Christine
WIRELESS

Radio Internet-Protocol Communications Module Z (RIC-Mz)

FIPS 140-2 Non-Proprietary Security Policy

Cryptographic module for use in Project 25 Radio Systems

Document Version: R01:00:03

Date: November 8, 2021

Table of Contents

List of Tables

List of Figures

1. Introduction

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST) and Canadian Centre for Cyber Security (CCCS) and Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. The NVLAP accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. Validated is the term given to a module that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at:
http://csrc.nist.gov/groups/STM/cmvp/index.html

1.1. Scope

This Security Policy specifies the security rules under which RIC-Mz must operate. In addition to the security requirements derived from FIPS 140-2 are those imposed by Christine Wireless, Inc. These rules, in total, define the interrelationship between the:

- Module Operators,
- Module Services, and
- Critical Security Parameters (CSPs).

1.2. Overview

The RIC-Mz provides Internet-Protocol interconnectivity of voice and data services for Project 25 Radio Systems. This interconnectivity is provided by the RIC-Mz through the conversion of analog or digital radio equipment baseband signals to/from Internet Protocol UDP packets. There are three basic modes of operation:

1. **Digital Fixed Station Interface (DFSI) Host:** In this mode of operation the RIC-Mz can connect over Internet Protocol to another RIC-Mz or other device that is acting as a DFSI Fixed Station. In this mode the RIC-Mz is, in essence, acting as the Dispatch Console for the Fixed Station. The RIC-Mz can transfer analog voice, digital voice (externally encrypted or unencrypted), digital packet data (externally encrypted or unencrypted) as well as providing channel change and other controls to the Fixed Station. The RIC-Mz supports both TIA Standards 102.BAHA and 102.BAHA-A. The RIC-Mz supports the conversion of DFSI messages into V.24 synchronous serial or analog E and M control as is appropriate.

2. **DFSI Fixed Station:** In this mode of operation the RIC-Mz acts as a DFSI Fixed Station and supports IP connection to another RIC-Mz or other device (such as a Dispatch Console) acting as a DFSI Host. The RIC-Mz can transfer analog voice, digital voice (externally encrypted or unencrypted), digital packet data (externally encrypted or unencrypted) as well as accepting channel change and other controls from the DFSI Host. The RIC-Mz supports both TIA Standards 102.BAHA and 102.BAHA-A. The RIC-Mz supports the conversion of DFSI messages into V.24 synchronous serial or analog E and M control as is appropriate.

3. **Tunnel Mode:** In the Tunnel Mode, two RIC-Mzs can exchange digital voice and packet data (externally encrypted or unencrypted) using a UDP data mode similar to that used in TIA Standards 102.BAHA and 102.BAHA-A. This provides a transparent connection of data present on the two RIC-Mz V.24 connectors in both directions. If it is desired to encrypt the UDP data packets, the pair of RIC-Mzs can support DTLSv1.2 security. The DTLSv1.2 is implemented as a Diffie Helman Ephemeral Key AES 256-bit key GCM encryption with a new key being established for each new connection between the two RIC-Mzs.

1.3. RIC-Mz Implementation

The RIC-Mz is implemented as a multi-chip standalone cryptographic module as defined by FIPS 140-2.

1.4. RIC-Mz Hardware/Firmware Version Numbers

Table 1: FIPS Validated Version Numbers

FIPS Validated Cryptographic Module Hardware Version Number	FIPS Validated Cryptographic Module Firmware Version Number
RIC-Mz Spin 4	DTLS_FIPS_Final_10_31_20

1.5. FIPS 140-2 Security Levels

The RIC-Mz can be configured to operate at FIPS 140-2 overall Security Level 2. The table below shows the FIPS 140-2 security levels met for each of the eleven areas specified in the FIPS 140-2 security requirements.

Table 2: RIC-Mz Security Levels

FIPS 140-2 Security Requirements Section	Validated Level
Cryptographic Module Specification	2
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	2
Mitigation of Other Attacks	N/A

1.6. RIC-Mz Cryptographic Boundary

The RIC-Mz is housed in an aluminum case. A single printed circuit board contained in the aluminum enclosure implements all RIC-Mz functionality. The cryptographic boundary is the outside of the aluminum enclosure. The screw head patterns have been removed from all of the 8 screws used to secure the endplates thus preventing disassembly of the case and access to the printed circuit board contained therein. In addition, epoxy has been applied to the screw threads when installed preventing removal of the screws.

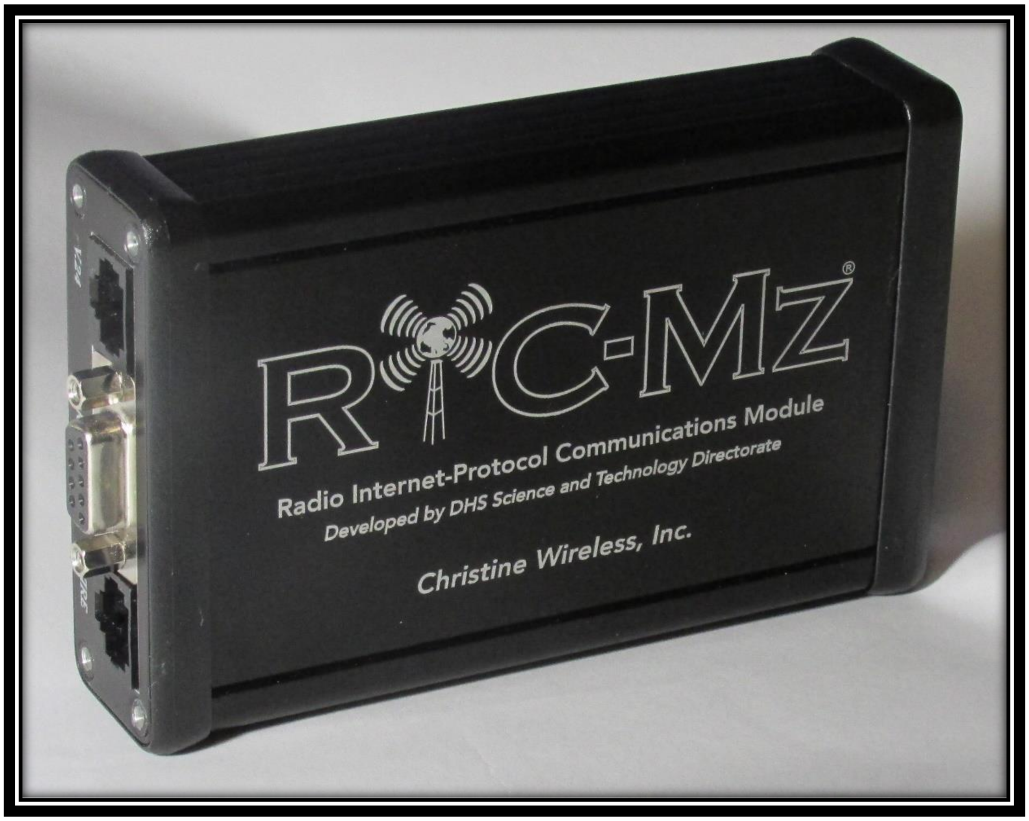
RIC-Mz®
Radio Internet-Protocol Communications Module
Developed by DHS Science and Technology Directorate
Christine Wireless, Inc.

Figure 1: RIC-Mz Top/Rear View

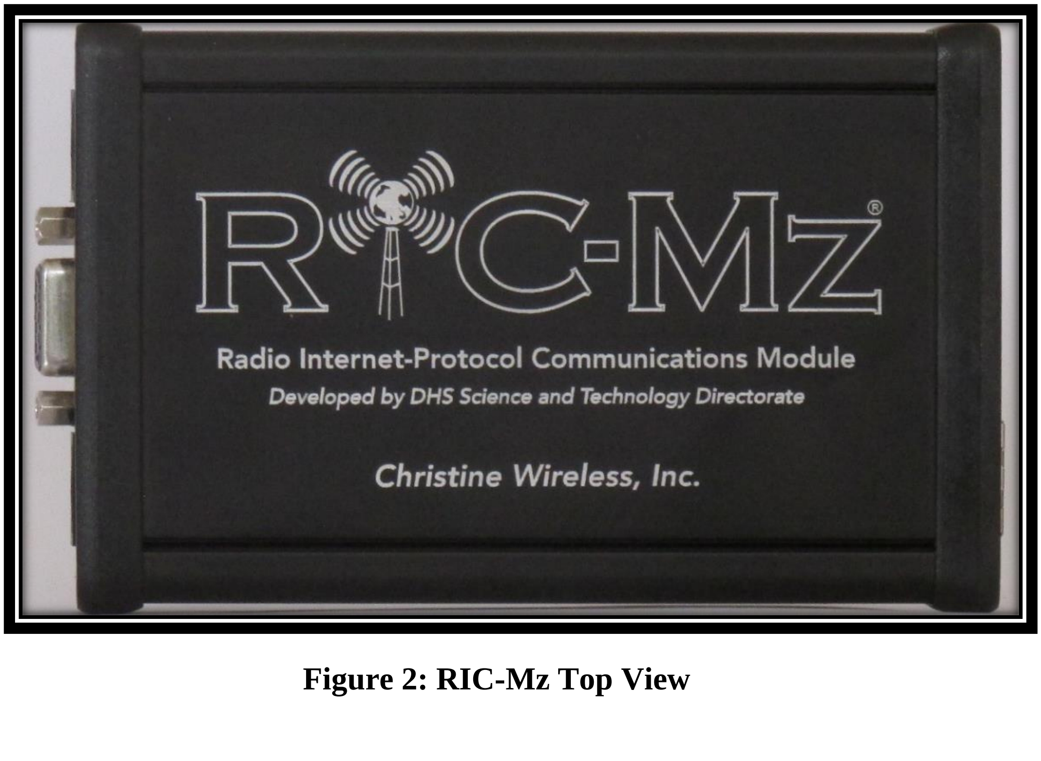
RIC-Mz®
Radio Internet-Protocol Communications Module
Developed by DHS Science and Technology Directorate
Christine Wireless, Inc.

Figure 2: RIC-Mz Top View

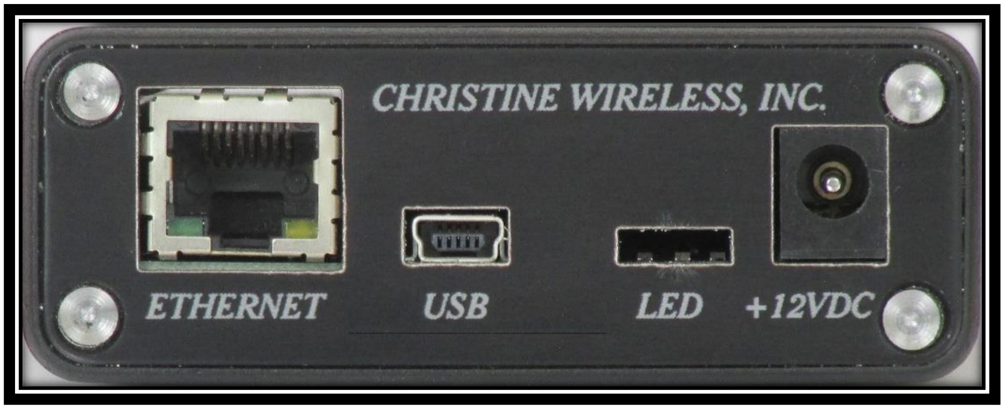

Figure 3: RIC-Mz Front View

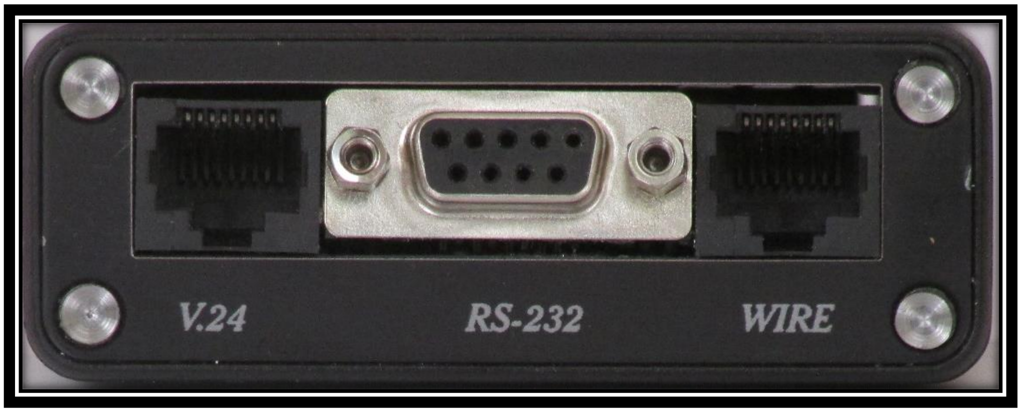

Figure 4: RIC-Mz Rear View

1.7.Ports and Interfaces

The RIC-Mz provides the following physical ports and logical interfaces:

Table 3: Ports and Interfaces

Physical Port	Qty	Logical Interface Definition	Description
Power	1	Power Input	+12VDC power into module
Wire	1	Data Input/Data Output	Analog Interface for unencrypted radio
V.24	1	Data Input/Data Output (Base Station Interface)	Synchronous serial interface for Tx/Rx of digital radio messages
RS-232	1	Status Output (Base Station Interface)	Asynchronous serial interface for Tx/Rx of radio messages
Main LED (Yellow) (Right LED)	1	Status Output	Indicates firmware is operating normally
Tx LED (Red) (Center LED)	1	Status Output	Indicates outgoing Base Station radio message
Rx LED (Green) (Left LED)	1	Status Output	Indicates incoming Base Station radio message
USB	1	Status Output (Firmware Status Monitor)	Used only for troubleshooting-no access to CSPs
Ethernet Black	1	IP Base Station Connection (Data Input/Data Output)	Internet Protocol interface for unencrypted or encrypted UDP Tx/Rx of radio messages
Ethernet Red TLSv1.2 on shared physical port logically separated from black ethernet port	(1) Shared with above physical port	Data Input, Data Output, Control Input and Status Output Firmware Update	Crypto-Officer access for setup and monitoring Crypto-Officer upload of new firmware

2. FIPS 140-2 Approved Operational Modes

The RIC-Mz only operates in a FIPS 140-2 Approved mode of operation. Documented below are the configuration settings that are required for the RIC-Mz to be used in a FIPS 140-2 mode of operation at overall Security Level 2.

3. Identification and Authentication Policy

The RIC-Mz supports a User Role and a Crypto-Officer Role.

The Crypto-Officer Name and Crypto-Officer Password are set as default values at the manufacture. Before any setup is permitted, the Crypto-Officer must log into the RIC-Mz with the default Crypto-Officer Name and Crypto-Officer Password and set the two entries to non-default values. The new Crypto-Officer Name and Crypto-Officer Password are stored in non-volatile memory. To continue, the Crypto-Officer must log out and log back into the RIC-Mz with the new credentials. The RIC-Mz can now be configured and firmware files uploaded.

In the event that the Crypto-Officer Name/Password are lost, the RIC-Mz can be returned to a factory default condition which will result in the erasure of all Crypto-Officer entered setup/configuration data.

The User role is defined by the entities that access the RIC-Mz via the IP UDP connection. In order for a device to utilize the User Role, the device IP address and UDP ports must first be entered into the RIC-Mz by the Crypto-Officer. The User is authenticated using an HMAC.

Table 4: Roles and Authentication

Role	Authentication Type	Authentication Mechanism	Strength of Authentication
Crypto-Officer (Basic Operation and Firmware update)	Role-Based	8-12 character ASCII password	The minimum password length must be 8 ASCII characters. There are 95 printable ASCII characters. The chance of guessing the correct 8 characters is 1 in 6.63e+15 (i.e. 1/95^8), which is less than 1/1,000,000. The user interface is intentionally delayed by 3 seconds after each

Role	Authentication Type	Authentication Mechanism	Strength of Authentication
			incorrect entry to limit password entry tries to 20 per minute, resulting in a probability of guessing the password during a one-minute period to 1 in 3.3e+14 (i.e. 20/95^8), which is less than 1/100,000.
User Role (DTLSv1.2 Connection)	Role -Based	HMAC SHA-256	Each packet sent by the user must include an 8-byte HMAC that is verified by the module. Since the HMAC is 8 bytes long, the probability of a random authentication attempt succeeding is 1/256^8, which is less than 1/1,000,000. When the module is idle, there is an average 24 microsecond delay between each received packet, preventing the module from receiving more than 2,500,000 packets per minute. Based on an 8-byte MAC, the likelihood of a random attempt succeeding during a one-minute period is 2,500,000/256^8, which is less than 1/100,000.

4. Access Control Policy

4.1. RIC-Mz Supported Roles

The RIC-Mz supports two roles. These roles are defined to be:

- User Role and
- Crypto-Officer authenticated Role.

4.2.RIC-Mz Services Available to the User Role.

- Project 25 Operation (requires prior CO provisioning of User IP address and ports)
    - Exchange of unencrypted analog voice messages
    - Exchange of unencrypted digital voice messages
    - Exchange of externally-encrypted digital voice messages
    - Exchange of unencrypted digital packet data messages
    - Exchange of externally-encrypted digital packet data messages
    - Exchange of internally encrypted encapsulated voice and packet data messages using DTLS
    - Exchange of Project 25 Radio Control messages

4.3.RIC-Mz Services Available to the Authenticated Crypto-Officer

- Validate Crypto-Officer Name/Password: Entry of a CO Name and Password is required to access anything other than the "Home" page on the RIC-Mz. The only function supported by the "Home" page is entry of the CO Name/Password. Time retry restrictions are applied to minimize the success of automated attack.
- Change Crypto-Officer Name/Password: After entry of the valid Crypto-Officer Name/Password, the Crypto-Officer will be able to access a page which allows resetting of the Crypto-Officer Name/Password.
- Firmware Update: Update the module using a TLSv1.2 Red Ethernet encrypted connection and a browser file upload function. A second file containing the HMAC SHA-256 hash for the Firmware image must be uploaded to complete the firmware update process. If the hash value calculated by the RIC-Mz does not match the hash value contained in the second file upload, the update fails.
- Reset RIC-Mz: Force a power-up reset of the RIC-Mz.
- Version Query: The Crypto-Officer can access the revision information on the RIC-Mz firmware from a web page.
- Factory Default and Zeroize: The Crypto-Officer can initiate a reset of the RIC-Mz to factory defaults including Crypto-Officer Name and Password. Keys stored in firmware are zeroized by loading an empty firmware.
- Base Station Configuration: The Crypto-Officer can set up the Base Station/Configuration, IP address, ports etc. to be used by the RIC-Mz.

- IP Address: The Crypto-Officer can set the IP address that will be used by the RIC-Mz. TLSv1.2 and DTLSv1.2 parameters are factory configured and cannot be changed by the Crypto-Officer.

4.4.RIC-Mz Services Available Without a Role.

- Reset RIC-Mz by removing/restoring the main power connection
- Monitor LED Status
- Power-On Self-tests (run by power cycling)

5. Cryptographic Algorithms

5.1. Approved Algorithms

The RIC-Mz supports the following Approved algorithms*:

Table 5: Approved Algorithms

CAVP Cert. #	Algorithm	Mode/Method	Standard	Description	Use/ Function
C1775	AES	ECB, GCM[1]	SP 800-38A SP 800-38D SP 800-38F	Key Size: 256	Encryption, Decryption, Authentication GCM is used in TLSv1.2 and DTLSv1.2
Vendor Affirmed	CKG		SP 800-133	Key generation using unmodified output of the DRBG	Key generation
C1775	CVL	TLS KDF	SP 800-135rev1	SHA-384	Key Derivation
C1775	DRBG	Hash_DRBG	SP 800-90Arev1	SHA-256	Random Bit Generation

[1] AES GCM is used as part of TLS 1.2 cipher suites conformant to IG A.5, RFC 5288 and SP 800-52 Section 3.3.1. The construction of the 64-bit nonce_explicit part of the IV is deterministic via a monotonically increasing counter. The module ensures that that when the deterministic part of the IV uses the maximum number of possible values, a new session key is established. The module generates new AES-GCM keys if the module loses power.

CAVP Cert. #	Algorithm	Mode/Method	Standard	Description	Use/ Function
A881	ECDSA	Keypair Generation	FIPS PUB 186-4	P-521	Keypair Generation
C1775	HMAC	SHA-256	FIPS PUB 198-1	Key Size: 256	Message Authentication Used to verify integrity of Firmware Upload, verify passwords and for TLSv1.2.
C1775	RSA	SigGenPKCS1.5 SigVerPKCS1.5	FIPS PUB 186-4	n=2048 (SHA-384)	Signature Generation, Signature Verification
C1775	SHS	SHA-256 SHA-384	FIPS PUB 180-4	Secure Hashing	Message Digest Generation
Vendor Affirmed	KAS-SSC	P-521	SP 800-56A rev 3	EC DH Key agreement methodology provides 256 bits of encryption	Key Agreement during TLS 1.2
N/A	KTS	AES Cert. #C1775	SP800-38F	Key establishment methodology provides 256 bits of encryption strength	Key Encryption

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

5.2. Non-Approved but Allowed Algorithms

Table 6: Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use/ Function
NDRNG	N/A	Derived from PIC32 Thermal Noise Source to seed the SP800-90A Hash_DRBG

5.3.Critical Security Parameters (CSPs) and Public Keys

Table 7: CSP Definition

CSP	Description / Usage
KAS_Private	Private component of an ECC (P-521) key pair used for EC Diffie-Hellman shared secret generation.
KAS_SS (TLS Pre-master Secret)	The EC Diffie-Hellman shared secret. ECC: (security strength 256-bits).
TLS Master Secret	Derived from the TLS Pre-master Secret.
SC_EDK	AES GCM (256-bit) key used for symmetric encryption (including AES authenticated encryption) within TLS.
RIC-Mz Server Private Key	RSA private key for verifying the TLSv1.2 handshake for RIC-Mz server connections.
RIC-Mz Client Private Key	RSA Public Key for verifying the TLSv1.2 handshake for RIC-Mz client connections.
DRBG_Seed	4096 bits of entropy input derived from PIC32 Thermal Noise Source providing 256 bits of entropy.
DRBG_State	Hash_DRBG (SHA-256) state V (440-bit) and C (440-bit).
Crypto-Officer Password	8-12 character ASCII Password value stored in flash.
Firmware Load Key	HMAC-SHA-256 key used to authenticate firmware images loaded by the module.

Table 8: Public Keys

Public Key	Description / Usage
RIC-Mz Server X.509 Certificate	RSA certificate for initiating TLSv1.2 handshake for RIC-Mz server connections

RIC-Mz Client X.509 Certificate	RSA certificate for initiating TLSv1.2 handshake for RIC-Mz client connections
KAS_Public	ECC (P-521) key pair used for EC Diffie-Hellman shared secret generation.

5.4. CSP Access Types

Table 9: CSP Access Types

CSP Access Type	Description
C – Check CSP	Checks status and key identifier information of key
E- Entry	CSP is entered into the module
G – Generate CSP	Generate CSP using the SP 800-90A DRBG
U – Use CSP	Uses the CSP internally for encryption/decryption services
Z – Zeroize CSP	Zeroizes CSP

Table 10: CSP Access Types

CSP											**Role**		
Service	KAS_Private	KAS_SS	TLS Master Secret	SC_EDK	RIC-Mz Server Private Key	RIC-Mz Client Private Key	DRBG_Seed	DRBG_State	Crypto-Officer Password	Firmware Load Key	User Role	Crypto-Officer Role	No Role Required
Validate Crypto-Officer Name/Password	-	-	-	-	-	-	-	-	C	-		✓	
Change Crypto-Officer Name/Password	-	-	-	-	-	-	-	-	G, U	-		✓	

CSP											Role		
Firmware Update	-	-	-	-	Z	Z	-	-	Z	E, U, Z		✓	
Reset RIC-Mz	Z	Z	Z	Z	-	-	Z	Z	-	-		✓	✓
Version Query	-	-	-	-	-	-	-	-	U	-		✓	
Factory Default/Zeroize[2]	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z		✓	
Base Station Configuration	-	-	-	-	-	-	-	-	U	-		✓	
IP Address	-	-	-	-	-	-	-	-	-	-		✓	
Project 25 Operation	G, U	G, U	G, U	G, U	G, U	G, U	G, U	G, U	-	-	✓		
Monitor Status LED Status	-	-	-	-	-	-	-	-	-	-		✓	✓
Power On Self-Tests	-	-	-	-	-	-	-	-	-	-		✓	✓

6. Physical Security

The RIC-Mz is a production grade, multi-chip standalone cryptographic module as defined by FIPS 140-2 and is designed to meet Level 2 Physical Security requirements.

The RIC-Mz is entirely contained within an aluminum production grade enclosure. All RIC-Mz functionality is provided by a single printed circuit board. The cryptographic boundary for the RIC-Mz is the outer enclosure of the module. Disassembly of the RIC-Mz is prevented by removal of the screw head patterns and epoxying the 8 screws during factory assembly.

No maintenance access interface is available.

7. Self-Tests

1. The RIC-Mz performs the following self-tests:
    a. Power up and On-Demand tests:
        i. Firmware Integrity Test (HMAC SHA-256)
        ii. AES-256 ECB (Cert. #C1775) encrypt/decrypt KAT
        iii. AES-256 GCM (Cert. #C1775) encrypt/decrypt KAT
        iv. HMAC SHA-256 (Cert. #C1775) KAT
        v. SHA-256 (Cert. #C1775) KAT
        vi. SHA-384 (Cert. #C1775) KAT

[2] Keys stored in firmware are zeroized by loading an empty firmware.

vii. DRBG (Cert #C1775) KAT
viii. RSA Sign/Verify (Cert. #C1775) KAT
ix. TLS KDF (Cert. #C1775) KAT

b. Conditional Tests:
   i. Firmware load test
   ii. NDRNG Continuous test

c. Critical Functions Test
   i. SP 800-90A DRBG Section 11.3 Health Checks

8. Mitigation of Other Attacks Policy

The RIC-Mz is not designed to mitigate any specific attacks outside those required by FIPS 140-2, including but not limited to power consumption, timing, fault indication, or TEMPEST attacks.

9. Security Rules and Guidance

The RIC-Mz enforces the following security rules:

9.1.FIPS 140-2 Imposed Security Rules

1. The RIC-Mz inhibits all input and output data paths whenever an error state exists or during self-tests.
2. Authentication data is not output during entry.
3. The RIC-Mz enforces Role-Based authentication.
4. The RIC-Mz supports a Crypto-Officer Role and a User Role.
    a. The Crypto-Officer is authenticated by entry of a CO Name and Password on the TLSv1.2 encrypted Red Ethernet interface.
    b. The User requires prior provisioning (IP addresses and port numbers) entered by the Crypto-Officer.
5. The RIC-Mz reauthenticates the Crypto-Officer when powered off, when an IP session times out due to inactivity and after the Crypto-Officer logs off and attempts to log back in to the RIC-Mz.
6. The RIC-Mz implements all firmware using a high-level language. The firmware is loaded as a single non-modifiable executable image running on an infinite loop "bare metal" processor without an operating system.
7. The RIC-Mz stores all CSPs in volatile RAM that is erased at the end of each connection session.
8. The RIC-Mz denies access CSPs contained within the module.
9. The RIC-Mz conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A requirements.
10. The RIC-Mz enters a Critical Error state if the Cryptographic Algorithm Test or the NDRNG test fails.
11. The RIC-Mz enters a firmware failure state if the Firmware Load test fails.
12. If all power up self-tests pass, the yellow Main LED will begin to flash at a 25 per second rate.
13. The RIC-Mz will not perform any cryptographic operations while in an error state.
14. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

9.2.Christine Wireless, Inc. Imposed Security Rules

The following security rules are established by Christine Wireless, Inc. for the RIC-Mz;

1. All connections to the RIC-Mz web server must be https.
2. Only one https connection at a time is permitted.
3. The https web connection is limited to only one TLSv1.2 mode: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, 256-bit keys, TLS 1.2.

4. All web pages with sensitive content can only be accessed after entering the Crypto-Officer User Name and Password. Per this SP, the User is required to enter a new User Name and Password to replace the factory defaults (admin, dhsricm) prior to setting up the RIC-Mz for the first time.
5. The Crypto-Officer is responsible for setting up the module User role connections in accordance with the Setup section in the following link: https://www.christinewireless.com/wp-content/uploads/2018/06/RIC-M_SetupInfo_06.26.18.pdf

9.3. Crypto-Officer and User Guidance

Administration of the RIC-Mz in a secure manner (Crypto-Officer)

The RIC-Mz requires no special administration for secure use after it is setup for use in a FIPS Approved manner.

Assumptions regarding User Behavior

The RIC-Mz has been designed in such a way that no special assumptions regarding User Behavior have been made that are relevant to the secure operation of the unit.

Approved Security Function, Ports and Interfaces available to Users

The RIC-Mz services available to the User Role are listed in section 8.2.

User Responsibilities necessary for Secure Operation

No special responsibilities are required of the User for secure operation of the RIC-Mz.

10. Definitions

AES	Advanced Encryption Standard
ALGID	Algorithm Identifier
CBC	Cipher Block Chain
CSP	Critical Security Parameter
DTLS	Datagram Transport Layer Security
ECB	Electronic Code Book
GCM	Galois Counter Mode
HMAC	Keyed Message Authentication Code
IV	Initialization Vector
LED	Light Emitting Diode
DRBG	Deterministic Random Bit Generator
NDRNG	Non-Deterministic Random Number Generator
OFB	Output Feed Back encryption
RAM	Random Access Memory
TLS	Transport Layer Security