## Non-Proprietary FIPS 140-2 Security Policy:

# Motorola Solutions Cryptographic Firmware Module

The cryptographic module is used in multiple Motorola Solutions subscribers. Visit the Motorola Solutions website to verify your subscriber has this module by viewing the subscriber specifications sheet.

Document Version: 1.2

Date: January 27, 2022

# Table of Contents

# List of Tables

# List of Figures

# 1 Introduction

This document defines the Security Policy for the Motorola Solutions Cryptographic Firmware Module, hereafter denoted the module. The module is a firmware-based cryptographic module that runs on a Motorola Solutions radio hardware platform. The module provides FIPS 140-2 approved cryptographic functionalities via an Application Programming Interface (API) to the application layer running in Motorola Solutions radio products supporting the APCO Project 25 standard.

The module is intended for use by the markets that require FIPS 140-2 validated overall Security Level 1.

Firmware Version: R01.09.01, R01.11.00

**Table 1: FIPS Validated Operational Environment**

| Operating Environment | Operating System | Hardware Platform |
|---|---|---|
| OE #1 | Mentor Graphics Nucleus 3.0 (version 2013.08.1) | ARM926EJ-S core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM |
| OE #2 | Texas Instrument (TI) DSP/BIOS 5.41.04.18 | TMS320C674x DSP core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM |

The module has also been confirmed by Motorola Solutions to be operational on the following OE shown in Table 2, as allowed by the FIPS 140-2 Implementation Guidance G.5. However, no target testing was performed on this OE for FIPS 140-2 validation with the specific firmware versions listed in this document.

**Table 2: FIPS Non-Validated Operational Environment**

| *Operating System* | Hardware Platform and Processor |
|---|---|
| *Enea OSE, Version 5.8* | Motorola Solutions GRV 8000 Comparator, NXP QorIQ P1021 |

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.

The FIPS 140-2 security levels for the module are as follows:

**Table 3: Security Level of Security Requirements**

| Security Requirement | Security Level |
|---|---|
| Cryptographic Module Specification | 1 |
| Cryptographic 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 |
| Overall | 1 |

### 1.1 Module Description and Cryptographic Boundary

The module is classified by FIPS 140-2 as a firmware module, and multi-chip standalone module embodiment. The physical cryptographic boundary is the Motorola Solutions Radio Platform on which the module is installed. The logical cryptographic boundary of the module is the static linked library that is linked into the application running on Motorola Solutions radio products.

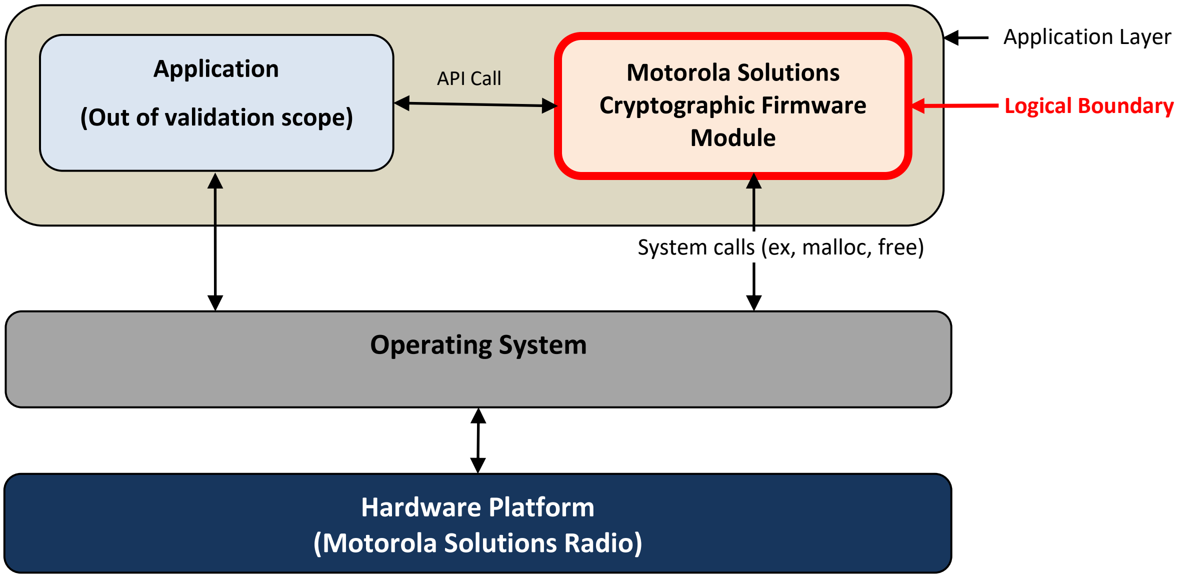
Application Layer
Application
(Out of validation scope)
API Call
Motorola Solutions Cryptographic Firmware Module
Logical Boundary
System calls (ex, malloc, free)
Operating System
Hardware Platform
(Motorola Solutions Radio)

**Figure 1: Module Block Diagram**

The module's ports and associated FIPS defined logical interface categories are listed in Table 4.

**Table 4: 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 |

## 2 Modes of Operation

The module can operate in a FIPS 140-2 Approved mode of operation and a non-Approved mode of operation. The mode of operation is determined by the services used by the operator of the module. To operate in a FIPS 140-2 Approved mode, the operator shall only use the approved cryptographic functions listed in Section 3 in conjunction with the approved services listed in Section 4.2. Using non-Approved cryptographic functions or non-Approved services constitutes running the module in a non-Approved mode.

The user can verify the firmware version matches an approved version listed on NIST's website: http://csrc.nist.gov/groups/STM/cmvp/validation.html

## 3 Cryptographic Functionality

The module's supported cryptographic functions are listed in the following tables.

**Table 5: Approved Algorithms**

| Cert | Algorithm | Mode | Key Size | Functions/Caveats |
|---|---|---|---|---|
| A936, A1168 | AES [197] | ECB [38A] | Key Sizes: 256 | Encrypt, Decrypt |
| | | CBC [38A] | Key Sizes: 256 | Encrypt, Decrypt |
| | | OFB [38A] | Key Sizes: 256 | Encrypt, Decrypt |
| | | GCM [38D][1] | Key Sizes: 256 | Encrypt, Decrypt |
| | DRBG [90A] | CTR[2] | AES-256 | Deterministic Random Bit Generation |
| | HMAC [198-1] | HMAC-SHA-384 | (1024 bit) | Message authentication, Code Integrity tests |
| | KTS [38F] | AES-KW | Key Sizes: 256 | Key Wrap |
| | KTS [IG D.9] | GCM | Key Sizes: 256 | Key Wrap |
| | PBKDF [132] | Option 1a<br>Option 2a | sLen = 16 – 512 bytes<br>C = 1 – 100,000<br>SHA2-384 | Password-Based Key Derivation. Supported only on OE #1. |
| | SHS [180] | SHA-256<br>SHA-384<br>SHA-512 | N/A | Message Digest Generation, Password Obfuscation |
| Vendor Affirmed | CKG | CTR_DRBG | N/A | Symmetric key generation in accordance with SP 800-133rev2 and IG D.12 |

**Table 6: Non-Approved but Allowed Cryptographic Functions**

| Algorithm | Description |
|---|---|
| AES MAC | [IG G.13] AES MAC for Project 25 APCO OTAR (Cert. #A936) |

[1] Per IG A.5 option 2, the module generates 96-bit GCM IVs randomly as specified in SP800-38D section 8.2.2 using an approved DRBG (Cert. #A936).

[2] The entropy for seeding the SP 800-90A DRBG is determined by the user of the module which is outside of the module's logical 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 function. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys.

The following algorithms and services are supported by the module, but do not satisfy FIPS 140-2 requirements:

**Table 7: Non-Approved Cryptographic Functions**

| Algorithm | Description |
|---|---|
| DES | DES Encryption/Decryption – ECB, OFB and CBC Mode. |
| KAS [56Ar3] | Key Agreement Scheme provides 192 bits of encryption strength. Supported only on OE #1. |
| ECDSA [186] | P-384, SHA(384) KeyGen. Supported only on OE #1. |
| KDM [56Cr2] (§4.1) | SP 800-56Cr2 Section 4.1, Option 1 with SHA-384. Supported only on OE #1. |

### 3.1 Critical Security Parameters

All CSPs used by the module are described in this section. Usage of these CSPs by the module (including all CSP lifecycle states) is described in the services detailed in the Section 4. All CSPs are stored plaintext in the volatile memory while in use, and zeroized by power cycling the module.

**Table 8: Critical Security Parameters (CSPs)**

| CSP | Generation | Description / Usage |
|---|---|---|
| SP800-90A Seed | Externally generated and imported into the module. | 384-bit seed value used within the SP800-90A DRBG. |
| SP800-90A Internal State (“V” and “Key”) | Internally generated. | Internal state of SP800-90A CTR_DRBG (V and Key). |
| Keyed Hash Key | Externally generated and imported into the module. | Key used for generating HMAC SHA384 Message Authentication Code. |
| AES-256 Key | Externally generated and imported into the module. | AES-256 key used for voice and data encryption/decryption. |
| AES-256 Key Wrap Key | Externally generated and imported into the module. | Key used for AES Key Wrapping/Unwrapping. |
| PBKDF Secret Value | Externally generated and imported into the module. | PBKDF [SP 800-132] Secret value used in construction of Keyed-Hash key for the specified PRF. |
| OTAR MAC Key | Externally generated and imported into the module. | AES256 key used for APCO OTAR MAC Generation. |

## 4 Roles, Authentication and Services

### 4.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). A user is considered the owner of the thread that instantiates the module and, therefore, only one concurrent user is allowed.

Table 9 lists all operator roles supported by the module. The module does not support a maintenance role and/or bypass capability.

**Table 9: Roles Description**

| Role ID | Role Description | Authentication Type |
|---|---|---|
| CO | Cryptographic Officer | N/A – Authentication not required for Level 1 |
| User | User | N/A – Authentication not required for Level 1 |

## 4.2 Services

All services supported by the module are listed in the Table 10 and Table 11 below. The user of the module may change the mode of operation to FIPS non-Approved mode by using non-Approved services, or by using Approved services which use non-Approved cryptographic functions.

**Table 10: Approved Services**

| Service | Description | Role | |
|---|---|---|---|
| | | CO | User |
| Self-Test | Perform all KATs prior to module initialization | X | X |
| Module Status | Show the module status and version number. | X | X |
| Utility | Key check and other services | X | X |
| Encrypt | Encryption  of voice and data | X | X |
| Decrypt | Decryption of voice and data | X | X |
| AES Key Wrapping | Used for the encryption of keys using the AES Key Wrap [SP 800-38F] algorithm. | X | X |
| AES Key Unwrapping | Used for the decryption of keys using the AES Key Wrap [SP 800-38F] algorithm. | X | X |
| Generate OTAR MAC | Used to generate MAC (Message Authentication Code) as defined in [OTAR]. | X | X |
| DRBG | Used for random number, IV and key generation using DRBG [SP 800-90A]. | X | X |
| Hashing | Used to generate SHA-256/384/512 message digest. | X | X |
| HMAC-SHA | Used to calculate data integrity codes with HMAC. | X | X |

| Service | Description | Role | |
|---|---|---|---|
| | | CO | User |
| Zeroize[3] | Zeroize all CSPs | X | X |
| PBKDF[4] | Used to generate keys using PBKDF [SP 800-132] | X | X |

**Table 11: Non-Approved Services**

| Service | Description | Role | |
|---|---|---|---|
| | | CO | User |
| KAS | Used for key agreement process using ECDH | X | X |
| KDM | Key derivation function used after key exchange negotiation. | X | X |
| ECDSA Key Gen | Used for generating asymmetric key pair | X | X |

Table 11 defines the relationship between access to the security parameters and the different module services. The modes of access shown in the table are defined as:

- G= Generate CSP. Internally create the CSP.
- S = Store CSP: Stores CSP in the volatile memory. The module uses CSPs passed in by the calling application on the stack.
- U = Use CSP: Uses key internally for encryption/decryption services.
- Z = Zeroize: The service zeroizes the CSP in the volatile memory.
- - = No access: The service does not access the CSP.

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 can only be accessed through the APIs provided by the module. The keys can be zeroized in the module's volatile memory by calling appropriate API function.

[3] The Zeroize service zeroizes the key in the volatile memory by power cycling the module.

[4] As per NIST SP 800-132, keys generated by the module shall be used as recommend in Section 5.4 of [132]. Any other use of the approved PBKDF is non-conformant. In approved mode the operator shall enter a password no less than 8 hexadecimal digits in length. The probability of guessing the password will be equal to 1:$16^8$. The iteration count associated with the PBKDF should be as large as practical. Keys derived from passwords may only be used in storage applications.

**Table 11: Security Parameters Access by Service**

| Services | CSPs | | | | | | |
|---|---|---|---|---|---|---|---|
| | AES Key | Keyed Hash Key (384) | SP800-90A Seed | SP800-90A Internal State (V and Key) | AES-256 Key Wrap Key | OTAR MAC Key | PBKDF Secret Value |
| Configure | – | – | – | – | – | – | – |
| Module Status | – | – | – | – | – | – | – |
| Utility | – | – | – | – | – | – | – |
| Encrypt | U,S,Z | – | – | U | – | – | – |
| Decrypt | U,S,Z | – | – | – | – | – | – |
| AES Key Wrapping | – | – | – | U | U,S,Z | – | – |
| AES Key Unwrapping | – | – | – | – | U,S,Z | – | – |
| Generate OTAR MAC | – | – | – | – | – | U,S,Z | – |
| DRBG | – | – | U,S | U,S | – | – | – |
| Hashing | – | – | – | – | – | – | – |
| HMAC-SHA | – | U,S | – | – | – | – | – |
| Zeroize | Z | Z | Z | Z | Z | Z | Z |
| PBKDF | – | – | – | – | – | – | U |

# 5 Self-Tests

## 5.1 Power-up Self-Tests

- Cryptographic algorithm tests
  - AES256 Encrypt/Decrypt (ECB,GCM) KAT
  - SHA-256/512 KAT
  - DRBG [SP 800-90A] KAT (Instantiate and Generate)
  - PBKDF [SP 800-132]
- Firmware integrity test: HMAC-SHA384

# 6 Physical Security Policy

The module is firmware only and operates in a Motorola Solutions 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.

# 7 Operational Environment

The module operates and was tested on the following non-modifiable operational environment:

- Motorola Solutions Radio using hardware platform as specified in Table 1.

# 8 Mitigation of Other Attacks Policy

The module is not designed to mitigate any specific attacks outside of those required by FIPS 140-2.

# 9 Security Rules and Guidance

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

## 9.1 Invariant Rules

1. The module does not provide any operator authentication.
2. The module is available to perform services only after successfully completing the power-up self-tests.
3. Data output is inhibited during key generation, self-tests, zeroization, and while in critical error state.
4. The module shall not support a concurrent operator.
5. The module enters the Uninitialized state if any power-up self-tests or conditional self-tests fail. The Uninitialized state can be exited by restarting the module.
6. The module does not perform any cryptographic functions while in the Uninitialized state.
7. The module returns the results of the power-up and integrity self-tests to the operator.
8. The module may be power cycled to zeroize all CSPs.
9. The module is to be installed on Motorola Solutions radio products.
10. The module only runs in FIPS-approved mode when using approved or allowed cryptographic functions in conjunction with approved services

## 10 References and Definitions

The following standards are referred to in this Security Policy.

**Table 12: References**

| Abbreviation | Full Specification Name |
|---|---|
| [FIPS140-2] | *Security Requirements for Cryptographic Modules, May 25, 2001* |
| [IG] | *Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program* |
| [131A] | *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019* |
| [132] | *NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, Part 1: Storage Applications, December 2010* |
| [133r2] | *NIST Special Publication 800-133 Revision 1, Recommendation for Cryptographic Key Generation, June 2020* |
| [186] | *National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.* |
| [197] | *National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001* |
| [198] | *National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008* |
| [180] | *National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015* |
| [38A] | *National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001* |
| [38B] | *National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, October 2016* |
| [38D] | *National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007* |
| [38F] | *National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012* |
| [56Ar3] | *NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018* |

| Abbreviation | Full Specification Name |
|---|---|
| [90A] | *National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.* |
| [OTAR] | *Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014* |
| [56Cr2] | *NIST Special Publication 800-56C Revision 2, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, August 2020* |

**Table 13: Acronyms and Definitions**

| Acronym | Definition |
|---|---|
| AES | Advanced Encryption Standard |
| API | Application Programming Interface |
| CBC | Cipher Block Chaining |
| CKG | Cryptographic Key Generation |
| CSP | Critical Security Parameter |
| DES | Data Encryption Standard |
| DPK | Data Protection Key |
| DRBG | Deterministic Random Bit Generator |
| ECB | Electronic Code Book |
| ECDH | Elliptic Curve Diffie-Hellman |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| FIPS | Federal Information Processing Standards |
| GCM | Galois/Counter Mode |
| HMAC | Keyed-hash Hash Message Authentication Code |
| IV | Initialization Vector |
| KAT | Known Answer Test |
| KDF | Key Derivation Function |
| MAC | Message Authentication Code |
| MK | Master Key |
| OFB | Output Feedback |
| PBKDF | Password-Based Key Derivation Function |
| RTOS | Real-Time Operating System |
| SHS | Secure Hash Standard |

| Acronym | Definition |
|---|---|
| VA | Vendor Affirmed |