Non-Proprietary Security Policy: ASTRO CDEM Motorola Advanced Crypto Engine (MACE)

Cryptographic module used in Motorola Solutions ASTRO CDEM MACE

Version: R01.00.11

Date: July 22, 2019

Table of Contents

1. Introduction

1.1. Scope

This Security Policy specifies the security rules under which the ASTRO CDEM MACE Motorola Advanced Crypto Engine, herein identified as the ASTRO CDEM MACE, must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and those imposed additionally by Motorola Solutions Inc. (Motorola). These rules, in total, define the interrelationship between the:

- Module Operators,
- Module Services, and
- Critical Security Parameters (CSPs).

1.2. Definitions

ALGID	Algorithm Identifier
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CKR	Common Key Reference
CO	Crypto-Officer
CSP	Critical Security Parameter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
EI	Ethernet Interface
IV	Initialization Vector
KEK	Key Encryption Key
KPK	Key Protection Key
KVL	Key Variable Loader
LED	Light-emitting diode
LFSR	Linear Feedback Shift Register
MACE	Motorola Advanced Crypto Engine
PEK	Password Encryption Key
RAM	Random Access Memory
RNG	Random Number Generator
TEK	Traffic Encryption Key

1.3. Overview

The ASTRO CDEM MACE provides secure key management and data encryption/decryption for the Astro System.

1.4. ASTRO CDEM MACE Implementation

The ASTRO CDEM MACE is implemented as a single-chip cryptographic module as defined by FIPS 140-2.

1.5. ASTRO CDEM MACE Hardware / Firmware Version Numbers

FIPS Validated Cryptographic Module Hardware Kit Numbers	FIPS Validated Cryptographic Module Firmware Version Numbers
5185912Y01, 5185912Y03 and 5185912Y05	R01.03.00

1.6. ASTRO CDEM MACE Cryptographic Boundary

The ASTRO CDEM MACE Cryptographic Boundary is drawn around the MACE IC as shown below.

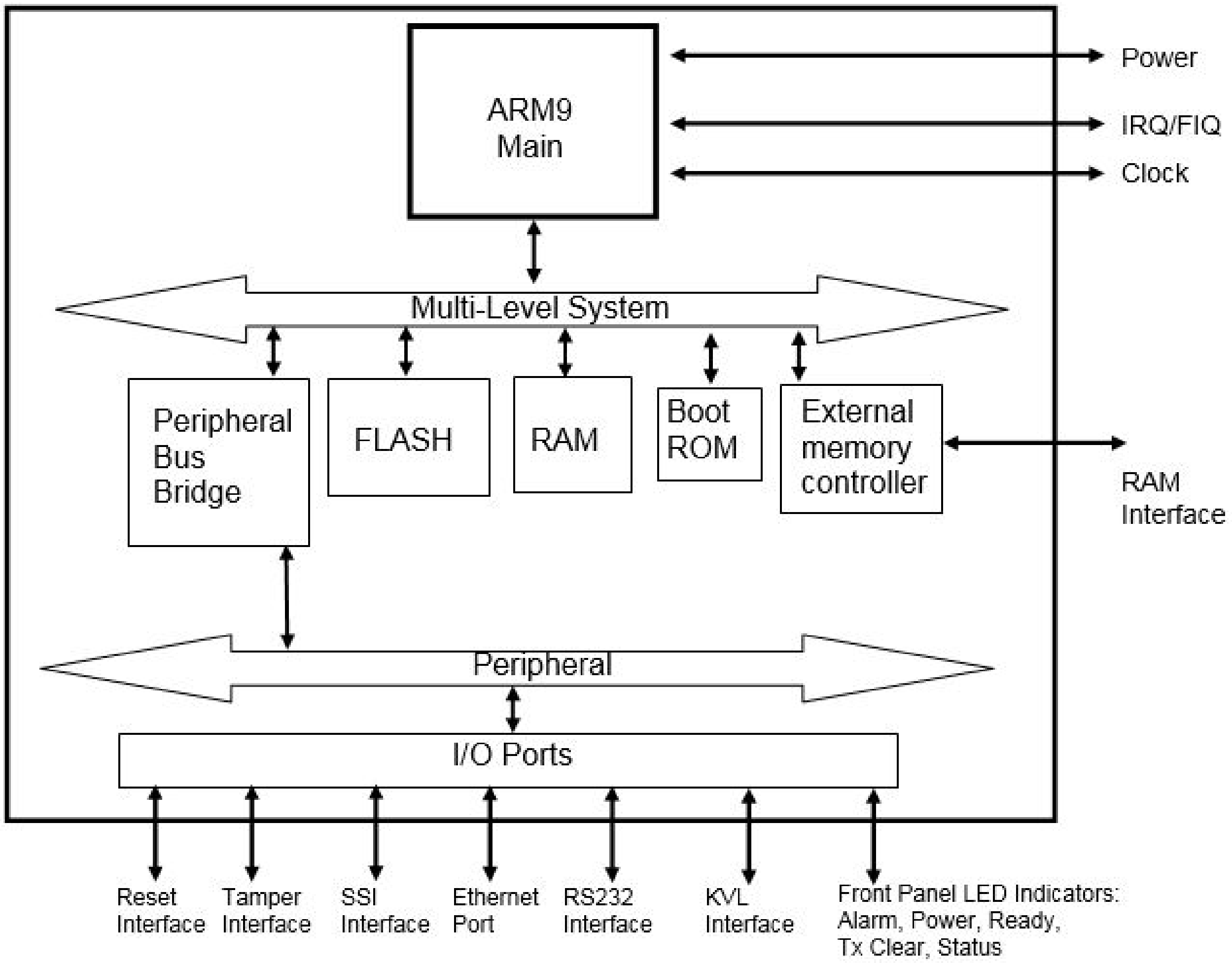

Figure 1: ASTRO CDEM MACE Block Diagram

The Crypto Boundary is drawn around the ASTRO CDEM MACE IC which is responsible for all key storage and generation and performs all crypto processing for the ASTRO CDEM MACE.

1.7. Ports and Interfaces

The ASTRO CDEM MACE provides the following ports and logical interfaces defined in Table 1. Please note, although physically all of the ports are pins (as shown in Figure 3) logically they map to the interfaces (as shown in Figures 4 and 5).

Table 1**: Ports and Interfaces**

Physical Port	Qty	Logical interface definition	Description
Serial Synchronous Interface (SSI)	1	• Data Input • Data Output • Control Input • Status Output	Provides an interface to the unprotected network and entry of the User password in encrypted form. This interface does not support output of CSP's.
Ethernet Port (EP)	1	• Data Input • Data Output • Control Input • Status Output	This interface routes packets, including TEKs, between subnets. The IP stack of this interface will use the subnet information to determine how to route packets between physical network interfaces. This interface does not support any other input / output of CSP's.
RS232 Interface	1	• Control Input • Status Output • Data Output • Data Input	Provides an interface for factory programming and execution of RS232 shell commands. This interface does not support output of CSP's.
Key Variable Loader (KVL)	1	• 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. This interface does not support output of CSP's.
RAM	1	• Data Input • Data Output • Control Input • Status Output	This interface provides storage for non-security related stack information. This interface does not support input / output of CSP's.
Power	1	• Power Input • Internal battery-backed RAM	This interface powers all circuitry. This interface does not support input / output of CSP's.
Tamper Interface	1	• Control Input	The interface is used for zeroization of Traffic Encryption Keys (TEKs), KPK.
Reset Interface	1	Control Input	This interface forces a reset of the module.
Alarm LED output	1	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	1	Status Output	The Power LED output is used to drive the external Power LED green when power is supplied to the module.
Ready LED output	1	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	1	Status Output	The TX Clear LED output is disabled in the ASTRO CDEM MACE.
Status LED output	1	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	2	Control Input	External interrupts.
Clock	1	Control Input	Clock input

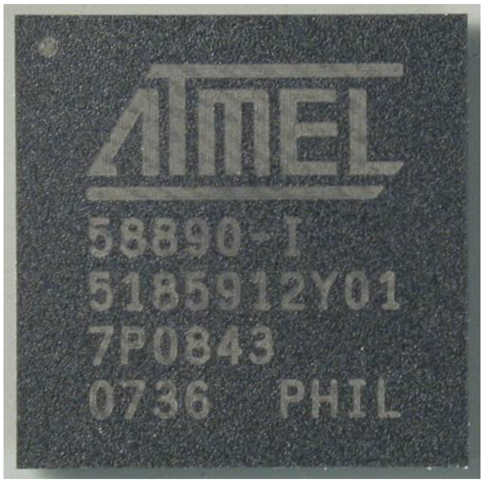

Figure 2: CDEM MACE Chip (Top)

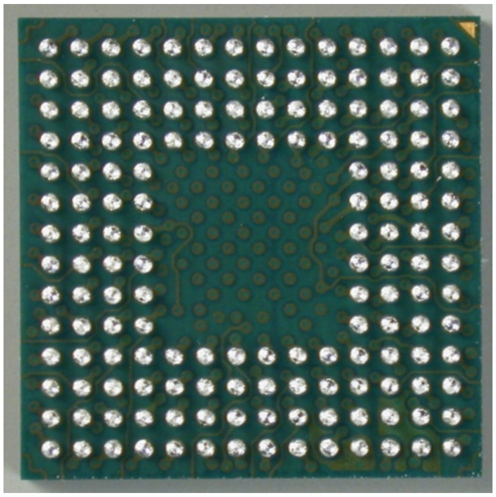

Figure 3: CDEM MACE Chip (Interfaces)

Figures 4 and 5 are provided below in to show what the pins in Figure 3 map to. The enclosure and related components are not part of the cryptographic boundary, only the CDEM MACE chip shown in Figures 2 and 3.

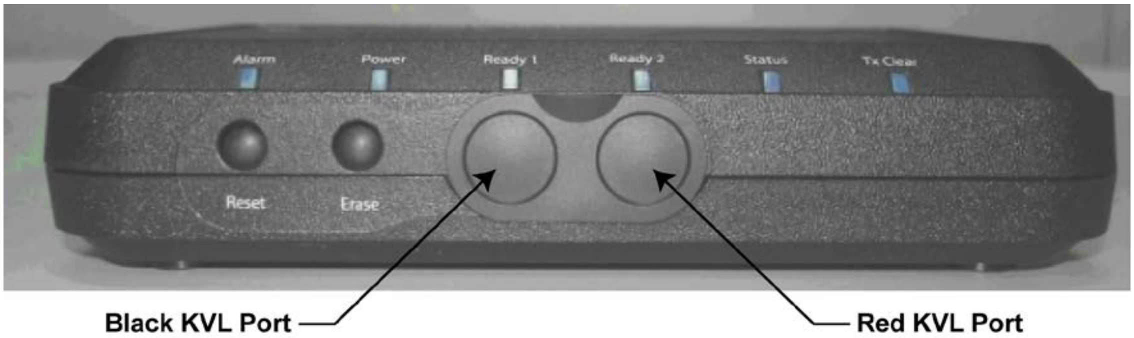

Figure 4: CDEM Front View

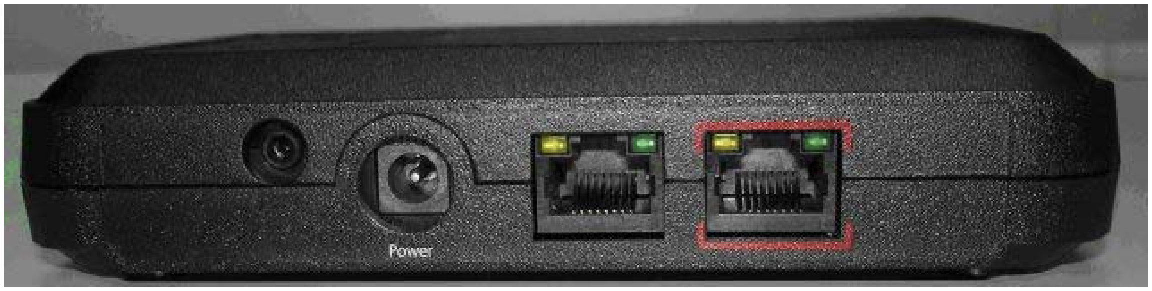

Figure 5: CDEM Back View

2. FIPS 140-2 Security Levels

The ASTRO CDEM MACE is designed to operate at FIPS 140-2 overall Security Level 3. 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 2: ASTRO CDEM MACE Security Levels

FIPS 140-2 Security Requirements Section	Validated Level at overall Security Level 3
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI / EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

3. FIPS 140-2 Approved Operational Modes

The ASTRO CDEM MACE can be configured to operate in a FIPS 140-2 Approved mode of operation and a non-FIPS Approved mode of operation. CSPs are not shared between FIPS Approved mode and non-FIPS Approved mode. The transition from a FIPS Approved mode to a non-FIPS approved mode, and vice versa, causes all CSPs to be zeroized. The FIPS mode is indicated by issuing the "fips" command on the serial command shell. The result from this command will display whether or not the module is in FIPS approved operating 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

3.1. Configuration Settings for operation at FIPS 140-2 overall Security Level 3

Documented below are the configuration settings that are required for the module to be used in a FIPS 140-2 Approved mode of operation at overall Security Level 3.

1. Disable Red Keyfill. The Module Configuration service, issued from the ASTRO CDEM MACE command line, is used to configure this parameter in the module.
2. Only Approved and Allowed algorithms used. The module supports the following Approved algorithms:

Table 3: Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
819	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	
		CFB8 [38A]	Tested, not used	
		OFB [38A]	Key Sizes: 256	
1297	AES [197]	CFB8 [38A]	Key Sizes: 256	Encrypt, Decrypt
VA	AES MAC [IG G.13]	AES MAC for Project 25 APCO OTAR (Cert. #819)		Message Authentication
VA	CKG [IG D.12]	[133] Section 7.1 Direct symmetric key generation using unmodified DRBG output		Key Generation
505	DRBG [90A]	AES-CTR	Strength: 256 bits	Random Number Generation
N/A	KTS [38F]	AES, RSA	AES Cert. #819 and RSA Cert. #396	Key establishment methodology provides 112 bits of encryption strength
396	RSA [186]	PKCS1.5	RSA-2048 SHA(256)	SigVer
817	SHS [180]	SHA-256		Message Digest Generation, Password Obfuscation

- AES-256 8-bit CFB (Cert. #1297) – used for symmetric encryption/ decryption of keys and parameters stored in the internal database
- AES-256 OFB (Cert. #819) – for symmetric encryption/decryption of keys
- AES-256 ECB (Cert. #819) – used for inner layer encryption

- AES-256 CBC (Cert. #819) – for firmware upgrades and OTAR
- AES MAC (AES Cert. #819, vendor affirmed; P25 AES OTAR)
- KTS (AES Cert. #819 and RSA Cert. #396)
- RSA-2048 (Cert. #396) – used for digital signature verification during firmware integrity test and firmware load test
- SHA-256 (Cert. #817) – used for digital signature verification during firmware integrity test and firmware load test. Used for password hashing for internal password storage.
- SP800-90A CTR-DRBG (Cert. #505) – used for IV and pseudo-random number generation.
- SP 800-133 CKG (vendor affirmed) – symmetric keys are the direct result of DRBG output.

3. The module supports the following non-FIPS Approved algorithms, allowed in FIPS Approved mode:
    - AES (AES Cert. #819, key unwrapping))
    - Non-deterministic Hardware Random Number Generator – used to provide seeds for the FIPS approved RNG; provides at least 384 bits of entropy for seeding the DRBG.

3.2. Non Approved Mode of Operation

A non-FIPS Approved mode of operation is transitioned to when any or all of the following conditions are met:

1. Red Keyfill is enabled.
2. Non-Approved algorithms are used.

The module supports the following non-Approved algorithm if loaded:

- DES-OFB - Used for symmetric encryption / decryption of data traffic/keys for APCO OTAR.

4. Security Rules

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

1. The ASTRO CDEM MACE inhibits all data output via the data output interface whenever an error state exists and during self-tests.
2. The ASTRO CDEM MACE logically disconnects the output data path from the circuitry and processes when performing key generation, or key zeroization.
3. Authentication data (e.g. passwords) are entered in encrypted form. Authentication data is not output during entry.
4. The ASTRO CDEM MACE does not support manual key entry.
5. Secret cryptographic keys are entered in encrypted form over a physically separate port.
6. The ASTRO CDEM MACE protects secret keys and private keys from unauthorized disclosure, modification, and substitution.
7. The module does not support the output of plaintext or encrypted secret keys.
8. The module does not support bypass.
9. The ASTRO CDEM MACE enforces Identity-Based authentication. Similarly, the authentication data is not output during entry.
10. The ASTRO CDEM MACE supports a User role, Cryptographic Officer, and a KVL role. Authenticated operators are authorized to assume either supported role. The module does not allow the operator to change roles.
11. The ASTRO CDEM MACE re-authenticates an operator when it is powered-up after being powered-off.
12. The ASTRO CDEM MACE implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
13. The ASTRO CDEM MACE provides a means to ensure that a key entered into or stored within the ASTRO CDEM MACE is associated with the correct entities to which the key is assigned. Each key in the ASTRO CDEM MACE is entered encrypted and stored with the following information:
    - Key Identifier – 16 bit identifier
    - Algorithm Identifier – 8 bit identifier
    - Key Type – Traffic Encryption Key or Key Encryption Key
    - Physical ID, Common Key Reference (CKR) number, and Keyset number – Identifiers indicating storage locations.

    Along with the encrypted key data, this information is stored in a key record that includes a CRC over all fields to protect against data corruption.
14. The ASTRO CDEM MACE uses RSA-2048 to prevent brute-force attacks on the digital signature used to verify firmware integrity during a Program Update. As the Program Update service requires more than one minute to complete the random attempt success rate during a one minute period cannot be lowered to less than 1 in 100,000.
15. The ASTRO CDEM MACE denies access to plaintext secret keys contained within the ASTRO CDEM MACE.
16. The ASTRO CDEM MACE provides the capability to zeroize all plaintext

cryptographic keys and other unprotected critical security parameters within the module.

17. The ASTRO CDEM MACE will zeroize all keys from the Key Database after the configured max number of consecutive unsuccessful login attempts is reached. The default max is 15.
18. The ASTRO CDEM MACE conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.
19. The ASTRO CDEM MACE performs the following self-tests. Powering the module off then on or resetting the module using the Reset service will initiate the power up self-tests.
    - Power up and on-demand tests:
        - Cryptographic algorithm test: A cryptographic algorithm test using a known answer is conducted for all cryptographic functions (e.g., encryption, decryption, authentication, random number generation, and hashing) for each. The test passes if the final data matches the known data, otherwise it fails. This test is done for the following algorithms:
            - AES-256 (ECB, CBC, and OFB modes) encrypt KATs (Cert. #819)
            - AES-256 (ECB, CBC, and OFB modes) decrypt KATs (Cert. #819)
            - AES-256 CFB8 encrypt KAT (Cert. #1297)
            - AES-256 CFB8 decrypt KAT (Cert. #1297)
            - SHA-256 KAT
            - SP800-90A DRBG KAT
            - SP 800-90A Section 11.3 Health Tests
            - RSA-2048 (verification) KAT
        - Firmware integrity test: A digital signature is generated over the code when it is built using SHA-256 and RSA-2048 and is stored with the code upon download into the module. When the module is powered up the digital signature is verified. If the digital signature matches the test passes, otherwise it fails.
        - DRBG KAT test: the DRBG is initialized with a known, predetermined seed value. The DRBG is run and the result compared to known answer data. The test passes if the generated data matches the known answer data, otherwise the test fails.
        - Critical Function Test: upon every power up, the MACE will assert and de-assert each signal connected to an external indicator, so that the User may verify that the indicators are functioning and controlled by the MACE.
    - Conditional tests:
        - Firmware load test: A digital signature is generated over the code when it is built using SHA-256 and RSA-2048. Upon download into the module, the digital signature is verified. If the digital signature matches the test passes, otherwise it fails.
        - Continuous Random Number Generator test: The continuous random number generator test is performed on all RNGs supported by the module (SP800-90A DRBG, NDRNG). For each RNG, an initial value is generated and stored. This value is not used for anything other than comparison data.

A successive call to any one of the RNGs generates a new set of data, which is compared to the comparison data. If a match is detected, this test fails; otherwise the new data is stored as the comparison data and returned to the caller.

20. The ASTRO CDEM MACE enters the Critical Error state if the Cryptographic Algorithm Test, Critical Functions Test, or Continuous Random Number Generator Test fails. An error indicator is output by turning the Alarm LED red while in the Critical Error state. The Critical Error state may be entered by powering the module off then on.
21. The ASTRO CDEM MACE enters the Programming Error
22. state if the Firmware Integrity test or Firmware Load test fails. As soon as an error indicator is output via the status interface, the module transitions from the error state to a state that only allows new firmware to be loaded. An operator shall send the module to the Motorola service center for recovery if this state is reached.
23. The ASTRO CDEM MACE outputs an error indicator by turning the Alarm LED output red whenever an error state is entered due to a failed self-test. If all power up self-tests pass, the Alarm LED output will be clear.
24. The ASTRO CDEM MACE does not perform any cryptographic functions while in the Critical Error state.
25. The ASTRO CDEM MACE does not support multiple concurrent operators.
26. Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

5. Identification and Authentication Policy

The ASTRO CDEM MACE supports a User role, a Crypto-Officer role, and a KVL role. The identification, and authentication policy for each of these roles is detailed in the table below:

The Crypto-Officer and User roles are authenticated with passwords. The Crypto-Officer and User passwords are initialized to a default value during manufacturing and are sent in encrypted form to the module for authentication. After authenticating, the Crypto-Officer and User passwords may be changed at any time.

Table 4: Roles and Authentication Mechanisms

Role	Authentication Type	Authentication Mechanism	Strength of Authentication
Crypto-Officer	Identity-Based	Identity: a 4-byte identifier is used to identify the identity and role. The ASTRO CDEM MACE supports a single identity. Crypto-Officer Password: a password that is a minimum of 14-16 ASCII (printable) characters password is authenticated to gain access to all Crypto-Officer services. It should be noted that after authenticating, this password may be changed at any time.	Since the minimum password length is 14 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in 95 ^ 14 or 1 in 4,876,749,791,155,298,590,087,890,625. The module limits the number of authentication attempts to in one minute to 10. The probability of a successful random attempt during a one-minute period is 10 in 95 ^ 14 or 1 in 2.050546e+27
User	Identity-Based	Identity: a 4-byte identifier is used to identify the identity and role. The ASTRO CDEM MACE supports a single identity. User Password: a 10 hexadecimal digit (5 bytes) long password is authenticated to gain access to all User services. It should be noted that after authenticating, this password may be changed at any time.	Since the minimum password length is 5 bytes long printable characters and there are 40 bits, the probability of a successful random attempt is 1 in 2 ^40 or 1 in 1,099,511,627,776. The module limits the number of authentication attempts in one minute to 15. The probability of a successful random attempt during a one-minute period is 15 in 2 ^40 or 1 in 1.364242e+11.
KVL	Identity-Based	Identity: a 1-byte identifier is used to identify the identity and role. The ASTRO CDEM MACE supports a single identity.	The probability of a successful random attempt is 1 in 2 ^ 256.

Role	Authentication Type	Authentication Mechanism	Strength of Authentication
KVL	Identity-Based	BKK: a 256-bit AES key is authenticated to gain access to the services performed over the KVL interface. This CSP is used as the method of authentication in the following KVL-centric services: • "Configure Module via KVL Interface" • "Zeroize Keys via KVL Interface" • "Store & Forward"	The maximum number of authentication attempts that can be performed over the KVL interface with the BKK in one minute is 745. Therefore, the probability of a successful random attempt during a one-minute period is 745 in 2 ^ 256 or 1 in 1.55425e+74.

6. Physical Security Policy

The ASTRO CDEM MACE is a production grade, single-chip cryptographic module as defined by FIPS 140-2 and is designed to meet Level 3 physical security requirements.

The ASTRO CDEM MACE is covered with a hard opaque epoxy coating that provides evidence of attempts to tamper with the module. Tampering with the module will cause it to enter a lock-up state in which no crypto services will be available. The ASTRO CDEM MACE does not contain any doors, removable covers, or ventilation holes or slits. No maintenance access interface is available.

Note: Motorola Solutions did not provide operating and storage temperature ranges to the test lab, so module hardness testing was only performed at ambient temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.

7. Access Control Policy

The module supports the following roles and services. Note that these roles and services are the same in both the non-Approved and Approved modes, the only difference is non-Approved algorithms / key establishment is available when using the services listed below in the non-Approved mode.

7.1. ASTRO CDEM MACE Supported Roles

The ASTRO CDEM MACE supports the following roles:

- User Role
- Crypto-Officer Role
- KVL Role

7.2. ASTRO CDEM MACE Services Available to the Crypto-Officer Role

- Program Update: Update the module firmware via the KVL interface. Firmware upgrades are verified using a digital signature. The following points should be noted regarding the Program Update
    - The Program Update image is AES-256 encrypted
    - The Program Update image is RSA-2048 signed
    - Keys/CSPs stored in non-volatile memory/storage are normally preserved during a Program Update. However all keys /CSPs are zeroized during a Program Update if one or more of the following occurs:
        - The key database format/version changes between the resident and upgrade software images
        - The module's FIPS status changes, post-upgrade (this indicates that a non-FIPS compliant algorithm has been loaded onto the module)
- Validate Crypto-Officer Password: Validate the role's current password via the RS232 interface. Successful authentication will allow entry/access to the RS232 shell command services. Ten consecutive failed validation attempts will cause the KPK to be zeroized, a new KPK to be generated, and the TEKs and KEKs to be invalidated (key status is marked invalid). The password shall be reset to the default.
- Change Crypto-Officer Password: Modify the current password used to identify and authenticate this role via an RS232 shell command.
- Logout Crypto-Officer: Exits the RS232 shell command interface and logs out of the Crypto-Officer role.

- Configure Module:
    - Set configuration to toggle between FIPS 140-2 Level 3, or the non-FIPS compliant mode. Toggling this option causes the KPK to be zeroized, a new KPK to be generated, the TEKs and KEKs to be invalidated (key status is marked invalid), and the module to enter an error state that can only be cleared by power cycling the module.
    - Set configuration parameters used for the network functionality via an RS232 shell command.
- Extract Action Log: Status request via an RS232 shell command. Provides detailed history of error events.
- Version Query: Provides module firmware and hardware version numbers via an RS232 shell command.
- Red Keyfill (Fips): Shell command that is used to enable/disable the ability to perform unencrypted keyload operations. This command allows for the reporting out of the rs232 shell whether operating in FIPS 140-2 Level 3 mode or not. Toggling this option causes the KPK to be zeroized, a new KPK to be generated, the TEKs and KEKs to be invalidated (key status is marked invalid), and the module to enter an error state that can only be cleared by power cycling the module.
- RS232 Shell Help: Shell command to get help on the format of other RS232 shell commands.
- Exit RS232 Shell: Exits the RS232 shell command interface and logs out of the Crypto-Officer role.

7.3. ASTRO CDEM MACE Services Available to the User Role

- Decrypt: Decrypt ciphertext data received over the Ethernet and send plaintext back.
- Encrypt: Encrypt plaintext data received over the Ethernet port and send ciphertext back.
- Validate User Password: Validate the current User password used to identify and authenticate the User role via the SSI interface. Ten consecutive failed validation attempts will cause the KPK to be zeroized, a new KPK to be generated, and the TEKs and KEKs to be invalidated (key status is marked invalid). The password shall be reset to the default.
- OTAR: Decrypt KEKs and TEKs.

7.4. ASTRO CDEM MACE MACE Services Available to the KVL Role

- Configure Module via KVL Interface: Perform configuration of the module (e.g., OTAR configuration) via the KVL interface.
- Store & Forward: Modify and query the KEKs and TEKs stored internally via the KVL interface.
- Transfer Key Variable: Transfer key variables (TEKs and KEKs) to the MACE key database via the KVL interface.
- Delete Key Variable: Zeroize KEKs and TEKs via the KVL interface.
- Key Check: Obtain status information about a specific TEK or KEK via the KVL interface.
- Version Query via KVL Interface: Provides module firmware version numbers via the KVL UI.
- Algorithm List Query: Provides module algorithm list via the KVL UI.

7.5. ASTRO CDEM MACE Services Available Without a Role

- Perform Self-Tests: Performs module self-tests comprised of cryptographic algorithms test and firmware test. Initiated by module reset or transition from power off state to power on state.
- Reset Crypto Module: Toggle the Reset input or a transition from power off to power on state.
- Erase Crypto Module: Zeroizes the TEK, KEK, and KPK, via the Tamper interface.

7.6. Critical Security Parameters (CSPs) and Public Key

Table 5: CSP Definition

CSP Identifier	Description
SP800-90A Seed	This is a 384-bit seed value used within the SP800-90A DRBG. The seed is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The seed is not entered into or output from the module. Entry - n/a Output - n/a Storage – in plaintext in volatile memory Zeroization - on power off Generation - Non-deterministic Hardware Random Number Generator
SP800-90A Internal State (“V” and “Key”)	This is the internal state of the SP800-90A DRBG during initialization. The internal state is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The internal state is not entered into or output from the module. Entry - n/a Output - n/a Storage – in plaintext in volatile memory Zeroization - on power off Generation - Internal to the SP800-90A DRBG
Key Protection Key (KPK)	This is a 256-bit AES-CFB8 key used to encrypt all other keys besides the PEK, BKK and the IDK stored in non-volatile memory. Generated internally using the SP800-90A DRBG. Stored in plaintext in non-volatile memory. The KPK is not entered into or output from the module. Entry - n/a Output - n/a Storage – stored in plaintext in non-volatile memory Zeroization - Program Update, Validate Crypto-Officer Password, Change Crypto-Officer Password, Configure Module, Red Keyfill (Fips), Validate User Password, Delete Key Variable, or Erase Crypto Module services Generation - SP800-90A DRBG
Black Keyloading Key (BKK)	256-bit AES-OFB Key used for decrypting keys entered into the module via a KVL. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The BKK is entered using the Program Update service and is not output from the module.
Image Decryption Key (IDK)	A 256-bit AES-CBC key used to decrypt downloaded images. The IDK is not output from the module. Entry - on Program Update service request Output - n/a Storage - in plaintext in non-volatile memory Zeroization - on Program Update service request Generation - n/a

CSP Identifier	Description
Traffic Encryption Keys (TEKs)	TEKs are AES-OFB keys entered encrypted (AES Key Wrapping) over the Ethernet interface. The TEKS are stored encrypted with the KPK (AES256-CFB8) in non-volatile memory. TEKs are stored in plaintext in RAM only as long as needed. Entry – input encrypted with AES Key Wrap over the Ethernet Interface Output – N/A Storage – stored encrypted with the KPK with AES256-CFB8 in non-volatile memory Zeroization – on Delete Key Variable, Erase Crypto Module, Store and Forward and Program Update service requests
Key Encryption Keys (KEKs)	256-bit AES-KW or AES-OFB Keys used for encryption of keys in OTAR. Entry - KEKs are entered in encrypted form via the KVL and via OTAR. KEKs entered via the KVL are wrapped with the BKK; KEKs received via OTAR are encrypted with another KEK. Output - N/A Storage - in plaintext in RAM and encrypted by the KPK in flash. Zeroization - via the Erase Crypto Module, Delete Key Variable, Program Update service, and Store and Forward services.
User Password	A 10-digit hexadecimal value used to authenticate the User role. The User Password is entered encrypted by the PEK (AES256-CFB8). The User Password is not stored in the module or output from the module. Entry – entered encrypted by the PEK with AES256-CFB8 Output – n/a Storage – a hash of the User Password is stored in non-volatile memory Zeroization – on Program Update service request and Validated User Password Generation – n/a
Crypto-Officer Password	The Crypto Officer password is entered encrypted on the PEK (AES256-CFB8). After decryption the plaintext password is not stored but temporarily exists in volatile memory. The SHA-256 hash value of the plaintext password is stored encrypted by the PEK in non-volatile memory. The SHA-256 hash of the decrypted password is compared with the SHA-256 hash value stored in non-volatile memory during password validation. Entry – entered encrypted by the PEK with AES256-CFB8 Output – n/a Storage – SHA-256 hash of the plaintext password is stored in non-volatile memory Zeroization – on Program Update service request, Validate Crypto – Officer Password, Change Crypto-Officer password Generation – n/a

CSP Identifier	Description
Password Encryption Key (PEK)	This is a 256-bit AES-CFB8 Key used for decrypting passwords during password validation. Loaded via the Program Update service. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. Also stored encrypted on the KPK in non-volatile memory. The PEK is not output from the module. Entry – on Program Update service request Output – n/a Storage – in plaintext in non-volatile memory; encrypted on the KPK in non-volatile memory Zeroization – on Program Update service request Generation – n/a

Table 6: Public Keys

Public Keys	Description
Public Programmed Signature Key	A 2048-bit RSA public key used to validate the signature of the firmware image being loaded before it is allowed to be executed. Stored in non-volatile memory. Loaded during manufacturing and as part of the boot image during a Program Update service. The Public Programmed Signature Key is not output from the module. Entry - on Program Update service request Output - n/a Storage - in plaintext in non-volatile memory Zeroization - on Program Update service request Generation - n/a

7.7. CSP Access Types

Table 7: CSP Access Types

CSP Access Type	Description
C – Check CSP	Checks status of the CSP.
D – Decrypt CSP	Decrypts entered KEKs and TEKs using the BKK during CSP entry over the KVL interface. Decrypts KEKs and TEKs entered via OTAR using a KEK. Decrypts entered passwords using the PEK during entry over the serial interface.
E – Encrypt CSP	Encrypts KEKs and TEKs prior to output over the Ethernet or KVL interface using another KEK.
G – Generate CSP	Generates KPK, SP800-90A seed, or SP800-90A internal state.
I – Invalidate CSP	Marks encrypted KEKs and TEKs stored in volatile memory as invalid. KEKs and TEKs marked invalid can then be over-written when new KEKs and/or TEKs are stored.
S – Store CSP	Stores KPK in non-volatile and volatile memory. Stores encrypted KEKs and TEKs in non-volatile memory, over-writing any previously invalidated KEK or TEK in that location. Stores plaintext BKK, PEK, or IDK in non-volatile memory. Stores Hash of the User and Crypto-Officer password in non-volatile memory (encrypted on PEK).
U – Use CSP	Uses CSP internally for encryption / decryption services.
Z – Zeroize CSP	Zeroizes CSP.

Table 8 – CSP Service Descriptions

Service	CSP											Role		
	SP800-90A seed	SP800-90A seed internal state	PEK	TEKs	KEKs	KPK	BKK	IDK	User Password	Crypto-Officer Password	User Role	Crypto-Officer Role	KVL Role	No Role Required
Program Update			z,s	z	z	z	z, s	u, z, s	z	z		√		
Validate Crypto-Officer Password			u	i	i	z, g, s				d, u, z		√		
Change Crypto-Officer Password			u	i	i	z, g, s				d, u, z,s		√		
Logout Crypto-Officer Role												√		
Configure Module				i	i	z, g						√		
Extract Action Log												√		
Version Query (serial console)												√		
Red Keyfill (Fips)						g, z						√		
RS232 Shell Help												√		
Exit RS232 Shell											√	√		
Encrypt				d,u		u					√			
Decrypt				d,u		u					√			
Validate User Password			u	i	i	z, g, s			d, u, z		√			
OTAR				d, u, i, e, z, s	d, u, i, e, z, s						√			
Configure Module via KVL Interface							u						√	
Store & Forward				d, u, i, e, z, s	d, u, i, e, z, s	u	u						√	
Transfer Key Variable				d, i, e, s	d, i, e, s	u	u						√	
Delete Key Variable				i, z	i, z	z	u						√	
Key Check				c	c		u						√	
Version Query via KVL interface							u						√	
Algorithm List Query							u						√	
Perform Self-Tests														√
Reset Crypto Module	g,u	g,u,z		i	i	g, s								√
Erase Crypto Module	g, u	g, u, z		i	i	g, s								√

8. Mitigation of Other Attacks Policy

The ASTRO CDEM MACE 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.