Cubic Corporation

Vocality RoIP and DTECH M3-SE Multi-Function Gateway Appliances

Firmware Version: 5.0.1

FIPS 140-2 Non-Proprietary Security Policy

FIPS Security Level: 2
Document Version: 1.7

Prepared for:

CUBIC Mission Solutions

Cubic Corporation
9333 Balboa Avenue
San Diego, CA 92123
United States of America

Phone: +1 858 277 6780
www.cubic.com

Prepared by:

Corsec

Corsec Security, Inc.
13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

List of Tables

List of Figures

1. Introduction

1.1 Purpose

This is a non-proprietary Cryptographic Module Security Policy for the Vocality RoIP[1] and DTECH M3[2]- SE[3] Multi-Function Gateway (MFGW) Appliances from Cubic Corporation (hereafter referred to as Cubic). This Security Policy describes how the Cubic Vocality RoIP and DTECH M3-SE Multi-Function Gateway Appliances meet the security requirements of Federal Information Processing Standards (FIPS) Publication 140-2, which details the U.S.[4] and Canadian government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the Cryptographic Module Validation Program (CMVP) website, which is maintained by the National Institute of Standards and Technology (NIST) and the Canadian Centre for Cyber Security (CCCS).

This document also describes how to run the module in a secure FIPS-Approved mode of operation. This policy was prepared as part of the Level 2 FIPS 140-2 validation of the module. The Cubic Vocality RoIP and DTECH M3-SE Multi-Function Gateway Appliances are referred to in this document as "RoIP and M3-SE appliances" or "the module".

This Security Policy was produced by Corsec Security, Inc. under contract to Cubic.

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 Cubic website (www.cubic.com) contains information on the full line of products from Cubic.
- The search page on the CMVP website (https://csrc.nist.gov/Projects/cryptographic-module-validation-program/Validated-Modules/Search) can be used to locate and obtain vendor contact information for technical or sales-related questions about the module.

1.3 Document Organization

The Security Policy document is organized into two (2) primary sections. Section 2 provides an overview of the validated module. This includes a general description of the capabilities and the use of cryptography, as well as a presentation of the validation level achieved in each applicable functional area of the FIPS standard. It also provides high-level descriptions of how the module meets FIPS requirements in each functional area. Section 3 documents the guidance needed for the secure use of the module, including initial setup instructions and management methods and policies.

[1] RoIP – Radio over Internet Protocol
[2] M3 – Micro, Mobile, Modular
[3] SE – Single Enclave
[4] U.S. – United States

2. Vocality RoIP and DTECH M3-SE-MFGW

2.1 Overview

Cubic Corporation provides a wide range of deployable and tactical communications products and solutions to meet the diverse mission requirements of their military, government, first-responder and civilian customer base. Cubic is the parent company of Cubic Mission Solutions (CMS), which provides networked C4ISR[5] solutions for defense, intelligence, security and commercial missions. The CMS C4ISR solutions include the Vocality RoIP Appliance and the DTECH M3-SE-MFGW Appliance.

The Vocality RoIP Appliance (Figure 1 below) provides users with a simple-to-use, small form factor radio connectivity solution that allows the connection of traditional PTT[6] and digital radio systems to IP[7]- and SIP[8]-based networks. The Vocality RoIP includes audio, serial, and radio auxiliary I/O[9] ports to maximize compatibility with an extensive range of radio types, frequencies, and manufacturers. The (optionally) built-in 4G LTE[10], Wi-Fi, and network ports for connecting to fixed line and satellite services are used to create and extend radio networks beyond normal PTT radio range. The Vocality RoIP can be expanded with the addition of RoIP Connect and Rack Kit to offer up to a 12-port RoIP solution.

Figure 1 – Vocality RoIP Appliance

The Vocality RoIP appliance base model provides communications via Ethernet. There are 5 additional variants of the appliance that also include various combinations of LTE modules and antennas that provide for radio communications in different frequency bands across the globe. See Table 1 below for a listing of the RoIP variants.

[5] C4ISR – Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
[6] PTT – Push-to-talk
[7] IP – Internet Protocol
[8] SIP – Session Initiation Protocol
[9] I/O – Input/Output
[10] LTE – Long Term Evolution

Table 1 – Vocality RoIP Variants

RoIP Device	Part Number	LTE Module	Antenna
Vocality RoIP Retail Pack 1 Port	ROIP/RP/1	-	-
Vocality RoIP LTE(NA) Retail Pack 1 Port	ROIP/LTENA/RP/1	19-0040-02 LTE Module Mini PCIe North America (AT&T)	19-0048-01 External 4G antenna SMA W5095K
Vocality RoIP LTE(NAFD) Retail Pack 1 Port	ROIP/LTENAV/RP/1	19-0049-01 LTE Module Mini PCIe North America (FirstNet)	19-0048-01 External 4G antenna SMA W5095K
Vocality RoIP LTE(NAV) Retail Pack 1 Port	ROIP/LTENAFD/RP/1	19-0046-01 LTE Module Mini PCIe North America (Verizon)	19-0048-01 External 4G antenna SMA W5095K
Vocality RoIP LTE(EU) Retail Pack 1 Port	ROIP/LTEEU/RP1	19-0039-02 LTE Module Mini PCIe Europe	19-0045-01 External 4G antenna SMA RA 2.14dBi
Vocality RoIP LTE(ANZ) Retail Pack 1 Port	ROIP/LTEANZ/RP/1	19-0047-01 LTE Module Mini PCIe Australia and New Zealand	19-0045-01 External 4G antenna SMA RA 2.14dBi

The DTECH M3-SE-MFGW is a portable network appliance designed to communicate over any available networking technology (including IP over satellite, cellular, radio, ISDN[11], and IP broadband/baseband networks). The M3-SE-MFGW is a low-power, high-capability RoIP voice crossbanding and gateway module for the M3-SE product family. The M3-SE-MFGW provides the ability to crossband up to eight (8) separate radio voice networks. It is compatible with any tactical radio or Land Mobile Radio (LMR) system that supports analog E&M signaling.

The M3-SE-MFGW is also capable of extending single radio networks by bridging voice traffic over an existing data network. Two 1Gbps[12] Ethernet interfaces allow for LAN[13] and WAN[14] network segmentation. A removable 4G[15]/LTE cellular radio provides additional WAN uplink capability. The system is also able to operate directly off PoE[16] provided by another network device, extending the functional range of the system. Additionally, a power pass through connection allows direct mounting to existing M3-SE product family devices without the need for additional power supplies or external power cabling.

The M3-SE-MFGW is available in two colors (see Figure 2 and Figure 3 below):

- Black – part number M3-SE-MFGW-BK
- Tan – part number M3-SE-MFGW-DT

[11] ISDN – Integrated Services Digital Network
[12] Gbps – Gigabits per second
[13] LAN – Local Area Network
[14] WAN – Wireless Area Network
[15] 4G – Fourth Generation
[16] PoE – Power Over Ethernet

Figure 2 – DTECH M3-SE-MFGW Appliance (Black)

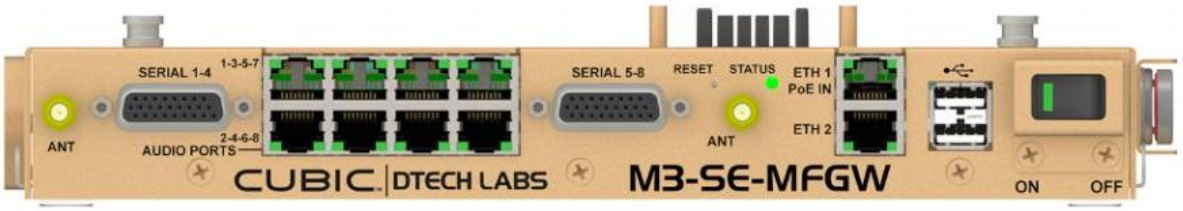

Figure 3 – DTECH M3-SE-MFGW Appliance (Tan)

Each appliance includes the Radio Gateway feature, which connects PTT radios into IP infrastructure. Radio Gateway supports several RoIP protocols, including SRTP[17]/SRTCP[18] and SIP over TLS[19]. The RoIP and M3-SE appliances are also pre-installed with the modular application-based Vocality Gateway Suite software which provides the following additional features (when licensed):

- **Vocality Secure Tunnels** – provides security for network traffic via secure VPN[20] tunneling, encryption, and NAT[21] traversal. This component allows for the configuration of IPsec[22], IP-in-IP, and GRE[23] tunnels.

- **Vocality Failover** – rule-based software component that interfaces directly with wireless and wired technologies. Failover allows users to automatically switch between networks by selecting the most suitable bearer based on availability and user-priorities and works with Secure to maintain secure tunnels as bearers change.

- **Vocality Dispatch** – lightweight console application used to create and manage radio talk groups and provides interoperability between multiple radio devices and manufacturers. This component includes Registry, which allows the nodes to register with a central server.

The RoIP and M3-SE appliances support local or remote management using the Web-based management interface supported by the module called the Node UI[24], which is accessed over HTTPS[25] . The appliances also provide an

[17] SRTP – Secure Real-time Transport Protocol
[18] SRTCP – Secure Real-time Transport Control Protocol
[19] TLS – Transport Layer Security
[20] VPN – Virtual Private Network
[21] NAT – Network Address Translation
[22] IPsec – Internet Protocol Security
[23] GRE – Generic Routing Encapsulation
[24] UI – User Interface
[25] HTTPS – Hypertext Transfer Protocol Secure

SNMPv3[26] interface for remote management and non-security relevant information about node state and statistics.

The RoIP and M3-SE appliances are validated at the FIPS 140-2 Section levels shown in Table 2 below.

Table 2 – 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[27]
7	Cryptographic Key Management	2
8	EMI/EMC[28]	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A

2.2 Module Specification

The RoIP and M3-SE appliances are validated as a hardware cryptographic module with a multiple-chip standalone embodiment. The overall security level of the module is 2. The module runs Cubic's proprietary Linux operating system (OS) and consists of hardware and firmware components enclosed in a secure, production-grade metal case. The cryptographic boundary of the module surrounds the entire enclosure of each appliance.

The module includes the following appliances:

- Vocality RoIP (including RoIP variants with onboard LTE modules)
- DTECH M3-SE-MFGW (with no onboard LTE module)

Each appliance is composed of the following components:

- CPU[29]
- MCU[30]
- SDRAM[31]
- Flash memory

[26] SNMPv3 – Simple Network Management Protocol version 3
[27] N/A – Not Applicable
[28] EMI/EMC – Electromagnetic Interference / Electromagnetic Compatibility
[29] CPU – Central Processing Unit
[30] MCU – Microcontroller Unit
[31] SDRAM – Synchronous Dynamic Random-Access Memory

- Line CODECs[32]
- Serial converter
- Power supplies
- LEDs[33]
- USB hub (M3-SE-MFGW only)
- Network component(s)

Table 3 below lists the libraries supporting the cryptographic algorithm implementations in the RoIP and M3-SE appliances. These cryptographic algorithms provide the cryptographic primitives and support secure networking protocols.

Table 3 – Cryptographic Algorithm Implementation Libraries

Implementation Name	Use
Cubic OpenSSL Cryptographic Library 1.0	Firmware-based cryptographic primitives (based on OpenSSL 1.0.2r)
Cubic Mbed TLS Cryptographic Library 1.0	Firmware-based cryptographic primitives (based on Mbed TLS 2.8.0)
Cubic Kernel Cryptographic Library 1.0	Firmware-based cryptographic primitives (based on Kernel 4.15.18 Crypto Library)
Cubic Libgcrypt Cryptographic Library 1.0	Firmware-based cryptographic primitives (based on Libgcrypt 1.8.2)
Cubic IKE[34] KDF[35] 1.0	KDF implementations for IKE (based on StrongSwan 5.6.2)
Cubic SRTP KDF 1.0	KDF implementations for SRTP (based on libSRTP 2.2.0)
Cubic SNMP KDF 1.0	KDF implementations for SNMP (based on Net-SNMP 5.7.3)
Cubic TLS KDFs 1.0	KDF implementations for TLS (based on Libssl 1.0.2r)

The module implements the FIPS-Approved algorithms listed in Table 4, Table 5, Table 6, and Table 7 below.

Table 4 – FIPS-Approved Algorithm Implementations – Cubic OpenSSL Cryptographic Library 1.0

Certificate Number	Algorithm	Standard	Mode /Method	Key Lengths / Curves / Moduli	Use
C2184	AES[36]	FIPS PUB[37] 197 NIST SP[38] 800-38A	CBC[39], CTR[40]	128, 192, 256	data encryption/decryption

[32] CODEC – Compression/Decompression
[33] LED – Light Emitting Diode
[34] IKE – Internet Key Exchange
[35] KDF – Key Derivation Function
[36] AES – Advanced Encryption Standard
[37] PUB – Publication
[38] SP – Special Publication
[39] CBC – Cipher Block Chaining
[40] CTR – Counter

Certificate Number	Algorithm	Standard	Mode /Method	Key Lengths / Curves / Moduli	Use
		NIST SP 800-38D	GCM[41]	128, 256	data encryption/decryption and message authentication
		SP 800-38C	CCM	128, 256	data encryption/decryption
A835	AES	FIPS PUB 197 NIST SP 800-38A	CFB[42]	128	data encryption/decryption
C2184	DSA[43]	FIPS PUB 186-4	SigGen	2048, 3072 (SHA[44]-256, SHA-384)	digital signature generation
			SigVer	1024, 2048, 3072 (SHA-1, SHA-256, SHA-384)	digital signature verification
C2184	ECDSA[45]	FIPS PUB 186-4	SigGen	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-384, P-521	digital signature generation
			SigVer	B-163, B-233, B-283, B-409, B-571, K-163, K-233, K-283, K-409, K-571, P-192, P-224, P-384, P-521	digital signature verification
C2184	HMAC[46]	FIPS PUB 198-1	SHA-1, SHA-256, SHA-384, SHA-512	KS<BS, KS=BS, KS>BS	message authentication
Vendor Affirmed	KAS-SSC[47]	NIST SP 800-56Arev3	FFC[48] DH[49] Primitive	2048, 3072, 4096, 6144, 8192	shared secret computation
Vendor Affirmed	KAS-SSC	NIST SP 800-56Arev3	ECC[50] CDH[51] Primitive	B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521	shared secret computation
C2184	KTS	NIST SP 800-38F	AES (unauthenticated mode) with HMAC	[AES] 128, 256	Key transport (TLS) *Key establishment methodology provides between 128 and 256 bits of encryption strength*
			AES (authenticated mode)	[AES] 128, 256	Key transport (TLS) *Key establishment methodology provides between 128 and 256 bits of encryption strength.*
Vendor Affirmed	PBKDF	NIST SP 800-132	Option 1(a)	-	password-based key derivation

[41] GCM – Galois Counter Mode
[42] CFB – Cipher Feedback
[43] DSA – Digital Signature Algorithm
[44] SHA – Secure Hash Algorithm
[45] ECDSA – Elliptic Curve Digital Signature Algorithm
[46] HMAC – (keyed-) Hashed Message Authentication Code
[47] KAS-SSC – Key Agreement Scheme Shared Secret Computation
[48] FFC – Finite Field Cryptography
[49] ECDH – Elliptic Curve Diffie-Hellman
[50] ECC – Elliptic Curve Cryptography
[51] CDH – Cofactor Diffie-Hellman

Certificate Number	Algorithm	Standard	Mode /Method	Key Lengths / Curves / Moduli	Use
C2184	RSA[52]	FIPS PUB 186-2	SigVer 9.31, SigVer PSS[53]	4096 (SHA-1, SHA-256, SHA-384, SHA-512)	digital signature verification
		FIPS PUB 186-4	SigGen 9.31, SigGen PSS	2048, 3072 (SHA-256, SHA-384, SHA-512)	digital signature generation
			SigVer 9.31, SigVer PSS	1024, 2048, 3072 (SHA-1, SHA-256, SHA-384, SHA-512)	digital signature verification
A835	RSA	FIPS PUB 186-4	SigGen 9.31, SigGen PSS	4096 (SHA-256, SHA-384, SHA-512)	digital signature generation
			SigVer 9.31, SigVer PSS	4096 (SHA-1, SHA-256, SHA-384, SHA-512)	digital signature verification
C2184	SHS[54]	FIPS PUB 180-4	SHA-1, SHA-256, SHA-384, SHA-512	-	message digest *The cryptographic library supports the truncation of HMAC SHA-1 to 96 bits according to NIST SP 800-107rev1.*

The Cubic OpenSSL Cryptographic Library 1.0 AES GCM IV generation method complies with technique #2 in section A.5 of the *Implementation Guidance for FIPS PUB 140-2 and the CMVP* as follows: The AES GCM IV is used in the TLS protocol. The AES GCM IV is internally generated via RBG-based construction in compliance with Section 8.2.2 of *NIST SP 800-38D* using the Approved DRBG within the module's physical boundary and is 96 bits in length.

The vendor affirms the following cryptographic security method implemented by the Cubic OpenSSL Cryptographic Library:

- Password-based key derivation – The module performs PBKDF2 in compliance with *NIST SP 800-132* using option 1(a) in Section 5.4 to derive the Distribution Upgrade Decryption Key using a password of 52 characters. The 52-character password consists of upper-case and lower-case letters and numbers. An upper bound on the probability of guessing the password is equal to $1:62^{52}$, or $1:60x10^{93}$. The PBKDF2 is used for storage applications only. HMAC-SHA-1 is used as the approved PRF[55]. The iteration count is 1000 iterations. The length of the salt is 128 bits, and it is generated by a FIPS-Approved DRBG.

- Key agreement scheme (shared secret computation) – The module implements an FFC DH shared secret computation for its DH key agreement schemes. The shared secret computation is compliant with section 5.7.1.1 of *NIST SP 800-56Arev3*. This compliance claim follows scenario X1 of FIPS IG D.8, the *Implementation Guidance for FIPS PUB 140-2 and the CMVP*. This primitive is used by the dhHybrid1, dhEphem, dhHybridOneFlow, dhOneFlow and dhStatic schemes found in section 6 of that recommendation.

[52] RSA – Rivest Shamir and Adleman
[53] PSS – Probabilistic Signature Scheme
[54] SHS – Secure Hash Standard
[55] PRF – Pseudo-Random Function

- Key agreement scheme (shared secret computation) – The module implements an ECC CDH shared secret computation for its ECDH key agreement schemes. The shared secret computation is compliant with section 5.7.1.2 of *NIST SP 800-56Arev3*. This compliance claim follows scenario X1 of FIPS IG D.8, the *Implementation Guidance for FIPS PUB 140-2 and the CMVP*. This primitive is used by the Full Unified Model, Ephemeral Unified Model, One-Pass Unified Model, One-Pass Diffie-Hellman, and Static Unified Model schemes found in section 6 of that recommendation.

Table 5 – FIPS-Approved Algorithm Implementations – Cubic MbedTLS Cryptographic Library 1.0

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
C2187	AES	FIPS PUB 197 NIST SP 800-38A	CBC, CTR	128, 256	data encryption/decryption
		FIPS PUB 197 NIST SP 800-38C	CCM[56]	128, 256	data encryption/decryption
		FIPS PUB 197 NIST SP 800-38D	GCM	128, 256	data encryption/decryption and message authentication
C2187	ECDSA	FIPS PUB 186-4	SigGen	P-224, P-256, P-384, P-521	digital signature generation
			SigVer	P-192, P-224, P-256, P-384, P-521	digital signature verification
C2187	HMAC	FIPS PUB 198-1	SHA-1, SHA-256, SHA-384	KS<BS, KS=BS, KS>BS	message authentication
A849	HMAC	FIPS PUB 198-1	SHA-512	KS<BS, KS=BS, KS>BS	message authentication
Vendor Affirmed	KAS-SSC	NIST SP 800-56Arev3	FFC DH Primitive	2048	shared secret computation
Vendor Affirmed	KAS-SSC	NIST SP 800-56Arev3	ECC CDH Primitive	P-224, P-256, P-384, P-521	shared secret computation
C2187	RSA	FIPS PUB 186-2	SigVer PKCS[57]1.5, SigVer PSS	4096 (SHA-1, SHA-256, SHA-384)	digital signature verification
		FIPS PUB 186-4	SigGen PKCS1.5, SigGen PSS	2048, 3072 (SHA-256, SHA-384)	digital signature generation
			SigVer PKCS1.5, SigVer PSS	1024, 2048, 3072 (SHA-1, SHA-256, SHA-384)	digital signature verification
A849	RSA	FIPS PUB 186-4	SigGen PKCS1.5, SigGen PSS	4096 (SHA-256, SHA-384)	digital signature generation
			SigVer PKCS1.5, SigVer PSS	4096 (SHA-1, SHA-256, SHA-384)	digital signature verification
C2187	SHS	FIPS PUB 180-4	SHA-1, SHA-256, SHA-384	-	message digest
A849	SHS	FIPS PUB 180-4	SHA-512	-	message digest

The Cubic MbedTLS Cryptographic Library 1.0 AES GCM IV generation method complies with technique #2 in section A.5 of the *Implementation Guidance for FIPS PUB 140-2 and the CMVP* as follows: The AES GCM IV is used

[56] CCM – Counter with Cipher Block Chaining-Message Authentication Code
[57] PKCS – Public Key Cryptography Standard

in the TLS protocol. The AES GCM IV is internally generated via RBG-based construction in compliance with Section 8.2.2 of *NIST SP 800-38D* using the Approved DRBG within the module's physical boundary and is 96 bits in length.

The vendor affirms the following cryptographic security method implemented by the Cubic MbedTLS Cryptographic Library:

- Key agreement scheme (shared secret computation) – The module implements an FFC DH shared secret computation for its DH key agreement scheme. The shared secret computation is compliant with section 5.7.1.1 of *NIST SP 800-56Arev3*. This compliance claim follows scenario X1 of FIPS IG D.8, the *Implementation Guidance for FIPS PUB 140-2 and the CMVP*. This primitive is used by the dhHybrid1, dhEphem, dhHybridOneFlow, dhOneFlow and dhStatic schemes found in section 6 of that recommendation.

- Key agreement scheme (shared secret computation) – The module implements an ECC CDH shared secret computation for its ECDH key agreement scheme. The shared secret computation is compliant with section 5.7.1.2 of *NIST SP 800-56Arev3*. This compliance claim follows scenario X1 of FIPS IG D.8, the *Implementation Guidance for FIPS PUB 140-2 and the CMVP*. This primitive is used by the Full Unified Model, Ephemeral Unified Model, One-Pass Unified Model, One-Pass Diffie-Hellman, and Static Unified Model schemes found in section 6 of that recommendation.

Table 6 – FIPS-Approved Algorithm Implementations – Cubic Kernel Cryptographic Library 1.0

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
C2183	AES	FIPS PUB 197 NIST SP 800-38A	CBC, CTR	128, 192, 256	data encryption/decryption
Vendor Affirmed	CKG	NIST SP 800-133rev1	-	-	symmetric key generation
C2183	DRBG	NIST SP 800-90Arev1	CTR-based	256-bit AES	deterministic random bit generation
			HMAC-based	SHA-1, SHA-256, SHA-384, SHA-512	
C2183	HMAC	FIPS PUB 198-1	SHA-1, SHA-256, SHA-384, SHA-512	-	message authentication
C2183	SHS	FIPS PUB 180-4	SHA-1, SHA-256, SHA-384, SHA-512	-	message digest *The cryptographic library supports the truncation of HMAC SHA-1 to 96 bits according to NIST SP 800-107rev1.*

The vendor affirms the following cryptographic security method implemented by the Cubic OpenSSL Cryptographic Library:

- Cryptographic key generation – As per *NIST SP 800-133rev1*, the module uses the Cubic Kernel Cryptographic Library 1.0 FIPS-Approved CTR-based and HMAC-based DRBGs specified in *NIST SP 800-90Arev1* to generate cryptographic keys. The resulting symmetric key or generated seed is an unmodified

output from the DRBG. Entropy for the module's DRBGs is provided by a CPU jitter-based non-deterministic random number generator (NDRNG) internal to the module, which was assessed per the guidance in *FIPS 140-2 IG* 7.15. The entropy source provides 1.199384 bits of entropy per 4 bits of raw noise data.

Table 7 – FIPS-Approved Algorithm Implementations – Cubic Libgcrypt Cryptographic Library 1.0

Certificate Number	Algorithm	Standard	Mode / Method	Key Lengths / Curves / Moduli	Use
C2182	AES	FIPS PUB 197 NIST SP 800-38A	CFB[58]128	128, 192, 256	data encryption/decryption

In addition, the RoIP and M3-SE appliances include several protocol libraries that implement FIPS-Approved KDFs:

- IKE KDFs implemented by the Cubic IKE KDF 1.0 protocol library
- SRTP KDF implemented by the Cubic SRTP KDF 1.0 protocol library
- SNMP KDF implemented by the Cubic SNMP KDF 1.0 protocol library
- TLS v1.2 KDF implemented by the Cubic Mbed TLS Cryptographic Library 1.0
- TLS v1.0/1.1/1.2 KDFs implemented by the Cubic TLS KDFs 1.0 protocol library

The FIPS-Approved KDFs are listed in Table 8 below.

Table 8 – FIPS-Approved KDFs

Certificate Number	Algorithm	Specification	Mode / Method	Key Lengths / Curves / Moduli	Use
C2186	CVL	NIST SP 800-135rev1	IKEv1/v2	-	key derivation
C2185	CVL	NIST SP 800-135rev1	SNMPv3	-	key derivation
Vendor Affirmed	CVL	NIST SP 800-135rev1	SRTP	-	key derivation
C2188	CVL	NIST SP 800-135rev1	TLS v1.0, 1.1, 1.2	-	key derivation
C2187	CVL	NIST SP 800-135rev1	TLS v1.2	-	key derivation

**No parts of the IKE, SNMP, and TLS protocols, other than the KDFs, have been tested by the CAVP[59] or CMVP.*

Note that the module implements the SRTP KDF per *RFC[60] 3711* (as documented in *NIST SP 800-135rev1*) using the 48-bit index value in SRTCP[61] per the NIST-published Informative Note. However, no CAVP or ACVP testing was available for this component at the time of this evaluation. Thus, in accordance with *FIPS 140-2 IG* G.20, the SRTP KDF algorithm is listed individually in Table 8 above as "vendor affirmed" and considered Approved for use in FIPS mode.

[58] CFB – Cipher Feedback
[59] CAVP – Cryptographic Algorithm Validation Program
[60] RFC – Request for Comment
[61] SCRTP – Secure Real-Time Transport Control Protocol

The RoIP and M3-SE appliances employ the non-FIPS-approved algorithm implementations shown in Table 9, which are allowed for use in a FIPS-Approved mode of operation.

Table 9 – Allowed Algorithm Implementations

Algorithm	Caveat	Use
SHA-1	Legacy-use	DSA, ECDSA and RSA signature verification
NDRNG	-	seeding for the DRBGs
SHA-1	-	Digital signature generation in TLS[62]

2.3 Module Interfaces

The RoIP appliance provides the following physical ports and interfaces:

- Quad Serial & Radio Auxiliary I/O*
  - Serial
  - GPIO[63]
- Audio
- Ethernet
- USB[64]
- Antenna connectors
- SIM[65] card slot
- LEDs
- Reset button
- Power connector

***NOTE**: The serial connections and radio auxiliary I/O (programmable GPIO signals) are not available over individually separated connector ports, but rather are available using the 26-way DB15HD data port located on the front panel of the appliance. The serial connection is available through pins 1-8 and 10-17. The GPIO connection is available through pins 9, 18, 20, 22, 24, and 26. The remaining pins are designated as ground.

[62] Per *NIST SP 800-52*, SHA-1 is an allowed hashing technique for generating digital signatures within the TLS protocol.
[63] GPIO – General Purpose Input/Output
[64] USB – Universal Serial Bus
[65] SIM – Subscriber Identity Module

Figure 4 – Vocality RoIP Front Panel

Figure 5 – Vocality RoIP Rear Panel

The M3-SE appliance provides the following physical ports and interfaces:

- Serial & Auxiliary I/O
  - Serial
  - GPIO
- Audio
- Ethernet
- USB
- Antenna connectors
- LEDs
- Reset button
- Power connector

Figure 6 – M3-SE-MFGW Front View

Figure 7 – M3-SE-MFGW Angled View

Each of the listed physical ports maps to one of the defined FIPS 140-2 logical interfaces. These interfaces provide:

- Data Input
- Data Output
- Control Input
- Status Output
- Power

Physical interfaces for the RoIP and M3-SE appliances are described in Table 10 below:

Table 10 – FIPS 140-2 Logical Interface Mappings

Physical Port/Interface	Quantity		FIPS 140-2 Interface
	RoIP	M3-SE	
Ethernet	2	2	Data Input Data Output Control Input Status Output
USB	1	2	Data Input Data Output
Audio	4	8	Data Input Data Output
Serial	4	8	Data Input Data Output

Physical Port/Interface	Quantity		FIPS 140-2 Interface
	RoIP	M3-SE	
GPIO	6	12	Data Input Data Output
Antenna Connector	2	2	Data Input Data Output
SIM Card Slot	1	-	Control Input
LEDs	1	1	Status Output
Reset Button	1	1	Control Input
Power	1	1	Power Input

2.4 Roles, Services, and Authentication

The sections below describe the module's roles and services and define any authentication methods employed.

2.4.1 Authorized Roles

The RoIP and M3-SE appliances support explicit role-based authentication. There are two roles (as required by FIPS 140-2) that operators may assume:

- Crypto Officer (CO) – The CO role performs administrative services on the module, such as initialization, configuration, and monitoring of the module. The CO has access to all Vocality Gateway Suite "Administrator" and "Read-Write" privileges. Read-Write privileges are the same as Administrator except that the User menu is not accessible.

- User – Users can view the current status of the module and employ the services of the module (including IPsec, TLS, SRTP, and SNMPv3 services). Users have access to Vocality Gateway Suite "Read-Only" privileges.

2.4.2 Operator Services

Descriptions of the services available to the CO role and User role are provided in Table 11 below. Please note that the keys and Critical Security Parameters (CSPs) listed in the table indicate the type of access required using the following notation:

- R – Read: The CSP is read, sent, or input.
- W – Write: The CSP is established, generated, or modified.
- X – Execute: The CSP is used within an Approved or Allowed security function or authentication mechanism.
- Z – The CSP is zeroized.

Table 11 – Mapping of Module Services to Roles, CSPs, and Type of Access

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Perform initial configuration	✓		Define the node name, type, and license.	Commands and parameters	Command response; Status output	None
View platform information	✓	✓	View platform information including status, statistics, and processes	Commands and parameters	Command response; Status output	None
Switch to backup image	✓		Switch to node backup image (this results in an automatic reboot)	Command and parameters	Command response	All ephemeral keys/CSPs – Z
Restart	✓		Restart the node	Command	Command response	All ephemeral keys/CSPs – Z
Upgrade distribution image	✓		Upgrade distribution image firmware	Command and parameters	Command response; Status output	Distribution Upgrade Authentication Key – X PBKDF2 Backup Password – R/X Distribution Upgrade Decryption Key – W/X All keys/CSPs – Z
Backup	✓	✓	Backup configuration files	Command and parameters	Command response; Status output	SNMPv3 Passphrase – W
Restore	✓		Restore configuration files	Command and parameters	Command response; Status output	SNMPv3 Passphrase – W
Factory reset	✓		Reset system configuration and zeroize all keys/CSPs	Command	Command response; Status output	All keys/CSPs – Z
Configure platform settings	✓		Configure NTP[66], logging, and HTTPS settings; export audit logs; manage registry client settings	Commands and parameters	Command response; Status output	TLS Public Key – W
Configure network settings	✓		Set networking mode; manage IPv4/IPv6 settings; manage LAN and WAN ports; configure routing; configure rate/QoS[67] settings; Manage links	Commands and parameters	Command response; Status output	None
Perform diagnostics	✓	✓	Perform ping and traceroute commands for node	Command	Command response; Status output	None

[66] NTP – Network Time Protocol
[67] QoS – Quality of Service

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Manage licenses	✓		Upload license files	Commands and parameters	Command response; Status output	None
Manage users	✓		Manage users and change their passwords	Commands and parameters	Command response; Status output	User Password – R/W CO Password – R/W
Change password	✓	✓	Change own password	Commands and parameters	Command response; Status output	User Password – R/W CO Password – R/W
Manage Audio and Talk-Group settings	✓		Manage audio ports and talk groups; configure radio gateway TLS and SRTP settings; add SIP accounts; configure voice data bypass mode	Commands and parameters	Command response; Status output	None
Manage Secure Tunnel settings	✓		Configure tunnel settings; manage IPsec certificates and keys; configure IP data bypass mode	Commands and parameters	Command response; Status output	IKE Private Key – W IKE Public Key – W IKE Pre-Shared Key (PSK) – W IKE CA[68] Root Public Key – W
Manage Failover settings	✓		Set Multi-bearer policies (including selection mode, priority, and revert settings) and manage multi-bearer availability	Commands and parameters	Command response; Status output	None
Manage Registry settings	✓		Configure registry server settings	Commands and parameters	Command response; Status output	None
Manage Dispatch settings	✓		View unassigned ports, create new talk groups	Commands and parameters	Command response; Status output	None
Manage Serial settings	✓		Configure serial port information	Commands and parameters	Command response; Status output	None
Configure SNMP	✓		Configure SNMP settings and SNMP user information	Commands and parameters	Command response; Status output	SNMPv3 Passphrase – R/W/X SNMPv3 Privacy Key – W SNMPv3 Authentication Key – W

[68] CA – Certificate Authority

Service	Operator		Description	Input	Output	CSP and Type of Access
	CO	User				
Establish IPsec connection	✓		Establish an IPsec session	Command	Status output	IKE Public Key – R IKE PSK – X IKE CA Root Public Key – X IKE Session Key – X IKE Authentication Key – X IPsec Session Key – X IPsec Authentication Key – X DRBG Seed – R/W/X DRBG Entropy – R/X DRBG 'V' Value – R/W/X DRBG 'Key' Value – R/W/X
Establish TLS session	✓		Establish a TLS session	Command	Status output	TLS Public Key – R TLS Private Key – R/X TLS Peer Public Key – R/X DH/ECDH Private Key Component – W/X DH/ECDH Public Key Component – R/W DH/ECDH Peer Public Key Component – R/X TLS Premaster Secret – R/W/X TLS Master Secret – W/X TLS Session Key – W/X TLS Authentication Key – W/X AES GCM IV[69] – W/X DRBG Seed – R/W/X DRBG Entropy – R/X DRBG 'V' Value – R/W/X DRBG 'Key' Value – R/W/X
Establish SRTP session	✓		Establish SRTP session	Command	Status output	SRTP Master Key – W/X SRTP Session Key – W/X SRTP Authentication Key – W/X
Show status	✓	✓	Show the system status	Command	Status output	None

2.4.3 Additional Services

The RoIP and M3-SE appliances provide a limited number of services for which the operator is not required to assume an authorized role. Table 12 lists these unauthenticated services. None of these services disclose or substitute cryptographic keys and CSPs or otherwise affect the security of the module.

Table 12 – Additional Services

Service	Description	Input	Output	CSP and Type of Access
Zeroize	Zeroize ephemeral keys and CSPs	Power cycle	Status output	All ephemeral keys/CSPs – Z
Perform On-Demand Self-Tests	Perform self-tests on demand	Power cycle	Status output	All ephemeral keys/CSPs – Z

[69] IV – Initialization Vector

Service	Description	Input	Output	CSP and Type of Access
Reset	Resets module to factory mode	Reset button	Status output	All keys/CSPs – Z
Authenticate operators	Authenticate operators to the module	Command and parameters	Status output	User Password – X CO Password – X

2.4.4 Authentication

The RoIP and M3-SE appliances support role-based authentication. Role assumption is explicit and based on the authentication credential employed. Module operators must authenticate to the module to assume an authorized role and access module services. When changing roles, the operator must first log out of their current role, and then re-authenticate to the module to assume the new role.

All operators authenticate to the RoIP and M3-SE appliances using a username and password (see Section 3.2.1 below for the password complexity rules). Table 13 provides the strength of the authentication mechanism used by the module.

Table 13 – Authentication Mechanism Used by the Module

Authentication Type	Strength
Password	By design, operator passwords must be a minimum of 8 characters, with 69 characters (52 case-sensitive letters, 10 digits, and 7 special characters) possible for usage as described in section 3.2.1. The chance of a random attempt falsely succeeding is at minimum: 1:202,087,559,770,880 which is less than 1:1,000,000 as required by FIPS 140-2. This calculation is the result of taking all possible combinations (69^8) and subtracting the invalid combinations as the password requires at least one digit and one special character. Therefore, (69^8) - possible combinations without a digit (59^8) - possible combinations without a special character (62^8) + combinations without either a digit or a special character (52^8), since these are double-counted by the previous two terms = 202,087,559,770,880 possible combinations. The authentication mechanism includes a one-second delay for each authentication attempt, and after three consecutive login failures, the module locks out further login attempts for 15 seconds. Assuming that no time is taken for each attempt, three attempts would require 3 seconds (accounting for the one-second delay). This allows for a maximum of 12 password attempts in a one-minute window. The probability that a random attempt will succeed in one minute is: 1:202,087,559,770,880 / (12 passwords per minute), or 1:16,840,629,980,907 which is less than 1:100,000 as required by FIPS 140-2.

The feedback of authentication data to an operator is obscured during authentication to the Node UI. The module does not allow the disclosure, modification, or substitution of authentication data to unauthorized operators.

2.5 Physical Security

The module is a multiple-chip standalone hardware cryptographic module. The enclosures of each appliance consist of hard, production-grade, metal components. These components are opaque within the visible spectrum. The module includes only standard, production-quality integrated circuits, designed to meet typical production-grade specifications for power, temperature, reliability, shock/vibration, etc. The integrated circuits used in the module are coated with commercial standard passivation.

The RoIP and M3-SE appliances contain tamper-evident seals which are pre-applied at the factory before delivery. The tamper-evident seals are placed over at least two screws securing the lid to the enclosure.

2.6 Operational Environment

The operational environment of the module does not provide the module operator with access to a general-purpose OS. The RoIP and M3-SE appliances employ a non-modifiable operating environment. The module's firmware (Firmware version: 5.0.1) is executed by an Intel Atom E3805 processor. The module runs the Yocto 2.5 (Sumo) OS, kernel version 4.15.

2.7 Cryptographic Key Management

The module supports the CSPs listed below in Table 14. In compliance with IG 7.14, the module generates cryptographic keys whose strengths are modified by available entropy.

Table 14 – Cryptographic Keys, Cryptographic Key Components, and CSPs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
AES GCM IV	96-bit IV	[Radio GW TLS] Generated internally via FIPS-Approved DRBG with RBG construction per Section 8.2.2 of NIST SP 800-38D [HTTPS] Generated internally via FIPS-Approved DRBG with RBG construction per Section 8.2.2 of NIST SP 800-38D	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle	IV for AES GCM
DH Private Key Component	[Radio GW TLS] 256-bit DH private key [HTTPS] 256-bit DH private key [IKE] 256-bit DH private key	Generated internally via Approved DRBG	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Generation of TLS and IKE shared secrets

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DH Public Key Component	[Radio GW TLS] 2048-bit DH public key [HTTPS] 2048-bit DH public key [IKE] 2048, 3072, 4096, 6144, 8192-bit DH public key	[for the module] Generated internally via Approved DRBG [for a peer] Input in plaintext form	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Generation of TLS and IKE shared secrets
ECDH Private Key Component	Private component of ECDH protocol	Generated internally via Approved DRBG	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Generation of TLS shared secrets
ECDH Public Key Component	Public component of ECDH protocol	[for the module] Generated internally via Approved DRBG [for a peer] Input in plaintext form	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Generation of TLS shared secrets
TLS Public Key	[Radio GW[70] TLS] 1024, 2048, 3072, 4096-bit RSA public key P-192, P-224, P-256, P-384, P-521 ECDSA public key [HTTPS] 1024, 2048, 3072, 4096-bit RSA public key 1024, 2048, 3072-bit DSA public key All NIST-recommended ECDSA curves	[for the module] Generated externally, imported in encrypted form via TLS session [for a peer] Input in plaintext form as part of TLS session negotiation	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	[for the module] Plaintext in eMMC[71] flash [for a peer] Plaintext in volatile memory	Factory reset	TLS authentication **1024-bit RSA public keys and P-192, B-163, and K-163 ECDSA curves are used for signature verification only**

[70] GW – Gateway
[71] eMMC – embedded Multi-Media Controller

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
TLS Private Key	[Radio GW TLS] 2048, 3072, 4096-bit RSA private key P-224, P-256, P-384, P-521 ECDSA private key [HTTPS] 2048, 3072, 4096-bit RSA private key 2048, 3072-bit DSA private key All NIST-recommended ECDSA curves	Generated externally, imported in encrypted form via TLS session	Never exits the module	Plaintext in eMMC flash	Factory reset	TLS authentication
TLS Pre-Master Secret	DH/ECDH shared secret	Derived internally via DH/ECDH shared secret computation	for DH/ECDH cipher suites] Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; upon completion of TLS Master Secret computation	Derivation of the TLS Master Secret
TLS Master Secret	384-bit shared secret	Derived internally using the TLS Pre-Master Secret via TLS KDF	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Derivation of the TLS Session Key and TLS Authentication Key
TLS Session Key	128/256-bit AES key 128/256-bit AES GCM key	Derived internally using the TLS Master Secret via TLS KDF	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Encryption and decryption of TLS session packets
TLS Authentication Key	[Radio GW TLS] 160/256/384-bit HMAC key [HTTPS] 160/256/384-bit HMAC key	Derived internally using the TLS Master Secret via the TLS KDF	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Authentication of TLS session packets
SRTP Master Key	128/256-bit shared secret	Generated internally using FIPS approved CTR DRBG	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Keying material used in derivation of the SRTP session and authentication keys
SRTP Session Key	128/256-bit AES-CTR key	Derived internally using SRTP Master Key	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Encryption or decryption during SRTP session

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
SRTP Authentication Key	160-bit HMAC key	Derived internally using SRTP Master Key	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Authentication of SRTP session packets
SNMPv3 Passphrase	Minimum of eight (8) characters	Input in encrypted form via TLS session	Exits the module in encrypted form via TLS session as part of config backup file	Plaintext in eMMC flash	Factory reset	Derivation of SNMPv3 privacy and authentication keys
SNMPv3 Privacy Key	128-bit AES CFB key	Derived internally using the SNMPv3 passphrase via SNMP KDF	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Encrypting SNMPv3 packets
SNMPv3 Authentication Key	160-bit HMAC key	Derived internally using the SNMPv3 passphrase via SNMP KDF	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Authenticating SNMPv3 packets
IKE Public Key	1024, 2048, 3072, 4096-bit RSA public key All NIST-recommended ECDSA curves	[for the module] Generated externally, imported in encrypted form via TLS session [for a peer] Input in plaintext form as part of IKE/IPsec session negotiation	[for the module] Exits the module in plaintext form [for a peer] Never exits the module	Plaintext in eMMC flash	Factory reset	Authentication during IKE key exchange **1024-bit RSA public keys and P-192, B-163, and K-163 ECDSA curves are used for signature verification only**
IKE Private Key	2048, 3072, 4096-bit RSA private key All NIST-recommended ECDSA curves	Generated externally, imported in encrypted form via TLS session	Never exits the module	Plaintext in eMMC flash	Factory reset	Authentication during IKE key exchange
IKE CA Root Public Key	1024, 2048, 3072, 4096-bit RSA public key All NIST-recommended ECDSA curves	Generated externally, imported in encrypted form via TLS session	Never exits the module	Plaintext in eMMC flash	Factory reset	Authentication during IKE key exchange **1024-bit RSA public keys and P-192, B-163, and K-163 ECDSA curves are used for signature verification only**

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
IKE PSK	8-64 character string	Input in encrypted form via TLS session	Never exits the module	Plaintext in eMMC flash	Factory reset	Authentication during IKE key exchange [for IKEv1 only] Keying material used in derivation of the IPsec/IKE session keys and authentication keys
IKE Shared Secret	Shared secret	Derived internally via DH shared secret computation	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Keying material used in derivation of the IKE/IPsec session keys and authentication keys
IKE Session Key	128/192/256-bit AES key	Derived internally via IKE KDF	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Encryption and decryption of IKE session packets
IKE Authentication Key	160/256/384/512-bit HMAC key	Derived internally via IKE KDF	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Authentication of IKE session packets
IPsec Session Key	128/192/256-bit AES key	Derived internally via IKE KDF	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Encryption and decryption of IPsec session packets
IPsec Authentication Key	160/256/384/512-bit HMAC key	Derived internally via IKE KDF	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle; session termination	Authentication of IPsec session packets
User Password	8-32-character string	Input in encrypted form via TLS session	Never exits the module	Plaintext in eMMC flash	Factory reset	Authentication to the module
CO Password	8-32-character string	Input in encrypted form via TLS session	Never exits the module	Plaintext in eMMC flash	Factory reset	Authentication to the module
DRBG Seed	[for CTR DRBG] 384-bit value [for HMAC DRBG] 440 bits (SHA1, SHA-256) 888 bits (SHA-384, SHA-512)	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle	Seed material for SP 800-90A DRBGs

CSP	CSP Type	Generation / Input	Output	Storage	Zeroization	Use
DRBG Entropy	[for CTR DRBG] Minimum 256-bit value [for HMAC DRBG] Minimum 128-bit value (SHA-1) Minimum 256-bit value (SHA-256, SHA-384, SHA-512)	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle	Entropy material for SP 800-90A DRBGs
DRBG 'V' Value	Internal state value	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle	Used for SP 800-90A HMAC DRBG and CTR DRBG
DRBG 'Key' Value	Internal state value	Generated internally	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle	Used for SP 800-90A HMAC DRBG and CTR DRBG
Distribution Upgrade Authentication Key	P-384 ECDSA public key	Generated externally, input at factory	Never exits the module	Plaintext in eMMC flash	Not applicable – hardcoded public key	Used to verify signature on distribution firmware image upgrades
PBKDF2 Backup Password	52-character string	Input electronically in encrypted form via TLS session	Never output from module	Plaintext in volatile memory	Reboot; power-cycle	Deriving Distribution Upgrade Decryption Key
Distribution Upgrade Decryption Key	256-bit AES CBC key	Derived internally using PBKDF2 Backup Password per NIST SP 800-132	Never exits the module	Plaintext in volatile memory	Reboot; power-cycle	Used to decrypt firmware images during distribution firmware image upgrades

2.8 EMI / EMC

The base RoIP appliance was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (home use).

Additionally, three of the five remaining RoIP variants employ LTE modules from Quectel Wireless Solutions Co., Ltd. that are designed for operation in North America. These LTE modules were tested and awarded FCC IDs as shown in Table 15 below.

Table 15 – Vocality RoIP Variant FCC IDs

RoIP Device	LTE Module Model	FCC ID	FCC Test Lab
Vocality RoIP LTE(NA) Retail Pack 1 Port	Quectel EC25-A	XMR201605EC25A	TA Technology (Shanghai) Co., Ltd.
Vocality RoIP LTE(NAFD) Retail Pack 1 Port	Quectel EC25-AF	XMR201808EC25AF	TA Technology (Shanghai) Co., Ltd.
Vocality RoIP LTE(NAV) Retail Pack 1 Port	Quectel EC25-V	XMR201607EC25V	TA Technology (Shanghai) Co., Ltd.

The M3-SE appliance was tested and found conformant to the EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A (business use).

2.9 Self-Tests

Cryptographic self-tests are performed by the module when the module is first powered up and conditionally during run-time. The following sections list the self-tests performed by the module, their expected error status, and the error resolutions.

2.9.1 Power-Up Self-Tests

The RoIP and M3-SE appliances perform the power-up self-tests automatically when power is provided to the module. Additionally, an operator can also perform the power-up self-tests on demand by rebooting the module or power-cycling the appliance. Successful completion of the power-up self-tests is indicated by the module successfully booting and a success message is written to */var/log/fips.log*.

The RoIP and M3-SE appliances perform the following self-tests at power-up:

- Firmware integrity check (HMAC SHA-256)
- Known Answer Tests (KATs)
    - Cubic OpenSSL Cryptographic Library 1.0
        - AES CTR mode encrypt KAT
        - AES CTR mode decrypt KAT
        - AES GCM encrypt KAT
        - AES GCM decrypt KAT
        - RSA signature generation KAT
        - RSA signature verification KAT

        - DSA PCT[72]
        - ECDSA PCT
        - SHA KAT using SHA-1, SHA-256, SHA-512
        - HMAC KAT using SHA-1, SHA-256, SHA-512
        - DH Primitive "Z" computation test
        - ECDH Primitive "Z" computation test

    - Cubic MbedTLS Cryptographic Library 1.0
        - AES CTR mode encrypt KAT
        - AES CTR mode decrypt KAT
        - AES GCM encrypt KAT
        - AES GCM decrypt KAT
        - AES CCM encrypt KAT
        - AES CCM decrypt KAT
        - RSA sign/verify KAT
        - ECDSA PCT
        - SHA KAT using SHA-1, SHA-256, SHA-512
        - HMAC KAT using SHA-1, SHA-256, SHA-512
        - DH Primitive "Z" computation test
        - ECDH Primitive "Z" computation test

    - Cubic Kernel Cryptographic Library 1.0
        - AES CTR mode encrypt KAT
        - AES CTR mode decrypt KAT
        - SHA KAT using SHA-1, SHA-256, SHA-512
        - HMAC KAT using SHA-1, SHA-256, SHA-512
        - CTR DRBG KAT
        - HMAC DRBG KAT

    - Cubic Libgcrypt Cryptographic Library 1.0
        - AES CFB encrypt KAT
        - AES CFB decrypt KAT

2.9.2 Conditional Self-Tests

Conditional self-tests are performed by the RoIP and M3-SE appliances whenever a new random number is generated, the module returns from a bypass state (see section 3.2.5 for additional information on cryptographic bypass), and when the module receives new firmware to be installed. Public-Key Validation of DH and ECDH key pairs is also performed. Successful completion of the conditional self-test is indicated by the successful execution of the service that required the test and is also recorded in */var/log/fips.log*.

The RoIP and M3-SE appliances perform the following conditional self-tests:

- Firmware update/load test using ECDSA signature verification
- Bypass tests
    - IPSec tunnel bypass test
    - Radio talk group bypass test

[72] PCT – Pairwise Consistency Test

- CRNGT[73] for NDRNG

2.9.3 Critical Function Self-Test

The RoIP and M3-SE appliances implement the SP 800-90A HMAC DRBG and CTR DRBG random number generators. The SP 800-90A specification requires that certain critical functions be tested to ensure the security of the DRBGs. These critical functions are instantiation, generation, and reseed. Each of these critical functions are tested by the module during the module's power-up self-tests. Successful completion of the critical function self-test is indicated by the module successfully booting and is recorded to */var/log/fips.log*.

2.9.4 Self-Test Failures

The module immediately transitions to the "Critical Error" state in the event of a power-up self-test failure, CRNGT for the NDRNG conditional self-test failure, or critical functions test failure. In the "Critical Error" state the module logs the error to */var/log/fips.log*, and automatically reboots the appliance (effectively inhibiting all data output via the data output interfaces) to clear the error state. If the self-tests continue to fail, the CO should contact Cubic support for assistance.

Failure of the Firmware Update/Load Test and the Bypass Test results in the module transitioning to the "Soft Error" state. The failure of the Firmware Update/Load Test results in the module discarding the new firmware image and continuing with the current image. In the event of a Bypass Test failure for an IPsec tunnel, an error is logged, and the tunnel disabled. For a Bypass Test failure for a Radio talk group, an error is logged, and the talk group is disabled.

2.10 Mitigation of Other Attacks

This section is not applicable. The RoIP and M3-SE appliances do not claim to mitigate any attacks beyond the FIPS 140-2 Level 2 requirements for this validation.

[73] CRNGT – Continuous Random Number Generator Test

3. Secure Operation

The sections below describe how to place and keep the Vocality RoIP and DTECH M3-SE Multi-Function Gateway Appliances in the FIPS-Approved mode of operation. **Operating the module without following the guidance herein (including the use of undocumented services) will result in non-compliant behavior and is outside the scope of this Security Policy**.

3.1 Setup and Configuration

The CO shall receive the module from Cubic via trusted couriers (e.g. United Parcel Service, Federal Express, etc.). On receipt, the CO must check the package for any irregular tears or openings. If any such damage exists, the CO shall contact Cubic immediately for instructions. The CO shall also retain the packing list, making sure all the items on the list are present.

The RoIP and M3-SE appliances are shipped to the customer in a non-configured state. The CO is responsible for inspecting, initializing, and configuring the module to run in the FIPS-Approved mode of operation.

To configure the module for the FIPS-Approved mode of operation, the CO must:

1. Inspect all tamper-evident seals
2. Perform setup and initialization steps
3. Configure network access
4. Upload licenses
5. Set up IPsec tunnels
6. Set up secure radio talk groups

To accomplish these tasks, the CO must follow the procedures detailed in the sections below (for more information, please see the *Vocality RoIP User Manual* and the *Vocality Gateway Suite User Manual*.

3.1.1 Tamper-Evident Seal Inspection and End-User Application

The Vocality RoIP appliance has three tamper-evident seals applied to the device by the vendor during manufacturing. Five tamper-evident seals are applied to the M3-SE appliance by the vendor during manufacturing. Upon receipt of the modules, the CO shall visually inspect the factory-applied seals to ensure they are in the proper locations and that they have not already been tampered.

On the Vocality RoIP appliance, three factory-applied seals cover a screw head on the bottom right of the front cover and a screw head on each side of the device (for screws that secure the device cover). The label on the left side of the device is placed on the screw head closest to the front of the device. The label on the right side of the device is placed on the screw head farthest from the front of the device. Figure 8 below shows the factory-applied seal locations for the Vocality RoIP appliance.

On the M3-SE-appliance, two factory-applied seals cover the screw heads on the bottom of the appliance that secure the device cover as shown in Figure 9, Figure 10, and Figure 11. Three additional seals are applied at the factory to cover the screw heads on the M3-SE appliance fan cover (two seals) and radio module access cover (one seal) as shown in Figure 12 and Figure 13. Figure 12 shows the placement of the two seals to cover the screw

heads on the fan cover. Figure 13 shows the placement of the one seal to cover one of the screw heads on the radio module access cover.

The CO is required to periodically inspect the appliance for evidence of tampering at intervals specified per end-user policy. The CO must visually inspect the tamper-evident seals for tears, rips, dissolved adhesive, and other signs of attempted tampering. If evidence of tampering is found during periodic inspection, the CO must take the device out of operation and contact Cubic.

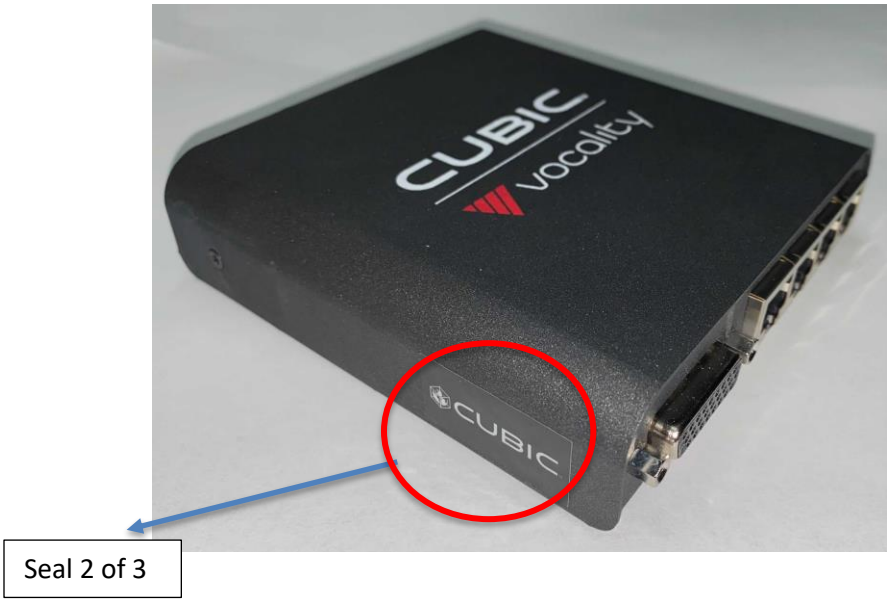

Figure 8 – Vocality RoIP Factory-Applied Tamper-Evident Seals

Figure 9 – M3-SE-MFGW Factory-Applied Tamper-Evident Seals – Bottom Straight View

Figure 10 – M3-SE-MFGW Factory-Applied Tamper-Evident Seals – Bottom Angled View

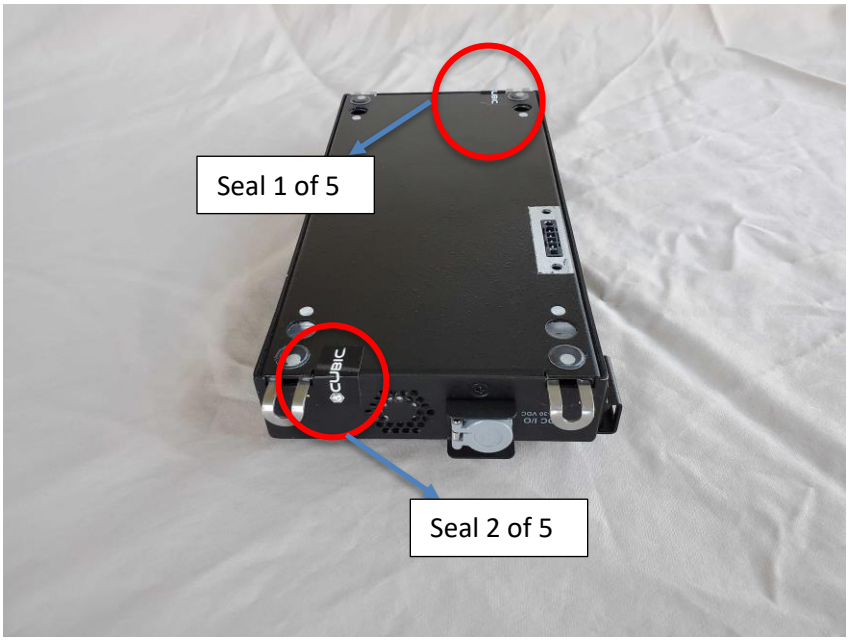

Figure 11 – M3-SE-MFGW Factory-Applied Tamper-Evident Seals – Bottom Side View

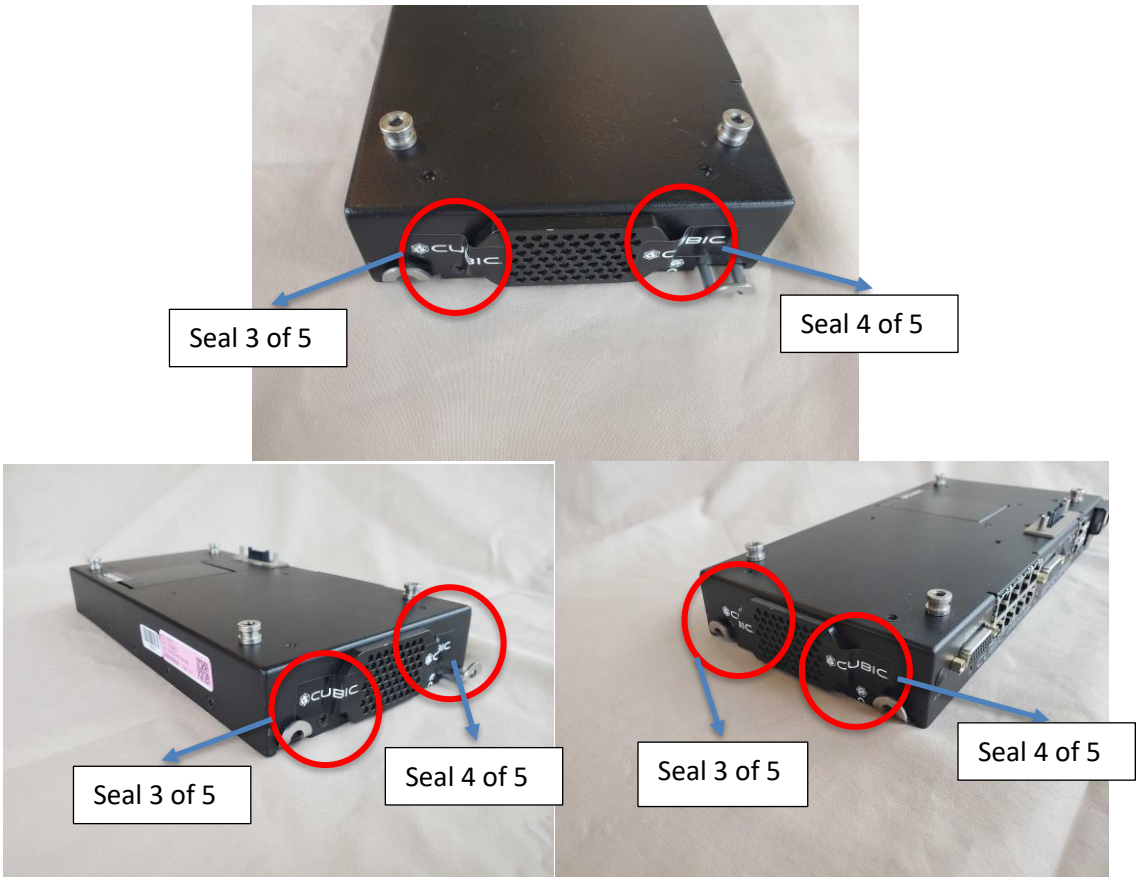

Figure 12 – M3-SE-MFGW Factory Applied Tamper-Evident Seals – Fan Cover (Top and Angled Views)

Figure 13 – M3-SE-MFGW Factory Applied Tamper-Evident Seal – Radio Access Cover

3.1.2 Initialization

First time access to the RoIP and M3-SE appliances requires the CO to connect locally to each appliance's Node UI and perform the initialization steps via the Initial Configuration Wizard.

To complete the initial configuration, the CO shall perform the following steps:

1. Fit the external antennas to the SMA[74] female ports of the appliance.
2. Connect the appliance to an IP network using the WAN (ETH1) Ethernet port.
3. Connect power.
4. Connect radios to audio and serial connectors, as required.
5. Ensure that the PC is connected to the ETH2 port and set to automatically acquire an IP address via DHCP[75].
6. Open your desktop web browser and type http://192.168.0.199 (default IP address for the unit).
7. The Initial Configuration Wizard will start.
8. Check Accept box and click Next.
9. Create the initial administrator user account by entering username and password and repeating password in the configuration wizard box.
10. Click Next.
11. Select Enable to enable the WAN port and then click Finish.

3.1.3 Configure Secure Network Access

Each appliance has two Ethernet ports: one WAN port (ETH1) and one LAN port (ETH2). By default, all WAN access to the appliance is disabled, and the LAN port is assigned to the default known IP address (refer to Section 3.1.2) to perform the initialization steps.

After initialization, the CO must replace the known IP address for the LAN port, enable access to the WAN port, and set up HTTPS access to the Node UI, the module's Web-based management interface. After ensuring that the WAN port is connected to an IP network and the LAN port is connected to Customer Premises Equipment (CPE), the CO shall perform the following steps via the Node UI:

1. Login to Vocality RoIP using the administrator account created in Section 3.1.2.
2. If the customer wants to change the default LAN and WAN ports, navigate to **Network > LAN Port** and **Network > WAN Port** and set up the IP address and network settings for each Ethernet port.
3. If the customer wants to change the default certificate, navigate to **Tunnels > Certificate & Key Management** and upload a public HTTPS certificate and private key to be used by the appliance. This certificate should be issued by a trusted CA.
4. If a certificate was loaded, navigate to **Platform > Access** and select the uploaded HTTPS certificate from step 3.
5. Select the **Minimum TLS Version** (TLS V1.0, TLS V1.1, or TLSV 1.2).

For more information, refer to the *Vocality RoIP User Manual* and the *Vocality Gateway Suite User Manual*.

3.1.4 Upload Licenses

Certain Vocality Gateway Suite features are locked and must be activated by uploading pre-purchased licenses. Once purchased, Vocality Support provides the CO with a single license file containing all feature licenses. The CO shall upload the license file using the **Licence** menu of the Node

1. Select Upload new license file and browse.
2. Select the license file and click open.
3. Click Upload.

[74] SMA – SubMiniature version A
[75] DHCP – Dynamic Host Configuration Protocol

4. A pop-up window “Upload Licence” appears. Click continue.
5. At this point, it takes about five minutes while the unit restores factory defaults and reboots. Upon the reboot, FIPS self-tests are performed.
6. Repeat steps 7-11 in section 3.1.2 (recreating the initial administrator account) and all the steps in section 3.1.3.

The following Vocality Gateway Suite features require licenses:

- Secure
- Failover
- Dispatch
- Radio (first radio port is licensed by default)

After the license file has been uploaded, the **Licence** page will display the current status of all licenses in use.

3.1.5 Set up IPsec Tunnels

If the Secure License Tunnel feature has been purchased, the CO shall set up IPsec tunnels to secure all IP traffic communication between the module and peer nodes. To set up IPsec tunnels, the CO shall follow these steps:

1. If the customer wants to change the default public IKE certificate and private key, navigate to **Tunnels > Certificate & Key Management** and upload a public IKE certificate and private key to be used by the appliance. This certificate should be issued by a trusted CA.
2. If the customer want to change the defaults, upload the CA root certificate of the peer node, and the peer node certificate ID[76].
3. Navigate to **Tunnels > Summary > Add Tunnel > Launch Wizard** to start the Tunnel Configuration Wizard.
4. Follow the steps in the *Vocality RoIP Application Note 010 V1.1- IPsec Configuration* to configure the IPsec tunnel. Clicking in the question marks next to each field in the wizard also provides helpful information.
5. After reviewing configuration, click the **Finish** button. The tunnel will appear as **Disabled** by default on the **Tunnels > Summary** page.
6. Configure the peer node with the same tunnel type and encryption parameters as the source node.
7. Using the Node UI for each node, navigate to **Tunnels > Summary** and select **Enabled** for the configured tunnel. Click Continue on Enable Tunnel window.

For more information, refer to the “Define tunnels” and “Set up IPsec” sections of the *Vocality Gateway Suite User Manual*. All the application notes referred to above may be found here:
https://support.vocality.com/hc/en-us/sections/360002860840-Application-Notes

3.1.6 Set up Secure Radio Talk Groups

The CO shall configure SRTP or TLS to secure radio talk group communication. To configure SRTP or TLS for radio talk groups, the CO shall follow these steps:

1. First, configure radio audio ports by following the instructions in the *Vocality RoIP Application Note 001 V1.0 - Audio Port Configuration Wizard.*
2. Navigate to Modules → **Radio > Talk Groups > Add Talk Group** to open the Radio Talk Group Wizard.
3. Configure TLS by following the instructions in the *Vocality RoIP Application Note 003 V1.0 -TLS Radio Talk Group Wizard.* Note that Radio Security must be licensed for TLS setup.

[76] ID – Identifier

4. Configure SRTP by following the instructions in the *Vocality RoIP Application Note 007 V1.0 - Secure SIP.*

For more information, refer to the "Set up Radio Talk Groups" section of the *Vocality Gateway Suite User Manual*.

3.2 Crypto Officer Guidance

The CO is responsible for ensuring that the module is operating in its FIPS-Approved mode of operation. When configured according to section 3.1 in this Security Policy, the module only runs in a FIPS-Approved mode of operation.

3.2.1 Password Complexity

Passwords have a 69-character password space (26 uppercase letters, 26 lowercase letters, 10 digits, and 7 special characters). COs shall follow the password complexity policy below for creating the CO and User password:

- Passwords must contain at least eight characters
- Passwords must contain at least one digit (0 – 9)
- Passwords must contain one of the following special characters: !, £, $, %, ^, &, *

3.2.2 Monitoring Status

The CO shall be responsible for regularly monitoring the module's status for FIPS-Approved mode of operation. When configured according to the CO guidance in this security policy, the module only operates in the FIPS-Approved mode.

The module's operational status is indicated with LEDs (refer to the "LED meanings" section of the *Vocality RoIP User Manual* for more information). The CO can also view the operational status by navigating to **Platform > Status** via the Node UI, which displays general information about the appliance.

Navigating to License will show that a FIPS license is being used and indicates that all the FIPS self-tests have passed.

3.2.3 Firmware Loading

The module's firmware can be updated using the Node UI. After the CO uploads a new firmware image, the RoIP performs the Firmware update/load test using ECDSA P-384 signature verification. If the test is passed, the CO is notified of the success and the module automatically reboots to load the new firmware image. If the test is failed, the module transitions to the "Soft Error" state and the module discards the new image.

Please note that, in order to maintain the modules' validation status, only FIPS-validated firmware shall be loaded. Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this Security Policy and will require a separate FIPS 140-2 validation.

3.2.4 Zeroization

In order to zeroize all plaintext non-ephemeral keys and CSPs (except for hardcoded keys), the module must be returned to the factory state. Zeroization can be accomplished in the following ways:

- Press the reset button on the appliance for more than five seconds
- Navigate to **Platform > Config Files** and click the **Reset** button via the Node UI

Once invoked, the effect of the zeroization process is immediate and will not allow sufficient time to compromise any stored plaintext CSPs. After zeroization, the module will need to be rebooted and reinitialized to return to operation.

3.2.5 Cryptographic Bypass Modes

While operating in the FIPS-Approved mode of operation, radio talk group and IP network communications may operate in a bypass mode, wherein voice and/or IP data is transmitted and received by the module as plaintext. The module requires multiple independent actions in order to be placed into a bypass mode.

IPsec tunnels are configured and enabled as part of the initial configuration steps in section 3.1.5. To set the exclusive bypass mode to bypass encryption for IP network connections, a CO must disable/delete the configured IPsec tunnels or replace the IPsec tunnels with GRE or IP-in-IP tunnels (or IPsec with AH mode enabled). To do this, the CO must follow one of these set of steps:

Option 1 (disable or delete all IPsec tunnels):

1. Navigate to **Tunnels > Summary**.
2. For each configured IPsec tunnel, select **Disabled** from the drop-down menu or click the **Delete** icon next to the IPsec tunnel. A prompt will appear asking to confirm.
3. Click **Continue** to confirm changes.
4. Repeat steps 1-3 for the peer node.

Option 2 (replace IPsec tunnels with GRE or IP-in-IP tunnels):

1. Navigate to **Tunnels > Summary**.
2. For each configured IPsec tunnel, click the adjacent **Edit** icon.
3. Change the Tunnel Type field to **IP-in-IP** or **GRE** to send IP network data in plaintext or configure the IPsec tunnel to use AH mode.
4. Configure all applicable parameters and review changes. Click **Finish**.
5. Repeat steps 1-4 for the peer node.

Radio talk groups are configured to use SRTP or TLS as part of the initial configuration steps in section 3.1.6. To set the exclusive bypass mode to bypass encryption for radio talk group communication, a CO must set the secure protocol to “none”. To do this, the CO must follow these steps:

1. Navigate to **Radio > Talk Groups > Edit** to open the Radio Talk Group Wizard.
2. Click the **Next** button to view the Secure Configuration page.
3. Under Secure Configuration, change the Type field to **None.** Configure all other relevant parameters.
4. Review the configuration and click the **Finish** button.
5. The customer must ensure that the remote server supports an unencrypted connection.

To determine if the connections are operating in a bypass mode, the CO can navigate to **Tunnels > Summary** to check if IP network traffic is secured using IPsec tunnels, or to **Radio > Talk Groups** to check if radio talk group traffic is secured using SRTP or TLS. If the SRTP or TLS protocols are not configured, or if one or more IP tunnels are not configured to use IPsec (excluding AH mode), the module is operating in a bypass mode.

When returning from the bypass mode back to the non-bypass mode, the module performs the Cryptographic Bypass Test to ensure correct encryption functionality.

For more information, refer to the "Define tunnels", "Set up IPsec", and "Set up Radio Talk Groups" sections of the *Vocality Gateway Suite User Manual*.

3.3 User Guidance

While the CO is responsible for ensuring that the module's physical security mechanisms are in place and that the appliances are running in their FIPS-Approved mode of operation, Users should also monitor appliance status. Any changes in the status of the appliances should immediately be reported to the CO. Additionally, when changing their own password, Users should follow the password complexity rules listed in Section 3.2.1.

3.4 Additional Guidance and Usage Policies

This section notes additional guidance and policies that must be followed by module operators.

- Module operators shall ensure that only those algorithms and key sizes mentioned in Section 2.7 (Cryptographic Key Management) of this document are in use to remain in the FIPS-Approved mode of operation.
- After initial configuration and setup is complete, module operators shall ensure that all access to the Node UI occurs over HTTPS to remain in the FIPS-Approved mode of operation.
- If power to the module is lost and subsequently restored, then any AES-GCM keys used for encryption or decryption must be re-distributed.
- SNMPv3 mode must be configured, not SNMPv2C.
- When selecting DH groups for IKE, only the following groups shall be selected: 2048, 3072, 4096, 6144, and 8192-bit DH public keys.
- PoE is not recommended to be used.
- DTLS shall not be configured for Radio talk groups.

3.5 Non-FIPS-Approved Mode

When configured according to the CO guidance in this Security Policy, the module does not support a non-FIPS-Approved mode of operation.

4. Acronyms and Abbreviations

Table 16 provides definitions for the acronyms and abbreviations used in this document.

Table 16 – Acronyms and Abbreviations

Acronym	Definition
4G	Fourth Generation
AES	Advanced Encryption Standard
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CA	Certificate Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CCM	Counter with CBC-MAC
CCCS	Canadian Centre for Cyber Security
CDH	Cofactor Diffie-Hellman
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CMS	Cubic Mission Solutions
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CODEC	Compression/Decompression
CPE	Customer Premises Equipment
CPU	Central Processing Unit
CRNGT	Continuous Random Number Generator Test
CSP	Critical Security Parameter
CTR	Counter
CVL	Component Validation List
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
eMMC	embedded Multi-Media Controller

Acronym	Definition
FIPS	Federal Information Processing Standard
FOM	FIPS Object Module
Gbps	Gigabits per second
GCM	Galois/Counter Mode
GPIO	General Purpose Input/Output
GRE	Generic Routing Encapsulation
GW	Gateway
HMAC	(keyed-) Hash Message Authentication Code
HTTPS	Hypertext Transfer Protocol Secure
ID	Identifier
IKE	Internet Key Exchange
I/O	Input/Output
IP	Internet Protocol
IPsec	Internet Protocol Security
ISDN	Integrated Services Digital Network
IV	Initialization Vector
KAS	Key Agreement Scheme
KAS-SSC	Key Agreement Scheme - Shared Secret Computation
KAT	Known Answer Test
KDF	Key Derivation Function
LAN	Local Area Network
LED	Light Emitting Diode
LMR	Land Mobile Radio
LTE	Long Term Evolution
M3	Micro, Mobile, Modular
MCU	Microcontroller Unit
MFGW	Multi-Function Gateway
N/A	Not Applicable
NAT	Network Address Translation
NDRNG	Non-Deterministic Random Number Generator
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OS	Operating System
PCT	Pairwise Consistency Test
PKCS	Public Key Cryptography Standard
PoE	Power over Ethernet

Acronym	Definition
PSK	Pre-shared Key
PSS	Probabilistic Signature Scheme
PTT	Push-to-talk
PUB	Publication
QoS	Quality of Service
RoIP	Radio over Internet Protocol
RSA	Rivest Shamir and Adleman
SDRAM	Synchronous Dynamic Random-Access Memory
SE	Single Enclave
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SNMPv3	Simple Network Management Protocol version 3
SMA	SubMiniature version A
SP	Special Publication
SRTCP	Secure Real-time Transport Control Protocol
SRTP	Secure Real-time Transport Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
UI	User Interface
U.S.	United States
USB	Universal Serial Bus
VPN	Virtual Private Network
WAN	Wireless Area Network

Prepared by:

Corsec Security, Inc.

13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com