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

Non-Proprietary FIPS 140-3 Security Policy

Document Version: 1.3

Date: October 08, 2024

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.

Table of Contents

Copyright Motorola Solutions, Inc. 2024   Version 1.3   Page 2 of 30

Motorola Solutions Public Material – May be reproduced only in its original entirety (without revision).

List of Tables

List of Figures

Copyright Motorola Solutions, Inc. 2024   Version 1.3   Page 3 of 30

Motorola Solutions Public Material – May be reproduced only in its original entirety (without revision).

1 General

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 meet FIPS 140-3 level 2 physical security requirements as defined by FIPS 140-3 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.

The FIPS 140-3 security levels for the MACE are as follows:

Table 1 – Security Levels

ISO/IEC 24759 Section 6 [Number below]	FIPS 140-3 Section Title	Security Level
1	General	2
2	Cryptographic Module Specification	2
3	Cryptographic Module Interfaces	2
4	Roles, Services, and Authentication	3
5	Software/Firmware Security	3
6	Operational Environment	N/A
7	Physical Security	2
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	2
10	Self-Tests	3
11	Life-Cycle Assurance	3
12	Mitigation of Other Attacks	N/A
Overall		**2**

2 Cryptographic Module Specification

The MACE cryptographic module is a single chip hardware cryptographic module. The MACE is used in multiple Motorola Solutions, Inc. subscribers. The MACE cryptographic module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated overall Security Level 2.

2.1 Operational Environment

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

Table 2 – Cryptographic Module Tested Configuration

Model	HW P/N, Version	Base Firmware version	Distinguishing Features
Astro Subscriber Motorola Advanced Crypto Engine (MACE)	5185912Y03, 5185912Y05, 5185912T05	R01.13.04	Single chip embodiment

The 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 (ECB, CBC, and OFB)	R01.00.00	R01.13.04	A2261
AES256 (ECB, CBC, OFB, and GCM)	R01.00.01	R01.13.04	A2262

2.2 Cryptographic Boundary

The physical form of the MACE cryptographic module is depicted in Figure 1 and Figure 2. The MACE is a single chip embodiment. The cryptographic boundary is drawn around the perimeter of the MACE IC as shown in Figure 3.
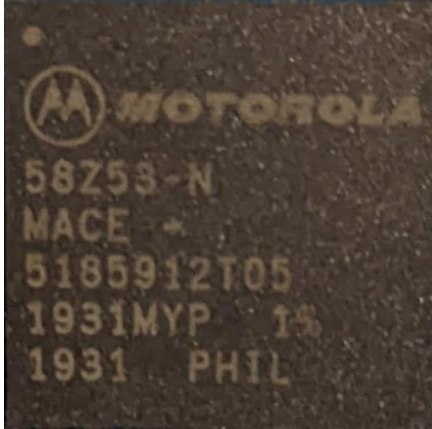
Figure 1: MACE Chip (Top)
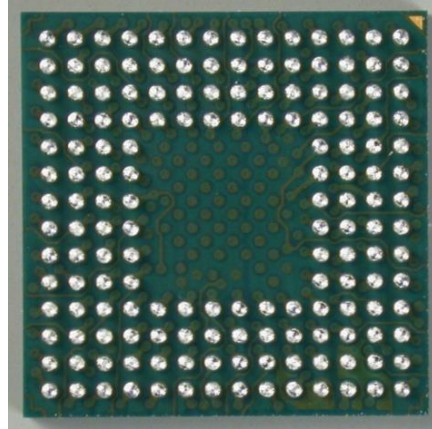
Figure 2: MACE Chip (Interfaces)

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.
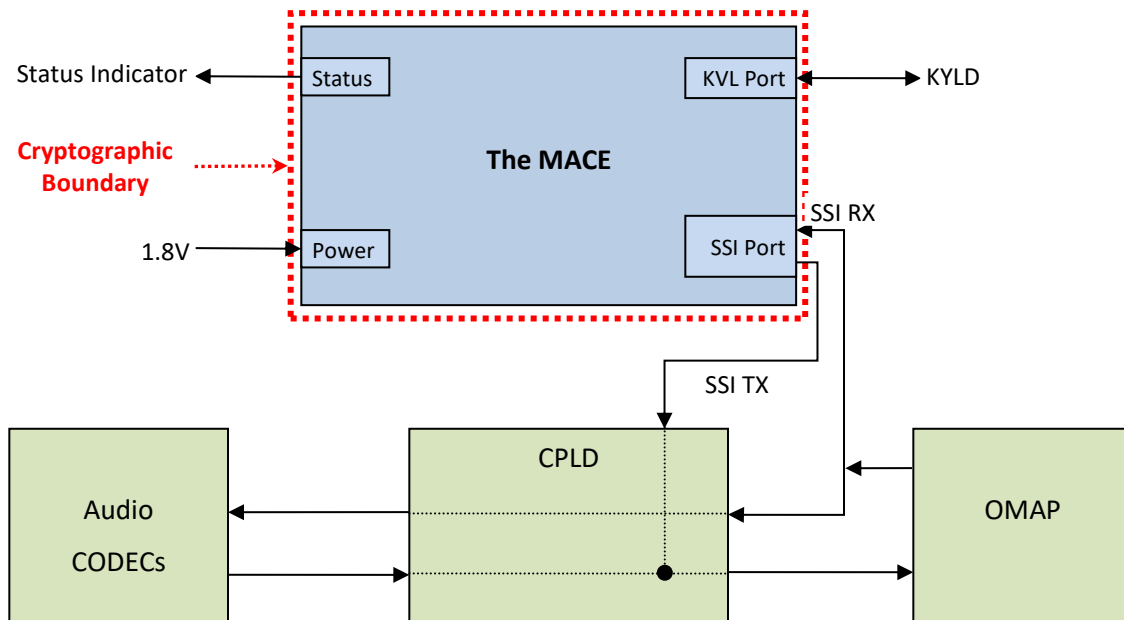
Figure 3: Cryptographic Boundary Block Diagram

2.3 Modes of Operation

The 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 2. At any given time, the Module status service can be used to determine whether the MACE is operating at overall Security Level 2.

There is no Non-approved Mode.

Table 4 – Approved Mode Indicator

Approved Mode Indicator Value	Meaning
303B020002	Approved Mode at overall Security Level 2

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.

Also, the module status service will output the AES-256 DIA version installed with a display of 52 (ASCII "R") 01 00 00 -> R01.00.00 - AES256 DIA or 52 (ASCII "R") 01 00 01 -> R01.00.01 - AES256 DIA.

2.3.1   Configuration of the Approved Mode of Operation

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

The operator shall configure the periodic self-tests timer as part of the Module configuration. Please refer to Section 11 for further details.

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 Approved Mode, only Approved and Allowed algorithms are loaded into the MACE during initialization; in particular AES-256 (Certs #A2261 and #A2262). The loading and unloading of any firmware within the validated cryptographic module invalidates the Module and zeroizes all SSPs except those entered at manufacturing. The Module is then in a non-compliant state.

2.4   Security Functions

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

Note: The brackets [] reference the corresponding documents that can be found in the References - Table 19

Table 5 – Approved Algorithms

Cert #	Algorithm	Mode	Description / Key Size(s) / Key Strength(s)	Use/Functions
A2260	AES [197]	CFB8 [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
A2261	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt

Cert #	Algorithm	Mode	Description / Key Size(s) / Key Strength(s)	Use/Functions
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
A2262	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
		GCM [38D][1]	Key Sizes: 256	Encrypt, Decrypt
A2263	AES [197]	KW [38F]	Forward. Key Sizes: 256	Authenticated Encrypt, Decrypt for storing SSPs
A2264	AES [197]	KW [38F]	Forward. Key Sizes: 256	Authenticated Decrypt for KTS
VA	CKG [IG D.H]		[133] Sections 4 and 5.2 Asymmetric key establishment key generation using unmodified DRBG output	Key Generation
			[133] Section 4 and Section 6.1 Direct symmetric key generation using unmodified DRBG output	
			[133] Section 6.3 Symmetric Keys Produced by Combining (Multiple) Keys and Other Data	
A2265	DRBG [90A]	CTR with derivation function	AES-256	Deterministic Random Bit Generation[2]
A655	ECDSA [186-4]		P-384 (SHA2-384)	Key Generation
HMAC 1796	HMAC [198]	SHA2-384	Key Sizes: 32 bytes $\lambda = 48\ bytes$	Message Authentication
A2266	KAS-ECC [56Ar3]	KASECC (Initiator, Responder), KPG, Partial, oneStepKdf (SP800-56Cr1)	P-384 SHA2-384	Key Agreement Scheme Key establishment methodology provides 192 bits of encryption strength
A2264	KTS [38F]	KW	AES KW Cert. #A2264	Decrypt OTAR Key blocks encrypted with AES 256 bit keys. Key establishment methodology provides 256 bits strength
A5253	RSA [186-5]	PKCS1_v1.5	2048	SigVer
RSA 396	RSA [186-2][3]	PKCS1_v1.5	2048	SigVer

[1] Per IG C.H Scenario 2, the MACE generates GCM IVs randomly as specified in SP800-38D section 8.2.2 using approved DRBG (Cert #A2265) and the IV length is 96 bits.

[2] The entropy for seeding the SP 800-90A DRBG is determined by the operator of the MACE which is outside of the Module's physical and logical boundary. The operator shall use entropy sources that meet the security strength required for the random number generation mechanism as shown in [SP 800-90A] Table 3 (CTR_DRBG) and set required bits into the Module by using Load Entropy service listed in Section 4.3. Since entropy is loaded passively into the Module, there is no assurance of the minimum strength of generated keys. The MACE will not operate in an Approved Mode if the Module is not seeded by the external entropy.

[3] RSA SigVer [FIPS 186-2] is approved for legacy use only: verifying signatures that were performed starting September 1st 2020 and onwards is a not a FIPS 140-3 compliant use of this algorithm/service and cannot

Cert #	Algorithm	Mode	Description / Key Size(s) / Key Strength(s)	Use/Functions
SHS 817	SHS [180]	SHA2-256		Message Digest Generation, Password Obfuscation
SHS 2399	SHS [180]	SHA2-384		Message Digest Generation

Table 6 – Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Caveat	Use/Function
KTS [38F]	key unwrapping only; Key establishment methodology provides 256 bits strength	[IG D.G] AES CBC Cert. #A2261 or #A2262

Table 7 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Caveat	Use/Function
AES MAC	N/A	[IG 2.4.A] P25 AES OTAR. No Security Claimed. AES MAC is used as part of OTAR but is considered obfuscation. KTS encryption is performed on the OTAR key components using AES KW and decrypted using AES KW Cert. #A2264

Note: The Module does not implement any Non-Approved Algorithms and Not Allowed Cryptographic Functions in the Approved Mode of Operation.

2.5   Overall Security Design

1. The MACE provides two distinct operator roles: User and Cryptographic Officer.

2. The MACE provides identity-based authentication.

3. The MACE 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 MACE allows the operator to initiate power-up self-tests by power cycling power or resetting the MACE.

6. Power up 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 MACE.

9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.

10. The MACE does not support concurrent operators.

---

claim security. Verifying signatures generated before September 1st 2020 is the approved legacy use of RSA SigVer [FIPS 186-2].

11. The MACE does not support a maintenance interface or role.

12. The MACE does not support manual SSP establishment method.

13. The MACE does not have any proprietary external input/output devices used for entry/output of data.

14. The MACE does not output intermediate key values.

15. The MACE does not provide bypass services on ports/interfaces.

2.6   Rules of Operation

The MACE shall be installed in the Motorola Solutions subscriber products. After authentication with the default password, the operator shall change the default password for the User role. The MACE is not usable until the factory default password is changed for the User role. Note that this makes it very important that physical access to the MACE is strictly controlled.

The MACE shall be operated such that only approved Drop-in algorithms listed in the Table 3 are installed including Section 11 secure installation, initialization, startup and operation of the MACE.

3   Cryptographic Module Interfaces

The MACE's ports and associated FIPS defined logical interface categories are listed in Table 8.

Table 8 – Ports and Interfaces

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

4   Roles, Services and Authentication

4.1   Assumption of Roles and Related Services

The MACE supports one distinct operator role, Cryptographic Officer (CO). Table 9 lists the operator role supported by the MACE and their related services. In addition, the MACE supports services which does not require to be authenticated, listed UA in Table 9.

The MACE does not support a maintenance role and/or bypass capability.

Table 9 – Roles, Service Commands, Input and Output

Role		Service	Input	Output
CO	**UA**			
–	X	Program Update	Firmware Image	The MACE is upgraded to new firmware.
X	–	Load Entropy	DRBG Seed	The DRBG is seeded and initialized. Success/failure status.
X	–	Import Keys Over KYLD Interface	Encrypted Keys	Keys imported into the MACE. Success/failure status.
X	–	Privileged APCO OTAR	Encrypted Keys	Keys imported into the MACE. Success/failure status.
X	–	Change Active Keyset	Keyset Index	Changed the active keyset as requested. Success/failure status.
X	–	Change Password	Password	Updated the User password. Success/failure status.
X	–	Encrypt	Plaintext	Ciphertext. Success/failure status.
X	–	Decrypt	Ciphertext	Plaintext. Success/failure status.
X	–	Zeroize Key	Key Index	Zeroized the key. Success/failure status.
X	–	Key/Keyset Check	Key/Keyset Index	Success/failure status.
X	–	Generate Signature	Service Request	Signature out. Success/failure status.
X	–	Key Agreement Process	Service Request	Keys imported into the MACE. Success/failure status.
X	–	Zeroize All Keys and Password	Command In	Success/failure status.
–	X	Module Status	Command in	Module HW version, version information, and FIPS status.
–	X	Self-Tests	Command In	Success/Reset.
–	X	Validate Password	Password	Successful authentication will allow access to the services allowed for User role.
–	X	Extract Error Log	Command In	Error logs out. Success/Failure status.
–	X	Clear Error Log	Command In	Success/Failure status.
–	X	Reset	Command In	Reset the MACE.
–	X	Module Configuration	Configuration Parameters	The MACE is configured as requested. Success/Failure status.

4.2   Authentication Methods

The MACE supports one distinct operator roles (Crypto-Officer). The MACE uses a 10-digit password to authenticate the Crypto-Officer.

The Module ensures that there is no visible display of the authentication data.

Table 10 – Roles and Authentication

Role	Authentication Method	Authentication Strength
CO	Identity-based: The CO role is authenticated to the MACE over SSI interface with 10-digit hexadecimal number.	The strength of the authentication method is $1/16^{10}$. 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 probability of a successful random attempt during a one-minute period is $15/16^{10}$.

4.3 Services

All services implemented by the MACE are listed in Table 11 and indicated use is based on the Module being in Approved Mode per Table 4. The MACE does not allow any non-approved services while operating in FIPS 140-3 level 2 mode.

The SSPs modes of access shown in Table 11 are defined as:

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

Table 11 – Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
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.	RSA [186-5], Cert. #A5253	FW-LD-Pub	UA	Z	Approved Mode
			IDK-ROM		E	
			IDK-Block		EZ	
			IDK		Z	
			BKK		Z	
			UKKPK		Z	
			PEK		Z	
			KPK		Z	
			KEK		Z	
			TEK		Z	
			Password		Z	
			PWD Hash		Z	
			PKPK		Z	
			DH-Priv		Z	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
			DH-Pub		Z	
			DH-SS		Z	
			DH-CLI-Pub		Z	
Load Entropy	Load entropy into the MACE.	AES Key Unwrap, AES Certs. #A2261 or #A2262, DRBG Cert. #2265	DRBG-EI/Seed	CO	WE	Approved Mode
			DRBG-State		G	
			BKK		E	
Import keys over KYLD interface	Imports keys to the MACE via a Key Variable Loader (KVL) in plaintext.	AES Key Unwrap (KTS), AES Cert. #A2260 AES Cert. #2264	KPK	CO	E	Approved Mode
			KEK		W	
			TEK		W	
Privileged APCO OTAR	Import, modify and query the keys.	KW [38F], Cert. #A2264. AES Certs. #A2261 or #A2262.	KPK	CO	E	Approved Mode
			KEK		WEZ	
			TEK		WEZ	
Change Active Keyset	Modify the currently active keyset used for selecting keys for encryption/decryption services.	N/A	N/A	CO	N/A	Approved Mode
Change Password	Modify the current password used to identify and authenticate the User role.	CKG, AES-256, Cert. #A2260. SHS [180], Cert. #817	UKKPK	CO	E	Approved Mode
			PEK		E	
			KPK		GEZ	
			KEK		Z	
			TEK		Z	
			Password		GEZ	
			PWD Hash		GEZ	
Symmetric Key Generation	Generates the symmetric keys	CKG, AES [197] CBC Cert. #A2261 or #A2262 AES CFB-8 Cert. #A2260, DRBG Cert. #A2265	IDK-ROM	CO	EZ	Approved Mode
			IDK-Block		EZ	
			IDK		GZ	
			KPK		GZ	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
Encrypt	Encrypt digital voice or data.	AES [197], Cert. #A2261 or #A2262 DRBG Cert. #2265	TEK	CO	E	Approved Mode
Decrypt	Decrypt digital voice or data.	AES [197], Cert. #A2261 or #A2262	TEK	CO	E	Approved Mode
Zeroize Keys	Zeroize selected key variables from the MACE.	N/A	KEK	CO	Z	Approved Mode
			TEK		Z	
Key/Keyset Check	Obtain status information about a specific key/keyset.	N/A	N/A	CO	N/A	Approved Mode
Generate Signature	Generate HMAC-SHA2-384 signature.	HMAC [198], Cert. #1796	TEK	CO	E	Approved Mode
Key Agreement Process	Perform a key agreement process to create an ECDH Shared Secret, and ECDH Public and Private Keys.	CKG DRBG Cert. #2265, KAS-ECC [56Ar3], Cert. #A2266, ECDSA Cert. #A655	KEK	CO	W	Approved Mode
			PKPK		GE	
			DH-Priv		GE	
			DH-Pub		GRE	
			DH-SS		GE	
			DH-CLI-Pub		WE	
			DRBG-State		GE	
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.	N/A	UKKPK	CO	E	Approved Mode
			KPK		GZ	
			KEK		Z	
			TEK		Z	
			Password		Z	
			PWD Hash		Z	
			PKPK		Z	
			DH-Priv		Z	
			DH-Pub		Z	
Module Status	Provide module version, firmware version, FIPS status	N/A	N/A	UA	N/A	Approved Mode

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
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.	N/A	FW-LD-Pub	UA	E	Approved Mode
Validate Password	Validate the current password used to identify and authenticate the User role.	AES-256, Cert. #A2260. SHS [180], Cert. #817	UKKPK	UA	E	Approved Mode
			PEK		E	
			KPK		GEZ	
			KEK		Z	
			TEK		Z	
			Password		Z	
			PWD Hash		Z	
Extract Error Log	Provide the history of error events.	N/A	N/A	UA	N/A	Approved Mode
Clear Error Log	Clears the history of error events.	N/A	N/A	UA	N/A	Approved Mode
Reset	Reset/power cycle the MACE.	N/A	DRBG-EI/Seed	UA	Z	Approved Mode
			DRBG-State		Z	
			DH-SS		Z	
			DH-CLI-Pub		Z	
Module Configuration	Download configuration parameters used to specify module behavior.	N/A	KPK	UA	GEZ	Approved Mode
			KEK		Z	
			TEK		Z	
			Password		WZ	
			PWD Hash		Z	

Note: The Module does not implement any Non-Approved Services and only provides an Approved Mode of operation.

5   Firmware Security

The MACE is composed of base firmware version identified in Table 2. In addition, the customer shall load at least one of the Drop-in algorithms listed in Table 3.

The firmware components are protected with the approved firmware integrity technique described in Table 17.

The Module includes a firmware verification and load service to support necessary updates for the base firmware.

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

The Module is composed of the following firmware component(s):
- non-modifiable operating system - binary

6   Operational Environment

The MACE has a limited operational environment under the FIPS 140-3 definitions with a Physical Security at Level 2 therefore this section in not applicable.

7   Physical Security

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

Table 12 – Physical Security Inspection Guidelines

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

8 Non-Invasive Security

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

9   Sensitive Security Parameter (SSP) Management

The SSPs access methods are described in Table 13 below:

Table 13 – SSP Management Methods

Method	Description
G1	Generated external to the MACE and installed during manufacturing.
G2	Derived from the DRBG input per SP800-90Ar1.
G3	FIPS 186-4 compliant ECDSA key generation, using the internal CAVP validated DRBG.
G4	CKG - Symmetric key generated by internal CAVP validated DRBG.
G5	EC Diffie-Hellman shared secret generation using the internal CAVP validated 56Arev3 protocol
G6	Generated per SP800-133r2 (Section 6.3 #2) via XOR of 2 other keys (IDK ROM and IDK Block)
S1	Stored in the volatile memory (RAM) in plaintext.
S2	Stored in the flash in plaintext, associated by memory location (pointer).
S3	Stored in the flash in encrypted, associated by memory location (pointer).
E1	Electronically input, AES-256 CBC encrypted by the IDK Block and ROM using AES KTS (Cert. #s A2261, #A2262)
E2	Electronically input, AES-256 ECB encrypted by the BKK using AES KTS (Cert. #s A2261, #A2262)
E3	Electronically input, AES-256 CFB-8 encrypted by the PEK using AES KTS (Cert. #s A2261, #A2262)
E4	Electronically input in plaintext through the directly connected KVL.
E5	Electronically input using SP800-38F AES key transport by the KEK or TEK using AES KW Cert. #A2264.
E6	Electronically established through ECDH Key Agreement Process (SP 800-56A KASrev3, Cert. #A2266)
Z1	Zeroized by program update service by overwriting with a fixed pattern "0s". *
Z2	Zeroized by module power cycle or hard reset by overwriting with a fixed pattern "0s". *
Z3	Zeroized by the "zeroize keys" service by overwriting with a fixed pattern of "0s".
Z4	Zeroized by the "zeroize all keys and password" service by overwriting with a fixed pattern of "0s".
Z5	Zeroized by the "validate password" service by overwriting with a fixed pattern "0s".
Z6	Zeroized by the "change password" service by overwriting with a fixed pattern "0s".
Z7	Zeroized by the "module configuration" service by overwriting with a fixed pattern "0s".
Z8	Zeroized by the "privileged APCO OTAR" service by overwriting with a fixed pattern "0s".
Z9	Zeroized by the "import keys over KYLD interface" service by overwriting with a fixed pattern "0s".

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.

9.1 Sensitive Security Parameters (SSP)

All SSPs (CSPs and PSPs) used by the MACE are described in this section. All usage of these CSPs by the MACE is described in the services detailed in 4.3.

Table 14 – SSPs

Key/SSP Name/ Type	Strength (in bits)	Security Function / Cert. #	Genera- tion	Import /Export	Establish- ment	Storage	Zeroiza- tion	Use / Related SSPs
CSPs								
DRBG-EI/Seed	N/A	N/A	N/A	E2	N/A	S1	Z2	Externally generated, a minimum of 48 bytes are passively entered into the MACE by the User.
DRBG-State	256	DRBG Cert. #A2265	G2	N/A	N/A	S1	Z2	CTR_DRBG internal state: V (128 bits) and Key (AES 256) and derived from DRBG-EI/Seed
IDK ROM	256	AES CBC Cert. #A2261 or #A2262	G1	N/A	N/A	S1, S2	Z1, Z2	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
IDK Block	256	AES CBC Cert. #A2261 or #A2262	G1	E1	N/A	S1, S2	Z1, Z2	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
IDK	256	AES CBC Cert. #A2261 or #A2262	G6	N/A	N/A	S1	Z2	A 256-bit AES CBC key used to decrypt downloaded firmware images.
BKK	256	AES ECB Cert. #A2261, #A2262	G1	N/A	N/A	S1, S2	Z1, Z2	A 256 bit AES key used for decrypting Load entropy into the MACE.
UKKPK	256	AES CBC Cert. #A2261 or #A2262	G1	N/A	N/A	S1, S2	Z1, Z2	256 bit AES Key used for encrypting the KPK in flash.
PEK	256	AES CBC Cert. #A2261 or #A2262	G1	N/A	N/A	S1, S2	Z1, Z2	256-bit AES CFB-8 key used for decrypting passwords.

Key/SSP Name/ Type	Strength (in bits)	Security Function / Cert. #	Genera- tion	Import /Export	Establish- ment	Storage	Zeroiza- tion	Use / Related SSPs
KPK	256	AES CFB-8 Cert. #A2260, DRBG Cert. #A2265	G4	N/A	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7	256 bit AES CFB-8 key used to encrypt all TEKs and KEKs stored in flash.
KEK	256	AES KW Cert. #A2264, AES OFB Cert. #A2260	N/A	E4, E5, E6	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9	256-bit AES Keys used for decrypting key blocks in the OTAR service.
TEK	256	AES KW Cert. #A2264 AES OFB Cert. #A2260	N/A	E4, E5	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7, Z8, Z9	256-bit AES key used for voice and data decryption.
Password	N/A	AES CFB-8 Cert. #A2260	N/A	E3	N/A	S1	Z1, Z2, Z4, Z5, Z6, Z7	10-digit hexadecimal number user authentication password
PWD Hash	128	SHS [180] Cert. #817 SHA2-256	G1	N/A	N/A	S1, S2	Z1, Z2, Z4, Z5, Z6, Z7	256-bit password hash stored in the non-volatile memory.
PKPK	256	AES KW #A2263	G4	N/A	N/A	S1, S3	Z1, Z2, Z4	256-bit AES KW used to store encrypted, the ECDH generated private key.
DH-Priv	192	KAS #A2266, ECDSA Cert. #A655	G3	N/A	N/A	S1, S3	Z1, Z2, Z4	The Elliptic Curve Diffie-Hellman (DH) private key used for establishing a shared secret over an insecure channel.
DH-SS	192	KAS #A2266	N/A	N/A	G5	S1	Z2	The Elliptic Diffie-Hellman (DH) Shared Secret (SS) is established as a part of DH key agreement scheme.
PSPs								
FW-LD-Pub	112	AES CBC #A2261 or #A2262, RSA Cert. #A5253	G1	N/A	N/A	S1, S2	Z1, Z2	2048-bit RSA key used to validate the signature of the firmware image before it is allowed.

Key/SSP Name/ Type	Strength (in bits)	Security Function / Cert. #	Genera-tion	Import /Export	Establish-ment	Storage	Zeroiza-tion	Use / Related SSPs
DH-Pub	192	KAS Cert. #A2266, ECDSA Cert. #A655	G3	E6	N/A	S1, S2	Z1, Z2	The Elliptic Curve (EC) Diffie-Hellman (DH) public key, used for establishing a shared secret over an insecure channel.
DH-CLI-Pub	192	KAS Cert. #A2266	N/A	E6	N/A	S1, S2	Z1, Z2	The Elliptic Curve (EC) Diffie-Hellman (DH) public key from the other party, used for establishing a shared secret over an insecure channel.

Table 15 – Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum number of bits of entropy	Details
External	384 bits of entropy	The Load Entropy service provides the security strength required for the random number generation mechanism

10 Self-Tests

The MACE performs self-tests to ensure the proper operation of the MACE. 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 MACE. Conditional self–tests are periodically performed by the MACE as configured by the operator during module configuration as shown in Section 11.1.1. The 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 MACE at the end of periodic self-test when the I/O buffer is emptied. The MACE will reset if any self-tests fail, otherwise it will continue to operate normally. The MACE logs the most recent self-test errors to the internal flash; the operator (UA) can extract the error logs using Extract Error Log service list in section 4.3.

The self-tests error states and status indicator are described in table below:

Table 16 – Error States and Indicators

Error state	Description	Indicator
ES1	The MACE fails a KAT.	The MACE enters the critical error state. In this state, the MACE stores the status into the internal flash memory and then halts all further operation by entering an infinite loop. The operator may correct this state by power cycling the MACE.
ES2	The MACE fails a firmware loading during program upgrade and/or firmware integrity pre-operational self-test.	The MACE enters the firmware signature validation failure state. In this state, the MACE halts all further operations by entering the flash programming mode. The operator may correct the issue by power cycle and/or re-flashing a new image.
ES3	The MACE fails an ECDSA PCT.	The MACE enters a temporary error state. The generated key is not used, and the Module returns an error code (0x1) to the operator. The key is discarded, and the process abandoned.

The MACE performs the following pre-operational self-tests:

Table 17 – Pre-Operational Self-Test

Security Function	Method	Description	Error state
Firmware integrity	RSA (Cert. #396 and #A5253), SHA2-256 (Cert. #817)	A digital signature is generated over the Boot Block and Base firmware using RSA-2048 (Cert. #A5253) code when it is built and the Drop-in algorithms code uses RSA-2048 (Cert. #396) 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, then the test passes, otherwise it fails.	ES2

The MACE performs the following conditional self-tests:

Table 18 – Conditional Self-Tests

Security Function	Method	Description	Error state
AES – ECB (Cert. #A2261)	KAT	AES-256 ECB encryption KAT - Inclusive to AES CBC and OFB encryption mode testing with 256-bit key per IG 10.3.A.	ES1
AES – ECB (Cert. #A2261)	KAT	AES-256 ECB decryption KAT – Inclusive to AES CBC and OFB inverse function testing with 256-bit key per IG 10.3.A.	ES1
AES – ECB (Cert. #A2262)	KAT	AES-256 ECB encryption KAT – Inclusive to AES CBC and OFB encryption mode testing with 256-bit key per IG 10.3.A.	ES1
AES – ECB (Cert. #A2262)	KAT	AES-256 ECB decryption KAT – Inclusive to AES CBC and OFB inverse function testing with 256-bit key per IG 10.3.A.	ES1
AES – CFB8 (Cert. #A2260)	KAT	AES-256 CFB-8 encryption KAT – Inclusive to AES-256 OFB testing with 256-bit key per IG 10.3.A.	ES1
AES – CFB8 (Cert. #A2260)	KAT	AES-256 CFB-8 decryption KAT – Inclusive to AES-256 OFB testing with 256-bit key per IG 10.3.A.	ES1
AES – GCM (Cert. #2262)	KAT	AES-256 GCM encryption KAT as per IG 10.3.A,	ES1
AES – GCM (Cert. #2262)	KAT	AES-256 GCM decryption KAT as per IG 10.3.A,	ES1
AES KW (Cert. #A2263)	KAT	AES-256 key wrapping KAT.	ES1
AES KW (Cert. #A2263)	KAT	AES-256 key unwrapping KAT.	ES1
AES KW (Cert. #A2264)	KAT	AES-256 key unwrap KAT.	ES1
DRBG (Cert. #A2265)	KAT	AES-256 CTR_DRBG Health Tests (instantiation, generate, and reseed) KATs performed before the first random data generation.	ES1
ECDSA Key Generation	PWCT	ECDSA P-384 Key Generation Pair-Wise Consistency Test	ES3
Firmware Load (Cert. #A5253)	RSA-2048 SigVer	A digital signature is generated over the code when it is built using SHA2-256 and RSA-2048 (FIPS 186-5). The digital signature is verified upon download into the MACE.	ES2
HMAC (Cert. #1796)	KAT	HMAC-SHA2-384 KAT.	ES1
KAS-ECC (Cert. #2266)	KAT	Per IG D.F, separately tested KAS Shared Secret generation with P-384 and SP 800-56Cr2 one-step KDA	ES1
RSA SigVer (Cert. #A5253)	KAT	RSA-2048 SigVer, performed before FW integrity tests. Inclusive for 186-2 (Cert. #396)	ES2
SHS 256-bit (Cert. #817)	KAT	SHA2-256 KAT, performed before FW integrity tests.	ES2
SHS 384-bit (Cert. #2399)	KAT	SHA2-384 KAT	ES1

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 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 MACE from the instructions below:

1. Upon first access, the operator will use the default password provided by Motorola in a separate communication.
2. The operator will then change the default password based on the requirements in Table 10 – Roles and Authentication
3. The operator will then configure the MACE using the Module configuration service as specified in the section 2.3.1.
4. Finally, 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 minute and maximum value = 712,800 minutes (495 days). Note: the default minimum = 0* but must be changed to a minimum of 1.

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

11.1.2 Delivery

The MACE is embedded in multiple Motorola Solutions, Inc. radios (aka, subscribers). Motorola uses commercially available courier systems such as UPS, FedEx, and DHL with a tracking number and requires a signature at the end by an authorized client.

11.2 Administrator Guidance

Use radio specific user guide available on the www.motorolasolutions.com website for secure operations.

11.3 Non-Administrator Guidance

Use radio specific user guide available on the www.motorolasolutions.com website for secure operations.

11.4 Maintenance Requirements

The MACE does not require any special maintenance.

11.5 End of Life

After the end-of-life, the operator should zeroize all SSPs using the "Zeroize all keys and password" service listed in the Section 4.3 followed by shredding the MACE chip.

12 Mitigation of Other Attacks

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

13 References and Definitions

The following standards are referred to in this Security Policy.

Table 19 – References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, May 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, November 2021.*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[186-2]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, January 2001.*
[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*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[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*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Cr2]	*NIST Special Publication 800-56C Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, August 2020*
[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.*

Abbreviation	Full Specification Name
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*

Table 20 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
BKK	Black Keyloading Key
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CSP	Critical Security Parameter
DH-CLI-Pub	Diffie-Hellman Client Public Key
DH-Priv	Diffie-Hellman Private Key
DH-Pub	Diffie-Hellman Public Key
DH-SS	Diffie-Hellman Shared Secret
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 Algorithm
KEK	Key Encryption Key
KPK	Key Protection Key
KYLD	Keyload
KVL	Key Variable Loader
MAC	Message Authentication Code
MACE	Motorola Advanced Crypto Engine
MDC	Motorola Data Communication
OFB	Output Feedback

Acronym	Definition
OTAR	Over The Air Rekeying
PEK	Password Encryption Key
PKPK	Private Key Protection Key
PWCT	Pair-Wise Consistency Test
PWD Hash	Password Hash
RSA	Rivest–Shamir–Adleman
SSI	Synchronous Serial Interface
SSP	Sensitive Security Parameter
TEK	Traffic Encryption Key
UA	Unauthenticated Service
UKEK	Universal Key Encryption Key
UKKPK	Universal Key for Key Protection Key