AN/GRC-262 Non-Proprietary FIPS 140-2 Cryptographic Module Security Policy

Hardware Version AN/GRC-262(V)1
Firmware Version 1.13.10.1356

Ultra Electronics TCS Inc.
5990 Côte-de-Liesse
Montréal, Québec, Canada
H4T 1V7

MODIFICATION TABLE		
Revision	**Description**	**Date** (YYYY-MM-DD)
-	Initial Release	2021-04-21
A	Update after laboratory review	2021-05-07
B	Added details about the Operational Environment	2021-05-19
C	Added FW build number and Certificate numbers	2021-06-18
D	Updated section 7.1 to add the 3rd tamper evident seal Updated guidance in section 12.3 Maintenance	2021-08-05
E	Added description of Access Methods in section 6.2, Updated reset and zeroize definitions on Table 3, Added information on NIST SP 800-90B in section 9, Corrected SHA -> SHS, Added details for status, zeroization, NIU use and other small fixes.	2021-08-30
F	Fixed typographic and spelling errors.	2021-09-02
G	Update after CMVP review.	2022-04-21
H	Update after CMVP review #2.	2022-05-25
I	Update after CMVP review #3.	2022-07-19
J	Update after CMVP review #4.	2022-09-01
K	Update to add changes for FIPS 140-2 1SUB	2023-03-14

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 SCOPE

The purpose of this Non-Proprietary Security Policy is to describe to individuals and organizations the capabilities, protection, and access rights provided by the AN/GRC-262 radio, thereby allowing an assessment of whether the AN/GRC-262 radio will adequately serve the individual or organizational security requirements.

2 REFERENCE DOCUMENTS

FIPS 140-2 Security Requirements for Cryptographic Modules[1]

5090-1010 – AN/GRC-262 FIPS Operation Guide

3 ACRONYMS AND DEFINITIONS

3.1 Acronyms

AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
Bps	Bits per second
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCCS	Canadian Centre for Cyber Security
CLI	Command Line Interface
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSP	Critical Security Parameters
DC	Direct Current
DRBG	Deterministic Random Bit Generator
ECC	Elliptic Curve Cryptography
EDC	Error Detection Code
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference

[1] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf

ETH	Ethernet
FIPS	Federal Information Processing Standards
GND	Ground
GPS	Global Positioning System
HMAC	Hash-Based Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
IP	Internet Protocol
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
NIST	National Institute of Standards and Technology
PKCS	Public Key Cryptography Standard
PMP	Point to Multipoint
PTP	Point to Point
PWR	Power
RF	Radio Frequency
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SNMPv3	Simple Network Management Protocol Version 3
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VLAN	Virtual Local Area Network
WebGUI	Web-based Graphical User Interface

4 INTRODUCTION

The AN/GRC-262 radio is manufactured by Ultra Electronics TCS Inc., operating as Ultra Communications. It is a multiband, point-to-point (PTP), point-to-multipoint (PMP) and Mesh radio system capable of providing at-the-halt communications across multiple echelons and on-the-move access capability. The system offers up to 1Gbps throughput and operational flexibility in a compact form factor. This document is the Non-Proprietary Security Policy for the AN/GRC-262 radio, hereafter denoted as the "Module" or AN/GRC-262.

4.1 Security Level

The AN/GRC-262 radio meets the FIPS 140-2 Level 2 requirement as detailed in the table below.

Table 1 Security Level per FIPS 140-2 Section

Security Requirements	*Level*
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles and Services and Authentication	2
Finite State Machine Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A
Overall Level of Certification	2

4.2 Background

More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website[2], which is maintained by the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS).

[2] https://csrc.nist.gov/projects/cryptographic-module-validation-program

5 CRYPTOGRAPHIC MODULE SPECIFICATION

5.1 Identification

The Module is marketed as the X500-G01 Radio.

The Module's hardware designation and version is AN/GRC-262(V)1. The identification label is located as shown in Figure 1 and Figure 2 which includes the Module's part number 100-817451-022.

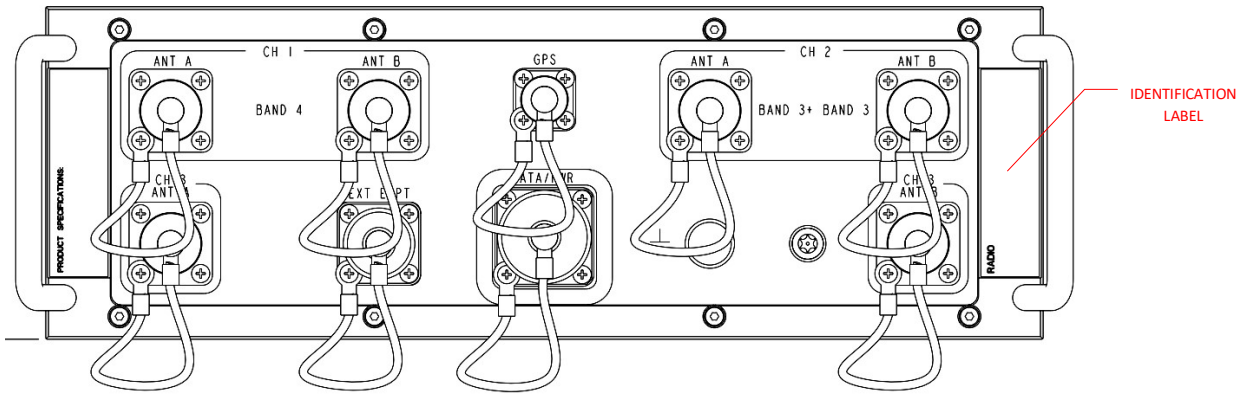


Figure 1 – Identification Label

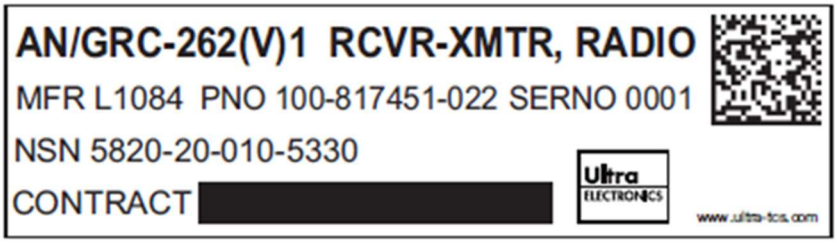


Figure 2 – Label Detail

5.2 Firmware and Mode of Operation

The Module runs Ultra Communications' firmware version 1.13.10.1356. The firmware always operates in the FIPS Approved mode. The firmware installation image is identified by the code 169-817312-01356.zip and the firmware status service in the GUI identifies itself as shown in Figure 3. The Module includes a firmware upgrade service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP.

Any other hardware or firmware version not listed in this Security Policy is out of the scope of this FIPS 140-2 validation.

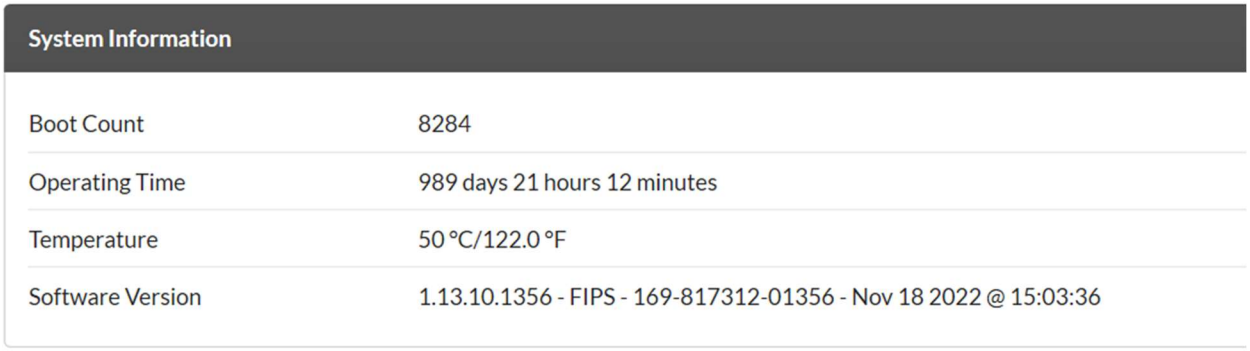


Figure 3 – Firmware Version Identification

5.3 Distinguishing Features

The module is distinguished by its solid aluminum alloy housing with heat dissipation fins integrated to four sides and a total of six antenna ports located on the front panel (two of them not functional in this model) as shown in Figure 4 and Figure 5 below.

The module may be connected to the optional Network Interface Unit (NIU) via the DATA/PWR interface. The NIU is commonly used to extend the module's network functionalities and provide limited control input (zeroize) and status output (alarm status).

5.4 Cryptographic Boundary

The AN/GRC-262 radio is a multi-chip standalone hardware cryptographic module, as defined in Section 4.5 of FIPS PUB 140-2.

The cryptographic boundary of the Module is defined by its aluminum alloy housing which physically encloses the complete set of hardware and firmware components of the Module.

The cryptographic boundary does not include the connector protective caps. These do not perform any security function and can be replaced without compromising the cryptographic boundary of the Module.

The physical form of the Module is depicted in Figure 4 and Figure 5 below.

Figure 4 – AN/GRC-262 (Top-Front view)

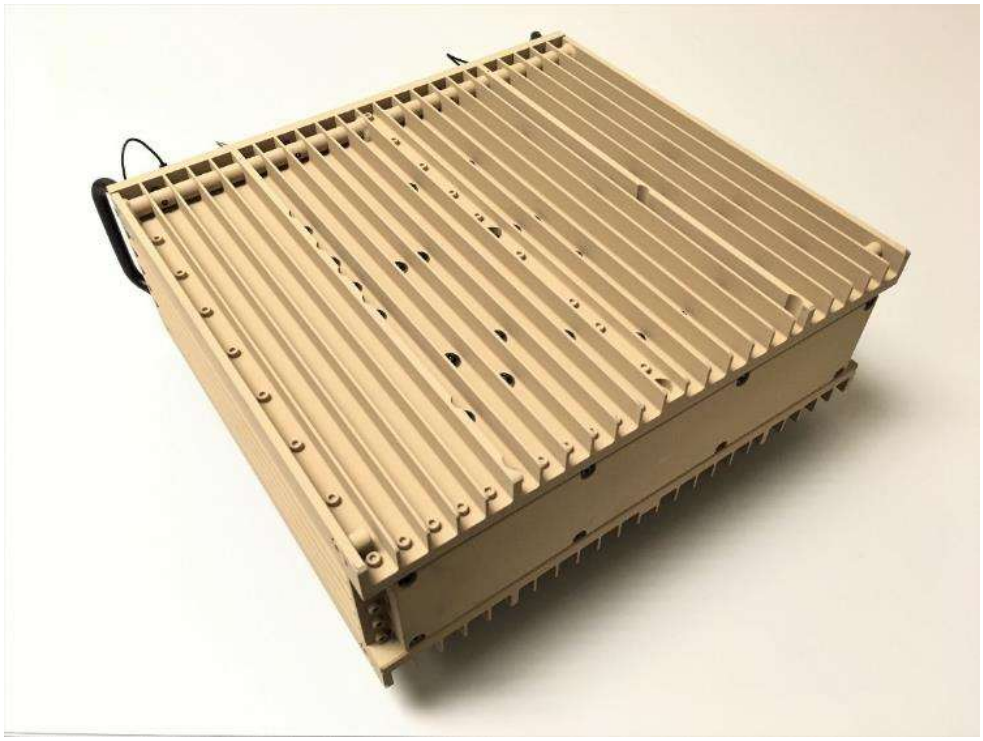


Figure 5 – AN/GRC-262 (Bottom-Back view)

5.5 Module Ports and Interfaces

The location of the physical ports is shown in Figure 6.

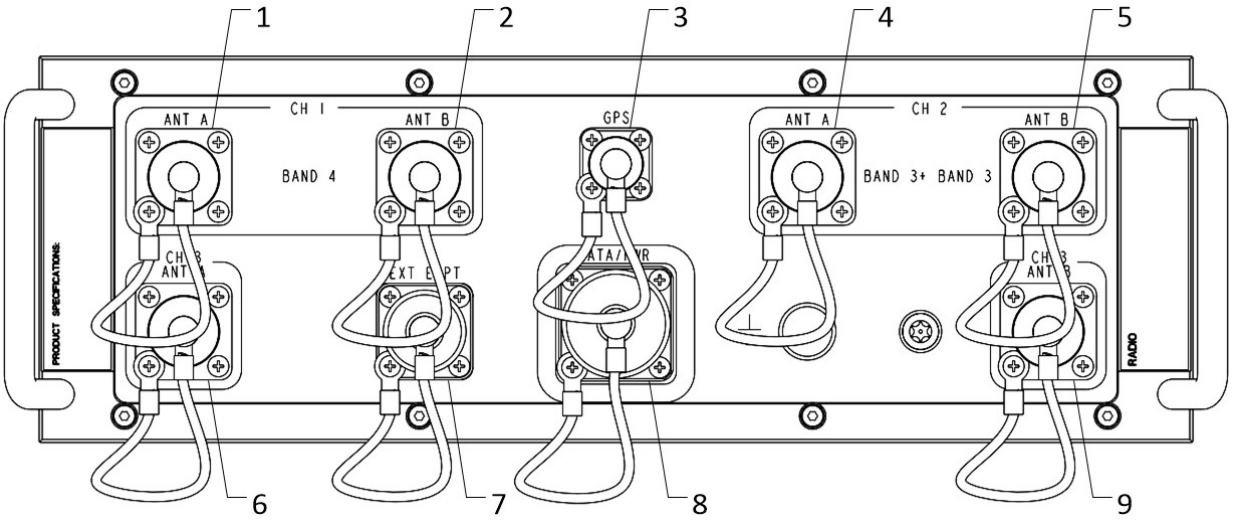


Figure 6 – FIPS 140-2 Location of Physical Ports

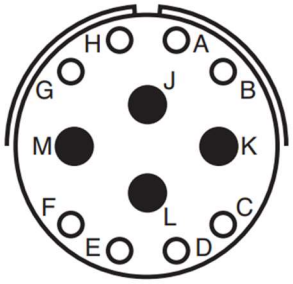
The module's physical ports and associated FIPS 140-2 logical interfaces are listed in Table 2.

Table 2 – FIPS 140-2 Logical Interfaces

#	Module Label	Physical Port	FIPS 140-2 Logical Interface
1	CH1 Band 4 ANT A	Band 4 RF antenna port	Data Input; Data Output; Control Input; Status Output
2	CH1 Band 4 ANT B	Band 4 RF antenna port	Data Input; Data Output; Control Input; Status Output
3	GPS	Non-functional	Not applicable
4	CH2 Band 3+ ANT A	Band 3+ RF antenna port	Data Input; Data Output; Control Input; Status Output
5	CH2 Band 3 ANT B	Band 3 RF antenna port	Data Input; Data Output; Control Input; Status Output
6	CH3 ANT A	Non-functional	Not applicable
7	EXT EQPT	Serial RS-232 (Pins A to C)	Control Input; Status Output

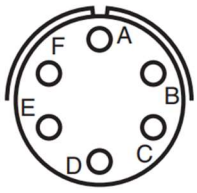
		Ext GPS (serial) Pins (E, F)	Control Input
		Reset Dongle (Pin D)	Control Input
8	DATA/PWR	Gigabit Ethernet LAN (Pins A to H)	Data Input; Data Output; Control Input; Status Output
		Input DC power supply (Pins J to M)	Power
9	CH3 ANT B	Non-functional	Not applicable

The pin-out of the DATA / PWR port is illustrated in the Figure 7 and the pin-out of the EXT EQPT port is illustrated in Figure 8



Pin	Signal Name
K	Chassis GND
L	DC Power -
J	DC Power +
M	Radio Det N
A	ETH1 MX1 P
B	ETH1 MX1 N
G	ETH1 MX2 P
H	ETH1 MX2 N
C	ETH1 MX3 P
D	ETH1 MX3 N
E	ETH1 MX4 P
F	ETH1 MX4 N

Figure 7 – Pin-out of the DATA / PWR port



Pin	Signal Name
A	TXD 1
B	RXD 1
C	GND
F	Ext GPS 1PPS
E	Ext GPS 10 MHz
D	Ext Trigger

Figure 8 – Pin-out of the EXT EQPT port

6 ROLES, AUTHENTICATION AND SERVICES

6.1 Roles

The AN/GRC-262 radio supports role-based authentication. There are three roles in the AN/GRC-262 radio that operators may assume:

- Admin Role, equivalent to the FIPS 140-2 Crypto Officer (CO) Role,
- Operator Role, equivalent to the FIPS 140-2 User Role, and
- Monitor Role, which has read only access to all data, including non-security critical data.

The AN/GRC-262 allows multiple concurrent users. Up to 10 operators may be logged concurrently on the AN/GRC-262.

The Module does not support a Maintenance Role as per FIPS 140-2 definition.

Table 3 – Roles and required identification and authentication.

FIPS 140-2 Role	System Profile	User Interface	Type of Authentication	Authentication Data
Crypto Officer	Admin/root	HTTPS/ CLI (serial)	role-based	password
User	Operator	HTTPS	role-based	password
User	Monitor	HTTPS	role-based	password

6.2 Access Methods

The Web-based Graphical User Interface (WebGUI) is the user interface designed for configuration, operation and monitoring of the Module using the Hypertext Transfer Protocol Secure (HTTPS) for secure communication protocol. By default, the WebGUI is accessed through the ethernet interface on the DATA/PWR port. The module also supports remote access, which is disabled by default, through any of the RF Antenna ports. Configuration of the management parameters is part of the service “Configure System”.

The Command Line Interface (CLI) is accessed through the serial port. The CLI is intended for debugging functions only and therefore not documented.

6.3 Authentication

The AN/GRC-262 radio supports role-based authentication. The module employs the following authentication methods to authenticate Crypto Officers and Users. Passwords are used for authenticating all users and roles with the AN/GRC-262 radio.

Table 4 – Authentication Strength

Authentication Mechanism	Strength of Mechanism
Username/ Password	The minimum password length is 15 characters. The maximum password length is 30 characters. The minimum password length cannot be changed. Allowed characters: • 26 lowercase letters: a-z, • 26 uppercase letters: A-Z, • 10 decimal numerals: 0-9 and, • 32 non-alphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/ The character set contains 94 characters. The password strength is 1 in 94^15 = 3.95 x 10^29

Table 5 – Timeout Mechanism

Access Method	Timeout Mechanism
WebGUI (HTTPS)	The Module imposes a 3 second timeout between authentication attempts limiting the total attempts possible to 20 per minute. The authentication of a known user is locked for 15 minutes after 3 consecutive failed attempts for that user. If the Module reboots due to a power cycle the 15-minute lockdown is reset and new authentication attempts may be possible after the 60 to 70 seconds required for the Module to finish the booting sequence. The probability for a successful attempt in a one-minute period is 3 in 94^15.
CLI (serial)	The Module imposes a 3 second timeout between authentication attempts limiting the total attempts possible to 20 per minute. The probability for a successful attempt in a one-minute period is 20 in 94^15.

6.4 Services

Table 6 – Services

Service	Approved Security Function(s)	Description	CSPs	Input	Output	Admin	Operator	Monitor
Access						**Type of Access**		
HTTPS Key Agreement	KAS ECC SSC [SP 800-56Arev3], AES, RSA, SHS, CVL (TLS 1.2), DRBG	Used to establish keys for setting up a secure communication tunnel (TLS 1.2)	TLS session key, TLS session authentication key, RSA public key, RSA Private key, ECDH Public Param, ECDH Private parameter, TLS pre-Master secret, TLS Master secret	TLS Client key exchange	TLS server key exchange	E	E	E
Authentication (Login)		Used to log in to the module	Admin (CO) password, Operator (User) password, Monitor (User) password	Username and password commands	Login Command response	E	E	E
Logout		Logout of the module	None	Logout Commands and parameters	Logout Command response	E	E	E
Configuration								
Enable Encryption (Exit-bypass)	HMAC	Allows to configure an RF interface with an encrypted VLAN	Configuration HMAC Integrity Key	Commands and parameters	Command response	E	E	N
Disable Encryption (Bypass)	HMAC	Allows to configure the RF interface with a non-encrypted VLAN	Configuration HMAC Integrity Key	Commands and parameters	Command response	E	E	N
Configure Keys for traffic data encryption	AES	Allows to configure the keys	AES Key per VLAN , HMAC key per VLAN	Configure Command and parameters	Configure Command response	W	N	N
Configure SNMPv3	CVL (SNMP), AES, SHS	Allows to configure SNMPv3 privacy and authentication password	SNMPv3 Authentication password, SNMPv3 Privacy password	Configure Command and parameters	Configure Command response	W	N	N

Configure User Role		Allows to configure, add, and delete Operator, Monitor password	Operator (User) password, Monitor (User) password	Configure Command and parameters	Configure Command response	W	N	N
Configure System		Allows to configure the system, IP address, management, and RF settings	None	Configure Command and parameters	Configure Command response	W	W	N
Backup Configuration	HMAC	Allows to backup and export a signed radio configuration package from the module	FW Load HMAC Integrity Key	Module current radio configuration parameters[3]	Signed radio Configuration package and Command response	E	N	N
Restore Configuration	HMAC	Allows to import and restore a signed radio configuration package in the module	FW Load HMAC Integrity Key	Module Signed radio configuration package	Command response	E	N	N
Monitoring								
Get state of encryption on RF interfaces		Allows to view the configuration of the encrypted or non-encrypted VLAN on an RF interface	None	State Command and parameters	State of encryption Command response	R	R	R
System Status		Allows to view the system, Ethernet, and RF statistics	None	Command and parameters	Status Command response	R	R	R
System Log		Allows to view the system log	None	Command and parameters	Log command response	R	R	R
General information		Allows to view the general system identification and configuration	None	Command and parameters	General information command response	R	R	R
NIU LED indicator		If the NIU is in use, the LED labeled “Radio LED” indicates the alarm status of the module. Green means the module is powered and there are no alarms active. Red means there is an alarm active. The user must use the WebGUI to analyze the source of the alarm.	None	None	Alarm status	R	R	R
Services								

[3] Except CSP (critical security parameters, authentication, privacy, and secrets) used by the module.

Data Encryption / Decryption	AES	Encrypt/Decrypt data traffic on VLAN network and RF interface	AES Key per VLAN , HMAC key per VLAN	Traffic plaintext / encrypted	Traffic encrypted / plaintext	E	E	E
Upload Firmware	HMAC	Allows to upload new validated firmware	FW Load HMAC Integrity Key	Signed Firmware file	Command response	W, E	W, E	N
Change Password		Allows to modify the CO and the User passwords	CO password, Operator password, Monitor password	Password Command and parameters	Command response	W, E	N	N
Reset settings to default (Zeroize) – zeroize non-volatile CSPs		Allows to zeroize all keys and CSPs. All Keys and CSPs will be cleared, and all settings will be reset to factory default.	All keys and CSPs[4]	Command and parameters	Command response	W, E	W, E	N
NIU Push-button Zeroize – zeroize non-volatile CSPs		If the NIU is in use, pressing the button on the back of the unit for 10 seconds allows the function "Reset settings to default" to be executed.	All keys and CSPs	Command and parameters	Command response	W, E	W, E	W, E
Perform self-tests	AES, HMAC, SHS, KAS ECC SSC[SP 800-56A rev3], CVL (SNMP), CVL(TLS 1.2), DRBG [SP 800-90A]	Allows to perform on-demand self-tests (Reboot)	None	Reboot commands	Reboot Commands response	E	E	N
Reboot – zeroize volatile CSPs in memory		Allows to reboot the radio	None	Reboot commands	Reboot Commands response	E	E	N
SNMP								
SNMPv3 access to MIB data and information	CVL (SNMP), AES, SHS	Allows to access Mibs data	SNMPv3 Authentication password, SNMPv3 Privacy password	SNMPv3 command and parameters	SNMP Command response	R, W	R, W	R

Type of Access Legend

R = Output data access is allowed by the module.

W = Input data access is allowed by the module.

E = Execution access of the service is allowed by the module.

N = No access.

[4] Except for factory embedded RSA Public/private Keys, FW Integrity Key and Configuration Integrity Key.

Except for the services listed below no other services can be performed or accessed by an unauthenticated user:

- NIU LED indicator,
- NIU Push-button Zeroize,
- Reboot (by physically cycling the power),
- Perform self-tests (as part of the reboot process).

6.5 SNMPv3

The SNMPv3 users share the same system roles (admin, operator, monitor) as for the HTTPS user interface but they are not the same user account authentication. The module firmware has been designed to prevent the ability to read or write critical security parameters (CSPs) through the SNMPv3 interface.

Only the Crypto Officer can enable the SNMPv3 service and configure the passphrases used for authentication and privacy. The passphrases shall be composed by a minimum 15 up to 64 non-repetitive mixed alphanumeric characters [A-Z a-z 0-9].

6.6 Bypass Capability

The cryptographic module supports alternate permanent bypass capability by being able to simultaneously provide services with cryptographic processing and services without cryptographic processing. The operator may assign multiple encrypted or non-encrypted VLANs per Waveform.

The bypass capability is defined as when the operator sets any Waveform from an encrypted VLAN to a non-encrypted VLAN. A confirmation action will be required from the operator. Furthermore, a bypass alarm will remain active to inform the operator which waveform is set to accept unencrypted VLANs, regardless of the administrative status of the Waveform.

The exit-bypass condition is defined as when the operator switches all Waveforms from non-encrypted VLANs to encrypted VLANs.

7 PHYSICAL SECURITY

The module is enclosed in a production-grade weatherproof aluminum alloy case that is opaque within the visible spectrum, which defines the cryptographic boundary of the module. There are no openings (slits and/or holes) in the casing to give any visual or physical access to internal components.

7.1 Tamper evident seals

The module's enclosure is sealed using three (3) tamper evident seals, which prevent the enclosure from being opened without signs of tampering.

The tamper evident seals shall be properly installed for the module to operate in the approved mode of operation.

The part number for ordering the tamper evident seal is 612-990309-088.

7.1.1 Storage

The Crypto Officer is responsible for securing and having control at all times of any unused tamper evidence seals.

Store at a maximum temperature of 90° F or 32° C, with relative humidity at 35% to 90%. The shelf life is a minimum of 1 year. Cooler temperatures extend the shelf life.

7.1.2 Application

If the tamper evidence seals have not been pre-installed in factory, the Crypto Officer is responsible for the application of tamper evidence seals.

The tamper evidence seals should be applied in a clean environment.

Observe views of the module in Figure 9, Figure 10 and Figure 11 to select the location to which the seals shall be applied.

The surface temperature must be a minimum of 35° F or 2° C.

The surface must be clean and dry. Clean the surface using 90% isopropyl alcohol and a clean paper towel. After cleaning, use another clean paper towel to dry the surface. Do not allow the alcohol to air dry as contaminants may remain on the surface.

Peel back a portion of the liner (backer) to expose a portion of the adhesive side of the label. Affix the exposed portion of the adhesive to the intended surface, then peel away the balance of the liner to fully affix the label making sure that no bubbles or wrinkles are formed. The label will indicate tampering if removed immediately.

7.1.3 Verification

The location of the three (3) tamper-evident seals is indicated in Figure 9, Figure 10 and Figure 11.

The Crypto Officer is responsible for periodic verification that installed seals have not been removed or damaged.

It is the responsibility of the user (Operator) - during deployment or repositioning of the module - to ensure that the tamper evident seals were not removed or damaged to be certain that the security of the module is maintained, and the module is ready to operate in the FIPS approved state. If the Module shows any signs of tampering the Module shall not be put in operation and the Crypto Officer must be notified immediately.

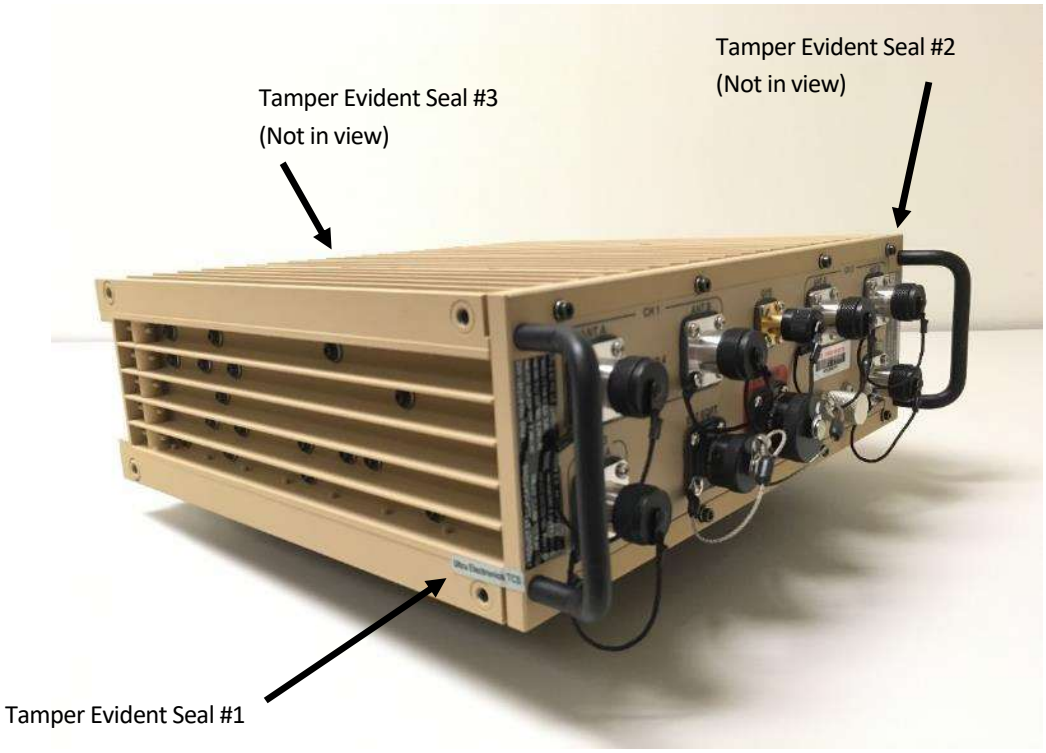


Figure 9 – Tamper-Evident Seal #1

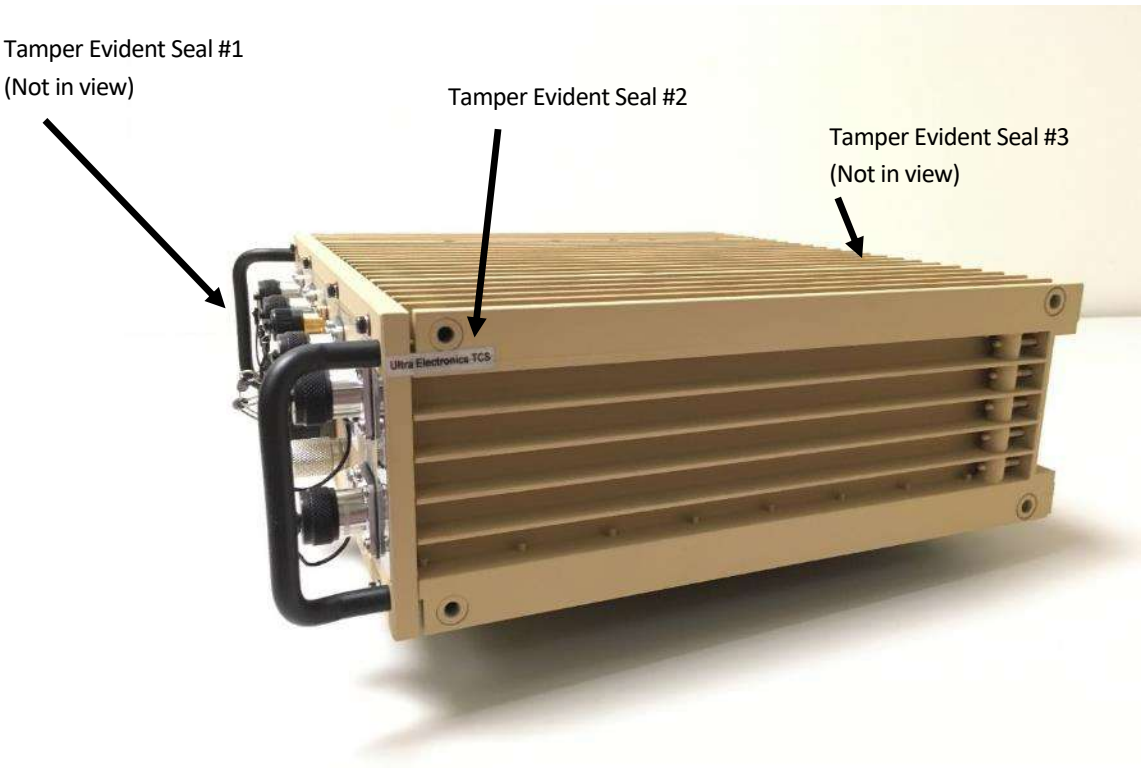


Figure 10 – Tamper Evident Seal #2

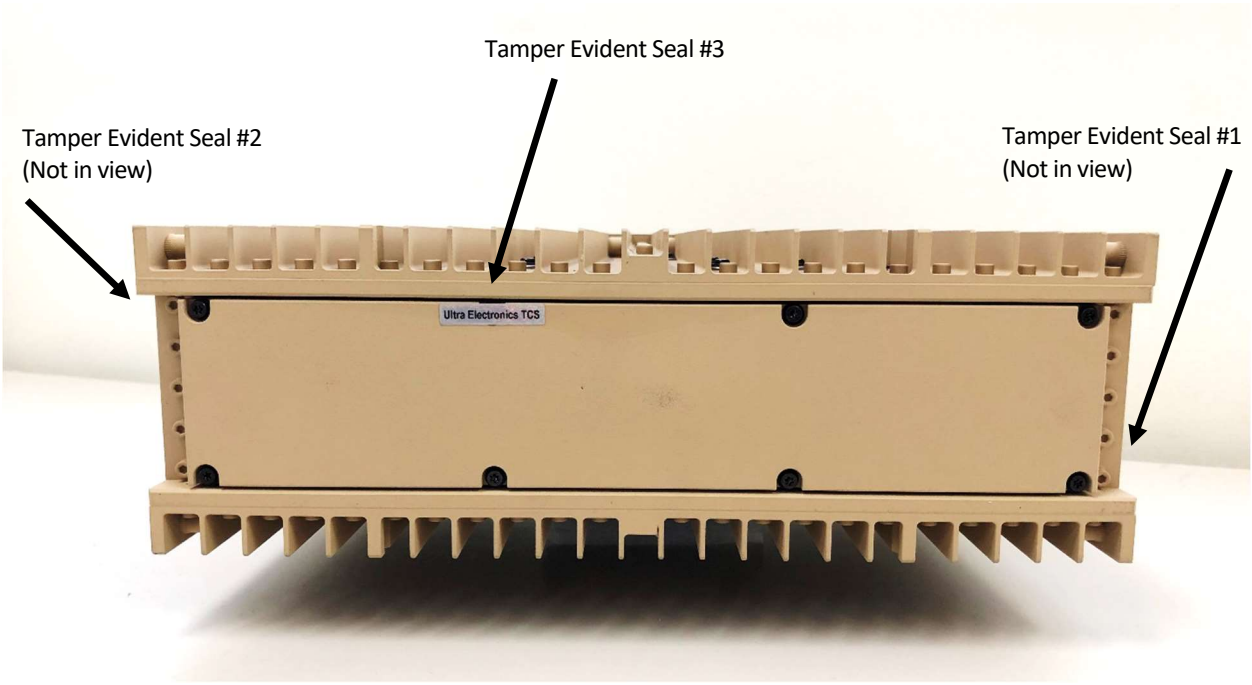


Figure 11 – Tamper Evident Seal #3

8 OPERATIONAL ENVIRONMENT

The Module is designated as a non-modifiable operational environment under the FIPS 140-2 definitions; therefore, the FIPS 140-2 Operational Environment requirements are not applicable.

The operational environment for each of the Approved Cryptographic Algorithms is described in Table 7.

Table 7 – Operational Environment

Approved Cryptographic Algorithm	Firmware Version	Processor	Implementation Description
AN/GRC-262 – WolfSSL	WolfSSL 4.7.0 commercial FIPS	Freescale QorIQ P2020-Power PC	WolfSSL is a library which provides encryption and authentication services for HTTPS, SNMP and for digital signature within the AN/GRC-262 radio.
AN/GRC-262 – *Freescale QorIQ P2020*	Freescale QorIQ P2020 - Security - SEC3.3	Freescale QorIQ P2020-P2020NXE2MHC	The Freescale *QorIQ P2020 hardware accelerator provides encryption and authentication services for data traffic within the AN/GRC-262 radio.*
AN/GRC-262 – Linux Kernel Crypto	Linux Kernel Crypto 3.12.19	Freescale QorIQ P2020-Power PC	The Linux kernel Crypto provides hash algorithm services for entropy source conditioning component within the AN/GRC-262 radio.

9 CRYPTOGRAPHIC KEY MANAGEMENT

The product supports the following FIPS-approved cryptographic algorithms. The algorithms are listed below, along with their corresponding CAVP certificate numbers.

Table 8 – FIPS Approved Cryptographic Algorithms

Approved Cryptographic Algorithm		Mode and Description	Certificate Number	Use
AN/GRC-262 – WolfSSL (WolfSSL 4.7.0 commercial FIPS)	AES	AES Mode: CBC (128, 256 bits), GCM (128, 256 bits)[5], CFB128	A1493	Data Encryption / Decryption
	RSA	Signature authentication (Sign and verify 2048 modulo), PKCS	A1493	Digital Signature Generation / Digital Signature Verification
	SHS	SHA-1, SHA-256, SHA-384	A1493	Message Digest
	HMAC	Message Authentication with SHA-1, SHA256, SHA384	A1493	Message Authentication
	CVL (TLS 1.2)	TLS 1.2 KDF with SHA-256/SHA384 [SP 800-135rev1]	A1493	Key Derivation
	CVL (SNMP)	SNMP KDF with SHA-1 [SP 800-135rev1]	A1493	SNMP Authentication/ Privacy Key Derivation
	KAS ECC SSC[SP 800-56A rev3]	ECC CDH (curve P-256)[6]	A1493	Shared Secret Computation
	DRBG [SP 800-90A]	Pseudo Random bit generation (HASH DRBG, SHA-256)[7]	A1493	Deterministic Random Bit Generation

[5] AES GCM is only used as part of TLS 1.2 GCM cipher suites. Adherence to [140IG] A.5 Key/IV Pair Uniqueness Requirements from SP 800-38D, the module complies to A.5 1 (a), tested per option (ii) under A.5 TLS protocol IV generation. The module supports internal IV generation for TLS 1.2 protocol with the approved the Hash DRBG. **T**he counter portion of the IV is set by the module within its cryptographic boundary. Per RFC 5246, when the nonce explicit part of the IV exhausts the maximum number of possible values for a given session key, the module will trigger a handshake to establish a new encryption key.

[6] Security strength 128-bits for ECC key Pair P-256, use for TLS Key agreement scheme. The module claimed compliance to IG. D8 scenario X1. path (1) as annotated KAS-ECC-SSC in the module's validation certificate A1493. The module perform KAT for shared secret Z computation verification for ECC curve P-256 as per SP800-56A rev3

[7] This cryptographic module has been validated for compliance with NIST SP 800-90B. Based on noise source testing and analysis, the estimated minimum amount of entropy per the source output bit is 0.9 bits. The overall amount of generated entropy meets the required security strength of 256 bits based on the entropy per bit and amount of entropy requested by the module.

Approved Cryptographic Algorithm		Mode and Description	Certificate Number	Use
AN/GRC-262 – Freescale QorIQ P2020 (Freescale QorIQ P2020 - Security - SEC3.3)	AES	Symmetric Key AES 128, 256 in CBC	A1494	Data Encryption / Decryption
	HMAC	Message authentication using SHA-1	A1494	Message Authentication
	SHS	Secure HASH using SHA-1	A1494	Message Digest
AN/GRC-262 – Linux Kernel Crypto (Linux Kernel Crypto 3.12.19)	SHS	Vetted conditioning component SHA-1	A1495	Vetted conditioner
ENT (NP)		Entropy source(s) tested to SP 800-90B	Not required	Seeding for FIPS-Approved DRBG

As per IG A.5, the module supports the following AES GCM cipher suites for TLS 1.2 from section 3.3.1 of SP 800-52 rev2: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384.

For TLS and SNMP no parts of the protocol, other than the KDF from SP 800-135rev1, have been tested by the CAVP and CMVP.

SHA-1 is used as underlying function to HMAC-SHA1 for message authentication with AN/GRC-262 WolfSSL and AN/GRC-262 Freescale QorIQ P2020 and not used to generate signature in the module.

SHA-1 is used in the vetted conditioner component with AN/GRC-262 – Linux Kernel Crypto.

The module is always in "approved mode" using the above cryptographic algorithms.

The AN/GRC-262 radio supports the following Critical Security Parameters (CSPs):

Table 9 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

General Keys							
Key/CSP	**Key Type**	**Generation / Input**	**Output**	**Storage**	**Zeroization**	**Service/Use**	**Access Rights**
Password							

General Keys							
Key/CSP	**Key Type**	**Generation / Input**	**Output**	**Storage**	**Zeroization**	**Service/Use**	**Access Rights**
Admin (CO) password	ASCII string	Entered in undisclosed plaintext	No output	Plaintext in non-volatile memory	when zeroize, reset to factory settings	Authentication for CO login	W, Z
Operator (User) password	ASCII string	Entered in undisclosed plaintext	No output	Plaintext in non-volatile memory	when zeroize, reset and clear	Authentication for User login	W, Z
Monitor (User) password	ASCII string	Entered in undisclosed plaintext	No output	Plaintext in non-volatile memory	when zeroize, reset and clear	Authentication for Read-Only login	W, Z
Data Encryption							
AES Key per VLAN	AES CBC (128, 256 bits key)	Entered in undisclosed plaintext then encrypted (using TLS session key)	No output	Plaintext in non-volatile memory	when zeroize, reset and clear	Configure Keys for traffic data encryption	W, E, Z
HMAC key per VLAN	HMAC-SHA1 (160 bit)	Entered in undisclosed plaintext then encrypted (using TLS session key)	No output	Plaintext in non-volatile memory	when zeroize, reset and clear	Configure Hashing Keys for traffic data encryption	W, E, Z
SSL/Cryptographic FIPS Library (WolfSSL)							

General Keys							
Key/CSP	**Key Type**	**Generation / Input**	**Output**	**Storage**	**Zeroization**	**Service/Use**	**Access Rights**
TLS Session Key	AES (128, 256 bits key)	Internally generated and derived using TLS protocol	No output	Plaintext in volatile memory	Power cycle, reboot or HTTPS session termination	Data encryption for TLS sessions	G, E, Z
TLS Session Authentication Key	HMAC-SHA1, HMAC-SHA256	Internally generated and derived using TLS protocol	No output	Plaintext in volatile memory	Power cycle, reboot, or HTTPS session termination	Data authentication for TLS sessions	G, E, Z
RSA Private key	RSA 2048 bits	Generated outside module and embedded in FW image	No output	Plaintext in non-volatile memory	no	For RSA signature generation and TLS RSA key wrap operations	W, E
RSA Public key (TLS Certificate)	RSA 2048 bits	Generated outside module and embedded in FW image	Only to client in TLS encrypted web session	Plaintext in non-volatile memory	no	Identity certificate and to verify RSA signatures and TLS RSA key wrap operations	W, R, E
FW Load HMAC Integrity Key	HMAC-SHA256 (256 bits)	Factory generated and internally embedded in FW image	No output	embedded in non-volatile memory	no	To authenticate firmware load integrity and to authenticate radio configuration backup and restore.	W, E

General Keys							
Key/CSP	**Key Type**	**Generation / Input**	**Output**	**Storage**	**Zeroization**	**Service/Use**	**Access Rights**
Configuration HMAC Integrity Key	HMAC-SHA256 (256 bits)	Factory generated and internally embedded in FW image	No output	embedded in non-volatile memory	no	To authenticate configuration and bypass mechanism switch integrity	W, E
ECDH public param	P 256 EC Diffie-Hellman public parameters	Internally Generated	No output	Plaintext in volatile memory	Power cycle, reboot or HTTPS session termination	For Key agreement session to establish TLS Pre-Master	G, E, Z
ECDH private param	P 256 EC Diffie-Hellman local parameters	Internally Generated	No output	Plaintext in volatile memory	Power cycle, reboot or HTTPS session termination	For Key agreement session to establish TLS Pre-Master	G, E, Z
TLS Pre-master Secret	48-byte size value	Internally established by ECDH Key agreement	No output	Plaintext in volatile memory	Power cycle or HTTPS session termination	Used to derive the TLS Master Secret and session keys	G, E, Z
TLS Master Secret	48-byte size value	Internally established using SP 800-135 KDF TLS 1.2	No output	Plaintext in volatile memory	Power cycle or HTTPS session termination	Used in TLS connections to derive the session keys	G, E, Z
SNMPv3							

General Keys							
Key/CSP	**Key Type**	**Generation / Input**	**Output**	**Storage**	**Zeroization**	**Service/Use**	**Access Rights**
SNMPv3 privacy password	ASCII string	Entered in undisclosed plaintext then encrypted (using TLS session key)	No output	Plaintext in non-volatile memory	when zeroize, reset and clear immediately after use	The derived key provides secured channel for SNMPv3 management	W, E, Z
SNMPv3 Authentication password	ASCII string	Entered in undisclosed plaintext then encrypted (using TLS session key)	No output	Plaintext in non-volatile memory	when zeroize, reset and clear immediately after use	The derived key provides secured authentication for SNMPv3 management	W, E, Z
RNG Keys/CSPs							
DRBG entropy input string	196-byte value	Internally generated from entropy source (Ultra Communications RNG)	No output	Plaintext in volatile memory	when zeroize, reset and clear immediately after use	Entropy source used to construct seed used by the DRBG	G, E, Z
DRBG C Value	55-byte value	Internally Generated	No output	Plaintext in volatile memory	when zeroize, reset and clear immediately after use	Constant C used for SP 800-90A HASH_DRBG	G, E, Z
DRBG V Value	55-byte value	Internally Generated	No output	Plaintext in volatile memory	when zeroize, reset and clear immediately after use	Value V internally for SP 800-90A HASH_DRBG	G, E, Z

Access Rights Legend

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, embedded at factory, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroize: The module zeroizes the SSP.

10 EMI/EMC

The AN/GRC-262 radio was tested and found to be conformant to the Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC) requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (i.e., for business use).

Compliance with these regulations meets FIPS Level 2 requirements for EMI/EMC.

11 SELF-TEST

POST (Power on Self Tests) is performed on each boot and conditional self-tests during operations to prevent any secure data from being released and to ensure all components are functioning correctly.

If any of the self-tests fail, the module enters a "error state" where actions are taken to secure sensitive data. An error message is logged in the module System Log, a service status is show for the Crypto Officer through the WebGUI for review.

To clear the error state, the following actions can be taken according to the user type of access: Reboot the unit, zeroize the unit and/or re-upload the firmware.

The Crypto Officer or Operator may initiate on demand self-tests by rebooting the module. To confirm the successful execution of the self-test the Crypto Officer shall review the entries contained in the module's System Log.

11.1.1 Power-Up Self-Test

During the boot process, the AN/GRC-262 radio executes a Known Answer Test (KAT) for different algorithms. Using KAT, a cryptographic algorithm is run on data for which the correct output is already known, and then the calculated output is compared to the previously generated output. If the calculated output does not equal the known answer, the known-answer test fails.

The detail of the power-on self-tests for SSL/Cryptographic FIPS library (WolfSSL) are given in Table 10.

Table 10 – Self-Tests for WolfSSL

Algorithm	Type	Test Attributes
AES CFB	KAT	Separate encrypt and decrypt, CFB mode
AES CBC	KAT	Separate encrypt and decrypt, CBC mode
AES GCM	KAT	Separate encrypt and decrypt, GCM mode
RSA	KAT	Sign and verify using 2048 bit key
SHS	KAT	SHA-1, SHA-256, SHA-384, SHA-512
HMAC	KAT	HMAC-SHA1, HMAC-SHA256 and HMAC-SHA512
DRBG	KAT	[SP800-90A] Section 11.3 Instantiate, Generate, Reseed health tests for SHA-256 HASH_DRBG.
KAS ECC SSC	KAT	KAS ECC Shared Secret Computation (SP 800-56A rev3, ECC, P-256)
TLS 1.2 KDF	KAT	KDF with SHA-256/SHA-384
SNMP KDF	KAT	SMNP v3 KDF with SHA-1

Bypass test is also performed at boot-up see section 11.1.4 Bypass Tests below for details.

The power-on self-tests for the Freescale P2020-SEC3.3 Crypto Engine are given in Table 11.

Table 11 – Self-Tests for Freescale P2020

Algorithm	Type	Test Attributes
AES CBC	KAT	Separate encrypt and decrypt, CBC mode, 128, 256-bits key lengths
HMAC	KAT	HMAC with SHA-1
SHA-1	KAT	SHA-1 hash

The power-on self-test for Firmware integrity check is given in Table 12.

Table 12 – Self-Tests for Firmware Integrity Check

Algorithm	Type	Test Attributes
Firmware integrity	EDC	32-bit Error Detection Code (EDC) against firmware image

Table 12 – Self-Tests for Kernel Crypto

Algorithm	Type	Test Attributes
SHA-1	KAT	SHA-1 hash

11.1.2 Conditional Self-Test

The module performs the following conditional self-tests periodically or when called by the module.

SSL/Cryptographic FIPS Library Continuous DRBG Test

Continuous Random Number Generator test to verify that the output of approved-DRBG is not the same as the previously generated value for both DRBGs. This test is run when a random number is generated by application request.

Entropy Source Continuous Health Tests

The entropy source module continuously performs the SP800-90B health tests stuck test, Repetition Count Test (RCT) and Adaptative Proportion Test (APT) as per section 4.4 over at least 1024 consecutive samples.

Firmware Load test

When a new firmware upgrade is loaded into the AN/GRC-262 through the web interface, a HMAC-SHA-256 signature (with the embedded FW load HMAC integrity key) verification is done by the firmware. The signature is distributed as part of the firmware package. The firmware computes the signature of the newly received firmware and validates it against the signature contained in the firmware package. If the signature is the same, the firmware then accepts the new firmware and copies it into the non-volatile memory of the AN/GRC-262.

11.1.3 Critical Function Test

SSL/Cryptographic FIPS Library DRBG (HASH_DRBG) self-test as required by SP800-90A (Instantiate, Generate, Reseed and Un-instantiate) is performed as KAT when the module boot-up and when reseed.

The module entropy generator performs health tests as required by SP800-90B (stuck test, RCT and APT) at module start-up and continuously.

11.1.4 Bypass Tests

The AN/GRC-262 radio can alternate between a bypass service and a cryptographic service.

A bypass test is implemented to verify the correct operation of the cryptographic service configuration.

The bypass tests are performed to ensure that a single point of failure of module components will not result in the unintentional output of plaintext. The bypass test is executed at boot-up with the Configuration HMAC integrity (HMAC-SHA-256) check over the CSP stored in the configuration file and the result MAC is compared with the previous MAC value calculated when any CSP configuration including the bypass configuration changed. Each calculated MAC is stored in a non-volatile memory location. The test is intended to authenticate the AN/GRC-262 configuration and to assure the correct operation of the module services providing cryptographic or bypass processing. If the bypass test failed, it raised FIPS configuration alarm the system step into a soft error state and inhibit cryptographic and traffic operation. The operator must do a reset setting (a zeroized configuration) and reset the system to clear the error condition.

12 SECURITY RULES AND GUIDANCE

The AN/GRC-262 radio meets the Level 2 requirements for FIPS 140-2. The sections below describe how to place and keep the module in FIPS-approved mode of operation.

The Module does not support non-FIPS Mode of Operation.

12.1 Crypto Officer Guidance

The Crypto Officer is responsible for the initialization, configuration, and management of the Module. The Crypto Officer can receive the AN/GRC-262 radio from the vendor via trusted delivery courier including but not limited to DHL, UPS, and FedEx. The Crypto Officer can also arrange for pick up directly from Ultra Communications.

Upon receipt of the Module, the Crypto Officer should check the package for any irregular tears or openings. Upon opening the package, the Crypto Officer should inspect the tamper-evident labels. If there is suspicion of tampering, the Crypto Officer shall contact Ultra Communications immediately.

12.1.1 Secure Operation Initialization

The Crypto Officer is responsible for the initialization of the module through the Web Interface. The Crypto Officer must login to the module using the default username "CryptoOfficer" and password "password". Once the first authentication has been completed, the Crypto Officer is forced to create a new password respecting the password restrictions enforced by the Module as defined in section 6.3.

The following steps are required to enable the secure operation of the Module:

1. The Crypto Officer must change the default authentication password upon first-time login,
2. The Crypto Officer must verify that the installed firmware version number is listed in the certificate. Only a CMVP validated version is allowed to be used.
3. The Crypto Officer may choose to rename the default "CryptoOfficer" username (optional),
4. The Crypto Officer may choose to add users with Operator or Monitor profiles (optional). The Operator profile is equivalent to the User role per FIPS definitions,
5. The Crypto Officer must configure an encrypted VLAN by selecting the AES key length (128 or 256 bits) and entering the AES key.
6. The Crypto Officer may enable HMAC hashing mode and enter the hashing key (optional).
7. The Crypto Officer must assign one of the two previously configured encrypted VLANs to the wireless interface. By default, the wireless interfaces are in bypass mode.
8. The Crypto Officer must ensure that the module does not show any FIPS alarm.
9. The module is ready for configuration of non-security related parameters.

For additional initialization guidance, please reference the "AN/GRC-262V1 FIPS Operation Guide".

12.1.2 Management

The Crypto Officer can configure and monitor the Crypto Module via the secure WebGUI. The Crypto Officer should check the System Status and System Logs frequently for errors. If the Crypto Module ceases to function normally, then contact Ultra Communications customer support.

The Module's CLI port is intended for debugging and offers limited configuration options to the Crypto Officer. Module initialization, Cryptographic Key Management, Firmware Update, Bypass Capability and

User Management configuration options are NOT available via the CLI port. The Crypto Officer is not allowed to log in to the CLI before changing the default password through the WebGUI as described in section 12.1.1.

12.2 Operator Guidance

The Module's web-based interface and configuration options available to the Operator are a subset of the interface and configuration options available to the Crypto Officer. Refer to Section 12.1 for details.

The Operator has access to the same web-based interface and configuration options as the Crypto Officer, except for the following.

The Operator cannot:

- Perform any user management action such as add or delete users,
- Change user password,
- Add, modify, or delete any encryption keys,
- Enable, modify parameters, or disable SNMP,
- Enable, modify parameters, or disable NTP,
- Backup and restore configuration.

12.3 Maintenance

The internal components of the Module cannot be replaced on the field. In case of hardware malfunction or defect, the CO shall zeroize the unit whenever possible and send the Module to the maintenance facility for repair via a trusted delivery courier.

13 MITIGATION OF OTHER ATTACKS

The Module is not designed to mitigate other attacks.