Aviat Networks, Inc.

Aviat Networks Eclipse Cryptographic Module

FIPS 140-3 Non-Proprietary Security Policy

Document Version: 00E
Date: July 10, 2026

Aviat Networks, Inc.
200 Parker Drive, Suite C100A
Austin, Texas 78728
United States
(512) 265-3680
www.aviatnetworks.com

Prepared for Aviat Networks by

Rycombe Consulting Limited
http://www.rycombe.com +44 7780 682240

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version 10.01.03 of the Aviat Networks Eclipse Cryptographic Module. It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 2 module.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are as follows from Table 1:

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
	Overall Level	2

Table 1: Security Levels

1.3 Additional Information

For more information on Aviat Networks Eclipse please visit: https://aviatnetworks.com/products/all-outdoor/.

2 Cryptographic Module Specification

This Aviat Networks, Inc. Aviat Networks Eclipse Cryptographic Module, hereafter denoted as the Module. The Module is Aviat Networks Eclipse. Eclipse is an all-in-one next generation dual hybrid and packet microwave radio. Eclipse provides superior networking features to address cost-optimized mobile backhaul, public, and private networking applications, along with high performance RF and Carrier Ethernet capabilities. Aviat Eclipse delivers a "complete" set of microwave nodal networking capabilities. Eclipse delivers multi-directional integrated microwave switching within a single system, supporting up to 6 RF or up to 45 Ethernet radios in a single rack unit.

Eclipse also supports both native TDM and Ethernet services and provides fully integrated Ethernet switching and IP networking, eliminating the need for external TDM grooming or Ethernet aggregation devices.

Additionally, Eclipse can deliver greater than 2Gbps wireless transport with intelligent and fully integrated bandwidth optimization features like XPIC, ACM, and data compression.

The cryptographic module includes the Eclipse Intelligent Node Unit (INUe) chassis.

The Eclipse INUe supports hardware redundancy to maintain data traffic by protecting a link with a backup card that takes over in the event of hardware failure. It is possible to have up to 6 non-protected links or:

- 1 protected/diversity and 4 non-protected links
- 2 protected/diversity and 2 non-protected links
- 3 protected/diversity links

The module provides data security by encrypting the payload traffic on the microwave link between up to three radios. It also provides the Strong Encryption Suite for secure module management and uses AES encryption to secure SNMP v3 management traffic.

2.1 Description

Purpose and Use:

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated data encryption over a microwave radio link in a securely managed environment, the Module is intended to be used in a microwave network.
Module Type: Hardware

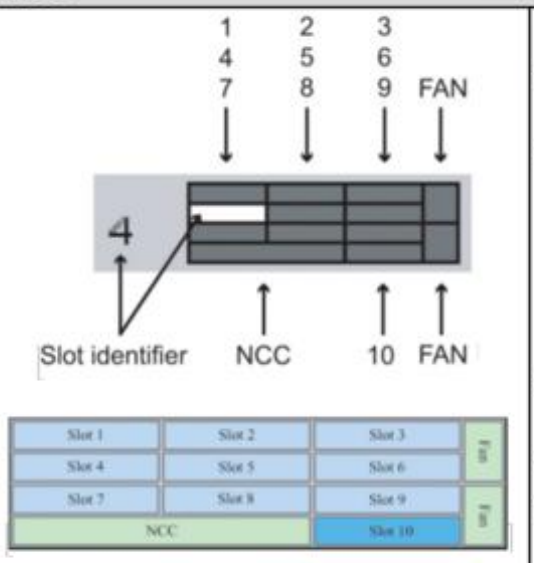
Module Embodiment: MultiChipStand

Module Characteristics:
The module runs on proprietary hardware. The hardware consists of a number of plug-in cards housed in a proprietary chassis in 2RU format (88mm high x 482mm wide x 282.5mm deep).

The module consists of an Eclipse Node Control Card (NCC), one or more Radio access cards (RAC)s and a number of other plug-in cards in combination. Only the NCC and RAC cards are involved with cryptography. The remaining cards provide physical security via tamper evidence but do not provide any other security-relevant functionality.

Figure 1 - Example INUe

INUe



The INUe slot numbering conventions are as follows:

- 1, 2, 3, 4, 5, 6 are universal slots for any RAC, DAC, NCM, or AUX.
- 7, 8, 9 are restricted. Backplane access to NMS is not supported on these slots, meaning they may be used for all DACs, NCM, and AUX except where they are to be used to transport NMS. This restriction only applies to DAC 155oM, DAC 155eM, and AUX (Other DACs and NCM do not support an NMS transport option).
- DAC 155oM, DAC 155eM, and AUX must only be installed in slots 1 to 6 **where NMS access is required**.
- 10 is for NPC only.
- NCC and FAN slots are dedicated. The INUe is now supplied standard with a single 2RU FAN, though still accepts two 1RU FANs.
- For protected operation RAC/RAC or RAC/DAC155oM pairings must be in slots 1 and 4, and/or 2 and 5, and/or 3 and 6.
- For protected DAC or NCM operation the partners can be installed in slots 1 to 9, except for the DAC 155oM/eM where NMS access is required, in which case only use slots 1 to 6.

Figure 2 - Module Hardware Variant Locations for INUe

- Any of the Slots 1 through 10 may be covered with a blank panel. They shall not be left unpopulated and shall have tamper seals applied per Section 7.2 below.

NCC: Node control card
FAN: Fan card (cooling)
RAC: Radio access card (supports the ODU/IRU)
DAC: Digital access card (user interfaces)
AUX: Auxiliary card (auxiliary data and alarm I/O)
NPC: Node protection card (NCC protection)
NCM: Node Convergence Module

Interface traffic options include:

- Ethernet, E1/DS1, E3/DS3, STM1/OC3
- Auxiliary data and alarm I/O

The minimum module configuration requires baseline components, INUe 2RU Chassis, an NCC card, at least one suitable security relevant RAC card, a fan card and the FIPS installation kit to be installed in order to support the Payload Encryption and Payload Decryption services.

Required Baseline Components Cards:

Item *	Part number and revision	Firmware/FPGA Version Information Baseline configuration	Quantity in module	Cryptographic Functionality
INUe 2RU Chassis	EXE-002	N/A	1	No
Node Controller Card	EXN-006-001	FPGA_NCCv4_PDH-1.10.4.bit FPGA_NCCv4_SDH-2.8.3.bit	1	Yes
Fan Card	EXF-103	N/A	1	No
FIPS Installation Kit	Either: 179-530153-001 (customer fitted) or: 179-530153-002 (partially factory fitted)	N/A	1	No
Replacement Seals	007-600331-001	N/A	1	No
RAC 70 V2	EXR-700-002	FPGA_RAC7X_PDH_ACM-2.37.13.bit FPGA_RAC7X_SDH_ACM-3.12.15.bit	0-6	Yes
RAC 7X V2	EXR-770-002	FPGA_RAC7X_PDH_ACM-2.37.13.bit FPGA_RAC7X_SDH_ACM-3.12.15.bit	0-6	Yes
Aux	EXA-001	FPGA_AUX_132.bit	0-1	No
DAC 155o v2	EXD-150-001	FPGA_DAC_155o_v2-0.6.12.bit	0-6	No
DAC 155oM v3	EXD-155-001	FPGA_DAC_155_MUXV3-0.6.1.bit	0-6	No
DAC GE3	EXD-181-002	FGPA_DACGEV3-9.0.30.bit	0-3	No
NCM	EXD-400-002	FPGA_NCM-1.1.112.bit FPGA_NCM_CES-1.1.417.bit FPGA_NCM_CES1-1.1.474.bit	0-6	No

Item *	Part number and revision	Firmware/FPGA Version Information Baseline configuration	Quantity in module	Cryptographic Functionality
		FPGA_NCM_HSF-1.0.133.bit FPGA_NCM_HSF_FIX-1.1.152.bit		
DAC 3XE3/DS3M, MUXED TO E1/DS1	EXD-331-001	FPGA_DAC_DS3_MUX-10.0.20.bit FPGA_DAC_E3_MUX_132.bit	0-6	No

Table 1 - Required Baseline Components Cards

If a suitable card is not installed, then the Payload Encryption and Payload Decryption services are not available. All other cards that can be installed in the 2RU chassis are interchangeable. No slot shall be left unpopulated.

Optional hardware components:

Item*	Part number and revision	Firmware/FPGA Version Information	Quantity in module	Cryptographic Functionality
Fan filter kit, 2RU	131-501768-001	N/A	0-1	No
Aux	EXA-001	FPGA_AUX_132.bit	0-5	No
DAC 155o v2	EXD-150-001	FPGA_DAC_155o_v2-0.6.12.bit	0-5	No
DAC 155oM v3	EXD-155-001	FPGA_DAC_155_MUXV3-0.6.1.bit	0-5	No
DAC 16xV2	EXD-161-001	FPGA_DAC16V2_E1_DS1-4.1.8.bit	0-5	No
DAC 16xV3	EXD-161-002	FPGA_DAC16V2_E1_DS1-4.1.8.bit	0-5	No
DAC GE3	EXD-181-002	FGPA_DACGEV3-9.0.30.bit	0-5	No
NCM	EXD-400-002	FPGA_NCM-1.1.112.bit FPGA_NCM_CES-1.1.417.bit FPGA_NCM_CES1-1.1.474.bit FPGA_NCM_HSF-1.0.133.bit FPGA_NCM_HSF_FIX-1.1.152.bit	0-5	No
NPC, high output	EXS-002	N/A	0-1	No
Blank panel	EXX-001	N/A	0-10	No

Table 2 - Optional Hardware Components

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 1. The Module is a multi-chip standalone embodiment. The cryptographic boundary is the hardware chassis. The module is a hardware module with firmware running on the NCC card within the chassis.

The processor of this platform executes all firmware. All firmware components of the module are persistently stored within the device and, while executing, are stored in the device local RAM.

Optionally, an ASIC on the RAC card provides the necessary functionality to support the Payload Encryption and Payload Decryption services.

The module has a Hardware module, so the cryptographic boundary is the same as the physical perimeter of the INUe.

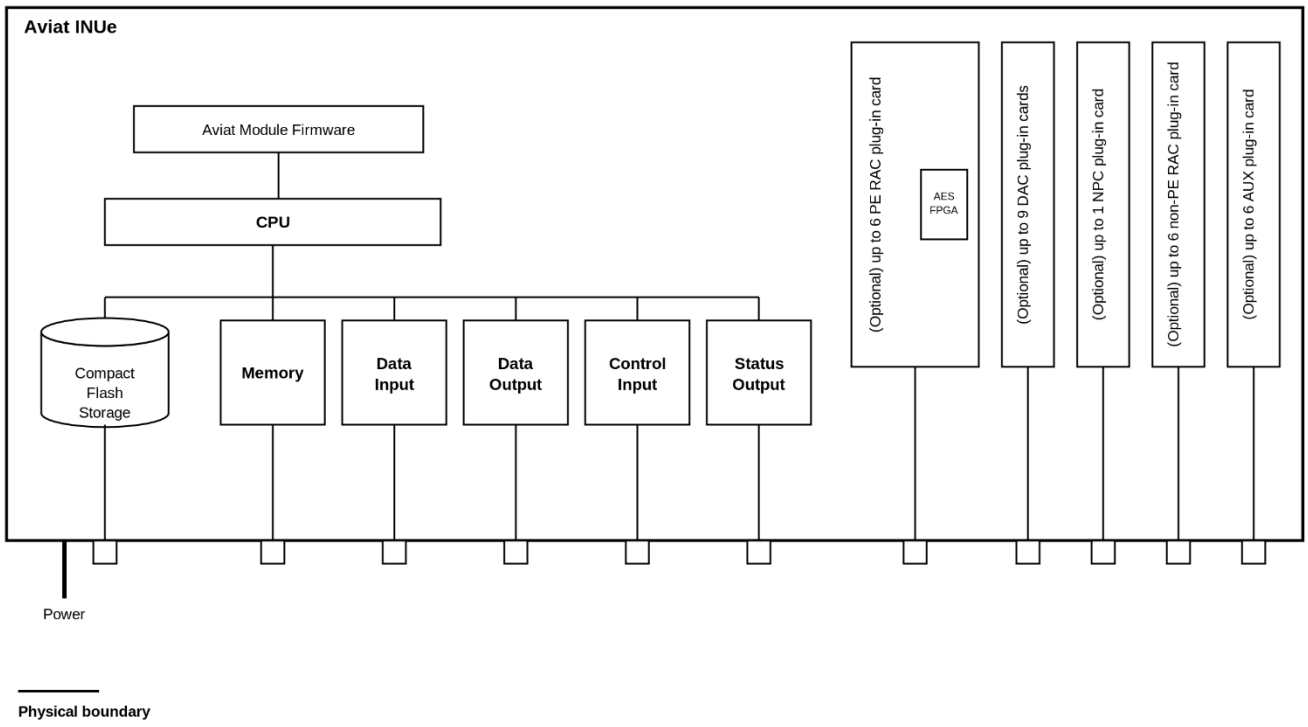


Figure 3 - Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Aviat Networks Eclipse Cryptographic Module cryptographic module, displayed as NCC-INUv4 under view status, is tested on the following operational environment.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
INUe 2RU Chassis (P/N EXE-002), Node Controller Card (P/N EXN-006-001 with FPGA_NCCv4_PDH-1.10.4.bit and FPGA_NCCv4_SDH-2.8.3.bit), Fan Card (P/N EXF-103), FIPS Installation Kit (P/N 179-530153-001 or 179-530153-002), Replacement Seals (P/N 007-600331-001), RAC 70 V2 (P/N EXR-700-002 with FPGA_RAC7X_PDH_ACM-2.37.13.bit and FPGA_RAC7X_SDH_ACM-3.12.15.bit), RAC 7X V2 (P/N EXR-770-002 with FPGA_RAC7X_PDH_ACM-2.37.13.bit and FPGA_RAC7X_SDH_ACM-3.12.15.bit), Aux (P/N EXA-001 with FPGA_AUX_132.bit), DAC 155o v2 (P/A EXD-150-001 with FPGA_DAC_155o_v2-0.6.12.bit), DAC 155oM v3 (P/N EXD-155-001 with FPGA_DAC_155_MUXV3-0.6.1.bit), DAC GE3 (P/N EXD-181-002 with FGPA_DACGEV3-9.0.30.bit), NCM (P/N EXD-400-002 with FPGA_NCM-1.1.112.bit, FPGA_NCM_CES-1.1.417.bit, FPGA_NCM_CES1-1.1.474.bit, FPGA_NCM_HSF-1.0.133.bit, FPGA_NCM_HSF_FIX-1.1.152.bit), DAC 3XE3/DS3M, MUXED TO E1/DS1 (P/N EXD-331-001 with FPGA_DAC_DS3_MUX-10.0.20.bit and FPGA_DAC_E3_MUX_132.bit), Fan filter kit, 2RU (P/N 131-501768-001), Aux (P/N EXA-001 with FPGA_AUX_132.bit), DAC 155o v2 (P/N EXD-150-001 with FPGA_DAC_155o_v2-0.6.12.bit), DAC 155oM v3 (P/N EXD-155-001 with FPGA_DAC_155_MUXV3-0.6.1.bit), DAC 16xV2 (P/N EXD-161-001 with FPGA_DAC16V2_E1_DS1-4.1.8.bit), DAC 16xV3 (P/N EXD-161-002 with FPGA_DAC16V2_E1_DS1-4.1.8.bit), DAC GE3 (P/N EXD-181-002 with FGPA_DACGEV3-9.0.30.bit), NCM (P/N EXD-400-002 with FPGA_NCM-1.1.112.bit FPGA_NCM_CES-1.1.417.bit, FPGA_NCM_CES1-1.1.474.bit, FPGA_NCM_HSF-1.0.133.bit, FPGA_NCM_HSF_FIX-1.1.152.bit), NPC, high	Please see under "Model/Part Number(s)".	10.01.03 with Bootloader version 1.0.549	NXP LS1026A (Arm Cortex A72)	N/A

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
output (P/N EXS-002), Blank panel (P/N EXX-001)				

Table 2: Tested Module Identification – Hardware

Table 3 - Tested Module Identification – Hardware

2.3 Excluded Components

No components are excluded from the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved Mode	Approved mode of operation	Approved	NCC solid green status LED. Once configured, the module only has a single mode of operation

Table 4: Modes List and Description

The module does not have a degraded mode of operation.

Mode Change Instructions and Status:

The module is originally non-compliant and must be configured to operate in an approved mode of operation. The module only operates in an approved mode of operation once it is set into the "Approved Mode" as follows:

1. Power up NCC.
2. The end user needs to securely download the Eclipse Portal firmware (also referred to as "Portal" and "Craft Tool" within this SP) from the module and install it on the PC used for the configuration of the module. The Eclipse Portal Installer, version 08.19.00, can be obtained at https://arc.aviatnetworks.com/s/qfjsmfm9wqb256hghbhqfhk.
3. Connect to NCC with Portal.
4. Install S/W license containing Strong Security, FIPS compliance, and optional Payload Encryption. The part numbers for this module's licenses are EZF-04-EC.
5. Set security mode to "FIPS".
6. The CO is prompted to enter the default credentials and click OK to confirm.
7. Hit the "Send" button to accept the configuration changes.
8. NCC reboots.
9. Connect to NCC using Portal.
10. Log in to NCC using default Crypto-Officer credentials documented in the user manual and when prompted update the default login credentials. Upon initial login, the crypto officer's password must be changed before access is granted.
11. Configure desired security settings and add local users and/or RADIUS servers as required.
12. By default, the FIPS non-compliant entropy mode alarm is raised against NCC.

13. Login as a user with Crypto-Officer permissions and enter a hex string containing between 196 and 980 bytes, the entropy input string, to be used as entropy, then press “Send”.
14. The module will zeroize internal keys and reboot. Once restarted the module will be using the supplied entropy source.
15. By default, Payload Encryption is disabled, Bypass warning alarm raised against RAC.
16. Log in as a user with Crypto-Officer permissions.
17. Perform RAC configuration to establish radio links and enable Payload Encryption.

For more details, please see the Eclipse User Manual Addendum for FIPS 140-3.

Once the module has been commissioned, the front panel of the module should be sealed, with no visible gaps and tamper evident seals applied as shown in Figure 6. The tamper-evident seals shall be installed for the module to operate in the approved mode of operation.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A6135	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-CCM	A6136	Key Length - 256	SP 800-38C
AES-CCM	A6537	Key Length - 256	SP 800-38C
AES-CFB128	A6135	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
AES-ECB	C5	Direction - Encrypt Key Length - 128, 192, 256	SP 800-38A
AES-GCM	A6135	Direction - Decrypt, Encrypt IV Generation - External IV Generation Mode - Key Length - 256	SP 800-38D
ECDSA KeyGen (FIPS186-5)	A6135	Curve - P-256, P-384 Secret Generation Mode - extra bits	FIPS 186-5
ECDSA KeyVer (FIPS186-5)	A6135	Curve - P-256, P-384	FIPS 186-5
ECDSA SigGen (FIPS186-5)	A6135	Curve - P-256, P-384 Hash Algorithm - SHA2-384 Component - No	FIPS 186-5
ECDSA SigVer (FIPS186-5)	A6135	Curve - P-256, P-384 Hash Algorithm - SHA2-384	FIPS 186-5
Hash DRBG	A6135	Prediction Resistance - Yes Mode - SHA2-256	SP 800-90A Rev. 1
HMAC-SHA-1	A6135	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-256	A6135	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-384	A6135	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
HMAC-SHA2-512	A6135	Key Length - Key Length: 112-524288 Increment 8	FIPS 198-1
KAS-ECC-SSC Sp800-56Ar3	A6135	Domain Parameter Generation Methods - P-256, P-384 Scheme - ephemeralUnified - KAS Role - initiator, responder	SP 800-56A Rev. 3
RSA SigVer (FIPS186-5)	A6135	Modulo - 2048, 4096 Signature Type - pkcs1v1.5	FIPS 186-5
SHA-1	A6135	Message Length - Message Length: 160, 0-65536 Increment 2048	FIPS 180-4
SHA2-256	A6135	Message Length - Message Length: 256, 0-65536 Increment 2048	FIPS 180-4
SHA2-384	A6135	Message Length - Message Length: 384, 0-65536 Increment 2048	FIPS 180-4
SHA2-512	A6135	Message Length - Message Length: 512, 0-65536 Increment 2048	FIPS 180-4
TLS v1.2 KDF RFC7627 (CVL)	A6135	Hash Algorithm - SHA2-384	SP 800-135 Rev. 1
TLS v1.3 KDF (CVL)	A6135	HMAC Algorithm - SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 5: Approved Algorithms

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

Vendor-Affirmed Algorithms:

The Module implements the Vendor Affirmed cryptographic algorithms listed in .

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

Table 6: Vendor-Affirmed Algorithms

The module uses a [133r2] compliant cryptographic key generation method for generating both asymmetric and symmetric keys.

Non-Approved, Allowed Algorithms:

N/A for this module.

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

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

The module does not implement any Non-Approved, but Allowed Algorithms with No Security Claimed in the approved mode of operation.

Non-Approved, Not Allowed Algorithms:

N/A for this module.

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

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
AsymKeyPair-KeyGen (SFI #3)	AsymKeyPair-KeyGen	Asymmetric Key Pair Generation (and verification)	IG C.E:	Hash DRBG: (A6135) ECDSA KeyGen (FIPS186-5): (A6135) SHA2-256: (A6135) SHA2-384: (A6135) CKG - Asym: ()
AsymKeyPair-KeyVer (SFI #17)	AsymKeyPair-KeyVer	Asymmetric Key Pair Verification	IG C.E:	Hash DRBG: (A6135) ECDSA KeyVer (FIPS186-5): (A6135) SHA2-256: (A6135) SHA2-384: (A6135)
BC-AUTH (SFI #8)	BC-Auth	Symmetric Encryption	Authenticated Block Cipher:	AES-GCM: (A6135) AES-CBC: (A6135)
BC-AUTH-DEC (SFI #16)	BC-Auth	Symmetric Decryption	Authenticated Block Cipher:	AES-GCM: (A6135) AES-CBC: (A6135)
BC-AUTH-DEC-CCM1 (SFI #21)	BC-Auth	Symmetric Decryption (FPGA1)	Authenticated Block Cipher:	AES-CCM: (A6136) AES-ECB: (C5)

Name	Type	Description	Properties	Algorithms
BC-AUTH-DEC-CCM2 (SFI #23)	BC-Auth	Symmetric Decryption (FPGA2)	Authenticated Block Cipher:	AES-CCM: (A6537) AES-ECB: (C5)
BC-AUTH-ENC-CCM1 (SFI #20)	BC-Auth	Symmetric Encryption (FPGA1)	Authenticated Block Cipher:	AES-CCM: (A6136) AES-ECB: (C5)
BC-AUTH-ENC-CCM2 (SFI #22)	BC-Auth	Symmetric Encryption (FPGA2)	Authenticated Block Cipher:	AES-CCM: (A6537) AES-ECB: (C5)
BC-UNAUTH (SFI #7)	BC-UnAuth	Symmetric Encryption	Unauthenticated Block Cipher:	AES-CBC: (A6135) AES-CFB128: (A6135)
BC-UNAUTH-DEC (SFI #15)	BC-UnAuth	Symmetric Decryption	Unauthenticated Block Cipher :	AES-CBC: (A6135) AES-CFB128: (A6135)
CKG (SFI #2)	CKG	Symmetric Key Generation	IG D.L: IG D.R:	Hash DRBG: (A6135) CKG - Sym: ()
DigSig-SigGen (SFI #5)	DigSig-SigGen	Digital Signature Generation		ECDSA SigGen (FIPS186-5): (A6135) SHA2-256: (A6135) SHA2-384: (A6135) Hash DRBG: (A6135)
DigSig-SigVer (SFI #6)	DigSig-SigVer	Digital Signature Verification		ECDSA SigVer (FIPS186-5): (A6135) SHA2-256: (A6135) SHA2-384: (A6135) Hash DRBG: (A6135)
DRBG (SFI #14)	DRBG	Deterministic Random Bit Generator	Security Strength = 256:	Hash DRBG: (A6135) HMAC-SHA2-256: (A6135) SHA2-256: (A6135)
Integrity (SFI #11)	DigSig-SigVer	Digital Signature Verification		RSA SigVer (FIPS186-5): (A6135)

Name	Type	Description	Properties	Algorithms
				SHA2-512: (A6135)
KAS-ECC-SSC (SFI #13)	KAS-SSC	Shared Secret Calculation	Shared Secret Calculation [56Ar3]:	KAS-ECC-SSC Sp800-56Ar3: (A6135)
KAS-TLS1.2KDF (SFI #4)	KAS-135KDF	Key Derivation	TLS 1.2 Key Derivation:	TLS v1.2 KDF RFC7627: (A6135)
KAS-TLS13KDF (SFI #12)	KAS-135KDF	Key Derivation	TLS 1.3 Key Derivation:	TLS v1.3 KDF: (A6135) HMAC-SHA2-384: (A6135) SHA2-384: (A6135)
KAS1 (SFI #18)	KAS-Full	SSP Agreement with TLS 1.2	SSP Agreement : IG D.F:	KAS-ECC-SSC Sp800-56Ar3: (A6135) TLS v1.2 KDF RFC7627: (A6135) SHA2-384: (A6135)
KAS2 (SFI #19)	KAS-Full	SSP Agreement with TLS 1.3	SSP Agreement: IG D.F:	KAS-ECC-SSC Sp800-56Ar3: (A6135) TLS v1.3 KDF: (A6135) HMAC-SHA2-384: (A6135) SHA2-384: (A6135)
MAC (SFI #9)	MAC	Message Authentication	IG C.B:	HMAC-SHA-1: (A6135) HMAC-SHA2-256: (A6135) HMAC-SHA2-384: (A6135) HMAC-SHA2-512: (A6135) SHA-1: (A6135) SHA2-256: (A6135) SHA2-384: (A6135) SHA2-512: (A6135)
SAML (SFI #10)	DigSig-SigVer	Digital Signature Verification		RSA SigVer (FIPS186-5):

Name	Type	Description	Properties	Algorithms
				(A6135) SHA2-256: (A6135)
SHA (SFI #1)	SHA	Secure Hash Standard	IG C.B:	SHA-1: (A6135) SHA2-256: (A6135) SHA2-384: (A6135) SHA2-512: (A6135)

Table 7: Security Function Implementations

2.7 Algorithm Specific Information

AES GCM IV Uniqueness

FIPS140-3 IG C.H, Option 1

The AES GCM implementation generates GCM IVs deterministically as specified in [38D] Section 8.2.1 using the following protocols:

TLS 1.2

The Module is compliant with TLS v1.2 and [52r2], Section 3.3.1. The Module supports TLS 1.2 GCM Cipher Suites for TLS, as described in RFCs 5116, 5246, 5288 and 5289 and shall only be used for the TLS protocol version 1.2 to be compliant with FIPS140-3 IG C.H, scenario 1.

The module uses the extended master secret in the TLS 1.2 KDF. The module uses the RFC 7627 version of the TLS 1.2 KDF.

The generated IV is only used in the context of the AES-GCM encryption executing the provisions of the protocol within which the IV was generated. The IV is generated wholly within the module boundary.

The counter portion of the IV is set by the Module within its cryptographic boundary.

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

In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.

No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

The module uses DTLS 1.2 to tunnel to a remote module. It uses the following cipher suite for this: ECDHE-ECDSA-AES256-GCM-SHA384

TLS 1.3

The module is compliant with TLS v1.3 and [52r2], section 3.3.1, RFC 8446, TLS version 1.3 cipher suites and FIPS 140-3 IG C.H scenario 5.

The generated IV is only used in the context of the AES-GCM encryption executing the provisions of the protocol within which the IV was generated. The IV is generated wholly within the module boundary.

The counter portion of the IV is set by the Module within its cryptographic boundary.

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

In case the module's power is lost and then restored, a new key for use with the AES GCM encryption/decryption shall be established.
No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

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

SNMPv3

The module does not contain an SNMP KDF. SNMP keys are derived externally to the module, and so no claims are made regarding SNMP v3 management traffic.

2.8 RBG and Entropy

The module does not contain a validated entropy source.

The entropy for seeding the SP 800-90Ar1 DRBG is determined by the user of the module, which is outside of the module's cryptographic boundary. To be compliant, the target application shall supply at least 256 bits of entropy in order to meet the security strength required for the random number generation mechanism. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated SSPs (e.g., keys).

2.9 Key Generation

The module implements the following Key Generation Functions.

SFI #2, SFI #3

2.10 Key Establishment

Key Agreement Information

The module implements the following Key Agreement Functions.

SFI #4, SFI #12

Key Transport Information

The module implements the following Key Transport Functions.

SFI #4, SFI #12

2.11 Industry Protocols

Protocol *	Key Exchange	Server/ Host Auth	Cipher	Integrity
TLS (IG D.F and [52r2])	TLS_AES_256_GCM_SHA384 TLS v1.3			
	Ephemeral ECDH		AES-GCM-256	
TLS (IG D.F and [135r1])	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 TLS v1.2			
	Ephemeral ECDH		AES-GCM-256	
TLS (IG D.F and [135r1])	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 TLS v1.2			
	Ephemeral ECDH		AES-CBC-256	

Table 3 - Industry Protocols

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Physical Port	Logical Interface(s)	Data That Passes
NCC RJ-45 connector	Data Input Data Output Control Input	Data Input: The NCC component has six NMS connectors, providing Ethernet access for Portal or ProVision (http://www.aviatnetworks.com/products/network-managementoss/provision/). Pin assignments represent industry-standard LAN cable assembly for a 10/100Base-T, RJ-45 connector; Data Output: As per Data Input; Control Input: Service requests
NCC V.24 connector	Data Input Data Output Control Input	Data Input: A V.24 connector and a USB port providing serial data access for Portal; Data Output: As per Data Input; Control Input: Service requests

Physical Port	Logical Interface(s)	Data That Passes
NCC USB connector	Data Input Data Output Control Input	Data Input: A USB port providing serial data access for Portal; Data Output: As per Data Input; Control Input: Service requests
RAC RJ-45 connector	Data Input Data Output Control Input	Data Input: Data enter and leave RAC adapters via a single RJ-45 Ethernet socket and connects to a DAC GE3 RJ-45 socket; Data Output: As per Data Input; Control Input: Not Applicable
RAC I/F connector	Data Input Data Output Control Input	Data Input: Data enter and leave RAC adapters via a single I/F socket which connect the RAC to a radio transceiver so that the data can be sent and received on a microwave link; Data Output: As per Data Input; Control Input: Not Applicable
DAC GE3 RJ-45 connector	Data Input Data Output Control Input	Data Input: Data enters and leaves DAC GE3 adapters via six RJ-45 Ethernet sockets; Data Output: As per Data Input; Control Input: Not Applicable
DAC 16x TDM connector	Data Input Data Output Control Input	Data Input: Data enters and leaves DAC 16xV2 or DAC 16xV3 adapters via two TDM connectors each allowing up to 8 discrete TDM channels; Data Output: As per Data Input; Control Input: Not Applicable
NCM TDM connector	Data Input Data Output Control Input	Data Input: Data enters and leaves NCM adapters via two TDM connectors each allowing up to 16 discrete TDM channels; Data Output: As per Data Input; Control Input: Not Applicable
DAC 3xE3/DS3M BNC connector	Data Input Data Output Control Input	Data Input: Data enters and leaves DAC 3xE3/DS3M adapters via three pairs of TDM connectors. Each pair contains an input and output interface; Data Output: As per Data Input; Control Input: Not Applicable
DAC 155oV2 optical transceiver	Data Input Data Output Control Input	Data Input: Data enters and leaves DAC 155oV2 adapters via two optical transceivers. Each transceiver contains an input and output interface; Data Output: As per Data Input; Control Input: Not Applicable
DAC 155oMV3 optical transceiver	Data Input Data Output Control Input	Data Input: Data enters and leaves DAC 155oMV3 adapters via two optical transceivers. Each transceiver contains an input and output interface; Data Output: As per Data Input; Control Input: Not Applicable

Physical Port	Logical Interface(s)	Data That Passes
LEDs	Status Output	Service status (see "LED status indicators" table)
NCC power interface and optional NPC	Power	Power input limits are -40.5 to -60 V DC. The power connector is a D-Sub M/F 2W2. The positive DC return pin is connected to chassis ground.

Table 8: Ports and Interfaces

See Figure 5 for an image of the physical ports.

Note: The module does not support Control Output.

LED status indicators:

EVENT *	NCC STATUS LED	NCC TEST LED	RAC STATUS LED
Pre-operational self-tests in progress	Solid green	Flashing orange	Solid red
Zeroization	Solid green	Flashing orange	Solid red
Self-tests pass/Approved mode enabled	Solid green	Solid green	Solid green
Pre-operational self-test failure	Solid red	Off	Solid red

Table 9. LED Status Indicators

When the three indicated LEDs are green, the module is in the Approved mode of operation.
The use of the Approved mode locks out the use of non-Approved algorithms.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Locally defined passwords	Roles are authenticated locally to the module with a username and password	The passwords for the User and Crypto Officer roles, authenticating via the Portal GUI, are either strict: alphanumeric strings of between 15 and 32 alphanumeric characters comprised of at least one uppercase and one lowercase letter, one special character and one number or standard: 8-32 characters in length with	Strict: 1 in 3.95x10^29 Standard: 1 in 6.1x10^15	Assuming 10 attempts per minute, strict: 1 in 3.95x10^28 and standard: 1 in 6.1x10^14

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
		at least 1 number and 1 letter. Identity based authentication. Strict passwords: 32 special characters 26 upper case 26 lower case 10 numbers Each position has 94 possible options. 15 characters give 94^15 (3.95 x 10^29) passwords. Standard passwords: 32 special characters 26 upper case 26 lower case 10 numbers Each position has 94 possible options. 8 characters gives 94^8 (6.1 x 10^15) passwords		
RADIUS	Username and password are authenticated remotely by a RADIUS server and a centrally held database of users and credentials. If the user identity and password match stored values, then authentication is successful.	TLS tunneled RADIUS authentication (role-based for the purposes of FIPS 140-3). RADIUS is also secured by a shared secret. User authentication relies on a password. Overall strength of the security mechanism is provided by RADIUS password. RADIUS passwords are a minimum of 16 characters. Each character has 94 possible options (see locally defined passwords). 16 characters give 94^16 (3.72 x 10^31) passwords.	RADIUS password: 1 in 3.72 x 10^31	The module only allows three consecutive failures in a single one-minute period. 1 in 1.24 x 10^31
SAML	ADFS server may be used for operator authentication, in which case no usernames and passwords are sent from Eclipse. The user is simply redirected to the server URL in a browser to enter their details. Upon	SAML 2.0 - RSA signature verification. Role-based for the purposes of FIPS 140-3. RSA provides at least 112 bits of security strength (SFI #10).	1 in 2^112 (5.19 x 10^33	The module only allows three consecutive failures in a single one-minute period. 1 in 1.73 x 10^33

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	successful authentication, a SAML 2.0 token is sent to Eclipse which contains a username and credentials along with time range the token is good for. No password is contained within the token.			

Table 10: Authentication Methods

The Module's authentication methods are listed above.

4.2 Roles

The Module supports three distinct operator roles, User, maintenance and Crypto Officer (CO). The cryptographic module enforces the separation of roles using operator authentication for user and CO roles. The maintenance role supports the capability for users to add or remove plug-in cards to the module to provide extra bandwidth or different data formats. It also allows for the insertion and removal of an optional fan air filter. Crypto-Officer support is required to perform Maintenance services.

The table below lists all operator roles supported by the Module.

The Module supports concurrent operators. Up to five operators may be logged on to the module at any one time. It is possible for an operator in the User role and one in the Crypto-Officer role to be logged on concurrently. Previous authentications are cleared on power cycle. Operator authentication data entered manually is obscured using "*" characters to represent each authentication character.

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Role	CO	Locally defined passwords RADIUS SAML
User	Role	User	Locally defined passwords RADIUS SAML
Maintenance	Role	Maintenance	None

Table 11: Roles

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AUTH1	Craft tool authentication - local user access	Event log	Login credentials via craft tool GUI	Craft tool GUI feedback and event log entry indicating success/failure	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	User - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AUTH2	Craft tool authentication - RADIUS	Event log	Login credentials via craft tool GUI sent to RADIUS server and then RADIUS response	Craft tool GUI feedback and event log entry indicating success/failure	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	User - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
AUTH3	Craft tool authentication - ADFS authentication	Event log	SAML token from ADFS server containing user credentials	Craft tool GUI feedback and event log entry indicating success/failure	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SAML (SFI #10)	User - ADFS Server Certificate: W,E - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHA (SFI #1)	
AUTH4	SNMPv3	SNMPv3 request status code	Secure SNMPv3 session request	Secure SNMPv3 session response	BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) MAC (SFI #9)	User - SNMPv3 Authentication Key: R,E - SNMPv3 Privacy Key: R,E
Crypto library initialization	Pre-operational self-tests	LED	Power	Event log entry indicating success/failure	None	Crypto Officer - Hash DRBG C and V: Z - Hash DRBG Seed: Z - Payload Encryption DTLS HMAC Keys: Z - Payload Encryption DTLS Tunnel Keys: Z - Payload Encryption Key: Z - Payload Encryption Private Key: Z - SNMPv3 Authentication Key: Z - SNMPv3 Privacy Key: Z - TLS HMAC Keys: Z - TLS Private Key: Z - TLS Tunnel Keys: Z
ENT1	Entropy Configuration and	Event log	Configuration change	Craft tool GUI and/or	AsymKeyPair-KeyGen	Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	storage of external entropy		via craft tool GUI	Event log entry	(SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	- Entropy Input String: R - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E
ENT2	Entropy, Entropy pool management	Event log	Configuration change	Event log entry	AsymKeyPair-KeyGen (SFI #3)	Crypto Officer - TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			via craft tool GUI		AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E
Firmware	Logic for pre-operational firmware integrity tests	LED	Power or loading of new firmware	Event log entry indicating	Integrity (SFI #11) SHA (SFI #1)	Crypto Officer - Integrity key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
			via craft tool GUI	success/failure		
Firmware Upgrade	Updates the firmware on within the module and reboots the module to allow the new firmware to become operational. Upon failure the module rolls back to the previous firmware	LED	Update request on a selected image via the craft tool GUI	Event log entry indicating success/failure	Integrity (SFI #11) SHA (SFI #1)	Crypto Officer - Integrity key: R
LOG1	Secure logging Enable/disable secure event logs visible to non-crypto users	Event log	Configuration request via craft tool GUI	Craft tool GUI and/or Event log entry indicating status	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF	Crypto Officer - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	
LOG2	Secure logging Event logs over TLS to remote logging server	Event log	Configuration request via craft tool GUI	Craft tool GUI and/or Event log entry indicating status	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4)	Crypto Officer - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	
PAC1	Port access control: NMS Ethernet ports and forwarding enable/disable	Event log	Configuration request via craft tool GUI	Craft tool GUI and/or Event log entry	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-	Crypto Officer - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	
PAC2	Port access control: USB port	Event log	Configuration request via craft tool GUI	Craft tool GUI and/or Event log entry	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF	Crypto Officer - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	
PAC3	Port access control: V.24 Maintenance port	Event log	Configuration request via craft tool GUI	Craft tool GUI and/or Event log entry	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12)	Crypto Officer - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	
PE1	Payload encryption services: Power-on and bypass self-tests, conditional bypass tests	LED	Power and request to enable payload encryption	Event log entry	SHA (SFI #1)	Crypto Officer - Payload Encryption DTLS HMAC Keys: Z - Payload Encryption DTLS Tunnel Keys: Z - Payload Encryption Key: Z
PE2	Payload encryption services: Key handling: generation/exchange	Event log	Power and request to enable payload encryption and timed or manual request to regenerate key	Event log entry	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-AUTH-DEC-CCM1 (SFI #21) BC-AUTH-DEC-CCM2 (SFI #23) BC-AUTH-ENC-CCM1 (SFI #20) BC-AUTH-ENC-CCM2 (SFI #22) CKG (SFI #2)	Crypto Officer - Payload Encryption Certificate: G,R,W,E,Z - Payload Encryption Key: G,W,Z - Payload Encryption Private Key: G,R,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS1 (SFI #18) MAC (SFI #9) SHA (SFI #1)	
PE3	Payload encryption services: Control functions: bypass enable	Event log	Request to enable or disable payload encryption	Event log entry	None	Crypto Officer
PE4	Payload encryption services: Monitoring functions: fault and alarm monitoring	Event log	None	Event log entry	None	Crypto Officer
TLS1	Portal access, web server access	Event log	Craft tool access over Network interface	Event log indicating successful connection	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-	User - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	
TLS2	DTLS for PE key exchange	Event log	Request to enable payload encryption and timed or manual request to regenerate PE key	Event log entry indicating attempt to change PE keys	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-AUTH-DEC-CCM1 (SFI #21) BC-AUTH-DEC-CCM2 (SFI #23)	Crypto Officer - Payload Encryption DTLS HMAC Keys: G,R,W,E - Payload Encryption DTLS Tunnel Keys: G,R,W,E - Payload Encryption Key: G,R,W,E - Payload

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					BC-AUTH-ENC-CCM1 (SFI #20) BC-AUTH-ENC-CCM2 (SFI #22) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS1 (SFI #18) MAC (SFI #9) SHA (SFI #1)	Encryption Private Key: E
TLS3	Self-signed TLS certificate generation and storage	Event log	Power - certificate generated during power on sequence	None	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) DigSig-SigGen (SFI #5) SHA (SFI #1)	Crypto Officer - TLS Certificate: G,W,E - TLS Private Key: G,W,E
TLS4	Customer TLS certificate uploads and storage	Event log	Entry of keys via craft tool GUI	Craft tool GUI	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH	Crypto Officer - TLS Certificate: G,W,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					(SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	
TLS5	TLS 1.2 cipher suite configuration	Event log	Configuration request via craft tool GUI	Craft tool GUI and/or Event log entry	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8)	Crypto Officer - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	Key: E - TLS Tunnel Keys: G,W,E - P-256 TLS 1.2 Pre-Master Secret: G,E,Z - P-384 TLS 1.2 Pre-Master Secret: G,E,Z
TLS6	TLS 1.3 cipher suite configuration	Event log	Configuration request via craft tool GUI	Craft tool GUI and/or Event log entry	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-	Crypto Officer - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E - P-256 TLS

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	1.3 Handshake Secret: G,E,Z - P-384 TLS 1.3 Handshake Secret: G,E,Z
User Management	a. Localauthentication: user storage, add/remove, password changes, credentials b. RADIUSauthentication: RADIUS client and server configuration c. SAMLauthentication: configuration, SAML token	Event log	Configuration changes via craft tool GUI	Craft tool GUI and/or Event log entry indicating configuration change success/failure	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH	Crypto Officer - Crypto-Officer Password: R,W - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	parsing and optional token decryption d. SNMPv3service: user storage, add/remove, passkey changes, credentials e. User session management (logins, logouts, timeouts) f. Access control lists for Portal and SNMP g. Login warning banners, login information h. Mechanised attack prevention i. Forced user lockouts j. SNMPv3 configuration				(SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	- TLS Tunnel Keys: G,W,E - User Password: R,W
View configuration	Request via craft tool GUI	Event log	View request via craft tool GUI	Craft tool GUI display	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7)	User - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E - P-256 TLS 1.2 Pre-Master Secret: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					BC-UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	- P-384 TLS 1.2 Pre-Master Secret: E - P-256 TLS 1.3 Handshake Secret: E - P-384 TLS 1.3 Handshake Secret: E
View Firmware Version (Show Version)	Provides firmware version information for the NCC, DAC GE3 plug-ins, and attached ODU's/IRU's	Craft tool GUI	Version information request on a selected image via the craft tool GUI	Version information displayed via the craft tool GUI	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					UNAUTH-DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	
View Hardware Version (Show Version)	Provides hardware version information for the chassis, and all plug-in modules individually	Craft tool GUI	Version information request on a selected plug-in module image via the craft tool GUI	Version information displayed via the craft tool GUI	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					DEC (SFI #15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	
View status (Show Status)	View system status via Craft tool GUI	Event log	View status request via craft tool GUI	Craft tool GUI output and event log entry	AsymKeyPair-KeyGen (SFI #3) AsymKeyPair-KeyVer (SFI #17) BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI	Crypto Officer - TLS Certificate: E - TLS HMAC Keys: G,W,E - TLS Private Key: E - TLS Tunnel Keys: G,W,E - P-256 TLS 1.2 Pre-Master Secret: E - P-384 TLS 1.2 Pre-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					#15) CKG (SFI #2) DigSig-SigGen (SFI #5) DigSig-SigVer (SFI #6) DRBG (SFI #14) KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9) SHA (SFI #1)	Master Secret: E - P-256 TLS 1.3 Handshake Secret: E - P-384 TLS 1.3 Handshake Secret: E
Zeroization	Destroys all security parameters (Zeroize)	LED	Configuration request via craft tool GUI	Event log entry	None	Crypto Officer - Hash DRBG C and V: Z - Hash DRBG Seed: E - Payload Encryption DTLS HMAC Keys: Z - Payload Encryption DTLS Tunnel Keys: Z - Payload Encryption Key: Z - Payload

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Encryption Private Key: Z - SNMPv3 Authentication Key: Z - SNMPv3 Privacy Key: Z - TLS HMAC Keys: Z - TLS Private Key: Z - TLS Tunnel Keys: Z - P-256 TLS 1.2 Pre-Master Secret: Z - P-384 TLS 1.2 Pre-Master Secret: Z - P-256 TLS 1.3 Handshake Secret: Z - P-384 TLS 1.3 Handshake Secret: Z

Table 12: Approved Services

4.4 Non-Approved Services

The module does not implement Non-Approved services while running in an approved mode.
N/A for this module.

4.5 External Software/Firmware Loaded

NOTE: The module does not support the loading of external software/firmware other than through the firmware upgrade service. Only the firmware versions identified on the module's validation

certificate are included in the scope of this validation. Any other firmware loaded onto the module is not validated and would require a separate FIPS 140-3 validation.

4.6 Bypass Actions and Status

When entering bypass (payload encryption disable), the following two independent actions are required:

1. Disable the bypass lock – independent configuration sent to the module.
2. Disable payload encryption - independent configuration sent to the module.

The second action cannot be initiated until the bypass lock has been disabled in step 1.

4.7 Additional Information

Maintenance

Maintenance consists of inserting, removing or replacing plug-in cards and the fan air filter. The Crypto-Officer must perform the zeroize service and then power down the module. The module must remain powered down during maintenance and then the Crypto-Officer must power up the module and perform the zeroize service to complete the maintenance.

Plug-in Cards

To remove a plug-in card or blank, remove its tamper-evident seals, loosen its front-panel fastening screws and pull it towards you. Inserting a card may require the removal of a blank to access the card slot. To insert a plug-in card, push it into the appropriate slot. Ensure its backplane connector is correctly engaged before applying sufficient pressure to bring the plug-in panel flush with the front panel. Secure the card using its fastening screws.

Fan Air Filter

For the INUe, a fan air filter kit is supplied, comprising a filter frame, filter element, and fastening screw. It is installed in the INUe to the right side of the FAN module, as illustrated below.

Remove the FAN module and slide the air filter into the chassis so that it locates to the right side of the FAN module backplane connector, and up against the chassis side. FAN module removal and replacement do not affect traffic.

Installation instructions are included with the fan filter kit.

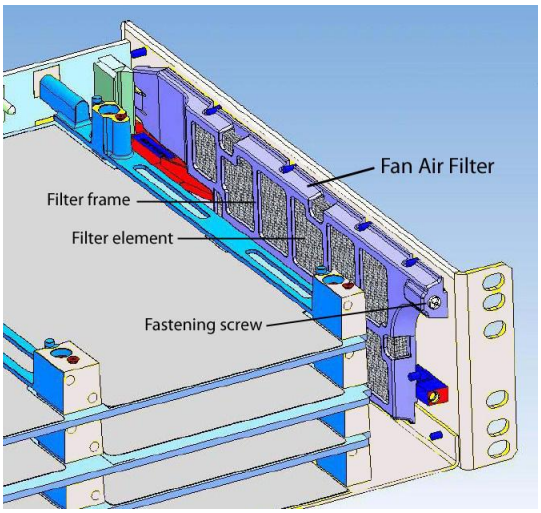


Figure 4 - Fan Air Filter Assembly

Renewing Physical Security Following a Maintenance Task
The physical security measures must be checked and renewed as appropriate following any module maintenance. When replacing a tamper-evident seal, any residue from a previous seal must be removed before a new seal is applied.

5 Software/Firmware Security

5.1 Integrity Techniques

The Module is composed of the following firmware component(s):

- Component 1: Node Controller Card firmware - binary

The firmware component is protected with the authentication technique of verifying the RSA-4096 signature of a SHA2-512 hash of the firmware image (CAVP Cert. #A6135). The same technique is used for the module integrity test and the software/firmware load test.

The Module does contain some open-source code and uses the GCC compiler to compile this.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by power cycling the Eclipse terminal.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited
Limited

The module has a limited operational environment under FIPS 140-3 definitions with Physical Security at Level 2. Therefore, per the FIPS 140-3 Management Manual Section 7.5 “Partial validations and non-applicable areas”, this section is not applicable.

7 Physical Security

The module is entirely encased by a thick steel chassis. The back of the chassis is completely closed off and internally has a backplane into which plug-in cards may be inserted. The front of the chassis, where plug-in cards are inserted, must be sealed in a commissioned module. The sides of the chassis have vent holes to allow air to flow across components within the module to provide cooling and prevent overheating.

7.1 Mechanisms and Actions Required

The module requires tamper evident seals and louvers to meet the FIPS 140-3 level 2 tamper evidence and opacity requirements. These are either factory fitted or operator fitted and the actions required for fitting are described below.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper-Evident Seals	6 months	Tamper-evident seals should be inspected for integrity (installed as per Figure 6, Figure 14 and Figure 15) at least once every six (6) months If tamper is suspected, remove the INUe from the network immediately and return the module to Aviat for examination

Table 13: Mechanisms and Actions Required

7.2 User Placed Tamper Seals

The louvers shown in Figure 6 and its tamper-evident seals are installed in the factory. The INUe is then installed in its equipment rack prior to shipment. If physical security kit 179-530153-002 is used, the tamper evident labels on the louvers must be checked for evidence of tampering when the equipment is received. The operator applies all of the front panel tamper-evident seals.

Number:
The module is supplied with a set of twenty-three (23) tamper-evident seals consisting of two (2) different types of seals. There are fifteen (15) white narrow seals that are used on the top front and on the front panel and must be fitted correctly to satisfy the physical security requirements for the module (see Figure 6 and Figure 10). In addition, there are eight (8) wider holographic seals used for the side louver panels (see Figure 14 and Figure 15). Once a module is commissioned, the seals must be applied by the operator to the NCC, plug-in cards and blanking plates, such that for each item that borders that chassis, there is a seal joining the item to the chassis. For each item that does not border the chassis, there is a seal linking it to its neighbor.

Placement:
See Figure 6, Figure 14 and Figure 15.

Surface Preparation:
Remove excessive grease, dirt, or oil from the cover if appropriate by using alcohol-based cleaning pads before applying the tamper evident seals. The chassis temperature should be above 10° C (50° F). All surfaces should be allowed to dry following cleaning.

Operator Responsible for Securing Unused Seals:
See below.

Part Numbers:
Physical security kits 179-530153-001 and 179-530153-002 are identical in content. However, for each installation only one kit is required. Kit 179-530153-001 is used where the operator installs the louvers and kit 179-530153-002 is used when the louvers are factory fitted.

All parts of Kit 179-530153-001 are installed by the operator.

Kit 179-530153-002 is partially factory fitted.

The INUe enclosure (below) has an NCC card and ten expansion slots, each of which must either contain a plug-in card or be covered by a blanking plate.

Figure 5 - INUe Enclosure

To install the tamper-evident seals on front panel (physical security kits 179-530153-001 and 179-530153-002):

- Verify that the front panel is contiguous
- For slots that do not contain plug-in cards, fit a blank panel (HW P/N EXX-001 per Figure 1)
- Remove excessive grease, dirt, or oil from the cover if appropriate by using alcohol-based cleaning pads before applying the tamper evident seals. The chassis temperature should be above 10° C (50° F).
- Affix (12) narrower tamper-evident seals as indicated in the figure below such that it is not possible to remove either a single card or a group of cards without also removing a seal and leaving tamper evidence.
- Install the INUe shelf into the rack and apply security seals over front of the cards in the chassis as shown. Use caution to avoid touching the adhesive with fingerprints to avoid damaging the seals. Allow the seal adhesive at least sixty (60) minutes to cure.
- At the conclusion of both installation and commissioning, the tamper evident labels must be inspected for integrity. If there is evidence of tampering, the equipment must be removed from service and returned to Aviat for examination.
- The tamper-evident seals should be replaced whenever components are added or removed from the module. Replacement seals can be ordered from Aviat Networks, part number 007-600331-001
- Tamper-evident seals should be inspected for integrity at least once every six (6) months
- If tamper is suspected, remove the INUe from the network immediately and return the module to Aviat for examination.

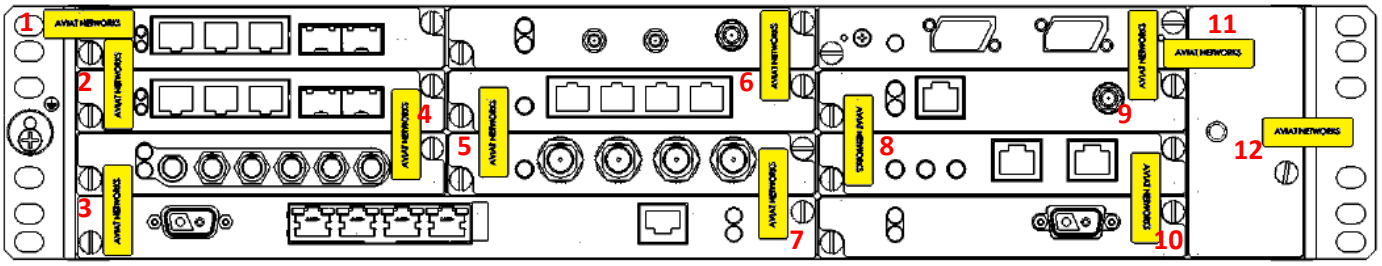


Figure 6 - Tamper-Evident Seal Locations (Front)

Opacity: The module enclosure has vent holes at the sides. The vent holes are covered by louver panels that provide no line-of-sight view of any internal components that are affixed with double sided PSA foam tape. Once secured, four (4) tamper-evident seals are fitted to each louver panel.

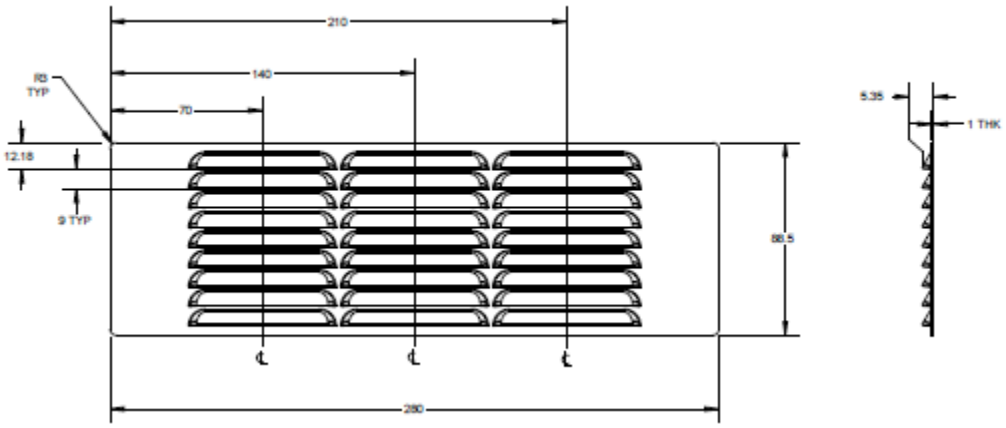


Figure 7 - Louver panel

The tamper-evident seals and louver panels/filters shall be installed for the module to operate in an Approved mode of operation.

The Crypto-Officer is responsible for the application and maintenance per the physical security policy:

To fit and affix the louver panels (physical security kit 179-530153-001):

All surfaces must be clean and dry prior to installation. Wipe the side of the INUe surfaces with isopropyl alcohol and let dry. Place the INUe shelf on flat surface and install the louver panels as shown below.

Left Hand Side (as viewed from the front)

- Locate the louver panel and remove the paper backing from the double-sided pressure sensitive adhesive (PSA) foam tape.

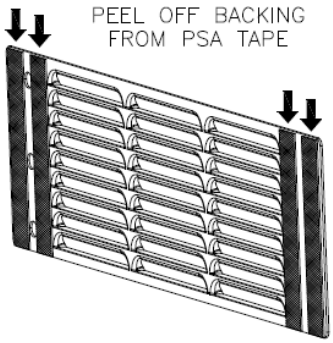


Figure 8 - Left Hand Louver Panel

- Align the front edge of the louver panel with the edge of the radius near the front mounting ear.
- Align the bottom edge of the louver panel with the bottom edge of the INUe shelf.

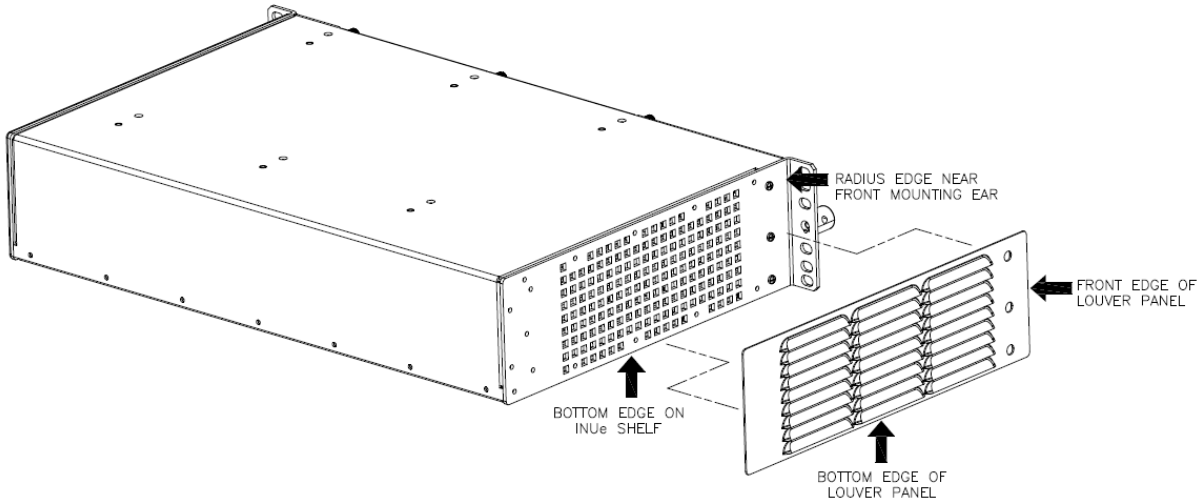


Figure 9 - Fitting the Left-Hand Louver Panel - 1

- Apply strong pressure to the side of the louver panel to bond the PSA to the INUe shelf.

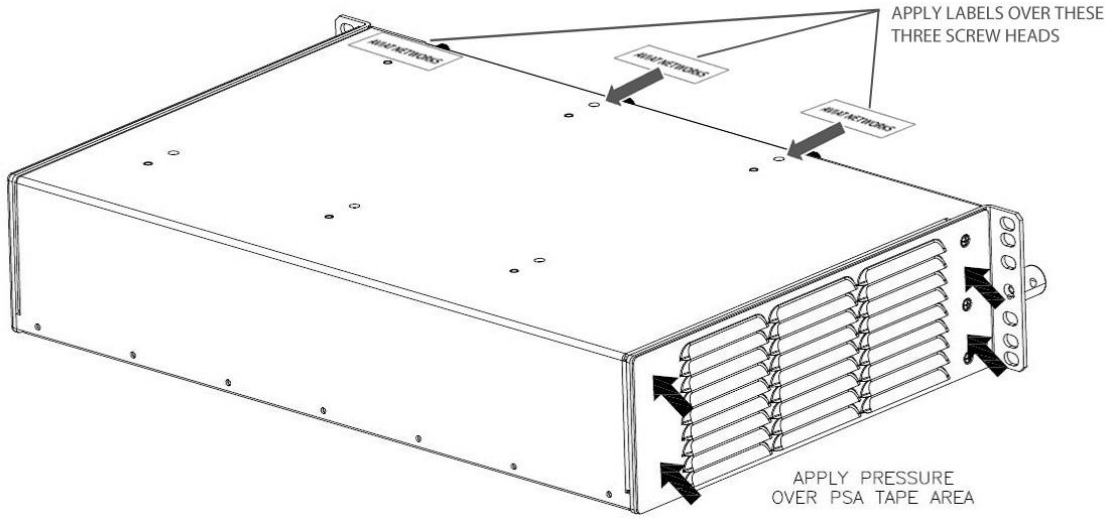


Figure 10 - Fitting the Left-Hand Louver Panel – 1 and Position of “Top” Tamper-Evident Seals

- Let the louver panel PSA cure for at least five (5) minutes before proceeding to install the right-hand side.

Right Hand Side (as viewed from the front)

- Locate the louver panel and remove the paper backing from the double-sided PSA foam tape.

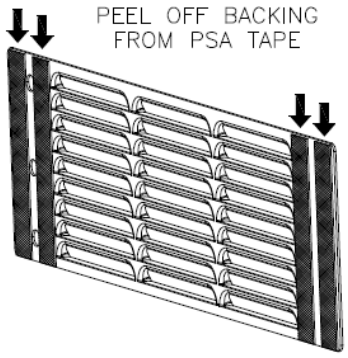


Figure 11 - Right-Hand Louver Panel

- Align the front edge of the louver panel with the edge of the radius near the front mounting ear.
- Align the bottom edge of the louver panel with the bottom edge of the INUe shelf.

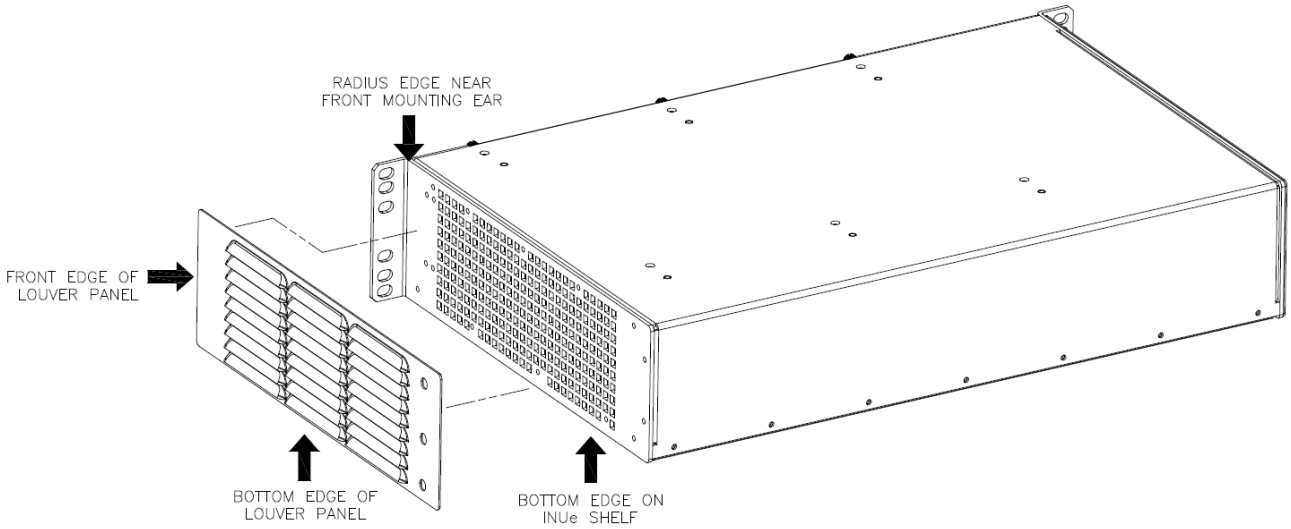


Figure 12 - Fitting the Right-Hand Louver Panel - 2

- Apply strong pressure to the side of the louver panel to bond PSA to the INUe shelf.

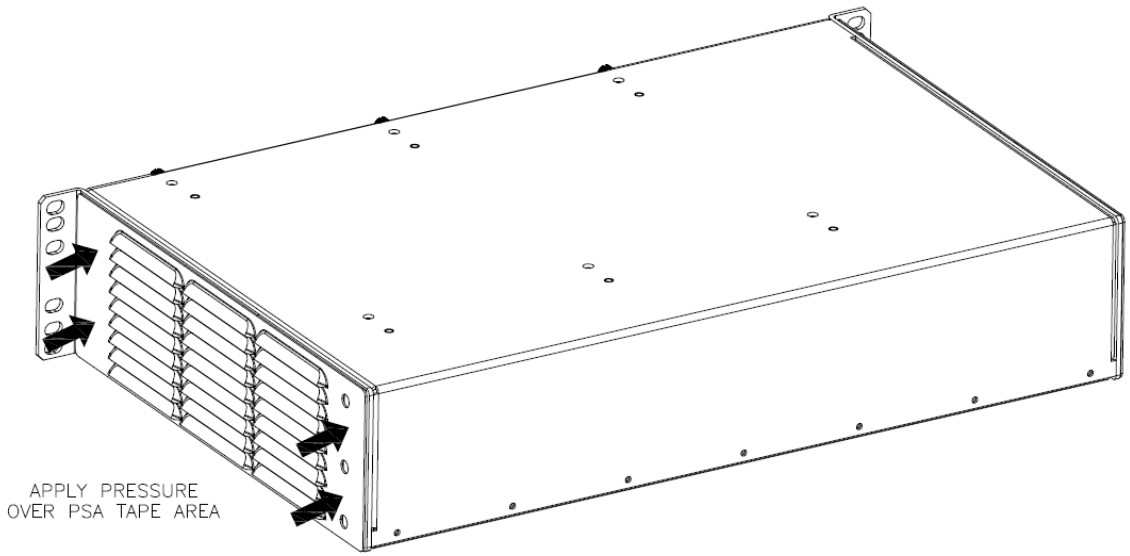


Figure 13 - Fitting the Right-Hand Louver Panel – 2

- Let the louver panel PSA cure for at least five (5) minutes then proceed to install the security seals to both sides.

- Apply security SEALS over louver panels:

Left hand side (as viewed from the front)

- Apply the wider security seal over louver panel and across INUe chassis. Use caution to avoid touching the adhesive with fingerprints to avoid damaging the seals. Allow the seal adhesive at least sixty (60) minutes to cure.

Figure 14 - Location of Security Seals on Louver Panel (Left Side)

Right hand side (as viewed from the front)

- Apply the wider security seal over louver panel and across INUe chassis. Use caution to avoid touching the adhesive with fingerprints to avoid damaging the seals. Allow the seal adhesive at least sixty (60) minutes to cure.

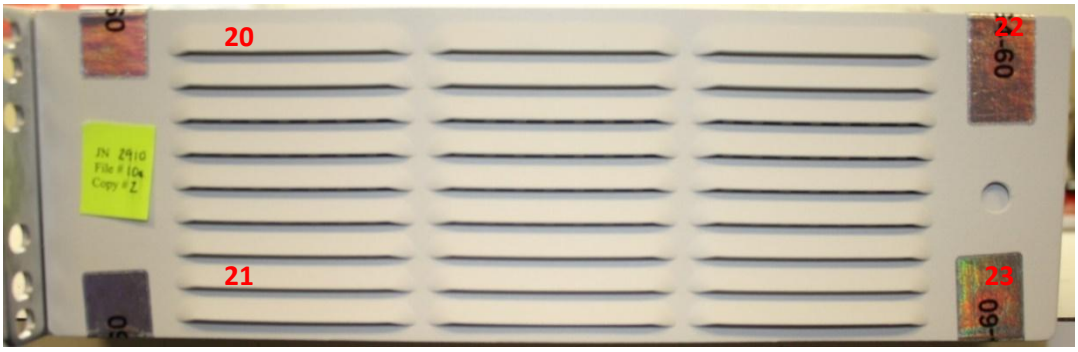


Figure 15 - Location of Security Seals on Louver Panel (Right Side)

Immediately before the INUe is installed into its rack/cabinet, apply the narrower tamper evident seals as shown in Figure 10 with a seal over each of the three (3) top-front screw heads, and apply the four (4) wider seals per side as indicated in Figure 14 and Figure 15.

- Clean the areas where the seals are to be applied as appropriate using alcohol-based cleaning pads or a rag moistened with isopropyl alcohol and let dry.
- When peeling and placing the seals avoid finger contact with the seal backing/adhesive to prevent damage to the seal. The use of tweezers applied on the edge of the seal is recommended.
- Ensure the seals are not damaged when installing the INUe into its rack/cabinet.

Louver panels (physical security kit 179-530153-002):

- Louvers and all associated tamper evident seals (detailed in the section above for kit 179-530153-001) will already be installed to the INUe.
- The operator must fully check the condition of the louvers and tamper evident seals applied to the louvers and replace any physical security items that are not fully intact.

8 Non-Invasive Security

8.1 Mitigation Techniques

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
Disk Drive (S2)	Stored in flash, associated by memory location (pointer).	Static
System Memory (S1)	Only stored in volatile memory (RAM).	Dynamic

Table 14: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input in plaintext (IO3)	Craft tool	Module (S1)	Plaintext	Manual	Direct	

Table 15: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Key zeroization service	Zeroization actively overwrites existing values with zeros. The new values are stored in the same place as the previous values and so the previous values are no longer retrievable.	Explicit

Table 16: SSP Zeroization Methods

9.4 SSPs

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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
ADFS Server Certificate	This is a user provided certificate for decrypting SAML 2.0 responses from an ADFS server (Microsoft Active Directory Federated Services) for user authentication.	2048-bit RSA certificate - 112 bits	Asymmetric public key - PSP			SAML (SFI #10)
Crypto-Officer Password	Used to authenticate Crypto-Officer to Craft Tool.	8 - 32 characters - N/A	Authentication Data - CSP			
Entropy Input String	Used to seed the Hash DRBG	1568 bits - N/A	Bit string - CSP			DRBG (SFI #14)
Hash DRBG C and V	These are variables used internally by the Hash DRBG that are required by Implementation Guidance 14.5 to be listed in the Cryptographic Module Security Policy document. They represent the internal state of the DRBG.	440 bits - N/A	DRBG security parameters - CSP	DRBG (SFI #14)		CKG (SFI #2)
Hash DRBG Seed	Seed for the Hash DRBG.	256 bits - 256 bits	DRBG security parameters - CSP	DRBG (SFI #14)		CKG (SFI #2)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Integrity key	A fixed and hard coded key used in the firmware load conditional self-test.	4096-bit RSA public key - 150 bits	Asymmetric public key - PSP	pre-loaded		Integrity (SFI #11)
Payload Encryption Certificate	Self-generated and self-signed certificate used to generate the Payload Encryption Tunnel Key and Payload Encryption HMAC Key. Certificate's public key is ECDSA/ECDH.	ECDSA/ECDH P-256 curve - 128 bits	Asymmetric public key - PSP	AsymKeyPair-KeyGen (SFI #3)		DigSig-SigVer (SFI #6)
Payload Encryption DTLS HMAC Keys	Used to authenticate the tunnel established using DTLS. HMAC-SHA-1.	160 bits Symmetric key - 160-bits	Symmetric key - CSP	CKG (SFI #2)		KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9)
Payload Encryption DTLS Tunnel Keys	Used to encrypt the tunnel established using DTLS. AES-256.	256 bits Symmetric key - 256 bits	Symmetric key - CSP		KAS-TLS1.2KDF (SFI #4) KAS-ECC-SSC (SFI #13) KAS1 (SFI #18)	BC-UNAUTH (SFI #7) BC-AUTH (SFI #8) BC-UNAUTH-DEC (SFI #15) BC-AUTH-DEC (SFI #16) KAS1 (SFI #18)
Payload Encryption Key	Used to encrypt/decrypt payload.	256 bits - 256 bits	Symmetric key - CSP		KAS-TLS1.2KDF (SFI #4)	BC-AUTH-ENC-

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Only AES- 256 bits is used for payload encryption.				KAS-TLS13KDF (SFI #12) KAS-ECC-SSC (SFI #13) KAS1 (SFI #18) KAS2 (SFI #19)	CCM1 (SFI #20) BC-AUTH-DEC-CCM1 (SFI #21) BC-AUTH-ENC-CCM2 (SFI #22) BC-AUTH-DEC-CCM2 (SFI #23)
Payload Encryption Private Key	ECDSA/ECDH P-256 key used to establish the Payload Encryption DTLS tunnel key.	ECDSA/ECDH P 256 curve - 128 bits	Asymmetric private key - CSP	AsymKeyPair-KeyGen (SFI #3)		DigSig-SigGen (SFI #5)
SNMPv3 Authentication Key	Used for authenticating SNMPv3 packets. HMAC-SHA-1.	128 bits - 128 bits	- CSP			SHA (SFI #1)
SNMPv3 Privacy Key	Used for encrypting SNMPv3 packets. AES-256.	128 bits - 128 bits	Asymmetric private key - CSP			BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) CKG (SFI #2)
TLS Certificate	This is used to establish TLS tunnel for HTTPS and WMTS ports for managing remote radio.	ECDSA/ECDH P-256 or P-384 curve - 128 bits or 192 bits	Asymmetric public key - PSP	AsymKeyPair-KeyGen (SFI #3)		DigSig-SigVer (SFI #6)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	Certificate's public key is ECDSA/ECDH. There are two options for the TLS Certificate. The default option is for a self-generated and self-signed certificate. The second option is for a user-uploaded, CA signed certificate that takes the place of the self-signed one when configured.					
TLS HMAC Keys	Message authentication within TLS. HMAC-SHA-1 or HMAC-SHA2-256, depending on cipher suite.	160 bits - 160 bits	Authentication Key - CSP	CKG (SFI #2)		KAS1 (SFI #18) KAS2 (SFI #19) MAC (SFI #9)
TLS Private Key	ECDSA/ECDH P-256 or P-384 key used to establish TLS tunnel for HTTPS and WMTS ports for managing remote radio.	Size: P-256, P-384 curves - Strength: 128-192 bits	Asymmetric private key - CSP	AsymKeyPair-KeyGen (SFI #3)		DigSig-SigGen (SFI #5) KAS1 (SFI #18) KAS2 (SFI #19)
TLS Tunnel Keys	Encrypt TLS session for the Craft tool and web server. AES-128 or AES-256, depending on cipher suite.	128 or 256 bits - 128 or 256 bits	Symmetric key - CSP		TLS v1.2 KDF RFC7627 (A6135) TLS v1.3 KDF (A6135)	BC-UNAUTH (SFI #7) BC-AUTH (SFI #8) BC-UNAUTH

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						-DEC (SFI #15) BC-AUTH-DEC (SFI #16) KAS1 (SFI #18) KAS2 (SFI #19)
User Password	Used to authenticate User to Craft Tool.	8 - 32 characters - N/A	Authentication Data - CSP			
P-256 TLS 1.2 Pre-Master Secret	Intermediate shared secret used to derive the Extended Master Secret	256 bits - 128 bits	Shared Secret - CSP		KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS1 (SFI #18)	BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) KAS1 (SFI #18)
P-384 TLS 1.2 Pre-Master Secret	P-256 TLS 1.2 Pre-Master Secret Intermediate shared secret used t	384 bits - 192 bits	Shared Secret - CSP		KAS-ECC-SSC (SFI #13) KAS-TLS1.2KDF (SFI #4) KAS1 (SFI #18)	BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) KAS1 (SFI #18)
P-256 TLS 1.3 Handshake Secret	Intermediate secret derived	256 bits - 128 bits	Shared Secret - CSP		KAS-TLS13KDF (SFI #12)	BC-AUTH (SFI #8)

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	from the initial key agreement				KAS1 (SFI #18) KAS2 (SFI #19)	BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) KAS2 (SFI #19)
P-384 TLS 1.3 Handshake Secret	Intermediate secret derived from the initial key agreement	384 bits - 192 bits	Shared Secret - CSP		KAS-TLS13KDF (SFI #12) KAS1 (SFI #18) KAS2 (SFI #19)	BC-AUTH (SFI #8) BC-AUTH-DEC (SFI #16) BC-UNAUTH (SFI #7) BC-UNAUTH-DEC (SFI #15) KAS2 (SFI #19)

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
ADFS Server Certificate	Input in plaintext (IO3)	Disk Drive (S2):Plaintext	N/A	Z1	
Crypto-Officer Password	Input in plaintext (IO3)	Disk Drive (S2):Plaintext	N/A	Z1	
Entropy Input String	Input in plaintext (IO3)	Disk Drive (S2):Plaintext	N/A	Z1	
Hash DRBG C and V		System Memory (S1):Plaintext	Zeroised when	Z1	Hash DRBG Seed:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
			module reset		
Hash DRBG Seed		System Memory (S1):Plaintext	Zeroised when module reset	Z1	Hash DRBG C and V:Derived From
Integrity key		Disk Drive (S2):Plaintext	N/A	Z1	
Payload Encryption Certificate		Disk Drive (S2):Plaintext	N/A	Z1	Payload Encryption Private Key:Paired With
Payload Encryption DTLS HMAC Keys		System Memory (S1):Plaintext	Zeroised when module reset	Z1	Payload Encryption DTLS Tunnel Keys:Used With
Payload Encryption DTLS Tunnel Keys		System Memory (S1):Plaintext	Zeroised when module reset	Z1	Payload Encryption DTLS HMAC Keys:Used With
Payload Encryption Key		System Memory (S1):Plaintext	Zeroised when module reset	Z1	
Payload Encryption Private Key		Disk Drive (S2):Plaintext		Z1	Payload Encryption Certificate:Used With
SNMPv3 Authentication Key	Input in plaintext (IO3)	System Memory (S1):Plaintext Disk Drive (S2):Plaintext	Zeroised when module reset	Z1	SNMPv3 Privacy Key:Used With
SNMPv3 Privacy Key	Input in plaintext (IO3)	System Memory (S1):Plaintext Disk Drive (S2):Plaintext	Zeroised when module reset	Z1	
TLS Certificate	Input in plaintext (IO3)	Disk Drive (S2):Plaintext	N/A	Z1	
TLS HMAC Keys		System Memory (S1):Plaintext	Zeroised when module reset	Z1	
TLS Private Key		Disk Drive (S2):Plaintext	N/A	Z1	TLS Certificate:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
TLS Tunnel Keys		System Memory (S1):Plaintext	Zeroized when module reset	Z1	
User Password	Input in plaintext (IO3)	Disk Drive (S2):Plaintext	N/A	Z1	
P-256 TLS 1.2 Pre-Master Secret	Input in plaintext (IO3)	Disk Drive (S2):Plaintext	N/A	Z1	
P-384 TLS 1.2 Pre-Master Secret	Input in plaintext (IO3)	Disk Drive (S2):Plaintext	N/A	Z1	
P-256 TLS 1.3 Handshake Secret	Input in plaintext (IO3)	Disk Drive (S2):Plaintext	N/A	Z1	
P-384 TLS 1.3 Handshake Secret	Input in plaintext (IO3)	Disk Drive (S2):Plaintext	N/A	Z1	

Table 18: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

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

Pre-operational self–tests are available on demand by power cycling the Module. Pre-operational Software/Firmware Integrity Test must pass their own CASTs prior to the Integrity Test.

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Bypass	Encryption of known data	KAT	Bypass	If the self-test fails, the module enters an error state and becomes unresponsive. If all pre-operational self-tests succeed, the module becomes operational.	RAC FPGA pre-operational bypass test is performed known Payload Encryption Key and known data (CAVP Cert. #A6136). Compares encrypted string to expected result.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity	RSA-4096 signature of a SHA2-512 hash of the firmware image.	KAT	SW/FW Integrity	If the self-test fails, the module enters an error state and becomes unresponsive. If all pre-operational self-tests succeed, the module becomes operational.	Firmware Integrity test performed by verifying the RSA-4096 signature of a SHA2-512 hash of the firmware image (CAVP Cert. #A6135)

Table 19: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC(A6135) Decrypt	AES-128-CBC, AES-256-CBC	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Decryption	Before first use of AES-CBC, or AES-GCM during boot-up
AES-CBC(A6135) Encrypt	AES-128-CBC, AES-256-CBC	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Encryption	Before first use of AES-CBC, or AES-GCM during boot-up
AES-CCM(A6136) Decrypt	AES-256-CCM	KAT	CAST	If the self-test fails, the module enters an	Decryption	Before first use of AES-CCM by the PDH version

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.		of the RAC FPGA during boot-up
AES-CCM(A6136) Encrypt	AES-256-CCM	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Encryption	Before first use of AES-CCM by the PDH version of the RAC FPGA during boot-up
AES-CCM(A6537) Decrypt	AES-256-CCM	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Decryption	Before first use of AES-CCM by the SDH version of the RAC FPGA during boot-up
AES-CCM(A6537) Encrypt	AES-256-CCM	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all	Encryption	Before first use of AES-CCM by the SDH version of the RAC FPGA during boot-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				algorithm bootup tests succeed, the module becomes operational.		
AES-CFB128 (A6135)	AES-CFB128	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Decryption	Before first use of AES-CFB128 during boot-up
AES-CFB128(A6135) Encrypt	AES-CFB128	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Encryption	Before first use of AES-CFB128 during boot-up
AES-GCM(A6135) Decrypt	AES-256-GCM	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module	Decryption	Before first use of AES-GCM during boot-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				becomes operational.		
AES-GCM(A6135) Encrypt	AES-256-GCM	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Encryption	Before first use of AES-GCM during boot-up
Bypass	Exclusive bypass	KAT	Bypass	RAC is disabled and no data is passed	RAC enters switches between a bypass mode and cryptographic mode of operation	
ECDSA KeyGen (FIPS186-5) (A6135)	Key pair correctness	ECDSA Pairwise Consistency test	PCT	Key rejected with error code	ECDSA Pairwise Consistency test	Asymmetric key pair generated
ECDSA SigGen (FIPS186-5) (A6135)	P-256	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Signature generation	Before first use of ECDSA during boot-up
ECDSA SigVer (FIPS186-5) (A6135)	P-256	KAT	CAST	If the self-test fails, the module	Signature verification	Before first use of ECDSA

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.		during boot-up
Firmware upgrade	Integrity test	KAT	SW/FW Load	Firmware upgrade fails. NCC Status LED illuminates solid red.	Firmware load test - Approved integrity technique using SHA2-512 and RSA. (RSA Cert. #A6135; SHS Cert. #A6135	Firmware upgrade
Hash DRBG (A6135)	[90A] Hash DRBG	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	[90A] Hash-based DRBG Known answer test [90A] Section 11.3 Health Tests	Before first use of DRBG during boot-up or immediately upon registering an external entropy source with the module
HMAC-SHA-1 (A6135)	HMAC-SHA-1	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the	Known answer test (CAVP Cert. #A6135)	Before first use of SHA-1 or HMAC-SHA-1 during boot-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				module becomes operational.		
HMAC-SHA2-256 (A6135)	HMAC-SHA2-256	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Known answer test (CAVP Cert. #A6135)	Before first use of SHA2-256 or HMAC-SHA2-256 during boot-up
HMAC-SHA2-512 (A6135)	HMAC-SHA2-512	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Known answer test (CAVP Cert. #A6135)	Before first use of SHA2-384, SHA2-512, HMAC-SHA2-384, or HMAC-SHA2-512 during boot-up
KAS-ECC-SSC Sp800-56Ar3 (A6135)	Shared secret Z	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Performs an ECC shared secret Z KAT using a NIST defined P-256 curve.	Before first use of ECC for shared secret generation during boot-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
Manual key entry	Duplicate key entry	Duplicate key entry	Manual Entry	Key rejected with error feedback	Operator enters the same key twice. The two entries are compared. If they match the test passes, if they do not match the test fails.	
RSA SigVer (FIPS186-5) (A6135)	2048-bit RSA	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Signature Verification. Performed before Pre-Operational FW integrity test.	Before first use of RSA during boot-up
TLS v1.2 KDF RFC7627 (A6135)	TLS v1.2 KDF	KAT	CAST	If the self-test fails, the module enters an error state and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.	Known answer test	Before first use of TLSv1.2 KDF during boot-up
TLS v1.3 KDF (A6135)	TLS v1.3 KDF	KAT	CAST	If the self-test fails, the module enters an error state	Known answer test	Before first use of TLSv1.3 KDF during boot-up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				and becomes unresponsive. If all algorithm bootup tests succeed, the module becomes operational.		

Table 20: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Bypass	KAT	Bypass	On Demand	Pre-operational self-tests are available on demand by power cycling the Module.
Firmware integrity	KAT	SW/FW Integrity	On Demand	Pre-operational self-tests are available on demand by power cycling the Module.

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC(A6135) Decrypt	KAT	CAST	On Demand	Manually
AES-CBC(A6135) Encrypt	KAT	CAST	On Demand	Manually
AES-CCM(A6136) Decrypt	KAT	CAST	On Demand	Manually
AES-CCM(A6136) Encrypt	KAT	CAST	On Demand	Manually
AES-CCM(A6537) Decrypt	KAT	CAST	On Demand	Manually
AES-CCM(A6537) Encrypt	KAT	CAST	On Demand	Manually
AES-CFB128 (A6135)	KAT	CAST	On Demand	Manually

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CFB128(A6135) Encrypt	KAT	CAST	On Demand	Manually
AES-GCM(A6135) Decrypt	KAT	CAST	On Demand	Manually
AES-GCM(A6135) Encrypt	KAT	CAST	On Demand	Manually
Bypass	KAT	Bypass	On Demand	Manually
ECDSA KeyGen (FIPS186-5) (A6135)	ECDSA Pairwise Consistency test	PCT	On Demand	Manually
ECDSA SigGen (FIPS186-5) (A6135)	KAT	CAST	On Demand	Manually
ECDSA SigVer (FIPS186-5) (A6135)	KAT	CAST	On Demand	Manually
Firmware upgrade	KAT	SW/FW Load	On Demand	Manually
Hash DRBG (A6135)	KAT	CAST	On Demand	Manually
HMAC-SHA-1 (A6135)	KAT	CAST	On Demand	Manually
HMAC-SHA2-256 (A6135)	KAT	CAST	On Demand	Manually
HMAC-SHA2-512 (A6135)	KAT	CAST	On Demand	Manually
KAS-ECC-SSC Sp800-56Ar3 (A6135)	KAT	CAST	On Demand	Manually
Manual key entry	Duplicate key entry	Manual Entry	On Demand	Manually
RSA SigVer (FIPS186-5) (A6135)	KAT	CAST	On Demand	Manually
TLS v1.2 KDF RFC7627 (A6135)	KAT	CAST	On Demand	Manually
TLS v1.3 KDF (A6135)	KAT	CAST	On Demand	Manually

Table 22: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ES1	The Module fails a KAT, PCT, or duplication, or conditional self-test.	The Module enters a failure state, and all input/output is suppressed and is automatically restarted.	Reboot	Outputs status of "FIPS self test failure" in the event log, otherwise it indicates successful completion by an output of "FIPS self tests passed" in the event log.
ES2	The Module fails a firmware loading	The module automatically attempts to roll back to the previous firmware version.	Reboot	Outputs status of "FIPS self test failure" in the event log, otherwise it indicates successful completion by an output of "FIPS self tests passed" in the event log.
ES3	The Module fails the firmware integrity pre-operational self-test.	The Module enters a failure state, and all input/output is suppressed and automatically attempts to roll back to the previous firmware.	Reboot	Outputs status of "FIPS self test failure" in the event log. No indication if no error detected.
ES4	The Module fails the manual duplicate key entry test.	The new input is rejected.	Manually re-enter keys.	Craft tool feedback to the CO is the pop-up message "Failed to commit changes to the terminal - Could not switch configuration."
ES5	A RAC plugin fails the pre-operational or conditional bypass test	The plugin enters a failure state, and all traffic output is suppressed. The plugin module is automatically reset. After three failed recovery attempts the plugin is disabled.	Reboot. If that fails, re-seat the RAC plugin module. Replace the RAC plugin module if previous recovery methods fail.	Outputs status of "FIPS self test failure" in the event log, otherwise it indicates successful completion by an output of "FIPS self tests passed" in the event log.

Table 23: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Delivery of the Cryptographic Module to customers from the vendor is via third party couriers. The parcels are sealed in tamper evident packaging, and each parcel is tracked from vendor to customer.

Once on site, the customer must follow vendor guidance (See Section 2.4) to securely install and configure the module.

Physical security measures must be installed as described in Section 7 above.

11.2 Administrator Guidance

Guidance appropriate to an operator's Role is provided with the module and provides all the necessary assistance to enable the secure operation of the module by an operator, including the Approved security functions of the module. The operator manual can be obtained at www.aviatcloud.com once an operator has been granted access to ARC (Aviat Resource Center).

11.3 Non-Administrator Guidance

Guidance appropriate to an operator's Role is provided with the module and provides all the necessary assistance to enable the secure operation of the module by an operator, including the Approved security functions of the module.

11.4 Design and Rules

Design documentation for the module is maintained to provide clear and consistent information within the document hierarchy to enable transparent traceability between corresponding areas throughout the document hierarchy, for instance, between elements of this Cryptographic Module Security Policy (CMSP) and the design documentation.

Rules of Operation

1. The Module provides three distinct operator roles: User, Maintenance and Crypto Officer.
2. The Module provides role-based authentication.
3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
6. All self-tests do not require any operator action.
7. Data output is inhibited during key generations, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The Module supports up to five concurrent operators.
11. The Module does not have any proprietary external input/output devices used for entry/output of data.
12. The Module does not store any plaintext CSPs

13. The Module does not output intermediate key values.

11.5 Additional Information

Aviat Networks employ industry standard best practices in the design, development, production and maintenance of the Aviat Networks Eclipse product, including the FIPS 140-3 module.

Aviat Networks has an ISO 9001 Quality Management System.

This includes the use of an industry standard configuration management system that is operated in accordance with the requirements of FIPS 140-3, such that each configuration item that forms part of the module is stored with a label corresponding to the version of the module and that the module and all of its associated documentation can be regenerated from the configuration management system with reference to the relevant version number.

12 Mitigation of Other Attacks

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

References and Definitions

The following standards are referred to in this Security Policy.

Abbreviation*	Full Specification Name
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, December 20, 2024*
[133r2]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[135r1]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, February 2023.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, May 9, 2023*

Abbreviation*	Full Specification Name
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38C]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, Special Publication 800-38C, May 2004*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[52r2]	*National Institute of Standards and Technology, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, Special Publication 800-52 revision 2, August 2019*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*

Table 24 – References

Acronym *	Definition
ECDH	Elliptic Curve Diffie-Hellman
KAT	Know Answer Test
SSP	Sensitive Security Parameter

Table 25 – Acronyms and Definitions