Voice Processing Module Cryptographic Module (VPMCM) Security Policy

Document *Version 1.4*

Revision Date: 9/22/2009

Copyright Motorola, Inc. 2009. May be reproduced only in its original entirety [without revision].

TABLE OF CONTENTS

1. Module Overview

The Voice Processor Module Cryptographic Module, otherwise referred to as the VPMCM (HW P/N VPMCRYPTO_B; FW Version R01.01.03), 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 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.

Figure 1 – Front of the Cryptographic Module

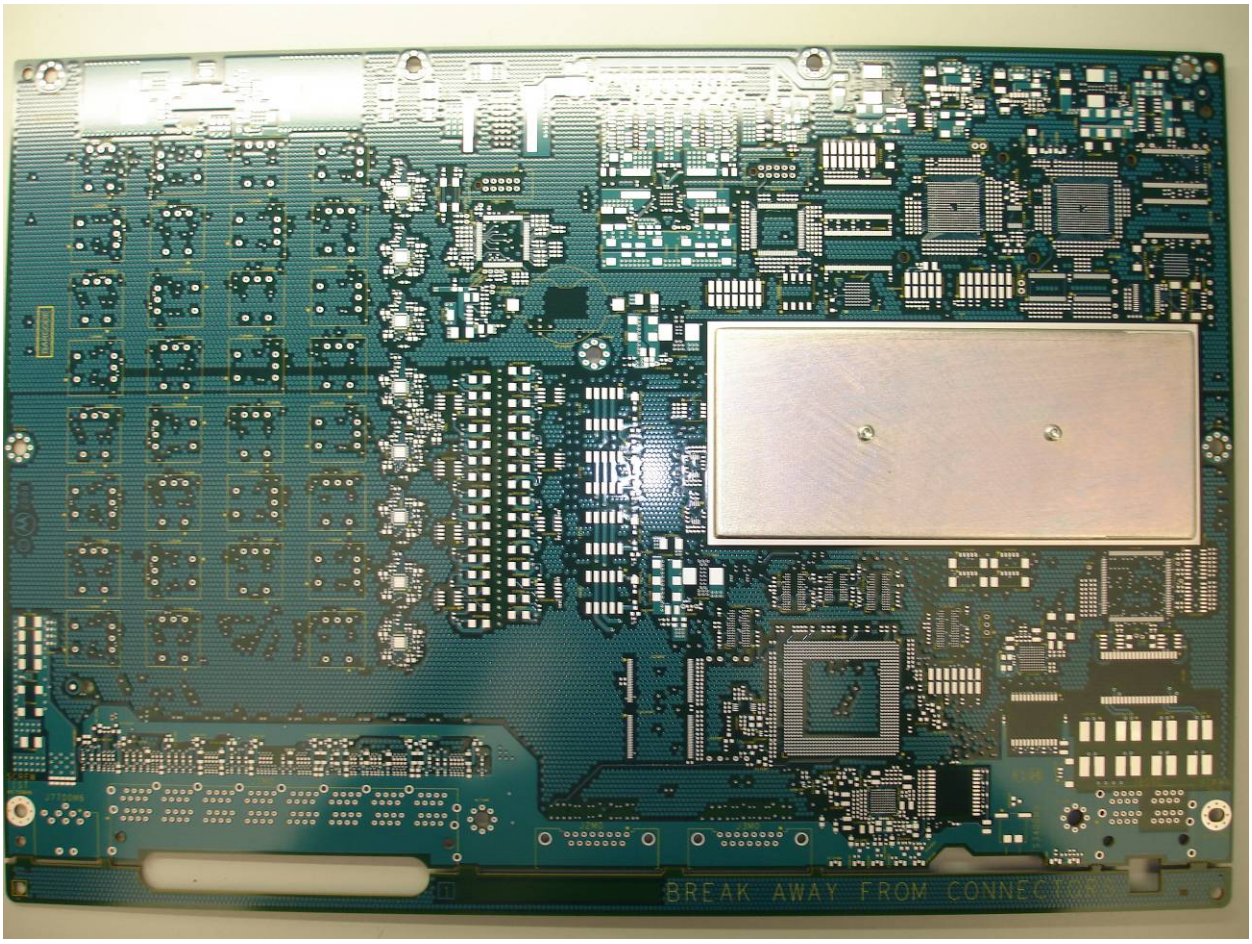
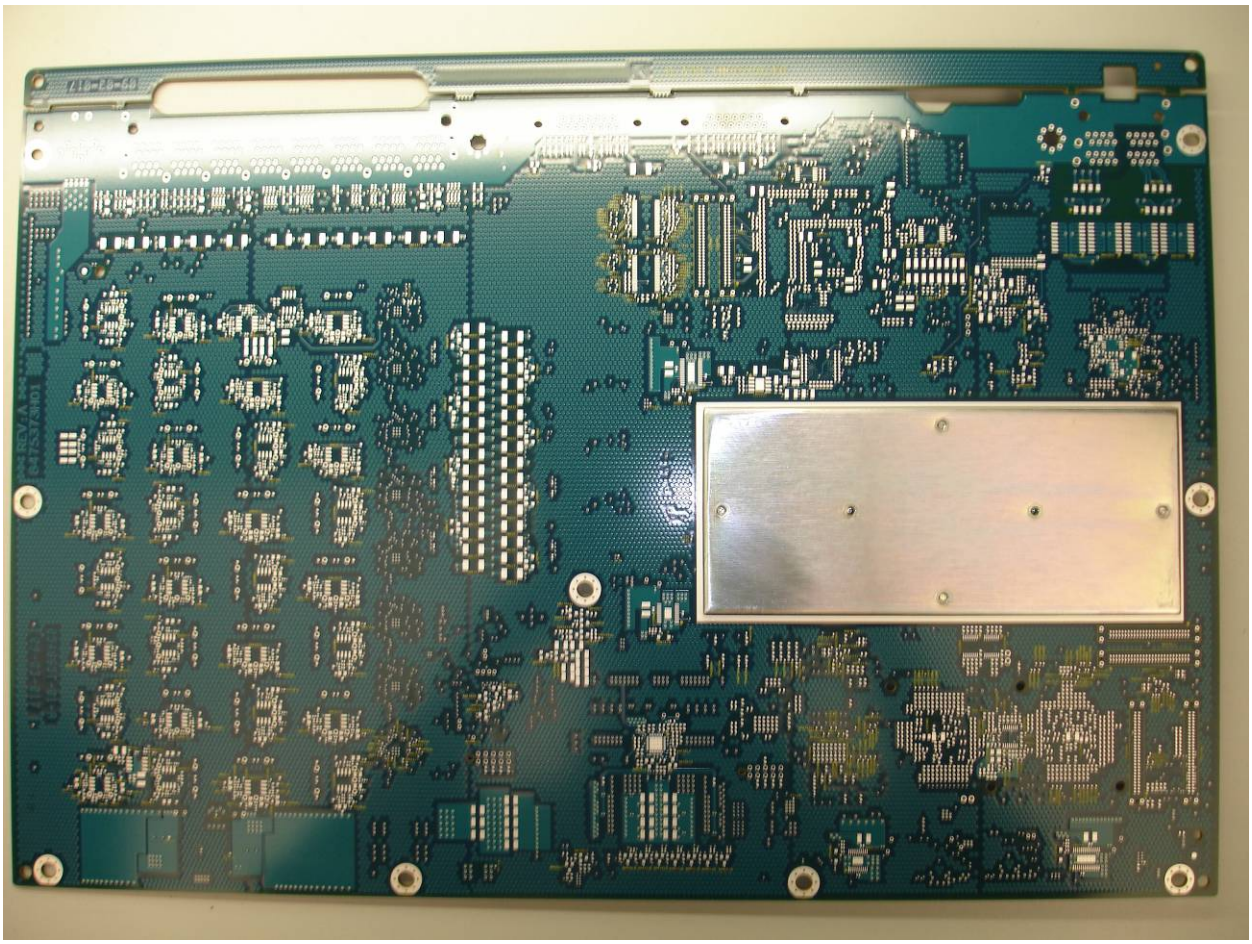


Figure 2 – Back of the Cryptographic Module



2. Security Level

The cryptographic module meets the overall requirements applicable to an overall Level 1 security of FIPS 140-2.

Table 1 – VPMCM Cryptographic Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	1
Module Ports and Interfaces	1
Roles, Services and Authentication	3
Finite State Model	1
Physical Security	1
Operational Environment	N/A
Cryptographic Key Management	1
EMI/EMC	2

Security Requirements Section	Level
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 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 Approved Mode

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.
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.
ANSI X9.31 Appendix 2.4 (2-key TDES) Deterministic Random Number Generator (RNG)	471	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).
64 bit Linear Feedback Shift Register (LFSR)	N/A	Used to provide IVs used during encryption and decryption.

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 - 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

Assumption of roles

The VPMCM supports two distinct operator roles (User and Cryptographic-Officer). The VPMCM uses a 10-digit password to authenticate the User and a digital signature to authenticate the Cryptographic Officer. The operator roles are uniquely identified by the specific service that they have requested.

Table 5 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data	Description
Cryptographic Officer Role	Identity-based operator authentication.	Digital Signature: Knowledge of the RSA Private key which corresponds to the Firmware Signature Key.	The Cryptographic Officer role is authorized to perform the program update service provided by the module.
User Role	Identity-based operator authentication.	Password: Knowledge of a 10 character 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
Cryptographic Officer Role	2048-bit Digital RSA Signature: The probability that a random attempt will succeed or a false acceptance will occur is no greater than 1/2^112, which is less than 1/1,000,000. The VPMCM will allow fewer than 30 program update attempts in a one minute period; therefore the random success rate for multiple retries is 30/2^112 , which is less than 1/100,000.
User Role	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. The VPMCM will allow fewer than 15 authentication attempts in a one minute period; therefore the random success rate for multiple retries is 10/10^10, which is less than 1/100,000.

6. Access Control Policy

User Services

Table 7 – User Services

Name of Service	Service Description
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).
Privileged APCO OTAR	Modify and query the Key Database via APCO OTAR Key Management Messages.
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.
Encrypt Digital	The Encrypt Digital service is used to configure and encrypt voice transmissions or other data.
Decrypt Digital	The Decrypt Digital service is used configure and decrypt voice transmissions or other data.
Keyset Check	Obtain status information about a specific keyset.
Validate Password	Validate the current password used to identify and authenticate the User 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.
Zeroize Selected Keys	Zeroize selected key variables from the Key Database by Physical ID (PID) or Common Key Reference (CKR).
Bypass	Configure a voice call in plaintext.

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 zeroized during a Program Update. Note: To maintain FIPS 140-2 validation, only validated firmware can be loaded.

Services Available to Unauthenticated Operators

Table 9 – Services Available to Unauthenticated Operators

Name of Service	Service Description
FIPS Status	Provides current FIPS status.
Initiate 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.
Zeroize All keys	Zeroize all keys from the Key Database. Available without a Role. (Module can be reinitialized using a Key Variable Loader)
Non-Privileged APCO OTAR	Status and Capabilities Key Management Messages (KMM) used to determine system compatibility and connectivity.
Reset Crypto Module	Soft reset of module to remove module from error states or a transition from power off to power on state.
Extract Error Log	Status Request. Provides detailed history of error events. Available without a Role.
Clear Error Log	Clears history of error events.
FIPS Diagnostic Status	Display the current number of calls, clear vs. secure.
Download Configuration Parameters	Download configuration parameters used to specify module behavior.

6. 1 Definition of Critical Security Parameters (CSPs)

The following CSPs and keys are contained within the module:

Table 10 – CSPs and Keys

CSP	Description/Usage
ANSI X9.31 seed	A 64-bit seed value used within the ANSI X9.31 RNG. The seed is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module.
ANSI X9.31 seed key	Key used to seed the ANSI X9.31 RNG during initialization. The seed key is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module.
Image Decryption Key (IDK)	A 256-bit AES key used to decrypt downloaded images. Stored in plaintext in non-volatile memory and zeroized through the Program Update service.
Key Encryption Keys (KEKs)	Keys used for encryption of other keys in OTAR. Stored encrypted on KPK in non-volatile memory.
Key Protection Key (KPK)	Key used to encrypt TEKs and KEKs stored in non-volatile memory.
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.

CSP	Description/Usage
Password Encryption Key (PEK)	Key used for decrypting password during password validation. Stored in plaintext in non-volatile memory and zeroized through the Program Update service.
Traffic Encryption Keys (TEKs)	Keys used for voice and data encryption. Stored encrypted on KPK in non-volatile memory.
Programmed Signature Key	2048 bit RSA public key used to validate the signature of the firmware image before it is allowed to be executed.

6. 2 CSP Modes of Access

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

Table 11 - 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. 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, ANSI X9.31 seed, or ANSI X9.31 seed key.
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. Stores encrypted TEKs or KEKs in non-volatile memory, over-writing any previously invalidated TEK or KEK in that location. 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 12 - CSP versus CSP Access

	CSP								Role		
Operator Service	ANSI X9.31 seed	ANSI X9.31 seed key	IDK (Image Decryption Key)	KEK (Key Encryption Key)	KPK (Key Protection Key)	Password	PEK (Password Encryption Key)	TEK (Traffic Encryption Key)	User Role	Crypto Officer Role	No Role Required
1. Program Update			u, z, s	z	z		z, s	z		√	
2. Transfer Key Variable				i, e, z, s	u			i, e, z, s	√		
3. Privileged APCO OTAR				d, u, i, e, z, s	u			d, u, i, e, z, s	√		
4. Change Active Keyset									√		
5. Bypass									√		
6. Encrypt Digital								d, u	√		
7. Decrypt Digital								d, u	√		
8. Zeroize Selected Keys				i				i	√		
9. Keyset Check				c				c	√		
10. FIPS Status				c				c	√	√	√
11. Initiate Self Tests									√	√	√
12. Validate Password				i	z, g, s	d, u, z	u	i	√		
13. Zeroize All Keys				i				i	√	√	√

	CSP								Role		
14. Non-Privileged APCO OTAR (not for key entry)									√	√	√
15. Reset Crypto Module	g, u, z	g, u, z			g, s				√	√	√
16. Extract Error Log									√	√	√
17. Clear Error Log									√	√	√
18. Download Configuration Parameters				i	z, g, s			i	√	√	√
19. FIPS Diagnostic Status									√	√	√

7. Operational Environment

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

8. Security Rules

The VPMCM 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. ANSI X9.31 RNG KAT
            4. 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. ANSI X9.31 Continuous Test
2. NDRNG Continuous Test
3. 64-bit LSFR 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 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.

9. Physical Security

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

Production-grade components.

10. Mitigation of Other Attacks Policy

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

11. Glossary

Ket Database	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
VPMCM	Voice Processing Module Cryptographic Module