FIPS 140-3 Non-Proprietary Security Policy

Ceragon Networks
IP-20G,
IP-20C,
IP-20S,
IP-20C-HP,
IP-20N,
IP-20A,
IP-50C,
IP-50E

Firmware:

12.0.1

Hardware:

IP-20N and IP-20A, with TEL P/N: BS-0341-2 and with components:

- IP-20 TCC-B2-XG-MC: N000082H003
- IP-20 TCC-U: N000082H005
- IP-20 RMC-B: N000082H004

IP-20G, IP-20C, IP-20S, IP-20C-HP, IP-50C and IP-50E (Rev. 6)

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

Ceragon Networks Ltd. assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Ceragon reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Ceragon does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Ceragon products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Ceragon intends to announce such Ceragon products, programming, or services in your country.

Copyrights

This document, Ceragon products, and 3rd Party software products described in this document may include or describe copyrighted Ceragon and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Ceragon, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Ceragon, its licensors, or the 3rd Party software supplied material contained in the Ceragon products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Ceragon. Furthermore, the purchase of Ceragon products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Ceragon or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Ceragon.

License Agreements

The software described in this document is the property of Ceragon and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Ceragon and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high-risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems (“High Risk Use”). Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High-Risk Use.

Table of Contents

List of Tables

List of Figures

Introduction

This is a non-proprietary FIPS 140-3 Security Policy for Ceragon Networks Ltd. and the following Ceragon Networks products: IP-20G, IP-20C, IP-20S, IP-20C-HP, IP-20N, IP-20A, IP-50C, and IP-50E. Below are the details of the certified products:

Hardware Version #:

- IP-20N and IP-20A, with TEL P/N: BS-0341-2 and with components:
  - IP-20 TCC-B2-XG-MC: N000082H003
  - IP-20 TCC-U: N000082H005
  - IP-20 RMC-B: N000082H004
- IP-20G, IP-20C, IP-20S, IP-20C-HP, IP-50C, and IP-50E (Rev. 6)

Firmware Version #: 12.0.1

FIPS 140-3 Security Level: 2

Purpose

This document was prepared as part of the Federal Information Processing Standard (FIPS) 140-3 validation process. The document describes how the Ceragon Networks IP-20G, IP-20C, IP-20S, IP-20C-HP, IP-20N, IP-20A, IP-50C and IP-50E meet the security requirements of FIPS 140-3. It also provides instructions to individuals and organizations on how to deploy the product in a secure 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 140-3 requirements.

Document Organization

The Security Policy document is one document in a FIPS 140-3 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, LLC. under contract to Ceragon Networks. With the exception of this Non-Proprietary Security Policy, the FIPS 140-3 Submission Package is proprietary to Ceragon Networks and is releasable only under appropriate non-disclosure agreements.

1. General

The Ceragon Networks IP-20G, IP-20C, IP-20S, IP-20C-HP, IP-20N, IP-20A, IP-50C and IP-50E (the module) are multi-chip standalone hardware modules validated at FIPS 140-3 Security Level 2. Specifically, the modules meet that following security levels for individual sections in FIPS 140-3 standard:

Section	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	2
4	Roles, services, and authentication	2
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	2
12	Mitigation of other attacks	N/A

Table 1 - Security Levels

2. Cryptographic Module Specification

The IP-20 and IP-50 series radios provide a service-centric microwave platform for HetNet[1] hauling. The platform includes a full complement of wireless products that provide backhaul and fronthaul solutions.

Powered by a software-defined engine and sharing a common operating system, IP-20 and IP-50 Release 12.0.1, the IP-20 and IP-50 platforms deliver ultra-high capacities while supporting any radio transmission technology, any network topology, and any deployment configuration.

2.1 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:

[1] Heterogenous Network

Figure 1 – IP-20G

Figure 2 – IP-20C

Figure 3 – IP-20S

Figure 4 – IP-20C-HP

Figure 5 – IP-20N and IP-20A

Figure 6 – IP-50C

Figure 7 – IP-50E (Rev. 6)

The IP-20G, IP-20C, IP-20S, IP-20C-HP, IP-50C and IP-50E are fixed configuration.

The IP-20N and IP-20A are modular configuration, and 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 and IP-20A units. It also provides Ethernet management and traffic interfaces. There are two variants of this card:
  - IP-20 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.
  - IP-20 TCC-U: N000082H005: Provides 6 x 1/10GE optical interfaces and 2 x RFU or 1/2.5 GbE electrical PoE interfaces. Two of the optical interfaces (1 and 2) can be configured as cascading interfaces. Supports up to two Multi-Carrier ABC groups, with capacity of 2.5 Gbps (non-configurable). Supports multiple high-capacity configurations with Link Bonding.
- Radio Modem Card-B (IP-20 RMC-B: N000082H004): The Radio Modem Card (RMC) provides the modem interface between the Indoor Unit (IDU) and the Radio Frequency Unit (RFU).

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

Model	Hardware	Firmware Version	Distinguishing Features
IP-20G	IP-20G	12.0.1	Fixed configuration IDU[2]. See Table 5
IP-20C	IP-20C	12.0.1	Fixed configuration ODU[3]. See Table 6
IP-20S	IP-20S	12.0.1	Fixed configuration ODU. See Table 7
IP-20C-HP	IP-20C-HP	12.0.1	Fixed configuration ODU. See Table 8

[2] Indoor unit
[3] Outdoor unit

Model	Hardware	Firmware Version	Distinguishing Features
IP-20N	IP-20N with TEL P/N: BS-0341-2 and with components: ○ IP-20 TCC-B2-XG-MC: N000082H003 ○ IP-20 TCC-U: N000082H005 ○ IP-20 RMC-B: N000082H004	12.0.1	Modular IDU. • Single or dual TCC • Dual RMC-B • Dual Power supplies See Table 9, Table 10 and Table 11
IP-20A	IP-20A with TEL P/N: BS-0341-2 and with components: ○ IP-20 TCC-B2-XG-MC: N000082H003 ○ IP-20 TCC-U: N000082H005 ○ IP-20 RMC-B: N000082H004	12.0.1	Modular IDU. • Single or dual TCC • Dual RMC-B • Dual Power supplies See Table 9, Table 10 and Table 11
IP-50C	IP-50C	12.0.1	Fixed configuration ODU. See Table 12
IP-50E	IP-50E (Rev. 6)	12.0.1	Fixed configuration ODU. See Table 13

Table 2 - Cryptographic Module Tested Configuration

Additionally, the following cards can be configured on 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
- TDM E1/T1
- 10Gb Ethernet/Optical Line Interface Card (LIC-X-E10)
- Radio Interface Card (RIC-D)

2.2 Modes of Operation

The module operates in the Approved mode of operation (when configured as per the instructions in Section 11 of this document). Any usage of the non-Approved services described in Table 17 would result in a non-Approved mode of operation.

2.3 Cryptographic Algorithms

The following table lists the Approved algorithms supported by the modules:

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
Management Security Algorithms Implementation (Firmware)				
A2758	AES (FIPS 197)	CBC	Direction: Decrypt, Encrypt Key Length: 128, 256	Used for control/ management plane encryption/ decryption
		ECB	Direction: Decrypt, Encrypt Key Length: 128, 256	
		CTR	Direction: Decrypt, Encrypt Key Length: 128, 192, 256 Payload Length: 8-128 Increment 8 Incremental Counter Counter Tests Performed	
		CFB128	Direction: Decrypt, Encrypt Key Length: 128	
		GCM[4]	Direction: Decrypt, Encrypt IV Generation: Internal IV Generation Mode: 8.2.1 Key Length: 128, 256 Tag Length: 32, 64, 96, 104, 112, 120, 128 IV Length: 96-1024 Increment 8 Payload Length: 8-65536 Increment 8 AAD Length: 0-65536 Increment 8	
		KW	Direction: Decrypt, Encrypt Cipher: Cipher, Inverse Key Length: 256 Payload Length: 128-524288 Increment 128	
	SHS (FIPS 180-4)	SHA-1 SHA2-256 SHA2-384 SHA2-512	Message Length: 0-65536 Increment 8	Used for control/ management plane message digests. SHA-1 is permitted within SSH, TLS and IPSec protocols, and legacy signature verification only.
	HMAC	HMAC-SHA1	MAC: 32-160 Increment 8 Key Length: 8-524288 Increment 8	Used for control/ management plane

[4] GCM IV generation tested in accordance with IG C.H, scenario 1 TLSv1.2 following RFCs 5516, 5246, 5288, and 5289 as well as SSH following RFCs 4251, 4252, 4253, 4254 and 5647. The IV is generated only for use with GCM encryption within the protocol being used. The TLS cipher suites supported by the module are identified in section 11.4.2 of this document which are included in SP 800-52 Rev2 section 3.3.1. The module also internally generates IVs for TLS 1.3 (RFC 8446) in accordance with scenario 5 in IG C.H. In the case the module's power is lost and then restored, a new key for use with AES-GCM encryption/decryption is established.

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
	(FIPS 198-1)	HMAC-SHA2-256	MAC: 32-256 Increment 8 Key Length: 8-524288 Increment 8	message authentication
		HMAC-SHA2-384	MAC: 32-384 Increment 8 Key Length: 8-524288 Increment 8	
		HMAC-SHA2-512	MAC: 32-512 Increment 8 Key Length: 8-524288 Increment 8	
	DRBG (SP800-90Arev1)	CTR_DRBG	Capabilities: Mode: AES-256 Derivation Function Enabled: Yes Additional Input: 0-256 Increment 256 Entropy Input: 2048 Increment 128 Nonce: 128 Personalization String Length: 0-256 Increment 256 Returned Bits: 256	Used for control/ management plane random bit generation
	ECDSA (FIPS 186-4)	KeyGen, KeyVer, SigGen, SigVer	Capabilities: Curve: P-256 Hash Algorithm: SHA2-256, SHA2-384, SHA2-512 Secret Generation Mode: Testing Candidates	Used for control/ management plane key generation, signature generation, and signature verification
	DSA (FIPS 186-4)	KeyGen	Capabilities: L: 2048 N: 224 L: 2048 N: 256 L: 3072 N: 256	Used for control/ management plane FCC key generation
	RSA (FIPS 186-4)	KeyGen	Capabilities: Key Generation Mode: B.3.3 Properties: Modulo: 2048 Primality Tests: Table C.2 Properties: Modulo: 3072 Primality Tests: Table C.2 Properties: Modulo: 4096 Primality Tests: Table C.2 Info Generated By Server Public Exponent Mode: Random Private Key Format: Standard	Used for control/ management plane key generation, signature generation, and signature verification

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
		SigGen	Capabilities: Signature Type: PKCS 1.5 Properties: Modulo: 2048 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 3072 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 4096 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Capabilities: Signature Type: PKCSPSS Properties: Modulo: 2048 Salt Length: 28 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Properties: Modulo: 3072 Hash Pair:	

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
			Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Properties: Modulo: 4096 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Capabilities: Signature Type: ANSI X9.31 Properties: Modulo: 2048 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 3072 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 4096 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384	

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
			Hash Pair: Hash Algorithm: SHA2-512	
		SigVer	Capabilities: Signature Type: PKCS 1.5 Properties: Modulo: 2048 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 3072 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 4096 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Capabilities: Signature Type: ANSI X9.31 Properties: Modulo: 2048 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 3072 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair:	

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
			Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Properties: Modulo: 4096 Hash Pair: Hash Algorithm: SHA2-256 Hash Pair: Hash Algorithm: SHA2-384 Hash Pair: Hash Algorithm: SHA2-512 Capabilities: Signature Type: PKCSPSS Properties: Modulo: 2048 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Properties: Modulo: 3072 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48 Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Properties: Moduli: 4096 Hash Pair: Hash Algorithm: SHA2-256 Salt Length: 32 Hash Pair: Hash Algorithm: SHA2-384 Salt Length: 48	

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
			Hash Pair: Hash Algorithm: SHA2-512 Salt Length: 64 Public Exponent Mode: Random	
	KTS-1	AES	AES-256 in KW mode	Used for key transport on the data plane; key establishment methodology provides 256 bits of encryption strength
	KTS-2	AES	AES-128 and AES-256 in GCM mode	Used for key transport on the management plane within TLS and SSH; key establishment methodology provides 128 or 256 bits of encryption strength
	KTS-3	AES HMAC	AES-128, AES-192 and AES-256 in CTR mode with HMAC SHA-1	Used for key transport on the management plane within SSH; key establishment methodology provides between 128 and 256 bits of encryption strength
	KTS-5	AES HMAC	AES-128 and AES-256 in CBC mode with HMAC-SHA-1 or HMAC SHA-256	Used for key transport on the management plane within TLS; key establishment methodology provides 128 or 256 bits of encryption strength

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
	KAS-FFC-SSC (SP800-56arev3)	Diffie-Hellman	Domain Parameter Generation Methods: FB, FC, ffdhe2048, ffdhe3072 Scheme: dhEphem: KAS Role: initiator, responder	Used for key transport on the management plane using Diffie-Hellman; key establishment methodology provides 112 and 128 bits of encryption strength
	KAS-ECC-SSC (SP800-56arev3)	Ephemeral Unified	Domain Parameter Generation Methods: P-256 Scheme: ephemeralUnified: KAS Role: initiator, responder	Used for key transport on the management plane using Elliptic Curve Diffie-Hellman; key establishment methodology provides 128 bits of encryption strength
	CVL RFC 7627	KDF TLSv1.2	Hash Algorithm: SHA2-256, SHA2-384, SHA2-512	Used for key derivation within management protocols
	CVL RFC 8446	KDF TLSv1.3	HMAC Algorithm: SHA2-256, SHA2-384 KDF Running Modes: DHE, PSK, PSK-DHE	
	CVL[5] (SP800-135-r1)	KDF SSHv2	AES-128, AES-192, AES-256 SHA-1, SHA2-256, SHA2-384, SHA2-512	
Vendor-affirmed	CKG[6]	SP800-133rev2	§4: Using the Output of a Random Bit Generator §5: Generation of Key Pairs for Asymmetric-Key Algorithms §6.1: The "Direct Generation" of Symmetric Keys §6.2: Derivation of Symmetric Keys	Symmetric key and asymmetric seed generation
A2758 A2756	KAS-1		KAS-FFC-SSC Cert. #A2758 with CVL Certs. #A2758 and #A2756	Diffie-Hellman key establishment

[5] Note that no parts of the SSH, SNMPv3, IKEv1 and TLS protocols, other than the approved cryptographic algorithms and the KDFs, have been tested by the CAVP and CMVP.

[6] In accordance with FIPS 140-3 IG D.H, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP 800-133r2 (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.

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
			ffdhe2048, ffdhe3072 providing 112 and 128 bits of encryption strength	using KAS-FFC-SSC with SP 800-135 SSHv2 KDF, IKEv1 KDF, RFC 7627 TLSv1.2 KDF and RFC 8446 TLSv1.3 KDF
A2758 A2756	KAS-2		KAS-ECC-SSC Cert. #A2758 with CVL Certs. #A2758, #A2756 and #A2757 P-256 providing 128 bits of encryption strength	Elliptic Curve Diffie-Hellman key establishment using KAS-ECC-SSC with SP 800-135 SSHv2 KDF, IKEv1 KDF, RFC 7627 TLSv1.2 KDF and RFC 8446 TLSv1.3 KDF
IKE KDF Implementation (Firmware)				
A2756	KDF IKEv1 CVL (SP800-135-r1)	KDF IKEv1	Capabilities: Authentication Method: Pre-shared Key Initiator Nonce Length: 64-2048 Increment 8 Responder Nonce Length: 64-2048 Increment 8 Preshared Key Length: 8-8192 Increment 8 Diffie-Hellman Shared Secret Length: 3072 Hash Algorithm: SHA2-256	Used for key derivation within IPsec Not implemented on Freescale P1021 or ARM based platforms
SNMP KDF Implementation (Firmware)				
A2757	CVL (SP800-135-r1)	KDF SNMPv3	Password Length: 64, 256 Engine ID: 3078313130663331626636303532333062 64, 3078333964653663643936303437353165 63	Used for key derivation within management protocols
Linux Kernel Crypto Implementation (Firmware)				
A2755	AES (FIPS 197)	CBC	Direction: Decrypt, Encrypt Key Length: 256; tested but not used on Freescale P1012 or ARM based platforms	Used for data encryption/ decryption within IPsec
	HMAC (FIPS 198-1)	HMAC-SHA2-256	MAC: 128; Key Length: 256; tested but not used on Freescale P1012 or ARM based platforms	Used for message authentication within IPSec
	SHS (FIPS 180-4)	SHA2-256	Message Length: 0-51200 Increment 8; not used on Freescale P1012 or ARM based platforms	Used for message digests within IPsec

CAVP Cert	Algorithm and Standard	Mode/Method	Description / Key Size(s) / Key Strength(s)	Use / Function
	KTS-4	AES HMAC	AES-256 in CBC mode with HMAC SHA-256	Used for key transport on the management plane within IPsec; key establishment methodology provides 256 bits of encryption strength
AES Core Implementation (Hardware)				
AES 4014	AES (FIPS 197)	OFB	Direction: Decrypt, Encrypt Key Length: 256	Used for data plane encryption/ decryption (IP-20C, -20S, -20C-HP)
A680	AES (FIPS 197)	CTR	Direction: Decrypt, Encrypt Key Length: 256 Payload Length: 128 Incremental Counter Counter Tests Performed	Used for data plane encryption/ decryption (IP-50C, -50E, -20G, -20A, -20N)
Entropy Source				
ENT (P)			Ring-oscillator noise source with no conditioning function Conformant to SP 800-90B and IG D.J and D.K. Min-entropy: 1.9 bits per byte	

Table 3 – Approved Algorithms

*Note that there are algorithms, modes, and key/moduli sizes that have been CAVP-tested but are not used by any approved service of the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by an approved service of the module.

Algorithm/Function	Use/Function
MD5	RADIUS
	TACACS+

Table 4 – Non-Approved Algorithms Not Allowed in the Approved Mode of Operation

3. Cryptographic Module Interfaces

The modules provide a number of physical ports/logical interfaces to the device, and the physical ports provided by the module are mapped to four FIPS 140-3 defined logical interfaces: data input, data output,

control input, and status output. The physical ports/logical interfaces and their mapping are described in the following diagrams/tables:

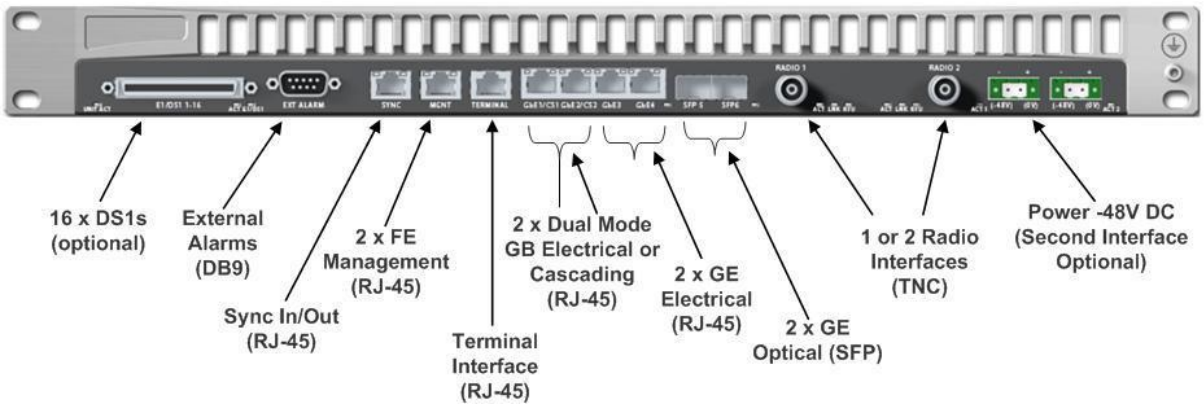


Figure 8 – IP-20G Physical Ports

Physical port	Logical interface	Data that passes over port/interface
(1x) FE Management Interfaces[7] (2x) GbE Electrical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Optical Interfaces (16x) E1/DS1s (2x) TNC Radio Interfaces	Data Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (FE) Data traffic (TNC, GbE, E1/DS1)
(1x) FE Management Interfaces (2x) GbE Electrical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Optical Interfaces (16x) E1/DS1s (2x) TNC Radio Interfaces	Data Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (FE) Data traffic (TNC, GbE, E1/DS1)
(1x) Sync In/Out RJ-45 Interface (1x) RJ-45 Terminal Interface (1x) FE Management Interfaces	Control Input	Clock signaling (Sync) TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (FE) Serial console (Terminal)
(1x) RJ-45 Terminal Interface (1x) FE Management Interfaces (1x) DB9 External Alarms LEDs	Status Output	Alarm signaling (DB9) TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (FE) Serial console (Terminal)

[7] Note that only one FE interface appears in the figure. With the addition of a Y-connector, the single port can be used to provide two FE interfaces.

Physical port	Logical interface	Data that passes over port/interface
		Activity (LED)
(1x) -48V DC Power Interface	Power Input	N/A

Table 5 – IP-20G Ports and Interfaces

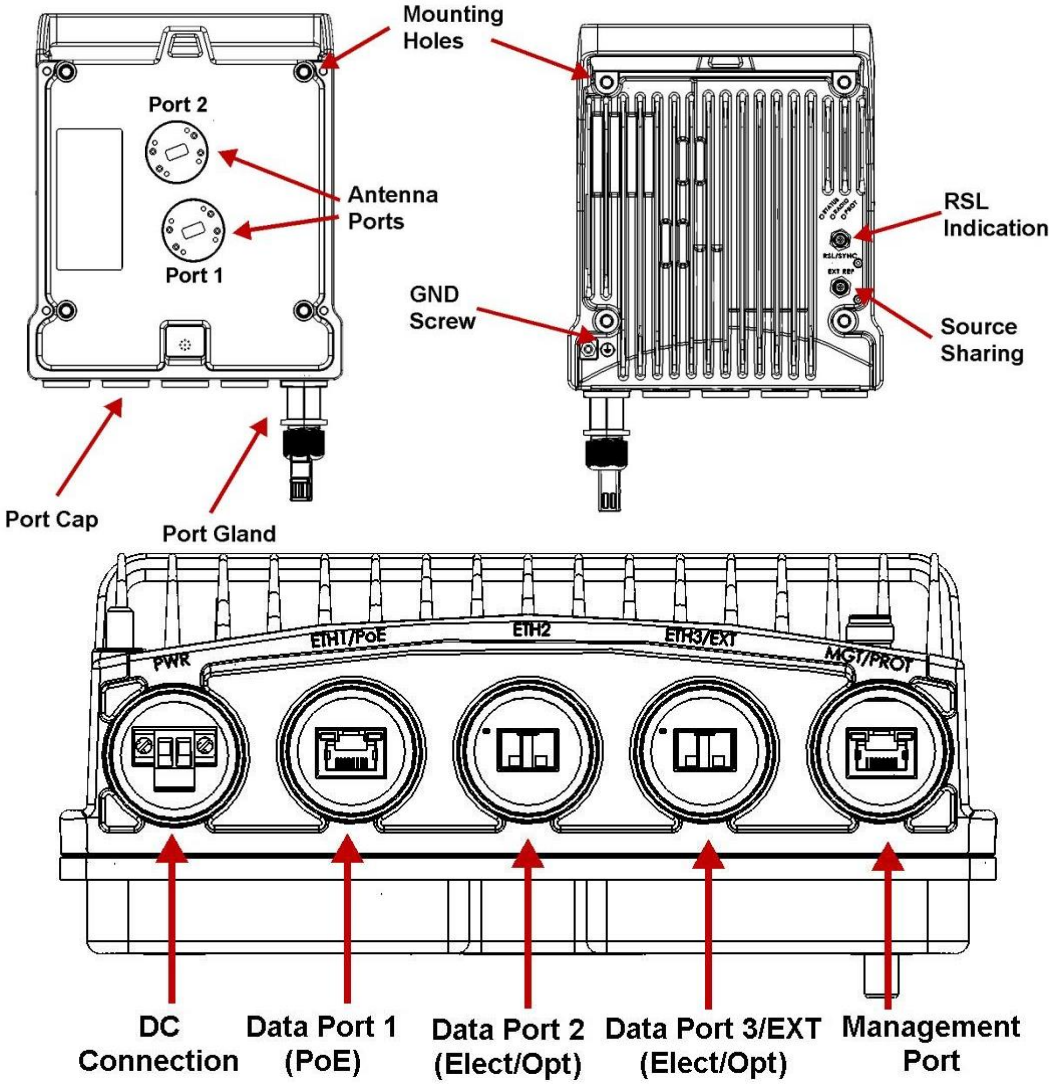
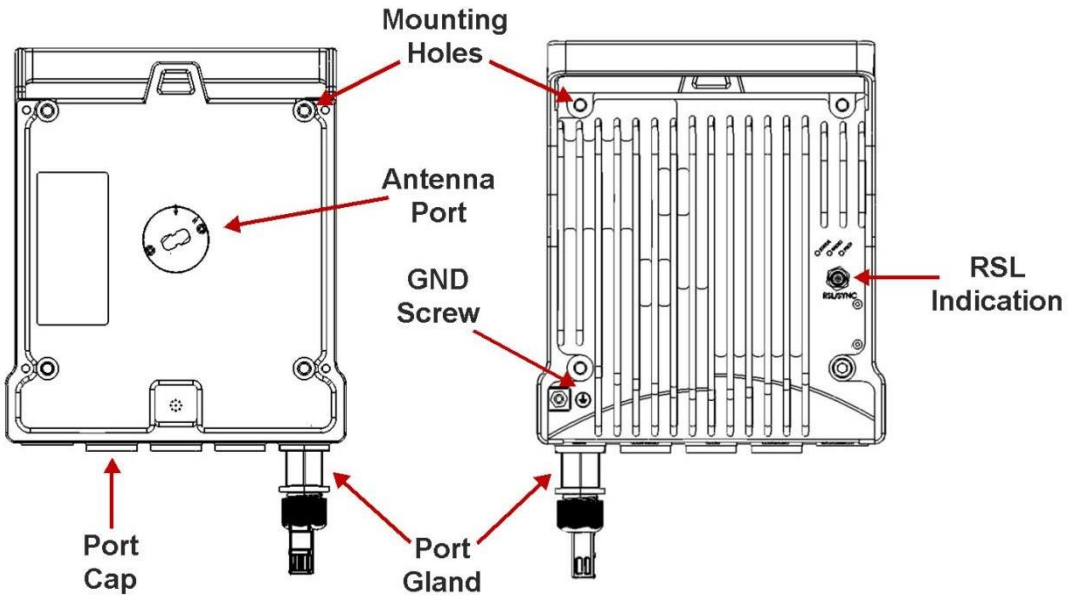


Figure 9 – IP-20C Physical Ports

Physical port	Logical interface	Data that passes over port/interface
(1x) RJ-45 Data Port (PoE) (1x) RJ-45 Management Interface (2x) Data port (Electrical or Optical)	Data Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) Data traffic (Data Port, Antenna Ports)

Physical port	Logical interface	Data that passes over port/interface
(2x) Antenna Ports		
(1x) RJ-45 Data Port (PoE) (1x) RJ-45 Management Interface (2x) Data port (Electrical or Optical) (2x) Antenna Ports	Data Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) Data traffic (Data Port, Antenna Ports)
(1x) Source Sharing (1x) RJ-45 Management Interface	Control Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) Signaling (Source Sharing)
(1x) RSL Indication (1x) RJ-45 Management Interface	Status Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) RSL signaling (RSL)
(1x) -48V DC Power Interface (1x) RJ-45 Data Port (PoE)	Power Input	N/A

Table 6 – IP-20C Ports and Interfaces



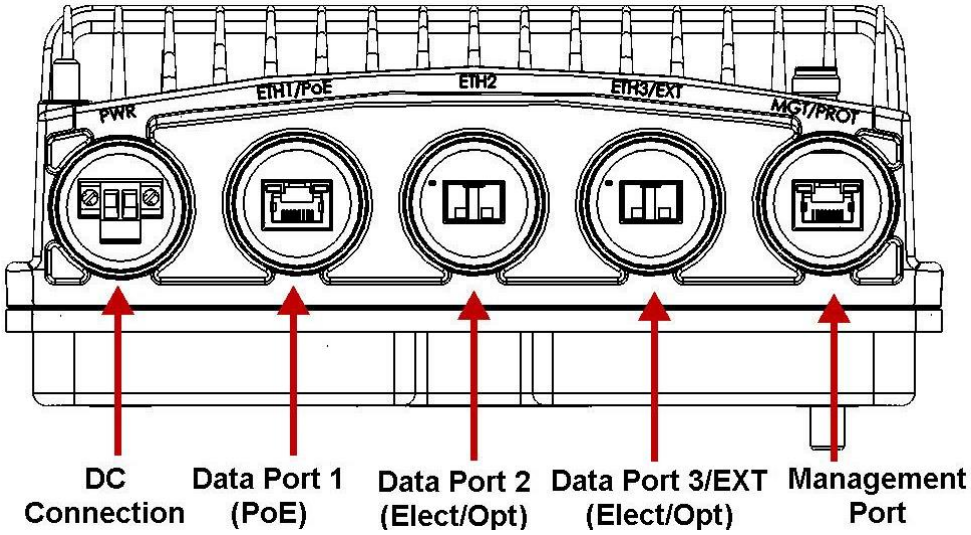


Figure 10 – IP-20S Physical Ports

Physical port	Logical interface	Data that passes over port/interface
(1x) RJ-45 Data Port (PoE) (1x) RJ-45 Management Interface (2x) Data port (Electrical or Optical) (1x) Antenna Ports	Data Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) Data traffic (Data Port, Antenna Ports)
(1x) RJ-45 Data Port (PoE) (1x) RJ-45 Management Interface (2x) Data port (Electrical or Optical) (1x) Antenna Ports	Data Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) Data traffic (Data Port, Antenna Ports)
(1x) RJ-45 Management Interface	Control Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45)
(1x) RSL Indication (1x) RJ-45 Management Interface	Status Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) RSL signaling (RSL)
(1x) -48V DC Power Interface (1x) RJ-45 Data Port (PoE)	Power Input	N/A

Table 7 – IP-20S Ports and Interfaces

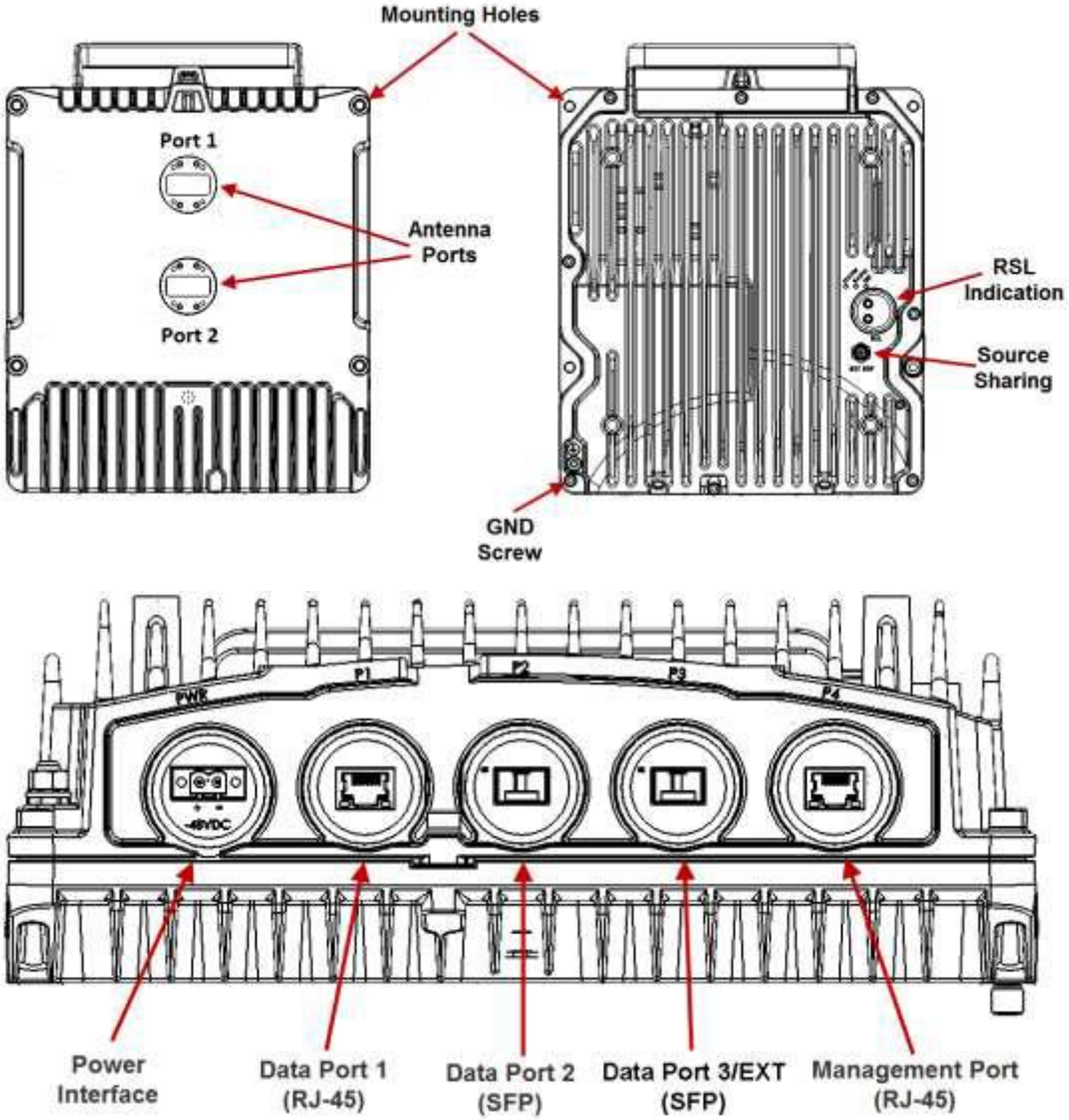


Figure 11 – IP-20C-HP Physical Ports

Physical port	Logical interface	Data that passes over port/interface
(1x) RJ-45 Data Port (1x) RJ-45 Management Interface (2x) Data port (Electrical or Optical) (2x) Antenna Ports	Data Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45 Management) Data traffic (Data Ports, Antenna Ports)
(1x) RJ-45 Data Port (1x) RJ-45 Management Interface	Data Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45 Management)

Physical port	Logical interface	Data that passes over port/interface
(2x) Data port (Electrical or Optical) (2x) Antenna Ports		Data traffic (Data Ports, Antenna Ports)
(1x) Source Sharing (1x) RJ-45 Management Interface	Control Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) Signaling (Source Sharing)
(1x) RSL Indication (1x) RJ-45 Management Interface	Status Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) RSL signaling (RSL)
(1x) -48V DC Power Interface	Power Input	N/A

Table 8 – IP-20C-HP Ports and Interfaces

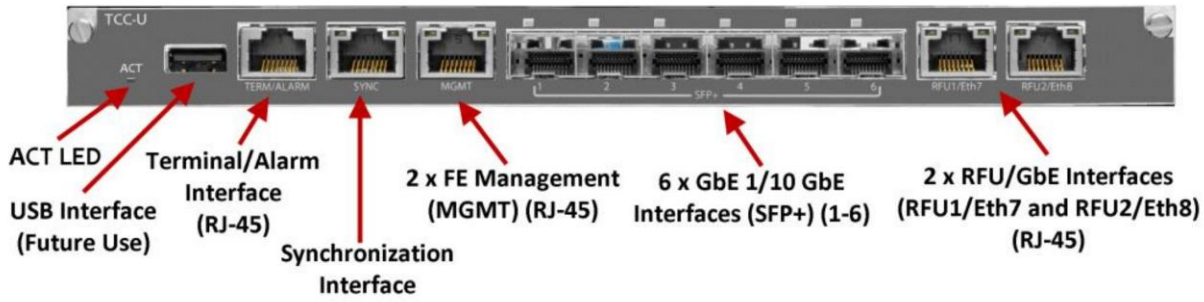


Figure 12 – IP-20 TCC-U: N000082H005 (IP-20N and IP-20A) Physical Ports

Physical port	Logical interface	Data that passes over port/interface
(6x) GbE Optical Interfaces (2x) Gbe Electrical Interfaces (2x) FE Management Interfaces	Data Input	TLS v1.2/1.3, SSH, and SNMPv3 management traffic (FE) Data traffic (GbE)
(6x) GbE Optical Interfaces (2x) Gbe Electrical Interfaces (2x) FE Management Interfaces	Data Output	TLS v1.2/1.3, SSH, and SNMPv3 management traffic (FE) Data traffic (GbE)
(1x) Synchronization Interface (1x) RJ-45 Terminal Interface (2x) FE Management Interfaces	Control Input	Clock signaling (Sync) TLS v1.2/1.3, SSH, and SNMPv3 management traffic (FE) Serial console (Terminal) Signaling (Synchronization)
(1x) RJ-45 Terminal Interface (2x) FE Management Interfaces	Status Output	Alarm signaling (DB9) TLS v1.2/1.3, SSH, and SNMPv3 management traffic (FE)

Physical port	Logical interface	Data that passes over port/interface
(1x) ACT LED (1x) RJ45 External Alarms		Serial console (Terminal) Activity (LED) Alarm signaling (RJ45)

Table 9 – IP-20 TCC-U: N000082H005 (IP-20N and IP-20A) Ports and Interfaces

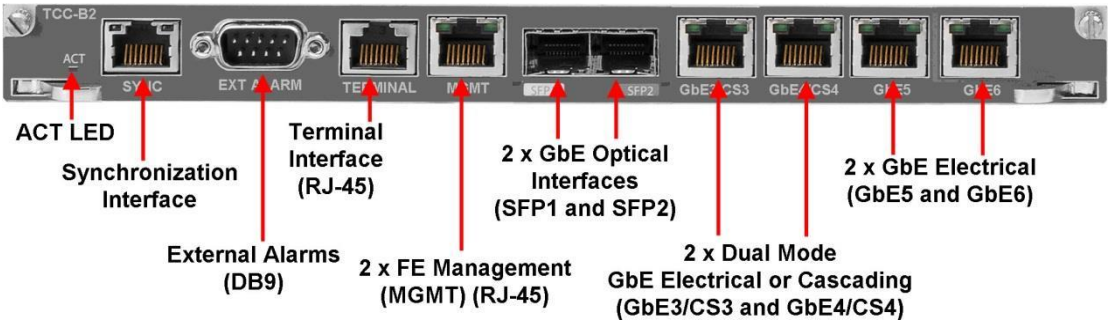


Figure 13 – IP-20 TCC-B2-XG-MC: N000082H003 (IP-20N and IP-20A) Physical Ports

Physical port	Logical interface	Data that passes over port/interface
(2x) GbE Optical Interfaces (2x) FE Management Interfaces[8] (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Electrical Interfaces	Data Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (FE) Data traffic (GbE)
(2x) GbE Optical Interfaces (2x) Dual Mode GbE Electrical or Cascading (2x) GbE Electrical Interfaces	Data Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (FE) Data traffic (GbE)
(1x) Synchronization Interface (1x) RJ-45 Terminal Interface (2x) FE Management Interfaces	Control Input	Clock signaling (Sync) TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (FE) Serial console (Terminal) Signaling (Synchronization)
(1x) RJ-45 Terminal Interface (2x) FE Management Interfaces (1x) ACT LED (1x) DB9 External Alarms	Status Output	Alarm signaling (DB9) TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (FE) Serial console (Terminal) Activity (LED) Alarm signaling (DB9)

[8] Note that only one FE interface appears in the figure. With the addition of a Y-connector, the single port can be used to provide two FE interfaces.

Table 10 –IP-20 TCC-B2-XG-MC: N000082H003 (IP-20N and IP-20A) Ports and Interfaces

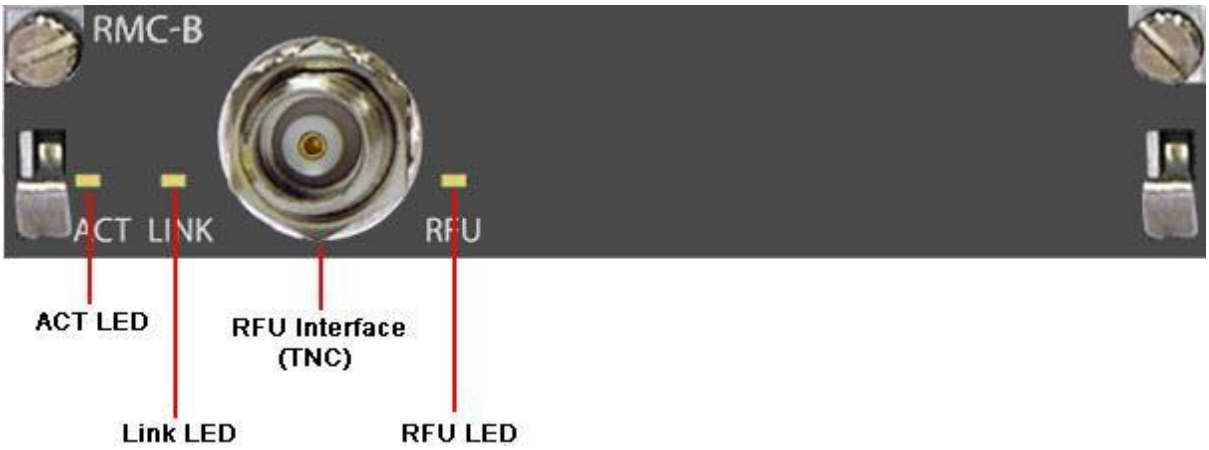
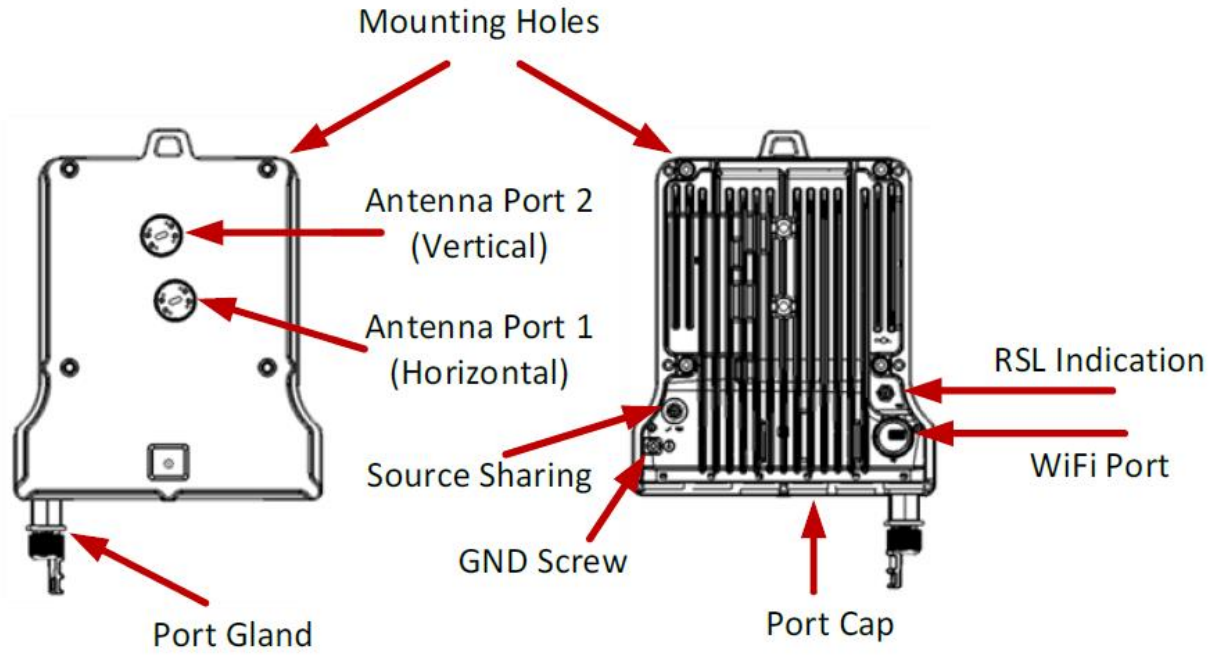


Figure 14 – IP-20 RMC-B: N000082H004 (IP-20N and IP-20A) Physical Ports

Physical port	Logical interface	Data that passes over port/interface
(1x) TNC RFU Interface	Data Input	Data traffic
(1x) TNC RFU Interface	Data Output	Data traffic
(1x) TNC RFU Interface	Control Input	Data plane control signaling
(1x) ACT LED (1x) Link LED (1x) RFU LED	Status Output	Activity

Table 11 – IP-20 RMC-B: N000082H004 (IP-20N and IP-20A) Ports and Interfaces



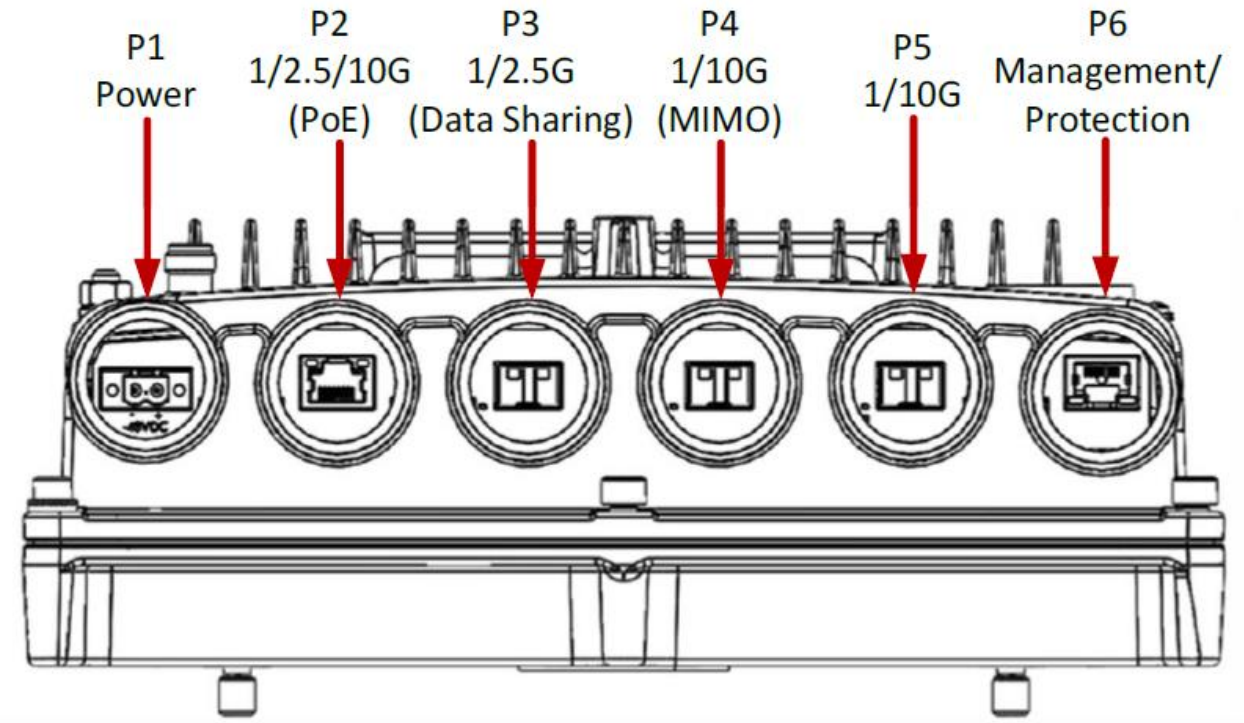


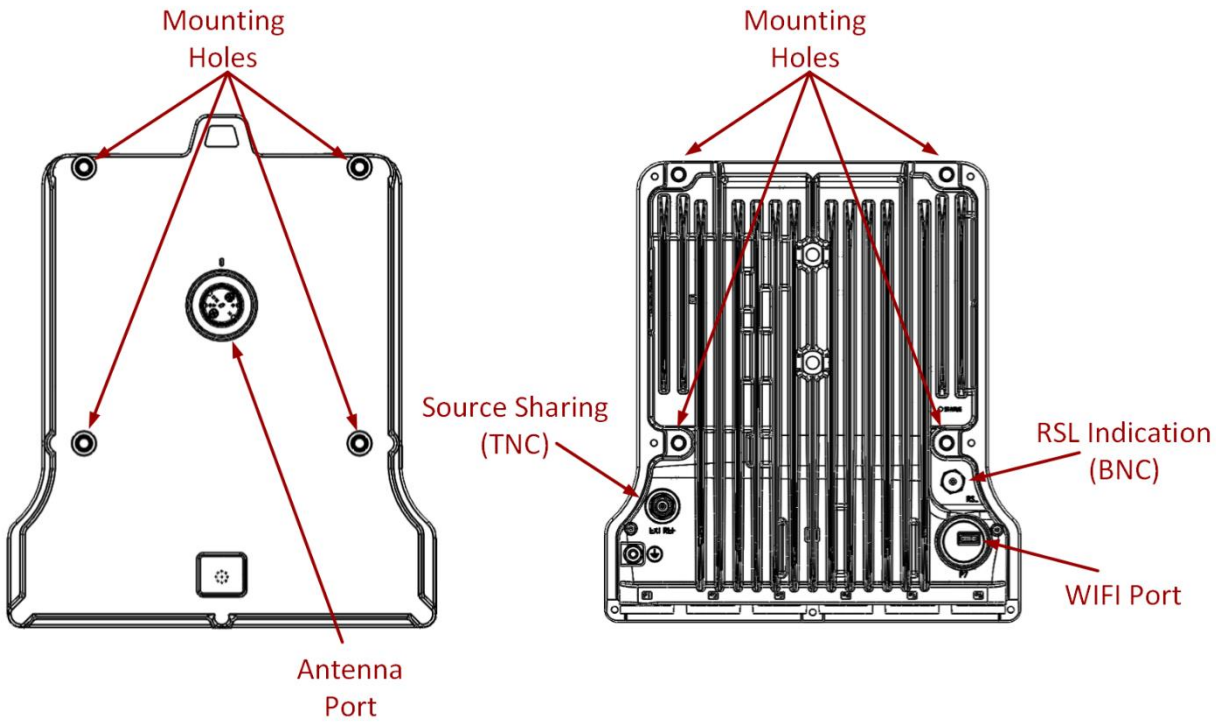
Figure 15 – IP-50C Physical Ports[9]

Physical port	Logical interface	Data that passes over port/interface
(1x) 1/2.5/10GbE Electrical Interface (1x) 1/2.5 GbE Electrical or Optical Interface (2x) 1/10GbE Electrical or Optical Interface (1x) RJ-45 GbE Management Interface (2x) Antenna Ports	Data Input	TLS v1.2/1.3, SSH, and SNMPv3 management traffic (RJ-45) Data traffic (Antenna ports, GbE)
(1x) 1/2.5/10GbE Electrical Interface (1x) 1/2.5 GbE Electrical or Optical Interface (2x) 1/10GbE Electrical or Optical Interface (1x) RJ-45 GbE Management Interface (2x) Antenna Ports	Data Output	TLS v1.2/1.3, SSH, and SNMPv3 management traffic (RJ-45) Data traffic (Antenna ports, GbE)
(1x) RJ-45 GbE Management Interface	Control Input	TLS v1.2/1.3, SSH, and SNMPv3 management traffic (RJ-45)

[9] The WiFi port is disabled.

Physical port	Logical interface	Data that passes over port/interface
(1x) Source Sharing		Signaling (Source Sharing)
(1x) RJ-45 GbE Management Interface (1x) RSL Indication	Status Output	TLS v1.2/1.3, SSH, and SNMPv3 management traffic (RJ-45) RSL signaling (RSL)
(1x) -48V DC Power Interface	Power Input	N/A

Table 12 – IP-50C Ports and Interfaces



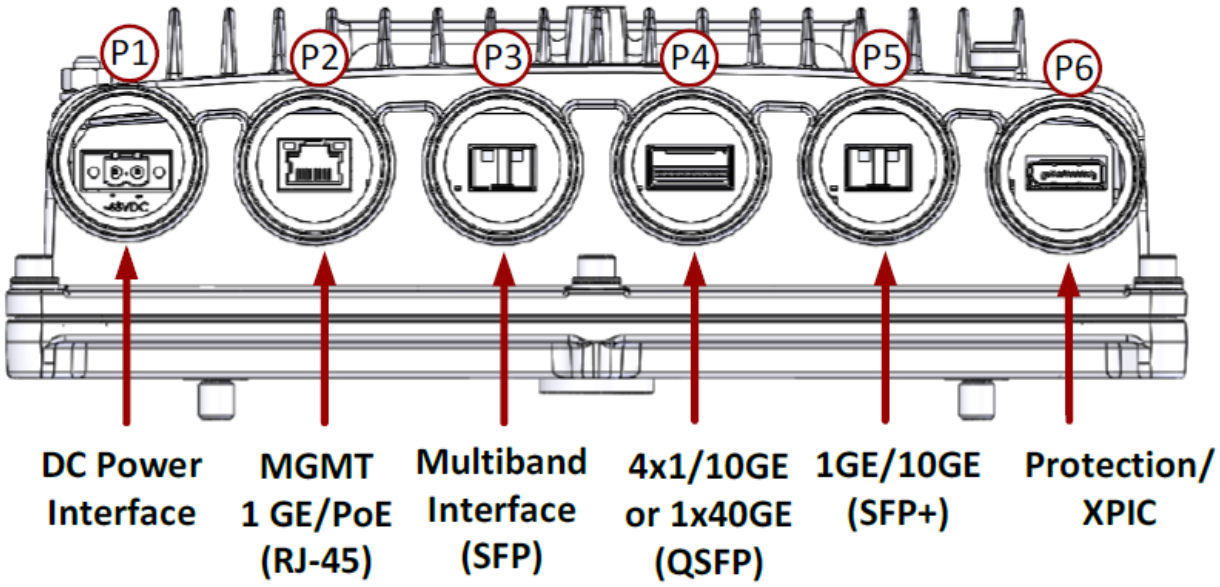


Figure 16 – IP-50E Physical Ports

Physical port	Logical interface	Data that passes over port/interface
(1x) 1/2.5GbE Multiband Interface (1x) 4x1/10GbE or 1x40GbE Electrical or Optical Interface (1x) 1/10GbE Electrical Interface (1x) RJ-45 GbE Management Interface (2x) Antenna Ports	Data Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) XPIC data (XPIC/IPsec) Data traffic (Antenna ports, GbE)
(1x) 1/2.5GbE Multiband Interface (1x) 4x1/10GbE or 1x40GbE Electrical or Optical Interface (1x) 1/10GbE Electrical Interface (1x) RJ-45 GbE Management Interface (2x) Antenna Ports	Data Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) XPIC data (XPIC/IPsec) Data traffic (Antenna ports, GbE)
(1x) RJ-45 GbE Management Interface (1x) Source Sharing (1x) Protection/XPIC	Control Input	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) XPIC data (XPIC/IPsec) Signaling (Source Sharing)

Physical port	Logical interface	Data that passes over port/interface
(1x) RJ-45 GbE Management Interface (1x) RSL Indication	Status Output	TLS v1.2/1.3, SSH, IPSec, and SNMPv3 management traffic (RJ-45) XPIC data (XPIC/IPsec) RSL signaling (RSL)
(1x) -48V DC Power Interface (1x) RJ-45 GbE Management Interface (PoE)	Power Input	N/A
WIFI Port	N/A	This port is disabled

Table 13 – IP-50E Ports and Interfaces

4. 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.

4.1 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 the Session keys. The Session keys are established from the remote peer using the Master Key to encrypt them. Successful decryption of the Session keys by the module, authenticates the User to the module. The CO is responsible for configuring the Master Key and the User role to pass encrypted data. Once the User is authenticated to the module, encrypted data can be transferred to and from the remote peer. If the CO does not configure the data-path for encryption, the User can still send un-encrypted data (bypass mode).

The following table specifies roles, with corresponding service with input and output:

Role	Service	Input	Output
Crypto Officer	Show Status	Web GUI forms, CLI commands	Web GUI status, CLI return messages

Role	Service	Input	Output
Crypto Officer	Perform Self-Tests	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	Change Password	Web GUI forms, CLI commands	Web GUI status, CLI return messages
User	Transmit/Receive Data	Data plane packets	Data plane packets
Crypto Officer	Administrative access over SSH	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	Administrative access over Web EMS	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	SNMPv3	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	Key Entry	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	IPSEC	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	Zeroize	Web GUI forms, CLI commands	Web GUI status, CLI return messages
N/A	Cycle Power	N/A	N/A
N/A	Status LED Output	N/A	LED Status
Crypto Officer	View Summaries	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	Platform Management	Web GUI forms, CLI commands	Web GUI status, CLI return messages

Role	Service	Input	Output
Crypto Officer	Fault Management	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	Radio Configuration	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	Ethernet Configuration	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	Sync Settings	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	Utilities	Web GUI forms, CLI commands	Web GUI status, CLI return messages
Crypto Officer	RBN	Web GUI forms, CLI commands	Web GUI status, CLI return messages

Table 14 – Roles, Service Commands, Input and Output

4.2 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.

Role	Authentication Method	Authentication Strength
CO	Password/Username	All passwords must be at least 8 characters and must 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. 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.
Users	AES-256 Master Key	When using AES key-based authentication, the key has a size of 256-bits. Therefore, an attacker would have a 1 in

Role	Authentication Method	Authentication Strength
		2^256 chance of randomly obtaining the key, which is much stronger than the one in a million chance. 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.

Table 15 – Roles and Authentication

4.3 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 tables below. The module supports a global indicator of "enabled" when the module is in the Approved mode and an indicator of "disabled" when the module is in the non-Approved mode. Please note that the keys and Sensitive Security Parameters (SSPs) listed below use the following indicators to show the type of access required:

- **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.
- **E = Execute:** The module uses the SSP in performing a cryptographic operation.
- **Z = Zeroise:** The module zeroises the SSP.

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSP's	Indicator
Show Status	Provides status of the module and module versioning	N/A	N/A	CO	N/A	N/A
Perform Self-Tests	Used to initiate on-demand self-tests (via power-cycle)	N/A	N/A	CO	N/A	N/A
Change Password	Update password with a new value	N/A	Crypto Officer Password CO Password Hash	CO	Crypto Officer Password (R/W) CO Password Hash (E)	N/A
Transmit/Receive Data	Encrypt/Decrypt data passing through the module	AES-OFB AES-ECB AES-CTR AES-KW	Session Key Tx Session Key Rx Master Key	User	Session Key Tx (R/W/Z) Session Key Rx (R/W/Z) Master Key (R)	Admin status (enabled)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSP's	Indicator
	(Bypass mode when feature is not enabled)	KTS (AES-KW)				
Administrative access over SSH	Secure remote command line appliance administration over an SSH tunnel.	AES-CTR HMAC KAS-ECC-SSC KAS-FFC-SSC KTS RSA SHS SSH KDF DRBG CKG DSA ECDSA	DRBG entropy input DRBG Seed DRBG V DRBG Key Diffie-Hellman / EC Diffie Hellman Shared Secret Diffie Hellman / EC Diffie Hellman private key Diffie Hellman / EC Diffie Hellman public key SSH Private Key SSH Public Key SSH Session Key SSH Integrity Key	CO	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)	Admin status (enabled) and session logs
Administrative access over Web EMS	Secure remote GUI appliance administration over a TLS tunnel.	AES-CBC AES-GCM HMAC KAS-ECC-SSC KAS-FFC-SSC KTS SHS RSA TLSv 1.2 KDF TLS v1.3 KDF DRBG CKG	DRBG entropy input DRBG Seed DRBG V DRBG Key Diffie-Hellman / EC Diffie Hellman Shared Secret Diffie Hellman / EC Diffie Hellman private key Diffie Hellman / EC Diffie	CO	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)	Admin status (enabled) and session logs

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSP's	Indicator
		DSA ECDSA	Hellman public key TLS Private Key TLS Public Key TLS Pre-Master Secret TLS Master Secret TLS Session Encryption Key TLS Session Integrity Key		TLS Pre-Master Secret (G/E/Z) TLS Master Secret (G/E/Z) TLS Session Encryption Key (G/E/Z) TLS Session Integrity Key (G/E/Z)	
SNMPv3	Secure remote SNMPv3-based system monitoring.	AES-CFB128 HMAC SHS SNMP KDF	SNMP Session Key SNMP Session Authentication Key SNMPv3 password	CO	SNMP Session Key (R/W/Z) SNMP Session Authentication Key (R/W/Z) SNMPv3 password (R/W/Z)	Admin status (enabled) and session logs
Key Entry	Enter key over management interfaces	KTS	Master Key	CO	Master Key (R/W)	Admin status (enabled) and session logs
IPSec[10]	Control plane traffic encryption using IKEv1 for key exchange (Self-initiated cryptographic output capability)	AES-CBC HMAC SHS KTS KAS-FFC-SSC DSA IKEv1 KDF	IKE session encrypt key IKE session authentication key ISAKMP preshared key IPsec encryption key IPsec authentication key Diffie Hellman Shared Secret Diffie Hellman private key	CO	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) Diffie Hellman Shared Secret (R/W/Z) Diffie Hellman private key (R/W/Z) Diffie Hellman public key (R/W/Z)	Admin status (enabled)

[10] Only available on MIPS CPU based models

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSP's	Indicator
			Diffie Hellman public key			
Zeroize	Zeroize all CSPs	N/A	All CSPs	CO	All CSPs (Z)	Admin status (enabled)
Cycle Power	Reboot of module	N/A	DRBG entropy input DRBG Seed DRBG V DRBG Key Diffie-Hellman / EC Diffie Hellman Shared Secret Diffie Hellman / EC Diffie Hellman private key Diffie Hellman / EC Diffie Hellman public key SSH Session Key SSH Integrity Key SNMPv3 session key SNMPv3 session authentication key TLS Pre-Master Secret TLS Master Secret TLS Session Encryption Key TLS Session Integrity Key IKE session encrypt key	N/A	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 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)	Console log

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSP's	Indicator
			IKE session authentication key IPsec encryption key IPsec authentication key Session Key Tx Session Key Rx			
Status LED Output	View status via the modules' LEDs	N/A	N/A	N/A	N/A	N/A
View Summaries	View unit summary information (Unit, Radio, Security)	N/A	N/A	CO	N/A	Admin status (enabled)
Platform Management	Shelf management, unit configuration, interfaces, firmware settings, activation key, and statistics	N/A	N/A	CO	N/A	Admin status (enabled)
Fault Management	Alarm settings	N/A	N/A	CO	N/A	Admin status (enabled)
Radio Configuration	Radio interface settings (includes Bypass setting and status)	N/A	N/A	CO	N/A	Admin status (enabled)
Ethernet Configuration	Ethernet interface settings	N/A	N/A	CO	N/A	Admin status (enabled)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to Keys/SSP's	Indicator
Sync Settings	Manage synchronization	N/A	N/A	CO	N/A	Admin status (enabled)
Utilities	Generic utilities	N/A	N/A	CO	N/A	Admin status (enabled)
RBN	Bandwidth notification	N/A	N/A	CO	N/A	Admin status (enabled)

Table 16 – Approved Services

Service	Description	Algorithms Accessed	Role	Indicator
SNMPv1/v2c	Secure remote SNMPv1, v2c-based system monitoring.	N/A	CO	Admin status (disabled)
RADIUS	RADIUS authentication	MD5		Admin status (disabled)
TACACS+	TACACS+ authentication	MD5		Admin status (disabled)
HTTP	Plaintext HTTP	N/A		Admin status (disabled)
Hot Standby	Hot Standby	N/A		Admin status (disabled)
Syslog	Audit log forwarding	N/A		Admin status (disabled)
NTP	Network Time Protocol servers	N/A		Admin status (disabled)
Telnet	Plaintext CLI access	N/A		Admin status (disabled)

Table 17 – Non-Approved Services

5. Software/Firmware Security

The module performs a Firmware Integrity Test using a 160-bit error detection code (EDC) at power-on. If the EDC fails to compute properly, the module enters a hard error state where all cryptographic functions are disabled. Repeated failures of the integrity test will result in a reset to the factory default state. The integrity test may be performed on-demand by power-cycling the module. The module also performs a firmware load test (RSA 4096 with SHA2-256) covering the entire binary image, when a new FW is uploaded to the module. The signature is calculated and verified upon uploading of the new FW. If the test fails, the image will be discarded.

6. Operational Environment

FIPS 140-3 Operational Environment requirements are not applicable since the module is a hardware module with a limited operational environment. The module runs Release 12.0.1 which includes Wind River Linux 4.1.0 or 4.14 depending on the CPU architecture.

7. Physical Security

The appliances have a multi-chip standalone embodiment. 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 have been designed to satisfy Level 2 physical security requirements.

Each of the appliances needs Tamper Evidence Labels (TELs) to meet Security Level 2 requirements. These labels are installed (as seen in the respective model images) at the factory before delivery to the customer, for the IP-20G, IP-20C, IP-20S, IP-20C-HP, IP-50C and IP-50 E. For IP-20N and IP-20A, the CO must place the twenty (20) TELs according to Figure 21-24 (below).

The preparation instructions of the module prior to installation of the tamper seals are as follows:

- Use caution to avoid touching the adhesive in such a way as to leave fingerprints and damage the labels.
- The curing time (drying time) for the labels is at least sixty minutes.
- The labels must be replaced whenever cards are added to or removed from the unit. Replacement labels can be ordered from Ceragon Networks, part number BS-0341-2.
- When replacing a label, gently cut the label, replace the module, and apply a new label in place of the previous label.

The extra tamper seals shall be in possession of the CO at all times. The CO shall observe any changes to the module such as reconfigurations where the tamper evident seals are removed or installed to ensure the security of the module is maintained during such changes and the module is returned to an Approved mode of operation. The Crypto Officer shall periodically (defined by organizational security policy, recommendation is once a month) monitor the state of all applied TELs 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 the Approved state.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evidence Label	During regular physical maintenance operations. At least every six months.	Inspect the labels for obvious signs of damage/removal. Placement should be according to the figures below.

Table 18 – Physical Security Inspection Guidelines

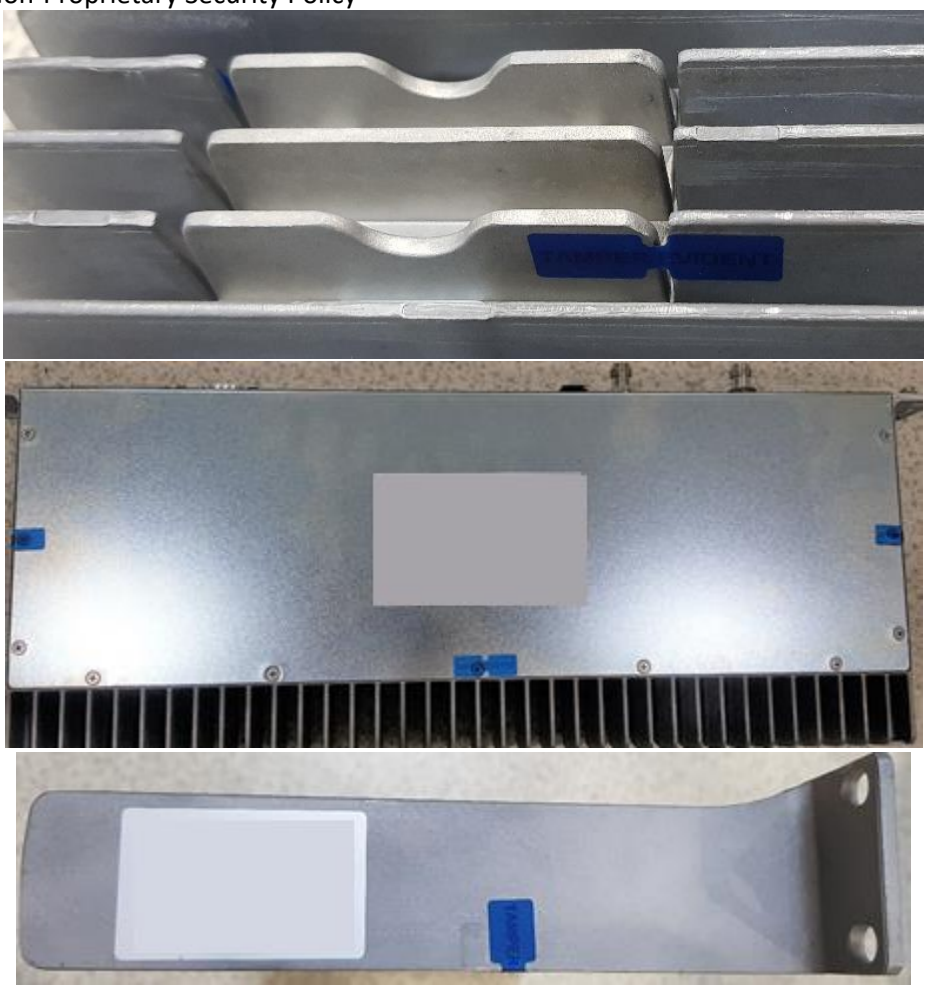


Figure 17 – IP-20G TEL Application Locations

Figure 18 – IP-20C TEL Application Locations

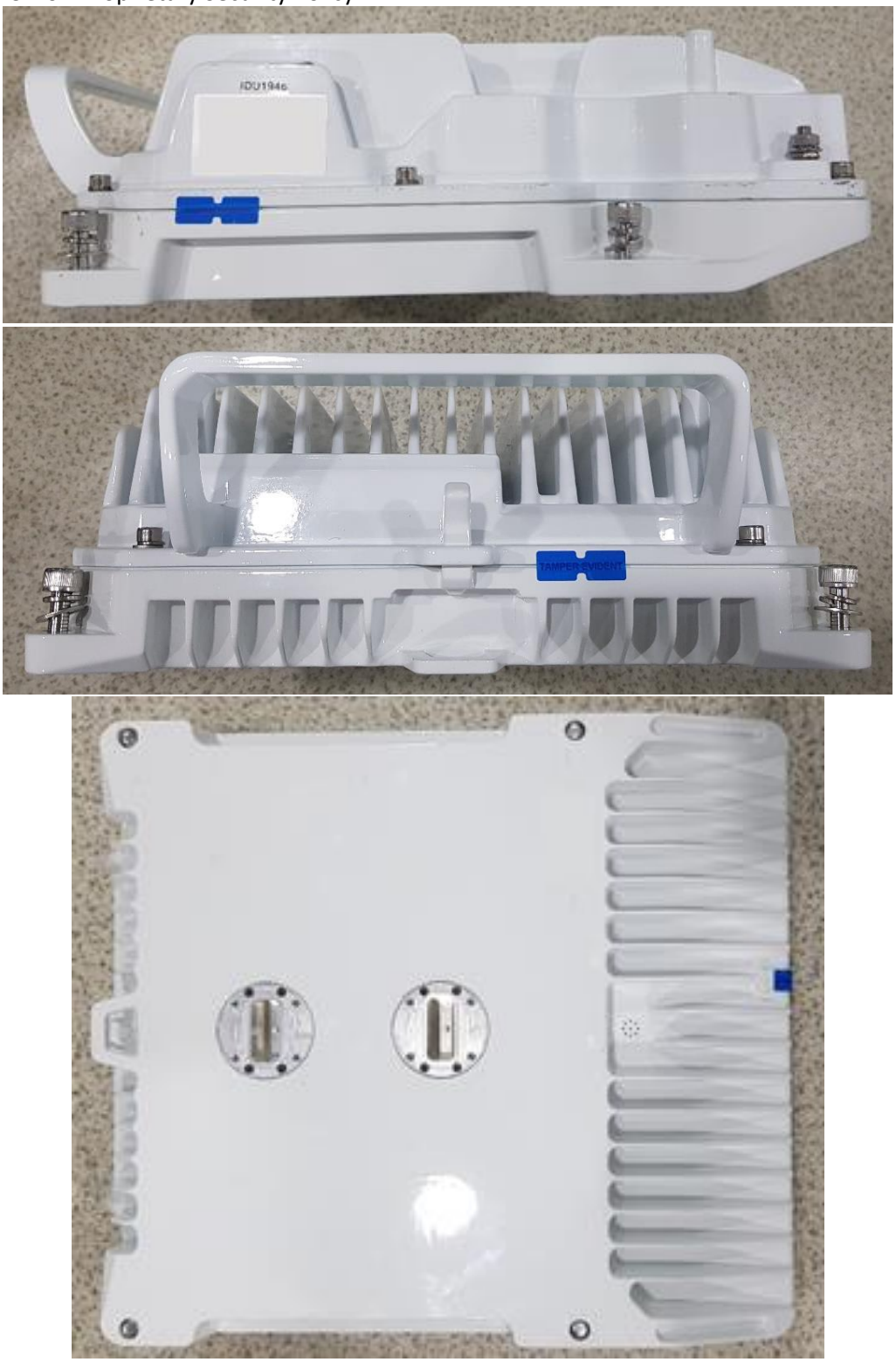


Figure 19 – IP-20C-HP TEL Application Locations

Figure 20 – IP-20S TEL Application Locations

Figure 21 – IP-20N and IP-20A Bottom

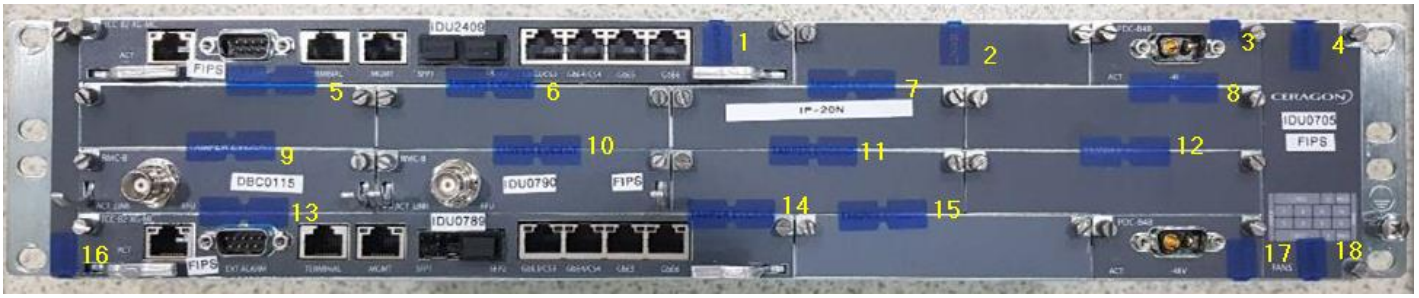
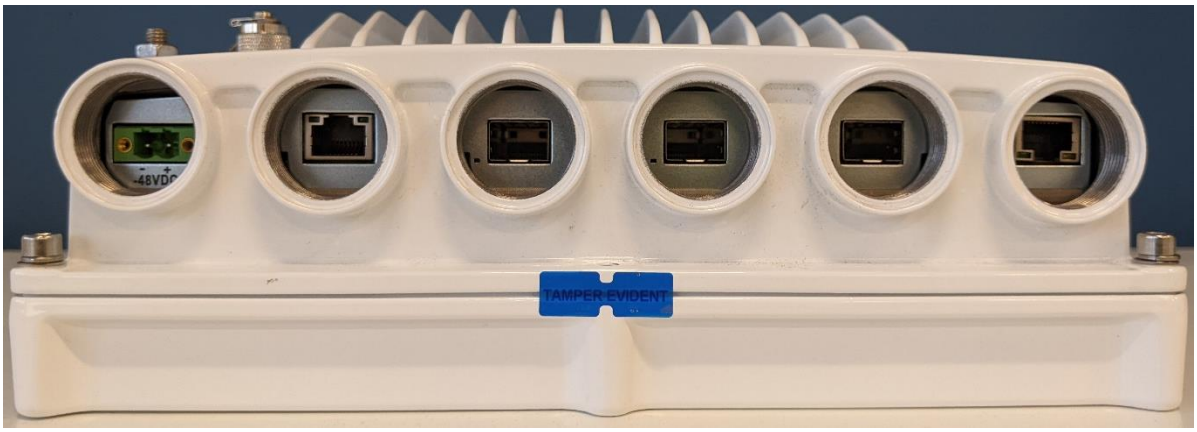


Figure 22 – IP-20N and IP-20A Front

Figure 23 – IP-20N and IP-20A Top

Figure 24 – IP-20N and IP-20A Back



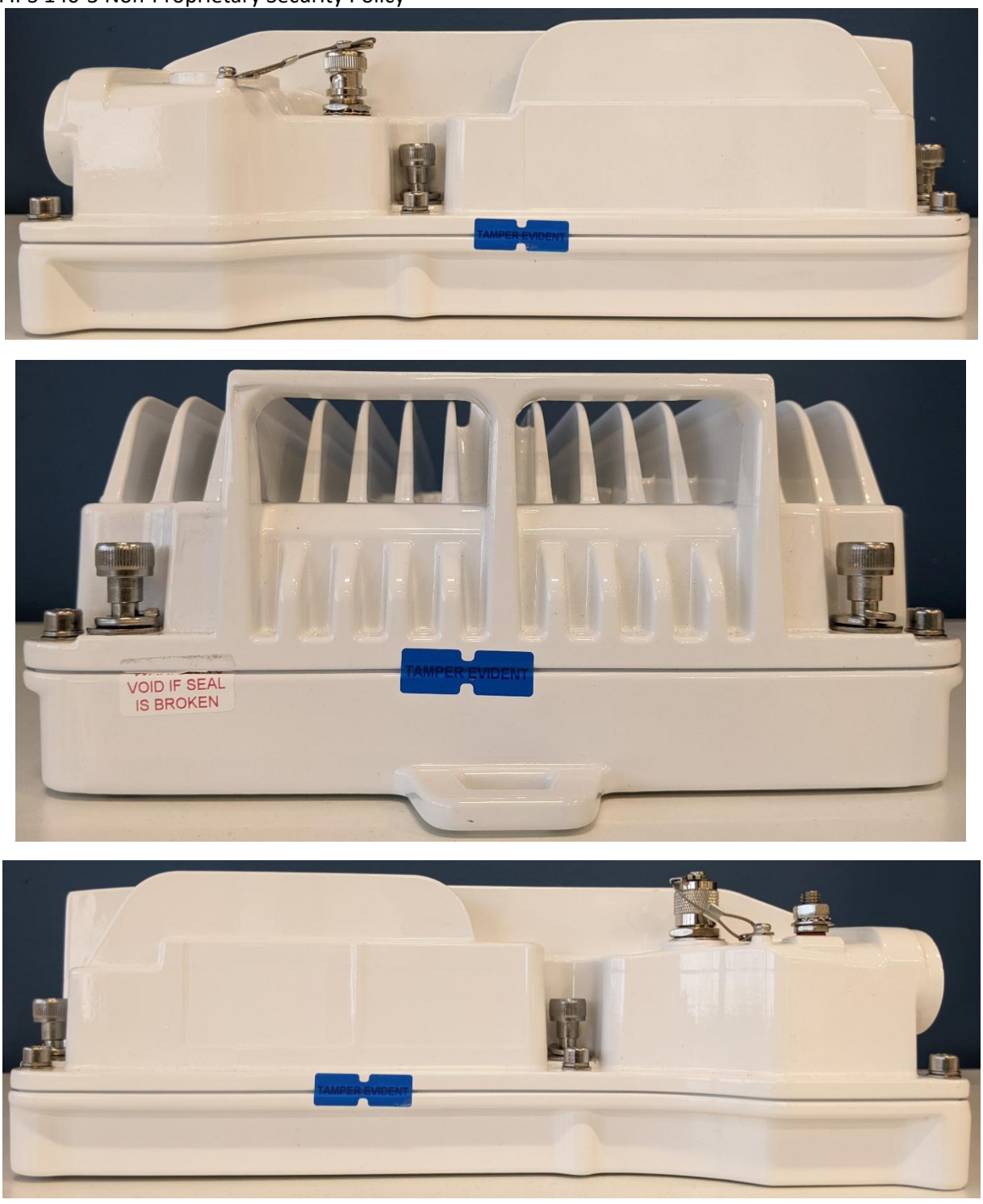


Figure 25 – IP-50C/IP-50E TEL Application Locations

8. Non-invasive Security

FIPS 140-3 Non-invasive Security requirements are not applicable.

9. Sensitive security parameter management

The following table identifies each of the Keys/SSPs associated with the modules:

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
DRBG entropy input (CSP)	256-bit	DRBG A2758	Generated using module entropy source	N/A	N/A	Plaintext temporarily in RAM	Device power cycle or cleared after use	Used for control/ management plane random bit generation
DRBG Seed (CSP)	256-bit	DRBG A2758	Generated using SP 800-90Ar1 DRBG seed construction	N/A	N/A	Plaintext temporarily in RAM	Device power cycle or cleared after use	Seed used for DRBG instantiation and reseed
DRBG V (CSP)	256-bit	DRBG A2758	SP 800-90Ar1 DRBG Internal State	N/A	N/A	Plaintext temporarily in RAM	Device power cycle or cleared after use	Used for control/ management plane random bit generation
DRBG Key (CSP)	256-bit	DRBG A2758	SP 800-90Ar1 DRBG Internal State	N/A	N/A	Plaintext temporarily in RAM	Device power cycle or cleared after use	Used for control/ management plane random bit generation
Diffie Hellman Shared Secret (CSP)	112 and 128 bits	KAS-FFC-SSC 2048 bits	N/A	N/A	Established using SP 800-	Plaintext temporarily in RAM	Device power cycle or	Used for key transport on the management plane using Diffie-Hellman; key

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
		and 3072 bits A2758			56Arev3 KAS-SSC		cleared after use Termination of protocol session	establishment methodology provides 112 and 128 bits of encryption strength
EC Diffie Hellman Shared Secret (CSP)	128-bit	KAS-ECC-SSC P-256 A2758	N/A	N/A	Established using SP 800-56Arev3 KAS-SSC	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for key transport on the management plane using Elliptic Curve Diffie-Hellman; key establishment methodology provides 128 bits of encryption strength
Diffie Hellman private key (CSP)	112 and 128 bits	KAS-FFC-SSC 2048 bits and 3072 bits A2758; DSA A2758	Generated according to SP 800-56Arev3	N/A	N/A	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for key transport on the management plane using Diffie-Hellman; key establishment methodology provides 112 and 128 bits of encryption strength
EC Diffie Hellman private key (CSP)	128-bit	KAS-ECC-SSC P-256 A2758; ECDSA A2758	Generated according to SP 800-56Arev3	N/A	N/A	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for key transport on the management plane using Elliptic Curve Diffie-Hellman; key establishment methodology provides

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
								128 bits of encryption strength
Diffie Hellman public key (PSP)	112 and 128 bits	KAS-FFC-SSC 2048 and 3072 bits A2758; DSA A2758	Generated according to SP 800-56Arev3	Output in plaintext	N/A	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for key transport on the management plane using Diffie-Hellman; key establishment methodology provides 112 and 128 bits of encryption strength
EC Diffie Hellman public key (PSP)	128-bit	KAS-ECC-SSC P-256 A2758; ECDSA A2758	Generated according to SP 800-56Arev3	Output electronically in plaintext	N/A	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for key transport on the management plane using Elliptic Curve Diffie-Hellman; key establishment methodology provides 128 bits of encryption strength
SSH Private Key (CSP)	112-bit	RSA 2048-bit A2758	Generated according to FIPS 186-4	Entered electronically in encrypted form via approved KTS-2, KTS-3 or KTS-5	N/A	Plaintext persistently in Flash	Zeroization command	Used for control and management plane authentication
SSH Public Key (PSP)	112-bit	RSA 2048-bit A2758	Generated according to FIPS 186-4	Output electronically in plaintext	N/A	Plaintext persistently in Flash	Zeroization command	Used for control and management plane authentication

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
SSH Session Key (CSP)	128, 192 or 256-bits	AES-CTR (128, 192, 256), AES-GCM (128, 256), SSH KDF A2758	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for control and management plane privacy
SSH Integrity Key (CSP)	160, 256 or 512-bits	HMAC, SSH KDF A2758	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle Termination of protocol session	Used for message integrity check in the control and management plane
SNMPv3 password (CSP)	Shared Secret, at least eight characters	SNMP KDF A2757	N/A	Entered electronically in encrypted form via approved KTS-2, KTS-3 or KTS-5	N/A	Plaintext persistently in Flash	Zeroization command	Used for key derivation within management protocols
SNMPv3 session key (CSP)	128-bit	SNMP KDF A2757, AES CFB128 A2758	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for encryption/decryption within management protocols

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
SNMPv3 session authentication key (CSP)	160-bit	SNMP KDF A2757, HMAC A2758	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for message integrity check within management protocols
TLS Private Key (CSP)	112-bit	RSA 2048-bit A2758	Generated according to FIPS 186-4	N/A	N/A	Plaintext persistently in Flash	Zeroization command	Used for authentication within management protocols
TLS Public Key (PSP)	112-bit	RSA 2048-bit A2758	Generated according to FIPS 186-4	Output electronically in plaintext	N/A	Plaintext persistently in Flash	Zeroization command	Used for authentication within management protocols
TLS Pre-Master Secret (CSP)	384-bit	KAS-FFC-SSC, KAS-ECC-SSC A2758	N/A	N/A	Established according to SP 800-56Arev3	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for key derivation within the TLS management protocol
TLS Master Secret (CSP)	384-bit	TLS 1.2 KDF A2758	N/A	N/A	Calculated as an element of the TLS 1.2 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for key derivation within the TLS management protocol. Derived from the TLS Pre-Master Secret

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
TLS Session Encryption Key (CSP)	128 or 256- bits	AES GCM, AES CBC A2758 TLS KDF A2758	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for encryption/decryption within management protocols
TLS Session Integrity Key (CSP)	160, 256 or 384-bits	HMAC SHA-1, SHA2-256, SHA2-384 A2758 TLS KDF A2758	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for message integrity check in the control and management plane
IKE session encrypt key (CSP)	256-bit	AES CBC A2755, IKEv1 KDF A2756	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for encryption/decryption within IPsec
IKE session authentication key (CSP)	256-bit	HMAC A2755, IKEv1 KDF A2756	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use	Used for message authentication within IPsec

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
							Termination of protocol session	
ISAKMP preshared (CSP)	Secret, 32 characters	IKEv1 KDF A2756	N/A	Entered electronically in encrypted form via approved KTS-2, KTS-3 or KTS-5	N/A	Plaintext temporarily in RAM	Zeroization command	Used for key derivation within IPsec
IPsec encryption key (CSP)	256-bit	AES CBC 2755, IKEv1 KDF A2756	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for encryption/decryption within IPsec
IPsec authentication key (CSP)	256-bit	HMAC, SHA2-256 A2755, IKEv1 KDF A2756	N/A	N/A	Derived using SP 800-135rev1 KDF	Plaintext temporarily in RAM	Device power cycle or cleared after use Termination of protocol session	Used for message authentication within IPsec
Session key Tx (CSP)	256-bit	AES CTR A680 or	Generated using DRBG	Electronically entered and output in	N/A	Plaintext temporarily in RAM	Device power cycle or	Used for encryption/decryption within data plane

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
		AES OFB 4014		encrypted form via approved KTS-1 or KTS-4			cleared after use Data plane rekey	
Session key Rx (CSP)	256-bit	AES CTR A680 Or AES OFB 4014	Generated using DRBG	Electronically entered and output in encrypted form via approved KTS-1 or KTS-4	N/A	Plaintext temporarily in RAM	Device power cycle Data plane rekey	Used for encryption/decryption within data plane
Master key (CSP)	256-bit	AES KW AES ECB A2758	N/A	Electronically entered via KTS-2, KTS-3 or KTS-5	N/A	Plaintext persistently in Flash	Zeroization command	Used for session key encryption for session key exchange between local and remote units
Crypto Officer Password (CSP)	95[8]	N/A	N/A	Electronically entered in encrypted form via approved KTS-2, KTS-3 or KTS-5	N/A	SHA2-512 hash persistently in Flash	Zeroization command	Used for Crypto Officer login
CO Password Hash	SHA2-512	SHA2-512 A2758	Generated upon	N/A	N/A	Persistently in Flash	Zeroization command	Used to verify Crypto Officer login

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/Export	Establishment	Storage	Zeroisation	Use & related keys
			password creation					

Table 19 – SSPs

9.1 Generation

The module generates symmetric and asymmetric keys in compliance with the requirements of the FIPS 140-3 standard. Specifically, symmetric keys are generated using output of the Approved SP 800-90A DRBG and in compliance with IG D.H. Asymmetric keys are generated as part applicable key generation standards. See Table 19 for additional details.

9.2 Import/Export

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 an approved KTS using a Master Key with the AES-KW algorithm. Additionally, SSPs provisioned by an operator can be entered using an approved KTS employing AES-GCM or AES and HMAC within the SSH, TLS, or IPsec protocols. See Table 19 for additional details.

9.3 Storage

SSPs are stored in plaintext in non-volatile and volatile memory. See Table 19 for additional details.

9.4 Zeroization Procedures

SSPs stored in volatile memory are zeroized automatically when no longer needed. SSPs stored in non-volatile memory are zeroized after repeated failure of the Pre-Operational Self-Tests or upon hard-zeroization command issued. The zeroization will permanently erase SSPs stored in Flash by overwriting with zeroes. When zeroization occurs via power cycle or the zeroization command the module provides an indicator in the console log. When zeroization occurs via session termination the zeroization indicator is provided via session log. For CSPs that are zeroized after use, the indicator is that the service continues. If there is a zeroization error, the service in process will be terminated. See Table 19 for additional details.

Entropy Sources	Minimum number of bits of entropy	Details
ENT (P)	The entropy source provides 2.79 bits of entropy per 8-bit sample. To achieve a security strength of 256 bits, the DBRG's deviation function will require a seed length of at least 138 samples. The DRBG is seeded with 2048 bits (256 samples) of data providing approximately 714 bits of entropy which is sufficient for generating the largest module SSPs of a maximum of 256 bits of security strength.	Ring-oscillator noise source with no conditioning function. Conformant to SP 800-90B and IG D.J and D.K

Table 20 – Non-Deterministic Random Number Generation Specification

10. 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 140-3 broadly fall within two categories:

1. Pre-Operational Self-Tests
2. Conditional Self-Tests

When the module is powered on, its power-up self-tests are executed without any operator intervention. CASTs are performed prior to first usage of an algorithm. The operator may run periodic self-tests by power-cycling the module.

Conditional tests are performed when a specific condition is met, such as usage of the entropy source or generation of key-pair.

10.1 Pre-Operational Self-Tests

The cryptographic module performs the following Pre-Operational Self-Tests on:

- Firmware Integrity Test: 160-bit Error detection code (EDC)
- Pre-operational Bypass Test

10.2 Conditional Self-Tests

The HW-based entropy source is conditionally tested (when entropy is consumed by any of the FW components). Tests are APT and RCT (mentioned in the SP 800-90B document).

The cryptographic module performs the following conditional self-tests:

- Conditional Cryptographic Algorithm Self-Tests:
  - Management Security Algorithms Implementation (Firmware) (Cert. #A2758):
    - HMAC-SHA2-256 CAST
    - SHA-1 CAST
    - SHA2-512 CAST
    - AES-128 ECB Decrypt CAST
    - AES KeyWrap Encrypt CAST
    - AES KeyWrap Decrypt CAST
    - AES-256 GCM Encrypt CAST
    - RSA PKCS#1 Sign/Verify CASTs
    - ECDSA Sign/Verify CASTs
    - DH Shared Secret Computation CAST
    - ECDH Shared Secret Computation CAST
    - TLS 1.2 KDF CAST
    - TLS 1.3 KDF CAST
    - SSH KDF CAST
    - DRBG CAST
  - IKE KDF Implementation (Firmware) (Cert. #A2756):
    - IKE KDF CAST
  - SNMP KDF Implementation (Firmware) (Cert. #A2757):

    - SNMP KDF CAST
  - Linux Kernel Crypto Implementation (Firmware) (Cert. #A2755):
    - AES-256 CBC Encrypt CAST
    - AES-256 CBC Decrypt CAST
    - HMAC-SHA2-256 CAST
    - SHA2-256 CAST
  - AES Core Implementation (Hardware):
    - AES-256 OFB Encrypt CAST (Cert. #AES 4014)
    - AES-256 OFB Decrypt CAST (Cert. #AES 4014)
    - AES-256 CTR Encrypt CAST (Cert. #A680)
    - AES-256 CTR Decrypt CAST (Cert. #A680)
  - Entropy Self-tests
    - SP 800-90B Repetition Count Test
    - SP 800-90B Adaptive Proportion Test
    - SP 800-90A Health Tests

- Conditional Pair-wise Consistency Self-Tests:
  - Pairwise Consistency Test (PWCT) for RSA
  - Pairwise Consistency Test (PWCT) for ECDSA
  - Pairwise Consistency Test (PWCT) for DSA
- Conditional software/firmware load test
  - Firmware Load Test (RSA 4096/SHA2-256 Signature Verification)

- Conditional Bypass Test

10.3 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 “Failed powerOnSelfTest”. If the failure persists after power-cycle, the module will then be placed in a Default State (where all keys/CSPs are zeroized) and the Approved mode enabled flag is reset to disabled. The module will enter the non-approved mode. Event logs will be updated accordingly.

If either of the SP 800-90B self-tests 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 conditional Bypass self-test fails, the error is reported, and the module does not transition into or out of bypass.

During execution of the self-tests, firmware loading, zeroization, and while in an error state, data output is inhibited.

11. Life-cycle assurance

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

11.1 Secure Operation

When configured as per this section of the Security Policy, the module only runs in the Approved mode of operation, with the exception of the non-Approved Services identified in Table 17. The non-Approved services described may make use of non-compliant cryptographic algorithms or plaintext data transfers. Use of these services is prohibited in an Approved mode of operation. The Crypto Officer is responsible for ensuring that any of the non-Approved Services (Table 17) in Section 4.3 are not used. Once the module is properly configured as outlined below, the non-Approved Services will not be available for use.

11.2 Installation

The module hardware is shipped in sealed boxes to indicate tamper. Upon delivery, the recipient should inspect the package to verify that there has been no tampering. IP-20G, IP-20C, IP-20S, IP-20C-HP, IP-50C, and IP-50E have a fixed configuration with TELs applied at factory. The Crypto Officer must verify at installation time that the TELs are affixed and intact.

IP-20N, and IP-20A have variable configurations and the CO must verify that they are configured as per one of the approved configurations identified in Section 2.1, Table 2. Moreover, the Crypto Officer must verify at installation time that the TELs are affixed and intact. The tamper evident seals installed as indicated in Section 7 are required for the module to be operated in the Approved mode of operation.

Please refer to the figures in Section 7 of this document for the proper placement of TELs.

11.3 Initialization

The CO must follow these steps to place the module in an Approved 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* for precise details.

1. Enable Password Enforcement to enforce password strength.

7.10 Configuring Login and Password Settings

- Select **Quick Configuration > Security > Access Control.**
- In the **Password change for first login** field, select **Yes.**
- In the **Enforce password strength** field, select **Yes.**

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

7.10 Configuring Login and Password Settings

- In the **Failure login attempts to block user** field, select the number of failed login attempts (3) that will trigger blocking.

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 for CO operators in Section 4 above. Ensure that “AES” and “SHA” are selected for the privacy and authentication ciphers, respectively.

7.9 Configuring SNMPv3

- Select **Quick Configuration > Security > Protocols**. The Quick Configuration Security Protocols page opens (*Figure 41*).
- In the **SNMP Admin** field, select **Enable** to enable SNMP
- In the **V1V2 Blocked** field, select **Yes** to block SNMPv1 and SNMPv2 access so that only SNMPv3 access will be enabled.

5. Disable Telnet

7.8 Blocking Telnet Access

- Select **Quick Configuration > Security > Protocols**.
- In the **Telnet Admin** field, select **Disable**.
- Click **Apply**.

6. Disable HTTP and enable HTTPS

7.7 Configuring HTTPS

- Select **Quick Configuration > Security > Protocols**.
- In the **HTTP protocol** field, select HTTPS

7. [Optional step] in case of External Protection configuration (relevant for IP-20G, IP-20C, IP-20S, IP-20C-HP), enable Protection Admin and supply a pre-shared key.

- *8.1 Encrypting the Protection Link*

8. [Optional step] In case of TCC Redundancy (relevant for IP-20N, IP-20A), 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 the Approved Mode

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

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

9. Change the default CO password

- *3.4 Changing Your Password*

10. Enable Approved Admin configuration, i.e., set operation mode to ‘Approved mode’.

- *7.1 Enabling 'Approved Mode'*

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 Approved mode status can be verified by selecting the **Security Summary** from the Web EMS main menu. The field for "FIPS Mode Admin" shows "enabled".

- *6 Viewing the Security Parameters*

11.4 Management

Protocols such as Telnet, RADIUS, TACACS+, HTTP, SNMPv1, and SNMPv2, Syslog, Hot Standby, NTP are not approved for use in the Approved mode and shall remain disabled.

When in FIPS 140-3 compliant mode, only the following algorithms are used for SSH and TLS communications.

11.4.1 SSH Usage

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

- aes128-ctr
- aes192-ctr
- aes256-ctr
- aes128-gcm@openssh.com
- aes256-gcm@openssh.com

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

- hmac-sha1

The following key exchange algorithms are supported in the Approved mode:

- ecdh-sha2-nistp256
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521
- diffie-hellman-group14-sha256
- diffie-hellman-group16-sha512
- diffie-hellman-group18-sha512

11.4.2 TLS Usage

When in the Approved mode, only the following cipher suites are available for TLSv1.2 communications:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA

When in the Approved mode, only the following cipher suites are available for TLSv1.3 communications:

- TLS_AKE_WITH_AES_256_GCM_SHA384
- TLS_AKE_WITH_AES_128_GCM_SHA256

11.5 Maintenance

There are no specific maintenance actions required.

12. Mitigation of other attacks

The module does not claim to mitigate any other attacks beyond those specified in FIPS 140-3.