

Motorola Solutions, Inc.

Astro Subscriber Motorola Advanced Crypto Engine (MACE) - Security Level 3

FIPS 140-3 Non-Proprietary Security Policy

Document Version: R01.01.00

Date: March 03, 2026

Table of Contents

1 General.....	5
1.1 Overview	5
1.2 Security Levels.....	5
2 Cryptographic Module Specification.....	5
2.1 Description	5
2.2 Tested and Vendor Affirmed Module Version and Identification	7
2.3 Excluded Components	8
2.4 Modes of Operation.....	8
2.5 Algorithms.....	9
2.6 Security Function Implementations.....	11
2.7 Algorithm Specific Information	14
AES GCM IV Generation	14
Legacy Use.....	15
Key Agreement Scheme	15
2.8 RBG and Entropy	15
2.9 Key Generation	15
2.10 Key Establishment.....	15
3 Cryptographic Module Interfaces	15
3.1 Ports and Interfaces	15
4 Roles, Services, and Authentication.....	16
4.1 Authentication Methods	16
4.2 Roles.....	17
4.3 Approved Services.....	17
4.4 Non-Approved Services.....	25
4.5 External Software/Firmware Loaded	25
5 Software/Firmware Security	26
5.1 Integrity Techniques	26
5.2 Initiate on Demand	26
6 Operational Environment	26
6.1 Operational Environment Type and Requirements	26
7 Physical Security.....	26
7.1 Mechanisms and Actions Required.....	26
7.5 EFP/EFT Information	27

7.6 Hardness Testing Temperature Ranges	27
8 Non-Invasive Security.....	28
9 Sensitive Security Parameters Management	28
9.1 Storage Areas	28
9.2 SSP Input-Output Methods	28
9.3 SSP Zeroization Methods	29
9.4 SSPs	30
10 Self-Tests	35
10.1 Pre-Operational Self-Tests	35
10.2 Conditional Self-Tests	36
10.3 Periodic Self-Test Information	39
10.4 Error States	40
11 Life-Cycle Assurance	41
11.1 Installation, Initialization, and Startup Procedures	41
11.2 Administrator Guidance.....	41
11.3 Non-Administrator Guidance.....	41
11.4 Design and Rules	42
Rules of Operation	42
11.5 Maintenance Requirements	42
11.6 End of Life	42
12 Mitigation of Other Attacks	43

List of Tables

Table 1: Security Levels.....	5
Table 2: Tested Module Identification – Hardware	7
Table 3 – Approved Mode Drop-in Algorithms.....	7
Table 4: Modes List and Description.....	8
Table 5: Approved Algorithms	10
Table 6: Vendor-Affirmed Algorithms.....	11
Table 7: Non-Approved, Allowed Algorithms	11
Table 8: Non-Approved, Allowed Algorithms with No Security Claimed.....	11
Table 9: Security Function Implementations	14
Table 10: Entropy Certificates.....	15
Table 11: Entropy Sources	15
Table 12: Ports and Interfaces	16
Table 13: Authentication Methods.....	17
Table 14: Roles	17
Table 15: Approved Services	25
Table 16: Mechanisms and Actions Required.....	27
Table 17: EFP/EFT Information	27
Table 18: Hardness Testing Temperatures	27
Table 19: Storage Areas	28
Table 20: SSP Input-Output Methods	29
Table 21: SSP Zeroization Methods	29
Table 22: SSP Table 1	32
Table 23: SSP Table 2	35
Table 24: Pre-Operational Self-Tests	36
Table 25: Conditional Self-Tests.....	39
Table 26: Pre-Operational Periodic Information	39
Table 27: Conditional Periodic Information.....	40
Table 28: Error States.....	41

List of Figures

Figure 1 – MACE IC (Top)	6
Figure 2 – MACE IC (Interfaces)	6
Figure 3 – Cryptographic Boundary for the MACE.....	7

1 General

1.1 Overview

This document defines the Security Policy for the Astro Subscriber Motorola Advanced Crypto Engine (MACE) – Security Level 3, hereafter denoted the MACE. The MACE is implemented as a single-chip cryptographic module to meet FIPS 140-3 Level 3 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.

1.2 Security Levels

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

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

Table 1: Security Levels

2 Cryptographic Module Specification

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

2.1 Description

Purpose and Use:

The MACE cryptographic module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated overall Security Level 3.

Module Type: Hardware

Module Embodiment: Single Chip

Cryptographic Boundary:

The physical form of the Module is depicted in Figure 1 and Figure 2. The Module is a single-chip embedded embodiment. The photos below depict all hardware kit numbers 5185912Y03, 5185912Y05, and 5185912T05, which have identical physical security characteristics. The cryptographic boundary is shown in Figure 3.

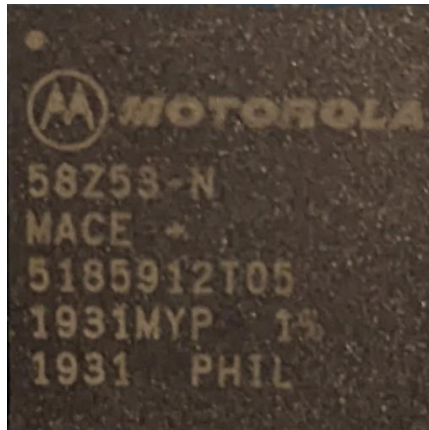


Figure 1 – MACE IC (Top)

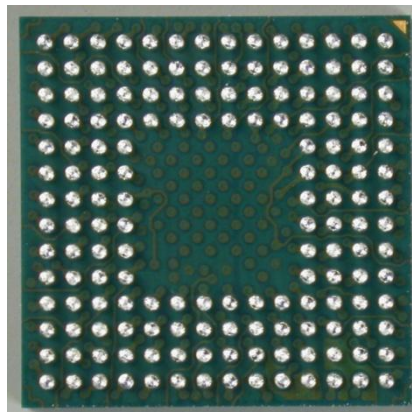


Figure 2 – MACE IC (Interfaces)

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.

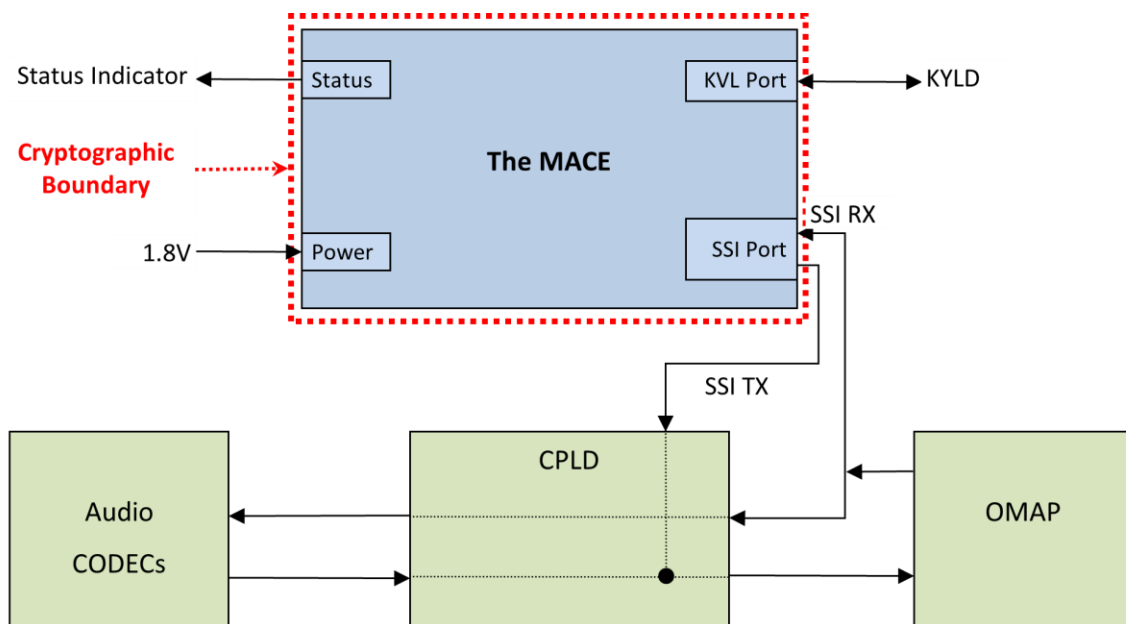


Figure 3 – Cryptographic Boundary for the MACE

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

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

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
5185912T05	5185912	R01.15.02 with [AES256 R01.00.00 or AES256 R01.00.01]	5185912 Family	N/A
5185912Y03	5185912	R01.15.02 with [AES256 R01.00.00 or AES256 R01.00.01]	5185912 Family	N/A
5185912Y05	5185912	R01.15.02 with [AES256 R01.00.00 or AES256 R01.00.01]	5185912 Family	N/A

Table 2: Tested Module Identification – Hardware

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	R01.00.00	R01.15.02	A2261
AES256	R01.00.01	R01.15.02	A2262

2.3 Excluded Components

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

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Types of Services	Status Indicator
Approved	Operating in approved mode	Approved	FIPS Status: 0x03 as a result of Module Info Service

Table 4: Modes List and Description

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 3.

The approved mode is indicated by using the “Module Status” service. The result from this service will return:

```
FIPS Status: 0x03
```

This indicates that the module is operating in Level 3 Approved Mode.

When the module is in the approved operating mode, the “Module Info” service can be used to verify the firmware version matches an approved version listed on NIST’s website:

<https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules>

Mode Change Instructions and Status:

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

1. Upon first access, the CCO will use the default passwords, provided by Motorola Solutions in a separate communication, to change the password based on the rules defined in Section 4.1.
2. Disable Motorola Data Communication Over the Air Rekeying (MDC OTAR)
3. Disable OTAR Generate Key-Loss-Key (KLK)
4. Enable KVL – FIPS Level 3 Approved Mode
5. Disable Infinite UKEK Retention
6. Activate the Periodic self-test timer interval
7. Then the Operational Crypto Officer (OCO) will need to change their password, as defined in Section 4.1

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 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’s validation and zeroizes all SSPs except those entered at manufacturing. The Module is then in a non-compliant state.

2.5 Algorithms

Approved Algorithms:

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

Algorithm	CAVP Cert	Properties	Reference
AES-CBC, AES-CFB8, AES-ECB, AES-OFB	A2261, A2262, A2260	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-GCM	A2262	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.2 Key Length - 256 Tag Length - 128 IV Length - IV Length: 96 Payload Length - Payload Length: 256-512 Increment 128 AAD Length - AAD Length: 256-512 Increment 128	SP 800-38D
AES-KW	A2263	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 256 Payload Length - Payload Length: 128-256 Increment 64	SP 800-38F
AES-KW	A2264	Direction - Decrypt Cipher - Cipher Key Length - 256 Payload Length - Payload Length: 128-256 Increment 64	SP 800-38F
Counter DRBG	A6380	Prediction Resistance - No Supports Reseed - No Mode - AES-256 Derivation Function Enabled - Yes Additional Input - Additional Input: 0 Entropy Input - Entropy Input: 256-1024 Increment 128 Nonce - Nonce: 128-512 Increment 128 Personalization String Length - Personalization	SP 800-90A Rev. 1

Algorithm	CAVP Cert	Properties	Reference
		String Length: 0 Returned Bits - 128	
ECDSA KeyGen (FIPS186-4)	A655	Curve - P-384 Secret Generation Mode - Extra Bits	FIPS 186-4
HMAC-SHA2-384	HMAC 1796	Key sizes < block size - Yes Key sizes > block size - No Key size = block size - No	FIPS 198-1
KAS-ECC Sp800-56Ar3	A2266	Domain Parameter Generation Methods - P-384 Function - Key Pair Generation, Partial Validation iutId - A1B2C3D4E5 Scheme - ephemeralUnified - KAS Role - Initiator, Responder KDF Methods - oneStepKdf - Auxiliary Function Methods - Auxiliary Function Name - SHA2-384 Fixed Info Pattern - algorithmId uPartyInfo vPartyInfo Fixed Info Encoding - Concatenation Key Length - 384	SP 800-56A Rev. 3
RSA SigVer (FIPS186-2)	RSA 396	Signature Type - PKCS 1.5 Modulo - 2048 Hash Pair - Hash Algorithm - SHA2-256	FIPS 186-4
RSA SigVer (FIPS186-5)	A5253	Hash Pair - Hash Algorithm - SHA2-256 Modulo - 2048 Signature Type - pkcs1v1.5 Fixed Public Exponent - 010001 Public Exponent Mode - fixed	FIPS 186-5
SHA2-256	SHS 817	Message Length - Message Length: 0-51200 Increment 8 Supports Bit-Oriented Messages - No Supports Empty Message - Yes	FIPS 180-4
SHA2-384	SHS 2399	Message Length - Message Length: 8-102400 Increment 8 Supports Bit-Oriented Messages - No Supports Empty Message - No	FIPS 180-4

Table 5: Approved Algorithms

Vendor-Affirmed Algorithms:

The Module implements the Vendor Affirmed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
CKG1	Key Type:Asymmetric and Symmetric	N/A	SP800-133rev2 Sections 4, Example 1 and IG D.H
CKG - IDK	Key Type:Symmetric	N/A	SP800-133rev2 Sections 6.3 #2 and IG D.H

Table 6: Vendor-Affirmed Algorithms

Non-Approved, Allowed Algorithms:

The Module implements the Non-Approved, but Allowed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
KTS2	key unwrapping only:Key establishment methodology provides 256 bits strength	AES CBC or OFB Cert. #A2261 or #A2262	IG D.G
KTS3	key unwrapping only:Key establishment methodology provides 256 bits strength	AES CFB8 Cert. #A2260	IG D.G

Table 7: Non-Approved, Allowed Algorithms

Non-Approved, Allowed Algorithms with No Security Claimed:

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

Name	Caveat	Use and Function
AES MAC	No security claimed - AES MAC is used as part of OTAR but is considered obfuscation	[IG 2.4.A] P25 AES OTAR. AES MAC is applied directly to the plaintext OTAR key components and then KTS encryption is performed on the OTAR key components and decrypted within the module using AES KW Cert. #A2264

Table 8: Non-Approved, Allowed Algorithms with No Security Claimed

Non-Approved, Not Allowed Algorithms:

The module does not implement any Non-Approved Algorithms, Not Allowed in the Approved Mode of Operation.

N/A for this module.

2.6 Security Function Implementations

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

Name	Type	Description	Properties	Algorithms
A2260 Decryption	BC- UnAuthDecrypt	Block Cipher		AES-CFB8: (A2260) AES-OFB: (A2260)
A2260 Encryption	BC- UnAuthEncrypt	Block Cipher		AES-CFB8: (A2260) AES-OFB: (A2260)
A2261 Decryption	BC- UnAuthDecrypt	Block Cipher		AES-CBC: (A2261) AES-ECB: (A2261) AES-OFB: (A2261)
A2261 Encryption	BC- UnAuthEncrypt	Block Cipher		AES-CBC: (A2261) AES-ECB: (A2261) AES-OFB: (A2261)
A2262 Authenticated Decryption	BC-AuthDecrypt	Authenticated Decrypt, Message Authentication		AES-GCM: (A2262) AES-CBC: (A2262)
A2262 Authenticated Encryption	BC-AuthEncrypt	Authenticated Encrypt, Message Authentication		AES-GCM: (A2262) AES-CBC: (A2262)
A2262 Decryption	BC- UnAuthDecrypt	Block Cipher		AES-CBC: (A2262) AES-ECB: (A2262) AES-OFB: (A2262)
A2262 Encryption	BC- UnAuthEncrypt	Block Cipher		AES-CBC: (A2262) AES-ECB: (A2262) AES-OFB: (A2262)
A2263 Decryption	BC-AuthDecrypt	Authenticated Decrypt for storing SSPs		AES-KW: (A2263) AES-CBC: (A2261, A2262)

Name	Type	Description	Properties	Algorithms
A2263 Encryption	BC-AuthEncrypt	Authenticated Encrypt for storing SSPs		AES-KW: (A2263) AES-CBC: (A2261, A2262)
Entropy	ENT-ESV	Entropy Source		
HMAC	MAC	Message Authentication		HMAC-SHA2-384: (HMAC 1796) SHA2-384: (SHS 2399)
IDKGen	CKG	Symmetric Key Generation		Counter DRBG: (A6380) CKG - IDK: () SHA2-256: (SHS 817)
KAS	KAS-Full	ECC Ephemeral Unified , (Initiator, Responder), KPG, Partial, oneStepKdf (SP800-56Cr1) IG D.F Scenario 2 path 2	Caveat:Key establishment methodology provides 192 bits strength Publication:[IG D.F]	KAS-ECC Sp800-56Ar3: (A2266) SHA2-384: (SHS 2399)
KeyGen1	CKG	Symmetric Key Generation		AES-CFB8: (A2260) AES-KW: (A2264) Counter DRBG: (A6380) CKG1: () Key Type: Asymmetric and Symmetric
KeyGen2	AsymKeyPair-KeyGen	Asymmetric Key Pair Generation		ECDSA KeyGen (FIPS186-4): (A655) CKG1: () Key Type: Asymmetric and Symmetric
KTS1	KTS-Unwrap	Key Transport - Unwrapping	Caveat:Key establishment	AES-KW: (A2264)

Name	Type	Description	Properties	Algorithms
			methodology provides 256 bits strength Publication:[IG D.G]	
KTS2	KTS-Unwrap	Key Transport - Unwrapping	Caveat:Key establishment methodology provides 256 bits strength Publication:[IG D.G]	AES-CBC: (A2261, A2262) AES-OFB: (A2261, A2262)
KTS3	KTS-Unwrap	Key Transport - Unwrapping	Caveat: Key establishment methodology provides 256 bits strength Publication:[IG D.G]	AES-CFB8: (A2260)
OTAR AES MAC	MAC	AES MAC is used as part of OTAR but is considered obfuscation	Note:No security claimed	AES MAC: ()
RNG	DRBG	AES-256 CTR Deterministic RBG		Counter DRBG: (A6380)
SHS2399	SHA	Secure Hash Standard Message Digest Generation		SHA2-384: (SHS 2399)
SHS817	SHA	Secure Hash Standard Message Digest Generation		SHA2-256: (SHS 817)
SigVer1	DigSig-SigVer	Digital Signature Verification		RSA SigVer (FIPS186-5): (A5253)
SigVer2 (Legacy)	DigSig-SigVer	Digital Signature Verification		RSA SigVer (FIPS186-2): (RSA 396)

Table 9: Security Function Implementations

2.7 Algorithm Specific Information

AES GCM IV Generation

The MACE, per IG C.H Scenario 2, generates GCM IVs randomly as specified in SP800-38D section 8.2.2 using approved DRBG (Cert #A6380) and the IV length is 96 bits.

Legacy Use

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

Key Agreement Scheme

KAS-ECC [56Ar3] Scheme: Ephemeral Unified - Per [IG] D.F Scenario 2 path (2), compliant key agreement scheme where testing is performed end-to-end for the shared secret computation and a KDF compliant with onestep KDF without key confirmation.

2.8 RBG and Entropy

Cert Number	Vendor Name
E132	Motorola Solutions Inc

Table 10: Entropy Certificates

The Module uses the following entropy sources:

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Motorola Advanced Crypto Engine (MACE) Entropy Source	Physical	Atmel 5185912	1 bit	0.138262	N/A

Table 11: Entropy Sources

2.9 Key Generation

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

2.10 Key Establishment

The appropriate public key validation assurance is implemented. The module checks the validity of the ECC P-384 ephemeral public key as defined in SP 800-56Arev3 Section #5.6.2.3.4 ECC Partial Public-Key Validation Routine. The module rejects the public key and returns an error. There are no actions needed by the operator.

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

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

Physical Port	Logical Interface(s)	Data That Passes
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.
Self-test Indicator	Status Output	This interface provides status output to indicate all power-up self-tests complete successfully.
Power	Power	This interface powers all circuitries.
Key Loading Port (KYLD)	Data Input Data Output Control Input Status Output	This interface provides the input and output to the Key Variable Loader (KVL)

Table 12: Ports and Interfaces

Note: The module does not support Control Output.

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
AM1	Identity-based. Configuration Crypto-Officer (CCO) Password: a 10-digit hexadecimal password is authenticated to gain access to CCO services. It should be noted that after authenticating, this password may be changed at any time through the SSI Port.	SHA2-256 (SHS 817)	The probability of a successful random attempt is 1 in $\{16^{10}\}$ which is 1 in 1,099,511,627,776.	After the CCO password has been incorrectly entered 15 consecutive times, the Module will erase all CSPs, reset all passwords back to their default and must be reinitialized. The strength per minute is 15 in 1,099,511,627,776
AM2	Identity-based. Operational Crypto-Officer (OCO) Password: a 10-digit hexadecimal password is authenticated to gain access to OCO services. It should be noted that after authenticating, this password may be	SHA2-256 (SHS 817)	The probability of a successful random attempt is 1 in $\{16^{10}\}$ which is 1 in 1,099,511,627,776.	After the OCO password has been incorrectly entered 15 consecutive times, the Module will erase all CSPs, reset the all passwords back to their default and must be reinitialized. The strength per minute is 15 in 1,099,511,627,776

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
	changed at any time through the SSI Port.			

Table 13: Authentication Methods

4.2 Roles

The Module supports two distinct operator roles, the Configuration Cryptographic Officer (CCO) and the Operational Crypto Officer (OCO). In addition, the Module supports services which do not require authentication (UA).

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

The Module does not support concurrent operators.

Name	Type	Operator Type	Authentication Methods
Configuration Crypto Officer	Identity	CCO	AM1
Operational Crypto Officer	Identity	OCO	AM2

Table 14: Roles

4.3 Approved Services

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

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

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Change Active Keyset	Modify the currently active keyset used for selecting keys for encryption/decryption services.	Approved mode	Keyset Index	Changed the active keyset as requested. Success/failure status.	None	Operational Crypto Officer
Change CCO Password (AM1)	Modify the current password used to identify and authenticate the CCO role using AM1.	Approved mode indicator and service	Password	Updated the CCO password. Success/failure status.	A2260 Decryption SHS817 KTS3	Configuration Crypto Officer - CCO PWD (AM1): Z - KEK: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
		status output				- PEK: E - PWD Hash: W,Z - TEK: Z
Change OCO Password (AM2)	Modify the current password used to identify and authenticate the OCO role using AM2.	Approved mode	Password	Updated the OCO password. Success/failure status.	A2260 Encryption A2260 Decryption KeyGen1 SHS817	Operational Crypto Officer - KEK: Z - KPK: G,E,Z - OCO PWD (AM2): Z - PEK: E - PWD Hash: W,Z - TEK: Z - UKKPK: E
Clear Error Log	Clears the history of error events	Approved mode	Command In	Success/Failure status.	None	Configuration Crypto Officer Operational Crypto Officer
Decrypt	Decrypt digital voice or data using AM2.	Approved mode	Ciphertext	Plaintext. Success/failure status.	A2260 Decryption A2261 Decryption A2262 Decryption KTS2 A2262 Authenticated Decryption	Operational Crypto Officer - KPK: E - TEK: E
Encrypt	Encrypt digital voice or data using AM2.	Approved mode	Plaintext	Ciphertext. Success/failure status.	A2260 Encryption A2261 Encryption A2262 Encryption A2262 Authenticated Encryption KTS2	Operational Crypto Officer - DRBG-El/Seed: E - DRBG-State: E - KPK: E - TEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Extract Error Log	Provide the history of error events.	Approved mode	Command In	Error logs out. Success/Failure status.	None	Configuration Crypto Officer Operational Crypto Officer
Generate Entropy	Generate Entropy for use inside the MACE	Approved mode	Power On	DRBG Seed	Entropy RNG	Unauthenticated - DRBG- EI/Seed: G - DRBG- nonce: G
Generate Keypair	Generate Asymmetric keys within the module using AM2.	Approved mode	Command in	Key stored inside Module, Success/Failure status.	A2263 Encryption KeyGen2 KAS	Operational Crypto Officer - BKK: E - DH-Priv: G - DH-Pub: G - DRBG-State: G,E - PKPK: E
Generate Signature	Generate HMAC-SHA2-384 signature	Approved mode	Command In	Signature, Success/failure status.	A2260 Encryption A2260 Decryption SHS2399 HMAC	Operational Crypto Officer - KPK: E - TEK: E
Import Keys Over KYLD Interface	Imports keys into the MACE encrypted using AM2.	Approved mode	Ciphertext	Key Stored inside the Module. Success/failure status.	A2260 Encryption A2260 Decryption KTS3	Operational Crypto Officer - BKK: E - KEK: W,Z - KPK: E - TEK: W,Z
Key/Keyset Check	Obtain status information about a specific key	Approved mode	Command In	Status information for key returned. Success/Failure Status	None	Operational Crypto Officer
Module Configuration	Set configuration parameters used to specify module behavior using AM1 or AM2	Approved mode	Configuration parameters	Updated module configuration.	KeyGen1	Configuration Crypto Officer - CCO PWD (AM1): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
				Success/failure status.		- KEK: Z - KPK: G,Z - PWD Hash: Z - TEK: Z - UKKPK: E Operational Crypto Officer - KEK: Z - KPK: G,Z - OCO PWD (AM2): Z - PWD Hash: Z - TEK: Z - UKKPK: E
Module Status	Provide module version, firmware version, FIPS status	Approved mode	Command In	Module HW version, Firmware version, and FIPS status	None	Unauthenticated
On Demand Self Tests	Perform on demand self-testing of algorithms within the MACE.	Approved Mode	Command In	Success/Failure status	A2260 Decryption A2260 Encryption A2261 Decryption A2261 Encryption A2262 Authenticated Decryption A2262 Authenticated Encryption A2262 Decryption A2262 Encryption A2263 Decryption A2263 Encryption	Operational Crypto Officer

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Entropy HMAC KAS KeyGen1 KeyGen2 KTS1 KTS2 KTS3 RNG SHS2399 SHS817 SigVer1 SigVer2 (Legacy)	
Perform Key Agreement Process	Perform a key agreement process to create an ECDH Shared Secret using AM2.	Approved mode	Command In	Generate Keys stored in the Module. Success/failure status	A2261 Encryption A2261 Decryption A2262 Encryption A2262 Decryption KeyGen2 RNG KAS	Operational Crypto Officer - BKK: E - DH-CLI-Pub: W,E - DH-Priv: G,E - DH-Pub: G,R,E - DH-SS: G,E - DRBG-State: G,E - PKPK: G,E
Privileged APCO OTAR	Import, modify and query the keys using AM2.	Approved mode	Encrypted Key	Store Keys internal to the Module. Success/Failure Indication.	KTS1 KTS2 OTAR AES MAC	Operational Crypto Officer - DH-SS: - KEK: W,E - KPK: E - TEK: W,E
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	Approved mode	Firmware image	The MACE is upgraded to new firmware.	A2261 Decryption A2262 Decryption SigVer1	Configuration Crypto Officer - BKK: Z - CCO PWD (AM1): Z - DH-CLI-Pub: Z - DH-Priv: Z - DH-Pub: Z - DH-SS: Z - DRBG-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	firmware image being loaded before it is allowed to be executed.					EI/Seed: Z - DRBG-nonce: Z - DRBG-State: Z - FW-LD-Pub: E,Z - IDK: E,Z - IDK Block: E,Z - KEK: Z - KPK: Z - PEK: Z - PKPK: Z - PWD Hash: Z - TEK: Z - UKKPK: Z Operational Crypto Officer - BKK: Z - DH-CLI-Pub: Z - DH-Priv: Z - DH-Pub: Z - DH-SS: Z - DRBG-EI/Seed: Z - DRBG-nonce: Z - DRBG-State: Z - FW-LD-Pub: E,Z - IDK: E,Z - IDK Block: E,Z - KEK: Z - KPK: Z - OCO PWD (AM2): Z - PEK: Z - PKPK: Z - PWD Hash: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TEK: Z - UKKPK: Z
Reset	Reset/power cycle the MACE.	Approved mode	Command In	Reset the MACE.	RNG	Unauthenticated - DH-Priv: Z - DH-SS: Z - DRBG-El/Seed: G,Z - DRBG-nonce: G,Z - DRBG-State: G,Z
Self-Tests	Perform module self-tests comprised of cryptographic algorithm tests, firmware integrity test, and critical functions test. Initiated by module reset or transition from power off state to power on state using UA.	Approved mode indicator and service status output	Power on/Command In	Success/Reset.	A2260 Decryption A2260 Encryption A2261 Decryption A2261 Encryption A2262 Authenticated Decryption A2262 Authenticated Encryption A2262 Decryption A2262 Encryption A2263 Decryption A2263 Encryption Entropy HMAC KAS KeyGen1 KeyGen2 KTS1 KTS2 KTS3 RNG SHS2399	Unauthenticated - FW-LD-Pub: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SHS817 SigVer1 SigVer2 (Legacy)	
Symmetric Key Generation	Generate symmetric [135] keys within the Module using AM2.	Approved mode	Command in	Key Stored inside Module. Success/failure status	A2261 Encryption A2261 Decryption A2262 Encryption A2262 Decryption KeyGen1 IDKGen RNG	Operational Crypto Officer - BKK: E - DRBG-State: G,E - IDK: G,Z - IDK Block: E,Z - IDK ROM: E,Z - KPK: G,Z - PKPK: G,Z
Validate CCO Password (AM1)	Validate the current password used to identify and authenticate the CCO role using AM1.	Approved mode	Password	Successful authentication will allow access to the services allowed for CO role.	A2260 Decryption SHS817 KTS3	Unauthenticated - CCO PWD (AM1): Z - KEK: Z - PEK: E - PWD Hash: W,Z - TEK: Z
Validate OCO Password (AM2)	Validate the current password used to identify and authenticate the OCO role using AM2.	Approved mode	Password	Successful authentication will allow access to the services allowed for User role	A2260 Encryption A2260 Decryption SHS817 KTS3	Unauthenticated - KEK: Z - KPK: G,E,Z - OCO PWD (AM2): Z - PEK: E - PWD Hash: W,Z - TEK: Z - UKKPK: E
Zeroize all keys and passwords	Zeroize the KPK and all keys and CSPs in the key database and causes a new KPK to be generated. Resets the	Approved mode	Command In	Keys marked for deletion. Success/failure status	KeyGen1	Configuration Crypto Officer - CCO PWD (AM1): Z - DH-Priv: Z - DRBG-State: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	passwords to the factory default.					- KEK: Z - KPK: G,Z - PKPK: Z - PWD Hash: Z - TEK: Z - UKKPK: E - Operational Crypto Officer - DH-Priv: Z - DRBG-State: G,E - KEK: Z - KPK: G,Z - OCO PWD (AM2): Z - PKPK: Z - PWD Hash: Z - TEK: Z - UKKPK: E
Zeroize Keys	Mark key for deletion using AM2.	Approved mode	Command In	Keys marked for deletion. Success/failure status.	KeyGen1	Operational Crypto Officer - DRBG-State: G,E - KEK: Z - KPK: G,Z - TEK: Z - UKKPK: E

Table 15: Approved Services

4.4 Non-Approved Services

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

N/A for this module.

4.5 External Software/Firmware Loaded

This module supports loading of external firmware via the Program Update service. Execution of the successfully loaded firmware is only effective after the next reset of the security module. Any firmware loaded into the module other than that listed in Section 2.2 Tested and Vendor Affirmed Module

Version and Identification, is outside the scope of this Security Policy and requires a separate FIPS 140-3 validation.

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

5 Software/Firmware Security

5.1 Integrity Techniques

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

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

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

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

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

Type of Operational Environment: Limited

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

7 Physical Security

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

7.1 Mechanisms and Actions Required

The 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 the temperature range of -40 to 85 degrees Celsius. No assurance of the epoxy hardness is claimed for this physical security mechanism outside of this range. The 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.

Mechanism	Inspection Frequency	Inspection Guidance
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.

Table 16: Mechanisms and Actions Required

7.5 EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-38.1°C	EFP	Shutdown - A tamper flag is raised, a wake-up reset of the product is triggered.
HighTemperature	101.4°C	EFP	Shutdown - A tamper flag is raised, a wake-up reset of the product is triggered.
LowVoltage	1.65V VDDCORE / 1.35V VVDBU	EFP	Shutdown - A general reset of the chip is asserted.
HighVoltage	2.04V VDDCORE / 2.293V VVDBU	EFP	Shutdown- A tamper flag is raised, a wake-up reset of the product is triggered.

Table 17: EFP/EFT Information

7.6 Hardness Testing Temperature Ranges

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

Table 18: Hardness Testing Temperatures

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

8 Non-Invasive Security

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

9 Sensitive Security Parameters Management

9.1 Storage Areas

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

Table 19: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input encrypted on the BKK through the KVL (A2260 AES-OFB) (I2)	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Automated	Electronic	KTS3
Input encrypted on the IDK (A2261, A2262 AES-CBC) (I1)	Application Software (outside)	Flash Memory (S2)	Encrypted	Automated	Electronic	KTS2
Input encrypted on the PEK using AES KTS (A2260 AES-CFB8) (I3).	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Automated	Electronic	KTS3
Input encrypted on the TEK (A2261, A2262 AES-OFB) (I5)	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Automated	Electronic	KTS2
Input encrypted using ECDH Key Agreement Process (I6).	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Automated	Electronic	KAS
Input encrypted using SP800-38F	OTAR (outside)	Flash Memory -	Encrypted	Automated	Electronic	KTS1

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
AES key transport by the KEK (A2264) (I4)		Encrypted (S3)				
Output in plaintext public key (O1)	Flash Memory - Encrypted (S3)	Application Software (outside)	Plaintext	N/A	Electronic	ECDSA KeyGen (FIPS186-4) (A655)

Table 20: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Z1	Zeroized by the "Program Update" service.*	SSPs zeroized upon loading of new firmware.	Yes
Z10	Zeroized by the "CCO Validate Password" service.	CO password zeroized after too many failed login attempts	Yes
Z11	Zeroized by the "CCO Change Password" service.	Old User password zeroized as new CO password set	Yes
Z2	Zeroized by module power cycle or hard reset.*	SSPs in volatile memory zeroized.	Yes
Z3	Zeroized by the "Zeroize Keys" service.	TEK/KEKs zeroized upon request	Yes
Z4	Zeroized by the "Zeroize all Keys and Password" service.	Old CO password zeroized as new CO password set	Yes
Z5	Zeroized by the "OCO Validate Password" service.	CO password zeroized after too many failed login attempts	Yes
Z6	Zeroized by the "OCO Change Password" service.	Old User password zeroized as new CO password set	Yes
Z7	Zeroized by the "Module Configuration" service.	User password zeroized after too many failed login attempts	Yes
Z8	Zeroized by the "Privileged APCO OTAR" service.	TEK/KEKs zeroized upon request	Yes
Z9	Zeroized by the "KVL Import Key" service.	TEK/KEKs zeroized upon request	Yes

Table 21: SSP Zeroization Methods

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

9.4 SSPs

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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
BKK	A 256-bit AES OFB (A2260) key used to decrypt keys loaded from KVL.	256 - 256	Symmetric Key - CSP	Pre-loaded		A2260 Decryption
CCO PWD (AM1)	8-32 ASCII characters CO password.	N/A - N/A	Authentication - CSP			A2260 Encryption A2260 Decryption
DH-CLI-Pub	The Elliptic Curve (EC) Diffie-Hellman (DH) public key for the other party, used for establishing a shared secret over an insecure channel.	768 - 192	Asymmetric Public Key - PSP			KAS
DH-Priv	The Elliptic Curve Diffie-Hellman (DH) private key used for establishing a shared secret over an insecure channel.	384 - 192	Asymmetric Private Key - CSP	KeyGen2		RNG KAS
DH-Pub	The Elliptic Curve (EC) Diffie-Hellman (DH) public key, used for establishing a shared secret over an insecure channel.	768 - 192	Asymmetric Public Key - PSP	KeyGen2		KAS
DH-SS	The Elliptic Diffie-Hellman (DH) Shared Secret (SS) is established as a part of DH key agreement scheme.	384 - 192	Symmetric Key - CSP		KAS	KAS
DRBG-El/Seed	Internally generated by the HWRNG	1856 - N/A	N/A - CSP	Entropy		RNG
DRBG-nonce	Internally generated by the HWRNG	960 - N/A	N/A - CSP	Entropy		RNG
DRBG-State	CTR_DRBG (A6380) internal state: V (128 bits) and Key (AES 256)	256 - 256	N/A - CSP	RNG		KeyGen1 KeyGen2

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
FW-LD-Pub	2048-bit RSA key used to validate the signature of the firmware image during FW integrity and FW Loading before it is allowed to be executed.	2048 - 112	Asymmetric Public Key - PSP	Pre-loaded		SigVer1 SigVer2 (Legacy)
IDK	A 256-bit AES CBC (A2261 or A2262)) key used to decrypt downloaded firmware images.	256 - 256	Symmetric Key - CSP	IDKGen		A2261 Decryption A2262 Decryption
IDK Block	A 256-bit AES CBC key (A2261 or A2262) used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK ROM	256 - 256	Symmetric Key - CSP	Pre-loaded		IDKGen
IDK ROM	A 256-bit AES CBC key (A2261 or A2262) used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK Block	256 - 256	Symmetric Key - CSP	Pre-loaded		IDKGen
KEK	256-bit AES-KW (A2264) keys used for encryption of keys in key transport operation	256 - 256	Symmetric Key - CSP			KTS1
KPK	256 bit AES CFB-8 (A2260) key used to encrypt all TEKs and KEKs stored in the flash.	256 - 256	Symmetric Key - CSP	KeyGen1		A2260 Encryption A2260 Decryption
OCO PWD (AM2)	8-32 ASCII characters User password.	N/A - N/A	Authentication - CSP			A2260 Encryption A2260 Decryption
PEK	256-bit AES-CFB8 (A2260) key used for decrypting	256 - 256	Symmetric Key - CSP	Pre-loaded		A2260 Encryption A2260 Decryption

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	passwords during password validation					
PKPK	256-bit AES KW (A2263) used to store encrypted, the ECDH generated private key	256 - 256	Symmetric Key - CSP	KeyGen1		A2263 Encryption A2263 Decryption
PWD Hash	256-bit password hash stored in the non-volatile memory.	256 - 128	Authentication - CSP	SHS2399		
TEK	256-bit AES (A2261 or A2262)) keys used for enabling secure communication with target devices.	256 - 256	Symmetric Key - CSP			KTS2
UKPKK	256 bit AES CFB8 (A2260) Key used for encrypting the KPK in flash.	256 - 256	Symmetric Key - CSP	Pre-loaded		A2260 Encryption A2260 Decryption

Table 22: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
BKK	Input encrypted on the IDK (A2261, A2262 AES-CBC) (I1)	System Memory (S1):Encrypted Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	KEK:Decrypts TEK:Decrypts PKPK:Encrypts PKPK:Decrypts
CCO PWD (AM1)	Input encrypted on the PEK using AES KTS (A2260 AES-CFB8) (I3).	System Memory (S1):Encrypted Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	PEK:Encrypted with PWD Hash:Hashed with
DH-CLI-Pub	Input encrypted using ECDH Key Agreement Process (I6).	System Memory (S1):Encrypted	When module is reset	Z1 Z2	DH-Priv:Paired With DH-SS:Used to establish
DH-Priv		System Memory (S1):Encrypted Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z2	PKPK:Encrypted with DH-SS:Used to establish DH-CLI-Pub:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
DH-Pub	Output in plaintext public key (O1)	System Memory (S1):Encrypted Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	
DH-SS		System Memory (S1):Encrypted	When module is reset	Z1 Z2	DH-Priv:Generated by DH-CLI-Pub:Generated by
DRBG-El/Seed		System Memory (S1):Encrypted	When module is reset	Z2	
DRBG-nonce		System Memory (S1):Encrypted	When module is reset	Z2	
DRBG-State		System Memory (S1):Encrypted	When module is reset	Z2	DRBG-El/Seed:Derived From DRBG-nonce:Derived From
FW-LD-Pub		System Memory (S1):Encrypted Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	
IDK		System Memory (S1):Encrypted	When module is reset	Z2	IDK ROM:Derived From IDK Block:Derived From
IDK Block		System Memory (S1):Encrypted Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	IDK ROM:Used With IDK:Generates
IDK ROM		System Memory (S1):Encrypted Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	IDK Block:Used With IDK:Generates
KEK	Input encrypted on the BKK through the KVL (A2260 AES-OFB) (I2) Input encrypted using SP800-38F AES key transport by the KEK (A2264) (I4)	System Memory (S1):Encrypted Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8 Z9	KPK:Encrypted with

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
				Z10 Z11	
KPK		System Memory (S1):Encrypted Flash Memory (S2):Plaintext	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7 Z8 Z9 Z10 Z11	DRBG- State:Derived From UKKPK:Encrypted with KEK:Encrypts TEK:Encrypts
OCO PWD (AM2)	Input encrypted on the PEK using AES KTS (A2260 AES-CFB8) (I3).	System Memory (S1):Encrypted Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	PEK:Encrypted with PWD Hash:Hashed with
PEK	Input encrypted on the IDK (A2261, A2262 AES-CBC) (I1)	System Memory (S1):Encrypted Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	IDK:Encrypted with CCO PWD (AM1):Encrypts CCO PWD (AM1):Decrypts OCO PWD (AM2):Encrypts OCO PWD (AM2):Decrypts
PKPK		System Memory (S1):Encrypted Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z2	BKK:Encrypted with DH-Priv:Encrypts DRBG- State:Derived From
PWD Hash		System Memory (S1):Encrypted Flash Memory - Encrypted (S3):Encrypted	When module is reset	Z1 Z3 Z4 Z5 Z6 Z7	CCO PWD (AM1):Hash of OCO PWD (AM2):Hash of
TEK	Input encrypted on the BKK through the KVL (A2260 AES-	System Memory (S1):Encrypted Flash Memory -	When module is reset	Z1 Z2 Z3	KPK:Encrypted with

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	OFB) (I2) Input encrypted on the TEK (A2261, A2262 AES-OFB) (I5)	Encrypted (S3):Encrypted		Z4 Z5 Z6 Z7 Z8 Z9 Z10 Z11	
UKKPK		System Memory (S1):Encrypted Flash Memory (S2):Plaintext	When module is reset	Z1 Z2	KPK:Encrypts

Table 23: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

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

Pre-operational self-tests are available on demand by power cycling the MACE. In addition, pre-operational self-tests are periodically performed by the MACE as configured by the operator during the module configuration as shown in Section 11.1 Installation, Initialization, and Startup Procedures. 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 after periodic self-test ends and will execute when the I/O buffer is emptied. The MACE logs the most recent self-test errors to the internal flash; the operator (CO) can extract the error logs using Extract Error Log service.

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity	SHA2-256 (Cert. #817), RSA-2048 (Cert. #396, #A5253)	KAT	SW/FW Integrity	Success or ES2 on failure	A digital signature is generated over the Boot Block, Base firmware (Cert. #A5253), and all Drop-in algorithms (Cert. #396) when it is built using SHA2-256 (Cert. #817), 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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
					matches then the test passes otherwise it fails.

Table 24: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CFB8 (A2260) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-CFB8 256 Decryption	Bootup
AES-CFB8 (A2260) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-CFB8 256 Encryption	Bootup
AES-ECB (2262) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-ECB 256 Decryption	Bootup
AES-ECB (A2261) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-ECB 256 Decryption	Bootup
AES-ECB (A2261) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-ECB 256 Encryption	Bootup
AES-ECB (A2262) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-ECB 256 Encryption	Bootup
AES-GCM 256 Authenticated Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-GCM 256 Authenticated Decryption	Bootup
AES-GCM 256 Authenticated Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-GCM 256 Authenticated Encryption	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-KW (A2263) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	Message Decryption	Bootup
AES-KW (A2263) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	Message Encryption	Bootup
AES-KW (A2264) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	Message Decryption	Bootup
Counter DRBG (A6380)	AES-256 CTR	KAT	CAST	Success or ES1 on failure	AES-256 CTR_DRBG instantiation, generate, and reseed KATs performed before the first random data generation.	Bootup
ECDSA KeyGen (FIPS186-4) (A655)	ECDSA KeyGen	PWCT	PCT	Success or ES3 on failure	ECDSA P-384 Pair-wise Consistency Test	Bootup
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	Fault Detection	CAST	Success or ES1 on failure	Designed to detect a large loss of entropy that might occur as a result of some physical failure or environmental change affecting the noise source	Bootup
Entropy 90B Start-up Repetition Count Test (RCT)	Repetition Count Test	Fault Detection	CAST	Success or ES1 on failure	Designed to quickly detect catastrophic failures that cause the noise source to become \"stuck\" on a	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					single output value for a long period of time.	
Firmware Load	2048-bit RSA Signature Verification/SHA2-256 RSA (Cert. #A5253)	KAT	SW/FW Load	Success or ES2 on failure	A digital signature is generated over the code when it is built using SHA-256 and RSA-2048. The digital signature is verified upon download into the MACE.	loading a new firmware image
HMAC-SHA2-384 (HMAC 1796)	HMAC-SHA2-384	KAT	CAST	Success or ES1 on failure	HMAC-SHA2-384	Bootup
KAS-ECC Sp800-56Ar3 (A2266)	KAS-ECC SP800-56Ar3	KAT	CAST	Success or ES1 on failure	Per IG D.F, separately tested KAS Shared Secret generation with P-384 and SP800-56Cr2 one-step KDA.	Bootup
RSA SigVer (FIPS186-5) (A5253)	RSA-2048 SigVer	KAT	CAST	Success or ES1 on failure	2048-bit RSA PKCSv1.5 Signature Verification, performed before Pre-Operational FW integrity tests. Inclusive for 186-2 (Cert. #396)	Bootup
SHA2-256 (SHS 817)	SHA2-256	KAT	CAST	Success or ES1 on failure	SHA2-256	Bootup
SHA2-384 (SHS 2399)	SHA2-384	KAT	CAST	Success or ES1	SHA2-384	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
				on failure		

Table 25: Conditional Self-Tests

10.3 Periodic Self-Test Information

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

Table 26: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CFB8 (A2260) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CFB8 (A2260) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-ECB (2262) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-ECB (A2261) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-ECB (A2261) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-ECB (A2262) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-GCM 256 Authenticated Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-GCM 256 Authenticated Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-KW (A2263) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-KW (A2263) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-KW (A2264) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
Counter DRBG (A6380)	KAT	CAST	On Demand/Periodically	Manually/programmatically
ECDSA KeyGen (FIPS186-4) (A655)	PWCT	PCT	On Demand/Periodically	Manually/programmatically
Entropy 90B Start-up Adaptive Proportion Test (APT)	Fault Detection	CAST	On Demand/Periodically	Manually/programmatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Entropy 90B Start-up Repetition Count Test (RCT)	Fault Detection	CAST	On Demand/Periodically	Manually/programmatically
Firmware Load	KAT	SW/FW Load		
HMAC-SHA2-384 (HMAC 1796)	KAT	CAST	On Demand/Periodically	Manually/programmatically
KAS-ECC Sp800-56Ar3 (A2266)	KAT	CAST	On Demand/Periodically	Manually/programmatically
RSA SigVer (FIPS186-5) (A5253)	KAT	CAST	On Demand	Manually
SHA2-256 (SHS 817)	KAT	CAST	On Demand/Periodically	Manually/programmatically
SHA2-384 (SHS 2399)	KAT	CAST	On Demand/Periodically	Manually/programmatically

Table 27: Conditional Periodic Information

Conditional self-tests are periodically performed by the MACE every X hours, where X is configured by the operator during module configuration (1 minute to 712,800 minutes). 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 end the periodic self-test executed when the I/O buffer is emptied.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ES1	The 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.	Reboot/Power cycle the module	Device will not respond to authentication requests.
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.	Reboot/Power cycle the module or re-flashing a new image.	Device will not respond to authentication requests.
ES3	The MACE fails an ECDSA PCT.	The MACE enters a temporary error state. The generated key is not discarded.	The error state is automatically cleared and the	The MACE will return an error code (0x01) to the operator.

Name	Description	Conditions	Recovery Method	Indicator
			module resumes normal operation.	

Table 28: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

Installation and Initialization:

The MACE 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 CO will use the default password provided by Motorola in a separate communication. Upon first access, the operator will use the default passwords for the specified product found on <https://support.motorolasolutions.com/>.
2. The CO will then change the default password based on the requirements in Table 10 – Roles and Authentication.
3. The CO 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

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 Design and Rules

Rules of Operation

1. The Module provides two distinct operator roles: Configuration Cryptographic Officer and the Operational Crypto Officer.
2. The Module provides identity-based authentication.
3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The MACE allows the operator to initiate power-up self-tests by power cycling power or resetting the MACE.
6. All self-tests do not require any operator action.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The MACE does not support concurrent operators by enforcing the following restrictions:
 - a. The CCO is automatically logged out if the OCO Authenticates.
 - b. The CCO cannot authenticate if the OCO is already logged on.
11. The Module does not support a maintenance interface or role.
12. The Module does not support manual SSP establishment method.
13. The Module does not have any proprietary external input/output devices used for entry/output of data.
14. The Module does not enter or output plaintext CSPs.
15. The Module does store some CSPs in plaintext.
16. The Module does not output intermediate key values.
17. The Module does not provide bypass services or ports/interfaces.

11.5 Maintenance Requirements

Not Applicable

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