MOTOROLA SOLUTIONS

Motorola Solutions Cryptographic Firmware Module

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

Firmware Version: R01.03.00

Non-Proprietary Security Policy

Document Version: 1.2

March 16, 2021

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: R01.03.00

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:

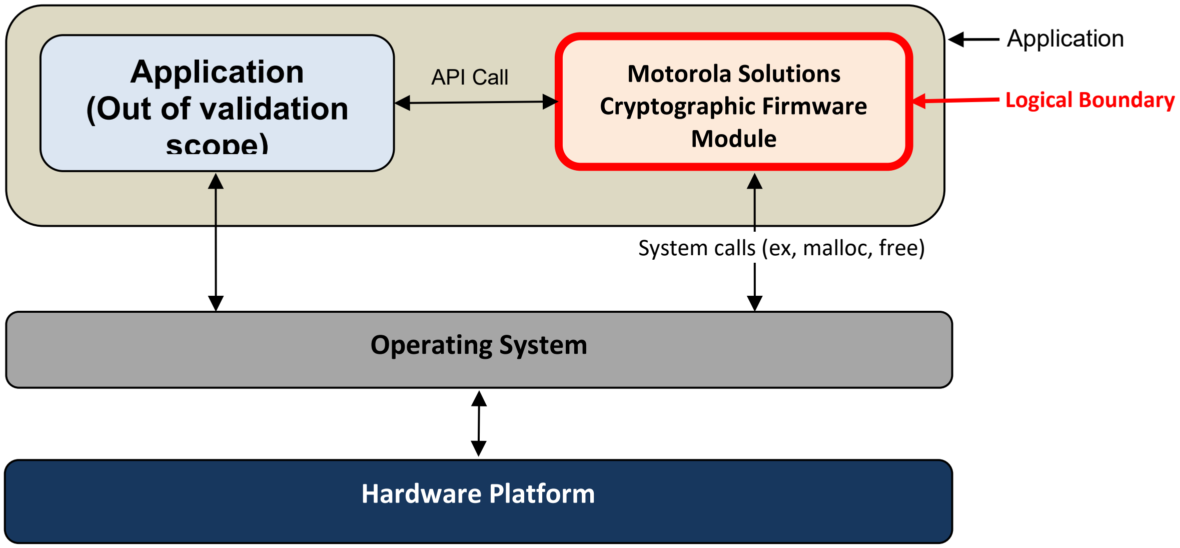
Application
(Out of validation scope)
API Call
Motorola Solutions Cryptographic Firmware Module
Application
Logical Boundary
System calls (ex, malloc, free)
Operating System
Hardware Platform

Figure 1: Motorola Solutions Cryptographic Firmware Module

MSCFM runs on the following operating system and hardware platforms:

- Motorola APX900 Radio, Mentor Graphics Nucleus 3.0 (version 2013.08.1) on ARM926EJ-S core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM
- Motorola APX900 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
- Microsoft Windows 7 and 10 Professional

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. The physical cryptographic boundary is the general-purpose computer on which the module is installed.

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

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 operates in two different modes of operation.

- FIPS Approved mode: DES Voice/Data Encryption/Decryption are blocked. All other services listed in the Section 10.2 are available when the module is operating in FIPS Approved mode.
- FIPS non-Approved mode: All services listed in the Section 10.2 are available when the module is operating in FIPS Non-Approved mode.

4.1 FIPS Approved Operational Modes

The module always powers up in FIPS Approved mode and executes power up self-tests as mentioned in the Section 7.1. The user of the module may change the mode of operation to FIPS non-Approved mode by calling "Set FIPS Mode" Service listed in the Section 10.2. The operator shall zeroize all CSPs by power cycling the module when transitioning between FIPS 140-2 Approved and non-Approved modes. The operator must retain control of the module while zeroization is in process.

Table 4: List of Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode/Method	Key Length	Use
C1702	AES	FIPS 197, SP 800-38A	ECB, OFB, CBC	256	Voice/Data Encryption/decryption
C1702	AES	FIPS 197, SP 800-38D	GCM[1], GMAC (GMAC tested, but not used)	256	Voice/Data Encryption/decryption
C1705	AES	SP800-38F	KW	256	Key Wrapping
C1704	DRBG	SP 800-90A Rev1	CTR_DRBG	AES-256	Deterministic Random Bit Generation
C1703	HMAC	FIPS 198-1	HMAC-SHA-384	Key Size: 1024 bit[2]	Message authentication, Code Integrity tests
C1705	KTS [38F]	SP800-38F	KW	256	Key establishment methodology provides 256 bits of encryption strength
C1702	KTS	IG D.9	GCM	256	
C1703	SHS	FIPS 180-4	SHA-384, SHA-512	N/A	Message Digest

The module supports the following allowed algorithms:

Table 5: Non-Approved but Allowed Cryptographic Functions

Algorithm	Caveat	Use
AES MAC (Cert. # C1702)	Vendor Affirmed. Project P25 AES OTAR	Provide authentication within P25 APCO OTAR

4.2 FIPS non-Approved Modes

The following FIPS non-Approved algorithms and protocols are allowed when the module is configured to operate in FIPS non-Approved mode of operation:

Table 6: List of FIPS Non-Approved Algorithms

Algorithm	Use
DES	DES Encryption/Decryption – ECB, OFB and CBC

[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.

[2] HMAC-SHA-384 supports keys sizes from 192-1024 bit but only 1024 bit was CAVP tested. Only the key size of 1024 bit shall be used in FIPS Approved Mode

	Mode

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 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 does not have bypass or maintenance mode.
4. The module encrypts/decrypts message traffic using AES algorithms.
5. The cryptographic module performs the following self-tests,
   Power-up Self-Tests:
    - Cryptographic algorithm tests

    - AES-256 Encrypt/Decrypt (ECB, OFB, CBC, GCM) KAT (AES Cert. #1702)
    - 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

6. 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.
7. Power-up self-tests do not require any operator action.
8. The module is available to perform services only after successfully completing the power-up self-tests.
9. Data output shall be inhibited during self-tests and error states.
10. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
11. The module shall not support a concurrent operator.
12. The module enters the Critical Error state if any Power-up Self-Tests and conditional self-tests fail. The Critical Error state can be exited by restarting the module.
13. The module does not perform any cryptographic functions while in the Uninitialized state.
14. The module preserves the results of power up and integrity Self-Tests; it can be retrieved out of the module using Show Status service.
15. The module is to be installed on a Motorola radio, which employs OTAR functionality.
16. 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 7: Available Services

Services	Role		Mode Of Operation	
	User	Cryptographic Officer	FIPS Mode	Non-FIPS Mode
Self-Tests	X	X	X	X
Initialize	X	X	X	X
Show Status	X	X	X	X
Initialization Status Query	X	X	X	X
Version Query	X	X	X	X
Utility	X	X	X	X
AES-256 Encryption Voice	X	X	X	X
AES-256 Decryption Voice	X	X	X	X
AES-256 Encryption Data	X	X	X	X
AES-256 Decryption Data	X	X	X	X
DES Encryption Voice	X	X		X
DES Decryption Voice	X	X		X
DES Encryption Data	X	X		X
DES Decryption Data	X	X		X
AES Key Wrapping	X	X	X	X
AES Key Unwrapping	X	X	X	X
Generate OTAR MAC	X	X	X	X
SHA384	X	X	X	X
SHA512	X	X	X	X
DRBG	X	X	X	X
HMAC-SHA384	X	X	X	X
Set FIPS Mode	X	X	X	X
Get FIPS Mode	X	X	X	X
Zeroize*	X	X	X	X

* The zeroize service zeroizes by cycling power to zeroize all CSPs and cryptographic keys stored in Volatile memory. Also, an application calling the API (End_Stream) as a part of cipher operations will zeroize the key in the volatile memory.

11. 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 services are described in Section 10.2.

Table 8: Critical Security Parameters

CSP Name	Description
AES-256 Encrypt Key	AES-256 key used for voice and data encryption
AES-256 Decrypt Key	AES-256 key used for voice and data decryption
Keyed Hash Key (384)	Key used for generating HMAC SHA384 Message Authentication Code
SP800-90A Seed	384-bit seed value used within the SP800-90A DRBG.
SP800-90A Internal State (“V” and “Key”)	Internal state of the SP800-90A DRBG during initialization.
AES Key Encrypt Key	Key used for AES Key Wrapping
AES Key Decrypt Key	Key used for AES Key Unwrapping
OTAR MAC Key	Key used for APCO OTAR MAC Generation

11.1 CSP Access Types

Table 9: 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 7: 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 4 (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. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys.

Table 10: CSP-Services Access Matrix

CSP Services	AES-256 Encrypt Key	AES-256 Decrypt Key	Keyed Hash Key (384)	SP800-90A Seed	SP800-90A Internal State (V” and “ Key”)	AES Key Encrypt Key	AES Key Decrypt Key	OTAR MAC Key
Self-Tests	–	–	–	–	–	–	–	–
Initialize	–	–	–	–	–	–	–	–
Show Status	–	–	–	–	–	–	–	–
Initialization Status Query	–	–	–	–	–	–	–	–
Version Query	–	–	–	–	–	–	–	–
Utility	–	–	–	–	–	–	–	–
Set FIPS Mode	–	–	–	–	–	–	–	–
Get FIPS Mode	–	–	–	–	–	–	–	–
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	–	–	–	–	–	–
DES Encrypt Voice	–	–	–	–	–	–	–	–
DES Decrypt Voice	–	–	–	–	–	–	–	–
DES Encrypt Data	–	–	–	–	–	–	–	–
DES Decrypt Data	–	–	–	–	–	–	–	–
AES Key Wrapping	–	–	–	–	U	U,S,Z	–	–
AES Key Unwrapping	–	–	–	–	–	–	U,S,Z	–
Generate OTAR MAC	–	–	–	–	–	–	–	U,S, Z
DRBG	–	–	–	U,S	U,S	–	–	–
SHA384	–	–	–	–	–	–	–	–
SHA512	–	–	–	–	–	–	–	–
HMAC-SHA384	–	–	U,S	–	–	–	–	–
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z

12. **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.