



**GE MDS LLC**

**Orbit MCR and Orbit ECR**

**FIPS 140-2 Cryptographic Module  
Non-Proprietary Security Policy**

**Version: 2.9**

**Date: 2020-03-12**

# Table of Contents

<b>1</b>	<b>Introduction .....</b>	<b>4</b>
1.1	Variants and Order Packages .....	4
1.2	Hardware and Physical Cryptographic Boundary.....	7
1.2.1	Excluded Components .....	8
1.3	Firmware and Logical Cryptographic Boundary .....	8
1.4	Modes of Operation .....	8
<b>2</b>	<b>Cryptographic Functionality.....</b>	<b>9</b>
2.1	Critical Security Parameters .....	16
2.2	Public Keys.....	20
<b>3</b>	<b>Roles, Authentication and Services.....</b>	<b>21</b>
3.1	Assumption of Roles.....	21
3.2	Authentication Methods .....	22
3.2.1	Normal Password .....	22
3.2.2	One Time Password .....	22
3.3	Services.....	22
<b>4</b>	<b>Self-tests.....</b>	<b>27</b>
<b>5</b>	<b>Physical Security Policy .....</b>	<b>30</b>
<b>6</b>	<b>Operational Environment .....</b>	<b>31</b>
<b>7</b>	<b>Mitigation of Other Attacks .....</b>	<b>31</b>
<b>8</b>	<b>Security Rules and Guidance.....</b>	<b>32</b>
<b>9</b>	<b>References and Definitions.....</b>	<b>33</b>

## List of Tables

Table 1 – Small Form Factor Cryptographic Module Configurations.....	4
Table 2 – Large Form Factor Cryptographic Module Configurations.....	5
Table 3 – Security Level of Security Requirements.....	6
Table 4 – Ports and Interfaces .....	7
Table 5 – Approved and CAVP Validated Cryptographic Functions.....	9
Table 6 – Approved Cryptographic Functions Tested with Vendor Affirmation.....	12
Table 7 – Non-Approved but Allowed Cryptographic Functions .....	13
Table 8 – Protocols Allowed in FIPS Mode*.....	14
Table 9 – Critical Security Parameters (CSPs) .....	16
Table 10 – Public Keys.....	20
Table 11 – Roles Description.....	21
Table 12 – Authenticated Services.....	22
Table 13 – Unauthenticated Services .....	24
Table 14 – CSP Access Rights within Services .....	25
Table 15 – Public Key Access Rights within Services.....	26
Table 16 – Power Up Self-tests .....	27
Table 17 – Conditional Self-tests .....	28
Table 18 – Physical Security Inspection Guidelines .....	31
Table 19 – References.....	33
Table 20 – Acronyms and Definitions .....	33

## List of Figures

Figure 1 – Module (Large Form Factor on left (MCR), Small Form Factor on right (ECR)) .....	7
Figure 2 – Tamper Seal Location (Large Form Factor) .....	30
Figure 3 – Tamper Seal Location (Small Form Factor) .....	30

# 1 Introduction

This document defines the Security Policy for the GE MDS Orbit Multiservice Connect Router (MCR) and Edge Connect Router (ECR) module family, hereafter denoted the Module. The Module is a secure wireless communications device, which operates on cellular bands (2G/3G/4G LTE), licensed and unlicensed bands, and 802.11 Wi-Fi. The Module meets FIPS 140-2 overall Level 2 requirements.

## 1.1 Variants and Order Packages

The Module validation encompasses the following components:

- **Chassis:** ECR Chassis v1.0, MCR Chassis v1.0
- **Internal components:** U91, L1B, L2X, L2B, L4A, L4E, L4C, L7A, L7W, L9C, 4G1, 4G2, 4G3, 4G4, 4G5, 4GP, 4GY, 4GZ, 4GA, E4S, E42, W51, W52, 3G1, NNN. These do not perform cryptographic operations.
- **Platform boards:** ECR: 1; MCR: 1, 2 and 3. Changes to these result in a new designated type.
- **Orbit Firmware** v7.1.1

These components are included with other options (e.g. faceplates, special handling, mounting brackets) to create an order package, as described in Tables 1 and 2 (below). The possible order packages are defined by a 21 character configuration string that is constructed upon order entry and determines which options are populated in the factory. The columns shown in gray, are for items that have no impact on the cryptographic modules (e.g. country/regulatory, safety certification, reserved fields). The NICs and GPS are not security relevant because they do not perform cryptographic operations or process critical security parameters (CSPs).

The Module is a multi-chip standalone embodiment; the cryptographic boundary is the device chassis.

**Table 1 – Small Form Factor Cryptographic Module Configurations**

Orbit ECR Product Configurations (21 Characters)																																																																																																																																																																																																																								
HARDWARE SPECIFIC FIELDS	1	2	3	NIC OPTION #1			7	NIC OPTION #2			11	12	PLATFORM BOARD	MOUNTING BRACKETS	FACEPLATE	16	17	18	19	20	SPECIAL HANDLING																																																																																																																																																																																																			
	4	5	6	8	9	10	13	14	15	21																																																																																																																																																																																																														
VALID COMBINATIONS	E	C	R	U91	1	W51	N	S	1	N	S	1	N	D	1	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																																																															
				L1B											2											NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																																								
				L2X																																													N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																
				L2B																																																																					N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																								
				L4A																																																																																													N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																
				L4E																																																																																																																					N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																								
				L4C																																																																																																																																													N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																
				L7A																																																																																																																																																																					N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																								
				L7W																																																																																																																																																																																													N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S
				L9C																																																																																																																																																																																																																				
4G1-5	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2		US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																																																															
4GP															N											NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																																								
E4S																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																
E42																																																																									N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																								
4GY																																																																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																
4GZ																																																																																																																									N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																								
4GA																																																																																																																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																
3G1																																																																																																																																																																									N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																								
W52																																																																																																																																																																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S
	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2		US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																																																															
															N											NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																																								
																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																
																																																																									N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																								
																																																																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																
																																																																																																																									N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																								
																																																																																																																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																
																																																																																																																																																																									N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																								
																																																																																																																																																																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S
	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2		US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																																																															
															N											NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																																								
																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																																																
																																																																									N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																																								
																																																																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																																																
																																																																																																																									N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																																								
																																																																																																																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																																																
																																																																																																																																																																									N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S																								
																																																																																																																																																																																																	N	NNN	N	S	1	N	S	1	N	S	1	N	D	2	US	CA	EU	BR	U	C	N	N	N	S
	N	NNN	N	S	1	N	S	1	N</																																																																																																																																																																																																															

**Table 2 – Large Form Factor Cryptographic Module Configurations**

Orbit MCR Product Configurations (21 Characters)																						
HARDWARE SPECIFIC FIELDS	1	2	3	4	NIC OPTION #1			8	NIC OPTION #2			12	GPS	14	PLATFORM BOARD	16	FACEPLATE	MOUNTING BRACKETS	19	20	SPECIAL HANDLING	
					5	6	7		9	10	11		13		15		17	18			21	
VALID COMBINATIONS	M	X	N	N	U91 L1B L2X L2B L4A L4E L4C L7A L7W L9C	N	N	N	N	N	N	N	N	N	S	1	F E B A Z M J S G H P Y U C X	2	N D S	U C X	N D S	N S F
				2												3						
				1												6						
				2												A						
				1												B						
				2												C						
				1												5						
				2												9						
				3												E						
				1												5						
				2												9						
				3												E						
			1	1																		
			2	7																		
			3	D																		
			1	4																		
			2	8																		
			1	1																		
			2	7																		
			3	F																		

The Module is intended for use by US Federal agencies and other markets that require FIPS 140-2 validated wireless network routers.

The FIPS 140-2 security levels for the Module are as follows:

**Table 3 – Security Level of Security Requirements**

Security Requirement	Level
Cryptographic Module Specification	2
Cryptographic 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	2
<b>Overall</b>	<b>2</b>

## 1.2 Hardware and Physical Cryptographic Boundary

The physical forms of the Module are depicted in Figure 1. The boundary is the chassis of the device. The Module relies on RF antennas as input/output devices.

The module has two form factors, both of which have multiple variants. All port possibilities are encompassed in Table 4.



**Figure 1 – Module (Large Form Factor on left (MCR), Small Form Factor on right (ECR))**

**Table 4 – Ports and Interfaces**

Port	Description	Logical Interface Type
Power input	10-60 V DC	Power
RJ-45 Eth Ports (1, 2, or 4*)	Ethernet ports (metal shielded)	Control in   Data in   Data out   Status out
RJ-45 Serial Ports (1 or 2*)	RS-232 or RS-485 (un-shielded)	Control in   Data in   Data out   Status out
USB Mini (type B)	Virtual console port	Control in   Data in   Data out   Status out
TNC port (0 or 1)	Licensed or unlicensed radio port	Control in   Data in   Data out   Status out
SMA ports (0, 1, 2, or 3, female)	Cellular radio and/or GPS port	Control in   Data in   Data out   Status out
RP-SMA port (0, 1, or 2, female)	802.11 Wi-Fi port	Control in   Data in   Data out   Status out
SIM card slot (0,1, or 2)	SIM card slot	Data in
LED Status indicators	Five (5) LEDs to indicate device status	Status out

\*Large Form Factor (MCR) only

### **1.2.1 Excluded Components**

In the MCR variant, the following components have been excluded:

- MAX3161 (serial transceiver)
- MAX3238 (serial transceiver)

These components are not security relevant and do not provide any cryptographic functionality. The data they process is taken directly from, or provided directly to, the module's ports and interfaces.

### **1.3 Firmware and Logical Cryptographic Boundary**

The module contains a processor card containing a CPU, RAM, FLASH, and firmware within the cryptographic boundary.

### **1.4 Modes of Operation**

The module supports both an Approved and a non-Approved mode of operation. The module is provided from the manufacturer in the non-approved mode. The Crypto Officer sets the mode of operation through the management interface. Internally, the module uses a boot parameter to explicitly operate in one of the modes of operation. To verify that a module is in the Approved mode of operation, the operator can query the FIPS Mode parameter through the system menu of any of the user interfaces.

FIPS mode for the device can be activated from the System menu in the UI. The user will be prompted for confirmation, as activating FIPS mode will result in a factory reset. A factory reset will clear all user settings, including CSPs. In addition, the non-Approved algorithms listed at the bottom of Section 2 are disabled.

Once the unit is brought into FIPS mode, default passwords and keys must be changed before the module will report that it has reached "FIPS operational status" (FIPS Approved mode + proper initialization). The user can query the FIPS operational status in the System menu in the UI. If these requirements have been met, FIPS operational status will be set to TRUE.

## 2 Cryptographic Functionality

The Module implements the FIPS Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

**Table 5 – Approved and CAVP Validated Cryptographic Functions**

Algorithm	Description	Cert #
<b>OpenSSL</b>		
AES	<a href="#">[FIPS 197, SP 800-38A]</a> Functions: Encryption, Decryption Modes: ECB, CBC, CFB-128, CTR Key sizes: 128, 192, 256 bits (ECB and CFB are 128-bit only)	4539
AES-CCM	<a href="#">[SP 800-38C]</a> Functions: Authenticated Encryption, Authenticated Decryption Key sizes: 128, 192, 256 bits	4539
AES-CMAC	<a href="#">[SP 800-38B]</a> Functions: Generation, Verification Key sizes: 128 bits	4539
AES-GCM*	<a href="#">[SP 800-38D]</a> Functions: Authenticated Encryption, Authenticated Decryption Key sizes: 128, 192, 256 bits	4539
CVL: KDF, Existing Application- Specific	<a href="#">[SP 800-135]</a> Functions: IKE v1 KDF, IKEv2 KDF, TLS v1.0/1.1 KDF, TLS 1.2 KDF, SSH KDF, SNMP KDF	1219
DRBG	<a href="#">[SP 800-90A]</a> Functions: CTR DRBG Modes: AES-256 Security Strengths: 256 bits	1496
DSA	<a href="#">[FIPS 186-4]</a> Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: 2048, 3072 bits	1210
HMAC	<a href="#">[FIPS 198-1]</a> Functions: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	2997

Algorithm	Description	Cert #
KTS	<a href="#">[SP800-38F §3.1]</a> Functions: Key Wrap, Key Unwrap Mode: AES-CBC + HMAC Strength: 128 or 256 bits	AES #4539 HMAC #2997
RSA	<a href="#">[FIPS 186-4, ANSI X9.31-1998, and PKCS #1 v2.1 (PKCS1.5)]</a> Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: 2048, 3072 bits	2471
SHA	<a href="#">[FIPS 180-4]</a> Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	3720
Triple-DES	<a href="#">[SP 800-20]</a> Functions: Encryption, Decryption Modes: TCBC Key sizes: 3-key	2416
<b>Mocana</b>		
AES	<a href="#">[FIPS 197, SP 800-38A]</a> Functions: Encryption, Decryption Modes: CBC, CTR Key sizes: 128, 192, 256 bits	5887
AES-KW	<a href="#">[SP 800-38F]</a> Functions: Key Wrap, Key Unwrap Mode: KW Key size: 128 bits	5887
CVL: KDF, Existing Application- Specific	<a href="#">[SP 800-135]</a> Functions: TLS v1.0/1.1 KDF, TLS 1.2 KDF	2118
DRBG	<a href="#">[SP 800-90A]</a> Functions: CTR DRBG (Derivation Function and Prediction Resistance Enabled) Modes: AES-256 Security Strengths: 256 bits	2450

Algorithm	Description	Cert #
DSA	<a href="#">[FIPS 186-4]</a> Functions: PQG Generation, PQG Verification, Key Pair Generation, Signature Generation, Signature Verification Key sizes: 2048, 3072 bits	1484
HMAC	<a href="#">[FIPS 198-1]</a> Functions: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	3864
KTS	<a href="#">[SP 800-38F]</a> Functions: Key Wrap, Key Unwrap Mode: AES-KW Strength: 128 bits	AES #5887
RSA	<a href="#">[FIPS 186-4 and PKCS #1 v2.1 (PKCS1.5)]</a> Functions: Key Pair Generation, Signature Generation, Signature Verification Key sizes: 2048, 3072 bits	3085
SHA	<a href="#">[FIPS 180-4]</a> Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	4639
Triple-DES	<a href="#">[SP 800-20]</a> Functions: Encryption, Decryption Modes: TCBC Key sizes: 3-key	2867
<b>Linux Kernel</b>		
AES	<a href="#">[FIPS 197, SP 800-38A]</a> Functions: Encryption, Decryption Modes: CBC, CTR Key sizes: 128, 192, 256 bits	5888
AES-CCM	<a href="#">[SP 800-38C]</a> Functions: Authenticated Encryption, Authenticated Decryption Key sizes: 128, 192, 256 bits	5888
AES-CMAC	<a href="#">[SP 800-38B]</a> Functions: Generation, Verification Key sizes: AES with 128 bits	5888

Algorithm	Description	Cert #
AES-GCM*	[SP 800-38D] Functions: Authenticated Encryption, Authenticated Decryption Key sizes: 128, 192, 256 bits	5888
AES-GMAC	[SP 800-38D] Functions: Generation and Verification of Message Authentication Code Key sizes: 128, 192, 256 bits	5888
SHA	[FIPS 180-4] Functions: Digital Signature Generation, Digital Signature Verification, non-Digital Signature Applications SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512	4640
Triple-DES	[SP 800-20] Functions: Encryption, Decryption Modes: TCBC Key sizes:3-key	2868
<b>IEEE 802.11 Crypto API</b>		
AES-KW	[SP 800-38F] Functions: Key Wrap, Key Unwrap Mode: KW Key size: 128 bits	5889
KTS	[SP 800-38F] Functions: Key Wrap, Key Unwrap Mode: AES-KW Strength: 128 bits	5889
<b>Libssh2</b>		
CVL: KDF, Existing Application- Specific	[SP 800-135] Functions: SSH KDF	1221

\* The module is compliant to IG A.5: GCM is used in the context of TLS and IPSec/IKEv2. In the event of power loss, GCM keys are re-established as part of the re-establishment of the TLS or IPSec channel. The above behavior ensures the same GCM IV is never used twice.

**Table 6 – Approved Cryptographic Functions Tested with Vendor Affirmation**

Algorithm	Description	IG Ref.
	[SP800-133] Function: Key Generation	IG D.12

Algorithm	Description	IG Ref.
CKG (Cryptographic Key Generation)	[133] Section 6.1 Asymmetric signature key generation using unmodified DRBG output	
	[133] Section 6.2 Asymmetric key establishment key generation using unmodified DRBG output	
	[133] Section 7.1 Direct symmetric key generation using unmodified DRBG output	
	[133] Section 7.3 Derivation of symmetric keys from a key agreement shared secret.	
	[133] Section 7.4 Derivation of symmetric keys from a pre-shared key	
	[133] Section 7.5 Derivation of symmetric keys from a password	
KDA, Key Extraction-then- Expansion	[SP 800-56C Rev 1] Functions: HMAC-SHA1 KDF PRF is used for expanding Group and Pairwise keys in 802.1x used by the NX/LN and Wi-Fi.	IG D.10
KDF, Password- Based	[SP 800-132] Options: PBKDF with Option 1a Functions: HMAC-based KDF SHA-256 with a 32-byte salt created from the username padded with zeros and 1024 rounds used to obfuscate the user password before storage. The user password is the input to the KDF and has a minimum length of 8 bytes. Keys derived from passwords, as shown in SP 800-132, may only be used in storage applications. The result is not used for generation of any MK material in FIPS mode.	IG D.6

**Table 7 – Non-Approved but Allowed Cryptographic Functions**

Algorithm	Description
Diffie-Hellman, non-compliant to SP800-56A	[IG D.8] Diffie-Hellman (CVL Cert. #1219, key agreement; key establishment methodology provides 112 or 128 bits of encryption strength) Diffie-Hellman (CVL Cert. #1221, key agreement; key establishment methodology provides 112 bits of encryption strength)
MD5 within TLS	[IG D.2] Use of MD5 along with SHA1 in TLS 1.0/1.1 KDF
NDRNG	[IG 7.15] Hardware Derived Non-Deterministic RNG, using a ring oscillator. Seeds the FIPS Approved DRBGs with 256 bits of strength. OpenSSL implementation seeds and reseeds with 1024 bits from the HW RNG. Mocana implementation seeds with 1152 bits and reseeds with 768 bits from the HW RNG.

Algorithm	Description
RSA, non-compliant to SP800-56B	<a href="#">[IG D.9]</a> RSA (key agreement; key establishment methodology provides 112 or 128 bits of encryption strength)
RSA, additional modulus sizes	<a href="#">[IG A.14]</a> RSA vendor affirmed moduli: 2049-3071 bits, 3073-16384 bits.

**Table 8 – Protocols Allowed in FIPS Mode\***

Protocol	Description
EAP-TLS	<a href="#">[IG D.9]</a> Uses the same cipher suites as TLS (see below). Used by IEEE 802.1x when performing mutual authentication, between Wi-Fi and NX/LN wireless devices and a RADIUS server. Uses Public Key (RSA or DSA) keys and X.509 Certificates.
IKE v1	<a href="#">[IG D.8 and SP 800-135]</a> Key Exchange Mechanisms: Oakley Groups 14 & 15, DH key agreement with Pre-Shared Key and RSA authentication Session Encryption: 3DES-CBC, AES-CBC, & AES-CTR encryption Session Authentication: HMAC with SHA-1, SHA-256, SHA-384, SHA-512 Session Key Derivation: IKEv1 KDF with SHA-1, SHA-256, SHA-384, SHA-512
IKE v2	<a href="#">[IG D.8 and SP 800-135]</a> Key Exchange Mechanisms: Oakley Groups 14 & 15, DH key agreement with Pre-Shared Key and RSA authentication Session Encryption: 3DES-CBC, AES-CBC, AES-CTR, AES-GCM (w/ 16 octet ICV) encryption Session Authentication: HMAC-SHA1-96, HMAC-SHA1-160, AES-GCM (AEAD), AES-GMAC (128, 192, 256), HMAC-SHA-256-128, HMAC-SHA-384-192, HMAC-SHA-512-256 integrity Session Key Derivation: IKEv2 KDF with CMACSHA-1, SHA-256, SHA-384, or SHA-512.
SNMPv3	<a href="#">[IG D.8 and SP 800-135]</a> Session Encryption: AES-128-CFB Session Authentication: HMAC-SHA1-96
SSH v2	<a href="#">[IG D.8 and SP 800-135]</a> Key Exchange Mechanisms: DH Group Exchange SHA1 & SHA256, DH Group 14 SHA1 Session Encryption: 3DES-CBC, AES-CBC (128, 192, 256), AES-CTR (128, 192, 256) Session Authentication: HMAC-SHA1, HMAC-SHA256, HMAC-SHA512

Protocol	Description
TLS v1.0/v1.1/v1.2	<p data-bbox="456 254 740 285">[IG D.8 and SP 800-135]</p> <p data-bbox="456 300 732 331"><u>OpenSSL Cipher suites:</u></p> <p data-bbox="456 344 1003 1598">             TLS_DHE_DSS_WITH_AES_128_CBC_SHA              TLS_DHE_DSS_WITH_AES_128_CBC_SHA256              TLS_DHE_DSS_WITH_AES_128_GCM_SHA256              TLS_DHE_DSS_WITH_AES_256_CBC_SHA              TLS_DHE_DSS_WITH_AES_256_CBC_SHA256              TLS_DHE_DSS_WITH_AES_256_GCM_SHA384              TLS_DHE_RSA_WITH_AES_128_CBC_SHA              TLS_DHE_RSA_WITH_AES_128_CBC_SHA256              TLS_DHE_RSA_WITH_AES_128_GCM_SHA256              TLS_DHE_RSA_WITH_AES_256_CBC_SHA              TLS_DHE_RSA_WITH_AES_256_CBC_SHA256              TLS_DHE_RSA_WITH_AES_256_GCM_SHA384              TLS_DH_DSS_WITH_AES_128_CBC_SHA              TLS_DH_DSS_WITH_AES_128_CBC_SHA256              TLS_DH_DSS_WITH_AES_128_GCM_SHA256              TLS_DH_DSS_WITH_AES_256_CBC_SHA              TLS_DH_DSS_WITH_AES_256_CBC_SHA256              TLS_DH_DSS_WITH_AES_256_GCM_SHA384              TLS_DH_RSA_WITH_AES_128_CBC_SHA              TLS_DH_RSA_WITH_AES_128_CBC_SHA256              TLS_DH_RSA_WITH_AES_128_GCM_SHA256              TLS_DH_RSA_WITH_AES_256_CBC_SHA              TLS_DH_RSA_WITH_AES_256_CBC_SHA256              TLS_DH_RSA_WITH_AES_256_GCM_SHA384              TLS_PSK_WITH_AES_256_CBC_SHA              TLS_RSA_WITH_AES_128_CBC_SHA              TLS_RSA_WITH_AES_128_CBC_SHA256              TLS_RSA_WITH_AES_128_GCM_SHA256              TLS_RSA_WITH_AES_256_CBC_SHA              TLS_RSA_WITH_AES_256_CBC_SHA256              TLS_RSA_WITH_AES_256_GCM_SHA384           </p> <p data-bbox="456 1612 727 1644"><u>Mocana Cipher Suites:</u></p> <p data-bbox="456 1656 928 1808">             TLS_RSA_WITH_AES_128_CBC_SHA              TLS_RSA_WITH_AES_128_CBC_SHA256              TLS_RSA_WITH_AES_256_CBC_SHA              TLS_RSA_WITH_AES_256_CBC_SHA256           </p>

\*Protocols are not reviewed or tested by the CMVP or CAVP.

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

- DES
- MD5
- RC4
- RSA, DSA, and ECDSA, disallowed variants (e.g. 1024, 1536, and non-NIST curves)
- PBKDF2 used for MK generation for use with Option 1b and 2a
- Ed25519
- Curve25519
- ChaCha20
- Poly1305

## 2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

**Table 9 – Critical Security Parameters (CSPs)**

CSP	Description / Usage
<b>Static Server Keys</b>	
RSA Private Keys (X.509)	RSA (size 2048 to 16384 bits) private keys for various protocols which use X.509 certificates: TLS, IPSEC, EAP-TLS (for Wi-Fi device auth, licensed radio device auth, unlicensed radio device auth)  Can be generated or imported. Used for signatures (w/DH) or for RSA key transport.
DSA Private Keys (X.509)	DSA-2048 or DSA-3072 private keys for various protocols which use X.509 certificates: TLS, IPSEC, EAP-TLS (for WiFi device auth, licensed radio device auth, unlicensed radio device auth)  Can only be imported. Used for signature generation (w/ephemeral DH) or directly as a DH key (TLS_DH_* cipher suites).
SSH Private Keys	RSA and DSA private keys for SSH, size 2048 or 3072. Generated internally on initialization or manually. Used for signature generation (w/DH).
<b>TLS Ephemeral Keys</b>	
DH Private Key	DH-2048 or DH-3072 Private key used for PFS during a TLS exchange.
Master Secret	384-bit TLS Master Secret derived from DH exchange
Session Encryption Keys	TLS Session encryption keys (AES-128, AES-256, or 3-key Triple-DES).
Session Auth Keys	TLS Session authentication keys (HMAC-SHA-1, or HMAC-SHA-256)

CSP	Description / Usage
<b>EAP-TLS Ephemeral Keys</b>	
DH Private Key	DH-2048 or DH-3072 Private key used for PFS during a TLS exchange
Master Secret	384-bit TLS Master Secret derived from DH exchange
Session Encryption Keys	TLS Session encryption keys (AES-128, AES-256, or 3-key Triple-DES)
Session Auth Keys	TLS Session authentication keys (HMAC-SHA-1 or HMAC-SHA-256)
<b>EAPOL Keys</b>	
Pairwise Master Key	256-bit shared secret keying material. Established as part of mutual authentication performed using EAP-TLS exchange between client and RADIUS server (802.1X). Can also be pre-shared.
Key Confirmation Key	128-bit HMAC/SHA-1 key used for authentication of the EAPOL exchange. Derived from Pairwise Master Key using a KDF.
Key Encryption Key	128-bit AES-CBC key used in AES-KEYWRAP protocol to encrypt the Unicast Temporal Key. Derived from Pairwise Master Key using a KDF.
Unicast Temporal Key	128-bit (Wi-Fi) or 256-bit (NX/LN) AES-CCM key. Derived from Pairwise Master Key using a KDF. The first 128 bits of the 256 bits of key material is used when doing AES-128 (NX/LN).
Group Temporal Key	128-bit (Wi-Fi) or 256-bit (Nx/LN) AES-CCM key. Created by access point and distributed to all peers, wrapped with key encryption key (enc) and key confirmation key (auth). The first 128 bits of the 256 bits of key material is used when doing AES-128 (NX/LN).
Integrity Group Temporal Key	128-bit AES-CMAC key (Wi-Fi). Created by access point and distributed to all peers, wrapped with key encryption key (enc) and key confirmation key (auth).
<b>IKEv1 Keys</b>	
Pre-Shared Key	160-512 bit key used to authenticate/encrypt VPN tunnel when using IKEv1
SKEYID	160-512 bit keys used by each IKE SA to derive the other key material
SKEYID_d	160-512 bit keys used by each IKE SA to derive keys
SKEYID_e	Keys used by each IKE SA to protect the confidentiality of its messages (AES-128, AES-256, or 3-key Triple-DES)
SKEYID_a	Keys used by each IKE SA to authenticate messages (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, or HMAC-SHA-512)
Child SA Keys	128-512 bit keys used to protect each Child SA
<b>IKEv2 Keys</b>	
Pre-Shared Key	160-512 bit key used to authenticate/encrypt VPN tunnel when using IKEv2

CSP	Description / Usage
KEYSEED	160-512 bit keys used by each IKE SA to derive the other key material
SK_d	160-512 bit keys used to derive new keys for each Child SA
SK_ai	160-512 bit HMAC key used for authenticating the message exchanges from the Initiator to the Responder
SK_ar	160-512 bit HMAC key used for authenticating the message exchanges from the Responder to the Initiator
SK_ei	Used for encrypting messages from the Initiator to the Responder (AES-128, AES-256, or 3-key Triple-DES)
SK_er	Used for encrypting messages from the Responder to the Initiator (AES-128, AES-256, or 3-key Triple-DES)
SK_pi	160-512 bit HMAC keys used to generate the AUTH payload messages from the Initiator to the Responder
SK_pr	160-512 bit HMAC keys used to generate the AUTH payload messages from the Responder to the Initiator
Child SA Keys	128-512 bit keys used to protect each Child SA
SSH Ephemeral Keys	
Shared Secret	Derived from Diffie-Hellman 2048 Exchange
Exchange Hash	Derived from Diffie-Hellman 2048 Exchange
Session ID	The initial Exchange Hash between a Client and a Server (160-512 bits). Copied of Exchange Hash from first connection between a Client and a Server.
Client to Server Initial IV	Initial IV (64 or 128 bits) used with block ciphers for messages from the Client to the Server. Computed from Shared Secret, Exchange Hash, SSH Session ID and the byte "A" using the selected hash function.
Server to Client Initial IV	Initial IV (64 or 128 bits) used with block ciphers for messages from the Server to the Client. Computed from Shared Secret, Exchange Hash, SSH Session ID and the byte "B" using the selected hash function.
Client to Server Encryption Key	Used to encrypt data from Client to Server. Computed from Shared Secret, Exchange Hash, SSH Session ID and the byte "C" using the selected hash function. (AES-128, AES-256, or 3-key Triple-DES)
Server to Client Encryption Key	Used to encrypt data from Server to Client. Computed from Shared Secret, Exchange Hash, SSH Session ID and the byte "D" using the selected hash function. (AES-128, AES-256, or 3-key Triple-DES)
Client to Server Integrity Key	160-512 bit HMAC key used to verify data from Client to Server. Computed from Shared Secret, Exchange Hash, SSH Session ID and the byte "E" using the selected hash function.

CSP	Description / Usage
Server to Client Integrity Key	160-512 bit HMAC key used to verify data from Server to Client. Computed from Shared Secret, Exchange Hash, SSH Session ID and the byte "F" using the selected hash function.
<b>SNMPv3 Keys</b>	
Session Authentication Key	HMAC-SHA-1 key. Specified directly by security officer, or derived from passphrase via the SNMP KDF (SP800-135).
Session Encryption Key	AES-128 key. Specified directly by security officer, or derived from passphrase via the SNMP KDF (SP800-135).
<b>Remote Management protocol Keys</b>	
Pre-shared key	Pre shared key for remote management and to protect the programming protocol. Also used as a session HMAC (SHA1) key to provide authentication of Remote Management protocol handshake messages. (Size varies)
Remote Management programming session asymmetric private key	2048-bit RSA key that is generated at the start of each reprogramming session. (Multicast file transport)
Remote Management programming session symmetric key	AES-256 key generated by RSA Key exchange, for use with AES-256-CCM protection of data blocks. (Multicast file transport)
<b>Other Keys &amp; CSPs</b>	
Parameter Store encryption key	Encrypts values in the parameter database which are marked to be protected. (e.g., PSK values.) Initialized to default value. AES-128-CFB.
Certificate Store encryption key	Encrypts the certificate database (stored CSP data which is not in the parameter store). Initialized to default value. AES-256-CBC.
DRBG Seeds	Output values from the NDRNG to initialize the module's DRBGs. (≥768 bits)
DRBG States	Internal state values of the module's CTR DRBGs. (128-bit V, 256-bit Key)
<b>Passwords</b>	
Local passwords	Passwords used for operator authentication
RADIUS shared secret	Shared secret to mutually authenticate the RADIUS server and the module
One Time Passwords	Temporary passwords for one-time authentication

CSP	Description / Usage
SSH Client Shared Secret	Password used by the module to authenticate as a client to an external SSH server

## 2.2 Public Keys

**Table 10 – Public Keys**

Key	Description / Usage
RSA Public Keys (X.509)	<p>RSA (size 2048 to 16384 bits) public device keys for various protocols which use X.509 certificates: TLS, IPSEC, EAP-TLS (for WiFi device auth, licensed radio device auth, unlicensed radio device auth)</p> <p>Can be generated or imported, although generation requires external signing by a CA. Passed to client; used for signatures (w/DH) or for RSA key transport.</p>
DSA Public Keys (X.509)	<p>DSA-2048 or DSA-3072 public device keys for various protocols which use X.509 certificates: TLS, IPSEC, EAP-TLS (for WiFi device auth, licensed radio device auth, unlicensed radio device auth)</p> <p>Can only be imported. Passed to client; used for signatures (w/DH).</p>
CA Public Keys (X.509)	<p>RSA (size 2048 to 16384 bits) or DSA public keys (size 2048 or 3072) corresponding to certificate authorities; for various protocols which use X.509 certificates: TLS, IPSEC, EAP-TLS (for WiFi device auth, licensed radio device auth, unlicensed radio device auth)</p> <p>Can only be imported.</p>
SSH Public Keys	RSA and DSA public keys for SSH (size 2048 or 3072). Generated internally on initialization or manually. Passed to client; used for signatures (w/DH).
Firmware package verification key	Used to verify new firmware packages. RSA-3072 with SHA-256.
HAB public key	RSA-3072 with SHA-256 to perform firmware integrity checking on boot.
TLS DH public key	DH-2048 or DH-3072 Public key used for PFS during a TLS exchange. Derived from TLS exchange.
Remote Management programming session asymmetric public key	RSA-2048 public key generated from the Remote Management programming session asymmetric private key at the start of each transmission of a data block. (Multicast file transport)

### 3 Roles, Authentication and Services

#### 3.1 Assumption of Roles

The module supports five (5) distinct operator roles: Admin (CO), Tech, Oper (User), SNMP, and Factory Reset. The cryptographic module enforces the separation of roles using individual sessions per operator. Re-authentication is enforced when changing roles. The module clears all authenticated sessions on power cycle.

The table below lists all operator roles supported by the module. The Module does not support a maintenance role or bypass capability. The Module supports concurrent operators, with the exception that each physical or virtual serial port can only support one operator at a time. The module supports a maximum of five (5) concurrent operators, which are physically separated by separate ports or logically separated by separate sessions. However, an Admin operator is always able to log in, in which case the Admin selects a currently active operator to be logged out.

Passwords (including One Time Passwords) are stored in the module in hashed form (1024-round PBKDF2 with HMAC/SHA-256) and are considered CSPs. Entered passwords are either manually distributed over a local channel (e.g., serial connection) or logically protected by an encrypted channel (e.g., TLS, SSH).

**Table 11 – Roles Description**

Role ID	Role Description	Authentication Type	Authentication Data
Admin (CO)	Access to all module functionality	Role-based	Username & Password
		Role-based	One-Time Password
		Role-based	RADIUS
Tech	Read/write access of non-CSPs; can also set own password	Role-based	Username & Password
		Role-based	RADIUS
Oper (User)	Read-only operations	Role-based	Username & Password
		Role-based	RADIUS
SNMP	Read-only operations over SNMP	Identity-based	ID & Password to derive SNMPv3 session key(s)
Factory Reset	Reset the module to factory defaults	Role-based	One-Time Password

## 3.2 Authentication Methods

### 3.2.1 Normal Password

The module can use password-based authentication over CLI (Serial, USB, or SSH) the WebUI, NETCONF, or SNMPv3. By default, the module enforces a minimum length of eight (8) characters, including one (1) capital, one (1) lowercase, and one (1) numerical character. The Admin role can modify the requirements but cannot reduce the minimum length.

For a worst-case scenario, the Admin may require that a password contain eight (8) numeric characters, in which case a minimum-length password would be all numeric. The resulting probability of false authentication would be 1 in  $10^8$ , which is less than 1 in 1,000,000.

The module allows 60 password attempts per minute. This is enforced by the time it takes the module to calculate a password hash with PBKDF2 (see Section 3.1). Combining this with the worst-case password complexity scenario, a one-minute session of random login attempts would have a success probability of 1 in 1,670,000, which is less than 1 in 100,000.

Note that the use of RADIUS does not affect the above password requirements.

### 3.2.2 One Time Password

The one-time password is a random 40-byte binary value. The value is hashed with PBKDF2 (see Section 3.1 for specifics) and compared against a stored digest.

Since the value is fully random, the probability of false authentication for a One Time Password is 1 in  $256^{40}$  (1 in approximately  $2.14 \times 10^{96}$ ), which is less than 1 in 1,000,000. The same velocity checking described in Section 3.2.1 applies (60 attempts per minute), which means the success probability of a one-minute attack is 1 in  $3.56 \times 10^{94}$ , which is less than 1 in 100,000.

## 3.3 Services

All services implemented by the Module are listed in the tables below. Each service description also describes all usage of CSPs by the service. These services are available in the Approved mode and in the non-Approved mode.

**Table 12 – Authenticated Services**

Service	Description	Admin	Tech	Oper	SNMP	Fact. Reset
Local User Authentication	Authenticate locally with a fixed username and password.	X	X	X		
RADIUS User Authentication	Authenticate remotely using RADIUS	X	X	X		
Authentication Data Management	Configure and change RADIUS shared secret, and passwords for all operators, excluding OTPs	X				
Update Tech Password	Admin or Tech user updates Tech password	X	X			

Service	Description	Admin	Tech	Oper	SNMP	Fact. Reset
Generate OTP	Generate a One-Time Password for Admin or Factory Reset	X				
One-Time Password Authentication	Authenticate using a One-Time Password (OTP)	X				X
SNMP Session	Authenticate and query using an SNMP session (SNMPv3 in FIPS mode, SNMPv1/v2c/v3 in non-FIPS mode)				X	
SSH Session	Establish a session with a client using the SSH Service	X	X	X		
SSH Client Session	Use SSH client to connect to remote SSH server.	X	X	X		
Web UI Session	Establish a Web session with a client via the WebUI service (HTTPS in FIPS mode, HTTP or HTTPS in non-FIPS mode)	X	X	X		
SSH Server Management	Generate private/public key pair for use by SSH service	X				X
Remote Management Service	Reprogram a device remotely via a secure file transfer	X	X			
IPSec/IKE VPN	Configure the secure end-to-end IP links, which use IPsec VPN and a pre-shared key or certificate-based setup	X				
PKI/Certificate Management	Generate/upload private keys/certificates for use in certificate-based security setup.	X				
Ethernet Device Authentication	Configure the IEEE 802.1X based authentication and MAC authentication bypass (MAB) based authentication.	X				
WiFi Device Security	Configure secure Wi-Fi link which uses a pre-shared key or EAP-TLS/RADIUS using certificates.	X				
NX/LN Device Security	Configure the secure radio link which uses a pre-shared key or EAP-TLS/RADIUS using certificates.	X				

Service	Description	Admin	Tech	Oper	SNMP	Fact. Reset
Event Logging	Securely send event logs to central SYSLOG sever by configuring SYSLOG over TLS.	X	X			
Show Status	View module status parameters.	X	X	X	X	
Reset to factory settings	Resets the module to factory settings.	X				X

The majority of the module’s authenticated services are for configuration purposes. Most of these are available over multiple interfaces – HTTPS, NETCONF, SSH, etc. Configuration of cryptography-related functionality is restricted to the Admin (CO) role. The Tech role is restricted to the configuration of non-cryptographic functionality.

**Table 13 – Unauthenticated Services**

Service	Description
Self-tests	Run self-tests by power cycling the module.
General network services	Communicate on a network; provide DHCP, DNS, NTP, SNTP, NHRP, etc.

Without authentication, the module is limited to generic network services. Unauthenticated operators cannot modify module CSPs in any way.

Table 14 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as:

- G = Generate: The module generates the CSP.
- R = Read: The module reads the CSP, and exports it from the module.
- E = Execute: The module executes using the CSP.
- W = Write: The module writes the CSP with specified data.
- Z = Zeroize: The module zeroizes the CSP.

**Table 14 – CSP Access Rights within Services**

Service	CSPs																			
	RSA Private Keys (X.509)	DSA Private Keys (X.509)	SSH Private Keys	TLS Ephemeral Keys	EAP-TLS Ephemeral Keys	EAPOL Pairwise Master Key	Other EAPOL Keys	IKEV1 Keys	IKEV2 Keys	SSH Ephemeral Keys	SNMPv3 Keys	Static Remote Management Protocol Keys	Ephemeral Remote Mgmt Protocol Keys	Parameter Store encryption key	Certificate Store encryption key	DRBG Seeds and DRBG States	Local passwords	RADIUS Shared Secret	One Time Passwords	SSH Client Shared Secret
Local User Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	GEZ	WE	--	--	--
RADIUS User Authentication	--	--	--	--	--	--	--	--	--	--	--	--	--	E	--	GEZ	--	E	--	--
Auth. Data Management	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	W	W	--	--
Update Tech Password	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	GEZ	W*	--	--	--
Generate OTP	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	GEZ	--	--	GRZ	--
OTP Auth.	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	WEZ	--
SNMP Session	--	--	--	--	--	--	--	--	--	GEZ	--	--	E	--	GEZ	--	--	--	--	--
SSH Session	--	--	E	--	--	--	--	--	--	GEZ	--	--	--	--	GEZ	--	--	--	--	--
SSH Client Session	--	--	--	--	--	--	--	--	--	GEZ	--	--	--	--	GEZ	--	--	--	--	RE
Web UI Session	E	E	--	GEZ	--	--	--	--	--	--	--	--	--	E	GEZ	--	--	--	--	--
SSH Server Management	--	--	GW	--	--	--	--	--	--	--	--	--	--	--	GEZ	--	--	--	--	--
Remote Management	--	--	--	--	--	--	--	--	--	--	--	WE	GEZ	E	--	GEZ	--	--	--	--
PKI/Certificate Management	GWEZ	GWEZ	--	--	--	--	--	--	--	--	--	--	E	WE	GEZ	--	--	--	--	--
IPSec/IKE VPN	--	--	--	--	--	--	--	WGEZ	WGEZ	--	--	--	--	E	GEZ	--	--	--	--	--
Ethernet Device Authentication	E	E	--	GEZ	GEZ	E	WGEZ	--	--	--	--	--	E	E	GEZ	--	--	--	--	--
Wi-Fi Device Security	E	E	--	GEZ	GEZ	GWEZ	WGEZ	--	--	--	--	--	E	E	GEZ	--	--	--	--	--
NX/LN Device Security	E	E	--	GEZ	GEZ	GWEZ	WGEZ	--	--	--	--	--	E	E	GEZ	--	--	--	--	--
Event Logging	E	E	--	GEZ	--	E	--	--	--	--	--	--	--	E	GEZ	--	--	--	--	--
Show Status	--	--	--	--	--	--	--	--	--	--	R	R	--	--	R	--	--	R	--	R
Reset to factory settings	ZG**	Z	ZG**	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z

\* For the Tech role, password change is limited to the role’s own password.

\*\* “ZG” keys are zeroized and then replaced with newly generated values.

**Table 15 – Public Key Access Rights within Services**

Service	Public Keys							
	RSA Public Keys (X.509)	DSA Public Keys (X.509)	CA Public Keys (X.509)	SSH Public Keys	FW Package Verification Key	HAB public key	TLS DH Public Key	Remote Management Asymmetric Public Key
Local User Authentication	-	-	-	-	-	-	-	-
RADIUS User Authentication	--	--	--	--	--	--	--	--
Auth. Data Management	-	-	-	-	-	-	-	-
Update Tech Password	--	--	--	--	--	--	--	--
Generate OTP	-	-	-	-	-	-	-	-
OTP Auth.	--	--	--	--	--	--	--	--
SNMP Session	--	--	--	--	--	--	--	--
SSH Session	--	--	--	E	--	--	--	--
SSH Client Session	--	--	--	--	--	--	--	--
Web UI Session	RE	RE	E	--	--	--	GEZ	--
SSH Server Management	--	--	--	GW	--	--	--	--
Remote Management	--	--	--	--	--	--	--	WE
PKI/Certificate Management	GWEZ	GWEZ	GWEZ	--	--	--	--	--
IPSec/IKE VPN	--	--	--	--	--	--	--	--
Ethernet Device Authentication	RE	RE	E	--	--	--	GEZ	--
Wi-Fi Device Security	RE	RE	E	--	--	--	GEZ	--
NX/LN Device Security	RE	RE	E	--	--	--	GEZ	--
Event Logging	RE	RE	E	--	--	--	GEZ	--
Show Status	--	--	--	--	--	--	--	R
Reset to factory settings	ZG*	Z	Z	ZG*	E	E	Z	Z

\* "ZG" keys are zeroized and then replaced with newly generated values.

## 4 Self-Tests

Each time the Module is powered up, it tests that the cryptographic algorithms still operate correctly and that the firmware has not been damaged. Power up self-tests are available on demand by power cycling the module.

On power up or reset, the Module performs the self-tests described in Table 16 below. All power-on self-tests must be completed successfully prior to any other use of cryptography by the Module. If any of the KATs fail, the Module enters the SOFT ERROR 1 state and reboots. If the Firmware Integrity test fails, the module either enters the HARD ERROR 1 state and halts (bootloader integrity failure) or enters the HARD ERROR 2 state and reboots (post-bootloader integrity failure).

The module will try to recover from Conditional Self-Test failures (SOFT ERROR 2 to retry the action or re-instantiate the library, and SOFT ERROR 3 to reject bad firmware); if this fails, the module enters the SOFT ERROR 1 state and reboots.

**Table 16 – Power Up Self-Tests**

Test Target	Description
Firmware Integrity	RSA 3072 / SHA-256 verification of internal firmware on boot.
<b>OpenSSL</b>	
AES Cert. #4539	KATs: Encryption, Decryption Mode: ECB Key sizes: 128 bits
CCM Cert. #4539	KATs: Encryption, Decryption Key sizes: 192 bits
CMAC Cert. #4539	KATs: Generation, Verification Key sizes: AES (128, 192, 256 bits), Triple-DES (192 bits)
DRBG Cert. #1496	KATs: HASH DRBG, HMAC DRBG, CTR DRBG Security Strengths: 128, 192, 256 bits
DSA Cert. #1210	PCT: Signature Generation, Signature Verification Key sizes: 2048 bits
GCM Cert. #4539	KATs: Encryption, Decryption Key sizes: 256 bits
HMAC Cert. #2997	KATs: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
RSA Cert. #2471	KATs: Signature Generation, Signature Verification Key sizes: 2048 bits
SHA Cert. #3720	KATs: SHA-1
Triple-DES Cert. #2416	KATs: Encryption, Decryption Modes: TECCB Key sizes: 3-key
<b>Mocana</b>	
AES Cert. #5887	KATs: Encryption, Decryption Modes: ECB, CBC, CTR, CFB Key sizes: 256 bits (128 for CFB)

Test Target	Description
DRBG Cert. #2450	KATs: CTR DRBG Modes: AES-256 Security Strengths: 256 bits
DSA Cert. #1484	PCT: Signature Generation, Signature Verification Key sizes: 2048 bits
HMAC Cert. #3864	KATs: Generation, Verification SHA sizes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
RSA Cert. #3085	KATs: Signature Generation, Signature Verification Key sizes: 2048 bits
SHA Cert. #4639	KATs: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
Triple-DES Cert. #2867	KATs: Encryption, Decryption Modes: TCBC, Key sizes: 3-key
<b>Linux Kernel</b>	
AES Cert. #5888	KATs: Encryption, Decryption Modes: CBC, CTR Key sizes: 128, 192, 256 bits
CCM Cert. #5888	KATs: Encryption, Decryption Key sizes: 128 bits
GCM Cert. #5888	KATs: Encryption, Decryption Key sizes: 128, 192, 256 bits
SHA Cert. #4640	KATs: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512
Triple-DES Cert. #2868	KATs: Encryption, Decryption Modes: TECB, TCBC Key sizes: 3-key
CMAC Cert. #5888	KATs: Generation, Verification Key sizes: AES with 128 bits
<b>IEEE 802.11 Crypto API</b>	
AES Cert. #5889 and Cert. #4539	KATs: Encryption, Decryption Modes: AES-KW Security Strengths: 128 bits Note: AES-KW Cert. #5889 uses the AES Cert. #4539 from OpenSSL, which provides the underlying KAT.

**Table 17 – Conditional Self-tests**

Test Target	Description
DRBG Health Checks	Performed conditionally per SP 800-90A-rev1 Section 11.3.
NDRNG	NDRNG Continuous Test performed when a random value is requested from the NDRNG.

Test Target	Description
DRBG Certs. #1496 and #2450	DRBG Continuous Test performed when a random value is requested from the DRBG.
DSA Certs. #1210 and #1484	DSA Pairwise Consistency Test performed on every DSA key pair generation.
RSA Certs. #2471 and #3085	RSA Pairwise Consistency Test performed on every RSA key pair generation.
Firmware Load	RSA 3072 / SHA-256 signature verification performed when firmware is loaded.

## 5 Physical Security Policy

The module is encased in a metal enclosure, protected by a tamper-evident seal. Each form factor contains one (1) seal, which is placed on the left side of the device in the factory (see Figures 2 and 3). Ensure the seal is in-place at the location shown in the figures below, and that neither it nor the module enclosure have been damaged. During operational usage, it is recommended to inspect the seal and enclosure once every three months (Table 18). If the magnetometer (see Section 7) is active and calibrated, it is also recommended to inspect the tamper seal if the magnetometer logs an event.



**Figure 2 – Tamper Seal Location (Large Form Factor)**



**Figure 3 – Tamper Seal Location (Small Form Factor)**

**Table 18 – Physical Security Inspection Guidelines**

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Evident Seal	3 months; whenever magnetometer logs an event (if active)	Verify that the tamper evident seal placed on the side of the chassis is intact and shows no sign of delamination. See Figures 2 and 3 above for seal placement.
Module enclosure	Same as above	Verify that the module enclosure does not show any sign of forced entry. Verify that the black cover (reading “MDS ORBIT MCR” or “MDS ORBIT ECR”) has not been removed or damaged.

If the above guidelines yield evidence of tamper, the Administrator should assume the module has been physically compromised, perform zeroization, and take system-level precautions as needed (e.g., revoke the trust of the module’s certificates on other systems).

## 6 Operational Environment

The Module is designated as a limited operational environment under the FIPS 140-2 definitions. The Module includes a firmware load 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 firmware loaded into this module is out of the scope of this validation and will require a separate FIPS 140-2 validation.

## 7 Mitigation of Other Attacks

The unit contains a three-axis magnetometer that can be used to detect changes in the unit’s “magnetic environment” after installation (e.g., if the module is moved such that local magnetic fields change, or if a metal cabinet containing the Module is opened, or if the metal chassis of the Module itself is opened) and generate notification of the change if it exceeds configurable thresholds.

This does not provide Level 3 physical security (e.g., tamper response) but can be used in conjunction with the tamper evident seal to remotely detect and then locally verify that tamper has occurred.

## 8 Security Rules and Guidance

The Module design corresponds to the Module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The module provides five (5) distinct operator roles: Admin (CO), Tech, Oper (User), SNMP, and Factory Reset.
2. The module provides a combination of role-based and identity-based authentication.
3. The module clears previous authentications on power cycle, as all session data is stored in volatile memory (RAM and tmpfs).
4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services aside from those allowed by IG 3.1.
5. The operator can command the module to perform the power up self-tests by cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output is inhibited during self-tests, zeroization, and error states. Data output is logically disconnected from the processes performing key generation. The network interface manager does not start up interfaces until long after FIPS tests are complete.
8. The UI provides the control/status/data interface separation for all network interfaces. The console port is a control interface except when the terminal server application has it in data mode.
9. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
10. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
11. The module supports concurrent operators.
12. The module does not support a maintenance interface or role.
13. The module does not support manual key entry.
14. The module does have external input/output devices used for entry/output of data.
15. Plaintext CSPs can be entered into the module, but the module will not output them upon being queried.
16. The module does not output intermediate key values.
17. The module limits the use of the same Triple-DES key to  $2^{20}$  encryptions, based on only using the following IETF protocols, and  $2^{16}$  for non-IETF protocols. The user is responsible for ensuring the module's compliance.
  - a. SSH - [RFC4251](#)
  - b. SCEP - [draft-nourse-scep-23](#)
  - c. IPSec/IKE VPN - [RFC6071](#), [RFC2409](#), [RFC7296](#), [RFC4307](#), [RFC2451](#)
18. The module supports communicating with a RADIUS server, which should be protected within an IPSEC tunnel setup by the user.

## 9 References and Definitions

The following standards are referred to in this Security Policy.

**Table 19 – References**

Abbreviation	Full Specification Name
[FIPS140-2]	<i>Security Requirements for Cryptographic Modules, May 25, 2001</i>

**Table 20 – Acronyms and Definitions**

Acronym	Definition
ECR	Edge Connect Router
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
HAB	High Assurance Boot
KAT	Known Answer Test
LN	Licensed radio module
MCR	Multiservice Connect Router
NX	Unlicensed radio module
OTP	One Time Password
RADIUS	Remote Authentication Dial-In User Service
RP-SMA	Reversed-Polarity SMA
SIM	Subscriber Identification Module
SMA	Sub-Miniature version A
TNC	Threaded Neill-Concelman
USB	Universal Serial Bus