Non-Proprietary FIPS 140-2 Security Policy:

Astro Subscriber Motorola Advanced Crypto Engine (MACE) – Security Level 2

The MACE is used in multiple Motorola Solutions, Inc. subscribers. Visit the Motorola Solutions, Inc. website to verify your subscriber has this module by viewing the subscriber specifications sheet.

Document Version: 1.1

Date: May 24, 2021

Table of Contents

List of Tables

List of Figures

1 Introduction

This document defines the Security Policy for the Astro Subscriber Motorola Advanced Crypto Engine (MACE) – Security Level 2, hereafter denoted the MACE. The MACE is implemented as a single-chip cryptographic module to the Physical Security requirements as defined by FIPS 140-2 and embedded in the Motorola Solutions subscribers. The MACE provides secure key management, Over-the-Air-Rekeying (OTAR), and voice and data encryption for multiple Motorola Solutions subscribers. Visit the Motorola Solutions website to verify your subscriber has this cryptographic module by viewing the subscriber specifications sheet.

Table 1 – Cryptographic Module Configuration

Module	HW P/N	Base FW Version
Astro Subscriber Motorola Advanced Crypto Engine (MACE)	5185912Y03, 5185912Y05, 5185912T05	R01.11.00

The MACE supports the following FIPS Approved algorithms which may be installed separately from the MACE 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 2 – Approved Mode Algorithms Firmware Version

Approved Algorithm	Cert. #	Part Number	Algorithm FW Version
AES256 (ECB, CBC, OFB, CFB)	819	5185912 Family	R01.00.00
AES256 (GCM)	1295	5185912 Family	R02.00.00

Table 3 – Non-Approved Mode Drop-in Algorithms

Algorithm	Algorithm FW Version
ADP	R01.00.00
DES-XL	R01.00.00
DES (ECB, OFB, and CBC)	R01.00.00
DVI-XL	R01.00.00
DVP-XL	R01.00.00

The MACE is intended for use by the markets that require FIPS 140-2 validated overall security level 2.

The MACE was previously FIPS 140-2 validated with the following FW versions:

Table 4 – Historical FIPS 140-2 Validation Status

CMVP Cert#	FW Version
2460, 2461	R01.07.25
2358, 2414	R01.05.12
1751, 1752	R07.11.10, R07.11.11, R01.03.13, R07.11.12, R01.04.07
1535, 1536	R01.02.00, R01.02.01, R01.02.02

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

Table 5 – Security Level of Security Requirements

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

1.1 Module Description and Cryptographic Boundary

The cryptographic boundary of the MACE is drawn around the perimeter of the MACE IC as shown in Figure 3 below.

Figure 1: MACE Chip (Top)

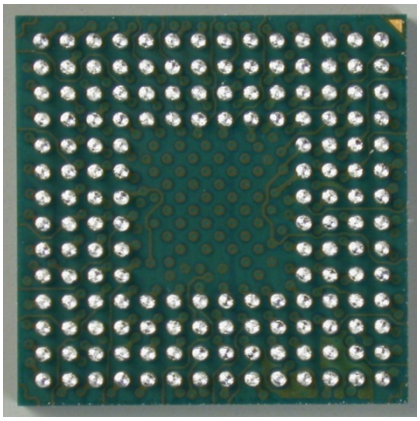

Figure 2: MACE Chip (Interfaces)

The MACE IC has an SSI port, a KVL port when connected to the Motorola Key Variable Loader (KVL), Self-Test Indicator Interface, and Power Connections.

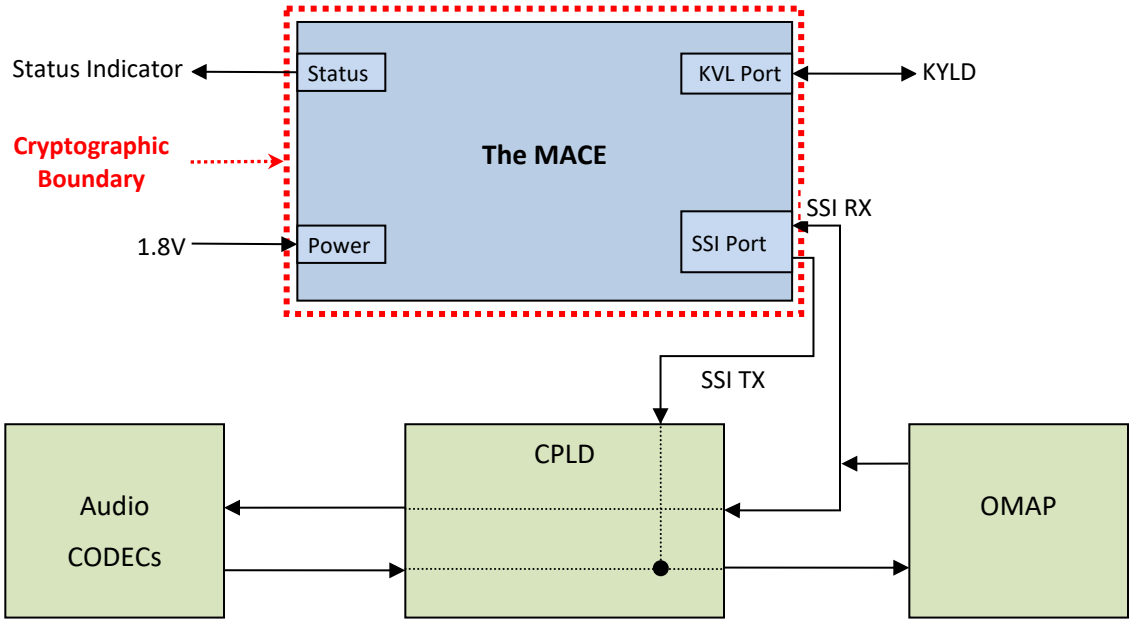

Figure 3: Cryptographic Boundary

The MACE's ports and associated FIPS defined logical interface categories are listed in Table 6.

Table 6 – Ports and Interfaces

Port	Description	Logical Interface Type
Serial Synchronous Interface (SSI)	The main physical port provided by the MACE. It provides access to the majority of the supported interfaces.	Data Input Data Output Control Input Status Output
Key Variable Loader (KVL)	This interface provides the input and output to a Key Variable Loader (KVL).	Data Input Control Input Status Output
Power	This interface powers all circuitry.	Power Input
Self-test Indicator	This interface provides status output to indicate all power-up self-tests completed successfully.	Status Output

2 Modes of Operation

The MACE must be configured to operate in either an approved or non-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 a FIPS compliant mode. Documented below are the additional configuration settings that are required for the MACE to be used in a FIPS 140-2 Approved mode of operation at overall Security Level 2. At any given time, the Module Status service can be used to determine whether the MACE is operating at overall Security Level 2 or in a non-FIPS Approved mode. The FIPS Approved mode indicator will display "303B020002".

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

2.1 Approved Mode Configuration

In order to configure the MACE into an Approved mode, the Module Configuration service must be used to ensure Red Keyloading is enabled and the following parameters are disabled.

1. Motorola Data Communication Over The Air Rekeying (MDC OTAR)
2. Key Loss Key (KLK) generation
3. Infinite UKEK Retention

Additionally, the MACE supports "drop-in algorithms" via the Program Update service. Drop-in algorithms may be added or removed from the MACE independent of the base FW. In order to remain in the Approved mode, only Approved and Allowed algorithms should be used; in particular AES-256 (Cert #819 and #1295).

3 Cryptographic Functionality

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

Table 7 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
819	AES [197]	CFB8 [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
		ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
1295	AES [197]	GCM [38D]*	Key Sizes: 256	Encrypt, Decrypt
A654	AES [197]	KW [38F]	Forward Key Sizes: 256	Authenticated Encrypt, Authenticated Decrypt
C1444	AES [197]	KW [38F]	Forward Key Sizes: 256	Authenticated Decrypt
VA	CKG [IG D.12]	[133] Section 6.1 Direct symmetric key generation using unmodified DRBG output		Key Generation
A656	CVL	ECC CDH	P-384	Shared Secret Computation
505	DRBG [90A]	CTR	AES-256	Deterministic Random Bit Generation
A655	ECDSA [186-4]		P-384	KeyGen
1796	HMAC [198]	SHA-384	Key Sizes: 32 bytes λ = *48 bytes*	Message Authentication
VA	KAS-SSC [56Ar3]	ECC (Initiator, Responder), KPG, Partial	P-384 SHA-384	Key Agreement Scheme Key establishment methodology provides 192 bits of encryption strength
VA	KDA [56Cr1] (§4.1)	SP 800-56Cr1 Section 4.1, Option 1 with SHA-384		Key Derivation
N/A	KTS [38F]	KW	AES CBC Cert. #819, RSA Cert. #396 (unwrapping only)	Key establishment methodology provides 256 bits strength
N/A	KTS [38F]	KW	AES CBC Cert. #C1444 (unwrapping only)	Key establishment methodology provides 256 bits strength
396	RSA [186-2]	PKCS1_v1.5	2048	SigVer
817	SHS [180]	SHA-256		Message Digest Generation, Password Obfuscation
2399	SHS [180]	SHA-384		Message Digest Generation

* Per IG A.5 Scenario 2, the MACE generates GCM IVs randomly as specified in SP800-38D section 8.2.2 using approved DRBG (Cert #505).

Table 8 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES MAC	[IG G.13] AES Cert. #819, vendor affirmed; P25 AES OTAR
NDRNG	[IG G.13] Non-Deterministic RNG used for seeding the DRBG with 256-bits of security strength; 32 bits per access.

Non-Approved Cryptographic Functions for use in non-FIPS mode only:

- ADP
- DES-XL
- DES (ECB, CBC, OFB)
- DVI-XL
- DVP-XL

Note that all the above are “drop-in” algorithms.

3.1 Critical Security Parameters

All CSPs used by the MACE are described in this section. Usage of these CSPs by the MACE (including all CSP lifecycle states) is described in the services detailed in Section 4. It should be noted that keys/CSPs stored in non-volatile memory are normally preserved during a Program Update. However, all keys/CSPs are zeroized during a Program Update if the MACE’s FIPS status changes, post-upgrade (this indicates that a non-FIPS compliant Drop-in algorithm has been loaded onto the MACE)

Table 9 – Critical Security Parameters (CSPs)

CSP	Description / Usage
DRBG Seed/Input String	A 384-bit is used in seeding of the CTR_DRBG during DRBG instantiation at power-up. Stored in plaintext in the volatile memory, and zeroized by power cycling. It is not entered into or output from the MACE. Internally generated using NDRNG.
DRBG Internal State (V and Key)	Internal state of SP800-90A CTR_DRBG (V and Key). Stored in plaintext in the volatile memory, and zeroized by power cycling. It is not entered into or output from the MACE, generated through SP800-90A CTR_DRBG state modification.
Image Decryption Key (IDK)	A 256-bit AES-CBC key used to decrypt downloaded images. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The IDK is entered using the Program Update service and is not output from the MACE.
Black Keyloading Key (BKK)	Not used in the Level 2 configuration. At Level 3, a 256-bit AES-OFB key used for decrypting keys entered into the MACE 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 MACE.

CSP	Description / Usage
UKKPK (Universal Key for Key Protection Key)	A 256-bit AES Key used for encrypting the KPK. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The UKKPK is entered using the Program Update service and is not output from the MACE.
PKPK (Private Key Protection Key)	A 256-bit AES Key used to encrypt ECDH generated private key. Stored AES256 AES KW (SP 800-38F) encrypted by the BKK, and zeroized through the Program Update, Zeroize all keys and password services. The PKPK is generated internally using SP 800-90A DRBG and is not output from the MACE.
Key Protection Key (KPK)	A 256-bit AES key used to encrypt the KEK/TEK. Stored in plaintext in non-volatile memory and zeroized through the Program Update, Zeroize all keys and password, Validate password, Change password, and Module Configuration services. The KPK is generated internally using SP 800-90A DRBG and is not output from the MACE.
Key Encryption Keys (KEKs)	A 256-bit AES-KW Keys used for decrypting keys in APCO OTAR. Stored encrypted by the KPK (AES256-CFB8) in non-volatile memory, and plaintext in the volatile memory only as long as needed. Entered through Import Keys, APCO OTAR, and Key Agreement Process services. KEKs are not output from the MACE. Zeroize/Invalidate through Program Update, Zeroize Keys, Zeroize all keys and password, Transfer Key Variable, OTAR, Module Configuration, Validate Password, Change Password services.
Traffic Encryption Keys (TEKs)	A 256-bit AES-KW key used for voice/data encryption/decryption, and OTAR key decryption. Stored encrypted by the KPK (AES256-CFB8) in non-volatile memory, and plaintext in the volatile memory only as long as needed. Entered through the KVL or APCO OTAR. TEKs are not output from the MACE. Zeroize/Invalidate through Program Update, Zeroize Keys, Zeroize all keys and password, Transfer Key Variable, OTAR, Module Configuration, Validate Password, Change Password services.
Password Encryption Key (PEK)	A 256-bit AES key used for decrypting password during password validation. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The PEK is entered using the Program Update service and is not output from the MACE.
Password	The 10-digit password is entered encrypted by the PEK. After decryption the plaintext password is not stored but temporarily exists in volatile memory. The SHA-256 hash of the decrypted password is compared with the hash value stored in non-volatile memory during password validation. The password is not output from the MACE. Zeroized through the Program Update, Change Password, Validate Password, and Module Configuration services.
ECDH Private Key	The Elliptic Curve (P-384) Diffie-Hellman private key used for establishing a shared secret over an insecure channel. Stored AES256 AES KW (SP 800-38F) encrypted by the PKPK, and zeroized through the Program Update, Zeroize all keys and password services. The key is generated internally using SP 800-90A DRBG and is not output from the MACE.
ECDH Shared Secret Key	The Elliptic Curve (P-384) Diffie-Hellman Shared Secret is established as part of the Diffie-Hellman key agreement scheme. Stored plaintext in the volatile memory while in use, and zeroized through power-cycle. The key is not output from the MACE.

3.2 Public Keys

Table 10 – Public Keys

Key	Description / Usage
RSA Programmed Signature Key	2048-bit RSA key used to validate the signature of the firmware image at power-on and during the FW Load test before it is allowed to be executed and is also used for authentication of the Crypto-Officer role and to support KTS in conjunction with AES CBC. Loaded during manufacturing and is not output from the MACE.
ECDH Public Key	The Elliptic Curve (P-384) Diffie-Hellman public key used for establishing a shared secret over an insecure channel. Stored plaintext in the non-volatile memory, and zeroized through the Program Update, Zeroize all keys and password services. The key is output from the MACE in plaintext.
ECDH Remote Party Public Key	The Elliptic Curve (P-384) Diffie-Hellman remote party public key used for establishing a shared secret over an insecure channel. Stored plaintext in the volatile memory while in-use, and zeroized through power-cycle. The key is entered into the MACE in plaintext.

4 Roles, Authentication and Services

4.1 Assumption of Roles

The MACE supports two distinct operator roles (User and Crypto-Officer). The MACE uses a 10-digit password to authenticate the User and an RSA-2048 digital signature to authenticate the Crypto-Officer. The role of the operator is specified by selecting which physical port will be used to authenticate and access module services.

Table 11 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer Role	Identity-based	RSA-2048 digital signature for Program Update service
User	User Role	Identity-based	10-digit hexadecimal number

4.2 Authentication Methods

RSA-2048 Digital Signature Authentication

The MACE uses RSA-2048 to prevent brute-force attacks on the digital signature used to verify firmware integrity during a Program Update. The probability of a successful random attempt is 1 in 2^{112} which is less than 1 in 1,000,000.

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.

Password Authentication

Since the password length is 10-digit hexadecimal number and there are 16 hexadecimal digits, the probability of a successful random attempt is 1 in 16^{10} which is less than 1 in 1,000,000.

The MACE limits the number of 15 consecutive failed authentication attempts. 15 consecutive failed authentication attempts cause all TEKs and KEKs to be invalidated and the password to be reset to the factory default. The worst-case probability of a successful random attempt within a one-minute period is $15/16^{10}$, which is less than 1 in 100,000.

Table 12 – Authentication Description

Authentication Method	Probability	Probability over a One-Minute Period
RSA-2048 Digital Signature	$1/2^{112}$	$1/2^{112}$
Password	$1/16^{10}$	$15/16^{10}$

4.3 Services

All services implemented by the MACE are listed in the tables below. Note that all services listed in Table 13 and Table 14 below are available in both the FIPS Approved and non-Approved mode. The only distinguishing factor between Approved and non-Approved services is whether non-Approved algorithms are available.

Table 13 – Authenticated Services

Service	Description	CO	User
Program Update	Update the 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.	X	
Import keys	Imports keys to the MACE via a Key Variable Loader (KVL). If the Red Keyloading configuration parameter is enabled, then keys will be transferred from the KVL in plaintext. If Red Keyloading is disabled (only available in the Level 3 configuration), all keys transferred from the KVL will be AES-OFB encrypted by the BKK.		X
Privileged APCO OTAR	Import, modify and query the keys.		X

Service	Description	CO	User
Change Active Keyset	The active keyset is used to store a group of keys for current use while inactive keysets are used to store keys for future use. This service modifies the currently active keyset used for selecting keys for encryption / decryption services.		X
Change Password	Modify the current password used to identify and authenticate the User role.		X
Encrypt	Encrypt digital voice or data.		X
Decrypt	Decrypt digital voice or data.		X
Zeroize Keys	Zeroize selected keys variables from the MACE.		X
Key/Keyset Check	Obtain status information about a specific key/keyset.		X
Generate Signature	Generate HMAC SHA 384 signature.		X
Key Agreement Process	Perform a key agreement process to create an ECDH Shared Secret, and ECDH Public and Private Keys in volatile memory.		X

Table 14 – Unauthenticated Services

Service	Description
Module Status	Provides firmware version, current FIPS status about whether the MACE is operating at overall Security Level 2, or in a non-Approved mode of operation.
Self-Tests	Performs 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.
Validate Password	Validate the current password used to identify and authenticate the User role.
Zeroize all keys and password	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. Allows user to gain controlled access to the module if the password is forgotten. The MACE can be reinitialized using a Key Variable Loader.
Non-Privileged APCO OTAR	Hello and Capabilities Key Management Messages may be performed without a role.
Reset	Reset/power cycle the MACE.
Shutdown	Prepares the MACE for removal of power.
Extract Error Log	Provides detailed history of error events.
Clear Error Log	Clears history of error events.
Module Configuration	Download configuration parameters used to specify module behavior.

Table 15 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- R = Read: The service reads the CSP.
- W = Write: The service writes to the CSP.
- X = Execute: The service uses the CSP for a cryptographic operation.
- G = Generate: The service generates to the CSP.
- Z = Zeroize: The service zeroizes to the CSP.
- – = No access: The service does not access the CSP.

Table 15 – Security Parameters Access by Service

Service	CSPs and Public Keys															
	DRBG Seed	DRBG Internal state (V and Key)	IDK	BKK	UKKPK	PEK	KPK	KEK	TEK	Password	PKPK	RSA Programmed Signature Key	ECDH Private Key	ECDH Public Key	ECDH Shared Secret Key	ECDH Remote Party Public Key
Program Update	–	–	RWXZ	WZ	WZ	WZ	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Import keys	–	–	–	X	–	–	X	W	W	–	–	–	–	–	–	–
Privileged APCO OTAR	–	–	–	–	–	–	X	RWXZ	RWXZ	–	–	–	–	–	–	–
Change Active Keyset	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Change Password	–	WX	–	–	X	X	GXZ	Z	Z	WXZ	–	–	–	–	–	–
Encrypt	–	–	–	–	–	–	–	–	X	–	–	–	–	–	–	–
Decrypt	–	–	–	–	–	–	–	–	X	–	–	–	–	–	–	–
Zeroize Keys	–	–	–	–	–	–	–	Z	Z	–	–	–	–	–	–	–
Key/Keyset Check	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Generate Signature	–	–	–	–	–	–	–	–	X	–	–	–	–	–	–	–
Key Agreement Process	–	–	–	–	–	–	–	W	–	–	GWX	–	GWX	GWX	GWX	WX
Module Status	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Self-Tests	–	–	–	–	–	–	–	–	–	–	–	X	–	–	–	–
Validate Password	–	WX	–	–	X	X	GXZ	Z	Z	WXZ	–	–	–	–	–	–

Service	CSPs and Public Keys															
	DRBG Seed	DRBG Internal state (V and Key)	IDK	BKK	UKKPK	PEK	KPK	KEK	TEK	Password	PKPK	RSA Programmed Signature Key	ECDH Private Key	ECDH Public Key	ECDH Shared Secret Key	ECDH Remote Party Public Key
Zeroize all keys and password	–	WX	–	–	U	–	GZ	Z	Z	Z	Z	–	Z	Z	–	–
Non-Privileged APCO OTAR	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Reset	GZ	GXW	–	–	–	–	–	–	–	–	–	–	–	–	Z	Z
Shutdown	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Extract Error Log	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Clear Error Log	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Module Configuration	–	–	–	–	–	–	GXZ	Z	Z	WXZ	–	–	–	–	–	–

5 Self-tests

The MACE performs self-tests to ensure the proper operation of the MACE. Per FIPS 140-2 these are categorized as either power-up self-tests or conditional self-tests. Power-up self–tests are available on demand by power cycling the MACE.

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptographic functionality by the MACE. The MACE outputs a status indicator via self-test Indicator Interface to indicate all self-tests passed. The MACE performs the following algorithm KATs on power-up.

- Firmware Integrity: 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 MACE. When the MACE is powered up the digital signature is verified. If the digital signature matches the test passes, otherwise it fails.
- AES-256 encrypt and decrypt KATs for ECB, CBC, CFB8, OFB, and GCM modes (Certs. #819 & #1295.
- AES KW (SP 800-38F) KAT (Cert# C1444).
- AES KW (SP 800-38F) KAT (Cert# A654).
- SHA-256 KAT (Cert. #817).
- SHA-384 KAT (Cert. #2399).
- HMAC-SHA-384 KAT.
- CTR DRBG KAT.
- One-Step KDA (SP 800-56Cr1).
- ECDSA P-384 key generation KAT.
- EC Diffie-Hellman primitive “Z” computation KAT per IG 9.6 #1.

The MACE performs the following conditional self-tests as indicated.

- Continuous Random Number Generator test: The continuous random number generator test is performed on the NDRNG and DRBG supported by the MACE. An initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. A successive call to NDRNG/DRBG 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. This testing is done for each 4 byte NDRNG and 8 byte DRBG. The MACE enters the critical error state if this test fails.
- SP800-90A DRBG health 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 MACE, the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.
- ECDSA pair-wise consistency test on ECDSA key pair generation.

6 Physical Security Policy

The 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 information below is applicable to

Cryptographic Module hardware kit numbers 5185912Y03, 5185912Y05, and 5185912T05, which have identical physical security characteristics.

The MACE is covered with a hard, opaque epoxy coating that provides evidence of attempts to tamper with the MACE. The security provided from the hardness of the MACE's epoxy encapsulate is claimed at ambient temperature (20 to 25 degrees Celsius) only. No assurance of the epoxy hardness is claimed for this physical security mechanism outside of this range. The 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 MACE while delivering to operators.

7 Operational Environment

The MACE has a non-modifiable operational environment under the FIPS 140-2 definitions. The MACE includes Program Update service to support necessary updates. Firmware versions validated through the FIPS 140-2 CMVP will be explicitly identified on a validation certificate. If firmware that is not identified in this Security Policy is loaded into the MACE, the MACE will be in a non-Approved mode.

8 Mitigation of Other Attacks Policy

The MACE is not designed to mitigate any specific attacks outside of those required by FIPS 140-2.

9 Security Rules and Guidance

This section documents the security rules for the secure operation of the MACE to implement the security requirements of FIPS 140-2.

9.1 Invariant Rules

1. An operator does not have access to any cryptographic services prior to assuming an authorized role.
2. Power up self-tests do not require any operator action.
3. Data output is inhibited during key generation, self-tests, zeroization, and while in critical error states.
4. The MACE does not perform any cryptographic functions while in a critical error state.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the MACE.
6. The MACE protects secret keys and private keys from unauthorized disclosure, modification, and substitution.
7. The MACE provides a means to ensure that a key entered into or stored within the MACE is associated with the correct entities to which the key is assigned. Each key in the MACE is entered 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.
8. Authentication data are entered in encrypted form. Authentication data is not output during entry.
9. The MACE denies access to plaintext secret and private keys contained within the MACE.
10. The MACE implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
11. The MACE conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.

10 References and Definitions

The following standards are referred to in this Security Policy.

Table 16 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, *March 2019*
[133]	*NIST Special Publication 800-133 Revision 1, Recommendation for Cryptographic Key Generation, July 2019*
[186-2]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January, 2000.*
[186-4]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[22r1a]	*National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Cr1]	*NIST Special Publication 800-56C Revision 1, Revision 1Recommendation for Key-Derivation Methods in Key-Establishment Schemes, April 2018*

Abbreviation	Full Specification Name
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*

Table 17 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Diffie-Hellman
FIPS	Federal Information Processing Standards
FW	Firmware
GCM	Galois/Counter Mode
HSM	Hardware Security Module
IDK	Image Decryption Key
IV	Initialization Vector
KAT	Known Answer Test
KDA	Key-Derivation Method
KDF	Key Derivation Function
KPK	Key Protection Key
KEK	Key Encryption Key
KYLD	Keyload
KVL	Key Variable Loader
MAC	Message Authentication Code
MACE	Motorola Advanced Crypto Engine

Acronym	Definition
MDC	Motorola Data Communication
NDRNG	Non-Deterministic Random Number Generator
OFB	Output Feedback
OTAR	Over The Air Rekeying
PKPK	Private Key Protection Key
RSA	Rivest–Shamir–Adleman
SSI	Synchronous Serial Interface
TEK	Traffic Encryption Key
UKEK	Universal Key Encryption Key
UKKPK	Universal Key for Key Protection Key