Aviat Networks Eclipse Cryptographic Module

FIPS 140-2 Non-Proprietary
Security Policy

Level 2 Validation

Document revision 053, January 2018

Contents

Figures

1   Introduction

This section identifies the cryptographic module; describes the purpose of this document; provides external references for more information; and explains how the document is organized.

1.1   Identification

Module Name   Aviat Networks Eclipse Cryptographic Module

Module Hardware

Component	Part number
INUe 2RU Chassis	EXE-002
Fan Card	EXF-101
Node Controller Card	EXN-004
Either FIPS Installation Kit (customer fitted)	179-530153-001
or FIPS Installation Kit (factory fitted)	179-530153-002
Replacement Labels	007-600331-001
At least one of:	
RAC 6X	EXR-600-001
RAC 6XE	EXR-600-002
RAC 60	EXR-660-001
RAC 60E	EXR-660-002
All remaining slots filled by one of the components listed in Figure 4	

Firmware Versions   08.02.91[1], 08.03.90

1.2   Purpose

This is the non-proprietary FIPS 140-2 Security Policy for the Aviat Networks Eclipse Cryptographic Module, also referred to as "the module" within this document. This Security Policy details the secure operation of Aviat Networks Eclipse Cryptographic Module as required in Federal Information Processing Standards Publication 140-2 (FIPS 140-2) as published by the National Institute of Standards and Technology (NIST) of the United States Department of Commerce and the Communications Security Establishment (CSE).

1.3   References

For more information on Aviat Networks Eclipse please visit:
http://aviatnetworks.com/products/microwave-switches/eclipse-carrier-ethernet-microwave-platform/

---

[1] This is the NCC firmware version. The module consists of a number of versioned components. For a complete list see Figure 3.

For more information on NIST and the Cryptographic Module Validation Program (CMVP), please visit http://csrc.nist.gov/groups/STM/cmvp/index.html.

1.4   Document Organization

This Security Policy document is one part of the FIPS 140-2 Submission Package. This document outlines the functionality provided by the module and gives high-level details on the means by which the module satisfies FIPS 140-2 requirements. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 submission documentation may be Aviat Networks proprietary or otherwise controlled and releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Aviat Networks.

The various sections of this document map directly onto the sections of the FIPS 140-2 standard and describe how the module satisfies the requirements of that standard.

1.5 Document Terminology

Term	Description
ACM	Adaptive Coding and Modulation
AES	Advanced Encryption Standard
API	Application Programming Interface
ASIC	Application Specific Integrated Circuit
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CSP	Critical Security Parameters
CVL	Component Validation List
DAC	Digital Access Card
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECCCDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
ECDSA	Elliptic Curve DSA
eM	Electrical MUX
FIPS	Federal Information Processing Standard
GUI	Graphical User Interface
HMAC	Keyed-Hash Message Authentication Code
INU	Intelligent Node Unit
IRU	Indoor Radio Unit
NCC	Node Control Card
NMS	Network Management System
NPC	Node Protection Card
ODU	Outdoor Unit
OS	Operating System
RAC	Radio Access Card
RSA	An algorithm for public-key cryptography. Named after Rivest, Shamir and Adleman who first publicly described it.
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SP	Security Policy
Storage Media	Any media for which Cryptographic Module protection in the form of data encryption is required. Storage Media include internal and external hard drives, memory sticks and floppy disks.
TCP/IP	Transmission Control Protocol/Internet Protocol
TDM	Time-Division Multiplexing
TLS	Transport Layer Security
XPIC	Cross Polarization Interference Cancellation

2 Aviat Networks Eclipse

This section provides the details of how the module meets the FIPS 140-2 requirements.

2.1 Overview

Aviat Networks' 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 is housed within 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.

2.2 Module Specification

2.2.1 Hardware and Firmware Components

The module runs on proprietary hardware. The hardware consists of a number of plug-in cards housed in a proprietary chassis in 2RU format.

The module consists of an Eclipse Node Control Card (NCC), one or more Radio access card (RAC) 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

Slot 1	Slot 2	Slot 3	F
Slot 4	Slot 5	Slot 6	A
Slot 7	Slot 8	Slot 9	N
NCC only		Slot 10	S

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 labels applied per Section 2.5 below.
- Slots 1, 2, 3, 4, 5, 6 are universal. Any RAC, DAC, NCM or AUX plug-in card.
- Slots 7, 8, 9 are restricted: any DAC, NCM or AUX, except DAC 155oM/eM where NMS is required.
- Slot 10 is for NPC option only
- NCC and FAN slots are dedicated – the INUe is supplied as standard with a single 2RU FAN, although it accepts two 1RU FANs.
- RAC/RAC or RAC/DAC 155oM/eM protected pairings must be installed in paired slots (Slot 1 and Slot 4, Slot 2 and Slot 5, or Slot 3 and Slot 6).
- For protected DACs or NCMs, the protection partners can be installed in Slots 1 through 9, except for the case of DAC 155oM/eM where NMS access is needed, which is restricted to Slots 1 through 6.

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, an NCC card, and at least one suitable security relevant RAC card to be installed in order to support the Payload Encryption and Payload Decryption services (see Figure 3).

ITEM	PART NUMBER AND REVISION	FIRMWARE/FPGA VERSION INFORMATION	QUANTITY IN MODULE	CRYPTOGRAPHIC FUNCTIONALITY
		BASELINE CONFIGURATION		
INUe 2RU Chassis	EXE-002	N/A	1	No
Node Controller Card	EXN-004	Firmware: 08.02.91, 08.03.90 Bootloader: 1.0.36 FPGA_NCCV2_E1_DS1_004.bit FPGA_NCCV2_STM1_006.bit	1	Yes
Fan Card	EXF-101	N/A	1	No
FIPS Installation Kit	Either: 179-530153-001 (customer fitted) or: 179-530153-002 (factory fitted)	N/A	1	No
Replacement Labels	007-600331-001	N/A	1	No
		And at least one of the following:		
RAC 6X	EXR-600-001	FPGA_RAC6X_PDH_ACM-14.19.52.bit FPGA_RAC6X_SDH-2.3.1.bit	0-6	Yes
RAC 6XE	EXR-600-002	FPGA_RAC6X_PDH_ACM-14.19.52.bit FPGA_RAC6X_SDH-2.3.1.bit	0-6	Yes
RAC 60	EXR-660-001	FPGA_RAC6X_PDH_ACM-14.19.52.bit FPGA_RAC6X_SDH-2.3.1.bit	0-6	Yes
RAC 60E	EXR-660-002	FPGA_RAC6X_PDH_ACM-14.19.52.bit FPGA_RAC6X_SDH-2.3.1.bit	0-6	Yes

Figure 3 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 (see Figure 4). No slot shall be left unpopulated.

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 4x	EXD-040-001	FPGA_DAC_4E1_DS1-15.1.4.bit FPGA_DAC_4E1_WAYSIDE-15.1.4.bit	0-5	No
DAC 155o	EXD-152-001	FPGA_DAC_155_MUXV2-2.1.3.bit	0-5	No
DAC 155oM (long)	EXD-153-001	FPGA_DAC_155_MUX_001.bit	0-5	No
DAC 155oM (short)	EXD-156-001	FPGA_DAC_155_MUXV2-2.1.3.bit	0-5	No
DAC 155eM	EXD-158-001	FPGA_DAC_155_MUXV2-2.1.3.bit.	0-5	No
DAC 16x	EXD-160-001	FPGA_DAC_16E1_DS1-15.1.4.bit	0-5	No
DAC 16xV2	EXD-161-001	FPGA_DAC16V2_E1_DS1-3.1.4.bit	0-5	No
DAC 16xV3	EXD-161-002	FPGA_DAC16V2_E1_DS1-3.1.4.bit	0-5	No
DAC ES	EXD-171-001	FPGA_DAC_ES_018.bit	0-5	No
DAC GE v2	EXD-180-002	N/A	0-5	No
DAC LL	EXD-180-005	N/A	0-5	No
DAC GE v2 no SFP	EXD-180-102	N/A	0-5	No
DAC GE3	EXD-181-001	FPGA_DAC_E3_MUX_132.bit	0-5	No
DAC GE3	EXD-181-002	FPGA_DAC_E3_DS3_NOMUX_002.bit	0-5	No
DAC 2x155o	EXD-252-001	FPGA_DAC_2STM1_020.bit	0-5	No
DAC 3xE3M	EXD-331-001	N/A	0-5	No
NCM	EXD-400-002	FPGA_NCM-1.1.112.bit FPGA_NCM_CES-1.1.417.bit FPGA_NCM_CES1-1.1.443.bit FPGA_NCM_HSF-1.0.133.bit FPGA_NCM_HSF_FIX-1.1.152.bit	0-5	No
24V card	EXP-024	N/A	0-1	No
RAC LL	EXR-910-001	FPGA_RACLL_IFC-3.1.8.bit	0-6	No
RAC 30v3	EXR-999-003	FPGA_RAC30_E3_DS3_002.bit	0-6	No
NPC	EXS-001	N/A	0-1	No
NPC, high output	EXS-002	N/A	0-1	No
Blank panel	EXX-001	N/A	0-10	No

Figure 4 Hardware Components

2.2.2   Cryptographic Boundary

The cryptographic boundary of the module 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.
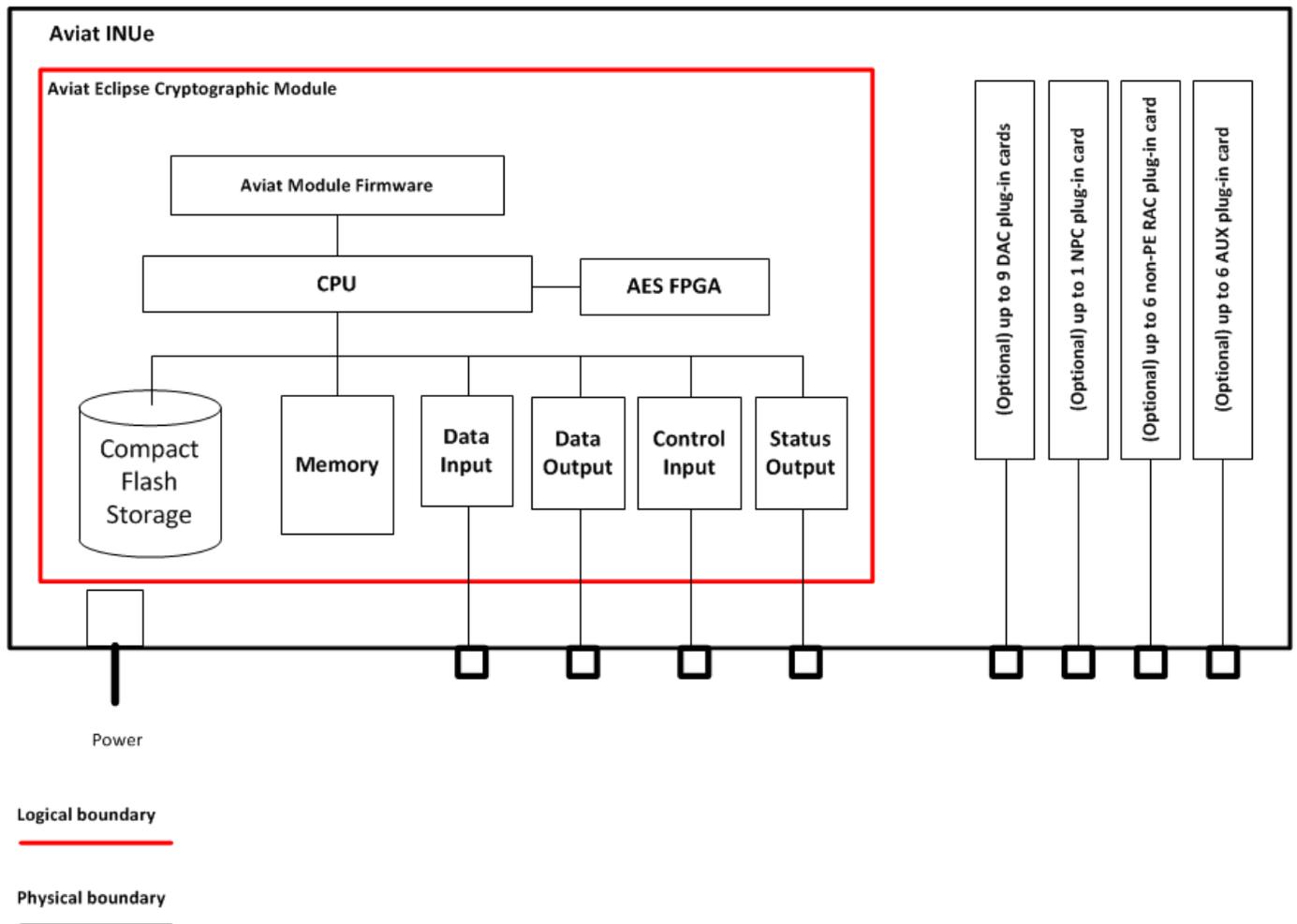
Figure 5 Block Diagram of the Cryptographic Boundary

2.2.3 Scope of Validation

The cryptographic module meets the overall requirements applicable to Level 2 security of FIPS 140-2, with Cryptographic Module Specification at Level 3 and Design Assurance at Level 3.

SECURITY REQUIREMENTS SECTION	LEVEL
Cryptographic Module Specification	3
Module Ports and Interfaces	2
Roles, Services and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

Figure 6 Security Level Specification Per Individual Areas of FIPS 140-2

2.2.4 Cryptographic Algorithms

2.2.4.1 Approved algorithms

The following table provides details of the Approved algorithms that are included within the module:

ALGORITHM TYPE	ALGORITHM	CAVP CERTIFICATE	USE
Symmetric key	AES-128-ECB, AES-192-ECB, AES-256-ECB, AES-128-CCM, AES-192-CCM and AES-256-CCM (Encryption only)	#2260	Payload Encryption
	AES-128-CBC, AES-256–CBC and AES-256–CFB128. (ECB was tested but is not used)	#2418	Strong Security Suite and Encryption of SNMPv3 sessions
SP 800-135 component	Section 4.2, TLS	#73	Within TLS (v1.0/1.1)

		#970	Within TLS (v1.2)
CVL	ECCCDH	#860	TLS cipher suites. ECCCDH SP 800-56A for NIST defined P-256 Curve
Deterministic Random Bit Generator	SP 800-90A Hash-based DRBG	#323	Key generation. Hash used is SHA-256.
Asymmetric key	ECDSA	#902	TLS cipher suites. NIST defined P-256 curve. Cipher suite uses signature generation and verification.
Authentication	HMAC-SHA-1 HMAC-SHA-256 (HMAC-SHA-384 was tested but is not used)	#2634	Within TLS and for SNMPv3
Asymmetric key	RSA	#2071	Firmware load test, module integrity test. Image has been hashed using SHA-256 and then signed with a 2048-bit RSA key. RSA signature verification is used in the self-test procedure.
	RSA	#2239	Bootloader integrity test.
Hashing	SHA-1	#3328	Used by SNMPv3 to obfuscate authentication messages.
	SHA-256 (SHA-384 was tested but is not used)		Firmware load test, Module integrity test, Hash DRBG, TLS cipher suite.
	SHA-256	#3397	Bootloader integrity test.

Figure 7 Approved Algorithms

For each Approved Key Derivation Function the module supports or uses a corresponding protocol. Any such related protocol can be used in the Approved mode of operation, but has not been reviewed or tested by the CAVP and CMVP as testing such protocols is not within the scope of CMVP or CAVP activities.

2.2.4.2   Non-Approved algorithms allowed in Approved mode

- Elliptic Curve Diffie-Hellman, not compliant (untested) to SP800-56A but allowed by IG D.8 (key agreement; key establishment methodology provides 128 bits of encryption strength)
- MD5
- NDRNG for seeding material to the FIPS Approved SP800-90A DRBG. The NDRNG provides at least 256 bits of entropy.

Elliptic Curve Diffie-Hellman is used for Payload Encryption key exchange. The module uses MD5 to hash firmware components to check integrity. This check is run in addition to the RSA integrity test and predates the FIPS Firmware integrity test. It is not security relevant. MD5 is also employed in RADIUS.

2.2.4.3   Non-Approved algorithms

The following algorithms are also included within the module and available in the Approved mode, but are only used by RADIUS for tasks related to authentication.
- MD5-CFB for encrypted password output to RADIUS server (RFC 2865 §5.2)
- MD5-MAC for authentication of RADIUS server (RFC 2865 §3, "Response Authenticator")

The following algorithms are also included within the module but *are only available within the module services in a non-FIPS mode* of operation:
- DES
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)

DES is used for securing the management interface (Portal) in a non-Approved mode of operation. Diffie-Hellman is used for Payload Encryption key exchange.

2.2.5   Components Excluded From the Security Requirements of the Standard

The following observable, non-security relevant components are excluded from FIPS 140-2 requirements:

- The components of all cards listed in Figure 4 except the faceplates. Since tamper evident seals are applied and necessary for physical security protection, the faceplates are security relevant and cannot be excluded. All other card components are excluded from FIPS requirements because they are non-security relevant.
- Components along both left and right sides of the RAC cards with the exception of U42 on cards RAC 6X, RAC 6XE, RAC 60, and RAC 60E. (Please see Appendix A for a complete list of excluded RAC card components.)

2.3   Physical Ports and Logical Interfaces

The module is classified as a multi-chip standalone module for FIPS 140-2 purposes. The module's physical boundary is that of the INUe chassis.

The module provides its logical interfaces via the physical interfaces provided in the chassis. These logical interfaces expose the services (described in section 2.4.2) provided by the module.

The logical interfaces provided by the module are mapped onto the FIPS 140-2 logical interfaces: data input, data output, control input, and status output as follows:

FIPS 140-2 LOGICAL INTERFACE	MODULE MAPPING
Data Input	INUe Front panel sockets. The NCC component has four 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. It also has a V.24 connector providing serial data access for Portal. (See Figure 15 for an image of the physical ports.) Data enter and leave RAC adapters via a single RJ-45 Ethernet socket. There is an RF socket to connect the RAC to a radio transceiver so that the data can be sent and received on a microwave link.
Data Output	INUe Front panel sockets
Control Input	INUe Front panel sockets
Status Output	INUe Front panel sockets and LEDs
Power Interface	NCC power interface and optional NPC. 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.

Figure 8 Module Interfaces

LED status indicators:

EVENT	NCC STATUS LED	NCC TEST LED	RAC STATUS LED
FIPS Power-up self-tests in progress	Flashing orange	Flashing orange	Solid red
Power-up self-test failure	Solid red	Off	Solid red
Self-tests pass/FIPS (Approved) mode enabled	Solid green	Solid green	Solid green

Figure 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.

2.4   Roles, Services and Authentication

2.4.1   Roles

The Cryptographic Module implements both a Crypto-Officer role and a User role. Roles are assumed explicitly using the authentication mechanisms described below. Section 2.4.2 summarizes the services available to each role.

ROLE	DESCRIPTION
Crypto-Officer	Mapping to a combination of the Eclipse's "Crypto", "Engineer" and "Admin" users. Crypto-Officer is able to configure security settings and payload encryption and manage user accounts.
User	Mapping on to the Eclipse "Read-only" user. A User is able to view the configuration for a specific link.
Maintenance	This 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.

Figure 10 Roles

Multiple concurrent operators are allowed. 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.

2.4.2   Services

2.4.2.1   User Services

The following services may only be performed by an operator with "User" access permissions who has been successfully authenticated to the module.

SERVICE	SERVICE INPUT	SERVICE OUTPUT	DESCRIPTION
RADIUS	Authentication request, username and password	Success/fail	User authentication using RADIUS. Successful authentication permits the identified User access to Craft Tool User Services.
Craft Tool Authentication	Authentication request, username and password	Success/fail	User authenticated locally by module. Successful authentication permits the identified User access to Craft Tool User Services. These allow a User to configure the characteristics of a specific microwave radio links, including enabling or disabling that link.
View Configuration	View Configuration	Event log entry	Provides a user with configuration

SERVICE	SERVICE INPUT	SERVICE OUTPUT	DESCRIPTION
	Request		information as an event log

Figure 11 User Services

2.4.2.2 Crypto-Officer Services

The following services may only be performed by an operator with "Crypto-Officer" access permissions who has been successfully authenticated to the module.

SERVICE	SERVICE INPUT	SERVICE OUTPUT	DESCRIPTION
Enable Payload Encryption	Request to switch on payload encryption for a specific link	Success/Fail	A Crypto-Officer may configure a secure data link to enable payload encryption.
Disable Payload Encryption	Request to switch off payload encryption for a specific link	Success/Fail	Although only a Crypto-Officer may configure a secure data link, a User may enable and disable encryption on a specific microwave radio link.
Craft Tool Authentication	Authentication request, username and password	Success/fail	Crypto-Officer authenticated locally by module. Successful authentication permits the identified Crypto-Officer access to Craft Tool Services.
Firmware Upgrade	Upgrade request and firmware image	Success/fail	Successfully upgrading the firmware loads the new image into module and reboots the module to allow the new firmware to become operational. If the firmware upgrade fails, then the new image is not loaded and the module rolls back to the original firmware and this remains operational.
Zeroize	Zeroize request	Success/fail	Zeroizes all plaintext secret and private cryptographic keys and CSPs within the module, specifically those listed in section 2.7.3.
Key Management (Payload Encryption)	Link ID. Service accessed via Craft tool GUI	Event log entry indicates success/failure	Generates a new key for the selected link.
Key Management (Secure Management)	Enable strong security via GUI	Event log entry indicates success/failure	Enabling strong security is a requirement of the FIPS mode of operation. Once enabled, the key management is automatic. Keys are established as required and used to secure the appropriate services.
Module	Craft tool GUI	Confirmation of	The Craft tool is used to configure the

SERVICE	SERVICE INPUT	SERVICE OUTPUT	DESCRIPTION
Configuration		parameters and actions	"strong security suite" within the module.
SNMP v3	Secure SNMP session request	Secure SNMP session	The module adds an extra layer of security to SNMP v3 by encrypting SNMP traffic using AES. SNMPv3 keys are manually entered. There is no internal key derivation.
RADIUS	Authentication request, username and password	Success/fail	Crypto-Officer authentication using RADIUS. Successful authentication permits the identified Crypto-Officer access to Craft Tool Services.
View Status Request	View Status Request	Event log entry	Provides a Crypto-Officer with status information as an event log.

Figure 12 Crypto-Officer Services

2.4.2.3 Unauthenticated Services

SERVICE	SERVICE INPUT	SERVICE OUTPUT	DESCRIPTION
Payload Encryption	Plaintext payload data	Encrypted payload data	Once a microwave link is configured and keys are established, any data sent on the link will be encrypted
Payload Decryption	Encrypted payload data	Plaintext payload data	Decrypts payload data received on a secure microwave link.
Perform Self-Tests	Power-up module	Self-test status	Self-tests are performed automatically at startup. If the self-tests fail, the module enters an error state. If they succeed, the module becomes operational.
View Status indicators	N/A	LED indicators	LED indicators provide information about the state of the payload encryption service and the self-test results.

Figure 13 Other Services

2.4.2.4   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 labels, 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 does not affect traffic.

Installation instructions are included with the fan filter kit.
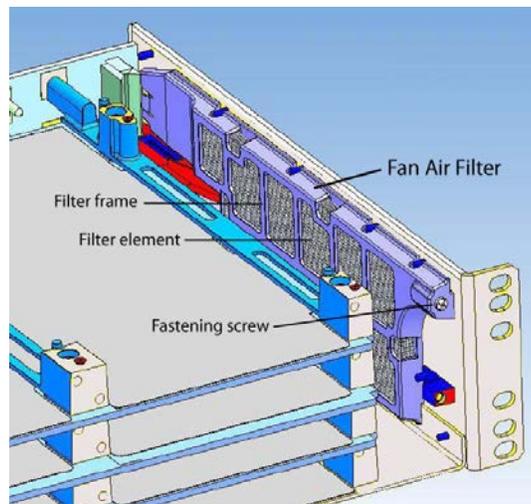

Figure 14 Location of Fan Air Filter in INUe

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 label, any residue from a previous label must be removed before a new label is applied.

2.4.3 Authentication

The module uses role-based and identity-based operator authentication. RADIUS may be used for user authentication and RADIUS is authenticated to the module using a shared secret. The RADIUS authentication is role-based. All other authentication is identity based.

User and Crypto-Officers are authenticated by presenting a username and password to the module for authentication. This is either done locally by the module using its own list of local users and their credentials or remotely using 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.

Locally defined passwords:
The passwords for the User and Cryptographic Officer roles, authenticating via the Portal GUI, are alphanumeric strings of between 8 and 32 alphanumeric characters comprised of at least one letter and one number.

The minimum number of possible passwords is, therefore, 94^6*10*52 or 3.59x10^14, which exceeds the minimum requirement of 1 in 1,000,000 for unsuccessful authentication probability.

With the minimum 8-character password of the required composition, that still gives a random chance of guessing the correct password in a single attempt of 1 in $94^6*10*52$, or 1 in $3.59x10^{14}$. Real-world passwords will normally be more complex than this. The module locks out user logon attempts for one minute after three consecutive logon failures. Assuming the weakest password and the ability of an attacker to make three logon attempts in a minute, this still gives the random chance of successfully guessing correctly a password given multiple attempts in a minute at slightly less than three times the single attempt chance, or very roughly 1 in $1x10^{13}$, which is significantly more secure than the than the 1 in 100,000 required.

RADIUS passwords:
The passwords for the User and Cryptographic Officer roles, authenticating via RADIUS, are alphanumeric strings consisting of a minimum of 5 characters. The minimum number of possible passwords is therefore 94^5, which exceeds the minimum requirement of 1 in 1,000,000 for unsuccessful authentication probability.

The module only allows three consecutive unsuccessful authentication attempts in any one minute period. Therefore, the probability of successfully authenticating to the module within one minute through random attempts is 3/94^5 which is less than 1/100,000.

2.5 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.

The INUe enclosure (Figure 15) 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 15 INUe Enclosure

The module is supplied with a set of tamper evident labels. Once a module is commissioned, the labels must be applied to the NCC, plug-in cards and blanking plates, such that for each item that borders that chassis, there is a label joining the item to the chassis. For each item that does not border the chassis, there is a label linking it to its neighbor.

Opacity: The module enclosure has vent holes at the sides. The vent holes are covered by louvers that provide no line of sight view of any internal components. Four (4) tamper evident labels are fitted to each louver.

Two (2) sizes of tamper evident labels are used in the module and must be fitted correctly to satisfy the physical security requirements for the module. The wider labels must be used for the louvers and the narrower labels must be used on the top front and on the front panel. Fitting instructions are provided below.
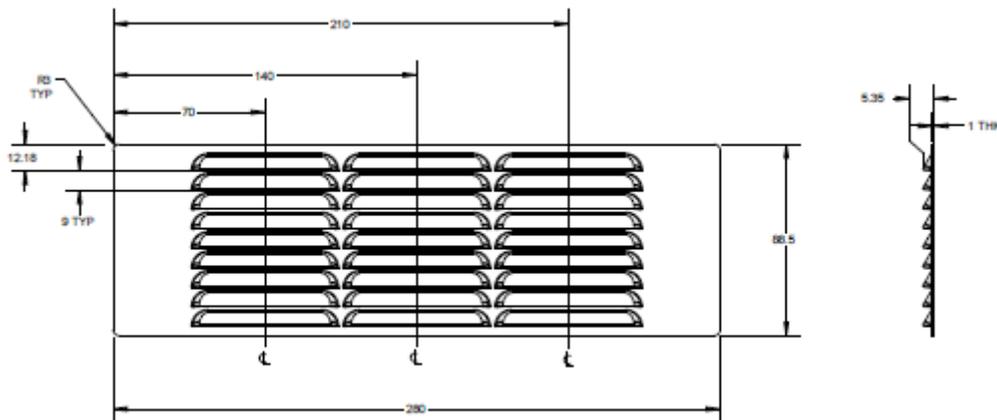
Figure 16 Louvers

The tamper evident labels and louvers/filters shall be installed for the module to operate in a FIPS Approved mode of operation.

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

To fit the louvers:

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 17 Left Hand Louver

- 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 18 Fitting the Left Hand Louver - 1

- Apply strong pressure to the side of the louver panel to bond the PSA to the INUe shelf.
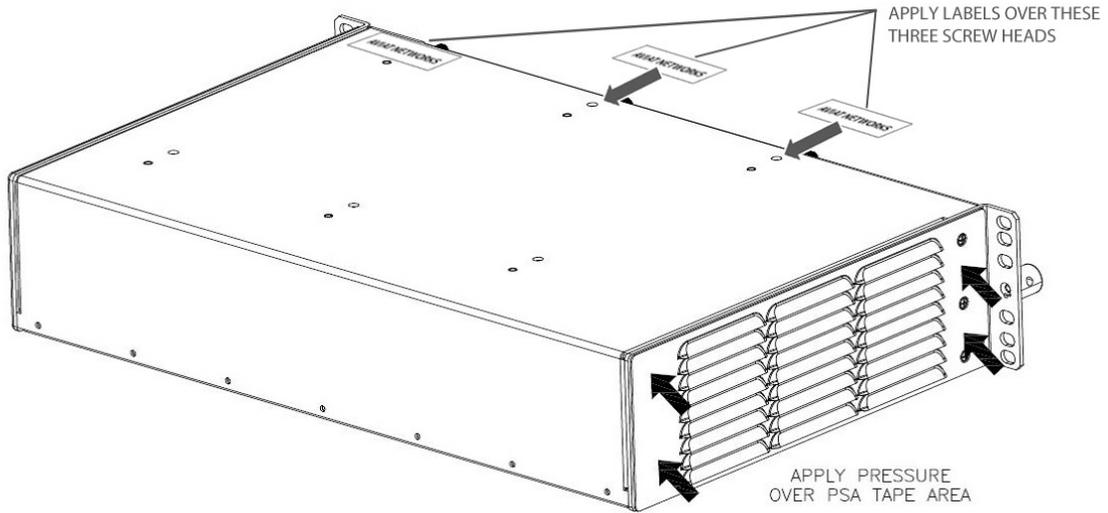
Figure 19 Fitting the Left Hand Louver – 2 and Position of "Top" Tamper Evident Labels

- Let the louver panel PSA cure for at least 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.
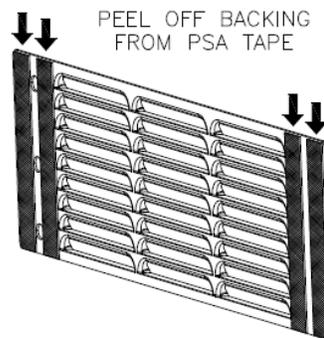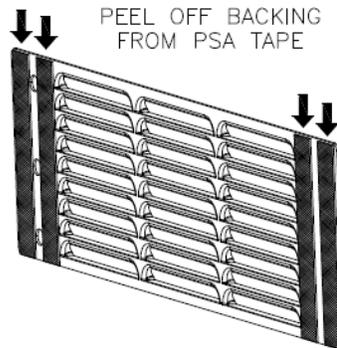

Figure 20 Right Hand Louver

- Align the front edge of the louver panel with the edge of the radius near the front mounting ear.
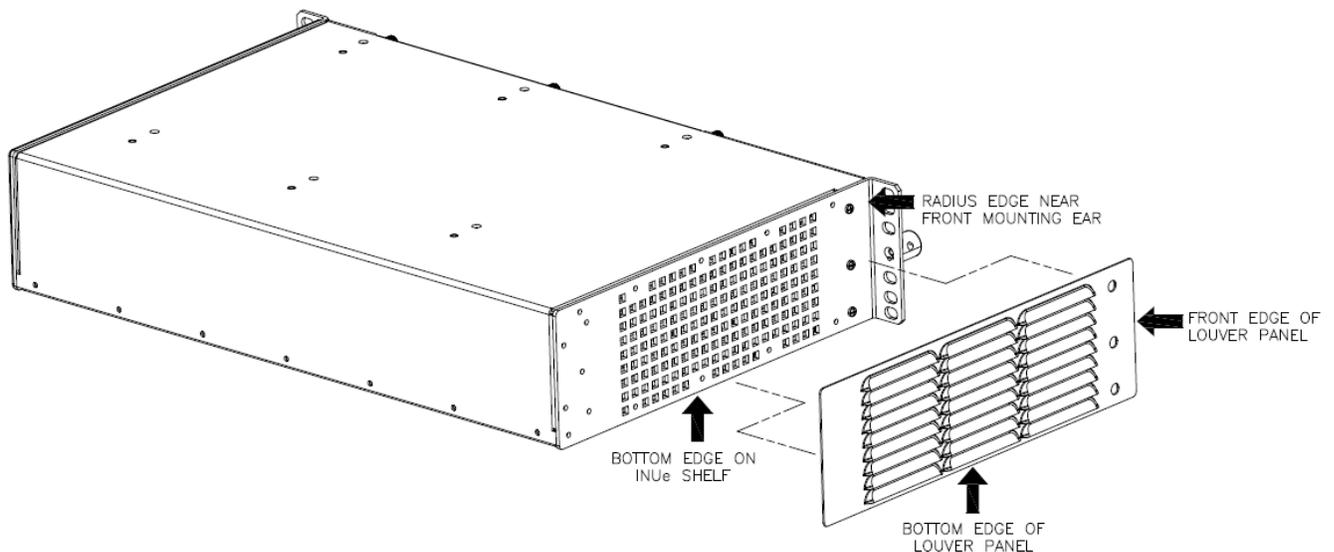- Align the bottom edge of the louver panel with the bottom edge of the INUe shelf.
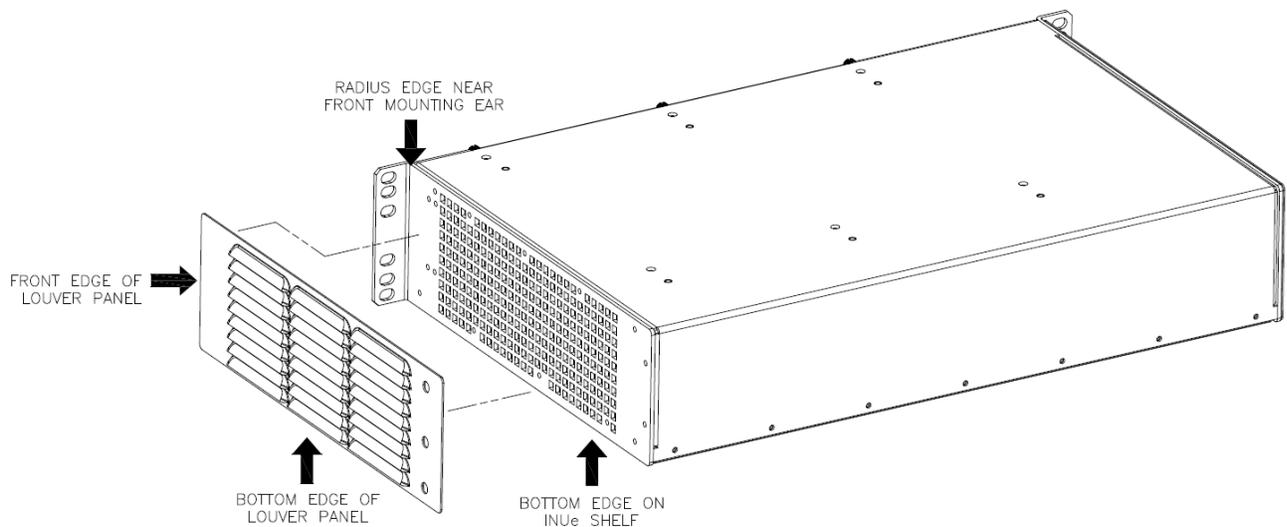
Figure 21 Fitting the Right Hand Louver - 1

- Apply strong pressure to the side of the louver panel to bond PSA to the INUe shelf.
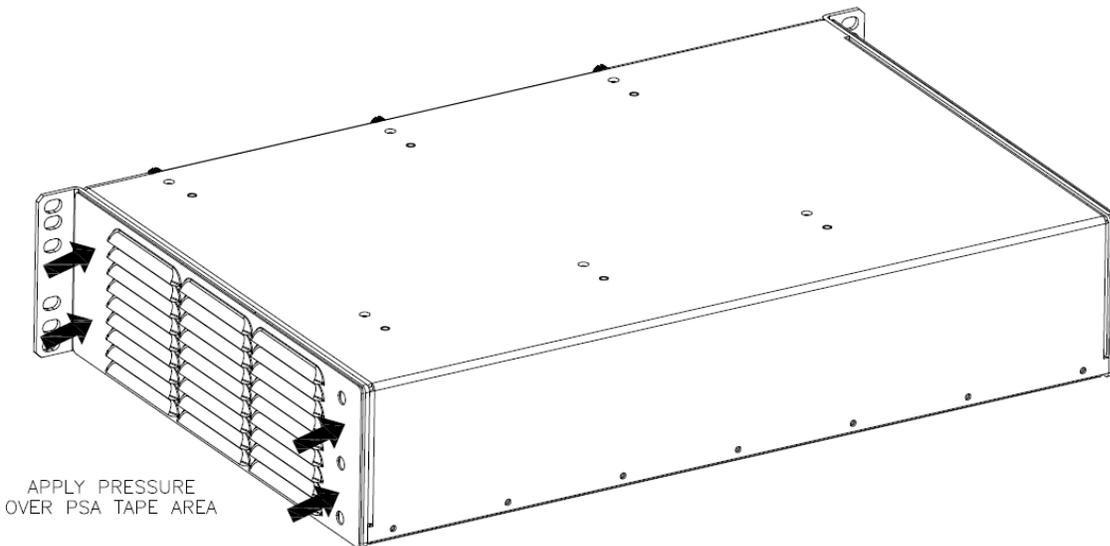
Figure 22 Fitting the Right Hand Louver – 2

- Let the louver panel PSA cure for at least 5 minutes then proceed to installing the security labels.

Apply security LABELS over louver panels:
Left hand side (as viewed from the front)
- Apply the wider security label over louver panel and across INUe chassis. Use caution to avoid touching the adhesive with fingerprints to avoid damaging the labels. Allow the label adhesive at least 60 minutes to cure.

Right hand side (as viewed from the front)
- Apply the wider security label over louver panel and across INUe chassis. Use caution to avoid touching the adhesive with fingerprints to avoid damaging the labels. Allow the label adhesive at least 60 minutes to cure.
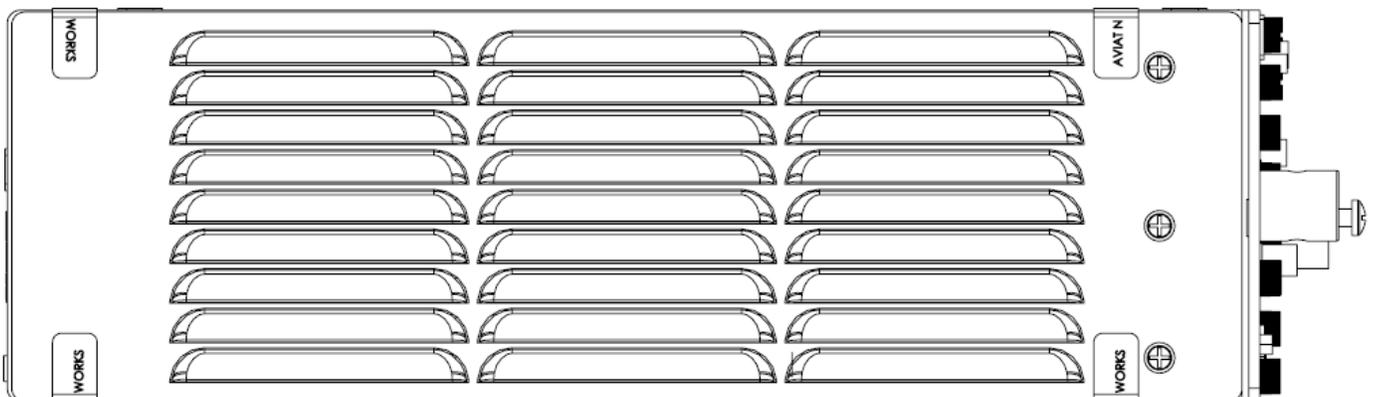
Figure 23 Location of Security Labels Over Louver Panel
(Left Hand Side Shown – Right Hand Side is Mirror Image)

Immediately before the INUe is installed into its rack/cabinet, apply the narrower tamper evident labels as shown in Figure 19 with a label over each of the three (3) top-front screw heads, and apply the four (4) wider labels per side as indicated in Figure 23.

- Clean the areas where the labels 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 labels avoid finger contact with the label backing to prevent damage to the label. The use of tweezers applied on the edge of the label is recommended.
- Ensure the labels are not damaged when installing the INUe into its rack/cabinet.

To install the tamper evident labels on front panel:
- 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 4)
- Remove excessive grease, dirt, or oil from the cover if appropriate by using alcohol-based cleaning pads before applying the tamper evident labels. The chassis temperature should be above 10° C (50° F).
- Affix (12) narrower tamper evident labels as indicated in Figure 24 below such that it is not possible to remove either a single card or a group of cards without also removing a label and leaving tamper evidence.
- Install the INUe shelf into the rack and apply security label over front of the cards in the chassis as shown. Use caution to avoid touching the adhesive with fingerprints to avoid damaging the labels. Allow the label adhesive at least 60 minutes to cure.
- The tamper evident labels should be replaced whenever components are added or removed from the module. Replacement labels can be ordered from Aviat Networks, part number 007-600331-001
- Tamper evident labels should be inspected for integrity at least once every six (6) months
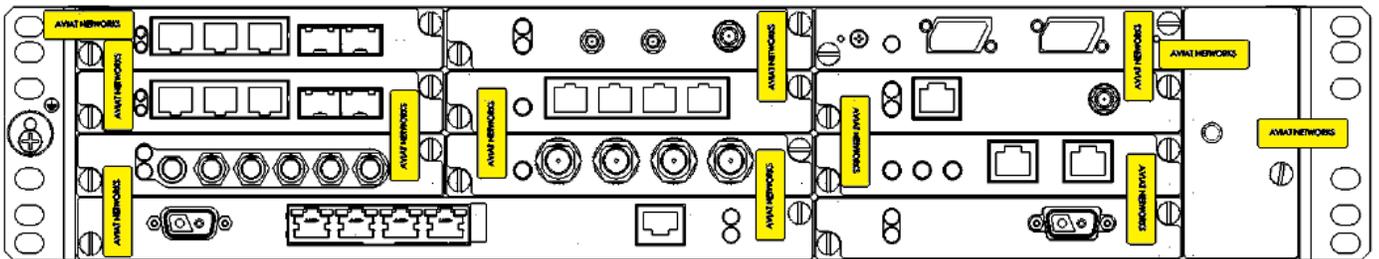
Figure 24 Tamper Evident Label Positions

2.6 Operational Environment

The module operational environment is derived from a version of embedded Linux. This has been adapted such that there is no general purpose operating system functionality available to an operator.

The only firmware that can be loaded is the module firmware. The module firmware can be updated using the "Firmware Upgrade" service. This requires the verification of a digital signature.

The Operating Environment of the module is a *limited operational environment* and so the Section 6 Operational Environment requirements are not applicable.

2.7   Cryptographic Key Management

2.7.1   Random Number Generators

The module contains an Approved SP 800-90A Hash-based DRBG.

2.7.2   Key Generation

Keys generated internally are generated by the SP 800-90A DRBG seeded by system entropy. The module uses the Hash-based DRBG to generate symmetric AES keys and Asymmetric ECDSA key pairs.

2.7.3   Key Table

The following tables list all of the keys and CSPs within the module, describe their purpose, and describe how each key is generated, entered and output, stored and destroyed.

KEY	PURPOSE
TLS Private Key	ECDSA/ECDH P-256 key used to establish TLS tunnel for HTTPS and WMTS ports for managing remote radio.
TLS Tunnel Keys	Encrypt TLS session for the Craft tool and web server. AES-128 or AES-256, depending on cipher suite.
TLS HMAC Keys	Message authentication within TLS. HMAC/SHA-1 or HMAC/SHA-256, depending on cipher suite.
RADIUS Shared Secret	Used to verify RADIUS messages.
SNMPv3 Privacy Key	Used for encrypting SNMPv3 packets. AES-128.
SNMPv3 Authentication Key	Used for authenticating SNMPv3 packets. HMAC/SHA-1.
Payload Encryption Private Key	ECDSA/ECDH P-256 key used to establish the Payload Encryption TLS tunnel key.
Payload Encryption TLS Tunnel Keys	Used to encrypt the tunnel established using TLS. AES-256.
Payload Encryption TLS HMAC Keys	Used to authenticate the tunnel established using TLS. HMAC/SHA-1.
Payload Encryption Key	Used to encrypt/decrypt payload. Only AES-128, 192 or 256 bits are used for payload encryption.
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.
Hash DRBG Seed	Seed for the Hash DRBG.
User Password	Used to authenticate User to Craft Tool.
Crypto-Officer Password	Used to authenticate Crypto-Officer to Craft Tool.

Figure 25 Module Cryptographic Keys and CSPs

KEY	PURPOSE
TLS Certificate	Self-generated and self-signed certificate used to establish TLS tunnel for HTTPS and WMTS ports for managing remote radio. Certificate's public key is ECDSA/ECDH. Can use any of the following cipher suites to establish tunnel: TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA
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. The mechanism for exchanging the Payload Encryption key is to create a TLS tunnel first and then transmit the generated AES key to the remote end. For this we are using a different self-signed TLS certificate and secret key from the HTTPS and WMTS TLS tunnel. The TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA cipher suite is used.
Integrity key	A fixed and hard coded key used in the firmware load conditional self-test

Figure 26 Module Public Keys

Key	Key Type and Strength	Generation/Establishment	Storage Location
TLS Private key	ECDSA/ECDH P-256 curve	Generated by module	Flash memory
TLS tunnel keys	128 or 256 bit depending on TLS cipher suite used	Key is established using TLS	RAM
TLS HMAC keys	160 bits	Established using TLS	RAM
RADIUS shared secret	5-32 characters	Entered by Crypto-Officer	RAM, Flash memory
SNMPv3 privacy key	128 bits	Entered by Crypto-Officer	RAM, Flash memory
SNMPv3 authentication key	128 bits	Entered by Crypto-Officer	RAM, Flash memory
Payload Encryption Private key	ECDSA/ECDH P-256 curve	Generated by module	Flash memory
Payload Encryption TLS tunnel keys	256 bits Symmetric key	Generated by the module and established using TLS.	RAM
Payload Encryption TLS HMAC keys	160 bits Symmetric key	Generated by the module and established using TLS.	RAM
Payload encryption key	128, 192 or256 bits	Generated by module.	RAM
Hash DRBG C and V CSP	440 bits	Hash of entropy bits, nonce bits, and personalization string	RAM
Hash DRBG Seed	[Entropy seed]	Generated by NDRNG	RAM
User Password	8-32 characters	N/A	A hash of the password is stored persistently although the password itself is only held in RAM until authentication is completed
Crypto-Officer Password	8-32 characters	N/A	Not persistently stored, held in RAM until authentication is completed

Figure 27 Key Table Part 1

KEY	ARE KEYS SUPPLIED ENCRYPTED OR PLAINTEXT?	ENTRY/OUTPUT	DESTRUCTION
TLS Private key	Plaintext	Generated in module, not entered. Not output.	Key is zeroized.
TLS Tunnel keys	Encrypted	Established using TLS	Key is zeroized.
TLS HMAC keys	Encrypted	Established using TLS	Key is zeroized.
RADIUS shared secret	Encrypted	Entered by Crypto-Officer through Craft tool. Not output	Key is overwritten. When the key is updated using portal, the new key is transmitted over TLS to the INU. The INU zeroizes the existing key in the encrypted key object. The INU then stores the new key in the encrypted key object. This key is used in all future requests to the RADIUS server. Encryption of the key is done using AES-128 in CBC mode.
SNMPv3 privacy key	Plaintext	Entered by Crypto-Officer through Craft tool. Not output	Key is overwritten. To zeroize the key, the CO needs to overwrite it by manually entering a new key.
SNMPv3 authentication key	Plaintext	Entered by Crypto-Officer through Craft tool. Not output.	Key is overwritten. To zeroize the key, the CO needs to overwrite it by manually entering a new key.
Payload Encryption Private key	Plaintext	The key neither enters nor leaves the module.	Key is zeroized.
Payload Encryption TLS tunnel keys	Encrypted	Established using TLS	Key is zeroized
Payload Encryption TLS HMAC keys	Encrypted	Established using TLS	Key is zeroized
Payload Encryption key	Encrypted	Exchanged with peer module using existing TLS tunnel	Key is zeroized
Hash DRBG C and V	Plaintext	N/A	Key is zeroized
Hash DRBG Seed	Plaintext	N/A	Key is zeroized
User Password	N/A	Entered by User during Craft Tool operator authentication. Not output.	Hashed passwords are stored to allow authentication. Actual passwords are zeroized once authentication is completed.
Crypto-Officer Password	N/A	Entered by Crypto-Officer during Craft Tool operator authentication. Not output.	Hashed passwords are stored to allow authentication. Actual passwords are zeroized once authentication is completed.

Figure 28 Key Table Part 2

KEY	KEY LENGTH/STRENGTH	GENERATION/ESTABLISHMENT	STORAGE LOCATION
TLS Certificate	ECDSA/ECDH P-256 curve	Generated by module	Flash memory.
Payload Encryption Certificate	ECDSA/ECDH P-256 curve	Derived from private key	Flash memory.
Integrity key	2048-bit RSA certificate	Fixed key	Public integrity key will be stored within the module. The private key will not.

Figure 29 Public Key Table Part 1

KEY	ARE KEYS SUPPLIED ENCRYPTED OR PLAINTEXT?	ENTRY/OUTPUT
TLS Certificate	Signed by ECDSA.	Generated in module, not entered. May be output.
Payload Encryption Certificate	Plaintext.	Generated in module, not entered. May be output.
Integrity key	Plaintext.	Fixed.

Figure 30 Public Key Table Part 2

2.7.4 CSP Destruction

All secret and private key material managed by the module can be zeroized using the key zeroization service. This is a Crypto-Officer service requiring Crypto-Officer authentication. CSP zeroization is performed procedurally and requires the Crypto-Officer to enter zero values for the manually entered CSPs (SNMPv3 passwords and RADIUS shared secret) and also perform the key zeroization service to zeroize the other secret and private keys. A reboot of the module is required to complete the CSP zeroization and the Crypto Office should remain in control of the module until the module self-tests have completed following the reboot.

2.7.5 Access to Key Material

The following table shows the access that an operator has to specific keys or other critical security parameters when performing each of the services relevant to his/her role.

Access Rights

Blank   Not Applicable
R   Read
W   Write
X   Execute
Z   Zeroize

KEY	TLS Private Key	TLS Tunnel Keys	TLS HMAC Keys	TLS Certificate	RADIUS Shared Secret	SNMPv3 Privacy Key	SNMPv3 Authentication Key	CA Public Key	CA Certificate	Payload Encryption Certificate	Payload Encryption Private Key	Payload Encryption Key	Payload Encryption TLS Tunnel Keys	Payload Encryption TLS HMAC Keys	Firmware Integrity Key	Hash DRBG "C" CSP	Hash DRBG "V" CSP	Hash DRBG Seed	User Password	Crypto-Officer Password
User Services																				
View Configuration	R	R	R	R	R								R	R						
Craft Tool	R	R	R	R	R								R	R					X	
Crypto-Officer Services																				
Disable Payload Encryption	R	R	R	R	R								R	R						
Enable Payload Encryption	R	R	R	R	R								R	R						
Craft Tool	R	R	R	R	R								R	R						X
Firmware Upgrade															R					
Zeroize	Z	Z	Z		Z	Z	Z			Z	Z	Z	Z	Z		Z	Z	Z		
Key Management (Payload Encryption)								R	R	R	R	W				X	X	X		
Key Management (Secure Management)	R	R	R	R	R								R	R						
Module Configuration	R	R	R	R	R															
SNMP v3						R, W	R, W													
RADIUS					R, W															
View Status	R	R	R	R	R								R	R						

KEY	TLS Private Key	TLS Tunnel Keys	TLS HMAC Keys	TLS Certificate	RADIUS Shared Secret	SNMPv3 Privacy Key	SNMPv3 Authentication Key	CA Public key	CA Certificate	Payload Encryption Certificate	Payload Encryption Private key	Payload Encryption Key	Payload Encryption TLS Tunnel Keys	Payload Encryption TLS HMAC Keys	Firmware Integrity key	Hash DRBG "C" CSP	Hash DRBG "V" CSP	Hash DRBG Seed	User Password	Crypto-Officer Password
Request																				
Unauthenticated Services												X								
Payload Encryption												X								
Payload Decryption																				
Perform Self-Tests		Z	Z													Z	Z	Z		
View Status indicators																				

Figure 31 Access to Keys by Services

Note: Key zeroization zeroizes all keys and CSPs; this is a "write" operation in that all keys are overwritten with zeroes.

2.8 Self-Tests

The module implements both power-up and conditional self-tests as required by FIPS 140-2.

The following two sections outline the tests that are performed.

2.8.1 Power-up Self-tests

After power cycling or booting the appliance the module executes the Power-Up Self-Tests with no further inputs or actions by the operator.

The module implements the following power-up self-tests. The module inhibits all data output while it is operating in the Self-Test state.

OBJECT	TEST
AES (#2418)	AES-128-CBC Encrypt Known answer test

OBJECT	TEST
	AES-256-CBC Encrypt Known answer test AES-256-CFB128 Encrypt Known answer test AES-128-CBC Decrypt Known answer test AES-256-CBC Decrypt Known answer test AES-256-CFB128 Decrypt Known answer test
AES (#2260)	AES-128-CCM Encrypt Known answer test AES-192-CCM Encrypt Known answer test AES-256-CCM Encrypt Known answer test
RSA	Known answer test (signature verification; RSA Cert. #2071)
ECDSA	Known answer test (signature generation) Known answer test (signature verification)
DRBG	SP 800-90A Hash-based DRBG Known answer test SP 800-90A Section 11.3 Health Tests
ECCCDH	Performs an ECCCDH KAT using a NIST defined P-256 curve.
Bootloader	Integrity test performed by verifying the RSA-2048 signature of a SHA-256 hash of the bootloader image (RSA Cert. #2239; SHS Cert. #3397)
Module firmware	Firmware Integrity test performed by verifying the RSA-2048 signature of a SHA-256 hash of the firmware image (RSA Cert. #2071; SHS Cert. #3328)
HMAC-SHA-1	Known answer test (SHS Cert. #3328)
HMAC-SHA-256	Known answer test (SHS Cert. #3328)
SHA-1	Known answer test (SHS Cert. #3328)

Figure 32 Power-up Self-tests

Note: For historical reasons, the module also performs an RSA signature generation known answer test at power-up, but the module no longer uses RSA signature generation in an Approved mode of operation.

2.8.2 Conditional Self-tests

Event	Test	Consequence of Failure
Module requests a random number from the FIPS Approved SP 800-90A DRBG	A continuous random number generator test	Random number is not generated and module enters an error state
Entropy is supplied to the FIPS Approved SP 800-90A Hash-based DRBG	A continuous random number generator test on the entropy NDRNG	Entropy is not added and module enters an error state
Firmware upgrade	Firmware load test – Approved integrity technique using SHA-256 and RSA. (RSA Cert. #2071; SHS Cert. #3328)	Firmware upgrade fails
Manual key entry test	Duplicate entries	Key not loaded
Asymmetric key pair generated	ECDSA Pairwise Consistency test	Key rejected and module enters an error state
RAC enters switches between a bypass mode and cryptographic mode of operation	Exclusive Bypass test – two independent actions are required to change mode (encrypted to bypass and vice versa) and test the correct operation of the services providing cryptographic processing when the switch occurs	RAC is disabled and no data is passed

Figure 33 Conditional Self-tests

2.9 Design Assurance

Aviat Networks employ industry standard best practices in the design, development, production and maintenance of the Aviat Networks Eclipse product, including the FIPS 140-2 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 140-2, 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.

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.

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

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 to securely install and configure the module.

2.10 Mitigation of Other Attacks

The module does not mitigate any other attacks.

3 FIPS Mode of Operation

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 described in section 2.5 above.

The module is set into FIPS mode as follows:

1.   Install FIPS capable NCC with CF card containing FIPS validated firmware
2.   Power up NCC
3.   Connect to NCC with Portal
4.   Install S/W license containing Strong Security, FIPS compliance, and optional Payload Encryption
5.   Set security mode to "FIPS"
6.   Select "Yes" when Portal asks for confirmation
7.   NCC reboots
8.   Connect to NCC using Portal
9.   Log in to NCC using a default Crypto-Officer
10. Configure desired security settings and add local users and/or RADIUS servers as required
11. By default Payload Encryption is disabled, Bypass warning alarm raised against RAC
12. Log in as a user with Crypto-Officer permissions
13. Perform other RAC and Payload Encryption configuration and enable Payload Encryption

The use of the Approved mode locks out the use of non-Approved algorithms.

For more details, please see the Eclipse User Manual Addendum for FIPS 140-2.

Appendix A- RAC 60E/6XE Excluded Components

None of these components process plaintext CSPs or represent a threat of the unit being compromised should they fail.

View 1		(Along Top of RAC Card)	
Ref	Part Number	Part Description	Circuit
J6		Connector (not fitted)	FPGA 1/2 (SCH Sheet 8) - Test Header
J4		Connector (not fitted)	Master Modem 2/3 (SCH Sheet 12) - Debug Connector
R211		Resistor	Master Modem 2/3 (SCH Sheet 12) - Debug pull-up
J5		Connector (not fitted)	Master Modem 2/3 (SCH Sheet 12) - BDM/JTAG Connector
U20	084-397128-001	IC, CPLD XC9572XL-10VQ64I	CPLD & JTAG Interface (SCH Sheet 5) - Logic
U40	083-845385-001	IC, BUFFER / LINE DRIVER	CPLD & JTAG Interface (SCH Sheet 5) - JTAG Buffer
J7		Connector	CPLD & JTAG Interface (SCH Sheet 5) - JTAG Connector
C404		Capacitor	Master Modem 1/3 (SCH Sheet 11) - 1.2V Regulator
C405		Capacitor	Master Modem 1/3 (SCH Sheet 11) - 1.2V Regulator
U16	080-417105-001	IC, REGULATOR 1.2V, 800MA	Master Modem 1/3 (SCH Sheet 11) - 1.2V Regulator
U26	080-417089-001	IC, 500 MA, 3.3 V, REGULATOR	Master Modem 1/3 (SCH Sheet 11) - 3.3V Regulator
C39		Capacitor	Master Modem 1/3 (SCH Sheet 11) - 3.3V Regulator
C35		Capacitor	Master Modem 1/3 (SCH Sheet 11) - 3.3V Regulator
R192		Resistor	Master Modem 2/3 (SCH Sheet 12) - Sys Clk pull-down
R195		Resistor	Master Modem 2/3 (SCH Sheet 12) - Sys Clk pull-up
C49		Capacitor	Master IF Transceiver (SCH Sheet 17) - 3.3V Regulator
FB17	063-501118-001	6A BEAD INDUCTOR	Master IF Transceiver (SCH Sheet 17) - 3.3V Regulator
U30	080-417089-001	IC, 500 MA, 3.3 VDC, REGULATOR	Master IF Transceiver (SCH Sheet 17) - 3.3V Regulator
C360		Capacitor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R420		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R422		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R423		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R425		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R426		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF

Ref	Part Number	Part Description	Circuit
			Power
R427		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
U35	081-306311-003	DUAL OPAMP LM2904	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R415		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R416		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R418		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R419		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R421		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
R424		Resistor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
C350		Capacitor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
L28	063-312470-720	IND,CHIP 47NH 2% 1008	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
C353		Capacitor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
C354		Capacitor	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
U12	082-433001-001	IC, 2.5GHZ PWR DETECT AD8361	N-Plexer / ODU INTF (SCH Sheet 20) - Tx IF Power
FL4	075-501032-001	N-PLEXER, DC SURGE ARREST	N-Plexer / ODU INTF (SCH Sheet 20) - N-Plexer

View 2		(Along Bottom of RAC Card)	
Ref	Part Number	Part Description	Circuit
F1	027-386008-001	FUSE, 5A, SMT 125VAC/DC, FAST	Power Regulation (SCH Sheet 3) - ODU Power
R7		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R8		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R30		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R31		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R32		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R33		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R34		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
C67		Capacitor	Power Regulation (SCH Sheet 3) - ODU Power
U33	081-306311-003	DUAL OPAMP LM2904	Power Regulation (SCH Sheet 3) - ODU Power Amux and Telemetry (SCH Sheet 6) - 48V Monitor
R121		Resistor	Amux and Telemetry (SCH Sheet 6) - 48V Monitor
R10		Resistor	Amux and Telemetry (SCH Sheet 6) - 48V Monitor
R123		Resistor	Amux and Telemetry (SCH Sheet 6) - 48V Monitor
CR8	077-313988-001	D'L SWIT'G 70V/.25A BAV99 S023	Amux and Telemetry (SCH Sheet 6) - 48V Monitor

C27		Capacitor	Power Regulation (SCH Sheet 3) - 1.2V Regulator
C394		Capacitor	Power Regulation (SCH Sheet 3) - 1.2V Regulator
C396		Capacitor	Power Regulation (SCH Sheet 3) - 1.2V Regulator
C398		Capacitor	Power Regulation (SCH Sheet 3) - 1.2V Regulator
C399		Capacitor	Power Regulation (SCH Sheet 3) - 1.2V Regulator
FL2	075-316592-003	FILTER 6800PF 110V/10A SMT	Power Regulation (SCH Sheet 3) - 1.2V Regulator
U18	080-417118-001	IC, 8A 4MHZ STEP-DOWN REG	Power Regulation (SCH Sheet 3) - 1.2V Regulator
C393		Capacitor	Power Regulation (SCH Sheet 3) - 1.2V Regulator
C401		Capacitor	Power Regulation (SCH Sheet 3) - 1.2V Regulator
U15	083-845422-002	IC, QAM XPIC MODEM, PVG610X	Slave Modem (SCH Sheets 14 & 15) - Modem
U3	081-302321-001	DUAL OPAMP LMC6482	Master IF Transceiver (SCH Sheet 17) - AGC Slave RX IF (SCH Sheet 18) - AGC
U34		DUAL OPAMP	Slave RX IF (SCH Sheet 18) - VCM Slave RX IF (SCH Sheet 18) - XPOL Alarm
C414		Capacitor	Slave RX IF (SCH Sheet 18) - AGC
C415		Capacitor	Slave RX IF (SCH Sheet 18) - AGC
R15		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R16		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R17		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R18		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R37		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
Q3	078-362091-002	XSTR GP PNP (2N)5401	Power Regulation (SCH Sheet 3) - ODU Power
Q11	078-381091-001	XSTR GP NPN (2N)5550	Power Regulation (SCH Sheet 3) - ODU Power
R38		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R39		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R40		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R41		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
C4		Capacitor	Power Regulation (SCH Sheet 3) - ODU Power
C63		Capacitor	Power Regulation (SCH Sheet 3) - ODU Power
C402		Capacitor	Power Regulation (SCH Sheet 3) - ODU Power
U8	081-399558-001	IC, -48V/2.5A HOT SWAP CNTRLR	Power Regulation (SCH Sheet 3) - ODU Power
R14		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R44		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R45		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
R46		Resistor	Power Regulation (SCH Sheet 3) - ODU Power
Q2	078-396196-001	XSTR FET N-CH IRF540NS, D2PAK	Power Regulation (SCH Sheet 3) - ODU Power