RDL-3000 and eLTE-MT

FIPS 140-2 Non-Proprietary Security Policy

Hardware: RDL-3000, eLTE-MT – Firmware: v3.1

April, 2016

Prepared by:

Redline Communications
302 Town Centre Blvd., Markham
ON L3R 0E8, CANADA.
t +1.905.479.8344 | **f** +1.905.479.5331
rdlcom.com

Prepared for:

Redline Communications
302 Town Centre Blvd., Markham
ON L3R 0E8, CANADA.
t +1.905.479.8344 | **f** +1.905.479.5331
rdlcom.com

Table of Contents

Table of Figures

List of Tables

1.0 Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for Redline Communications RDL-3000, Elte-MT Broadband Wireless Systems (running firmware version 3.1). This Security Policy describes how the RDL-3000, Elte-MT Broadband Wireless Systems meet the National Institute of Standards and Technology (NIST) and the Communications Security Establishment (CSE) requirements for cryptographic modules as specified in Federal Information Processing Standards Publication (FIPS) 140-2. This document also describes how to run the module in its Approved FIPS 140-2 mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module.

The Redline RDL-3000, Elte-MT Broadband Wireless Systems running firmware version 3.1 is referred to in this document as the RDL-3000 and Elte-MT, the cryptographic module, or the module.

1.2 References

This document deals only with operations and capabilities of the module in the technical terms of a FIPS 140-2 cryptographic module security policy. More information is available on the module from the following sources:

- The Redline website (http://www.rdlcom.com/) contains information on the full line of products from Redline.

The National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) website (http://csrc.nist.gov/groups/STM/cmvp/index.html) contains information about the FIPS 140-2 standard and validation program. It also lists contact information for answers to technical or sales-related questions for the module.

1.3 Document Organization

The Security Policy document is one document in a FIPS 140-2 Submission Package. In addition to this document, the Submission Package contains:

- Vendor Evidence document
- Finite State Machine
- Submission Summary
- Other supporting documentation as additional references

This Security Policy and the other validation submission documentation were produced by Redline Communications. With the exception of this Non-Proprietary Security Policy, the FIPS 140-2 Validation Documentation is proprietary to Redline and is releasable only under appropriate non-disclosure agreements. For access to these documents, please contact Redline.

2.0 Redline Communications RDL-3000, Elte-MT Broadband Wireless Systems

2.1 Overview

The RDL-3000, Elte-MT Broadband Wireless Systems by Redline Communications leverage proven orthogonal frequency-division multiplexing (OFDM) technology to deliver high-speed Ethernet throughput over wireless links. Under clear line-of-sight conditions, the RDL-3000 and Elte-MT can provide robust, long-range connectivity at distances beyond 50 kilometers. The all-Internet Protocol (IP) design of the RDL-3000 and Elte-MT deliver a seamless extension of Ethernet local area networks and wide area networks, at proven Ethernet data rates greater than 100 Mbps[1]. The RDL-3000 and Elte-MT provide unmatched spectral flexibility with support for several different channel sizes (3.5, 5, 7, 10 and 20 MHz[2]) in Point-to-Point (PTP) and Point-to-Multipoint (PMP) modes, and center frequency specification in 2.5 MHz increments. Extremely low latency in PTP (less than 4 ms3), and PMP (less than 10 ms) ensures the successful delivery of bandwidth-intensive applications such as Voice-over-IP (VoIP), real time video, teleconferencing, and SCADA. Designed for the harshest outdoor conditions, the radio receives Direct Current (DC) Power Over Ethernet (POE) from the indoor unit via standard CAT4-5 Ethernet cable.

Operating over the 600MHz–5.8 GHz5 frequency bands, covering the 4.94–4.99 GHz Public Safety band, and the 5.250-5.850 FCC, ETSI ISM bands, the RDL-3000 and Elte-MT can be considered for wireless networking solutions such as public safety, first responders, government and enterprise networks, and long/short-haul digital oil field communications connectivity. Transmissions can be secured via the embedded encryption capability or via external Ethernet Inline Network Encryption (INE) devices.

The lightweight RDL-3000 and Elte-MT is easy to configure and deploy. Using a standard Web browser, an operator has access to all required configuration items and statistics necessary to configure and monitor the operation of the radio. Third-party network management applications can also be utilized via the standard Simple Network Management Protocol (SNMPv3) interface.

Figure 1 – Redline RDL-3000, Elte-MT Broadband Wireless Systems

The RDL-3000 and Elte-MT are validated at the following FIPS 140-2 section Levels:

[1] *Mbps – Megabits per second*
[2] *MHz – megahertz*
[3] *ms – milliseconds*
[4] *CAT – Category*
[5] *GHz – Gigahertz*

Table 1 – Security Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	Electromagnetic Interference / Electromagnetic Compatibility (EMI/EMC)	3
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
14	Cryptographic Module Security Policy	2

2.2 Module Interfaces

The RDL-3000 and Elte-MT are of multi-chip standalone cryptographic module that meets overall Level 2 FIPS 140-2 requirements. The cryptographic boundary of the RDL-3000 and Elte-MT is defined by the aluminum case, which surrounds all the hardware and software components. Interfaces on the module can be categorized into the following FIPS 140-2 logical interfaces:

- Data Input Interface
- Data Output Interface
- Control Input interface
- Status Output Interface
- Power Interface

Ports on the module can be categorized into the following FIPS 140-2 physical interfaces:

- Ethernet port (RDL-3000 and eLTE-MT enclosures)
- RF ports (RDL-3000 enclosure only)
- Buzzer (RDL-3000 and eLTE-MT enclosures)
- GPS port (RDL-3000 enclosure only)

All of these physical interfaces are separated into logical interfaces defined by FIPS 140-2, as described in the following table:

Table 2 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Module Port/Interface	
	RDL-3000 Enclosure	eLTE-MT Enclosure
Data Input	Ethernet port, RF port, GPS port	Ethernet port
Data Output	Ethernet port, RF port	Ethernet port
Control Input	Ethernet port, RF port, PPS Port	Ethernet port
Status Output	Ethernet port, Buzzer	Ethernet port, Buzzer
Power	Ethernet port	Ethernet port

2.3 Roles and Services

The module supports role-based authentication. There are two roles in the module that operators may assume: a Crypto-Officer role and a User role. A Crypto-Officer can create/delete/modify identities in the module and assign them access to the module based on the two available roles. Operators access the system via one of the available secure management interfaces using their assigned identity and credentials.

All role-appropriate services are exposed via any of the 3 available secured management interfaces (SSH, HTTPS, or SNMPv3). The CO/User can use whichever management interface they are most comfortable with. The CO can disable any (but not all) of the management interfaces according to their preference.

Crypto-Officer Role

The Crypto-Officer performs administrative services for the module, such as initialization, configuration, and monitoring of the module. Before accessing the module for any administrative service, the operator must authenticate to the module. The module offers three management interfaces:

- Web Interface
- Command Line Interface (CLI)
- SNMPV3

The Web Interface is Redline's proprietary web-based GUI[6] that can be accessed via the local network using a web browser. The Web Interface serves as the primary management tool for the module. All Web Interface sessions with the module are protected over a secure TLS channel. Authentication of the CO requires the input of a username and password which is checked against the module's local database.

The CLI is accessed via the Ethernet port using a Secure Shell (SSH) session. Authentication of the CO on the CLI requires the input of a username and password which is checked against the modules local database.

[6] *GUI – Graphical User Interface*

The SNMPv3 interface is accessible using any standard SNMP client software or NMS which supports the SNMPv3 protocol. The module's Management Information Base (MIB) files which define the structure of the interface are available on Redline's website. Authentication of the CO via SNMPv3 requires the input of a username and password which is checked against the module's local database.

Descriptions of the services available to the Crypto-Officer role are provided in the table below.

Table 3 – Mapping of Crypto-Officer Role's Services to Type of Access

Service	Description	CSP and Type of Access
User Authenticate	Used to login to the module using TLS or SSH protocol	**CSPs:** 8+ character ASCII string, RSA/DSA 1024/2048 bit key, **Access:** Read
Access Graphical User Interface	Graphical User interface (HTTPS/TLS) by which the CO/User accesses the remainder of the services	**CSPs:** RSA 2048bit key, HMAC SHA256 key, AES-128/256 key **Access:** Read/Execute
Access Command Line Interface	Command Line interface (SSH) by which the CO/User access the remainder of the module's services.	**CSPs:** Diffie-Hellman 2048bit exponent, HMAC SHA1 160bit key, AES-128/256 key **Access:** Read/Execute
Access SNMPv3 Interface	Secured interface by which Network Management Systems access the available services	**CSPs:** 11 byte static value, 8+ character ASCII string, AES 128/256 bit CFB **Access:** Read/Execute
Transmit/Receive Wireless Data	Allows received Ethernet data to be sent securely across the wireless link	**CSPs:** AES-128/256 CCM key, AES-128/256 Pre-shared key **Access:** Read/Execute
Enable/Disable FIPS Mode	Allows Crypto-Officer to configure the module for FIPS Mode.	None
Get FIPS Status	Allows Crypto-Officer to view general system identification and Configuration Settings.	None
System Status	Allows Crypto-Officer to view system, Ethernet, and wireless statistics.	None
System Log	Allows Crypto-Officer to view the system status messages.	None
Configure System	Allows Crypto-Officer to view and adjust configuration system, IP address, management, and wireless settings.	None

Service	Description	CSP and Type of Access
Link Summary	Allows users to view the current status of wireless link conditions (e.g. signal strength, signal quality, wireless packet errors, etc.)	None
Upload Firmware	Allows Crypto-Officer to upload new software binary file	**CSPs:** RSA 2048 bit key **Access:** Read/Execute
Add/Delete Users	Allows Crypto-Officer to add/delete users	**CSPs:** 8+ character ASCII string **Access:** Read/Write
Change Password	Modify existing login passwords	**CSPs:** 8+ character ASCII string **Access:** Read/Write
Spectrum Sweep	Allows Crypto-Officer to scan radio frequencies to detect additional RF sources which could be a source of interference	None
Zeroize	Zeroize all keys and CSPs	CSPs: All CSPs listed in table 7 as zeroized “by zeroize command” Access: Write
Clear	Clears frequency list and log messages	None
Del	Deletes keys/certificates	CSPs: ECDSA P-384 key Access: Write
Freq	Used to enter the frequency ranges for autoscan and dynamic frequency selection	None
Generate	Creates new keys for use with SSH, TLS, and SNMPv3	CSPs: AES CFB Key, RSA/DSA KeyPair, All DRBG-associated CSPs Access: Write
Get	Displays statistic and parameter values	None
Load Cert	Loads new certificates	CSPs: ECDSA P-384 key Access: Write
Load Script	Loads a script for backup/restore	None
Ping	Ping utility	None
Reboot	Restarts the module. Also initiates power-up self-test.	None
Reset Statistics	Resets the statistical values stored in the module	None
Save	Saves the selected configuration settings	None
Export Script	Generates and outputs a config script	None
Set	Displays system parameter values and allows modification to the displayed values	None
Show	Displays configuration and additional system compound objects	None
Test Config	Allows configuration changes to be run for a five minute test period	None

Service	Description	CSP and Type of Access
Power-up self-test	Executes a series of Known-Answer-Tests against all certified cryptographic algorithms in the module. See section 2.8 for more details. This service is executed automatically on module startup, and can be executed by issuing a reboot command to the module.	CSPs: All Cryptographic components listed in section 2.8 under "Power-up Self Tests" Access: Read/Write

User Role

The User has the ability to view general status information about the module, and utilize the module's data transmitting functionalities via the Ethernet port. Descriptions of the services available to the User role are provided in the table below.

Table 4 – Mapping of User Role's Services to Type of Access

Service	Description	CSP and Type of Access
User Authenticate	Used to login to the module using TLS or SSH protocol	**CSPs:** 8+ character ASCII string, RSA/DSA 1024/2048 bit key, **Access:** Read
Access Graphical User Interface	Graphical User interface (HTTPS/TLS) by which the CO/User accesses the remainder of the services	**CSPs:** RSA 2048bit key, HMAC SHA256 key, AES-128/256 key **Access:** Read/Execute
Access Command Line Interface	Command Line interface (SSH) by which the CO/User access the remainder of the module's services.	**CSPs:** Diffie-Hellman 2048bit exponent, HMAC SHA1 160bit key, AES-128/256 key **Access:** Read/Execute
Access SNMPv3 Interface	Secured interface by which Network Management Systems access the available services	**CSPs:** 11 byte static value, 8+ character ASCII string, AES 128/256 bit CFB **Access:** Read/Execute
Transmit/Receive Wireless Data	Allows received Ethernet data to be sent securely across the wireless link	**CSPs:** AES-128/256 CCM key, AES-128/256 Pre-shared key **Access:** Read/Execute
Authenticate	Used to login to the module using TLS or SSH protocol	CSPs: 8+ character ASCII string Access: Read
General Information	Allows Users to view general system identification and Configuration Settings.	None
Link Summary	Allows users to view the current status of wireless link conditions (e.g. signal strength, signal quality, wireless packet errors, etc.)	None

Service	Description	CSP and Type of Access
System Status	Allows Users to view system, Ethernet, and wireless statistics.	None
System Log	Allows Users to view the system status messages.	None
Change Password	Allows Users to change login password	CSPs: 8+ character ASCII string Access: Read/Write

Authentication Mechanisms

The module employs the following authentication methods to authenticate Crypto-Officers and Users.

Table 5 – Authentication Mechanisms Employed by the Module

Type of Authentication	Authentication Strength
Password	Passwords are required to be at least 8 characters long. Alphabetic (uppercase and lowercase), numeric, and special characters can be used, which gives a total of 94 characters to choose from. With the possibility of repeating characters, the chance of a random attempt falsely succeeding is 1 in 94^8, or 1 in 6,095,689,385,410,816. The module forces a 1 second pause between failed login attempts. This means that in a 60-second period a maximum of 60 attempts can be made, making the chances of a random attempt falsely succeeding 1 in 101,594,823,090,180. This is well below the required 1 in 100,000 maximum.
Certificate	The minimum size certificate used by the module in an approved mode of operation is 2048 bits, which provides 112 bits of security. The probability of a random attempt falsely succeeding is 1 in 2^{112}, or 1 in 5.19229×10^{33}. Two modules exchange certificates for device authentication once every wireless registration attempt. The minimum possible time between registration attempts is 500 milliseconds, resulting in a maximum of 120 registration attempts in a 60-second period. This makes the chances of a random attempt falsely succeeding 1 in 5.19229×10^{33} divided by 120, or 1 in 4.32691×10^{31}. This is well below the required 1 in 100,000 maximum.

2.4 Physical Security

The Redline RDL-3000 and Elte-MT are both multi-chip standalone cryptographic modules. The module is enclosed in a weatherproof aluminum alloy case, which is defined as the cryptographic boundary of the module. The module's enclosure is opaque within the visible spectrum. The module's enclosure is sealed using two (2) tamper-evident labels, which prevent the case covers from being removed without signs of tampering.

Tamper-evident labels are applied at the factory. It is the responsibility of the Crypto-Officer to ensure that all tamper-evident labels are properly placed on the module before use. The location of the

tamper-evident labels is indicated with the red circles in Figure 2 below. The CO is responsible for the yearly inspection of the integrity of these seals. If CO suspects that the integrity of either of the seals has been compromised, then the module should be immediately decommissioned and returned to Redline for inspection.

Figure 2 – Tamper-Evident Label Locations for RDL-3000 and Elte-MT

2.5 Operational Environment

The module does not provide a general purpose operating system nor does it allow operators to load untrusted software. The operating system (OS) employed by the modules is referred to as Wind River VxWorks version 6.9 OS. The OS is not modifiable by the operators of the modules, and only the modules' custom written image can be run in the system. The modules provide a method to update the firmware in the module with a new version. This method involves uploading a digitally signed firmware update to the module.

The VxWorks operating system and firmware-implemented cryptographic functions are executed on a Cavium Networks ECONA CNS3411 (ARMv6) SoC.

2.6 Cryptographic Key Management

The module implements the FIPS-approved algorithms shown in Table 6 below.

Table 6 – Certificate Numbers for Cryptographic Algorithm Implementations

Approved Functions	Algorithm Implementation	Certificate #
Symmetric Key Algorithm	Advanced Encryption Standard (AES) 128-, 256-bit in ECB[7] and CCM[8] modes	Hardware Implementation: #3469
	Advanced Encryption Standard (AES) 128-, 256-bit in CBC[9]/CFB[10] mode, 256-bit in CTR[11] mode	Management Implementation: #3472

[7] *ECB – Electronic Codebook*
[8] *CCM – Counter with CBC-MAC*
[9] *CBC – Cipher-Block Chaining*
[10] *CFB – Cipher Feedback*

Approved Functions	Algorithm Implementation	Certificate #
Secure Hashing Algorithm (SHA)	SHA-1, SHA-256, SHA-384	Management Implementation: #2866
	SHA-384	ECDSA Implementation: #2867
Message Authentication Code (MAC) Function	HMAC[12] using SHA-1, SHA-256, SHA-384	Management Implementation: #2216
	HMAC using SHA-384	ECDSA Implementation: #2217
Deterministic Random Bit Generator (DRBG)	NIST[13] SP 800-90A DRBG[14]: Hash SHA-1 and Hash SHA-256	Management Implementation: #854
Key Derivation Function	TLS, SSH, SNMPv3 KDF	Management Implementation: #541
Key Agreement Scheme	Full MQV	KAS Implementation: #63
Asymmetric Key Algorithm	RSA[15] PKCS[16]#1 v1.5 SigGen 2048-bit w/ SHA256 SigVer 1024/2048-bit w/ SHA1/SHA256	Management Implementation: #1780
	DSA SigGen 2048-bit w/ SHA256 KeyPairGen 2048-bit SigVer 1024/2048-bit w/ SHA1/SHA256	Management Implementation: #981
	ECDSA – P-384 curve	ECDSA Implementation: #703

The module implements network protocols which make use of KDFs that are listed in **NIST SP 800-135rev1**. The KDF algorithms have been tested, validated, and assigned certificate #541 (see above). The testing of protocols is beyond the scope of FIPS 140-2. Thus, the following protocols have **not been reviewed or tested** by either CAVP or CMVP:

- TLS
- SSH
- SNMPv3

The module implements the following non-FIPS-approved algorithms which are allowed for use in FIPS mode:

- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- NDRNG

---

[11] *CTR – Counter Mode*
[12] *HMAC – Hash Message Authentication Code*
[13] *NIST – National Institute of Standards and Technology*
[14] *DRBG – Deterministic Random Bit Generator*
[15] *RSA – Rivest, Shamir, and Adleman*
[16] *PKCS – Public Key Cryptography Standard*

The module implements a Non-deterministic Random Number Generator (NDRNG) which is capable of providing a minimum of 256 bits of entropy. This NDRNG is entirely contained within the module's cryptographic boundary, is used for all key generation in the system, and operates in a blocking manner.

The module supports the following critical security parameters:

Table 7 – List of Cryptographic Keys, Cryptographic Key Components, and CSPs

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SNMPv3 Session Key	AES 128, 256-bit CFB key	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Provides secured channel for SNMPv3 management.
SNMPv3 Password	Minimum 8-character ASCII[17] string	Entered in plaintext	Never exits the module	Stored in non-volatile memory	By zeroize command	Authentication for remote client communication with the module via SNMPv3
SNMPv3 Engine ID	11-byte value unique to each module: SNMP-OID + MAC-ADDR	Internally generated	Output in plaintext (not a secret)	Stored in volatile memory	Not applicable (module-specific runtime identifier)	Uniquely identifies the module's SNMPv3 agent for use in communication with remote SNMPv3 clients
Pre-shared Key	AES 128-, 256-bit key	Internally generated	Never exits the module	Stored in non-volatile memory.	By Zeroize command	Provides confidentiality of data over PTP radio channel
Authentication public/private keys	RSA 1024 – 2048 bit keys or DSA 1024 – 2048 bit keys	DSA keys are Internally generated and RSA keys are externally generated and imported in certificate form	Public key exported electronically in plaintext via Ethernet port	Stored in non-volatile memory	By Zeroize command, or by termination of session, or by module reboot	Peer Authentication of SSH/TLS sessions
Peer RSA/DSA public keys	RSA/DSA 1024-, 2048-bit keys	Imported electronically during handshake protocol	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Peer Authentication for SSH and TLS sessions
Local public/private keys	ECDSA P-384 key, using FIPS 186-4 B.4.1 (extra random bits)	Internally generate	Public key exported electronically in plaintext via wireless port; private component not exported	Stored in non-volatile memory.	By Zeroize command	Establish trusted point in peer entity

[17] *ASCII – American Standard Code for Information Interchange*

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
SSH Key Agreement keys	Diffie-Hellman 2048-bit exponents	Internally generated	Public exponent electronically in plaintext; private component not exported	Stored in volatile memory	Upon reboot or session termination	Key exchange/agreement for SSH sessions
TLS Key Agreement Keys	RSA 2048-bit key	Externally generated	Public key electronically in plaintext; private key not exported	Stored in volatile memory	Upon reboot or session termination	Key exchange/agreement for TLS sessions
TLS Session Authentication Key	HMAC SHA256 256-bit key	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Data authentication for TLS sessions
TLS Session Key	AES-128, AES-256	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Data encryption for TLS sessions
SSH Session Authentication Key	HMAC SHA1 160-bit key	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Data authentication for SSH sessions
SSH Session Key	AES-128, AES-256	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot or session termination	Data encryption for SSH sessions
Redline Firmware Update Public Key	RSA 2048-bit public key	Externally generated and hard coded in the image	Never exits the module	Stored in non-volatile memory (hardcoded)	Not applicable	Verifies the signature associated with a broadband radio firmware update package
Administrator Passwords	Minimum 8-character ASCII string	Entered in plaintext	Never exits the module	Stored in non-volatile memory in plaintext	By Zeroize command	Authentication for administrator login
User Passwords	Minimum 8-character ASCII string	Entered in plaintext	Never exits the module	Stored in non-volatile memory in plaintext	By Zeroize command	Authentication for user login
NIST SP 800-90A DRBG seed	256-bit random value	Internally generated	Never exits the module	Generated after reset. Stored in volatile memory	Upon reboot, and also overwritten (as a circular buffer) by random value	Used during FIPS-approved random number generation
Entropy Input String	256-bit value	Internally generated using DRBG	Never exits the module	Stored in volatile memory	Upon reboot, and upon each use	Random number generation

Key	Key Type	Generation / Input	Output	Storage	Zeroization	Use
AES CCM Key	AES 128- and 256-bit keys	Internally generated	Encrypted via AES for wireless transmission using ECDSA-derived shared secret	Stored in volatile memory	Upon reboot, or zeroize command	Used for cryptographically securing wireless communications between connected modules.
DRBG 'C' Value	DRBG intermediate C-value: 440 bits	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot, or upon DRBG reset	Intermediate value used in DRBG
DRBG 'V' Value	DRBG intermediate V-value: 440 bits	Internally generated	Never exits the module	Stored in volatile memory	Upon reboot, or upon DRBG reset	Intermediate value used in DRBG

2.7 Electromagnetic Interference / Electromagnetic Compatibility

The Redline RDL-3000 and Elte-MT was tested and found to be conformant to the Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC) requirements specified by *Federal Communications Commission CFR*[18] *47, Parts 2 and 90 (Subpart Y) – Regulations Governing Licensing and Use of Frequencies in the 4940-4990 MHz Range, Federal Communications Commission CFR 47, Parts 15- Regulations Governing Use of Frequencies in the 5470-5725 and 5725-5850 MHz Range*. Compliance with these regulations meets FIPS Level 3 requirements for EMI/EMC.

2.8 Self-Tests

Power-up Self-Tests

The RDL-3000 and Elte-MT perform the following self-tests at power-up:

- Firmware integrity check using an Error Detection Code (16 bit CRC[19])
- AES Encryption KAT[20] (Firmware)
- AES Decryption KAT (Firmware)
- AES Encryption KAT (Hardware)
- AES Decryption KAT (Hardware)
- DSA Signature Generation PCT[21] using 2048-bit key
- DSA Signature Verification PCT using 1024, 2048-bit keys
- ECDSA Signature Generation PCT using P-384 curves
- ECDSA Signature Verification PCT using P-384 curves

[18] *CFR – Code of Federal Regulations*
[19] *CRC – Cyclic Redundancy Check*
[20] *KAT – Known Answer Test*
[21] *PCT – Pairwise Consistency Test*

- HMAC KAT (SHA-1, SHA-256, SHA-384)
- SHS KAT (SHA-1, SHA-256, SHA-384)
- NIST SP 800-90A Hash Based DRBG KAT
- RSA Signature Generation KAT using 2048-bit key
- RSA Signature Verification KAT using 1024, 2048-bit keys

If any of the power-up tests fail, the module enters into a critical error state. An error message is logged in the System Log and highlighted in both the GUI and CLI for the Crypto-Officer to review. A CO must perform actions to clear the error state.

Conditional Self-Tests

The RDL-3000 and Elte-MT also perform the following conditional self-tests:

- Continuous Random Number Generator Test (CRNGT) for the SP 800-90A Hash_Based_DRBG
- CRNGT for the Non-Deterministic Random Number Generator (NDRNG)
- ECDSA PCT for key pair generation
- DSA PCT for key pair generation
- Firmware Load Test using RSA Signature Verification

Critical Function Tests

The RDL-3000 and eLTE-MT also perform the following critical function self-tests:

- SP 800-90A Hash_Based_DRBG Instantiate Health Test
- SP 800-90A Hash_Based_DRBG Generate Health Test
- SP 800-90A Hash_Based_DRBG Reseed Health Test

2.9 Mitigation of Other Attacks

In a FIPS Mode of operation, the module does not claim to mitigate any additional attacks.

3.0 Secure Operation

The RDL-3000 and Elte-MT meet 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.

3.1 Crypto-Officer Guidance

The Crypto-Officer is responsible for the initialization and management of the module. Please view the RDL-3000 and Elte-MT User Manual for additional information on configuring and maintaining the module. The Crypto-Officer can receive the module from the vendor via trusted delivery couriers

including UPS, FedEx, and Roadway. The Crypto-Officer can also arrange for pick up directly from Redline.

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 which cover the screws at each side of the module. If the Crypto-Officer suspects tampering, he/she should immediately contact Redline.

Initialization

The Crypto-Officer is responsible for the Initialization of the module through the Web Interface or CLI. Please refer to the RDL-3000 Family User Manual for information on accessing the system's management interfaces. The Crypto-Officer must login to the module using the default username and password. Once initial authentication has completed, the Crypto-Officer must setup all Crypto-Officer and User accounts passwords (eight characters minimum) and verify via the System Configuration window that the module has the appropriate licensing installed. Once properly licensed, the module will enable the activation of **Secure Mode**. If Secure Mode is disabled, the Crypto-Officer can enable it by performing the following steps:

1. Change the default Crypto-Officer password and default User password
2. Set **Secure Mode to Enabled**
3. This will cause the module to disable any non-FIPS compliant interfaces and algorithms
4. Reboot

When in **Secure Mode** (assuming the proper licensing is installed), if the module is running the latest FIPS-certified firmware and all algorithmic self-tests have passed, the module will be operating in **FIPS Mode**. This will be indicated by a **FIPS** flag (specifically, the word "Secured") in the CLI and GUI banners, as well as a **FIPS Certification** field in the module's status page.

The Crypto-Officer must ensure that the module's cryptographic keys and CSPs are reinitialized any time the module's **Secure Mode** operational status is uncertain (e.g. upon first delivery of the module, or after Secure Mode has been disabled for any reason). This is done using the "zeroize" and "load certs" services listed in table 3. This operation should be done in a secure and trusted environment.

If **Secure Mode** has been enabled, but FIPS Mode is not indicated, the CO should verify:

- That the module is running a specifically FIPS-certified version of firmware
- That the module has licensing installed which has FIPS-certification activated

Management

The Crypto-Officer is able to configure and monitor the module via the Web Interface over TLS and CLI over SSH. The Crypto-Officer should check the System Status and System Logs frequently for errors. If the same errors reoccur or the module ceases to function normally, then Redline customer support should be contacted.

3.2 User Guidance

The User role is able to access the module over the Ethernet port and perform basic services including: viewing general system status information and changing their own password. A list of commands available to the User role is found in Table 4.

4.0 Acronyms

This section defines the acronyms used throughout this document.

Table 8 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
ASCII	American Standard Code for Information Interchange
CAT	Category
CBC	Cipher-Block Chaining
CCM	Counter with CBC-MAC
CFB	Cipher Feedback
CFR	Code of Federal Regulations
CLI	Command Line Interface
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CO	Crypto-Officer
CRC	Cyclic Redundancy Check
CSE	Communications Security Establishment
CSP	Critical Security Parameter
CTR	Counter (“CTR Mode”)
DC	Direct Current
DES	Digital Encryption Standard
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GHz	Gigahertz
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Hypertext Transfer Protocol

Acronym	Definition
ID	Identification
IP	Internet Protocol
KAT	Known Answer Test
MAC	Message Authentication Code
Mbps	Megabits per second
MHz	Megahertz
Ms	Milliseconds
NIST	National Institute of Standards and Technology
OFDM	Orthogonal Frequency-Division Multiplexing
OS	Operating System
PKCS	Public Key Cryptography Standard
PMP	Point-to-Multipoint
POE	Power Over Ethernet
PTP	Point-to-Point
RNG	Random Number Generator
RSA	Rivest Shamir and Adleman
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Socket Layer
TLS	Transport Layer Security