Motorola Solutions Cryptographic DLL Software Module

Cryptographic module used in Motorola Solutions ASTRO IP Dispatch Console products

Software Version: R01.03.00

Non-Proprietary Security Policy

Document Version: 1.5

October 25, 2022,

Revision History

Revision	Date	Change Summary
0.1	Apr 24th, 2017	Initial Creation
1.0	Aug 30th, 2017	Initial release version
1.1	Nov 7, 2017	Updates per CMVP Comments
1.2	Apr 17, 2018	Updates for SP 800-38F
1.3	May 1, 2018	Added AES Cert. #5356 to Table 2
1.4	Jan 12, 2022	Added additional FIPS Non-Validated Operating Environments (Vendor Affirmed) to Table 8
1.5	Oct 25, 2022	Added additional FIPS Non-Validated Operating Environments (Vendor Affirmed) to Table 8

Table of Contents

Table of Figures

1. Introduction

Motorola Solutions Cryptographic DLL Software Module (MSCDSM) is software based cryptographic module that runs on General Purpose Computer (GPC) hardware platform running Microsoft Windows operating system. The cryptographic module is delivered to the end customers as x86 based Dynamically Linked Library (DLL) module and named as “libalg.dll”. The module provides cryptographic functionality in Motorola Solutions ASTRO IP Dispatch Console products running on Microsoft Windows OS and supporting the APCO Project 25 standard. MSCDSM provides several FIPS Approved and non-Approved cryptographic algorithms.

1.1 Scope

This Security Policy (SP) document specifies the security rules under which MSCDSM must operate.

1.2 Acronyms and Definitions

Acronyms	Description
API	Application Programming Interface
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CSP	Critical Security Parameter
CST	Commercial Solutions Testing
DES	Data Encryption Standard
ECB	Electronic Code Book
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interface
FIPS	Federal Information Processing Standards
GCM	Galois/Counter Mode
GPC	General Purpose Computer
HMAC	Hash-Based Message Authentication Code
MSCDSM	Motorola Solutions Cryptographic DLL Software Module
NDRNG	Non-deterministic Random Number Generator
NVLAP	National Voluntary Laboratory Accreditation Program
OFB	Output Feedback
RBG	Random Bit Generator
SHA	Secure Hash Algorithm
SP	Security Policy

1.3 References

[1] FIPS 140-1 Security Requirements for Security Modules
[2] FIPS 140-2 Required Vendor Documentation
[3] Project 25 Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures
[4] Motorola Solutions MCC 7100 IP Dispatch Console

2. Cryptographic Module Specification

2.1 Cryptographic Module Name

Motorola Solutions Cryptographic DLL Software Module (MSCDSM).

2.2 Software Version Number

MSCDSM has the following FIPS 140-2 validated software version number.

Software Version Number: R01.03.00

2.3 Module Overview

The MSCDSM provides software based cryptographic solutions and is a multi-chip standalone cryptographic module that runs on General Purpose Computer (GPC) hardware platform and Microsoft Windows operating system as x86 based Dynamically Linked Library (DLL) module. The MSCDSM provides FIPS 140-2 Approved and non-Approved cryptographic functionalities to different applications running on Microsoft Windows operating system through Application Programming Interfaces (API).

Following block diagram (Figure 1: Module Block Diagram) shows how application interacts with MSCDSM.

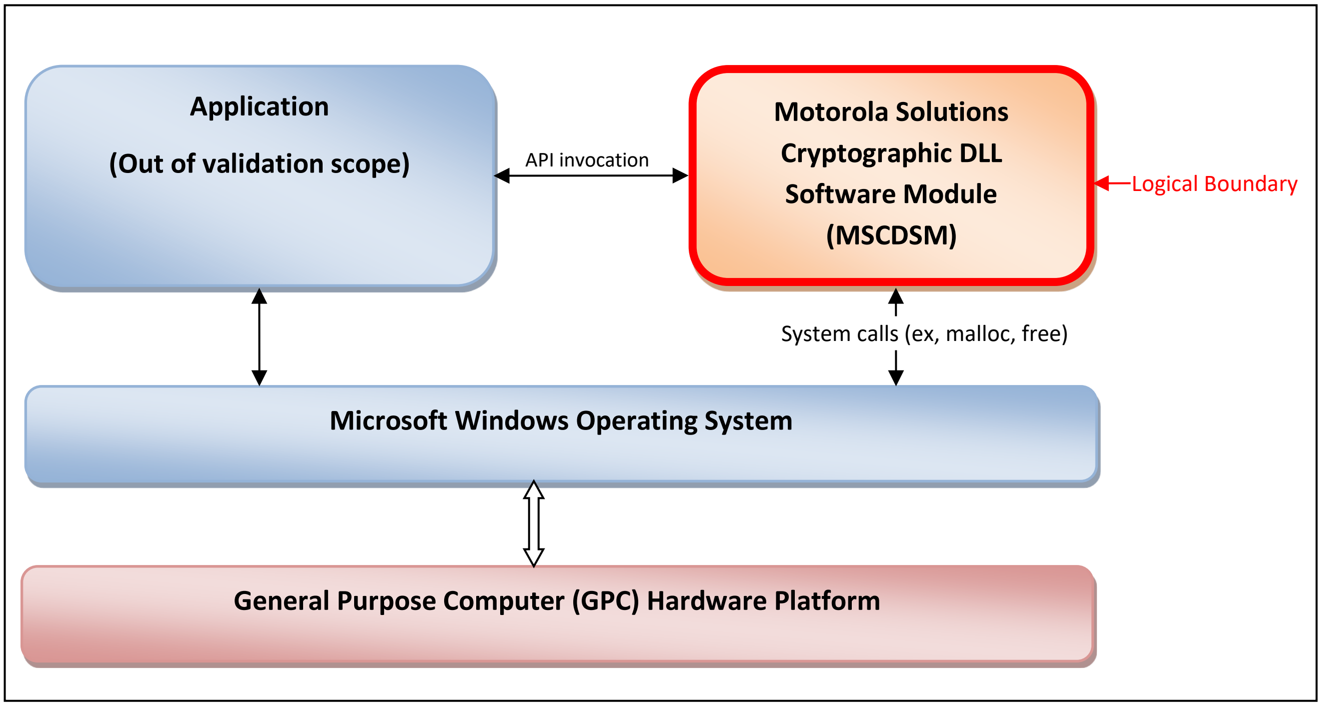
Application
(Out of validation scope)
API invocation
Motorola Solutions Cryptographic DLL Software Module (MSCDSM)
Logical Boundary
System calls (ex, malloc, free)
Microsoft Windows Operating System
General Purpose Computer (GPC) Hardware Platform

Figure 1: Module Block Diagram

2.4 Cryptographic Boundary

MSCDSM is delivered to the end customer as DLL, the DLL is the logical boundary of the cryptographic module. The physical boundary is defined as the outer perimeter of the general purpose computer on which the module is installed.

2.5 Mode of Operation

The MSCDSM operates in two different modes of operation.

- FIPS Approved mode: DES Voice/Data Encryption/Decryption are blocked. All other services listed in the Section 4.5 are available when the module is operating in FIPS Approved mode.
- FIPS non-Approved mode: All services listed in the Section 4.5 are available when the module is operating in FIPS Non-Approved mode.

2.6 Module Configuration

The MSCDSM always powers up in FIPS Approved mode and executes power up self-tests as mentioned in the Section 9.1. 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 4.5.

2.7 FIPS 140-2 Security Levels

MSCDSM operates in an FIPS Approved and non-Approved modes. When running FIPS Approved mode, it operates 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 1: Security Level

FIPS 140-2 Security Requirements Section	Security Level
Cryptographic Module Specification	1
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

2.8 FIPS Approved Algorithms

The MSCDSM supports the following approved algorithms when running in FIPS Approved mode.

Table 2: List of Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode/Method	Key Length, Curves or Moduli	Use
4683	AES	FIPS 197, SP 800-38A	ECB, OFB, CBC	256	Voice/Data Encryption/decryption
4683	AES	FIPS 197, SP 800-38D	GCM	256	Voice/Data Encryption/decryption
5356	AES	FIPS 197, SP 800-38F	AES-KW	256	Encryption/decryption
4683	KTS	FIPS 197, SP 800-38F	ECB, AES MAC	256	Key establishment
4683	KTS	FIPS 197, SP 800-38D, SP 800-38F	GCM	256	Key establishment
5356	KTS	SP 800-38F	KW	256	Key establishment
1587	DRBG	SP 800-90A	CTR_DRBG	256	Deterministic Random Bit Generation
3099	HMAC	FIPS 198-1	HMAC-SHA-384	(192 - 1024) (must be multiple of 8)	Message authentication, Code Integrity tests
3834	SHS	FIPS 180-4	SHA-384, SHA-512	N/A	Message Digest

2.9 FIPS Allowed Algorithms

The following algorithms and protocols are allowed within the FIPS Approved mode of operation:

Table 3: List of FIPS Allowed Algorithms

Algorithm	Caveat	Use
AES MAC (Cert. #4683)	Project P25 AES OTAR, vendor affirmed.	Provide authentication within P25 APCO OTAR

2.10 FIPS non-Approved Algorithms

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

Table 4: List of FIPS Non-Approved Algorithms

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

3. Module 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 software module support logical interfaces: data input, data output, control input, status output.

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

4. Roles, Services, and Authentication

4.1 Administration of the Module in a Secure Manner (CO)

The software based cryptographic module requires no special administration for secure use and automatically loads in the Approved mode of operation.

4.2 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.

4.3 Approved Security Functions, Ports, and Interfaces Available to Users

Services available to the User Role are listed in the Section 4.5.

4.4 User Responsibilities Necessary for Secure Operation

The module must be loaded successfully and passed power up code integrity, known answer tests.

4.5 Available Services

The following table shows different cryptographic and non-cryptographic services provided through APIs at different roles and mode of operations.

Table 6: List of 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

5. Security Rules

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

5.1 FIPS 140-2 Imposed Security Rules

1. The module does not provide any operator authentication.
2. The module encrypts/decrypts message traffic using AES-256 and DES.[1] cryptographic algorithms.
3. 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.
4. The module is available to perform services only after successfully completing the power-up self-tests.
5. Data output shall be inhibited during self-tests, and error states.
6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The module shall not support a concurrent operator.
8. 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.
9. The module does not perform any cryptographic functions while in the Uninitialized state.
10. The module returns the results of power-up and integrity Self-Tests to the user.
11. The module may be power cycled to zeroize all CSPs.
12. The module is to be installed on Motorola Solutions ASTRO IP Dispatch Console products, which employs APCO OTAR functionality.

6. Operational Environment

The MSCDSM operates on commercially available general purpose computing (GPC) hardware platform running on Microsoft Windows Operating system. The general purpose operating environment is a modifiable environment. Hence the FIPS 140-2 area 6 Operational Environment requirements are applicable to the MSCDSM. The cryptographic module is compiled on Microsoft Windows Operating System as DLL for x86 solution platform. For FIPS 140-2 validation purposes, the cryptographic module was tested on the following operational environments:

Table 7: FIPS Validated Operating Environment

Format	Operating System	Hardware Platform
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 7 Professional	HP ZBook 15 G3 Mobile Workstation, Intel Core i7

[1] Available only when module is running as non-FIPS approved mode

Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 Professional	HP ZBook 15 G3 Mobile Workstation, Intel Core i7

The cryptographic module also runs on the following operating systems when complied with compatible cross compiler, however no target testing was performed for FIPS 140-2 validation with the software version number mentioned in the Section 2.2. The CMVP makes no statement as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

Table 8: FIPS Non-Validated Operating Environment

Format	Operating System	Hardware Platform
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSB 2016 64bit	HP ZBook 15u G4 Mobile Workstation, Intel® Core i7 CPU
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSC 2019 64bit	HP ZBook 15u G5 Mobile Workstation, Intel® Xeon® E-2186M CPU
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSC 2019 64bit	HP ZBook 15u G6 Mobile Workstation, Intel® Xeon® E-2286M CPU
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSC 2019 64bit	HP ZBook Fury 15 G7 Mobile Workstation, Intel® Xeon® W-10885M CPU
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSB 2016 64bit	HP Z440 Workstation, Intel Xeon E5-1603v3 CPU
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSC 2019 64bit	HP Z440 Workstation, Intel Xeon E5-1603v3 CPU
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSB 2016 64bit	HP Z2 Mini G3 Workstation, Intel Xeon E3-1225v5 CPU
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSC 2019 64bit	HP Z2 Mini G4 Workstation, Intel Xeon E-2144G CPU
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSC 2019 64bit	HP Z2 Mini G5 Workstation, Intel Xeon W-1250 CPU
Microsoft Windows DLL (x86 Solution Platform)	Microsoft Windows 10 IoT Enterprise LTSC 2021	Command Central HUB (AIMB-276G2), Intel(R) Core(TM) i7-8700T CPU @ 2.40GHz, 2400MHz, 6 Core(s), 12 Logical Processor(s)
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	General Purpose Computing (GPC) Hardware Platform
Shared object (.so)	TI Embedded Linux	OMAP C6000 DSP+ARM Processor

7. Cryptographic Key Management

7.1 Critical Security Parameters (CSPs)

All CSPs used by the cryptographic module are described in this section and the list of CSPs and public keys are listed in the following table.

Table 9: List of 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

7.2 Random Number Generation

The MSCDSM implements an Approved SP 800-90A DRBG for creation of random numbers. The entropy for seeding the SP 800-90A DRBG is determined by the user of the module which is outside of the module. The assurance of the minimum strength of the generated random bits from the module depends on the strength of the 384 bits seed provided to the module. 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 seed into the Module by calling module defined API function.

7.3 Key Generation

The MSCDSM does not provide any key generation service or perform key generation for any of its supported algorithms. The keys/CSPs listed in Table 8 are not generated within the module and are instead passed into the module from the user application via module provided APIs. Seeds for random number generation are set into the module via module provided API.

7.4 Key Entry and Output

The MSCDSM does not support manual key entry or key output. Keys or other CSPs can only be exchanged between the module and the calling application using appropriate API calls.

7.5 Key Storage

Keys are not stored in the non-volatile storage by the cryptographic module; however, the module stores it in the volatile memory for temporary usages.

7.6 Zeroization Procedure

The zeroization mechanism for all of the CSPs is to replace 0s in the volatile memory which originally store the CSPs. It is the calling application’s responsibility to zeroize CSPs as part of normal Encrypt/Decrypt services. All CSPs are zeroized by power cycling the module, which is referenced as the “Zeroize” service in Table 6.

7.7 CSP Access Type

Table 10: CSP Access Type

Access Type	Description
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 internally for encryption/decryption services.
Z - Zeroize CSP	Zeroize CSP 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 the Section 7.1 can only be accessed through APIs provided by the module. The keys can be destroyed in the Module's volatile memory by calling appropriate API function calls.

Table 11: CSP-Services Access Matrix (Approved Mode Only)

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

8. Electromagnetic Interfaces/Electromagnetic Compatibility (EMI/EMC)

The MSCDSM is a software only module that runs on GPC hardware platform. It inherits EMI/EMC validation of the operating hardware platform that it operates on.

9. Self-Tests

9.1 Power Up Self-Tests

The MSCDSM shall perform the following 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 (Instantiate and Generate)
- Software Integrity Test: HMAC-SHA-384
- Critical Functions Tests: N/A
- Random Number Generation Tests

9.2 Conditional Self-Test

The MSCDSM shall perform following conditional self-test,

Random bit generation tests:

- DRBG Continuous Tests
- SP800-90A Health Tests (Instantiate and Generate)

10. Mitigation of Other Attacks

The software 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.