820A, with components:

- PTP820 TCC-B-MC: N000082H001
- PTP820 TCC-B2: N000082H002
- PTP820 TCC-B2-XG-MC: N000082H003
- PTP820 RMC-B: N000082H004

PTP 820GX with components:

- PTP820 RMC-B: N000082H004

PTP 820G, PTP 820C, PTP 820C-HP, PTP 820C 2E2SX, PTP 820S

Phn-4339-002v000

Cambium Networks™

Prepared by:
Acumen Security
2400 Research Blvd
Rockville, MD 20850
www.acumensecurity.net

Contents

Figures

Tables

1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for Cambium Networks and the following Cambium Networks products: PTP 820C, PTP 820C-HP, PTP 820C 2E2SX, PTP 820S, PTP 820N, PTP 820A, PTP 820G, PTP 820GX. Below are the details of the certified products:

Hardware Version #:

- PTP 820N, PTP 820A, with components:
  - PTP820 TCC-B-MC: N000082H001
  - PTP820 TCC-B2: N000082H002
  - PTP820 TCC-B2-XG-MC: N000082H003
  - PTP820 RMC-B: N000082H004
- PTP 820GX with components:
  - PTP820 RMC-B: N000082H004
- PTP 820G, PTP 820C, PTP 820C-HP, PTP 820C 2E2SX, PTP 820S

Software Version #: PTP820 Release 10.9.6b74

FIPS 140-2 Security Level: 2

1.1 Purpose

This document was prepared as part of the Federal Information Processing Standard (FIPS) 140-2 validation process. The document describes how PTP 820C, PTP 820C-HP, PTP 820C 2E2SX, PTP 820S, PTP 820N, PTP 820A, PTP 820G, and PTP 820GX meet the security requirements of FIPS 140-2. It also provides instructions to individuals and organizations on how to deploy the product in a secure FIPS-approved mode of operation. The target audience of this document is anyone who wishes to use or integrate any of these products into a solution that is meant to comply with FIPS 140-2 requirements.

1.2 Document Organization

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

- Vendor Evidence document
- Finite State Machine
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Acumen Security, under contract to Cambium Networks. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Cambium Networks and is releasable only under appropriate non-disclosure agreements.

1.3 Notices

2. PTP 820C, PTP 820C-HP, PTP 820C 2E2SX, PTP 820S, PTP 820N, PTP 820A, PTP 820G, PTP 820GX

PTP 820C, PTP 820C-HP, PTP 820C 2E2SX, PTP 820S, PTP 820N, PTP 820A, PTP 820G, and PTP 820GX (the module) are multi-chip standalone modules validated at FIPS 140-2 Security Level 2. Specifically, the modules meet that following security levels for individual sections in FIPS 140-2 standard:

Table 1 - Security Levels

#	Section Title	Security Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	3
9	Self-Tests	2
10	Design Assurances	3
11	Mitigation Of Other Attacks	N/A

2.1 Cryptographic Module Specification

The PTP 820 series is a service-centric microwave platform for HetNet hauling. The platform includes a full complement of wireless products that provide innovative, market-leading backhaul and fronthaul solutions.

Powered by a software-defined engine and sharing a common operating system, PTP820 Release 10.9.6b74, the PTP 820 platform, delivers ultra-high capacities while supporting any radio transmission technology, any network topology, and any deployment configuration.

2.1.1 Cryptographic Boundary

The cryptographic boundary for the modules is defined as encompassing the "top," "front," "left," "right," and "bottom" surfaces of the case and all portions of the "backplane" of the case. The following figures provide a physical depiction of the cryptographic modules:

Figure 1 - PTP 820C

Figure 2 - PTP 820C-HP

Figure 3 - PTP 820C 2E2SX

Figure 4 - PTP 820S

Figure 5 - PTP 820N and PTP 820A

Figure 6 - PTP 820G

Figure 7 - PTP 820GX

The PTP 820G, PTP 820C, PTP 820C 2E2SX, PTP 820C-HP and PTP 820S are fixed configuration.

The PTP 820GX has slots for Radio Modem Card RMC-B (PTP820 RMC-B: N000082H004). The PTP820 RMC-B: N000082H004 provides the modem interface between the Indoor Unit (IDU) and the Radio Frequency Unit (RFU).

Finally, the PTP 820N and PTP 820A have slots to insert the following cards:

- Traffic and Control Card (TCC): The Traffic Control Card (TCC) provides the control functionality for the PTP 820N and PTP 820A units. It also provides Ethernet management and traffic interfaces. There are three variants of this card:
  - PTP820 TCC-B2-XG-MC: N000082H003: Required for Multi-Carrier ABC configurations. Provides 2 x FE Ethernet management interfaces, 2 x GbE optical interfaces, 2 x GbE electrical interfaces, and 2 x dual mode electrical or cascading interfaces.
  - PTP820 TCC-B-MC: N000082H001: Required for Multi-Carrier ABC configurations. Provides 2 x FE Ethernet management interfaces and 2 x GbE combo interfaces (electrical or optical) for Ethernet traffic.

- PTP820 TCC-B2: N000082H002: Provides 2 x FE Ethernet management interfaces, 2 x GbE optical interfaces, 2 x GbE electrical interfaces, and 2 x dual mode electrical or cascading interfaces.
- Radio Modem Card-B (PTP820 RMC-B: N000082H004): The Radio Modem Card (RMC) provides the modem interface between the Indoor Unit (IDU) and the Radio Frequency Unit (RFU).

Additionally, the following cards can be configured on PTP 820GX, PTP 820N, and PTP 820A modules. These cards provide port density but do not contain any security-relevant functionality:

- Ethernet/Optical Line Interface Card (E/XLIC)
- STM-1/OC3
- STM-1 RST
- E1/T1
- 10Gb Ethernet/Optical Line Interface Card (LIC-X-E10)
- Radio Interface Card (RIC-D)

The models included in this FIPS validation have been tested in the following configurations:

Table 2 - Tested Configurations

Model	Cards
PTP 820N	• Single or dual TCC • Dual **PTP820 RMC-B: N000082H004** • Dual Power supplies
PTP 820A	• Single or dual TCC • Dual **PTP820 RMC-B: N000082H004** • Dual Power supplies
PTP 820G	Fixed configuration
PTP 820GX	• Dual **PTP820 RMC-B: N000082H004**
PTP 820C	Fixed configuration
PTP 820C-HP	Fixed configuration
PTP 820C 2E2SX	Fixed configuration
PTP 820S	Fixed configuration

2.1.2 Modes of Operation

The modules have a single mode of operation which is the FIPS-Approved mode (when configured as per the instructions in Section 3: *Secure Operation)*. Any usage of the Non-FIPS Approved services described in Table 13 would result in non-Approved operation.

The following table lists the FIPS approved algorithms supported by the modules:

Table 3 - Supported Algorithms

Cryptographic Algorithm	CAVP Cert. #	Usage
Firmware Cryptographic Implementation		
AES CBC (e/d; 128, 256); ECB (e/d; 128); CTR (int only; 256); CFB128 (e/d; 128) GCM[1] (e/d; 128, 256; 192 tested but not used) KW (AE , AD , AES-256 , INV , 128 , 256 , 192 , 320 , 4096)	4017	Used for control/management plane encryption/decryption
SHS SHA-1 (BYTE-only) SHA-224 (BYTE-only, tested but not used) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	3313	Used for control/management plane message digests. SHA-1 is permitted within SSH and IPSec protocols, and legacy signature verification only.
HMAC HMAC-SHA1 (Key Size Ranges Tested: KS<BS KS=BS KS>BS) HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS) HMAC-SHA384 (Key Size Ranges Tested: KS<BS KS=BS KS>BS) HMAC-SHA512 (Key Size Ranges Tested: KS<BS KS=BS KS>BS)	2619	Used for control/management plane message authentication
SP 800-90A DRBG (HMAC-SHA-256) HMAC_Based DRBG: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256)	1195	Used for control/management plane random bit generation

[1] GCM IV generation tested in accordance with IG A.5, scenario 1 (TLS). The IV is generated only for use with GCM encryption within the TLSv1.2 protocol. The ciphersuites supported by the module are identified in section 3.3.2 of this document.

Cryptographic Algorithm	CAVP Cert. #	Usage
FIPS 186-4 RSA Key Generation, Signature Generation and Signature Verification 186-4KEY(gen): FIPS186-4_Random_e PGM (ProbPrimeCondition): 2048 PPTT:(C.3) ALG[ANSIX9.31] Sig(Gen): (2048 SHA(256 , 384 , 512)) (3072 SHA(256 , 384 , 512)) Sig(Ver): (1024 SHA(1 , 256 , 384 , 512)) (2048 SHA(1 , 256 , 384 , 512)) (3072 SHA(1 , 256 , 384 , 512)) ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(224 , 256 , 384 , 512)) (3072 SHA(224 , 256 , 384 , 512)) SIG(Ver) (1024 SHA(1 , 224 , 256 , 384)) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 , 224 , 256 , 384 , 512)) [RSASSA-PSS]: Sig(Gen): (2048 SHA(224 , 256 , 384 , 512)) (3072 SHA(224 , 256 , 384 , 512)) Sig(Ver): (1024 SHA(1 SaltLen(128) , 224 SaltLen(128) , 256 SaltLen(128) , 384 SaltLen(128) , 512 SaltLen(128))) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 SaltLen(128) , 224 SaltLen(128) , 256 SaltLen(128) , 384 SaltLen(128) , 512 SaltLen(128)))	2060	Used for control/management plane key generation, signature generation, and signature verification
CVL (SNMPv3, SSH and TLS)[2] TLSv1.2 (SHA-256) SSH (SHA-1, 256) SNMP (SHA-1)	840	Used for key derivation within management protocols
CVL (IKEv1 SHA-256; tested but not used on Freescale P1012 based platforms)	C1315	Used for key derivation within IPsec
KTS (key establishment methodology provides 256 bits of encryption strength)	AES: 4017	Used for key transport on the data plane
KTS[3] (key establishment methodology provides 128 or 256 bits of encryption strength)	AES: 4017 HMAC: 2619	Used for key transport on the mnagement plane

[2] Note that CAVP and CMVP has not reviewed or tested the SSH, SNMPv3, IKEv1 and TLS protocols

[3] The management plane implements KTS using both AES (CBC and GCM modes) and optionally HMAC. If negotiating a GCM-based TLS cipher suite, then only GCM is used for the KTS function.

Cryptographic Algorithm	CAVP Cert. #	Usage
CKG[4] (vendor affirmed)	N/A	Symmetric key and asymmetric seed generation
KAS-SSC[5] (vendor affirmed) •dhEphem (2048- and 3072-bit safe primes •Ephemeral Unified (P-256 curve)	N/A	Diffie-Hellman and Elliptic Curve Diffie-Hellman Key Agreement
Kernel Cryptographic Implementation		
AES-CBC (e/d; 256; tested but not used on Freescale P1012 based platforms)	C1316	Used for data encryption/decryption within IPsec
HMAC-SHA-256 (Key Size Ranges Tested: KS<BS; tested but not used on Freescale P1012 based platforms)	C1316	Used for message authentication within IPSec
SHA-256 (BYTE-only; tested but not used on Freescale P1012 based platforms)	C1316	Used for message digests within IPsec
Hardware Cryptographic Implementation		
AES OFB (e/d; 256)	4014	Used for data plane encryption/decryption

Note that there are algorithms, modes, and keys that have been CAVS tested but not implemented by the module. Only the algorithms, modes, and keys shown in this table are implemented by the module.

Additionally, the module implements the following non-Approved algorithms that are allowed for use with FIPS-approved services:

- RSA (key unwrapping; key establishment methodology provides 112 bits of encryption strength)[6]
- Non-approved NDRNG for seeding the DRBG. The NDRNG generates a minimum of 256 bits of entropy for use in key generation.

The module supports the following algorithms in a non-Approved mode of operation.

- MD5

When configured to operate in the FIPS-Approved mode of operation as described in Section 3, the module does not provide any non-Approved algorithms. Usage of the Non-FIPS Approved services described in Table 13 will result in the module operating in a non-Approved mode.

[4] In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic KeyGeneration (CKG) as per SP800-133 (vendor affirmed). The resulting generated symmetric keys and the seed used in the asymmetric key generation are the unmodified output from an NIST SP 800-90A DRBG.

[5] Vendor affirmed in accordance with SP 800-56Ar3 as per IG D.1rev3, D.3, and D.8 X1. Safe primes are implemented in accordance with RFC 4492, 7919, and 3526.

[6] The module supports PKCS#1-v1.5 padding

2.2 Cryptographic Module Ports and Interfaces

The modules provide a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2-defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are described in the following tables:

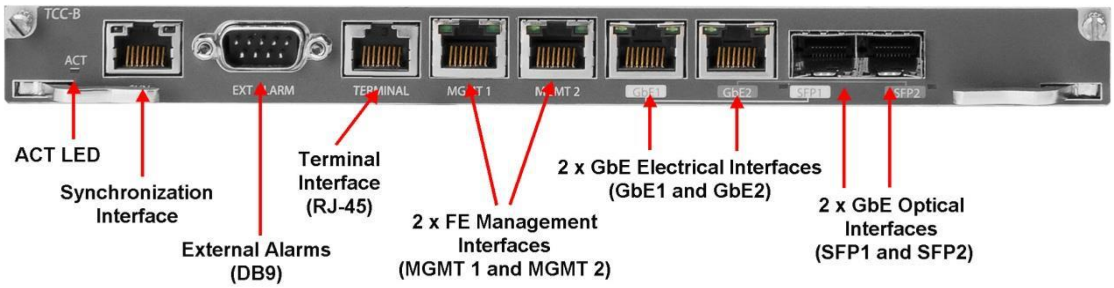

Figure 8 - PTP820 TCC-B-MC: N000082H001 Interfaces

Table 4 - Module Interface Mapping for PTP820 TCC-B-MC: N000082H001 (PTP 820N and PTP 820A)

FIPS Interface	Physical Interface
Data Input	(2x) GbE Electrical Interfaces or GbE Optical Interfaces
Data Output	(2x) GbE Electrical Interfaces or GbE Optical Interfaces
Control Input	(1x) Synchronization Interface (1x) RJ-45 Terminal Interface (2x) FE Management Interfaces (2x) GbE Electrical Interfaces or GbE Optical Interfaces
Status Output	(1x) RJ-45 Terminal Interface (2x) FE Management Interfaces (1x) ACT LED (1x) DB9 External Alarms (2x) GbE Electrical Interfaces or GbE Optical Interfaces

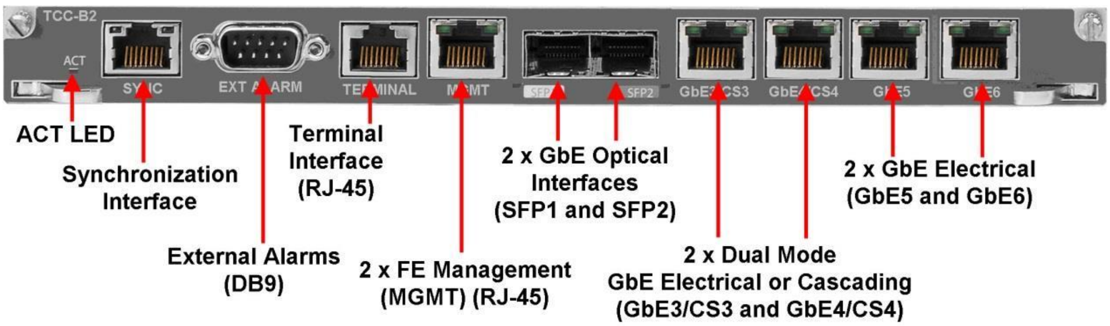

Figure 9 - PTP820 TCC-B2: N000082H002 and PTP820 TCC-B2-XG-MC: N000082H003 Interfaces

Table 5 - Module Interface Mapping for PTP820 TCC-B2: N000082H002 and PTP820 TCC-B2-XG-MC: N000082H003 (PTP 820N and PTP 820A)

FIPS Interface	Physical Interface
Data Input	(2x) GbE Optical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Electrical Interfaces
Data Output	(2x) GbE Optical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Electrical Interfaces
Control Input	(1x) Synchronization Interface (1x) RJ-45 Terminal Interface (2x) FE Management Interfaces
Status Output	(1x) RJ-45 Terminal Interface (2x) FE Management Interfaces (1x) ACT LED (1x) DB9 External Alarms

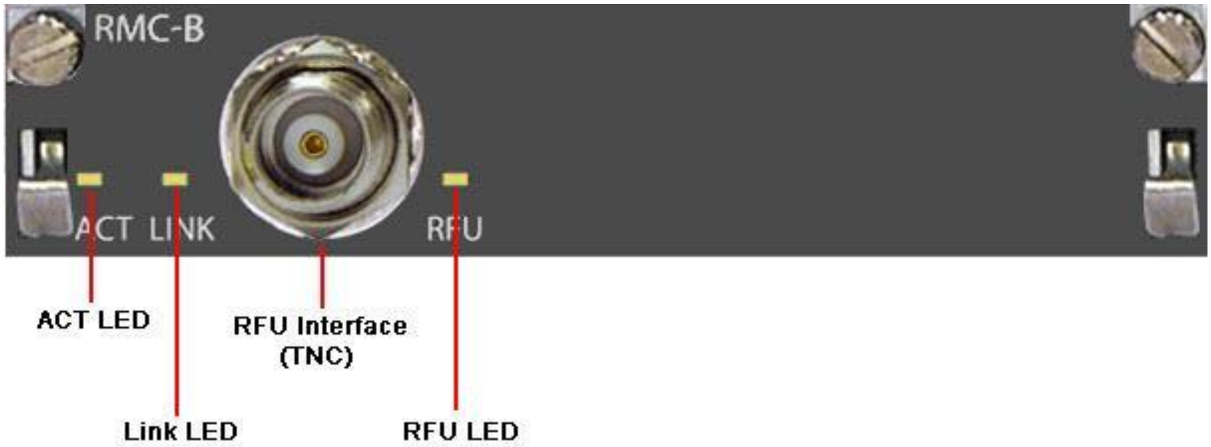

Figure 10 - PTP820 RMC-B: N000082H004 Interfaces

Table 6 - Module Interface Mapping for PTP820 RMC-B: N000082H004 (PTP 820N and PTP 820A)

FIPS Interface	Physical Interface
Data Input	(1x) TNC RFU Interface
Data Output	(1x) TNC RFU Interface
Control Input	(1x) TNC RFU Interface
Status Output	(1x) ACT LED (1x) Link LED (1x) RFU LED

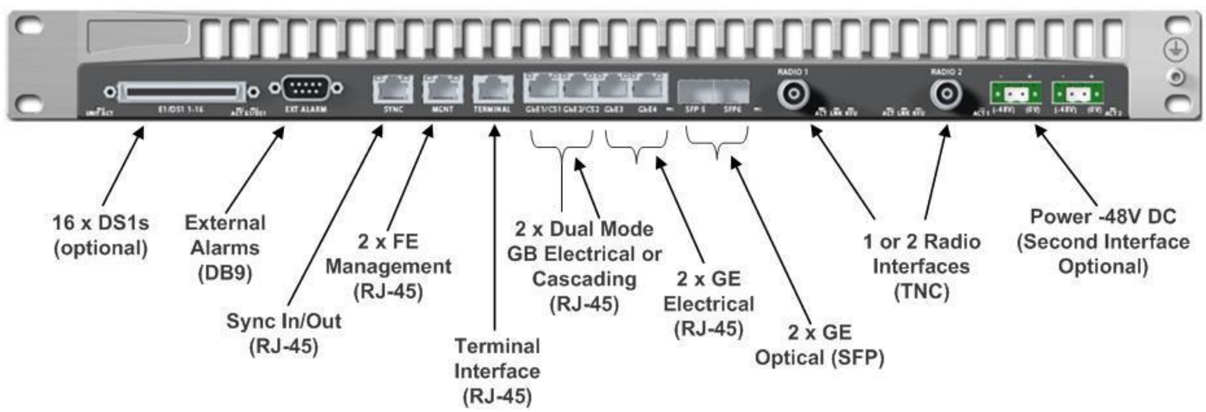

Figure 11 - PTP 820G Interfaces

Table 7 - Module Interface Mapping for PTP 820G

FIPS Interface	Physical Interface
Data Input	(2x) GbE Electrical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Optical Interfaces (16x) E1/DS1s
Data Output	(2x) GbE Electrical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Optical Interfaces (2x) TNC Radio Interfaces
Control Input	(1x) Sync In/Out RJ-45 Interface (1x) RJ-45 Terminal Interface (2x) FE Management Interfaces
Status Output	(1x) RJ-45 Terminal Interface (2x) FE Management Interfaces (1x) DB9 External Alarms LEDs

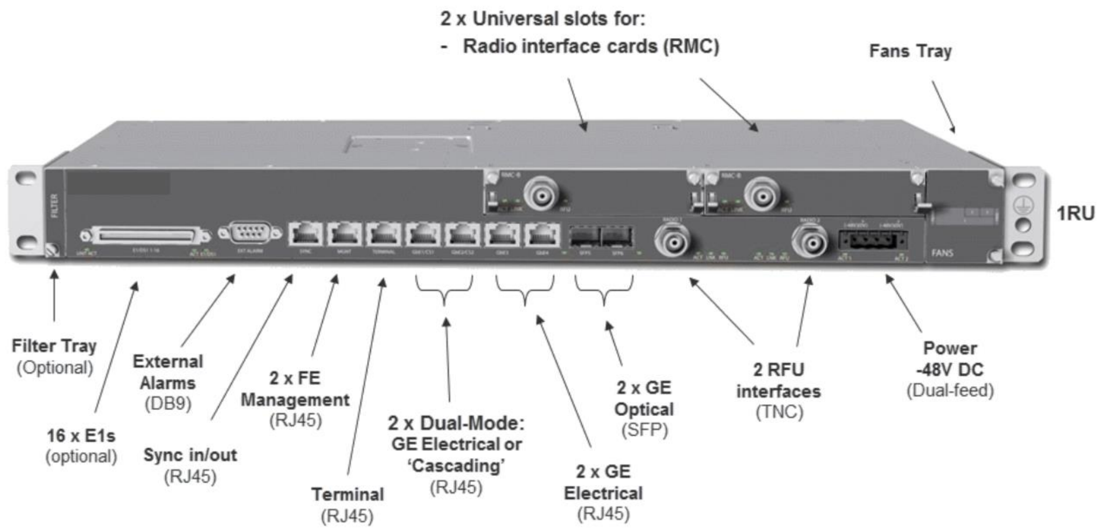

Figure 12 - PTP 820GX Interfaces

Table 8 - Module Interface Mapping for PTP 820GX

FIPS Interface	Physical Interface
Data Input	(2x) GbE Electrical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Optical Interfaces (16x) E1/DS1s (2x) PTP820 RMC-B: N000082H004 (optional)
Data Output	(2x) GbE Electrical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Optical Interfaces (2x) TNC Radio Interfaces (2x) PTP820 RMC-B: N000082H004 (optional)
Control Input	(1x) Sync In/Out RJ-45 Interface (1x) RJ-45 Terminal Interface (2x) FE Management Interfaces
Status Output	(1x) RJ-45 Terminal Interface (2x) FE Management Interfaces (1x) DB9 External Alarms LEDs

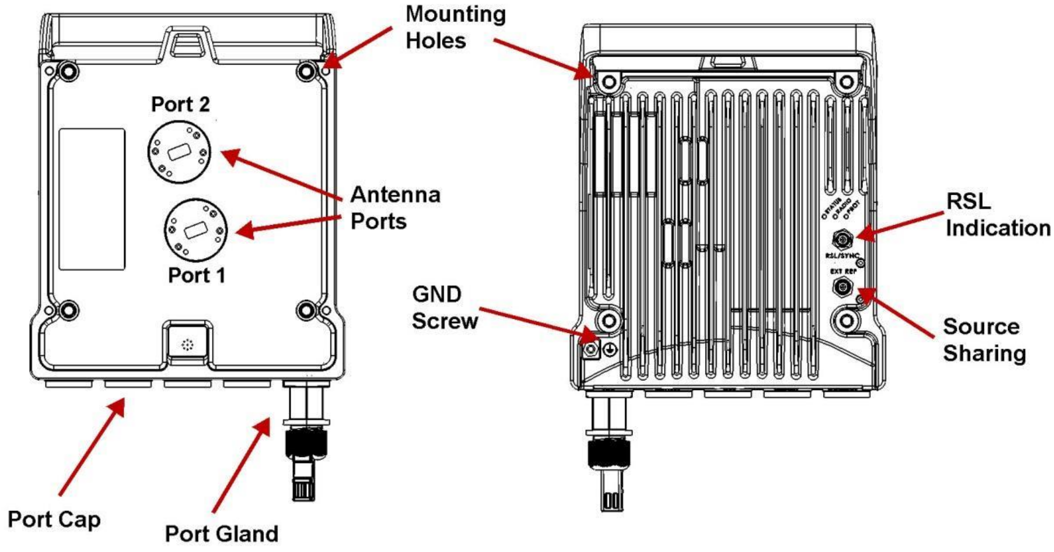

Figure 13 - PTP 820C Interfaces (Front and Back)

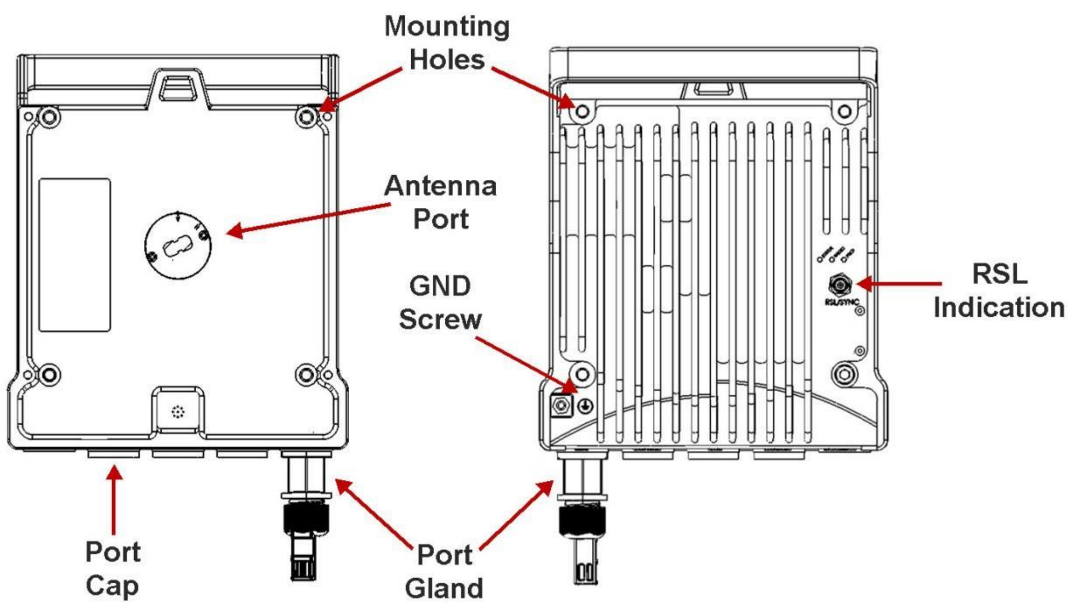

Figure 14 - PTP 820S Interfaces (Front and Back)

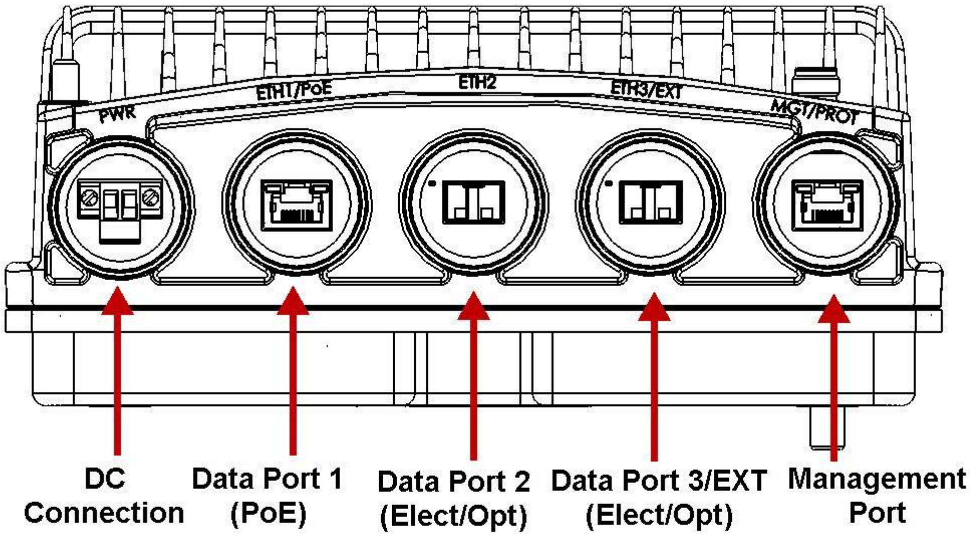

Figure 15 - PTP 820C and PTP 820S Interfaces Side

Table 9 - Module Interface Mapping for PTP 820C and PTP 820S

FIPS Interface	Physical Interface
Data Input	(1x) RJ-45 Data Port (PoE) (2x) Data port (Electrical or Optical) (2x) Antenna Ports (Only 1 port on PTP 820S)
Data Output	(1x) RJ-45 Data Port (PoE) (2x) Data port (Electrical or Optical) (2x) Antenna Ports (Only 1 port on PTP 820S)
Control Input	(1x) Source Sharing (only on PTP-820C) (1x) RJ-45 Management Interface
Status Output	(1x) RSL Indication (1x) RJ-45 Management Interface

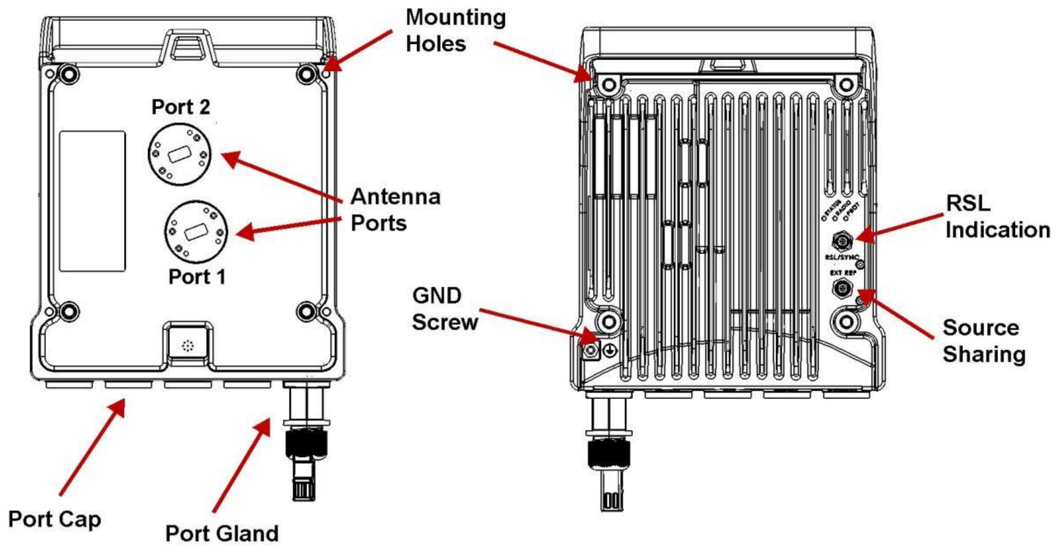

Figure 16 - PTP 820C 2E2SX Interfaces (Front and Back)

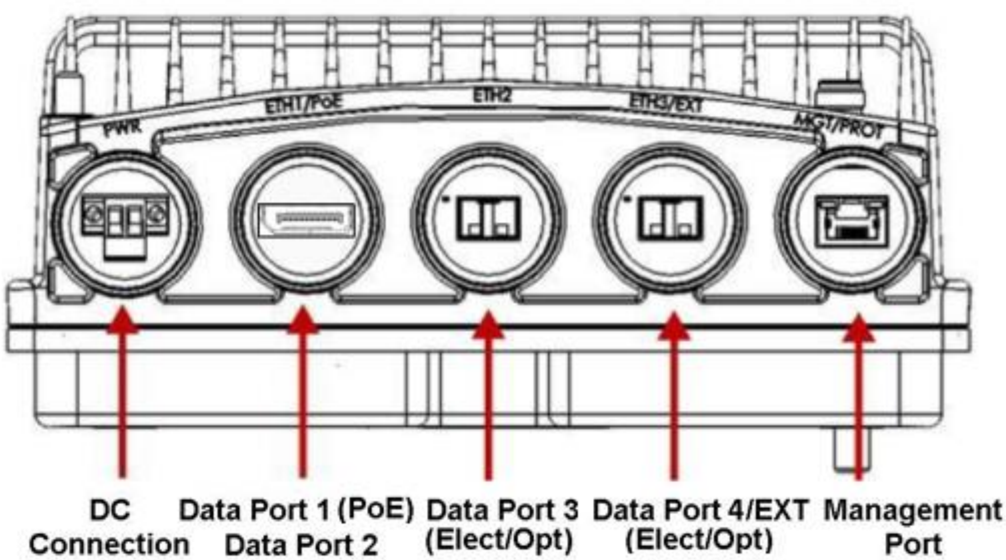

Figure 17 - PTP 820C 2E2SX Interfaces Side

Table 10 - Module Interface Mapping for PTP-820C 2E2SX

FIPS Interface	Physical Interface
Data Input	(2x) Data port (Electrical) - via a single DisplayPort connector (one with PoE) (2x) Data port (Electrical or Optical) (2x) Antenna Ports
Data Output	(2x) Data port (Electrical) - via a single DisplayPort connector (one with PoE) (2x) Data port (Electrical or Optical) (2x) Antenna Ports
Control Input	(1x) Source Sharing (1x) RJ-45 Management Interface
Status Output	(1x) RSL Indication (1x) RJ-45 Management Interface

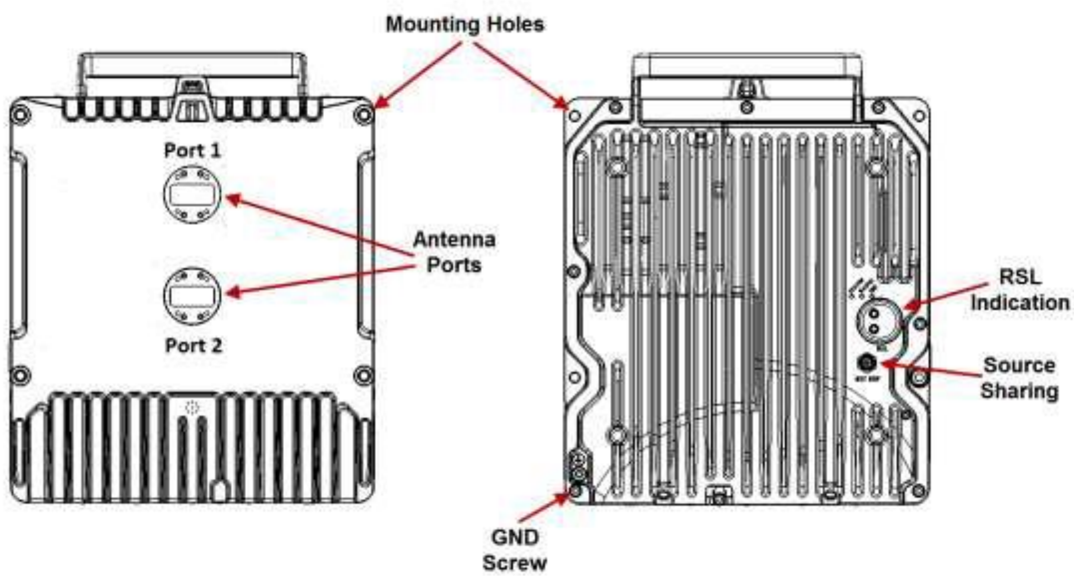

Figure 18 - PTP 820C-HP Interfaces (Front and Back)

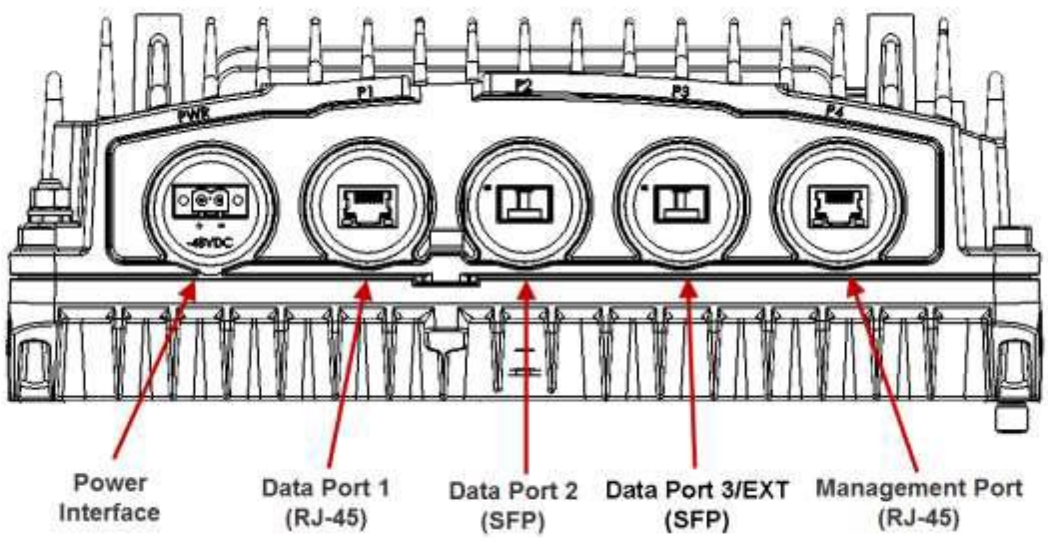

Figure 19 - PTP 820C-HP Interfaces Side

Table 11 - Module Interface Mapping for PTP 820C-HP

FIPS Interface	Physical Interface
Data Input	(1x) RJ-45 Data Port (2x) Data port (Electrical or Optical) (2x) Antenna Ports
Data Output	(1x) RJ-45 Data Port (2x) Data port (Electrical or Optical) (2x) Antenna Ports
Control Input	(1x) Source Sharing (1x) RJ-45 Management Interface
Status Output	(1x) RSL Indication (1x) RJ-45 Management Interface

2.3 Roles, Services, and Authentication

The following sections provide details about roles supported by the module, how these roles are authenticated, and the services the roles are authorized to access.

2.3.1 Authorized Roles

The module supports several different roles, including multiple Cryptographic Officer roles and a User role.

Configuration of the module can occur over several interfaces and at different levels depending upon the role assigned. There are multiple levels of access for a Cryptographic Officer as follows:

- **Security Officer, admin, SNMP User:** Entities assigned this privilege level have complete access to configure and manage the module.
- **Tech, Operator, Viewer:** These entities have more limited access to manage the module. For example, they can only manage the configuration of the data traffic interface.

The Users of the module are the remote peers to and from which backhaul traffic is transmitted. The Users are connected over a secure session protected using Session key.

2.3.2 Authentication Mechanisms

The module supports role-based authentication. Module operators must authenticate to the module before being allowed access to services, which requires the assumption of an authorized role. The module employs the authentication methods described in the table below to authenticate Crypto-Officers and Users.

Unauthenticated users are only able to access the module LEDs and power cycle the module.

Table 12 - Authentication Mechanism Details

Role	Type Of Authentication	Authentication Strength
Admin Tech Viewer Operator Security Officer SNMP User	Password/Username	All passwords must be at least 8 characters and may include letters, numbers, and special characters. If (8) integers are used for an eight digit password, the probability of randomly guessing the correct sequence is less than one (1) in 1,000,000 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 integer digits, 33 special characters, and 52 letter characters. The calculation should be 95^8 = 6,634,204,312,890,625). Therefore, the associated probability of a successful random attempt is less than 1 in 1,000,000 required by FIPS 140-2. In order to successfully guess the sequence in one minute would require the ability to make over 110,570,071,881,510 guesses per second, which far exceeds the operational capabilities of the module.

Role	Type Of Authentication	Authentication Strength
Users	AES 256-bit Session Key	When using AES key based authentication, the key has a size of 256-bits. Therefore, an attacker would have a 1 in 2^{256} chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. For AES based authentication, to exceed a 1 in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately $3.25X10^{32}$ attempts per minute, which far exceeds the operational capabilities of the modules to support.

2.3.3 Services

The services (approved and non-approved) that require operators to assume an authorized role (Crypto-Officer or User) as well as unauthenticated services are listed in the table below. Please note that the keys and Critical Security Parameters (CSPs) listed below use the following indicators to show the type of access required:

- **R (Read):** The CSP is read
- **W (Write):** The CSP is established, generated, or modified,
- **Z (Zeroize):** The CSP is zeroized

Table 13 - Services, Roles and Key/CSP access

Service	Description	Role		Key/CSP and Type of Access
		CO	**User**	
FIPS Approved Services				
Show Status	Provides status of the module	X		N/A
Perform Self-Tests	Used to initiate on-demand self-tests (via power-cycle)	X	X	N/A
Change Password	Update password with a new value	X		Crypto Officer Password (R/W)
Transmit/Receive Data	Encrypt/Decrypt data passing through the module		X	Session Key Tx (R/W/Z) Session Key Rx (R/W/Z) Master Key (R)

Service	Description	Role		Key/CSP and Type of Access
		CO	**User**	
Administrative access over SSH	Secure remote command line appliance administration over an SSH tunnel.	X		DRBG entropy input (R) DRBG Seed (R) DRBG V (R/W/Z) DRBG Key (R/W/Z) Diffie-Hellman / EC Diffie Hellman Shared Secret (R/W/Z) Diffie Hellman / EC Diffie Hellman private key (R/W/Z) Diffie Hellman / EC Diffie Hellman public key (R/W/Z) SSH Private Key (R/W) SSH Public Key (R/W) SSH Session Key (R/W/Z) SSH Integrity Key (R/W/Z)
Administrative access over Web EMS	Secure remote GUI appliance administration over a TLS tunnel.	X		DRBG entropy input (R) DRBG Seed (R) DRBG V (R/W/Z) DRBG Key (R/W/Z) Diffie-Hellman / EC Diffie Hellman Shared Secret (R/W/Z) Diffie Hellman / EC Diffie Hellman private key (R/W/Z) Diffie Hellman / EC Diffie Hellman public key (R/W/Z) TLS Private Key (R/W) TLS Public Key (R/W) TLS Pre-Master Secret (R/W/Z) TLS Session Encryption Key (R/W/Z) TLS Session Integrity Key (R/W/Z)
SNMPv3	Secure remote SNMPv3-based system monitoring.	X		SNMP Session Key (R/W/Z) SNMP Session Authentication Key (R/W/Z) SNMPv3 password (R/W/Z)
Key Entry	Enter key over management interfaces	X		Master Key (R/W)

Service	Description	Role		Key/CSP and Type of Access
		CO	**User**	
IPSec[7]	Control plane traffic encryption using IKEv1 for key exchange	X		IKE session encrypt key (R/W/Z) IKE session authentication key (R/W/Z) ISAKMP preshared key (R/W) IPsec encryption key (R/W/Z) IPsec authentication key (R/W/Z)
Zeroize	Zeroize all CSPs	X		All CSPs (Z)
Cycle Power	Reboot of module	Unauthenticated		DRBG entropy input (Z) DRBG Seed (Z) DRBG V (Z) DRBG Key (Z) Diffie-Hellman / EC Diffie Hellman Shared Secret (Z) Diffie Hellman / EC Diffie Hellman private key (Z) Diffie Hellman / EC Diffie Hellman public key (Z) SSH Session Key (Z) SSH Integrity Key (Z) SNMPv3 session key (Z) SNMPv3 session authentication key TLS Pre-Master Secret (Z) TLS Session Encryption Key (Z) TLS Session Integrity Key (Z) IKE session encrypt key (Z) IKE session authentication key (Z) IPsec encryption key (Z) IPsec authentication key (Z) Session Key Tx (Z) Session Key Rx (Z)
Status LED Output	View status via the modules' LEDs	Unauthenticated		N/A
Non-FIPS Approved Services				
SNMPv1/v2c	Secure remote SNMPv1, v2c-based system monitoring.	X		N/A
RADIUS	RADIUS authentication (MD5)	X		N/A

[7] Only available on MIPS CPU based models

Service	Description	Role		Key/CSP and Type of Access
		CO	**User**	
HTTP	Plaintext HTTP	X		N/A
Netconf	Netconf	X		N/A
Hot Standby	Hot Standby	X		N/A

R – Read, W – Write, Z – Zeroize

Table 14 – Non-Security Relevant Services

Service	Description	Role	
		CO	**User**
View Summaries	View unit summary information (Unit, Radio, Security)	X	
Platform Management	Shelf management, unit configuration, interfaces, software settings, activation key, and statistics	X	
Fault Management	Alarm settings	X	
Radio Configuration	Radio interface settings	X	
Ethernet Configuration	Ethernet interface settings	X	
Sync Settings	Manage synchronization	X	
Utilities	Generic utilities	X	

2.4 Physical Security

The appliances are multi-chip standalone cryptographic modules. The appliances are contained in a hard metal chassis, which is defined as the cryptographic boundary of the module. The appliances' chassis is opaque within the visible spectrum. The enclosure of the appliances has been designed to satisfy Level 2 physical security requirements.

Each of the appliances needs Tamper Evidence Labels to meet Security Level 2 requirements. These labels are installed at the factory before delivery to the customer.

The Crypto Officer shall periodically (defined by organizational security policy, recommendation is once a month) monitor the state of all applied seals for evidence of tampering. If tamper is detected, the CO must take the device out of commission, inspect it and if deemed safe, return it to FIPS approved state.

2.5 Operational Environment

Section 4.6.1 (of FIPS 140-2 standard) requirements are not applicable since the module is a hardware module with a non-modifiable operational environment.

2.6 Cryptographic Key Management

The following table identifies each of the CSPs associated with the modules. For each CSP, the following information is provided:

- The name of the CSP/Key
- The type of CSP and associated length
- A description of the CSP/Key
- Storage of the CSP/Key
- The zeroization for the CSP/Key

Table 15 - Details of Cryptographic Keys and CSPs

Key/CSP	Type	Description	Storage	Generated/Entry/Output	Zeroization
DRBG entropy input	256-bit	This is the entropy for SP 800-90A RNG.	RAM	Generated using entropy source	Device power cycle.
DRBG Seed	256-bit	This DRBG seed is collected from the onboard hardware entropy source.	RAM	Generated using entropy source	Device power cycle.
DRBG V	256-bit	Internal V value used as part of SP 800-90A DRBG	RAM	Generated using entropy source	Device power cycle.
DRBG Key	256-bit	Internal Key value used as part of SP 800-90A DRBG	RAM	Generated using entropy source	Device power cycle.
Diffie-Hellman / EC Diffie Hellman Shared Secret	DH 2048 bits and 3072 bits ECDH: P-256	The shared exponent used in Diffie-Hellman (DH)/ECDH exchange. Created per the Diffie-Hellman protocol.	RAM	Established using DH/ECDH	Device power cycle.
Diffie Hellman / EC Diffie Hellman private key	DH 2048 bits and 3072 bits ECDH: P-256	The private exponent used in Diffie-Hellman (DH)/ECDH exchange.	RAM	Generated using DRBG	Device power cycle.

Key/CSP	Type	Description	Storage	Generated/Entry/Output	Zeroization
Diffie Hellman / EC Diffie Hellman public key	DH 2048 bits and 3072 bits ECDH: P-256	The p used in Diffie-Hellman (DH)/ECDH exchange.	RAM	Generated using DRBG	Device power cycle.
SSH Private Key	RSA (Private Key) 2048 bits	The SSH private key for the module used for session authentication.	Flash	Generated using FIPS 186-4 / Entered electronically in encrypted form	Zeroization command
SSH Public Key	RSA (Public Key) 2048 bits	The SSH public key for the module used for session authentication.	Flash	Generated using FIPS 186-4 / Entered electronically in encrypted form	Zeroization command
SSH Session Key	AES 256 bits	The SSH session key. This key is created through SSH key establishment.	RAM	Established using SSH key exchange and derived using SP 800-135rev1 KDF	Device power cycle.
SSH Integrity Key	HMAC-SHA-1	The SSH data integrity key. This key is created through SSH key establishment.	RAM	Established using SSH key exchange and derived using SP 800-135rev1 KDF	Device power cycle.
SNMPv3 password	Shared Secret, at least eight characters	This secret is used to derive HMAC-SHA1 key for SNMPv3 Privacy or Authentication.	Flash	Entered electronically in encrypted form	Zeroization command
SNMPv3 session key	AES 128 bits	SNMP symmetric encryption key used to encrypt/decrypt SNMP traffic.	RAM	Established as part of SNMPv3 session using SP 800-135rev1 KDF	Device power cycle.
SNMPv3 session authentication key	HMAC-SHA-1	SNMP authentication key used to authenticate SNMP payloads	RAM	Established as part of SNMPv3 session using SP 800-135rev1 KDF	Device power cycle.
TLS Private Key	RSA (Private Key) 2048 bits	This private key is used for TLS session authentication.	Flash	Generated using FIPS 186-4	Zeroization command
TLS Public Key	RSA (Public Key) 2048 bits	This public key is used for TLS session authentication.	Flash	Generated using FIPS 186-4	Zeroization command

Key/CSP	Type	Description	Storage	Generated/Entry/Output	Zeroization
TLS Pre-Master Secret	Shared Secret, 384 bits	Shared Secret created using asymmetric cryptography from which new TLS session keys can be created.	RAM	Established using TLS exchange	Device power cycle.
TLS Session Encryption Key	AES 128 or 256 bits	Key used to encrypt/decrypt TLS session data.	RAM	Established using TLS exchange and derived using SP 800-135rev1 KDF	Device power cycle.
TLS Session Integrity Key	HMAC SHA-256 HMAC SHA-384	HMAC used for TLS data integrity protection.	RAM	Established using TLS exchange and derived using SP 800-135rev1 KDF	Device power cycle.
IKE session encrypt key	AES 256 bits	The IKE session encrypt key is created per the Internet Key Exchange Key Establishment protocol.	RAM	Established using IKE exchange and derived using SP 800-135rev1 KDF	Device power cycle.
IKE session authentication key	HMAC-SHA-256	The IKE session authentication key is created per the Internet Key Exchange Key Establishment protocol.	RAM	Established using IKE exchange and derived using SP 800-135rev1 KDF	Device power cycle
ISAKMP preshared	Secret 32 characters	The ISAKMP preshared key is used to derive the IKE session encrypt and authentication keys	Flash	Entered electronically in encrypted form	Zeroization command
IPsec encryption key	AES 256 bits	The IPsec encryption key is created per the Internet Key Exchange Key Establishment protocol.	RAM	Established using IKE exchange	Device power cycle.
IPsec authentication key	HMAC-SHA-256	The IPsec authentication key is created per the Internet Key Exchange Key Establishment protocol.	RAM	Established using IKE exchange	Device power cycle.
Session key Tx	AES 256 bits	This is the symmetric session key to protect transmission of back-haul data	RAM	Generated using DRBG. Wrapped and output using Master key	Device power cycle.

Key/CSP	Type	Description	Storage	Generated/Entry/Output	Zeroization
Session key Rx	AES 256 bits	This is the symmetric session key to decrypt back-haul data received by the module	RAM	Generated using DRBG. Input and unwrapped using Master key	Device power cycle.
Master key	AES 256 bits	This is the CO configured key used to protect transmission of session keys	Flash	Electronically entered in encrypted form	Zeroization command
Crypto Officer Password	Password	Authentication password for CO role	Flash	Electronically entered in encrypted form	Zeroization command

2.6.1 Key Generation

The module generates symmetric and asymmetric keys in compliance with the requirements of the FIPS 140-2 standard. Specifically symmetric keys are generated using output of the FIPS approved SP 800-90A DRBG and in compliance with IG 7.8. Asymmetric keys are generated as part applicable key generation standards. See Table 15 - Details of Cryptographic Keys and CSPs for details.

2.6.2 Key Entry/Output

See Table 15 - Details of Cryptographic Keys and CSPs for details. All keys are entered into or output from the module in a secure manner. Specifically, the Session Keys are output from the module encrypted with a Master Key with the AES key wrap algorithm.

2.6.3 Zeroization Procedures

See Table 15 - Details of Cryptographic Keys and CSPs for details.

2.7 Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)

The module conforms to FCC Part 15 Class B requirements for home use.

2.8 Self-Tests

Self-tests are health checks that ensure that the cryptographic algorithms within the module are operating correctly. The self-tests identified in FIPS 140-2 broadly fall within two categories:

1 Power-On Self-Tests

2 Conditional Self-Tests

2.8.1 Power-On Self-Tests

The cryptographic module performs the following self-tests at Power-On:

Firmware (Management Security Algorithms):

- Firmware Integrity Test (HMAC-SHA-1)
- HMAC-SHA-1 Known Answer Test
- HMAC-SHA-256 Known Answer Test
- HMAC-SHA-384 Known Answer Test
- HMAC-SHA-512 Known Answer Test
- AES-128 ECB Encrypt Known Answer Test
- AES-128 ECB Decrypt Known Answer Test
- AES KeyWrap Encrypt Known Answer Test

- AES KeyWrap Decrypt Known Answer Test
- AES-256 GCM Encrypt Known Answer Test
- AES-256 GCM Decrypt Known Answer Test
- RSA Sign/Verify Known Answer Test
- DRBG Known Answer Test
- DRBG Health Tests

Firmware (Kernel Crypto):

- AES-256 CBC Encrypt Known Answer Test
- AES-256 CBC Decrypt Known Answer Test
- HMAC-SHA-256 Known Answer Test
- SHA-256 Known Answer Test

Hardware:

- AES-256 OFB Encrypt Known Answer Test
- AES-256 OFB Decrypt Known Answer Test

2.8.2 Conditional Self-Tests

The cryptographic module performs the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for FIPS-approved DRBG
- Continuous Random Number Generator (CRNGT) for Entropy Source
- Firmware Load Test (RSA Signature Verification)
- Pairwise Consistency Test (PWCT) for RSA
- Bypass self-test

2.8.3 Self-Tests Error Handling

If any of the identified POSTs fail, the module will not enter an operational state and will instead provide an error message. The module will then be placed in a Default State (where all keys/CSPs are zeroized) and the FIPS validated flag is reset.

If either of the CRNGTs fail, the repeated random numbers are discarded and an error is reported. If the PWCT fails, the key pair is discarded and an error is reported. If the Firmware Load Test fails, the new firmware is not loaded. If the Bypass self-test fails, the error is reported and the module does not transition into or out of bypass.

Both during execution of the self-tests and while in an error state, data output is inhibited.

2.9 Mitigation of Other Attacks

The module does not claim to mitigate any other attacks beyond those specified in FIPS 140.

3. Secure Operation

This section describes the configuration, maintenance, and administration of the cryptographic module.

The Crypto Officer is responsible for ensuring that any of the plaintext protocols in Section 2.3.3 are not used. When configured according to Section 3 in this Security Policy, the modules only run in their FIPS-Approved mode of operation with the exception of the Services identified in Table 14. The non-approved services described may make use of non-compliant cryptographic algorithms or plaintext data transfers. Use of these services is prohibited in a FIPS-approved mode of operation.

When the module is powered on, its power-up self-tests are executed without any operator intervention.

3.1 Installation

PTP 820G, PTP 820C, PTP 820C-HP, PTP 820C 2E2SX and PTP 820S are fixed configuration with TELs applied at factory. The Crypto Officer must verify at installation time that the TELs are affixed and intact.

PTP 820GX, PTP 820N, and PTP 820A are variable configuration and the CO must verify that they are configured as per one of the approved configurations identified in Section 2.1.1. Moreover for these as well the Crypto Officer must verify at installation time that the TELs are affixed and intact.

Refer to the following figures for the proper placement of TELs.

Figure 20 - TEL Placement for PTP 820C and PTP 820S Models (1 of 5)

Figure 21 - TEL Placement for PTP 820C and PTP 820S Models (2 of 5)

Figure 22 - TEL Placement for PTP 820C and PTP 820S Models (3 of 5)

Figure 23 - TEL Placement for PTP 820C and PTP 820S Models (4 of 5)

Figure 24 - TEL Placement for PTP 820C and PTP 820S Models (5 of 5)

Figure 25 - TEL Placement for PTP 820C-HP (1 of 5)

Figure 26 - TEL Placement for PTP 820C-HP (2 of 5)

Figure 27 - TEL Placement for PTP 820C-HP (3 of 5)

Figure 28 - TEL Placement for PTP 820C-HP (4 of 5)

Figure 29 - TEL Placement for PTP 820C-HP (5 of 5)

Figure 30 - TEL Placement for PTP 820G (1 of 3)

Figure 31 - TEL Placement for PTP 820G (2 of 3)

Figure 32 - TEL Placement for PTP 820G (3 of 3)

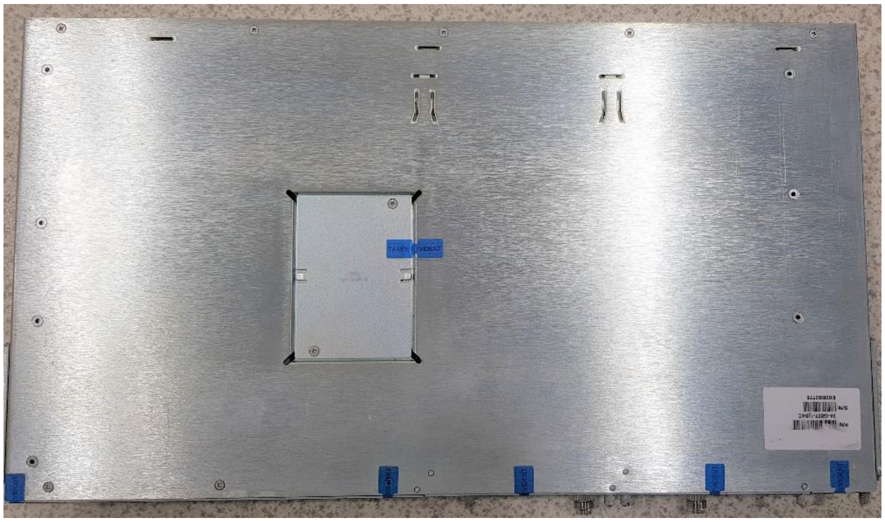

Figure 33 - TEL Placement for PTP 820GX (1 of 5)

Figure 34 - TEL Placement for PTP 820GX (2 of 5)

Figure 35 - TEL Placement for PTP 820GX (3 of 5)

Figure 36 - TEL Placement for PTP 820GX (4 of 5)

Figure 37 - TEL Placement for PTP 820GX (5 of 5)

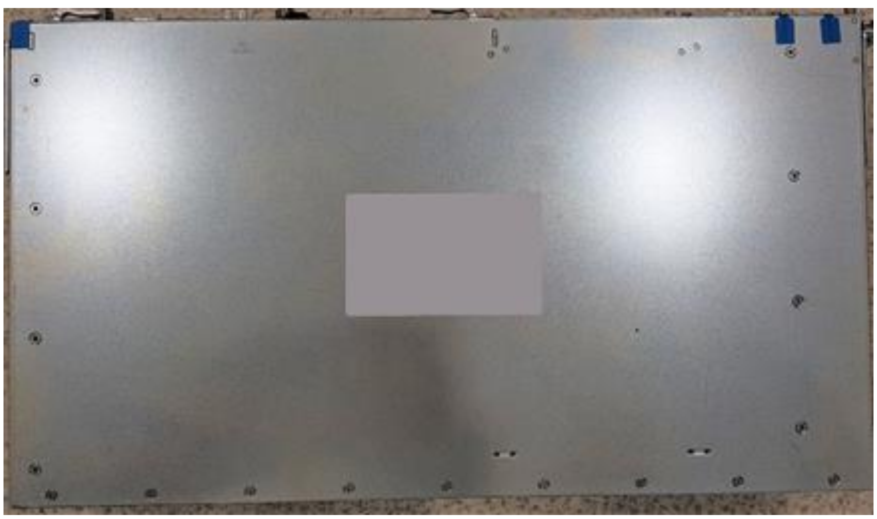

Figure 38 - TEL Placement for PTP 820N and PTP 820A (1 of 4)

Figure 39 - TEL Placement for PTP 820N and PTP 820A (2 of 4)

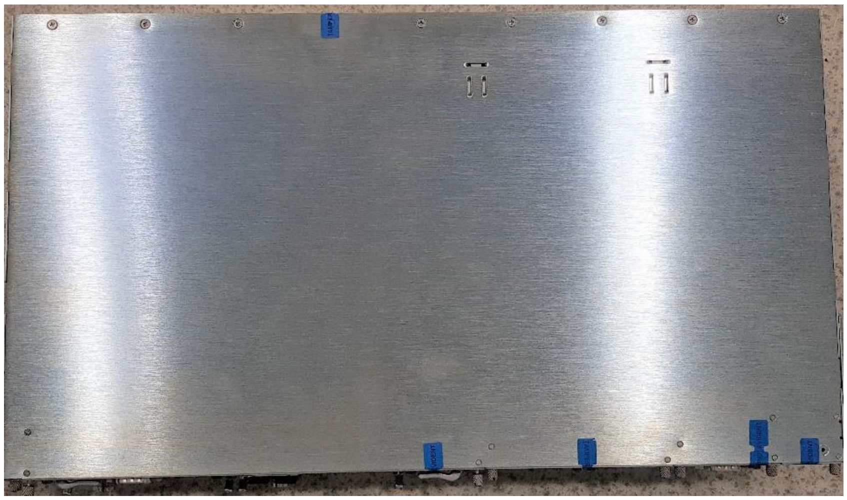

Figure 40 - TEL Placement for PTP 820N and PTP 820A (3 of 4)

Figure 41 - TEL Placement for PTP 820N and PTP 820A (4 of 4)

3.2 Initialization

The CO must follow these steps to place the module in a FIPS mode of operation. For the exact CLI command syntax or GUI instructions, please refer to the below referenced sections of the *FIPS Security Configuration Guide.*

1 Enable configuration to enforce password strength.

- *7.10 Configuring Login and Password Settings*

2 Configure failure login attempts for wrong passwords to 3 attempts (default value).

- *7.10 Configuring Login and Password Settings*

3 For radio encryption mode, configure Master Key and enable Payload Encryption.

- *7.5 Configuring AES-256 Payload Encryption*

4 Enable SNMP v3 (default) and disable SNMPv1 and v2. Add SNMP users as appropriate following the password complexity requirements specified in section 2.3.2. Ensure that "AES" and "SHA" are selected for the privacy and authentication ciphers, respectively.

- *7.9 Configuring SNMPv3*

5 Disable Telnet

- *7.8 Blocking Telnet Access*

6 Disable HTTP and enable HTTPS

- *7.7 Configuring HTTPS*

7 Enable FIPS Admin configuration, i.e., set FIPS mode of operation.

- *7.1 Enabling FIPS Mode*

8 [Optional step] in case of External Protection configuration (relevant for PTP 820G, PTP 820C, PTP 820C 2E2SX, PTP 820C-HP, PTP 820S), enable Protection Admin and supply a pre-shared key.

- *8.1 Changing the Protection Pre-Shared Key*

9 [Optional step] In case of TCC Redundancy (relevant for PTP 820A, PTP 820N), enable Protection Admin, and make sure TCC Protection switch mode is set to Cold Switch Over
Note: Hot Switch Over (HSO) shall not be used in FIPS Mode

- Web GUI: *Platform > Shelf Management > Main Card Redundancy*

  (*In the TCC Protection switch mode field, select Cold Switch Over)*

10 Change the default CO password

- *3.4 Changing Your Password*

Once the final step is performed the module will prompt the CO to reboot. Upon successful reboot the module will enter the approved mode of operation.

Once the module has been configured, the FIPS mode status can be verified:

- *6 Viewing the Security Parameters*

3.3 Management

Protocols such as RADIUS, netconf, HTTP, SNMPv1, and SNMPv2 are not approved for use and shall remain disabled.

When in FIPS 140-2 compliance mode, only the following algorithms are used for SSH and TLS communications.

3.3.1 SSH Usage

When in FIPS mode, the module supports only the following symmetric encryption algorithm:

- AES_256_CBC

The following Message Authentication Code (MAC) algorithm is supported in FIPS mode:

- hmac-sha1

The following key exchange algorithms are supported in FIPS mode:

- diffie-hellman-group-exchange-sha256
- diffie-hellman-group-exchange-sha1
- diffie-hellman-group14-sha1

Only the password-based authentication mode is supported.

3.3.2 TLS Usage

When in FIPS 140-2 compliance mode, only the following ciphersuites are available for TLSv1.2 communications:

- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- DHE-RSA-AES256-GCM-SHA384
- AES256-GCM-SHA384
- DHE-RSA-AES256-SHA256
- AES256-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256
- DHE-RSA-AES128-SHA256
- DHE-RSA-AES128-GCM-SHA256
- AES128-GCM-SHA256
- AES128-SHA256

3.4 Additional Information

For additional information regarding FIPS 140-2 compliance, see the relevant User Manuals.

4. Appendix A: Acronyms

This section describes the acronyms used throughout the document.

Table 16 - Acronyms

Acronym	Definition
TEL	Tamper Evidence Labels
CO	Crypto Officer
CRNGT	Continuous Random Number Generator Test
CSEC	Communications Security Establishment Canada
CVL	Component Validation List
FIPS	Federal Information Processing Standard
KDF	Key Derivation Function
NIST	National Institute of Standards and Technology
POST	Power-On Self-Test
PWCT	Pairwise Consistency Test