Motorola Solutions Cryptographic Firmware Module

Cryptographic module used in Motorola Solutions Astro APX series and VX series subscribers.

Firmware Version: R01.01.02

Non-Proprietary Security Policy

Document Version: 1.12

April 18, 2018

Table of Contents

1. Introduction

1.1 Scope

This Security Policy document specifies the security rules under which the Motorola Solutions Cryptographic Firmware module (MSCFM) must operate.

1.2 Definitions

ALGID	Algorithm Identifier
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CSP	Critical Security Parameter
DES	Data Encryption Standard
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interface
GCM	Galois/Counter Mode
MSCFM	Motorola Solutions Cryptographic Firmware Module
NDRNG	Non-deterministic Random Number Generator
OFB	Output Feedback
PEK	Password Encryption Key
PRNG	Pseudorandom Random Number Generator
RBG	Random Bit Generator
RNG	Random Number Generator

1.3 Firmware Version Number

The Cryptographic module has the following FIPS validated firmware version number.

Firmware Version Number: R01.01.02

1.4 Module Overview

The MSCFM provides firmware based cryptographic solutions. It is a multi-chip standalone cryptographic module that runs on a general purpose computer operating environment. This firmware module provides FIPS 140-2 Approved cryptographic functionalities to different applications through Application Programming Interfaces.

The following block diagram (Figure 1) shows how the application interacts with the MSCFM,

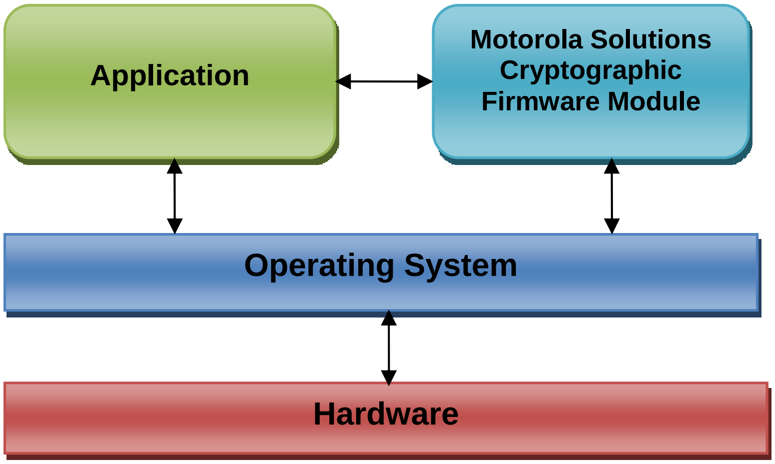

Figure 1: Motorola Solutions Cryptographic Firmware Module

MSCFM runs on the following operating system and hardware platforms:

- Motorola APX8000 Radio, Mentor Graphics Nucleus 3.0 (version 2013.08.1) on ARM926EJ-S core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM
- Motorola APX8000 Radio, Texas Instrument (TI) DSP/BIOS 5.41.04.18 on C674x Megamodule (v4.0) of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM

The cryptographic module also runs on the following operating systems for which operational testing was not performed:

- Linux 2.6.32-358.23.2.el6.x86_64 GNU/Linux
- Linux on OMAP C6000 DSP+ARM Processor

Note: the CMVP makes no statement as to the correct operation of the module on the operational environments for which operational testing was not performed.

1.5 Cryptographic Boundary

MSCFM is part of an application executable binary and delivered to the application as a static library, which is the logical boundary of the cryptographic module. The application linker pulls in required symbols from the static library and puts those symbols into a specific memory location.

Table 1: List of FIPS 140-2 Approved Crypto Libraries

Library Name	Operating System	Processor Name
libALG_nucleus.lib	Mentor Graphics Nucleus 3.0 (version 2013.08.1)	ARM926EJ-S core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM
libALG_dsp.lib	Texas Instrument (TI) DSP/BIOS 5.41.04.18	C674x Megamodule (v4.0) of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM

2. Ports and Interfaces

Physical ports of the module are provided by the general purpose computer operating system on which the module is running. The logical interfaces are defined as the API of the cryptographic module. All supported APIs in the firmware module support logical interfaces: data input, data output, control input, status output.

Table 2: Ports and Interfaces

Logical Interface Type	Description
Control input	API entry point and corresponding stack parameters
Data input	API entry point data input stack parameters
Status output	API entry point return values and status stack parameters
Data output	API entry point data output stack parameters

3. FIPS 140-2 Security Levels

MSCFM can only operate in an Approved mode 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 3: Security Levels

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	1
Mitigation of Other Attacks	N/A

4. Mode of Operation

The module can only operate in a FIPS 140-2 Approved mode of operation.

4.1 FIPS Approved Operational Modes

The cryptographic module always starts as FIPS 140-2 Approved mode of operation at overall Security Level 1; there is no configuration setting required during startup. The module supports the following Approved algorithms:

Table 4: List of Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode/Method	Key Length	Use
4517	AES	FIPS 197, SP 800-38A	ECB, OFB, CBC	256	Voice/Data Encryption/decryption
4517	AES	FIPS 197, SP 800-38D	GCM[1], GMAC (GMAC tested, but not used)	256	Voice/Data Encryption/decryption
5357	KTS[38F]	SP800-38F	KW	256	Key establishment methodology provides 256 bits of encryption strength
1478	DRBG	SP 800-90A	CTR_DRBG	AES-256	Deterministic Random Bit Generation
4517	KTS	IG D.9	GCM	256	Key Wrap
2984	HMAC	FIPS 198-1	HMAC-SHA-384	(192 - 1024) (must be multiple of 8)	Message authentication, Code Integrity tests
3705	SHS	FIPS 180-4	SHA-384, SHA-512	N/A	Message Digest

The module supports the following allowed algorithms:

Table 5: List of Allowed Algorithms

Algorithm	Caveat	Use
AES MAC (Cert. #4517)	Vendor Affirmed. Project P25 AES OTAR	Provide authentication within P25 APCO OTAR

5. Operational Environment

The MSCFM operates and was tested on the following non-modifiable operational environments:

- Motorola APX8000 Radio, Mentor Graphics Nucleus 3.0 (version 2013.08.1) on ARM926EJ-S core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM
- Motorola APX8000 Radio, Texas Instrument (TI) DSP/BIOS 5.41.04.18 on C674x Megamodule (v4.0) of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM

The cryptographic module is compiled on a Linux build server using a corresponding cross compiler and delivered as a static library that is linked into the application binary.

During power up of the target device, the cryptographic module calculates HMAC-SHA384 over only

[1] The AES GCM implementation complies with IG A.5, Scenario 2. The IV is randomly generated internally using an Approved DRBG, the DRBG seed is generated inside the module's physical boundary, and the IV length is at least 96 bits.

cryptographic .RODATA and .TEXT sections and compares the runtime calculated HMAC against application build time generated HMAC. The cryptographic module will enter into Uninitialized state (which is also considered as Error state) if the HMAC calculation does not match.

6. Crypto Officer and User Guidance

6.1 Administration of the module in a secure manner (CO)

The firmware based cryptographic module requires no special administration for secure use after it has successfully passed all Power-On Self-Tests.

6.2 Assumptions regarding User Behavior

The module has been designed in such a way that no special assumptions regarding User Behavior have been made that are relevant to the secure operation of the unit.

6.3 Approved Security Functions, Ports, and Interfaces available to Users

Services available to the User role are listed in section 10.2.

6.4 User Responsibilities necessary for Secure Operation

The module must be loaded successfully and pass code integrity, known answer tests.

7. Security Rules

The firmware module enforces the following security rules. These rules are separated into those imposed by FIPS 140-2 and those imposed by Motorola Solutions.

7.1 FIPS 140-2 Imposed Security Rules

1. The module does not provide any operator authentication.
2. The module implements all firmware using a high-level language.
3. The module encrypts/decrypts message traffic using AES algorithms.
4. The cryptographic module performs the following self-tests,
   Power-up Self-Tests:
   - Cryptographic algorithm tests
     - AES-256 Encrypt/Decrypt (ECB, OFB, CBC, GCM) KAT
     - SHA-384 KAT
     - SHA-512 KAT
     - HMAC-SHA384 KAT
     - DRBG KAT
   - Firmware Integrity Test: HMAC-SHA-384
   - Critical Functions Tests: N/A

   Conditional Self-Test: The cryptographic module performs the following conditional self-tests,
   Random number generation tests:
   - DRBG Continuous Tests
   - SP800-90A Health Tests
5. At any time, the application is capable of commanding the module to perform the power-up self-tests by

reloading the cryptographic module into memory.

6. The module is available to perform services only after successfully completing the power-up self-tests.
7. Data output shall be inhibited during self-tests and error states.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module shall not support a concurrent operator.
10. The module enters the Uninitialized state if any Power-up Self-Tests and conditional self-tests fail. The Uninitialized state can be exited by restarting the module.
11. The module does not perform any cryptographic functions while in the Uninitialized state.
12. The module preserves the results of power up and integrity Self-Tests; it can be retrieved out of the module via the module provided API.
13. The module is to be installed on a Motorola radio, which employs OTAR functionality.
14. The module may be power cycled to zeroize all CSPs.

7.2 Motorola Solutions Imposed Security Rules

The module does not support multiple concurrent operations.

8. Identification and Authentication Policy

As it is a firmware only cryptographic module, it does not provide any identification or authentication method of its own.

9. Physical Security Policy

The module is firmware only and operates on a radio that is built with production grade materials. For the purposes of FIPS 140-2, the embodiment is defined as a multiple-chip standalone cryptographic module and is designed to meet Level 1 security requirements.

10. Access Control Policy

10.1 Supported Roles

The module supports a User Role and Cryptographic Officer Role; no other roles are supported.

10.2 Available Services

Table 6: Available Services

Services	User	Cryptographic Officer
Self-Test	X	X
Show Status	X	X
Initialize	X	X
Initialization Status Query	X	X
Version Query	X	X
Utility	X	X
AES-256 Encryption Voice	X	X

AES-256 Decryption Voice	X	X
AES-256 Encryption Data	X	X
AES-256 Decryption Data	X	X
Key Wrapping	X	X
Key Unwrapping	X	X
Generate OTAR MAC	X	X
SHA384	X	X
SHA512	X	X
DRBG	X	X
HMAC-SHA384	X	X

12. Critical Security Parameters (CSPs)

All CSPs used by the cryptographic module are described in this section. All access to these CSPs by the cryptographic module service are described in Section 12.4.

Table 7: Critical Security Parameters

CSP Name	Description	Generation	Storage	Entry/Output	Destruction
AES-256 Encrypt key	AES Encryption	Externally	Volatile RAM	Entry: N/A Output: N/A	Power cycle. An application program that uses the module may destroy the key.
AES-256 Decrypt key	AES Decryption	Externally	Volatile RAM	Entry: N/A Output: N/A	Power cycle. An application program that uses the module may destroy the key.
Keyed hash key	HMAC SHA384 Message Authentication Code	Externally	Volatile RAM	Entry: N/A Output: N/A	Power cycle.
SP800-90A seed	This is a 384-bit seed value used within the SP800-90A DRBG.	Externally	Volatile RAM	Entry: N/A Output: N/A	The seed is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module.
SP800-90A internal state (“V” and “Key”)	This is the internal state of the SP800-90A DRBG during initialization.	Internally	Volatile RAM	Entry: N/A Output: N/A	The internal state is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module.
AES Key Encrypt Key	AES Key Wrapping	Externally	Volatile RAM	Entry: N/A Output: N/A	Power cycle. An application program that uses the module may destroy the key.
AES Key Decrypt Key	AES Key Unwrapping	Externally	Volatile RAM	Entry: N/A Output: N/A	Power cycle. An application program that uses the module may destroy the key.
OTAR MAC Key	APCO OTAR MAC Generation	Externally	Volatile RAM	Entry: N/A Output: N/A	Power cycle.

12.1 **CSP Access Types**

Table 8: CSP Access Type Acronyms

Access Type	**Description**
S - Store CSP	Stores CSP in volatile memory. The module uses CSPs passed in by the calling application on the stack.
U - Use CSP	Uses CSP internally for encryption / decryption services.
Z - Zeroize CSP	Zeroize key in volatile memory.

The target operating system protects memory and process space from unauthorized access. Keys residing in the Module's internally allocated data structure during the lifetime of the services defined in Table 6: Available Services can only be accessed through APIs defined in the module. The keys can be destroyed in the Module's volatile memory by power cycling or calling appropriate API function calls to overwrite keys.

The target applications 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 384 bits of entropy seed into the Module. The assurance of the minimum strength of the generated random bits from the module depends on the strength of the 384 bits of seed provided to the module. The target application collects 3840 bytes from each of 10 different Rx buffers, across all supported signaling modes and varied signal strength inputs, which results in 409.6 entropy bits that is then SHA-384 hashed to provide 384-bits of seed for DRBG initialization. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys.

Table 9: CSP-Services Access Matrix

CSP **Services**	AES-256 Encrypt key	AES-256 Decrypt key	Keyed hash key	SP800-90A seed	SP800-90A internal state (“V” and “Key”)	AES Key Encrypt Key	AES Key Decrypt Key	OTAR MAC Key
Self Test								
Show Status								
Initialize								
Initialization Status Query								
Version Query								
Utility								
AES-256 Encryption Voice	U,S,Z				U			
AES-256 Decryption Voice		U,S,Z						
AES-256 Encryption Data	U,S,Z				U			
AES-256 Decryption Data		U,S,Z						
Key Wrapping						U,S,Z		

CSP Services	AES-256 Encrypt key	AES-256 Decrypt key	Keyed hash key	SP800-90A seed	SP800-90A internal state (“V” and “Key”)	AES Key Encrypt Key	AES Key Decrypt Key	OTAR MAC Key
Key Unwrapping							U,S,Z	
Generate OTAR MAC								U,S
DRBG				U,S	U,S			
SHA384								
SHA512								
HMAC-SHA384			U,S					

13. **Mitigation of Other Attacks Policy**

The firmware module is not designed to mitigate any specific attacks outside of those required by FIPS 140-2, including but not limited to power consumption, timing, fault induction, or TEMPEST attacks.