Non-Proprietary FIPS 140-2 Security Policy:

Motorola Solutions Cryptographic Firmware Module

FW Version: R01.07.00

Document Version: 1.2

Date: March 17, 2021

Table of Contents

1 Introduction 4

1.1 Module Description and Cryptographic Boundary 6

2 Modes of Operation 6

2.1 Approved Mode Configuration 7

3 Cryptographic Functionality 7

3.1 Critical Security Parameters 8

4 Roles, Authentication and Services 9

4.1 Assumption of Roles 9

4.2 Services 9

5 Self-Tests 13

5.1 Power-up Self-Tests 13

5.2 Conditional Self-Tests 13

6 Physical Security Policy 13

7 Operational Environment 13

8 Mitigation of Other Attacks Policy 14

9 Security Rules and Guidance 14

9.1 Invariant Rules 14

10 References and Definitions 15

List of Tables

Table 1: FIPS Validated Operating Environment.......4

Table 2: Historical FIPS 140-2 Validation Status.......4

Table 3: FIPS Non-Validated Operating Environment.......4

Table 4 – Security Level of Security Requirements.......5

Table 5 – Ports and Interfaces.......6

Table 6 – Approved Algorithms.......7

Table 7: Non-Approved but Allowed Cryptographic Functions.......8

Table 8 – Non-Approved Cryptographic Functions.......8

Table 9 – Critical Security Parameters (CSPs).......8

Table 10 – Roles Description.......9

Table 11 – Services.......10

Table 12 – Security Parameters Access by Service.......12

Table 13 – References.......15

Table 14 – Acronyms and Definitions.......16

List of Figures

Figure 1: Module Block Diagram.......6

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 Motorola GRV8000 hardware platform. The module provides FIPS 140-2 approved cryptographic functionalities via Application Programming Interface (API) to the application layer running in Motorola Solutions GRV 8000 Comparator product and supporting 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: R01.07.00

Table 1: FIPS Validated Operating Environment

Format	Operating System	Hardware Platform	Processor
Static library (.lib)	Enea OSE, Version 5.8	Motorola Solutions GRV 8000 Comparator	NXP QorIQ P1021

The module was previously FIPS 140-2 validated on the following FW/SW versions as listed in Table 2.

Table 2: Historical FIPS 140-2 Validation Status

CMVP Cert#	FW/SW Version
3087	R01.01.02 (FW)
3181	R01.03.00 (SW)

The module also runs on the following OEs shown in Table 3 when complied with compatible cross compiler; however, no target testing was performed for FIPS 140-2 validation with this firmware version.

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.

Table 3: FIPS Non-Validated Operating Environment

Format	Operating System	Hardware Platform and Processor
Static library (.lib)	Mentor Graphics Nucleus 3.0 (version 2013.08.1)	ARM926EJ-S core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM
Static library (.lib)	Texas Instrument (TI) DSP/BIOS 5.41.04.18	TMS320C674x DSP core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM
Shared object (.so)	Linux 2.6.32-358.23.2.el6.x86_64 GNU/Linux	HP ProLiant Gen8 Intel Servers, Intel(R) Xeon(R) CPU E5-4620 v2 @ 2.60GHz

Dynamic-Linked Library (.dll)	Microsoft Windows 7 and 10 Professional	HP ZBook 15 G3 Mobile Workstation, Intel Core i7

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

Table 4 – 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 general-purpose computer 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 Solution GRV 8000 Comparator Hardware Platform.

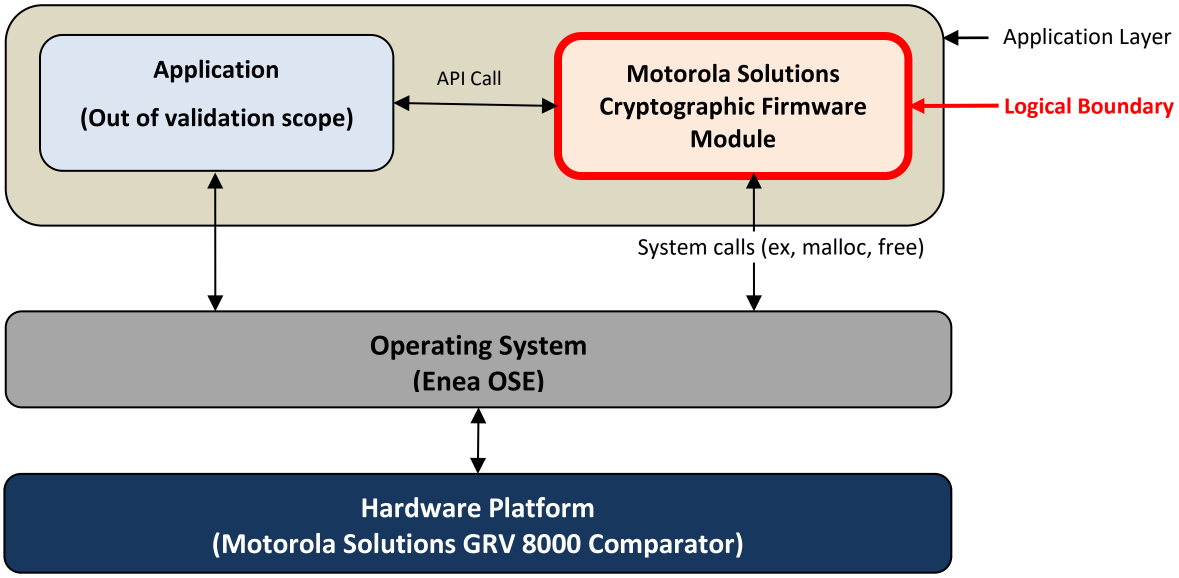
Application Layer
Application
(Out of validation scope)
API Call
Motorola Solutions Cryptographic Firmware Module
Logical Boundary
System calls (ex, malloc, free)
Operating System
(Enea OSE)
Hardware Platform
(Motorola Solutions GRV 8000 Comparator)

Figure 1: Module Block Diagram

The module's ports and associated FIPS defined logical interface categories are listed in Table 5.

Table 5 – 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 be configured to operate in a FIPS 140-2 Approved mode of operation and a non-Approved mode of operation. At any given time, the FIPS mode service can be used to determine whether the module is operating in FIPS approved or non-FIPS Approved mode.

- FIPS Approved mode: DES Voice/Data Encryption/Decryption are blocked. All other services listed in the Section 4.2 are available when the module is operating in FIPS Approved mode.
- FIPS non-Approved mode: All services listed in the Section 4.2 are available when the module is operating in FIPS Non-Approved mode.

The Version Query service can also be used to verify the firmware version matches an approved version listed on NIST's website: http://csrc.nist.gov/groups/STM/cmvp/validation.html

2.1 Approved Mode Configuration

The module powers up in FIPS approved mode by default. The operator can put the module in FIPS non-Approved mode by calling "Set FIPS mode" service. 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.

3 Cryptographic Functionality

The module implements the FIPS Approved and Non-Approved-but-Allowed cryptographic functions listed in the following tables.

Table 6 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
C1709	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
C1712	AES [SP800-38F]	KW	Key Sizes: 256	Key Wrapping
C1711	DRBG [90A]	CTR[2]	AES-256	Deterministic Random Bit Generation
C1710	HMAC [198-1]	HMAC-SHA-384	Key Size: 1024 bit[3]	Message authentication, Code Integrity tests
C1712	KTS [38F]	KW	Key Sizes: 256	Key establishment methodology provides 256 bits of encryption strength
C1709	KTS [IG D.9]	GCM	Key Sizes: 256	

A493	PBKDF [132]	With HMAC-SHA384[4]	sLen = 16 – 512 bytes
			C = 1 – 100,000
				Password Based Key Derivation

[1] Per IG A.5, the module generates GCM IVs randomly as specified in SP800-38D section 8.2.2 using approved DRBG (Cert. #C1711).

[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.

[3] 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

[4] PBKDF was tested for HMAC SHA-256, 384 and 512. HMAC SHA256 and HMAC SHA 512 have not been CAVP tested. Only PBKDF HMAC SHA-384 can be used in approved mode.

Cert	Algorithm	Mode	Description	Functions/Caveats
		Option 1a, 2a	SHA2 (384)	
C1710	SHS [180]	SHA-256 SHA-384 SHA-512	N/A	Message Digest Generation, Password Obfuscation

Table 7: Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES MAC	[IG G.13] AES MAC for Project 25 APCO OTAR (Cert. #C1709)

The following FIPS non-Approved algorithms are only supported when the module operates in FIPS non-approved mode:

Table 8 – Non-Approved Cryptographic Functions

Algorithm	Description
DES	DES Encryption/Decryption – ECB, OFB and CBC Mode
HMAC-SHA 256, HMAC-SHA 512	Available only through the PBKDF API but not CAVP tested. Not to be used in Approved mode

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. 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.

Table 9 – Critical Security Parameters (CSPs)

CSP	Description / Usage
SP800-90A Seed	384-bit seed value used within the SP800-90A DRBG.
SP800-90A Internal State (“V” and “Key”)	Internal state of SP800-90A CTR_DRBG (V and Key).
Keyed Hash Key	Key used for generating HMAC SHA384 Message Authentication Code.
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.

CSP	Description / Usage
AES-256 Key Encrypt Key	Key used for AES Key Wrapping
AES-256 Key Decrypt Key	Key used for AES Key Unwrapping
PBKDF Secret Value	PBKDF [SP 800-132] Secret value used in construction of Keyed-Hash key for the specified PRF.
OTAR MAC Key	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 10 lists all operator roles supported by the module. The module does not support a maintenance role and/or bypass capability.

Table 10 – 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 11 below. Note that all services listed in Table 11 below are available in both FIPS Approved and non-Approved mode.

Table 11 – Services

Service	Description	Role		FIPS Operational Mode	
		CO	User	Approved	Non-Approved
Self-Tests	The GRV 8000 Comparator will call the static constructor for self-tests on module initialization.	X	X	X	X
Initialize	Used to configure the module.	X	X	X	X
Show Status	Show the module status, version number, and FIPS status.	X	X	X	X
Initialization Status Query	Show the status of the module initialization	X	X	X	X
Version Query	Query module version	X	X	X	X
Utility	Used to retrieve various information such as alg id, key validity, esync size, etc. out of the module.	X	X	X	X
Set FIPS Mode	Set FIPS operational mode	X	X	X	X
Get FIPS Mode	Get FIPS operational mode	X	X	X	X
AES-256 Encryption Voice	AES-256 encrypt of voice	X	X	X	X
AES-256 Decryption Voice	AES-256 decrypt of voice	X	X	X	X
AES-256 Encryption Data	AES256 encrypt of data	X	X	X	X
AES-256 Decryption Data	AES-256 decrypt of data	X	X	X	X
DES Encrypt Voice	DES encrypt of voice	X	X	–	X
DES Decrypt Voice	DES decrypt of voice	X	X	–	X
DES Encrypt Data	DES encrypt of data	X	X	–	X
DES Decrypt Data	DES decrypt of data	X	X	–	X
AES Key Wrapping	Used to encrypt of keys using the AES Key Wrap [SP 800-38F] algorithm.	X	X	X	X
AES Key Unwrapping	Used to decrypt of keys using the AES Key Wrap [SP 800-38F] algorithm.	X	X	X	X

Service	Description	Role		FIPS Operational Mode	
		CO	User	Approved	Non-Approved
Generate OTAR MAC	Used to generate MAC (Message Authentication Code) as defined in [OTAR].	X	X	X	X
DRBG	Used for random number, IV and key generation using DRBG [SP 800-90A].	X	X	X	X
SHA-256	Used to generate SHA-256 message digest.	X	X	X	X
SHA-384	Used to generate SHA-384 message digest.	X	X	X	X
SHA-512	Used to generate SHA-512 message digest.	X	X	X	X
HMAC-SHA384	Used to calculate data integrity codes with HMAC.	X	X	X	X
Zeroize[5]	Zeroize all CSPs	X	X	X	X
PBKDF[6]	Used to generate keys using PBKDF [SP 800-132]	X	X	X	X

Table 12 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:

- 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

[5] The zeroize service zeroizes the key in the volatile memory by power cycling the module. Also an application calling the API (End_Stream) as a part of cipher operations will zeroize the key in the volatile memory.

[6] 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.

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

Table 12 – Security Parameters Access by Service

Services	CSPs								
	AES-256 Encrypt Key	AES-256 Decrypt Key	Keyed Hash Key (384)	SP800-90A Seed	SP800-90A Internal State (V and Key)	AES-256 Key Encrypt Key	AES-256 Key Decrypt Key	OTAR MAC Key	PBKDF Secret Value
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	–	–	–	–

Services	CSPs								
	AES-256 Encrypt Key	AES-256 Decrypt Key	Keyed Hash Key (384)	SP800-90A Seed	SP800-90A Internal State (V and Key)	AES-256 Key Encrypt Key	AES-256 Key Decrypt Key	OTAR MAC Key	PBKDF Secret Value
SHA-256	–	–	–	–	–	–	–	–	–
SHA384	–	–	–	–	–	–	–	–	–
SHA512	–	–	–	–	–	–	–	–	–
HMAC-SHA384	–	–	U,S	–	–	–	–	–	–
PBKDF	–	–	–	–	–	–	–	–	U
Zeroize	Z	Z	Z	Z	Z	Z	Z	Z	Z

5 Self-Tests

5.1 Power-up Self-Tests

- Cryptographic algorithm tests
    - AES256 Encrypt/Decrypt (ECB, OFB, CBC, GCM) KAT (AES Cert. #C1709)
    - AES256 KW [SP800-38F] Encrypt/Decrypt KAT (AES Cert. #C1712)
    - SHA-256/384/512 KAT
    - HMAC-SHA384 KAT
    - DRBG [SP 800-90A] KAT (Instantiate and Generate)
    - PBKDF [SP 800-132]
- Firmware integrity test: HMAC-SHA-384

5.2 Conditional Self-Tests

- Random bit generation tests
    - DRBG Continuous Tests
    - SP800-90A Health Tests (Instantiate and Generate)

6 Physical Security Policy

The module is firmware only and operates in the Motorola Solutions GRV 8000 Comparator 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 MSCFM operates and was tested on the following non-modifiable operational environment:

- Motorola Solutions GRV 8000 Comparator on NXP QorIQ P1021.

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 GRV 8000 Comparator products.

10 References and Definitions

The following standards are referred to in this Security Policy.

Table 13 – 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*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*

Abbreviation	Full Specification Name
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*

Table 14 – 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
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
VA	Vendor Affirmed