Non-Proprietary FIPS 140-2 Security Policy:

Motorola Solutions Cryptographic Software Module

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

Document Version: 1.2

Date: December 14, 2021

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Motorola Solutions Cryptographic Software Module, hereafter denoted the module. The module is a software-based cryptographic module that runs on a general-purpose computing platform. The module provides FIPS 140-2 approved cryptographic functionalities via an Application Programming Interface (API) to the application layer.

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

Software Version: R01.11.00

Table 1: FIPS Validated Operational Environment

Operating System	Hardware Platform
Red Hat OpenShift 4 on Red Hat UBI 8	HPE ProLiant DL20 Gen10 server, Intel(R) Xeon(R) E-2236 CPU with AES-NI
Red Hat OpenShift 4 on Red Hat UBI 8	HPE ProLiant DL20 Gen10 server, Intel(R) Xeon(R) E-2236 CPU without AES-NI

The module has also been confirmed by Motorola Solutions to be operational on the following OEs shown in Table 2, as allowed by the FIPS 140-2 Implementation Guidance G.5. However, no target testing was performed on these OEs 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
Microsoft Windows 7 and 10 Professional	HP ZBook 15 G3 Mobile Workstation, Intel Core i7
Mentor Graphics Nucleus 3.0 (version 2013.08.1)	ARM926EJ-S core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM
Texas Instrument (TI) DSP/BIOS 5.41.04.18	TMS320C674x DSP core of Texas Instrument (TI) OMAP-L138 C6000 DSP+ARM
Linux/ kernel 4.14	ARMv8-a (64-bit)
Red Hat OpenShift 3 on Red Hat UBI 7	HP DL20 Gen10 server, Intel(R) Xeon(R) E-2236 CPU
Red Hat OpenShift 4 on Red Hat UBI 8	HP DL160 Gen 10 Server, Intel(R) Xeon(R)-S 4215R CPU

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	N/A
Operational Environment	1
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 software 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 a shared object that is linked into the application running on a general-purpose computing platform.

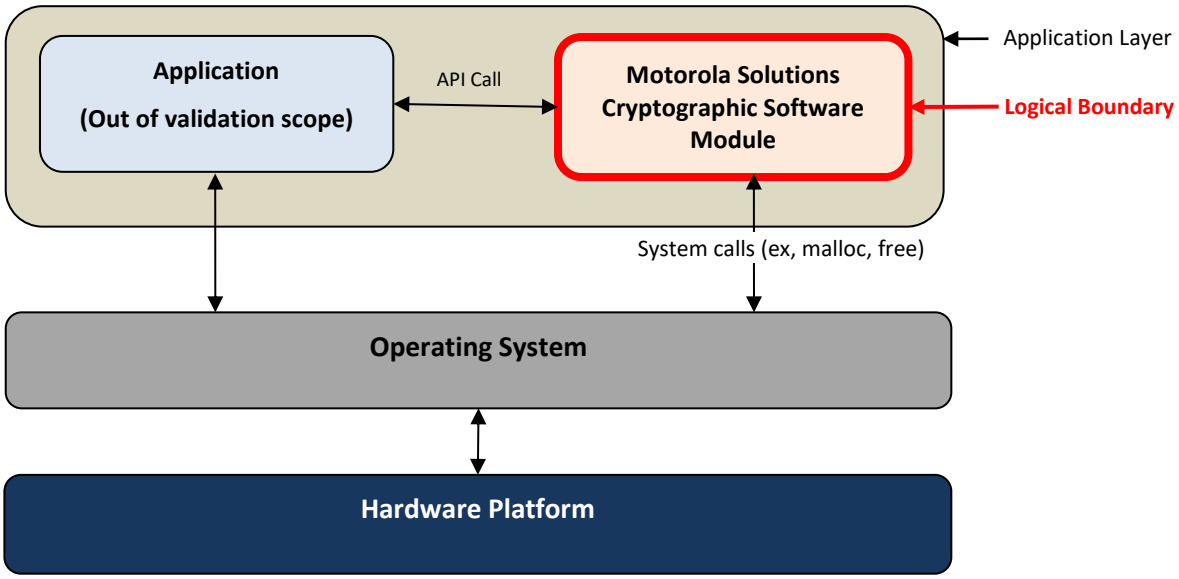

Figure 1: Module Block Diagram

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 software 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 starts up in the Approved mode of operation by default. The operator can put the module in FIPS non-Approved mode by calling the appropriate "Configure" services. The operator shall zeroize all CSPs by power cycling the module when transitioning between FIPS 140-2 Approved and non-Approved modes.

3 Cryptographic Functionality

The module implements the FIPS Approved and Non-Approved-but-Allowed cryptographic functions listed in the following tables. Note that the TLS KDF was tested, but is not used in the module's Approved mode.

Table 5: Approved Algorithms

Cert	Algorithm	Mode	Key Size/Description	Functions/Caveats
A1096	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
	ECDSA [186]		P-384 with SHA-384	Key Generation
				Signature Generation
				Signature Verification
	HMAC [198-1]	HMAC-SHA-384	(1024 bit)	Message authentication, Code Integrity tests
	KAS-ECC [56Ar3]	ECC (Initiator, Responder), Key pair generation, Partial public key validation, One-	P-384	Key Establishment

[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 approved DRBG (Cert. #A1096).

[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. To be compliant, the target application shall supply at least 384 bits of entropy in order to 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.

Cert	Algorithm	Mode	Key Size/Description	Functions/Caveats
		step key derivation		
	KTS [38F]	AES-KW	Key Sizes: 256	Key Wrap
	KTS [IG D.9]	GCM	Key Sizes: 256	Key Wrap
	PBKDF [132]	Option 1a Option 1b Option 2a Option 2b	sLen = 16 – 512 bytes C = 1 – 100,000 SHA2-384)	Password Based Key Derivation
	SHS [180]	SHA-256 SHA-384 SHA-512	N/A	Message Digest Generation, Password Obfuscation
Vendor Affirmed	CKG	CTR_DRBG	N/A	Symmetric key and asymmetric seed 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. #A1096)

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

Table 7: Non-Approved Cryptographic Functions

Algorithm	Description
ADP	Encryption/Decryption - Motorola Solutions proprietary algorithm.
DES	DES Encryption/Decryption – ECB, OFB and CBC Mode
TLS KDF	TLS IV/Key Derivation - Keys derived using this key derivation function cannot be used in the 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.

Table 8: Critical Security Parameters (CSPs)

CSP	Generation	Description / Usage
Input String	Externally generated and imported into the module.	String entered into the module from an external source used as entropy for DRBG seed generation.
SP800-90A Seed	Internally generated.	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.	1-512 byte PBKDF [SP 800-132] Secret value (i.e. password) used in construction of Keyed-Hash key
OTAR MAC Key	Externally generated and imported into the module.	AES256 key used for APCO OTAR MAC Generation
ECDH Private Key	Internally generated.	Random value used to establish a shared secret over an insecure channel.
ECDH Shared Secret	Internally generated.	Output as part of the Elliptic Curve Diffie-Hellman key agreement protocol.
ECDSA Private Key	Internally or externally generated.	384-bit ECDSA key used to generate the signature of the input data from the Generate Signature service request.
KDF Derived Key	Internally generated.	Keys derived using one-step KDF (SP 800-56Cr2).

3.2 Public Keys

Table 9: Public Keys

Key	Description / Usage
ECDH Public Key	Elliptic Curve (P-384) Diffie-Hellman public key used for establishing a shared secret over an insecure channel.
ECDH Remote Party Public Key	Elliptic Curve (P-384) Diffie-Hellman remote party public key used for establishing a shared secret over an insecure channel.
ECDSA Public Key	384-bit ECDSA key used to verify signatures.

4 Roles, Authentication and Services

4.1 Assumption of Roles

The module supports two 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. As the calling application is the sole operator of the module there is no distinction between CO and User services.

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 and Table 12 below. The user may change the mode of operation of the module to FIPS non-Approved mode by using non-Approved services, or by using a non-Approved cryptographic function while using an Approved service.

Table 11: Approved Services

Service	Description	Role	
		CO	User
Load Entropy	Load external entropy to be used to seed the DRBG.	X	X
Configure	Used to configure the module.	X	X
Module Status	Show the module status, version number, and FIPS status.	X	X
Self-Test	On-demand self-test performed on reboot	X	X
Utility	Various utility 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

Service	Description	Role	
		CO	User
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
Zeroize[3]	Zeroize all CSPs	X	X
PBKDF[4]	Used to generate keys using PBKDF [SP 800-132]	X	X
KAS	Used for key agreement process using ECDH in conjunction with the one-step KDF	X	X
ECDSA Key Generation	Used for generating asymmetric key pair	X	X
ECDSA Signature Generation	Used for generating a digital signature	X	X
ECDSA Signature Verification	Used for validating a digital signature	X	X

Table 12: Non-Approved Services

Service	Description	Role	
		CO	User
TLS KDF	Secret input used in the TLS-based derivation of KDF Derived Keys.	X	X

Table 13 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:

[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 the 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.

- 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 CSP for 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.

Table 13: Security Parameters Access by Service

Services	CSPs														
	Input String	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	KDF Derived Key	ECDH Private Key	ECDH Shared Secret	ECDH Public Key	ECDH Remote Party Public Key	ECDSA Private Key	ECDSA Public Key
Load Entropy	U	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Configure	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Module Status	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Self-Test	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
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	–	–	–	–	–	–	–	–	–	–

Services	CSPs														
	Input String	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	KDF Derived Key	ECDH Private Key	ECDH Shared Secret	ECDH Public Key	ECDH Remote Party Public Key	ECDSA Private Key	ECDSA Public Key
Hashing	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
HMAC-SHA	–	–	U,S	–	–	–	–	–	–	–	–	–	–	–	–
Zeroize	–	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
PBKDF	–	–	–	–	–	–	–	U	–	–	–	–	–	–	–
KAS	–	–	–	–	–	–	–	–	U, S	U, S,Z	U	U, S,Z	U, S	–	–
ECDSA Key Generation	–	–	–	–	–	–	–	–	–	–	–	–	–	U, S	U, S
ECDSA Signature Generation	–	–	–	–	–	–	–	–	–	–	–	–	–	U, S	U, S
ECDSA Signature Verification	–	–	–	–	–	–	–	–	–	–	–	–	–	U	U

5 Self-Tests

5.1 Power-up Self-Tests

- Cryptographic algorithm tests
  - AES256 Encrypt/Decrypt (ECB, CBC, GCM, OFB) KATs
  - AES256 KW [SP800-38F] Encrypt/Decrypt KAT
  - SHA-256/512 KAT
  - HMAC-SHA384 KAT
  - DRBG [SP 800-90A] KAT (Instantiate and Generate)
  - PBKDF [SP 800-132]
  - ECDSA P-384 pair-wise consistency tests
  - KDA [56Cr2] (§4.1) KAT
  - EC Diffie-Hellman primitive "Z" computation KAT per IG 9.6.
- Software integrity test: HMAC-SHA-384

5.2 Conditional Self-Tests

- ECDSA P-384 pair-wise consistency tests

6 Physical Security Policy

The module is software only and operates on a general-purpose computing platform 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:

- General purpose computing 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 general purpose computing platforms.

9.2 Operator Guidance for Non-Approved Mode of Operation

1. The operator of the module **shall** not use the Non-Approved Cryptographic Functions listed in Table 7 while in the FIPS Approved Mode. Use of these functions constitutes exiting the FIPS Approved Mode.
2. The operator **shall** zeroize all CSPs before entering the Non-Approved Mode by power cycling the module.
3. The operator **shall** zeroize all CSPs before returning to the FIPS Approved Mode by power cycling the module.

10 References and Definitions

The following standards are referred to in this Security Policy.

Table 14: 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*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[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*
[135r1]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[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*

Abbreviation	Full Specification Name
[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*
[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*
[RFC2246]	*The TLS Protocol, August 2008*
[RFC5246]	*The Transport Layer Security (TLS) Protocol, August 2008*

Table 15: 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

Acronym	Definition
RTOS	Real-Time Operating System
SHS	Secure Hash Standard
VA	Vendor Affirmed