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

Document *Version 2.5*

Revision Date: July 12, 2018

**TABLE OF CONTENTS**

# 1. Module Overview

The Voice Processing Module Cryptographic Module, otherwise referred to as the VPMCM (HW P/Ns VPMCRYPTO_B or VPMCRYPTO_C; FW Version R01.11.00, R01.11.01, R01.11.02, or R01.11.03), 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 VPMCM 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). 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 VPMCM (HW P/N VPMCRYPTO_B, VPMCRYPTO_C; FW Version R01.11.00, R01.11.01, R01.11.02, or R01.11.03) 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**

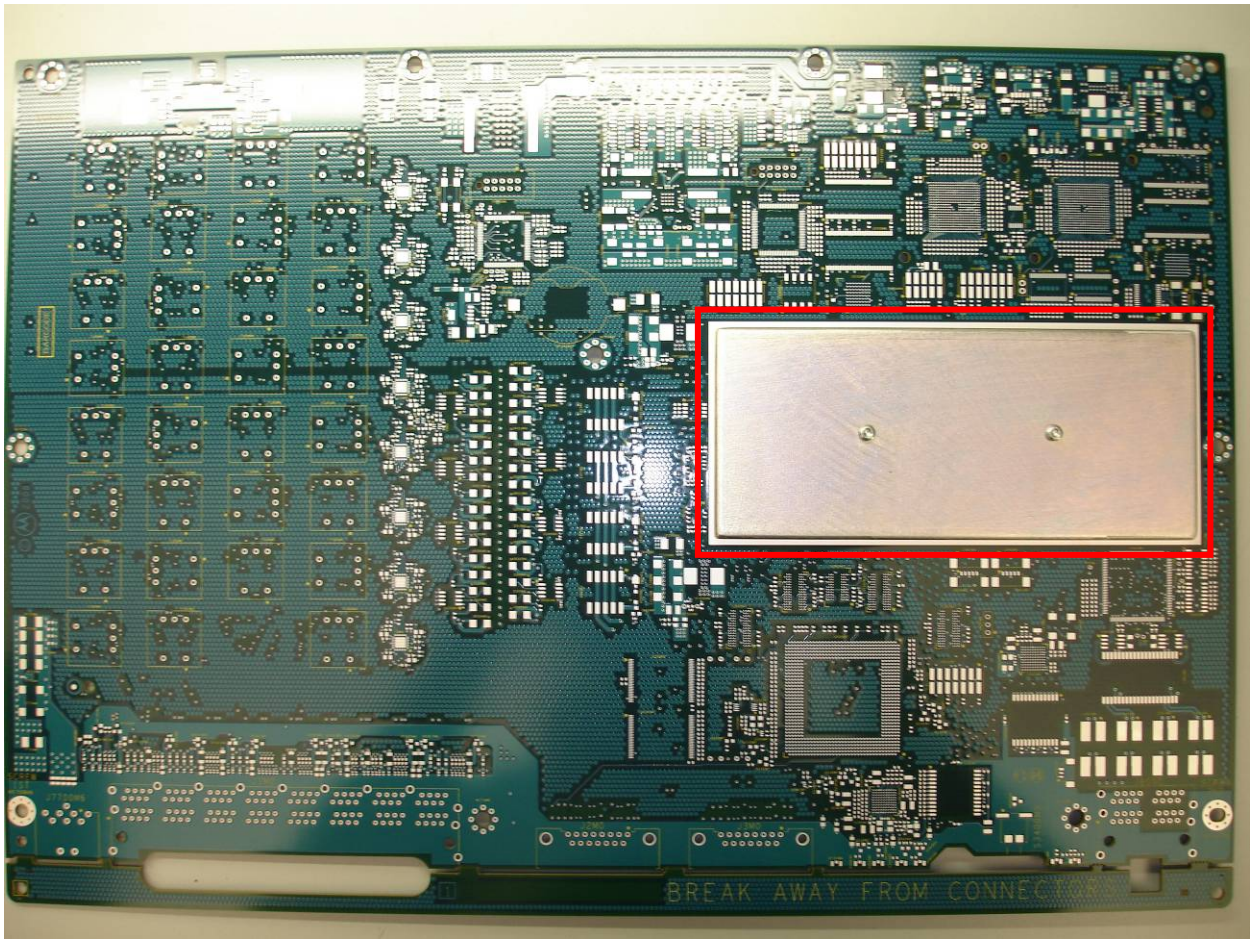
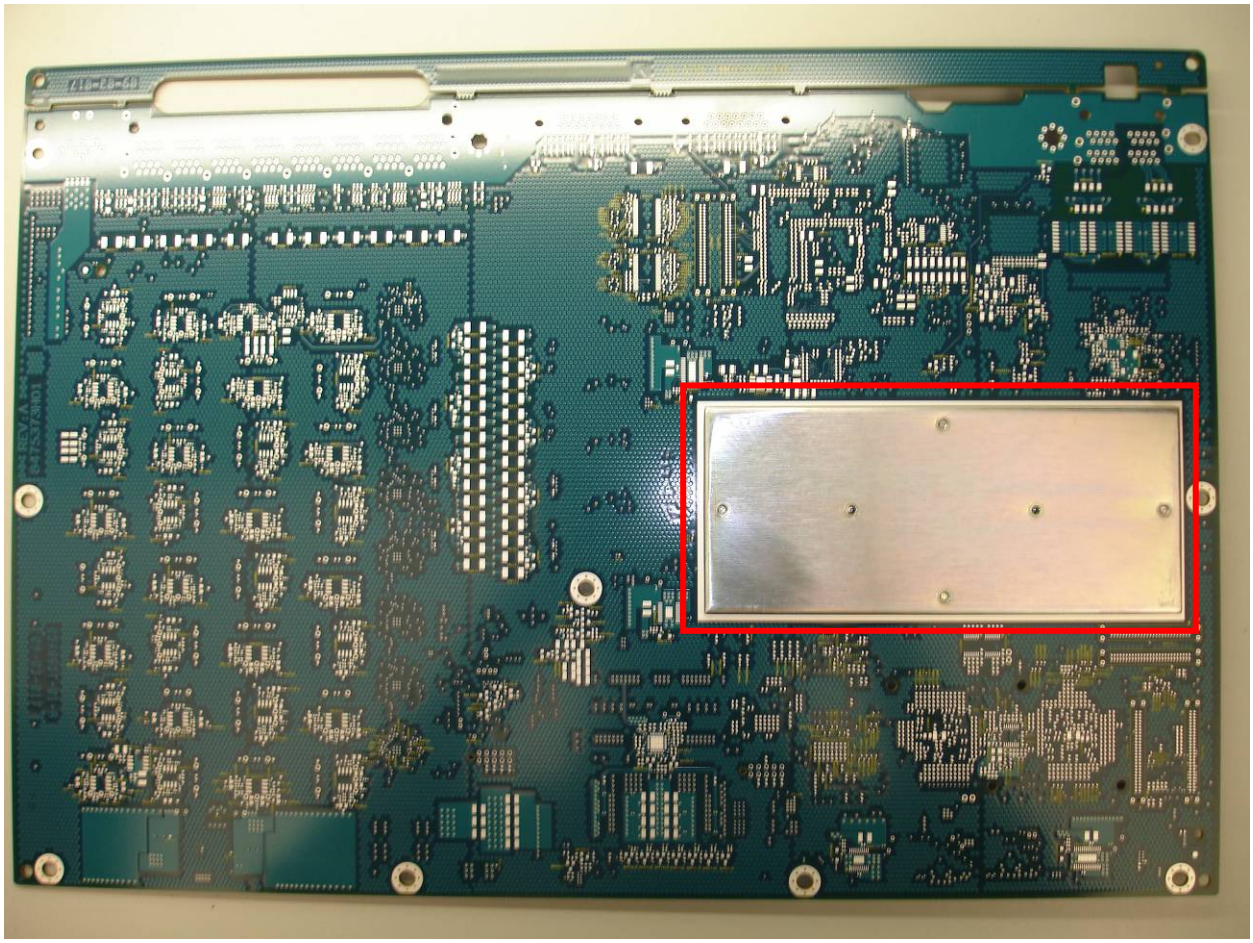


**Figure 2 – Back of the Cryptographic Module**



# 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 | 2 |
| 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 |

# 3. Mode of Operation

The VPMCM can operate in a FIPS 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. At any given time, the FIPS Status service can be used to confirm that the module is operating in FIPS Approved mode.

## *3.1. FIPS Approved Mode Configuration*

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

Use the Program Update service to install only the AES algorithm. 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 2 and 3.

## *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 2 – 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. Key Establishment methodology provides 256 bits of strength. |
| AES Key Unwrap | 5452 | Used to unwrap keys entered into the module |
| SHA-256 | 817 | Used for password hashing for internal password storage and digital signature verification during software/firmware integrity test and software/firmware load test. |
| RSA-2048 PKCS #1 V1.5 (signature verification) | 396 | Used for digital signature verification during software/firmware integrity test and software/firmware load test.<br>Note: signature generation was tested, but is not utilized. |
| SP800-90A AES-256 CTR DRBG | 505 | Used for IV and KPK generation. |

**Table 3 – 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. |
| Non-Deterministic Hardware Random Number Generator (NDRNG) | N/A | Used to provide Initialization Vectors (IV) and seeds to the FIPS Approved Deterministic Random Number Generator (RNG). The minimum number of bits of entropy generated by the module for key generation is at least 384 bits |

In the non-Approved mode of operation the module implements the following non-Approved cryptographic algorithms: DVP-XL, DVI-XL, DES-XL, and ADP. 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.

# 4. Ports and Interfaces

Table 4 below provides a listing and description of all VPM physical ports and logical interfaces.

**Table 4 – Ports and Interfaces Description**

| Physical Port | Qty | Logical interface definition | Technical Specification |
|---|---|---|---|
| Synchronous Serial Interface (SSI) | 1 | - Data input<br>- Data output<br>- Status output<br>- 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<br>- Status output<br>- Control input | This interface provides the input and output to a Key Variable Loader (KVL). |
| FPGA | 1 | - Data input<br>- Data output<br>- Status output<br>- 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 VPMCM/TMGCM supports two distinct operator roles (User, Cryptographic-Officer). The following tables explain these roles, and their respective authentication policies/mechanisms in further detail:

**Table 5 – Roles and Required Identification and Authentication**

| Role | Type of Authentication | Authentication Data | Description |
|---|---|---|---|
| Cryptographic Officer Role | Role Based authentication | Password: Knowledge of a 10 digit password string. | The Cryptographic Officer role is authorized to perform the program update service provided by the module. |
| User Role | Role Based authentication | Password: Knowledge of a 10 digit password string. | The User role is the day to day user of the module. |

**Table 6 – Strengths of Authentication Mechanisms**

| Authentication Mechanism | Strength of Mechanism |
|---|---|
| Password Authentication | The probability that a random attempt will succeed or a false acceptance will occur is no greater than 1/10^10, which is less than 1/1,000,000.<br>The VPMCM/TMGCM will allow fewer than 15 authentication attempts in a one minute period; therefore the random success rate for multiple retries is 15/10^10, which is less than 1/100,000. |

# 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. Access Control Policy

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. User Services*

**Table 7 – User Services**

| Name of Service | Service Description |
|---|---|
| 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. |
| Validate Password | Validate the current password used to identify and authenticate the User or CO role. Fifteen consecutive failed attempts causes the KPK to be zeroized, a new KPK to be generated, all TEKs and KEKs to be invalidated (key status is marked invalid), and the password to be reset to the factory default. Available in both FIPS and non-FIPS mode. |
| 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 | Zeroize 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. |
| Version Query | Provides module firmware version numbers via the KVL UI. Available in both FIPS and non-FIPS mode. |

## *7.2. Cryptographic Officer Services*

**Table 8 – Cryptographic Officer Services**

| Name of Service | Service Description |
|---|---|
| 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 only under the following circumstances:<br>1. Key Database Version/Format Change<br>2. Programming of non-FIPS algorithms, causing a FIPS mode transition<br>Available in both FIPS and non-FIPS mode.<br>Note: To maintain FIPS 140-2 validation, only validated firmware can be loaded. |
| Validate Password | Validate the current password used to identify and authenticate the User or CO role. Fifteen consecutive failed attempts causes the KPK to be zeroized, a new KPK to be generated, all TEKs and KEKs to be invalidated (key status is marked invalid), and the password to be reset to the factory default. Available in both FIPS and non-FIPS mode. |

## *7.3. Services Available to Unauthenticated Operators*

**Table 9 – Services Available to Unauthenticated Operators**

| Name of Service | Service Description |
|---|---|
| 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 all keys from the Key Database. Available without a Role. (Module can be reinitialized using a Key Variable Loader). 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 without a Role. 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. |

## *7.4. Definition of Critical Security Parameters (CSPs)*

The following CSPs and keys are contained within the module:

**Table 10 – 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 not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The seed is not entered into or output from the module.<br><br>Entry - n/a<br>Output - n/a<br>Storage – in plaintext in volatile memory<br>Zeroization - on power off<br>Generation - Non-deterministic Hardware Random Number Generator |
| 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. |

| CSP | Description/Usage |
|---|---|
| | Entry - n/a<br>Output - n/a<br>Storage – in plaintext in volatile memory<br>Zeroization - on power off<br>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.<br><br>Entry - on Program Update service request<br>Output - n/a<br>Storage - in plaintext in non volatile memory<br>Zeroization - on Program Update service request<br>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.<br><br>Entry – plaintext via KVL input encrypted with AES Key Wrap over the Ethernet Interface<br><br>Output – N/A<br><br>Storage – stored encrypted on KPK with AES256-CFB8 in non volatile memory<br><br>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.<br><br>Entry - n/a<br>Output - n/a<br>Storage – stored in plaintext in non volatile memory<br>Zeroization - on Program Update, and Erase Crypto Module service requests<br>Generation - SP800-90A DRBG |
| Password | The 10-digit password is entered encrypted on the PEK. After decryption the plaintext password is not stored but temporarily exists in volatile memory. The SHA-256 hash of the decrypted password is compared with the hash value stored in non-volatile memory during password validation. The Password is entered encrypted on the PEK (AES256-CFB8). |

| CSP | Description/Usage |
|---|---|
| | Entry – entered encrypted on the PEK with AES256-CFB8<br>Output - n/a<br>Storage – a hash of the Password is stored in non-volatile memory<br>Zeroization – on Program Update service request<br>Generation - n/a |
| Password Encryption Key (PEK) | This is a 256-bit AES Key used for decrypting passwords during password validation. Loaded via the Program Update service. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. Also stored encrypted on the KPK in non volatile memory. The PEK is not output from the module.<br><br>Entry - on Program Update service request<br><br>Output - n/a<br><br>Storage - in plaintext in non volatile memory; encrypted on the KPK in non volatile memory<br><br>Zeroization - on Program Update service request<br><br>Generation - n/a |
| 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.<br><br>Entry – input encrypted with AES Key Wrap over the Ethernet Interface<br><br>Output – n/a<br><br>Storage – stored encrypted on KPK with AES256-CFB8 in non volatile memory<br><br>Zeroization - on Delete Key Variable, Erase Crypto Module, and Program Update service requests |

**Table 11 – 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.<br>Entry - on Program Update service request |

| **Public Key** | **Description/Usage** |
|---|---|
| | Output - n/a<br>Storage - in plaintext in non volatile memory<br>Zeroization - on Program Update service request<br>Generation - n/a |

### *7.5. 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 12 – 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.<br><br>Decrypts entered password with PEK during password validation. |
| **E** – Encrypt CSP | Encrypts TEK or KEK with KPK prior to storage in non-volatile memory. |
| **G** – Generate CSP | Generates KPK, SP800-90A DRBG seed/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 KPK in volatile and non-volatile memory.<br><br>Stores encrypted TEKs or KEKs in non-volatile memory, over-writing any previously invalidated TEK or KEK in that location.<br><br>Stores plaintext PEK or IDK in non-volatile memory. |
| **U** – Use CSP | Uses CSP internally for encryption / decryption services. |
| **Z** – Zeroize CSP | Zeroizes key. |

**Table 13 – CSP versus CSP Access**

| Service | CSP | | | | | | | | Role | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | SP800-90 A seed | SP800-90 A seed internal state | IDK | KEKs | KPK | Password | PEK | TEKs | User Role | Crypto-Officer Role | No Role Required |
| Privileged APCO OTAR | | | | d, u, i, e, z, s | u | | | d, u, i, e, z, s | √ | | |
| Encrypt Digital | | | | | u | | | d,u | √ | | |
| Decrypt Digital | | | | | u | | | d,u | √ | | |
| Validate Password | | | | i | z, g, s | d, u, z | u | i | √ | √ | |
| Bypass | | | | | | | | | √ | | |
| Transfer Key Variable | | | | d, i, e, z, s | u | | | d, i, e, z, s | √ | | |
| Change Active Keyset | | | | | | | | | √ | | |
| Delete Key Variable | | | | i | z | | | 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 | z, s | z | | √ | |
| FIPS Status | | | | c | | | | c | | | √ |
| Perform Self-Tests | g | g | | | | | | | | | √ |
| Reset Crypto Module | g, u, z | g, u, z | | | g, s | | | | | | √ |
| Erase Crypto Module | g, u, z | g, u, z | | z | g, s | z | | z | | | √ |

| **Service** | **CSP** | | | | | | | | **Role** | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | SP800-90 A seed | SP800-90 A seed internal state | IDK | KEKs | KPK | Password | PEK | TEKs | User Role | Crypto-Officer Role | No Role Required |
| 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 supports a non-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. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
3. 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.
            3. SP800-90A DRBG KAT
            4. SP800-90A Section 11.3 Health Tests
            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. Continuous Random Number Generator test
            1. SP800-90A DRBG Continuous Test
            2. NDRNG Continuous Test
        iii. Alternating Bypass Test
        iv. 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.

8. Data output shall be inhibited during self-tests, zeroization, and error states.
9. 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 does not support multiple concurrent operators.
2. After a sufficient number (15) of consecutive unsuccessful user login attempts, the module will zeroize all keys from the Key Database.
3. 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 |
| **ECB** | Electronic Code Book |
| **IV** | Initialization Vector |
| **KEK** | Key Encryption Key |
| **KID** | Key Identifier |
| **KLK** | Key Loss Key |
| **KMM** | Key Management Message |
| **KPK** | Key Protection Key |
| **KVL** | Key Variable Loader |
| **LFSR** | Linear Feedback Shift Register |
| **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 |