Motorola Solutions, Inc. Voice Processing Module Cryptographic Module (VPMCM) / Telephone Media Gateway Cryptographic Module (TMGCM) Non-Proprietary Security Policy

Document *Version 1.1*

Revision Date: April 11, 2022

TABLE OF CONTENTS

1. Module Overview

The Voice Processing Module Cryptographic Module (VPMCM) / Telephone Media Gateway Cryptographic Module (TMGCM), otherwise referred to as the module (HW P/Ns VPMCRYPTO_B or VPMCRYPTO_C; FW Version R01.13.00), with AES256 Encryption Algorithm (FW Version R01.00.00) installed is a FIPS 140-2 validated cryptographic module whose central purpose is to provide cryptographic services to the Voice Processing Module in which it is embedded. The Voice Processing Module provides dispatch console audio routing between a dispatch operator (e.g., 911, dispatcher) and a local network. The module is a hardware module with a multi-chip embedded physical embodiment as defined by the FIPS 140-2 standard. The boundary is defined as being only the perimeter of the metal enclosure and the PC board within that enclosure (see red outline in Figures 1 and 2). Within this enclosure are multiple Motorola Advanced Crypto Engine (MACE) Atmel 518591 processors (Model #5185912Y01 or #5185912Y03) used for handling cryptographic services. There are 64 traces on the board that pass into the boundary and continue out of the boundary, with no connections to any components within the module; therefore, they are excluded from the interfaces of the module. The module (HW P/N VPMCRYPTO_B, VPMCRYPTO_C; FW Version R01.13.00) is referred to as the Telephone Media Gateway Cryptographic Module (TMGCM) when it provides cryptographic services for interconnect calls. In this context, TMGCM is simply another name for VPMCM.

Figure 1 – Front of the Cryptographic Module

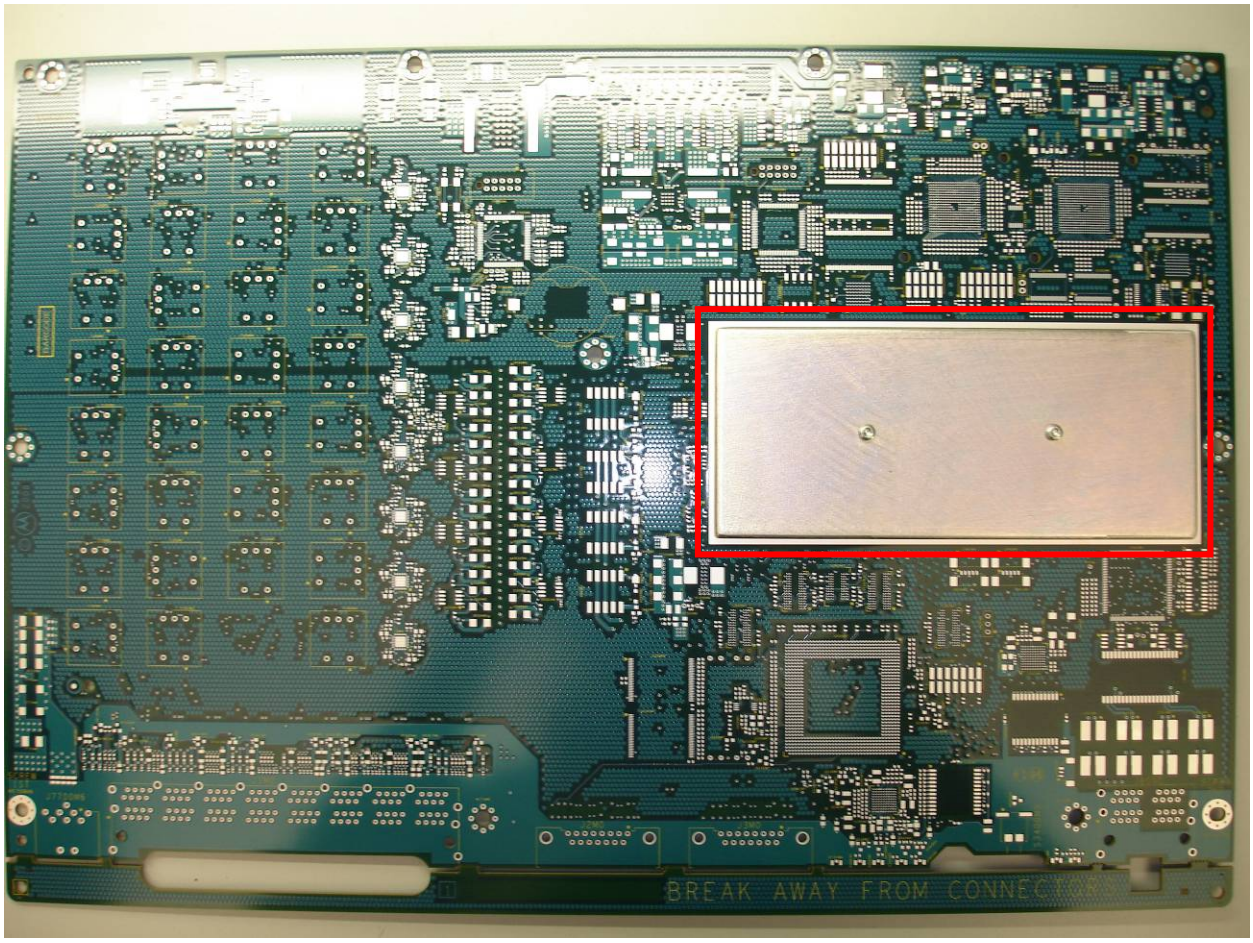
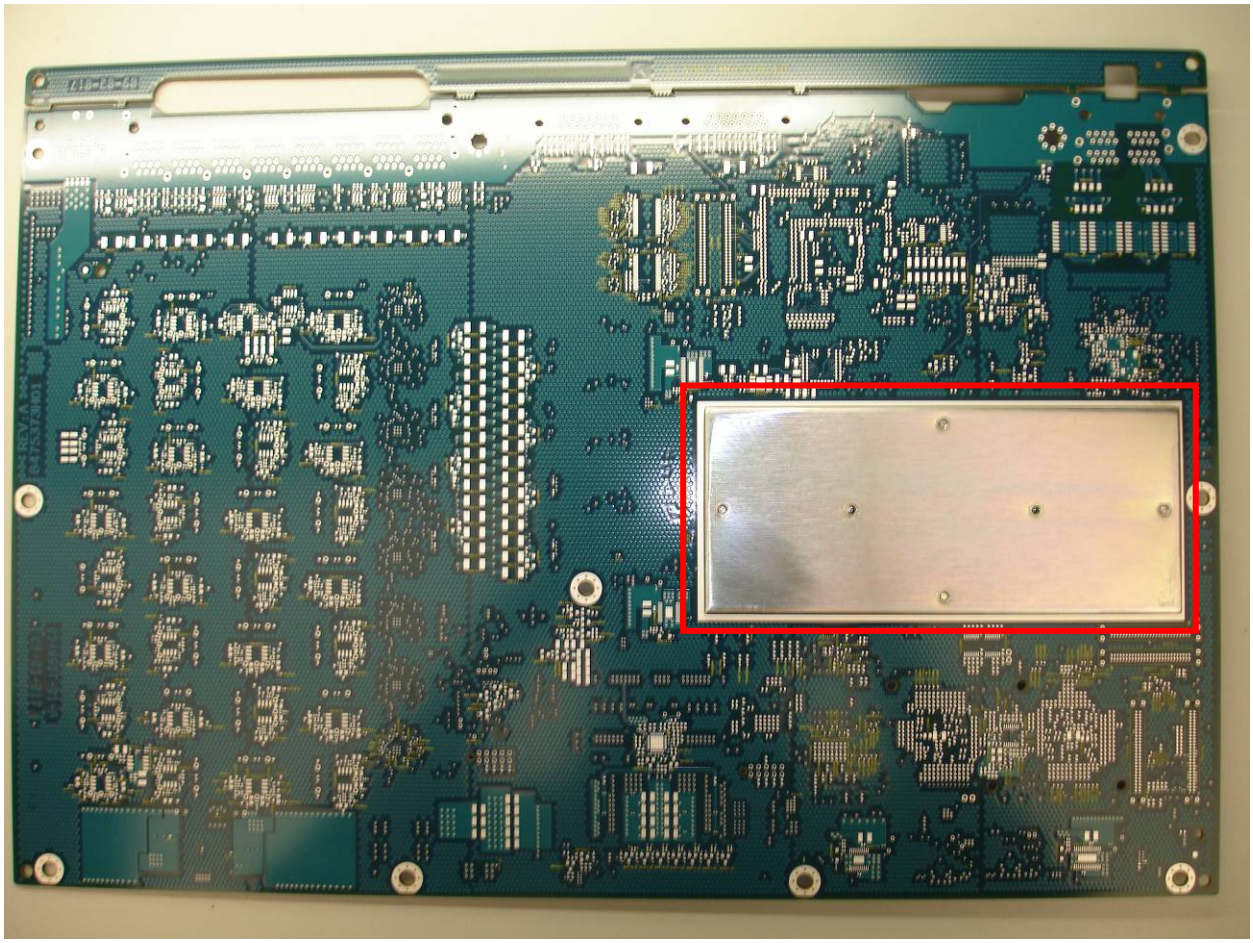


Figure 2 – Back of the Cryptographic Module



2. Security Level

This cryptographic module is designed to operate at FIPS 140-2 overall Security Level 1. The table below shows the FIPS 140-2 Level of security met for each of the eleven areas specified within the FIPS 140-2 security requirements.

Table 1 – VPMCM/TMGCM Cryptographic Module Security Level Specification

FIPS 140-2 Security Requirements Section	Validated Level at overall Security Level 1
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	1
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	1
Self-Tests	1
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall Security Level	**1**

3. Mode of Operation

The module must be configured to operate in either a FIPS Approved or Non-Approved mode of operation. Documented below are the configuration settings that are required for the module to be used in a FIPS 140-2 Approved mode of operation at overall Security Level 1. To verify that the Module is in the Approved mode of operation, output from the FIPS Status service can be obtained as specified in Table 2.

Table 2 - FIPS Mode Status

FIPS Mode	Status Message
Enabled	FIPS status is: FIPS Level 1
Disabled (Non-Compliant Algorithm)	FIPS status is: FIPS mode is disabled, due to non-compliant algorithms loaded
Disabled (No External Entropy)	FIPS status is: FIPS mode is disabled, due to lack of external entropy seed

3.1. FIPS Approved Mode Configuration

The following procedure shall be followed by an authorized operator during the initialization of the module upon first use:

Use the Program Update service to install only the AES256 Encryption Algorithm (FW Version R01.00.00). AES is the only Approved algorithm which is configurable using the Program Update service. For a full list of algorithms used in FIPS Approved Mode, please see Tables 3 and 4. Upon each power-up of the module, the external host is responsible for automatically uploading entropy to the module in order for the module to operate in FIPS mode. If external entropy is not provided to the module, the module will internally generate entropy and FIPS mode will be disabled.

3.2. FIPS Approved Mode

FIPS Approved mode is a mode of operation in which only Approved or Allowed algorithms are able to be utilized. The cryptographic module supports the following FIPS Approved algorithms.

Table 3 – FIPS Approved Algorithms

FIPS Approved Algorithm	CAVP Cert. #	Description of Use
AES-256 encrypt/decrypt (OFB, CBC, ECB, and CFB8)	819	When installed, used for Encryption/Decryption within APCO OTAR to provide secure key establishment and data confidentiality.
AES-256 Key Unwrap (SP800-38F)	5452	Used to unwrap keys entered into the module
CKG (Vendor Affirmed)	IG D.12	Key generation: [133rev2] Section 4 and 6.1 Direct symmetric key generation using unmodified DRBG output

FIPS Approved Algorithm	CAVP Cert. #	Description of Use
DRBG (SP800-90A AES-256 CTR DRBG)	A1635	Used for IV and KPK generation.[1]
KTS	N/A	AES KW Cert. #5462, Key Establishment methodology provides 256 bits of strength.
RSA-2048 PKCS #1 V1.5 (signature verification)	396	Used for digital signature verification during software/firmware integrity test and software/firmware load test.
SHA-256	817	Used for digital signature verification during software/firmware integrity test and software/firmware load test.

Table 4 – FIPS Allowed Algorithms

FIPS Allowed Algorithm	CAVP Cert. #	Description of Use
AES MAC	819	Used to provide authentication within APCO OTAR. AES MAC as used within APCO OTAR has been vendor affirmed and is approved when used for Project 25 APCO OTAR.

In the non-Approved mode of operation, the module implements the following non-Approved cryptographic algorithms: ADP, DES-OFB, DES-XL, DVI-XL and DVP-XL. It should be noted that if any or all of the aforementioned algorithms are loaded onto the module, it automatically defaults to the non-FIPS approved mode of operation. The non-FIPS approved algorithms must be removed, leaving only AES, for the module to function in FIPS Approved mode of operation. In addition, the module will zeroize/invalidate all keys when transitioning between FIPS approved and non-FIPS approved modes.

[1] The entropy for seeding the SP 800-90A DRBG is determined by the user of the module which is outside of the module's physical boundary. The target application shall use entropy sources that meet the security strength required for the random number generation mechanism as shown in [SP 800-90A] Table 3 (CTR_DRBG) and set required bits into the module by calling module defined API functions. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys.

4. Ports and Interfaces

Table 5 below provides a listing and description of all VPM physical ports and logical interfaces.

Table 5 – Ports and Interfaces Description

Physical Port	Qty	Logical interface definition	Technical Specification
Synchronous Serial Interface (SSI)	1	- Data input - Data output - Status output - Control input	The SSI interface provided by the module provides the central control interfaces accessible by an operator. It directly interfaces with a QUICC Ethernet controller.
Key Variable Loader (KVL)	1	- Data input - Status output - Control input	This interface provides the input and output to a Key Variable Loader (KVL).
FPGA	1	- Data input - Data output - Status output - Control input	The FPGA interface is used for audio and control data between the MACE ICs and the DSPs
Power Input	1	- 3.3v Power input	This port is the only power input port supported by the module.

5. Identification and Authentication Policy

5.1. Assumption of roles

The module supports two distinct operator roles (User, Cryptographic-Officer). The following tables explain these roles, and their respective authentication policies/mechanisms in further detail:

Table 6 – Roles

Role	Type of Authentication
Cryptographic Officer Role	The role is implicitly assumed.
User Role	The role is implicitly assumed.

6. Physical Security

The VPMCM/TMGCM module is a multi-chip embedded cryptographic module which includes the following physical security mechanisms:

- Production-grade components with standard passivation.

7. Services and Critical Security Parameters

This section lists the services available to the Module in the Approved and non-Approved Modes. Note that the services available to the non-Approved Mode are the same as those available to the Approved Mode; the only difference is that non-Approved algorithms will be used for some services while in the non-Approved Mode.

7.1. Services

Table 7 – Services

Name of Service	Service Description
Load Entropy	Load external entropy used to seed the DRBG. Available in both FIPS and non-FIPS mode.
Privileged APCO OTAR	Modify and query the Key Database via APCO OTAR Key Management Messages. Available in both FIPS and non-FIPS mode.
Encrypt Digital	The Encrypt Digital service is used to configure and encrypt voice transmissions or other data. Available in both FIPS and non-FIPS mode.
Decrypt Digital	The Decrypt Digital service is used configure and decrypt voice transmissions or other data. Available in both FIPS and non-FIPS mode.
AES Key Unwrapping	AES Key Unwrapping is for the decryption of keys using the AES Key Wrap algorithm.
Bypass	Configure a voice call in plaintext. Available in both FIPS and non-FIPS mode.
Transfer Key Variable	The Transfer Key Variable Service is used to manually establish keys to the module Key Database via a Key Variable Loader (KVL). Available in both FIPS and non-FIPS mode.
Change Active Keyset	This service modifies the currently active keyset used for selecting keys for encryption / decryption services. An active keyset is used to store a group of keys for current use, while inactive keysets are used to store keys for future use. Available in both FIPS and non-FIPS mode.
Delete Key Variable	Invalidate KEKs and TEKs via the KVL interface. Available in both FIPS and non-FIPS mode.
Keyset Check	Obtain status information about a specific keyset. Available in both FIPS and non-FIPS mode.
Key Query	Obtain status information about a specific TEK or KEK via the KVL interface. Available in both FIPS and non-FIPS mode.
Configure Module	Perform configuration of the module (e.g., OTAR configuration) via the KVL interface. Available in both FIPS and non-FIPS mode.
Algorithm List Query	Provides a list of algorithms loaded onto the Module via the KVL UI. Available in both FIPS and non-FIPS mode.
Program Update	The Program Update service is used to modify module firmware. Firmware upgrades are authenticated using a digital signature. The Program Update Public Signature Key (a 2048-bit public RSA key) is used to validate the signature of the firmware image being loaded before it is allowed to be executed. All keys and CSPs are preserved during a Program Update, and zeroized/invalidated only under the following circumstances: 1. Key Database Version/Format Change 2. Programming of non-FIPS algorithms, causing a FIPS mode transition Available in both FIPS and non-FIPS mode. Note: To maintain FIPS 140-2 validation, only validated firmware can be loaded.

Name of Service	Service Description
Version Query	Provides module firmware version numbers via the KVL UI. Available in both FIPS and non-FIPS mode.
FIPS Status	Provides current FIPS status. Available in both FIPS and non-FIPS mode.
Perform Self Tests	Performs module Power-On Self-Tests which are comprised of cryptographic algorithms test and firmware integrity and load tests. Initiated by module reset or transition from power off state to power on state. Available in both FIPS and non-FIPS mode.
Reset Crypto Module	Soft reset of module to remove module from error states or a transition from power off to power on state. Available in both FIPS and non-FIPS mode.
Erase Crypto Module	Zeroize/invalidate all keys from the Key Database. Available in both FIPS and non-FIPS mode.
Non-Privileged APCO OTAR	Status and Capabilities Key Management Messages (KMM) used to determine system compatibility and connectivity. Available in both FIPS and non-FIPS mode.
Extract Action Log	Status Request. Provides detailed history of error events. Available in both FIPS and non-FIPS mode.
Clear Error Log	Clears history of error events. Available in both FIPS and non-FIPS mode.
FIPS Diagnostic Status	Display the current number of calls, clear vs. secure. Available in both FIPS and non-FIPS mode.
Download Configuration Parameters	Download configuration parameters used to specify module behavior. Available in both FIPS and non-FIPS mode.

7.2. Definition of Critical Security Parameters (CSPs)

The following CSPs and keys are contained within the module:

Table 8 – CSP Definitions

CSP	Description/Usage
SP800-90A DRBG Seed	This is a 384-bit seed value used within the SP800-90A DRBG. The seed is derived using the Input String as external entropy (256-bits) and an internally generated personalization string (128-bits). The seed is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. Entry – n/a Output - n/a Storage – in plaintext in volatile memory Zeroization - on power off Generation – internally by combining entropy from an external source and an internally generated personalization string
Input String	This is a 256-bit string entered into the module from an external source for input into the DRBG Seed. The input string is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. Entry – Entropy supplied from an external source in plaintext. Output - n/a Storage – in plaintext in volatile memory Zeroization - on power off Generation –n/a
SP800-90A internal state (“V” and “Key”)	This is the internal state of the SP800-90A DRBG during initialization. The internal state is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The internal state is not entered into or output from the module. Entry - n/a Output - n/a Storage – in plaintext in volatile memory Zeroization - on power off Generation - Internal to the SP800-90A DRBG
Image Decryption Key (IDK)	A 256-bit AES key used to decrypt downloaded images. The IDK is not output from the module. Entry - on Program Update service request Output - n/a Storage - Plaintext in RAM, plaintext in Flash, with one half of the key stored in the boot block and the other stored in boot ROM Zeroization - on Program Update service request Generation - n/a
Key Encryption Keys (KEKs)	256-bit AES Keys used for encryption of keys in OTAR. KEKs are entered in plaintext form via the KVL and via OTAR. KEKs received via OTAR are encrypted with another KEK. Stored in plaintext in RAM and encrypted by the KPK in flash. KEKs are not output from the module. Entry – plaintext via KVL, input encrypted with AES Key Wrap over the Ethernet Interface Output – N/A

CSP	Description/Usage
	Storage – stored encrypted by KPK with AES256-CFB8 in non-volatile memory Zeroization - on Delete Key Variable, Erase Crypto Module, and Program Update service requests
Key Protection Key (KPK)	This is a 256-bit AES key used to encrypt all other keys stored in non-volatile memory. Generated internally using the SP800-90A DRBG. Stored in plaintext in non-volatile memory. The KPK is not entered into or output from the module. Entry - n/a Output - n/a Storage – stored in plaintext in non-volatile memory Zeroization - on Program Update, and Erase Crypto Module service requests Generation - SP800-90A DRBG
Traffic Encryption Keys (TEKs)	256-bit AES Keys used for enabling secure communication with target devices and for encryption and authentication of Key Management Messages in OTAR. TEKs are entered encrypted (AES Key Wrapping) over the Ethernet interface. The TEKS are stored encrypted with the KPK (AES256-CFB8) in non-volatile memory. TEKs are stored in plaintext in RAM only as long as needed. Entry – input encrypted with AES Key Wrap over the Ethernet Interface Output – n/a Storage – stored encrypted on KPK with AES256-CFB8 in non-volatile memory Zeroization - on Delete Key Variable, Erase Crypto Module, and Program Update service requests

Table 9 – Public Key(s)

Public Key	Description/Usage
Public Programmed Signature Key	A 2048-bit RSA public key used to validate the signature of the firmware image being loaded before it is allowed to be executed. Stored in non-volatile memory. Loaded during manufacturing and as part of the boot image during a Program Update service. The Public Programmed Signature Key is not output from the module. Entry - on Program Update service request Output - n/a Storage - in plaintext in non-volatile memory Zeroization - on Program Update service request Generation - n/a

7.3. CSP Modes of Access

The following tables describe the various methods in which keys are accessed in the VPMCM/TMGCM as well as how access is controlled per operator and service.

Table 10 – CSP Access Types

CSP Access Type	Description
C – Check CSP	Checks status and key identifier information of key.
D – Decrypt CSP	Decrypts TEK or KEK retrieved from non-volatile memory using the KPK.
E – Encrypt CSP	Encrypts TEK or KEK with KPK prior to storage in non-volatile memory.
G – Generate CSP	Generates KPK, SP800-90A DRBG internal state
I – Invalidate CSP	Marks encrypted TEKs or KEKs stored in non-volatile memory as invalid. TEKs or KEKs marked invalid can then be over-written when new TEKs or KEKs are stored.
S – Store CSP	Stores CSPS as follows: KPK in volatile and non-volatile memory. Encrypted TEKs or KEKs in non-volatile memory, over-writing any previously invalidated TEK or KEK in that location. Plaintext IDK in non-volatile memory.
U – Use CSP	Uses CSP internally to perform service
Z – Zeroize CSP	Zeroizes key/CSP.
- – No access	The service does not access the CSP.

Table 11 – CSP versus CSP Access

Service	CSP							Role	
	Input String	SP800-90 A seed	SP800-90 A seed internal state	IDK	KEKs	KPK	TEKs	User Role	Crypto-Officer Role
Load Entropy	U	G	-	-	-	-	-	√	√
Privileged APCO OTAR	-	-	-	-	D, U, E, Z, S	U	D, U, E, I, Z, S	√	√
Encrypt Digital	-	-	-	-	-	U	D, U	√	√
Decrypt Digital	-	-	-	-	-	U	D, U	√	√
AES Key Unwrap		-	-	-	U	-	-		
Bypass	-	-	-	-	-	-	-	√	√
Transfer Key Variable	-	-	-	-	D, E, Z, S	U	D, E, I, Z, S	√	√
Change Active Keyset	-	-	-	-	-	-	-	√	√
Delete Key Variable	-	-	-	-	I	-	I	√	√
Keyset Check	-	-	-	-	C	-	C	√	√
Key Query	-	-	-	-	D	U	D	√	√
Configure Module	-	-	-	-	-	-	-	√	√
Algorithm List Query	-	-	-	-	-	-	-	√	√
Version Query	-	-	-	-	-	-	-	√	√
Program Update	-	-	-	U, Z, S	Z	Z	Z	√	√
FIPS Status	-	-	-	-	C	-	C	√	√
Perform Self-Tests	-	-	-	-	-	-	-	√	√
Reset Crypto Module	Z	Z	G, U, Z	-	-	G, S	-	√	√
Erase Crypto Module	Z	Z	G, U, Z	-	I	G, S	I	√	√
Non-Privileged APCO OTAR (not for key entry)	-	-	-	-	-	-	-	√	√
Extract Action Log	-	-	-	-	-	-	-	√	√
Clear Error Log	-	-	-	-	-	-	-	√	√
FIPS Diagnostic Status	-	-	-	-	-	-	-	√	√
Download Configuration Parameters	-	-	-	-	I	Z, G, S	I	√	√

8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the VPMCM/TMGCM module supports a limited modifiable operational environment.

9. Security Rules

The VPMCM/TMGCM module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module.

1. The cryptographic module shall provide two distinct operator roles. These are the User role and the Cryptographic Officer role.
2. The cryptographic module shall perform the following tests:
    A. Power up Self-Tests
        i. Cryptographic algorithm test:
            1. SHA-256 Known Answer Test (KAT)
            2. AES-256 KAT for each mode in the OFB, CBC, ECB, and 8-bit CFB (encrypt and decrypt). (Cert. # 819)
            3. AES-256 KW KAT (decrypt only) (Cert. #5452)
            4. SP800-90A DRBG KAT Section 11.3 Health Tests (instantiate, reseed, and generate)
            5. RSA 2048 is tested as part of the Firmware integrity test. RSA is only used to perform signature verification.
        ii. Firmware integrity test: A digital signature is generated over the code when it is built using SHA-256 and RSA-2048 and is stored with the code upon download into the module. When the module is powered, up the digital signature is verified.
    B. Conditional Tests
        i. Firmware load test: A digital signature is generated over the code when it is built using SHA-256 and RSA-2048. Upon download into the module, the digital signature is verified. If the digital signature matches the test passes, otherwise it fails.
        ii. SP800-90A DRBG Continuous Test
        iii. Alternating Bypass Test: The module performs two independent internal tests to verify that clear calls are processed correctly.
3. At any time, the operator shall be capable of commanding the module to perform the power-up self-test by using the Reset service or by Power-cycling the module
4. Data output shall be inhibited during self-tests, zeroization, and error states.
5. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

This section documents the security rules imposed by the vendor:

1. The VPMCM/TMGCM module does not support multiple concurrent operators.
2. The module does not support the output of plaintext or encrypted keys.

10. Mitigation of Other Attacks Policy

The VPMCM/TMGCM has not been designed to mitigate any specific attacks.

11. Glossary

KeyDatabase	A database containing KEKs and TEKs.
KeySet	Logical grouping of keys. KeySets can be active (available for use) or inactive (not available for use).

12. Acronyms

ALGID	Algorithm Identifier
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CKR	Common Key Reference
CO	Crypto Officer
CPS	Customer Programming Software
CSP	Critical Security Parameter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
IV	Initialization Vector
KEK	Key Encryption Key
KAT	Known Answer Test
KID	Key Identifier
KLK	Key Loss Key
KMM	Key Management Message
KPK	Key Protection Key
KTS	Key Transport Scheme
KVL	Key Variable Loader
MAC	Message Authentication Code
MACE	Motorola Advanced Crypto Engine
OFB	Output Feedback
OTAR	Over The Air Rekeying
PRNG	Pseudo Random Number Generator
RNG	Random Number Generator
TEK	Traffic Encryption Key
TMGCM	Telephone Media Gateway Cryptographic Module
VPMCM	Voice Processing Module Cryptographic Module