FIPS 140-2 Security Policy:

FibeAir® IP-20C
FibeAir® IP-20S
FibeAir® IP-20N
FibeAir® IP-20A
FibeAir® IP-20G
FibeAir® IP-20GX

Firmware: CeraOS 8.3, CeraOS 8.3b512, CeraOS 8.3b517

Hardware:
IP-20N, IP-20A, IP-20G, IP-20GX, IP-20C, IP-20S
IP-20-TCC-B-MC+SD-AF: 24-T009-1|A
IP-20-TCC-B2+SD-AF: 24-T010-1|A
IP-20-TCC-B2-XG-MC+SD-AF: 24-T011-1|A
IP-20-RMC-B-AF: 24-R010-0|A

Ceragon Networks, Ltd.
FIPS 140-2 Non-Proprietary Security Policy
Document Revision: 1.2

Prepared By:
Acumen Security
18504 Office Park Dr.
Montgomery Village, MD 20886
www.acumensecurity.net

Notice

Trademarks

Statement of Conditions

Open Source Statement

The Product may use open source software, among them O/S software released under the GPL or GPL alike license ("Open Source License"). Inasmuch that such software is being used, it is released under the Open Source License, accordingly. The complete list of the software being used in this product including their respective license and the aforementioned public available changes is accessible at:

Network element site:

ftp://ne-open-source.license-system.com

NMS site:

ftp://nms-open-source.license-system.com/

Information to User

Any changes or modifications of equipment not expressly approved by the manufacturer could void the user's authority to operate the equipment and the warranty for such equipment.

Table of Contents

1. Introduction

This is a non-proprietary FIPS 140-2 Security Policy for Ceragon Networks, Ltd and the following Ceragon products: FibeAir® IP-20C FibeAir® IP-20S FibeAir® IP-20N FibeAir® IP-20A FibeAir® IP-20G FibeAir® IP-20GX. Below are the details of the product certified:

Hardware Version #: IP-20N, IP-20A, IP-20G, IP-20GX, IP-20C, IP-20S, IP-20-TCC-B-MC+SD-AF: 24-T009-1|A, IP-20-TCC-B2+SD-AF: 24-T010-1|A, IP-20-TCC-B2-XG-MC+SD-AF: 24-T011-1|A, IP-20-RMC-B-AF: 24-R010-0|A

Software Version #: CeraOS 8.3, CeraOS 8.3b512, CeraOS 8.3b517

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 FibeAir® IP-20C FibeAir® IP-20S FibeAir® IP-20N FibeAir® IP-20A FibeAir® IP-20G FibeAir® IP-20GX 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 Ceragon Networks, Ltd. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Submission Package is proprietary to Ceragon Networks and is releasable only under appropriate non-disclosure agreements.

1.3 Notices

This document may be freely reproduced and distributed in its entirety without modification.

2. FibeAir® IP-20C, FibeAir® IP-20S, FibeAir® IP-20N, FibeAir® IP-20A, FibeAir® IP-20G, and FibeAir® IP-20GX

The FibeAir® IP-20C, FibeAir® IP-20S, FibeAir® IP-20N, FibeAir® IP-20A, FibeAir® IP-20G, and FibeAir® IP-20GX (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 FibeAir® IP-20 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, CeraOS, the IP-20 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 FibeAir® IP-20C

Figure 2 FibeAir® IP-20S

Figure 3 FibeAir® IP-20N and FibeAir® IP-20A

Figure 4 FibeAir® IP-20G

Figure 5 FibeAir® IP-20GX

The IP-20G, IP-20C and IP-20S are fixed configuration.

The IP-20GX has slots for Radio Modem Card RNC-B (IP-20-RMC-B-AF). The IP-20-RMC-B-AF provides the modem interface between the Indoor Unit (IDU) and the Radio Frequency Unit (RFU).

Finally, the IP-20N and IP-20A have slots to insert the following cards:

- Traffic and Control Card (TCC): The Traffic Control Card (TCC) provides the control functionality for the IP- 20N unit. It also provides Ethernet management and traffic interfaces. There are three variants of this card:
  - IP-20-TCC-B2-XG-MC+SD-AF: 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.
  - IP-20-TCC-B-MC+SD-AF: 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.
  - IP-20-TCC-B2+SD-AF: 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 (IP-20-RMC-B-AF): 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 IP-20GX, IP-20N, and IP-20A 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

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

Table 2 - Tested Configurations

Model	Cards
IP-20N	• Single or dual TCC • Dual IP-20-RMC-B-AF • Dual Power supplies
IP-20A	• Single or dual TCC • Dual IP-20-RMC-B-AF • Dual Power supplies
IP-20G	Fixed configuration
IP-20GX	• Dual IP-20-RMC-B-AF
IP-20C	Fixed configuration
IP-20S	Fixed configuration

2.1.2 Modes of Operation

The modules have two modes of operation:

1 FIPS-approved mode: When the module is configured as per instructions in Section 3: Secure Operation section of this document, it is considered to be operating in FIPS approve mode.
2 Non-FIPS Approved mode: In this mode the module is not fully compliant with the configuration steps listed in Section 3 of this document, *Secure Operation*, and as such might allow non-FIPS approved algorithms or services to be executed.

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

Table 3 - Supported Algorithms

Cryptographic Algorithm	CAVP Cert. #	Usage
Software Cryptographic Implementation		
AES CBC (e/d; 256); CTR (int only; 256) KW (AE , AD , AES-256 , INV , 128 , 256 , 192 , 320 , 4096)	3865	Used for control/management plane
SHS SHA-1 (BYTE-only) SHA-224 (BYTE-only) SHA-256 (BYTE-only) SHA-384 (BYTE-only) SHA-512 (BYTE-only)	3185	
HMAC HMAC-SHA256 (Key Size Ranges Tested: KS<BS KS=BS KS>BS)	2509	
SP 800-90A DRBG (HMAC-SHA-256) HMAC_Based DRBG: [Prediction Resistance Tested: Enabled and Not Enabled (SHA-256)	1099	

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(16) , 224 SaltLen(16) , 256 SaltLen(16) , 384 SaltLen(16) , 512 SaltLen(16))) (2048 SHA(1 , 224 , 256 , 384 , 512)) (3072 SHA(1 SaltLen(16) , 224 SaltLen(16) , 256 SaltLen(16) , 384 SaltLen(16) , 512 SaltLen(16)))	1973	
CVL (SNMPv3, SSH and TLS)[1] TLSv1.2 (SHA-256) SSH (SHA-1, 256) SNMP (SHA-1)	742	
KTS (key establishment methodology provides 256 bits of encryption strength)	AES: 3865 HMAC: 2509	
Hardware Cryptographic Implementation		
AES OFB (e/d; 256)	3867	Used for data plan traffic protection

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.

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

[1] Note that CAVP and CMVP does not review or test the SSH, SNMPv3 and TLS protocols

- Diffie - Hellman (key establishment methodology provides 112 bits of encryption strength).
- Elliptic Curve Diffie - Hellman (key establishment methodology provides between 128 and 256-bits bits of encryption strength)
- Non-approved NDRNG for seeding the DRBG. The NDRNG generates a minimum of 256 bits of entropy for use in key generation.

Finally the module implements the following non-approved FIPS algorithms that are not to be used in FIPS mode of operation:

AES (non-compliant for: ECB (192, 256), CBC (128, 192), CTR (128, 192), CFB (128, 192, 256), OFB (128, 192, 256), CCM (128, 192, 256), GCM (128, 192, 256))	CRC7
CRC16	CRC32
DES	DSA (non-compliant)
Diffie-Hellman (non-compliant less than 112 bits of encryption strength)	ECDSA (non-compliant)
MD5	RC5

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:

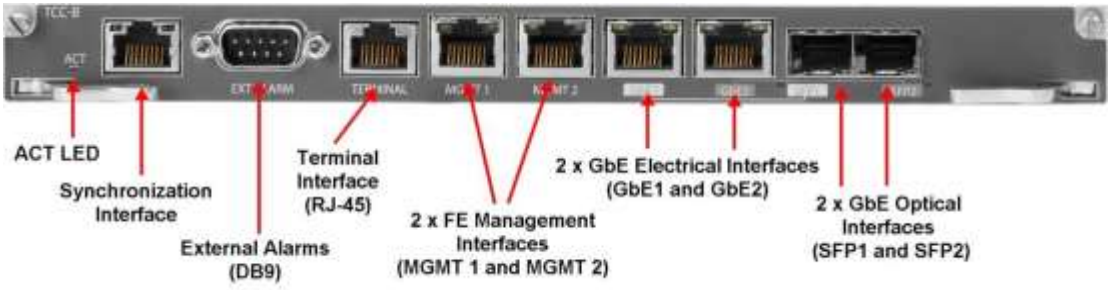

Figure 6 - IP-20-TCC-B-MC+SD-AF Interfaces

Table 4 - Module Interface Mapping for IP-20-TCC-B-MC+SD-AF (IP-20N and IP-20A)

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

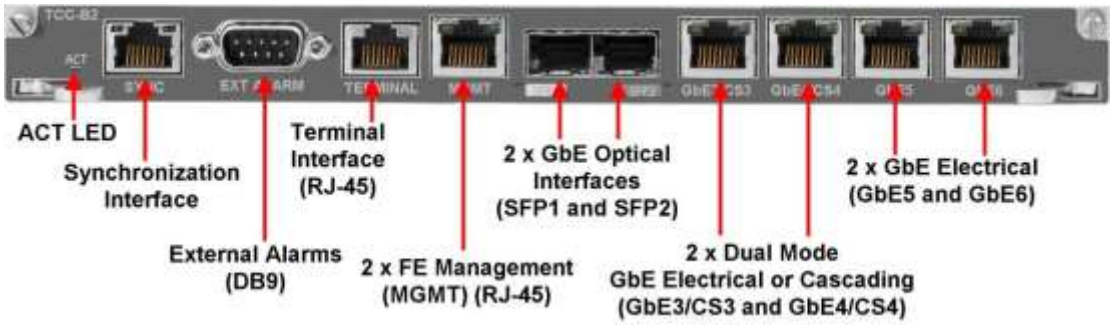

Figure 7 - IP-20-TCC-B2+SD-AF and IP-20-TCC-B2-XG-MC+SD-AF Interfaces

Table 5 - Module Interface Mapping for IP-20-TCC-B2+SD-AF and IP-20-TCC-B2-XG-MC+SD-AF (IP-20N and IP-20A)

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

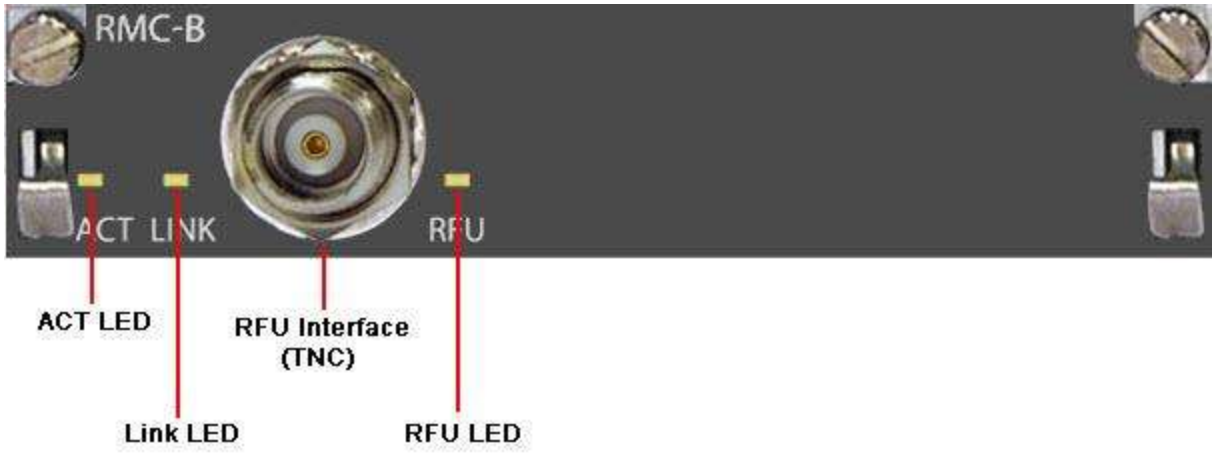

Figure 8 - IP-20-RMC-B-AFInterfaces

Table 6 - Module Interface Mapping for IP-20-RMC-B-AF (IP-20N and IP-20A)

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

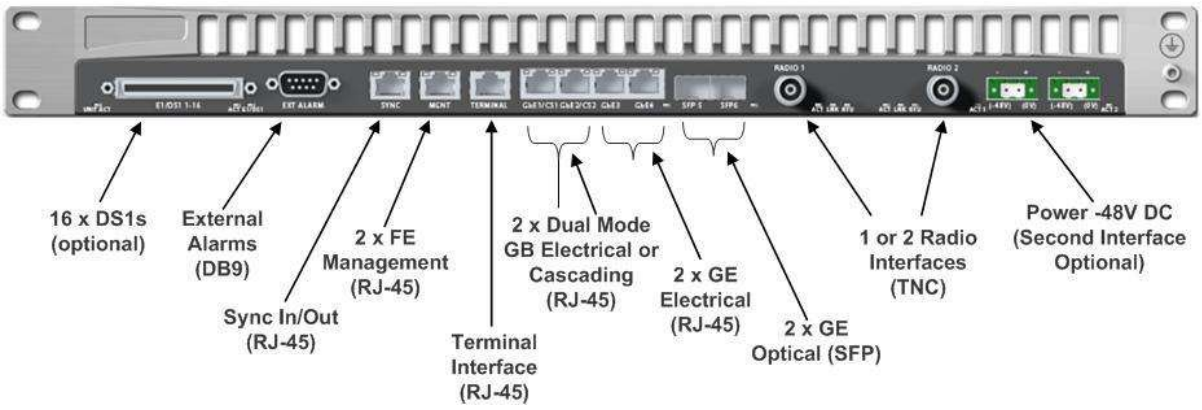

Figure 9 - IP-20G Interfaces

Table 7 - Module Interface Mapping for IP-20G

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

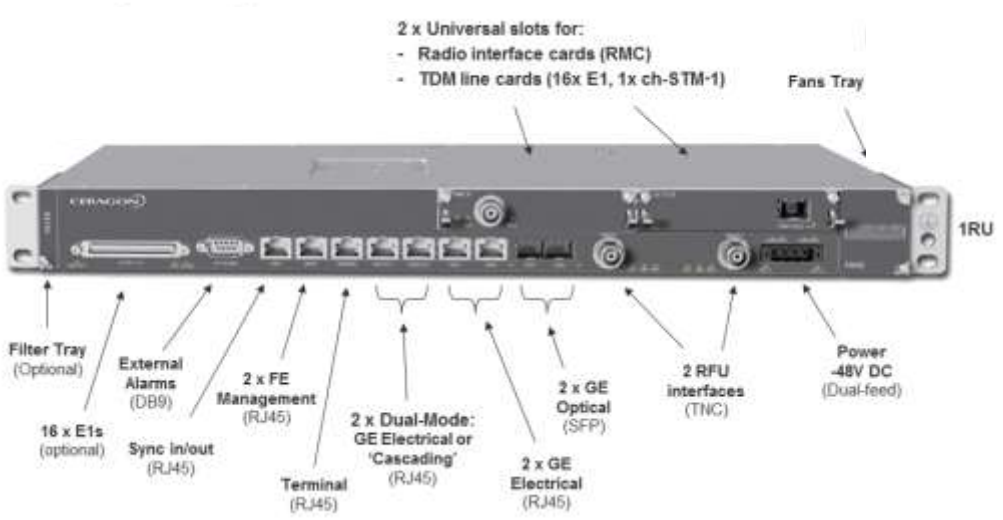

Figure 10 - IP-20GX Interfaces

Table 8 - Module Interface Mapping for IP-20GX

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) IP-20-RMC-B-AF (optional)
Data Output	(2x) GbE Electrical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Optical Interfaces (2x) TNC Radio Interfaces (2x) IP-20-RMC-B-AF (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

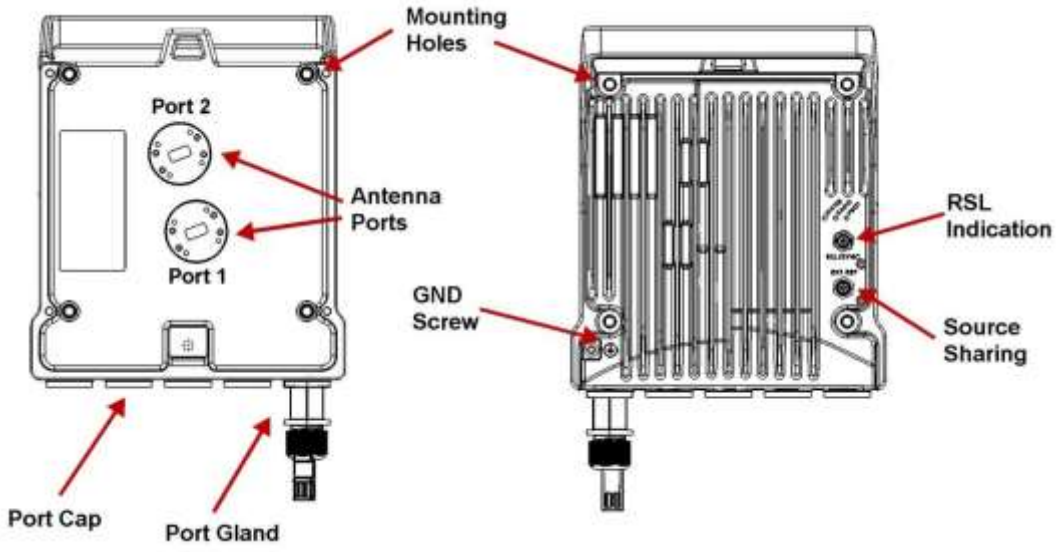

Figure 11 - IP-20C Interfaces (Front and Back)

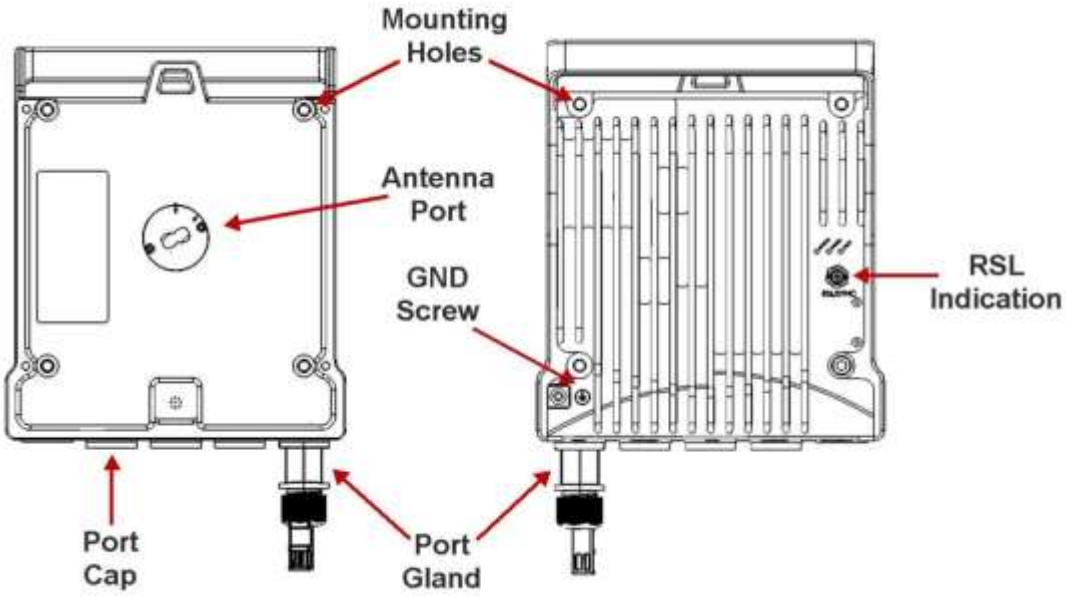

Figure 12 - IP-20S Interfaces (Front and Back)

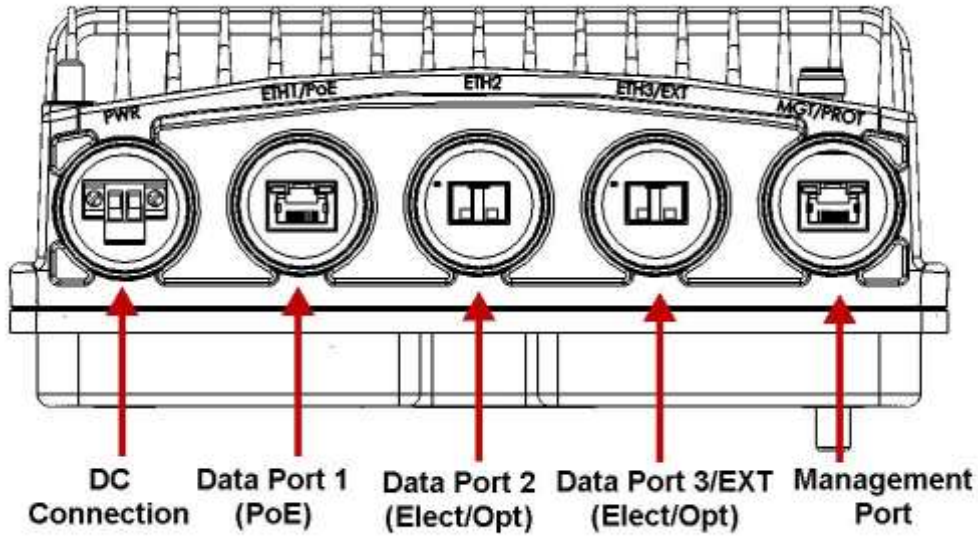

Figure 13 - IP-20C and IP-20S Interfaces Side

Table 9 - Module Interface Mapping for IP-20C and IP-20S

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 IP-20S)
Data Output	(1x) RJ-45 Data Port (PoE) (2x) Data port (Electrical or Optical) (2x) Antenna Ports (Only 1 port on IP-20S)
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 has 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 from which back haul traffic is transmitted to and fro. 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 require 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 10 - Authentication Mechanism Details

Role	Type Of Authentication	Authentication Strength
Admin	Password/Username	All passwords must be at least 8 . If (8) integers are used for an eight digit password, the probability of randomly guessing the correct sequence is one (1) in 100,000,000 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 integer digits. The calculation should be 10^8 = 100,000,000). Therefore, the associated probability of a successful random attempt is approximately 1 in 100,000,000, which 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 1,666,666 guesses per second, which far exceeds the operational capabilities of the module.
Tech		
Viewer		
Operator		
Security Officer		
SNMP User		

Role	Type Of Authentication	Authentication Strength
Users	AES 256-bit Session Key or RSA certificate (if TLS is used)	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 11 - 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
Transmit/Receive Data	Encrypt/Decrypt data passing through the module		X	Session Key Tx (R/W) Session Key Rx (R/W) 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		Crypto Officer Password (R/W/Z) 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/Z) SSH Public Key (R/W/Z) SSH Session Key (R/W/Z) SSH Integrity Key (R/W/Z) Master Key (R/W/X)
Administrative access over Web EMS	Secure remote GUI appliance administration over a TLS tunnel.	X		Crypto Officer Password (R/W/Z) 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/Z) TLS Public Key (R/W/Z) TLS Pre-Master Secret (R/W/Z) TLS Session Encryption Key (R/W/Z) Master Key (R/W/Z)
SNMPv3	Secure remote SNMPv3-based system monitoring.	X		SNMP Session 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	
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) TLS Pre-Master Secret (Z) TLS Session Encryption Key (Z) TLS Session Integrity 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				
Administrative Access over SSH	Secure remote command line appliance administration over an SSH tunnel using non-FIPS approved ciphers (See Section 2.1.2)	X		N/A
Administrative access over Web EMS	Secure remote GUI appliance administration over a TLS tunnel (See Section 2.1.2)	X		N/A
SNMP	Secure remote SNMPv1, v2c-based system monitoring.	X		N/A

R – Read, W – Write, Z – Zeroize

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 2physical 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 12 - 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 ECDH: P-256, P-384, P-521	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 ECDH: P-256, P-384, P-521	The private exponent used in Diffie-Hellman (DH)/ECDH exchange.	RAM	Generated using DRBG	Device power cycle.
Diffie Hellman / EC Diffie Hellman public key	DH 2048 bits ECDH: P-256, P-384, P-521	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	Zeroization command

Key/CSP	Type	Description	Storage	Generated/Entry/Output	Zeroization
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	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	Device power cycle.
SSH Integrity Key	HMAC-SHA-256	The SSH data integrity key. This key is created through SSH key establishment.	RAM	Established using SSH key exchange	Device power cycle.
SNMPv3 password	Shared Secret, at least eight characters	This secret is used to derive HMAC-SHA1 key for SNMPv3 Authentication.	Flash	Configured via HTTPs/SSH/Terminal/SNMPv3	Zeroization command
SNMPv3 session key	AES 256 bits	SNMP symmetric encryption key used to encrypt/decrypt SNMP traffic.	RAM	Established as part of SNMPv3 session	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
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 256 bits	Key used to encrypt/decrypt TLS session data.	RAM	Established using TLS exchange	Device power cycle.
TLS Session Integrity Key	HMAC SHA-256 256 bits	HMAC-SHA-256 used for TLS data integrity protection.	RAM	Established using TLS 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. Output using Master key	Device power cycle.
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 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	Configured using HTTPs/SSH/Terminal/SNMPv3	Zeroization command
Crypto Officer Password	Password	Authentication password for CO role	Flash	Configured	Zeroization command

2.6.1 Key Generation

The module generates symmetric and asymmetric keys in compliance with requirements of 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. Please see Table 12 - Details of Cryptographic Keys and CSPs for details.

2.6.2 Key Entry/Output

Please see Table 12 - 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 Master Key with AES key wrap algorithm.

2.6.3 Zeroization Procedures

Please see Table 12 - 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:

- Software integrity (HMAC-SHA-1)
- HMAC-SHA1 Known Answer Test
- HMAC-SHA224 Known Answer Test
- HMAC-SHA256 Known Answer Test
- HMAC-SHA384 Known Answer Test
- HMAC-SHA512 Known Answer Test
- AES-128 ECB Encrypt Known Answer Test
- AES-128 ECB Decrypt Known Answer Test
- RSA Known Answer Test
- DRBG Health Tests

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

The following steps are required to put the module into a FIPS-approved mode of operation.

3.1 Installation

IP-20G, IP-20C, and IP-20S are fixed configuration with TELs applied at factory. The Crypto Officer must verify at installation time that the TELs are affixed and intact.

IP-20GX, IP-20N, and IP-20A 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.

3.2 Initialization

The CO must follow these steps to place the module in a FIPS mode of operation

1 Enable configuration to enforce password strength.
2 Configure re-try timeouts for wrong passwords to 3 attempts (default value).
3 For radio encryption mode, configure Master Key and enable Payload Encryption.
4 Enable SNMP v3 (default) and disable SNMPv1 and v2.
5 Enable FIPS Admin configuration, i.e., set FIPS mode of operation.
6 Change default CO password

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

3.3 Management

When in FIPS 140-2 compliance mode, only the following algorithms may be used for SSH and TLS communications. Note that using any other algorithms or cipher suites will place the module in a non-FIPS approved mode of operation.

3.3.1 Symmetric Encryption Algorithms:

1 AES_256_CBC

3.3.2 KEX Algorithms:

1 diffie-hellman-group-exchange-sha256
2 diffie-hellman-group-exchange-sha1
3 diffie-hellman-group14-sha1

3.3.3 Message Authentication Code (MAC) Algorithms:

1 hmac-sha1

2 hmac-sha1-96

3.3.4 TLS Usage

When in FIPS 140-2 compliance mode, only the following ciphersuites may be used for TLS communications:

ECDHE-RSA-AES256-SHA384
DHE-RSA-AES256-SHA256
DH-RSA-AES256-SHA256
ECDH-RSA-AES256-SHA384
AES256-SHA256
AES256-SHA

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 13 - 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