Motorola Solutions, Inc.

ASTRO CDEM Motorola Advanced Crypto Engine (MACE)

FIPS 140-3 Non-Proprietary Security Policy

Document Version: R01.00.00
Date: January 16, 2025

Table of Contents

List of Tables

List of Figures

1 – General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version R03.01.02 of the ASTRO CDEM Motorola Advanced Crypto Engine (MACE) (Also referred to as ASTRO CDEM MACE). It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 3 module.

1.2 Security Levels

The FIPS 140-3 security levels for the Module are as follows from Table 1:

Section	Title	Security Level
1	General	3
2	Cryptographic module specification	3
3	Cryptographic module interfaces	3
4	Roles, services, and authentication	3
5	Software/Firmware security	3
6	Operational environment	N/A
7	Physical security	3
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	3
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	3

Table 1: Security Levels

2 – Cryptographic Module Specification

This document covers the Motorola Solutions ASTRO CDEM MACE module, hereafter denoted as the Module. The Module is implemented as a single-chip cryptographic module to meet FIPS 140-3 level 3 physical security requirements as defined by FIPS 140-3. The ASTRO CDEM MACE provides key storage and generation and performs all crypto processing for the Motorola Solutions ASTRO CDEM product.

2.1 Description

Purpose and Use:

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated overall Security Level 3. The Module is intended to be used in ASTRO CDEM unit.

Module Type: Hardware

Module Embodiment: SingleChip

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 1 and Figure 2. The Module is a single-chip embedded embodiment. The cryptographic boundary is shown in Figure 3.

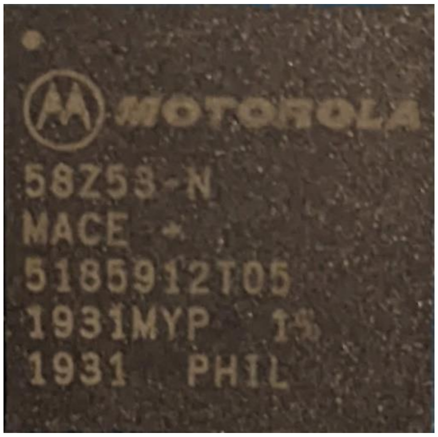

Figure 1 – ASTRO CDEM MACE IC (Top)

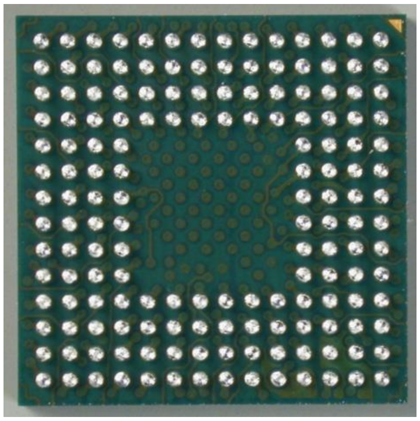

Figure 2 – ASTRO CDEM MACE IC (Interfaces)

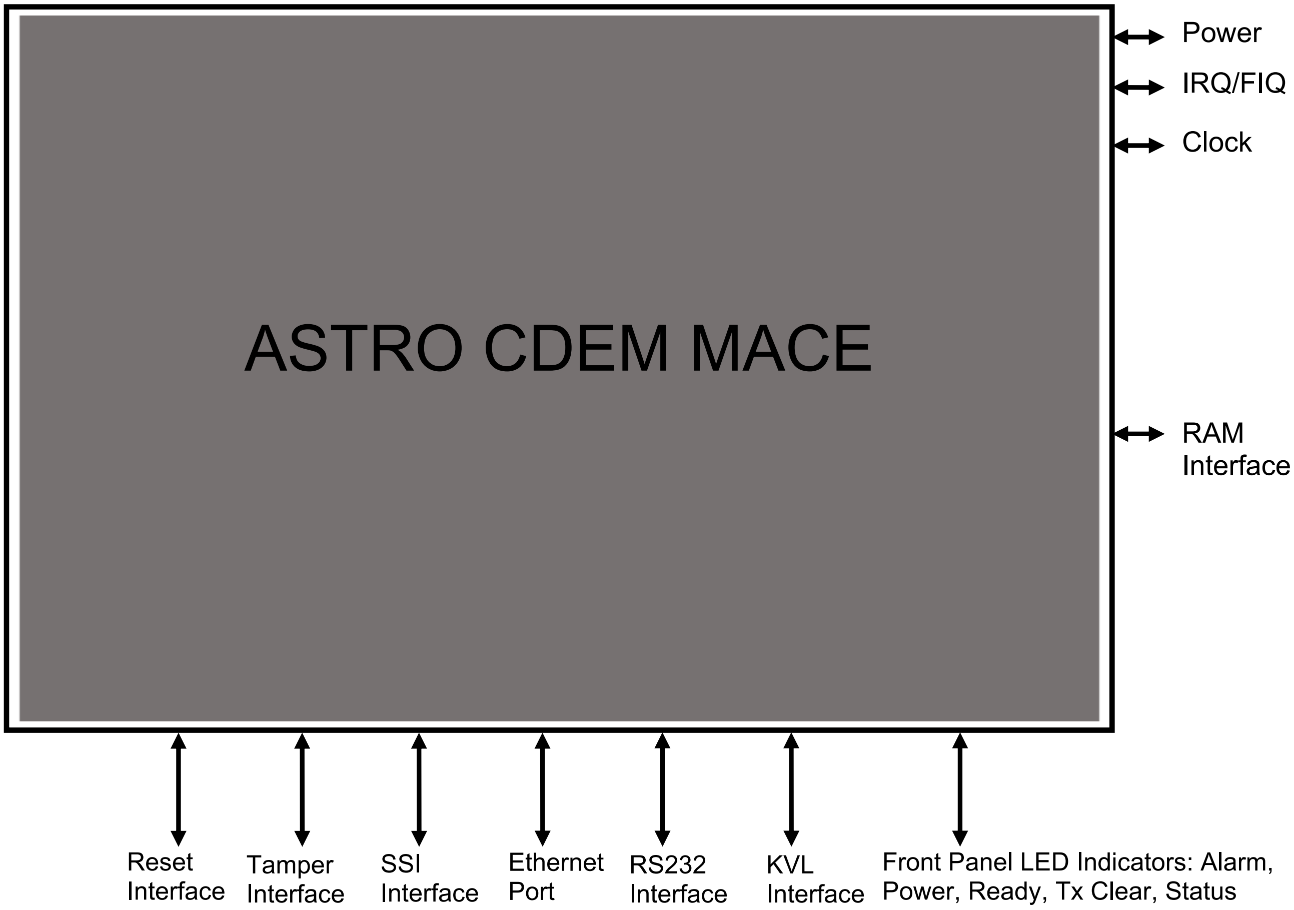

Figure 3 – Cryptographic Boundary

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

The ASTRO CDEM MACE cryptographic module is tested on the following operational environment.

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
ASTRO CDEM MACE	5185912Y03, 5185912Y05, 5185912T05	R03.01.02 with AES-256 DIA R01.00.07	Motorola Advanced Crypto Engine (MACE)	N/A

Table 2: Tested Module Identification – Hardware

The ASTRO CDEM MACE cryptographic module supports the following approved algorithms which may be installed separately from the MACE base firmware using the program update service. While the installation of AES may be done separately, for the purposes of this validation the MACE includes this firmware

Table 3 – Approved Mode Drop-in Algorithms

Algorithm*	Algorithm FW Version	Base FW Version	Cert. #
AES256	R01.00.07	R03.01.02	A5275

N/A for this module.

N/A for this module.

N/A for this module.

N/A for this module.

2.3 Excluded Components

The module does not exclude any components from the cryptographic boundary.

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
approved	Operating in approved mode	Approved	Display output

Table 4: Modes List and Description

The ASTRO CDEM MACE is originally non-compliant and must be configured to operate in an approved mode of operation. The MACE must be installed, initialized and configured, including a required change of the factory-default password in order to be in an approved mode. Documented below are the additional configuration settings that are required for the MACE to be used in an Approved Mode of operation at overall Security Level 3.

The approved mode is indicated by using the “Set FIPS Mode” service. The result from this service will display:

```
Encrypted only Key fill is Enabled.
Module is operating in FIPS 140-3 Level 3 approved mode
```

When the module is in the approved operating mode, the “Module Status” service can be used to verify the firmware version matches an approved version listed on NIST’s website: https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules

Mode Change Instructions and Status:

The module can be configured to operate in a FIPS 140-3 Approved mode of operation at overall Security Level 3. To configure the module to operate in Approved mode, the operator must log in as the CO using the default password and:

1. Change the default password
2. Activate and configure the periodic self-test timer
3. Type the command “`fips enable`” to configure the Module into approved mode(Level 3).

Additionally, the Module supports a “drop-in algorithm” via the Program Update service. Drop-in algorithms may be added or removed from the Module independent of the base FW. In order to remain in the Approved Mode, only Approved algorithms may be loaded into the Module, in particular AES-256 (Cert. # A5275). The loading and unloading of any firmware within the validated cryptographic module invalidates the Module’s validation and zeroizes all SSPs except those entered at manufacturing. The Module is then in a non-compliant state.

2.5 Algorithms

Approved Algorithms:

The Module implements the Approved cryptographic algorithms listed in the table below.

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5273	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-CBC	A5275	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-CFB8	A5273	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5275	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-KW	A5438	Direction - Decrypt Key Length - 256	SP 800-38F
AES-OFB	A5273	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-OFB	A5275	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
Counter DRBG	A5437	Prediction Resistance - No Mode - AES-256 Derivation Function Enabled - Yes	SP 800-90A Rev. 1
RSA SigVer (FIPS186-5)	A5253	Modulo - 2048 Signature Type - pkcs1v1.5	FIPS 186-5
SHA2-256	SHS 817	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4

Table 5: Approved Algorithms

ApprovedAlgorithmsTable From Web Cryptik ApprovedAlgorithmsTable

Vendor-Affirmed Algorithms:

The Module implements the FIPS Vendor Affirmed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric	N/A	SP800-133rev2 Sections 4 example 1 and IG D.H
CKG - IDK	Key Type:Symmetric	N/A	SP800-133rev2 Sections 6.3 #2 and IG C.I

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

The Module implements the FIPS Non-Approved, Allowed cryptographic Algorithms with No Security Claimed.

Name	Caveat	Use and Function
AES MAC	No Security Claimed. AES MAC is used as part of OTAR but is considered obfuscation.	[IG 2.4.A] P25 AES OTAR. AES MAC is applied directly to the plaintext OTAR key components and then KTS encryption is performed on the OTAR key components and decrypted within the module using AES KW Cert #5438

Table 7: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

N/A for this module.

2.6 Security Function Implementations

The following table shows the Security Function Implementations that the module implements:

Name	Type	Description	Properties	Algorithms
AES A5275 Encryption	BC-UnAuthEncrypt	Block Cipher		AES-CBC: (A5275) AES-OFB: (A5275) AES-ECB: (A5275)
AES A5275 Decryption	BC-UnAuthDecrypt	Block Cipher		AES-CBC: (A5275) AES-OFB: (A5275) AES-ECB: (A5275)
Key Generation	CKG	Symmetric Key Generation		Counter DRBG: (A5437) CKG : ()
Signature Verification	DigSig-SigVer	Digital Signature Verification		RSA SigVer (FIPS186-5): (A5253)
Entropy	ENT-ESV	Entropy Source		
KTS-Unwrap	KTS-Unwrap	Key Transport Unwrapping	Caveat:Key establishment methodology provides 256 bits strength Standard:SP 800-38F IG D.G:Approved method in KW mode	AES-KW: (A5438) AES MAC: ()
SHA	SHA	Secure Hash Standard		SHA2-256: (SHS 817)
AES A5273 Encryption	BC-UnAuthEncrypt	Block Cipher		AES-CFB8: (A5273) AES-CBC: (A5273) AES-OFB: (A5273)
AES A5273 Decryption	BC-UnAuthDecrypt	Block Cipher		AES-CFB8: (A5273) AES-CBC: (A5273) AES-OFB: (A5273)
IDK Generation	CKG	Symmetric Key Generation		CKG - IDK: ()

Name	Type	Description	Properties	Algorithms
DRBG	DRBG	AES-256 CTR Deterministic RBG		Counter DRBG: (A5437)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

The module does not have any algorithm specific information.

2.8 RBG and Entropy

Cert Number	Vendor Name
E132	Motorola Solutions Inc

Table 9: Entropy Certificates

The Module uses the following entropy sources:

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Motorola Solutions Advanced Crypto Engine Entropy Source	Physical	Atmel 5186912	1 bit	0.13862	N/A

Table 10: Entropy Sources

2.9 Key Generation

For Key Generation methods, see Section 2.6 Security Function Implementations above.

2.10 Key Establishment

For Key Establishment methods, see Section 2.6 Security Function Implementations above.

2.11 Industry Protocols

The module does not implement any Industry Protocols

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

The Module's ports and associated FIPS defined logical interface categories are listed below.

Physical Port	Logical Interface(s)	Data That Passes
Synchronous Interface (SSI)	Data Input Data Output Control Input Status Output	Provides an interface to the unprotected network and entry of the Crypto Officer password in encrypted form.
Ethernet Port (EP)	Data Input Data Output Control Input Status Output	This interface routes packets between subnets. The IP stack of this interface will use the subnet information to determine how to route packets between physical network interfaces.
RS232 Interface	Data Output Control Input Status Output	Provides an interface for factory programming and execution of RS232 shell commands.
Key Variable Loader (KVL)	Data Input Data Output Control Input Status Output	Provides an interface to the Key Variable Loader. The Traffic Encryption Key (TEK) is entered in encrypted form over the KVL interface.
RAM	Data Input Data Output Control Input Status Output	This interface provides storage for non-security related stack information.
Power	Power	This interface powers all circuitry.
Tamper Interface	Control Input	The interface is used for zeroization of Traffic Encryption Keys (TEKs), KPK.
Reset Interface	Control Input	This interface forces a reset of the module.
Alarm LED output	Status Output	The Alarm LED output is used to drive the external Alarm LED red to indicate a fatal error has been detected.
Power LED output	Status Output	The Power LED output is used to drive the external Power LED green when power is supplied to the module.

Physical Port	Logical Interface(s)	Data That Passes
Ready LED output	Status Output	The Ready LED output is used to drive the external Ready LED green when the module is ready to communicate with a KVL.
TX Clear LED output	Status Output	The TX Clear LED output is used to drive the external TX Clear LED orange when a "Bypass Rule" is programmed.
Status LED output	Status Output	The Status LED output is used to drive the external Status LED green to indicate a good battery, and a Traffic Encryption Key (TEK) has been loaded. The Status LED output is used to drive the external Status LED yellow to indicate a good battery, but no Traffic Encryption Key (TEK) has been loaded. The Status LED output is used to drive the external Status LED red to indicate a low or dead battery.
IRQ/FIQ	Control Input	External interrupts.
Clock	Control Input	Clock input

Table 11: Ports and Interfaces

Note: The module does not support Control Output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
AM1	Identity-based. Crypto-Officer Password: a 15-16 ASCII (printable) characters password is authenticated to gain access to Crypto-Officer services assocaited to the RS232 Interface. It should be noted that after authenticating, this password may be changed at any time.	SHA2-256 (SHS 817)	The password requires a minimum of 1 Upper case, 1 Lower case, 1 Numerical and 1 special character. Since the minimum password length is 15 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in {(10)*(262)*(32)*(9511)}, The password requires a minimum of 1 Upper case, 1 Lower case, 1 Numerical and 1 special character. Since the minimum password length is 15 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in {(10)*(262)*(32)*(95^11) }	After the CO password has been incorrectly entered 10 consecutive times, the Module will erase all CSPs, reset the CO password back to the default and set an alarm, at which time the module must be power cycled to become operational again. The strength per minute is 10 in {(10)*(262)*(32)*(95^11) }
AM2	Identity based. Crypto-Officer Password: a 10 hexadecimal digit long password is authenticated to gain access to Crypto	SHA2-256 (SHS 817)	The minimum password length is 10 hex digits. The probability of a successful random attempt is 10^16	After the CO password has been incorrectly entered 15 consecutive times, the Module will erase all CSPs, and set an alarm, at which time the module must be power cycled to become operational again. The strength per minute is 15x10^16.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	Officer services associated to the Synchronous Interface (SSI) port. It should be noted that after authenticating, this password may be changed at any time.			

Table 12: Authentication Methods

4.2 Roles

The Module supports one distinct operator role, the Cryptographic Officer (CO). The authentication method and services available to the CO will depend on the physical port used. The CO may be logged into both ports at the same time. In addition, the Module supports services which do not require authentication (UA).

The Roles Table below lists all operator roles supported by the Module.

The Module does not support concurrent operators.

Name	Type	Operator Type	Authentication Methods
Crypto-Officer (AM1)	Identity	CO	AM1
Crypto-Officer (AM2)	Identity	CO	AM2

Table 13: Roles

4.3 Approved Services

All approved services implemented by the Module are listed in the table below:

The SSPs modes of access shown in the table below are defined as:

- G = Generate: The Module generates or derives the SSP.
- R = Read: The SSP is read from the Module (e.g., the SSP is output).
- W = Write: The SSP is updated, imported, or written to the Module (SSP is input).
- E = Execute: The Module uses the SSP in performing a cryptographic operation.

- Z = Zeroize: The Module zeroizes the SSP

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Program Update	Update the ASTRO CDEM MACE firmware. Firmware upgrades are authenticated using a digital signature. The Program Update Public Signature Key is used to validate the signature of the firmware image being loaded before it is allowed to be executed using AM2.	Approved mode indicator and service status output	Firmware Image	The ASTRO CDEM MACE is upgraded to new firmware.	AES A5273 Decryption IDK Generation	Crypto-Officer (AM2) - FW-LD-Pub: Z - BKK: Z - IDK: Z - PEK: Z - KPK: Z - KEK: Z - TEK: Z - IDK-ROM: Z - IDK-Block: Z - CO PWD (AM1): Z - CO PWD (AM2): Z - PWD Hash: Z
Generate Entropy	Generate Entropy into the ASTRO CDEM MACE using AM2.	Approved mode indicator and service status output	DRBG Seed	The DRBG is seeded and initialized. Success/failure status	Entropy	Crypto-Officer (AM2) - DRBG-EI/Seed: G - DRBG-State: G - DRBG-nonce: G
OTEK	Load keys into the ASTRO CDEM	Approved mode indicator and	Encrypted Keys	Decrypted keys that were imported encrypted	AES A5273 Decryption	Crypto-Officer (AM2) - KEK: E - TEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	MACE using AM2.	service status output		into the ASTRO CDEM MACE. Success/failure status.		
Change CO Password (AM1)	Modify the current password used to identify and authenticate the CO role using AM1.	Approved mode indicator and service status output	Password	Updated the CO password. Success/failure status	SHA AES A5273 Encryption AES A5273 Decryption	Crypto-Officer (AM1) - PEK: E - KPK: G,E,Z - KEK: Z - TEK: Z - CO PWD (AM1): G,E,Z - PWD Hash: G,E,Z
Change CO Password (AM2)	Modify the current password used to identify and authenticate the CO role using AM2.	Approved mode indicator and service status output	Password	Updated the CO password. Success/failure status.	SHA AES A5273 Encryption AES A5273 Decryption	Crypto-Officer (AM2) - PEK: E - KPK: G,E,Z - KEK: Z - TEK: Z - CO PWD (AM2): G,E,Z - PWD Hash: G,E,Z
Validate CO Password (AM1)	Validate the current password used to identify and authenticate the CO role using AM1.	Approved mode indicator and service status output Approved mode indicator and service status output	Password	Successful authentication will allow access to the services allowed for CO role (AM1).	SHA AES A5273 Encryption AES A5273 Decryption	Crypto-Officer (AM1) - PEK: E - KPK: G,E,Z - KEK: Z - TEK: Z - CO PWD (AM1): Z - CO PWD (AM2): Z - PWD Hash: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Validate CO Password (AM2)	Validate the current password used to identify and authenticate the CO role using AM2.	Approved mode indicator and service status output	Password	Successful authentication will allow access to the services allowed for CO role (AM2).	SHA AES A5273 Encryption AES A5273 Decryption	Crypto-Officer (AM2) - PEK: E - KPK: G,E,Z - KEK: Z - TEK: Z - CO PWD (AM1): Z - CO PWD (AM2): Z - PWD Hash: Z
Logout CO (AM1)	Exits command shell interface using AM1.	Approved mode indicator and service status output	Command In	Logout CO/Exits command shell interface	None	Crypto-Officer (AM1)
Logout CO (AM2)	CO Logout	Approved mode indicator and service status output	Reboot/Command In	Logout CO	None	Crypto-Officer (AM2)
Encrypt	Encrypt data using AM2.	Approved mode indicator and service status output	Plaintext	Ciphertext. Success/failure status.	AES A5275 Encryption	Crypto-Officer (AM2) - TEK: E - KEK: E - KPK: E - DRBG-EI/Seed: E - DRBG-State: E - DRBG-nonce: E
Decrypt	Decrypt data using AM2.	Approved mode indicator and service	Ciphertext	Plaintext. Success/failure status.	AES A5275 Decryption	Crypto-Officer (AM2) - TEK: E - KEK: E - KPK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		status output				
Module Status	Provide firmware version, current FIPS status using AM1.	Approved mode indicator and service status output	Command in	Module HW version, version information, and FIPS status.	None	Crypto-Officer (AM1)
Self-Tests	Perform module self-tests comprised of cryptographic algorithm tests, firmware integrity test, and critical functions test. Initiated by module reset or transition from power off state to power on state using AM1 or UA.	Approved mode indicator and service status output	Power on/Command In	Success/Reset.	AES A5275 Encryption AES A5275 Decryption Key Generation Signature Verification Entropy KTS-Unwrap SHA AES A5273 Encryption AES A5273 Decryption IDK Generation DRBG	Crypto-Officer (AM1) - FW-LD-Pub: E Unauthenticated - FW-LD-Pub: E
Module Configuration	Set configuration parameters used to specify	Approved mode indicator and service	Configuration parameters	Updated module configuration. Success/failure status.	None	Crypto-Officer (AM1) - KPK: G,E,Z - KEK: Z - TEK: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	module behavior using AM1.	status output				- CO PWD (AM1): W,Z - PWD Hash: W,Z - CO PWD (AM2): W,Z
Set FIPS Mode	Update module approved mode using AM1.	Approved mode indicator and service status output	Configuration parameters	Updated module approved mode/Display current approved mode	None	Crypto-Officer (AM1)
Configure OTEK	Set configuration parameters used for communication with the KMF for OTEK using AM1.	Approved mode indicator and service status output	Configuration parameters	Updated OTEK configuration. Success/failure status.	None	Crypto-Officer (AM1)
Version Query	Provides module firmware and hardware version numbers using AM1.	Approved mode indicator and service status output	Command In	Show module version info	None	Crypto-Officer (AM1)
Delete Key	Mark key for deletion using AM2.	Approved mode indicator and service status output	Command In	Key is marked for deletion. Success/failure status.	None	Crypto-Officer (AM2)
Perform Key Transport Process	Perform a key transport process for OTEK service using AM2.	Approved mode indicator and service	Command In	Keys imported into the MACE. Success/failure status.	KTS-Unwrap AES A5273 Decryption	Crypto-Officer (AM2) - KEK: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		status output				
KVL Transfer Key	Imports keys to the ASTRO CDEM MACE via KVL using AM2.	Approved mode indicator and service status output	Encrypted Keys	Keys imported into the ASTRO CDEM MACE. Success/failure status.	KTS-Unwrap	Crypto-Officer (AM2) - BKK: E - KPK: E - KEK: W - TEK: W
KVL Delete Key	Zeroize selected key variables from the ATRO CDEM MACE using AM2.	Approved mode indicator and service status output	Command In	Keys deleted from the ASTRO CDEM MACE. Success/failure status.	None	Crypto-Officer (AM2) - KEK: Z - TEK: Z
KVL Check Key	Obtain status information about a specific key/keyset using AM2.	Approved mode indicator and service status output	Command In	Show key status	None	Crypto-Officer (AM2) - BKK: E
KVL Query Algorithm List	Provides algorithm version numbers using AM2.	Approved mode indicator and service status output	Command In	Show list of supported algorithms	None	Crypto-Officer (AM2)
KVL Query Version	Provides module firmware version numbers using AM2.	Approved mode indicator and service status output	Command In	Show module version info	None	Crypto-Officer (AM1)
Extract Error Log	Provide the history of error events using AM1.	Approved mode indicat	Command In	Error logs out. Success/Failure status.	None	Crypto-Officer (AM1)

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		or and service status output				
Reset Crypto Module	Reset/power cycle the ASTRO CDEM MACE.	Approved mode indicator and service status output	Reset Button press/Cycle power.	Reset the MACE.	None	Unauthenticated - DRBG-EI/Seed: Z - DRBG-State: Z - DRBG-nonce: Z - BKK: Z - IDK: Z - PEK: Z - KPK: Z - KEK: Z - TEK: Z - CO PWD (AM1): Z - CO PWD (AM2): Z - PWD Hash: Z - FW-LD-Pub: Z - IDK-ROM: Z - IDK-Block: Z
Erase Crypto Module	Zeroize the KPK and all keys and CSPs in the key database and causes a new KPK to be generated. Resets the password to the factory default.	Approved mode indicator and service status output	Erase Button press	Zeroize all CSPs	None	Unauthenticated - KPK: G,Z - KEK: Z - TEK: Z - CO PWD (AM1): Z - CO PWD (AM2): Z - PWD Hash: Z

Table 14: Approved Services

4.4 Non-Approved Services

There are no Non-Approved services available while the module is in the approved mode.

N/A for this module.

4.5 External Software/Firmware Loaded

This module supports loading of external firmware via the Program Update service. Execution of the successfully loaded firmware is only effective after the next reset of the security module. Any firmware loaded into the module other than that listed in section 2.2 Tested and Vendor Affirmed Module Version and Identification, is outside the scope of this Security Policy and requires a separate FIPS 140-3 validation.

The module validates the integrity of the externally loaded firmware via procedures described in section 5.1 Integrity Techniques

5 Software/Firmware Security

5.1 Integrity Techniques

The Module has a limited modifiable operational environment under the FIPS 140-3 definitions. The Module is composed of the following firmware components:

- Component 1: Executable - binary
- Component 2: Drop in Algorithms - binary

The firmware components are protected with the FW-LD-Pub key described in section 9.4 SSPs. The FW-LD-Pub key is loaded into the module at manufacturing

The operator can initiate the integrity test on demand by power cycling the Module.

5.2 Initiate on Demand

The operator can initiate the integrity test on demand by power cycling the Module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

The ASTRO CDEM MACE has a limited operational environment under the FIPS 140-3 definitions with a Physical Security at Level 3. Therefore, per the FIPS 140-3 Management Manual Section 7.5, partial validations and non-applicable areas in this section are not applicable.

7 Physical Security

The ASTRO CDEM MACE is a production grade, single-chip cryptographic module with standard passivation over the modules circuitry as defined by FIPS 140-3 and is designed to meet level 3 physical security requirements. The information below is applicable to cryptographic module hardware kit numbers 5185912Y03, 5185912Y05, and 5185912T05, which have identical physical security characteristics.

7.1 Mechanisms and Actions Required

The ASTRO CDEM MACE is covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the ASTRO CDEM MACE. The security provided from the hardness of the ASTRO CDEM MACE's epoxy encapsulate is claimed at the temperature range of -40 to 85 degrees Celsius. No assurance of the epoxy hardness is claimed for this physical security mechanism outside of this range. The ASTRO CDEM MACE does not contain any doors, removable covers, or ventilation holes or slits. No maintenance access interface is available. No special procedures are required to maintain physical security of the ASTRO CDEM MACE while delivering to operators.

Mechanism	Inspection Frequency	Inspection Guidance
Covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the ASTRO CDEM MACE.	Periodically	Look for signs of tampering. Remove from service if tampering found.

Table 15: Mechanisms and Actions Required

7.2 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-38.1°C	EFP	Shutdown - A tamper flag is raised, a wake-up reset of the product is triggered.
HighTemperature	101.4°C	EFP	Shutdown - A tamper flag is raised, a wake-up reset of the product is triggered.
LowVoltage	1.65V - VDDCORE : 1.350V - VVDBU	EFP	Shutdown - A general reset of the chip is asserted.
HighVoltage	2.04V - VDDCORE : 2.292V - VVDBU	EFP	Shutdown- A tamper flag is raised, a wake-up reset of the product is triggered.

Table 16: EFP/EFT Information

7.3 Hardness Testing Temperature Ranges

Temperature Type	Temperature
LowTemperature	-40°C
HighTemperature	85°C

Table 17: Hardness Testing Temperatures

Notes: The module is hardness tested at the lowest and highest temperatures within the module's intended temperature range of operation.

8 Non-Invasive Security

The Module does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
System Memory (S1)	Stored in the volatile memory (RAM).	Dynamic
Flash Memory (S2)	Stored in the flash in plaintext, associated by memory location (pointer).	Static
Flash Memory - Encrypted (S3)	Stored in the flash in encrypted, associated by memory location (pointer).	Static

Table 18: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input encrypted on the IDK (I1)	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Manual	Electronic	AES A5273 Decryption
Input encrypted on the PEK(I2)	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Manual	Electronic	AES A5273 Decryption
Input encrypted on the KEK (I3)	OTAR	Flash Memory - Encrypted (S3)	Encrypted	Automated	Electronic	KTS-Unwrap
Input encrypted on the BKK (I4)	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Manual	Electronic	AES A5273 Decryption

Table 19: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroized by the "Program Update" service by overwriting with a fixed pattern of 0s. *	SSPs zeroized upon loading of new firmware.	Yes

Zeroization Method	Description	Rationale	Operator Initiation
Z2	Zeroized by module power cycle or hard reset by overwriting with a fixed pattern of 0s. *	SSPs in volatile memory zeroized.	Yes
Z3	Zeroized by the "Configure Module" service by overwriting with a fixed pattern of 0s.	CO zeroize module when configuring into an Approved mode.	Yes
Z4	Zeroized by the "Change CO Password (AM1)" service by overwriting with a fixed pattern of 0s.	Old CO password zeroized as new CO password set	Yes
Z5	Zeroized by the "Validate CO Password (AM1)" service by overwriting with a fixed pattern of 0s.	CO password zeroized after too many failed login attempts	Yes
Z6	Zeroized by the "Change CO Password (AM2)" service by overwriting with a fixed pattern of 0s.	Old Crypto Officer password zeroized as new Crypto Officer password set	Yes
Z7	Zeroized by the "Validate CO Password (AM2)" service by overwriting with a fixed pattern of 0s.	Crypto Officer password zeroized after too many failed login attempts	Yes
Z8	Zeroized by Tamper event. (KPK) is zeroized with a fixed pattern of 0s.	Zeroizes KPK	N/A

Table 20: SSP Zeroization Methods

Note: For zeroization methods with an asterisk, once zeroization is complete the Module will reboot, indicating successful zeroization. The output status of all other methods of success of zeroization are implicit and any attempt to use previous keys/CSPs will trigger an error.

9.4 SSPs

All usage of these SSPs by the Module are described in the services detailed in Section 4.3

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
DRBG-EI/Seed	Internally generated by the HWRNG	2770 - N/A	N/A - CSP	Entropy		DRBG
DRBG-State	CTR_DRBG internal state: V (128 bits) and Key (AES 256)	256 - 256	N/A - CSP	DRBG		DRBG
DRBG-nonce	Internally generated by the HWRNG	128 - N/A	N/A - CSP	Entropy		DRBG
BKK	A 256-bit AES OFB (A5273) key used to decrypt keys loaded from KVL	256 - 256	Symmetric Key - CSP	Other		AES A5273 Decryption
IDK	A 256-bit AES CBC key used to decrypt downloaded firmware images.	256 - 256	Symmetric Key - CSP	IDK Generation		AES A5273 Decryption
PEK	256-bit AES-CFB8 key used for decrypting passwords during password validation	256 - 256	Symmetric Key - CSP	Pre-loaded at manufacturing		AES A5273 Decryption
KPK	256 bit AES CFB-8 key used to encrypt all TEKs and KEKs stored in the flash.	256 - 256	Symmetric Key - CSP	Key Generation		Key Generation AES A5273 Decryption
KEK	256-bit AES-KW key used for decryption of keys in key transport operation	256 - 256	Symmetric Key - CSP			KTS-Unwrap AES A5273 Decryption
TEK	256-bit AES-KW key used for enabling secure communication with target devices.	256 - 256	Symmetric Key - CSP			KTS-Unwrap AES A5273 Decryption
CO PWD (AM1)	8-32 ASCII characters CO password.	N/A - N/A	Authentication - CSP			AES A5273 Encryption AES A5273 Decryption

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
CO PWD (AM2)	8-32 ASCII characters Crypto Officer password.	N/A - N/A	Authentication - CSP			AES A5273 Encryption AES A5273 Decryption
PWD Hash	256-bit password hash stored in the non-volatile memory.	256 - 128	Authentication - CSP	SHA		SHA
FW-LD-Pub	2048-bit RSA key used to validate the signature of the firmware image during FW integrity and FW Loading before it is allowed to be executed.	2048 - 112	Asymmetric Public Key - PSP	Pre-loaded at manufacturing		Signature Verification
IDK-ROM	A 256-bit AES CBC key used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK Block	256 - 256	Symmetric - CSP	Pre-loaded at manufacturing		CKG - IDK
IDK-Block	A 256-bit AES CBC key used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK ROM	256 - 256	Symmetric Key - CSP	Generated with an approved RBG and pre-loaded at manufacturing		CKG - IDK

Table 21: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DRBG-EI/Seed		System Memory (S1):Plaintext	When module is reset	Z2	DRBG-nonce:Used With DRBG-State:Generates
DRBG-State		System Memory (S1):Plaintext	When the module is rest	Z2	DRBG-EI/Seed:Derived From DRBG-nonce:Derived From
DRBG-nonce		System Memory (S1):Plaintext	When module is reset	Z2	DRBG-EI/Seed:Used With DRBG-State:Generates

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
BKK	Input encrypted on the IDK (I1)	System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	KEK:Decrypts TEK:Decrypts
IDK		System Memory (S1):Plaintext	When module is reset	Z2	IDK-ROM:Derived From IDK-Block:Derived From PEK:Decrypts KEK:Decrypts
PEK	Input encrypted on the IDK (I1)	System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	CO PWD (AM1):Decrypts CO PWD (AM2):Decrypts PWD Hash:Used With
KPK		System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1 Z3 Z4 Z5 Z6 Z7 Z8	DRBG-State:Derived From
KEK	Input encrypted on the KEK (I3) Input encrypted on the BKK (I4)	System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	KPK:Encrypted by TEK:Decrypts
TEK	Input encrypted on the KEK (I3) Input encrypted on the BKK (I4)	System Memory (S1):Plaintext Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z2	KPK:Encrypted by
CO PWD (AM1)	Input encrypted on the PEK(I2)	System Memory (S1):Plaintext Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z3 Z4 Z5 Z6 Z7	PEK:Encrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CO PWD (AM2)	Input encrypted on the PEK(I2)	System Memory (S1):Plaintext Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z3 Z4 Z5 Z6 Z7	PEK:Encrypted by
PWD Hash		System Memory (S1):Plaintext Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z3 Z4 Z5 Z6 Z7	CO PWD (AM1):Hash of CO PWD (AM2):Hash of
FW-LD-Pub		System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1	IDK:Encrypted by
IDK-ROM		System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	IDK:Generates IDK-Block:Paired With
IDK-Block		System Memory (S1):Plaintext Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	IDK:Generates IDK-ROM:Paired With

Table 22: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

The ASTRO CDEM MACE performs self-tests to ensure the proper operation. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

Pre-operational self–tests are available on demand by power cycling the ASTRO CDEM MACE. In addition, pre-operational self–tests are periodically performed by the ASTRO CDEM MACE as configured by the operator during the module configuration as shown in section 11.1 Installation, Initialization, and Startup Procedures The ASTRO CDEM MACE will not accept any commands when a periodic self-test is required; the commands still in the I/O buffer will be processed by the ASTRO CDEM MACE after periodic self-test ends and will execute when the I/O buffer is emptied. The ASTRO CDEM MACE logs the most recent self-test errors to the internal flash; the operator (CO) can extract the error logs using Extract Error Log service.

The Module performs the following pre-operational self-tests in table below

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity	SHA2-256 (Cert. #817), RSA-2048 (Cert. #A5253)	KAT	SW/FW Integrity	E2 on failure	When the ASTRO CDEM MACE is powered up, the digital signature is verified.

Table 23: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

The Module performs the following conditional self-tests in the table below

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-Encryption (A5273)	AES-256	KAT	CAST	ES1 on failure	Encryption	Bootup/Periodic
AES-Decryption (A5273)	AES-256	KAT	CAST	ES1 on failure	Decryption	Bootup/Periodic
AES-Encryption (A5275)	AES-256	KAT	CAST	ES1 on failure	Encryption	Bootup/Periodic
AES-Decryption (A5275)	AES-256	KAT	CAST	ES1 on failure	Decryption	Bootup/Periodic
AES-KW (A5438)	AES-256	KAT	CAST	ES1 on failure	Decryption	Bootup/Periodic
Counter DRBG (A5437)	AES-256 CTR	KAT	CAST	ES1 on failure	AES-256 CTR_DRBG instantiation, generate KATs performed before the first random data generation	Bootup/Periodic
SHA2-256 (SHS 817)	SHA2-256	KAT	CAST	E2 on failure	SHA2, -256, KAT performed before Pre-Operational FW integrity tests.	Bootup
RSA SigVer (FIPS186-5) (A5253)	RSA-2048 SigVer	KAT	CAST	E2 on failure	RSA-2048 SigVer, performed before Pre-Operational FW integrity tests.	Bootup
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	RCT	CAST	ES1 on failure	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Bootup
Entropy 90B Start-up Adaptive Proportion Test (ADP)	Adaptive Proportion Test	ADP	CAST	ES1 on failure	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environment al change affecting the noise source	Bootup
Firmware Load	2048-bit RSA Signature Verification/SHA2-256	KAT	SW/FW Load	E2 on failure	A digital signature is generated over the code when it is built using SHA-256 and RSA-2048.	loading a new firmware image

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					The digital signature is verified upon download into the ASTRO CDEM MACE.	

Table 24: Conditional Self-Tests

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity	KAT	SW/FW Integrity	On Demand	Manually

Table 25: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-Encryption (A5273)	KAT	CAST	On Demand/Periodically	Manually/Programmatically
AES-Decryption (A5273)	KAT	CAST	On Demand/Periodically	Manually/Programmatically
AES-Encryption (A5275)	KAT	CAST	On Demand/Periodically	Manually/Programmatically
AES-Decryption (A5275)	KAT	CAST	On Demand/Periodically	Manually/Programmatically
AES-KW (A5438)	KAT	CAST	On Demand/Periodically	Manually/Programmatically
Counter DRBG (A5437)	KAT	CAST	On Demand/Periodically	Manually/Programmatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
SHA2-256 (SHS 817)	KAT	CAST	On Demand/Periodically	Manually/Programmatically
RSA SigVer (FIPS186-5) (A5253)	KAT	CAST	On Demand/Periodically	Manually/Programmatically
Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	On Demand	Manually
Entropy 90B Start-up Adaptive Proportion Test (ADP)	ADP	CAST	On Demand	Manually
Firmware Load	KAT	SW/FW Load	On Demand	Manually

Table 26: Conditional Periodic Information

Conditional self–tests are periodically performed by the ASTRO CDEM MACE every X hours, where X is configured by the operator during module configuration (1 hour to 720 hours). The ASTRO CDEM MACE will not accept any commands when a periodic self-test is required; the commands still in the I/O buffer will be processed by the ASTRO CDEM MACE end the periodic self-test executed when the I/O buffer is emptied.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ES1	The ASTRO CDEMMACE fails a KAT.	The ASTRO CDEM MACE enters the critical error state. In this state, the ASTRO CDEM MACE stores the status into the internal flash memory and then halts all further operation by entering an infinite loop.	Reboot/Power cycle the module	Sets the status alarm LED.
ES2	The ASTRO CDEMMACE fails a firmware loading during program upgrade and/or firmware integrity pre-operational self-test.	The ASTRO CDEM MACE enters the firmware signature validation failure state. In this state, the ASTRO CDEM MACE halts all further operations by entering the flash programming mode.	Reboot/Power cycle the module or re-flashing a new image.	Sets the status alarm LED.

Table 27: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Installation and Initialization:

The Module is originally a non-compliant module and must be initialized to be in Approved mode. There is no non-Approved mode. During initialization the operator shall configure the Module from the instructions below:

1. Upon first access, the operator will use the default passwords provided by Motorola in a separate communication.
2. The operator will then change the default passwords based on the requirements in the Roles and Authentication table.
3. The operator will set the periodic self-tests timer as part of the Module configuration in every X minutes, where X is a minimum value = 1 hour and maximum value = 720 hours. Note: the default minimum = 0* but must be changed to a minimum of 1.
4. The operator will then complete Module configuration using the Module Configuration and Configure OTEK services.
5. Finally, the operator will set the Module to the Approved mode using the Set FIPS Mode service.

   * periodic self-tests will not perform if minimum = 0

Delivery:

The Module is used in multiple Motorola Solutions, Inc. products. Motorola uses commercially available courier systems such as UPS, FedEx, and DHL with a tracking number and requires a signature at the end from an authorized client.

11.2 Administrator Guidance

Use vendor provided product specific user guide for secure operations.

11.3 Non-Administrator Guidance

N/A

11.4 Design and Rules

Rules of Operation

1. The Module provides one distinct operator role: Cryptographic Officer.
2. The Module provides identity-based authentication.

3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
6. All self-tests do not require any operator action.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The Module does not support concurrent operators.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual SSP establishment method.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module does not enter or output plaintext CSPs.
15. The Module does store some CSPs in plaintext.
16. The Module does not output intermediate key values.

The Module does not provide bypass services or ports/interfaces.

11.5 Maintenance Requirements

N/A

11.6 End of Life

After the end-of-life, the operator should zeroize all SSPs using "Erase Crypto Module" service followed by shredding the ASTRO CDEM MACE chip.

12 Mitigation of Other Attacks

The Module does not implement any mitigation method against other attacks.

References and Definitions

The following standards are referred to in this Security Policy.

Table 28 References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, August 30, 2024*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[186-5]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, February 2023.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001, Updated May 9, 2023*
[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*
[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, Revision 1, June 2015.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*

Table 29 Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
BKK	Black Keyloading Key
CAI	Common Air Interface
CBC	Cipher Block Chaining
CDEM	CAI Data Encryption Module
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DRBG-EI	DRBG Entropy Input
ECB	Electronic Code Book
FIPS	Federal Information Processing Standards
FW	Firmware
FW-LD-Pub	Firmware Load Public Key
IC	Integrated Circuit
IDK	Image Decryption Key
IV	Initialization Vector
KAT	Known Answer Test
KPK	Key Protection Key
KEK	Key Encryption Key
KVL	Key Variable Loader
MAC	Message Authentication Code
MACE	Motorola Advanced Crypto Engine
OFB	Output Feedback
OTAR	Over The Air Rekeying
PEK	Password Encryption Key
PWD Hash	Password Hash
RSA	Rivest–Shamir–Adleman
SSI	Synchronous Serial Interface
SSP	Sensitive Security Parameter
TEK	Traffic Encryption Key

Acronym	Definition
UA	Unauthenticated Service