Motorola Solutions, Inc.

Motorola Solutions Advanced Crypto Engine (MACE) HSM - Security Level 2

FIPS 140-3 Non-Proprietary Security Policy

Document Version: R01.00.00

Date: August 10, 2026

Table of Contents

List of Tables

List of Figures

1 General

1.1 Overview

This document is the non-proprietary FIPS 140-3 Security Policy for version R05.01.07 of the Motorola Solutions Advanced Crypto Engine (MACE) HSM – Security Level 2 (Also referred to as MACE HSM). It contains the security rules under which the module must operate and describes how this module meets the requirements as specified in FIPS PUB 140-3 (Federal Information Processing Standards Publication 140-3) for an overall Security Level 2 module.

1.2 Security Levels

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

Section	Title	Security Level
1	General	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 Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

This Motorola Solutions MACE HSM module, hereafter denoted as the Module. The Module is implemented as a single-chip cryptographic module to meet FIPS 140-3 Level 2 physical security requirements as defined by FIPS 140-3. The MACE HSM provides all key storage and generation and performs all crypto processing for the Motorola Solutions ASTRO HSM product.

2.1 Description

Purpose and Use:

The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated overall security level 2, the Module is intended to be used in ASTRO HSM unit.

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 embodiment. The cryptographic boundary is shown in Figure 3 below.

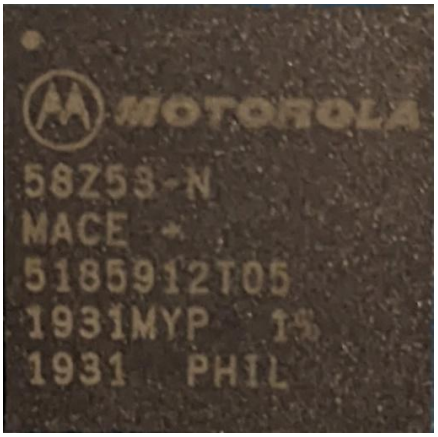

Figure 1 – MACE HSM IC (Top)

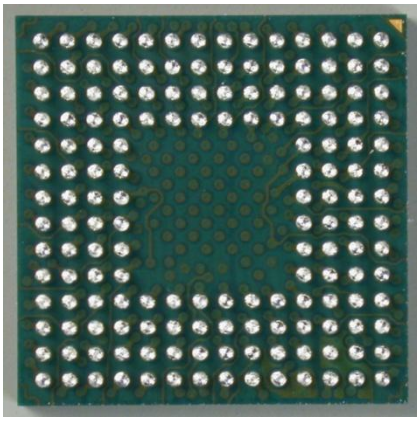

Figure 2 – MACE HSM IC (Interfaces)

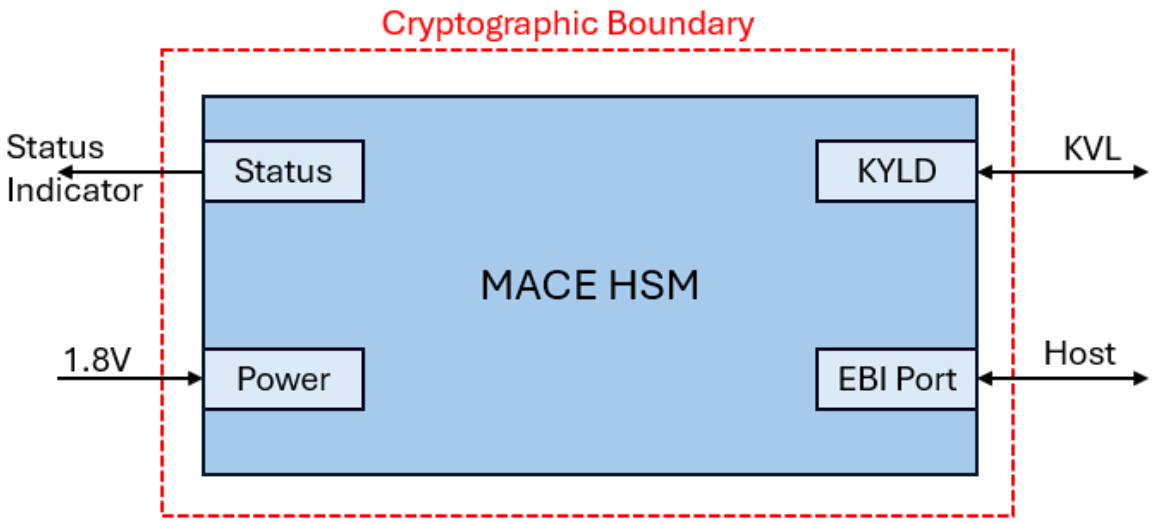

Figure 3 – Cryptographic Boundary for the MACE HSM

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

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

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
5185912T05	5185912	R05.01.07 with [AES256 R01.00.07 and/or AES128 R01.00.05]	5185912 family	N/A
5185912Y03	5185912	R05.01.07 with [AES256 R01.00.07 and/or AES128 R01.00.05]	5185912 family	N/A
5185912Y05	5185912	R05.01.07 with [AES256 R01.00.07 and/or AES128 R01.00.05]	5185912 family	N/A

Table 2: Tested Module Identification – Hardware

The MACE HSM 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. #
AES128	R01.00.05	R05.01.07	A5274
AES256	R01.00.07	R05.01.07	A5275

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):
N/A
N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:
N/A
N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:
N/A
N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:
N/A
N/A for this module.

2.3 Excluded Components

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

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Approved	Operating in approved mode	Approved	FIPS Status : 0x02

Table 4: Modes List and Description

The MACE HSM 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.

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

```
FIPS Status: 0x02
```

Which indicates that the module is operating in Level 2 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 2. To configure the module to operate in the Approved mode, the operator must log in as the CO using the default password and:

1. Change the default password for CO and User
2. Disable Clear Key Import
3. Disable Clear Key Export
4. Disable Key Loss Key (KLK)
5. Configure one of the options below
    a. Configure Key Load Mode to Black Only & Disable FIPS Level 3 Compliant Key Transport
    b. Configure Key Load Mode to Red
6. Disable KVL Role
7. Enable FIPS Algorithms Only

Additionally, the Module supports “drop-in algorithms” via the Program Update service. Drop-in algorithms may be added or removed from the Module independent of the base FW. In order to remain in the Approved Mode, only Approved algorithms may be loaded into the Module; in particular AES-128 (Cert. #A5274) and/or AES-256 (Cert. # A5275). The loading and unloading of any firmware within the validated cryptographic module invalidate the Module’s validation and zeroizes all SSPs except those entered at manufacturing. The Module is then in a non-compliant state.

2.5 Algorithms

Approved Algorithms:

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

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A5273	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-CBC	A5274	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
AES-CBC	A5275	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-CFB8	A5273	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-CTR	A5274	Direction - Decrypt, Encrypt Key Length - 128 Payload Length - Payload Length: 8-128 Increment 8 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	SP 800-38A
AES-CTR	A5275	Direction - Decrypt, Encrypt Key Length - 256 Payload Length - Payload Length: 8-128	SP 800-38A

Algorithm	CAVP Cert	Properties	Reference
		Increment 8 Supports Counter larger than maximum value - No Incremental Counter - Yes Counter Tests Performed - Yes	
AES-ECB	A5273	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-ECB	A5274	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
AES-ECB	A5275	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-GCM	A5273	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1, 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-GCM	A5274	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1, 8.2.2 Key Length - 128 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-GCM	A5275	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1, 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-GMAC	A5273	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1, 8.2.2 Key Length - 256 Tag Length - 128 IV Length - IV Length: 96	SP 800-38D

Algorithm	CAVP Cert	Properties	Reference
		AAD Length - AAD Length: 256-512 Increment 128	
AES-GMAC	A5274	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1, 8.2.2 Key Length - 128 Tag Length - 128 IV Length - IV Length: 96 AAD Length - AAD Length: 256-512 Increment 128	SP 800-38D
AES-GMAC	A5275	Direction - Decrypt, Encrypt IV Generation - Internal IV Generation Mode - 8.2.1, 8.2.2 Key Length - 256 Tag Length - 128 IV Length - IV Length: 96 AAD Length - AAD Length: 256-512 Increment 128	SP 800-38D
AES-KW	A2527	Direction - Decrypt, Encrypt Cipher - Cipher Key Length - 128, 256 Payload Length - Payload Length: 128-256 Increment 64	SP 800-38F
AES-OFB	A5273	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
AES-OFB	A5274	Direction - Decrypt, Encrypt Key Length - 128	SP 800-38A
AES-OFB	A5275	Direction - Decrypt, Encrypt Key Length - 256	SP 800-38A
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 String Length: 0 Returned Bits - 128	SP 800-90A Rev. 1
ECDSA KeyGen (FIPS186-4)	A2532	Curve - P-384 Secret Generation Mode - Extra Bits	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A2532	Component - No Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A2532	Component - No Curve - P-384 Hash Algorithm - SHA2-384	FIPS 186-4

Algorithm	CAVP Cert	Properties	Reference
HMAC-SHA2-384	A6378	MAC - MAC: 384 Key Length - Key Length: 256	FIPS 198-1
KAS-ECC Sp800-56Ar3	A2533	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||l||uPartyInfo||vPartyInfo Fixed Info Encoding - Concatenation Key Length - 384	SP 800-56A Rev. 3
KDF SRTP (CVL)	A2534	AES Key Length - 128, 256 Supports Empty KDR - Yes KDR Exponents - 1	SP 800-135 Rev. 1
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	A6379	Message Length - Message Length: 256, 8-2048 Increment 8	FIPS 180-4
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	A6379	Message Length - Message Length: 384, 8-2048 Increment 8	FIPS 180-4
TLS v1.3 KDF (CVL)	A2535	HMAC Algorithm - SHA2-384 KDF Running Modes - DHE, PSK, PSK-DHE	SP 800-135 Rev. 1

Table 5: Approved Algorithms

NOTE: Only the algorithms specified in this section are supported by the module in approved mode of operation.

Vendor-Affirmed Algorithms:

The Module implements the FIPS Vendor Affirmed cryptographic algorithms listed.

Name	Properties	Implementation	Reference
CKG1	Key Type:Asymmetric and Symmetric	N/A	SP800-133rev2 Section 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.

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

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

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

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

Non-Approved, Not Allowed Algorithms:

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
A5273 Authenticated Decrypt	BC-AuthDecrypt	Authenticated Decrypt, Message Authentication		AES-GCM: (A5273) AES-GMAC: (A5273)

Name	Type	Description	Properties	Algorithms
A5273 Authenticated Encrypt	BC-AuthEncrypt	Authenticated Encrypt, Message Authentication		AES-GCM: (A5273) AES-GMAC: (A5273)
A5273 Decryption	BC-UnAuthDecrypt	Block Cipher		AES-CBC: (A5273) AES-CFB8: (A5273) AES-ECB: (A5273) AES-OFB: (A5273)
A5273 Encryption	BC-UnAuthEncrypt	Block Cipher		AES-CBC: (A5273) AES-CFB8: (A5273) AES-ECB: (A5273) AES-OFB: (A5273)
A5274 Authenticated Decrypt	BC-AuthDecrypt	Authenticated Decrypt, Message Authentication		AES-GCM: (A5274) AES-GMAC: (A5274)
A5274 Authenticated Encrypt	BC-AuthEncrypt	Authenticated Encrypt, Message Authentication		AES-GMAC: (A5274) AES-GCM: (A5274)
A5274 Decryption	BC-UnAuthDecrypt	Block Cipher		AES-CBC: (A5274) AES-CTR: (A5274) AES-ECB: (A5274) AES-OFB: (A5274)
A5274 Encryption	BC-UnAuthEncrypt	Block Cipher		AES-CBC: (A5274) AES-CTR: (A5274) AES-ECB: (A5274) AES-OFB: (A5274)
A5275 Authenticated Decrypt	BC-AuthDecrypt	Authenticated Decrypt, Message Authentication		AES-GCM: (A5275) AES-GMAC: (A5275)

Name	Type	Description	Properties	Algorithms
A5275 Authenticated Encrypt	BC-AuthEncrypt	Authenticated Encrypt, Message Authentication		AES-GCM: (A5275) AES-GMAC: (A5275)
A5275 Decryption	BC-UnAuthDecrypt	Block Cipher		AES-CBC: (A5275) AES-CTR: (A5275) AES-ECB: (A5275) AES-OFB: (A5275)
A5275 Encryption	BC-UnAuthEncrypt	Block Cipher		AES-CBC: (A5275) AES-CTR: (A5275) AES-ECB: (A5275) AES-OFB: (A5275)
Common-SHA2	SHA	Secure Hash Standard		SHA2-256: (A6379) SHA2-384: (A6379)
Entropy	ENT-ESV	Entropy Source		
HMAC	MAC	Message Authentication		HMAC-SHA2-384: (A6378)
IDK-Gen	CKG	Symmetric Key Generation		CKG - IDK: () AES 256: Symmetric
KAS	KAS-Full	ECC Ephemeral Unified , (Initiator, Responder), KPG, Partial, oneStepKdf (SP800-56Cr1) IG D.F Scenario 2 path 2		SHA2-384: (A6379) KAS-ECC Sp800-56Ar3: (A2533) ECDSA KeyGen (FIPS186-4): (A2532) KDF SRTP: (A2534) TLS v1.3 KDF: (A2535)
KDF	KAS-135KDF	Key Derivation function		TLS v1.3 KDF: (A2535) KDF SRTP: (A2534)
KeyGen1	CKG	Symmetric Key Generation		AES-CBC: (A5273, A5274, A5275)

Name	Type	Description	Properties	Algorithms
				AES-CFB8: (A5273) AES-CTR: (A5274, A5275) AES-ECB: (A5273, A5274, A5275) AES-GCM: (A5273, A5274, A5275) AES-GMAC: (A5273, A5274, A5275) AES-KW: (A2527) AES-OFB: (A5273, A5274, A5275) KDF SRTP: (A2534) Counter DRBG: (A6380) CKG1: () Key Type: Asymmetric and Symmetric TLS v1.3 KDF: (A2535)
KeyGen2	AsymKeyPair-KeyGen	Asymmetric Key Pair Generation		ECDSA KeyGen (FIPS186-4): (A2532) KAS-ECC Sp800-56Ar3: (A2533) CKG1: () Key Type: Asymmetric and Symmetric
KTS1	KTS-Unwrap KTS-Wrap	Key Transport - Wrapping	Key establishment methodology: provides 128 or 256 bits strength IG D.G:Approved method in KW mode	AES-KW: (A2527)

Name	Type	Description	Properties	Algorithms
RNG	DRBG	AES-256 CTR Deterministic RBG		Counter DRBG: (A6380)
SHA	SHA	Secure Hash Standard		SHA2-256: (SHS 817)
SigGen1	DigSig-SigGen	Digital Signature Verification		ECDSA SigGen (FIPS186-4): (A2532) SHA2-256: (SHS 817)
SigVer1	DigSig-SigVer	Digital Signature Verification		ECDSA SigVer (FIPS186-4): (A2532) SHA2-256: (SHS 817)
SigVer2	DigSig-SigVer	Digital Signature Verification		RSA SigVer (FIPS186-5): (A5253) SHA2-256: (SHS 817)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

2.7.1 AES GCM IV Generation

2.7.1.1 Deterministic Construction

The Module generates GCM IVs deterministically as specified in SP800-38D Section 8.2.1 using the following protocols:

●TLS 1.3: Adherence to FIPS 140-3 IG C.H Key/IV Pair Uniqueness requirements from SP 800-38D is met through C.H Option 5. TLS1.3 is following RFC 8446 Section 5.3 & Section 8.1 for 96-bit IV Generation and with Section B.4 for AES-GCM usage. The IV is used only within the TLS1.3 context and uses an approved DBRG for generation. It is generated by XORing the lower 64-bit of 96-bit TLS 1.3 HKDF derived data (internal/static IV) and 64-bit SSL sequence numbers. Also, the (key, IV) pair collision probability does not exceed 2^{-32}.

- During operational testing, the Module was tested against an independent version of TLS1.3 and found to behave correctly.

●SRTP: The AES GCM IV generation is in compliance with RFC 7714, Section 8.1 IV construction and shall only be used for the SRTP protocol to be compliant with FIPS140-3 IG C.H, Option 5. The fixed field consists of a 32-bit Synchronization Source identifier and 16-bits of zeroes, and the invocation field consists of a 16-bit Sequence Number and 32-bit Rollover Counter. Both the fixed field and invocation field are passed into the Module as input parameters and XORed with a 96-bit random salt imported or generated internally. Note that the XOR operation does not have an impact on SP 800-38D requirements

because the salt is not regenerated until a key is re-established and therefore acts as a constant within an individual key's lifecycle.

- During operational testing, the Module was tested against an independent version of SRTP and found to behave correctly.

●SRTCP: The AES GCM IV generation is in compliance with RFC 7714, Section 9.1 IV construction and shall only be used for the SRTCP protocol to be compliant with FIPS140-3 IG C.H, Option 5. The fixed field consists of 16 bits of zeroes, a 32-bit Synchronization Source, 17 bits of zeroes, and the invocation field which consists of a 31-bit SRTCP Index. Both the fixed field and invocation field are passed into the Module as input parameters and XORed with a 96-bit random salt imported or generated internally. Note that the XOR operation does not have an impact on SP 800-38D requirements because the salt is not regenerated until a key is re-established and therefore acts as a constant within an individual key's lifecycle.

- During operational testing, the Module was tested against an independent version of SRTP and found to behave correctly.

If the Module's power is lost and restored for any of the protocols listed above, a new GCM key will be established. The invocation field is incremented externally and input to the Module; if the new invocation field is not greater than the last value then the Module will transition to an error state. Following an overflow of the invocation field, the Module will transition to an error state.

2.7.1.2 DRBG-based Construction

The Module generates GCM IVs randomly as specified in SP800-38D section 8.2.2 using approved DRBG (Cert #A2529) and is to be compliant with FIPS140-3 IG C.H, Option 2 and the IV length is 96 bits.

2.7.2 Protocol Information

Note for TLS 1.3 and SRTP, no parts of these protocols, other than the KDF, have been tested by the CAVP and CMVP.

2.7.3 Key Agreement Scheme

KAS [56Ar3] - 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

Table 9: Entropy Certificates

Name	Type	Operational Environment	Sample Size	Entropy per Sample	Conditioning Component
Motorola Solutions Advanced Crypto Engine (MACE) Entropy Source	Physical	Atmel 5186912	1 bit	0.138262	N/A

Table 10: Entropy Sources

2.9 Key Generation

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

2.10 Key Establishment

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 defined logical interface categories are listed below.

Physical Port	Logical Interface(s)	Data That Passes
External Bus Interface (EBI)	Data Input Data Output Control Input Status Output	The main physical port provided by the Module. It provides access to the majority of the supported interfaces.
Status Indicator	Status Output	This interface provides status output to indicate all power-up self-tests complete successfully.
Power	Power	This interface powers all circuitry.
Key Loading Port (KYLD)	Data Input Data Output Control Input Status Output	Provides an interface to the Key Variable Loader.

Table 11: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
AM1	Identity-based. Crypto-Officer Password: an 8-32 ASCII (printable) characters password is authenticated to gain access to Crypto-Officer services. It should be noted that after authenticating, this password may be changed at any time through the EBI Port.	SHA	The password requires a minimum of 1 Upper case, 1 Lower case, 1 Numerical and 1 special character. Since the minimum password length is 8 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in {(10)x(26^2)x(32)x(95^4)} which is 1 in 17,619,399,200,00.	After the CO password has been incorrectly entered 10 consecutive times, the Module will erase all CSPs, reset the CO password back to the default and must be reinitialized. The strength per minute is 15 in {(10)x(26^2)x(32)x(95^4)}
AM2	Identity based. User Password: an 8-32 ASCII (printable) characters password is authenticated to gain access to User services. It should be noted that after authenticating, this password may be	SHA	The password requires a minimum of 1 Upper case, 1 Lower case, 1 Numerical and 1 special character. Since the minimum password length is 8 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in {(10)x(26^2)x(32)x(95^4)} which is 1 in 17,619,399,200,00.	After the User password has been incorrectly entered 10 consecutive times, the Module will erase all CSPs, reset the User password back to the default and must be reinitialized. The strength per minute is 15 in {(10)x(26^2)x(32)x(95^4)}

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

Table 12: Authentication Methods

4.2 Roles

The Module supports two distinct operator roles, the Cryptographic Officer (CO) and the User. 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 support concurrent operators, on the EBI port, by utilizing logical channels to provide operator separation.

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	CO	AM1
User	Identity	User	AM2

Table 13: Roles

4.3 Approved Services

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

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

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

Note: The Program Update service requires the Crypto Officer to enable this service for the User.

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Algorithm List Query	Provides a list of drop-in	Approved mode	Command In	List of drop-in algorithms.	None	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	algorithms available in the Module using AM2.			Success/failure status.		
Change CO Password (AM1)	Modify the current password used to identify and authenticate the CO role using AM1.	Approved mode indicator and service status output	Password	Updated the CO password. Success/failure status.	A5273 Encryption A5273 Decryption Common-SHA2	Crypto Officer - CO PWD (AM1): G,E,Z - PEK: E - PWD Hash: G,E,Z
Change User Password (AM2)	Modify the current password used to identify and authenticate the User role using AM2.	Approved mode	Password	Updated the User password. Success/failure status.	A5273 Encryption A5273 Decryption Common-SHA2	User - PEK: E - PWD Hash: G,E,Z - User PWD (AM2): G,E,Z
Decrypt	Decrypt data using AM2.	Approved mode	Ciphertext	Plaintext. Success/failure status.	A5275 Decryption A5275 Authenticated Decrypt A5274 Decryption A5274 Authenticated Decrypt A5273 Decryption A5273 Authenticated Decrypt KeyGen1	User - KDF-DK: E - KEK: E - KPK: E - TEK: E
Delete Key	Mark key for deletion using AM2.	Approved mode	Command In	Key is marked for deletion. Success/failure status.	None	User
Encrypt	Encrypt data using AM2.	Approved mode	Plaintext	Ciphertext. Success/failure status.	A5275 Encryption A5275 Authenticated Encrypt	User - DRBG-EI/Seed: E - DRBG-State: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					A5274 Encryption A5274 Authenticated Encrypt A5273 Encryption A5273 Authenticated Encrypt RNG	- KDF-DK: E - KEK: E - KPK: E - TEK: E
Export Key	Transfer keys out of the Module using AM2.	Approved mode	Command In	Ciphertext. Success/failure status.	A5273 Encryption KTS1	User - BKWK: E - KDF-DK: R - KEK: E - MEK: E - SRTP-MK: R - SRTP-MS: R - TEK: R,E - TLS-MS: R
Export MEK	Transfer MEK out of the Module using AM1 & AM2.	Approved mode	Command In	Ciphertext. Success/failure status.	KTS1	Crypto Officer - DH-SS: E - MEK: R User - DH-SS: E - MEK: R
Extract Action Logs	Exports the history of actions performed by the operators	Approved mode	Command In	Error logs out. Success/Failure status.	None	Crypto Officer
Extract Error Logs	Provide the history of error events.	Approved mode	Command In	Error logs out. Success/Failure status.	None	Crypto Officer User
Generate Entropy	Generate Entropy for use inside the MACE HSM	Approved mode	Power On	DRBG Seed	Entropy RNG	Unauthenticated - DRBG-EI/Seed: G - DRBG-nonce: G - DRBG-State: G

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Generate Hash	Generate a hash of a block of data using AM2.	Approved mode	Data In.	Hash. Success/failure status	Common-SHA2	User
Generate Key	Generate symmetric [135] keys within the Module using AM2.	Approved mode	Command in	Key Stored inside Module. Success/failure status.	KeyGen1 IDK-Gen KDF	User - DRBG-nonce: E - DRBG-State: E - IDK: G,Z - IDK Block: E,Z - IDK ROM: E,Z - KDF-DK: G - KPK: G,Z - SRTP-MK: G,E - SRTP-MS: G,E - TLS-MS: E
Generate MAC	Generate a Message Authentication Code over a block of data using AM2.	Approved mode	Data to generate MAC	Generated MAC. Success/failure status	HMAC	User - KDF-DK: E - KEK: E - TEK: E
Generate MEK	Generate MEK within the Module using AM1 & AM2.	Approved mode	Command in	MEK Stored inside Module. Success/failure status.	KeyGen1	Crypto Officer - DRBG-EI/Seed: E - DRBG-State: E - MEK: G User - DRBG-EI/Seed: E - DRBG-State: E - MEK: G
Generate Random Number	Generate a Random Number using AM2.	Approved mode	Command in.	Generated Random Number. Success/failure status.	RNG	User - DRBG-EI/Seed: E - DRBG-State: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Generate Signature	Generate a signature using AM2.	Approved mode	Command In.	Signature, Success/failure status.	SigGen1 RNG	User - DRBG-EI/Seed: E - DRBG-State: E - ECDSA-PRIV: G,E - ECDSA-PUB: G,R
Import Key	Imports keys into the Module encrypted using AM2.	Approved mode	Ciphertext	Key Stored inside the Module. Success/failure status.	A5273 Decryption KTS1	User - BKWK: E - KDF-DK: R - KEK: W,E - MEK: W,E - SRTP-MK: R - SRTP-MS: R - TEK: W,E - TLS-MS: R
Import MEK	Import MEK into the Module encrypted using AM1 & AM2.	Approved mode	Ciphertext	MEK Stored inside the Module. Success/failure status.	KTS1	Crypto Officer - DH-SS: E - MEK: W User - DH-SS: E - MEK: W
Key Query	Retrieve the metadata for a given key present in the Module, using AM2.	Approved mode	Command in.	Key metadata. Success/failure status.	None	User
KVL Check Key	Obtain status information about a specific key/keyset using AM2.	Approved mode	Command in	Status information on keys Success/Failure Indication..	None	User
KVL Configuration	Display and Modify OTAR/OTEK Configuration	Approved mode	Command in	Configuration settings. Success/Failure Indication	None	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
	Parameters using AM2.					
KVL Delete Key	Delete Key(s) in the Module using AM2.	Approved mode	Command in	Success/Failure Indication.	None	User - KEK: Z - MEK: Z - TEK: Z
KVL Key Transfer Key	Import or Modify Keys in the Module using AM2.	Approved mode	Ciphertext	Store Keys internal to the Module. Success/Failure Indication.	None	User - KEK: W,E,Z - KPK: E - TEK: W,E,Z
KVL Version Info	Return Module specific version information using AM2.	Approved mode	Command in	Version Information. Success/Failure Indication	None	Unauthenticated
Logout CO (AM1)	Logs out CO role using AM1.	Approved mode	Command In	Logout CO	None	Crypto Officer
Logout User (AM2)	User Logout using AM2.	Approved mode	Command In	Logout User	None	User
Module Configuration	Set configuration parameters used to specify module behavior using AM1..	Approved mode	Configuration parameters	Updated module configuration. Success/failure status.	None	Crypto Officer - CO PWD (AM1): Z - DH-Priv: Z - DH-Pub: Z - DH-SS: Z - ECDSA-PRIV: Z - ECDSA-PUB: Z - KDF-DK: Z - KEK: Z - KPK: Z - MEK: Z - PWD Hash: Z - SRTP-MK: Z - SRTP-MS: Z - TEK: Z - TLS-MS: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- User PWD (AM2): Z
Module Info	Return Module specific information using UA. Module HW version, version information, and FIPS status.	Approved mode	Command in.	Module HW version, Firmware version, and FIPS status	None	Unauthenticated
Module Reset	Reset the Module	Approved mode	Command in.	Module Reset	None	Crypto Officer User
OTAR/OTEK Delete Key	Delete Key(s) in the Module using AM2.	Approved mode	Command In	Delete Keys stored in the Module. Success/Failure Indication	None	User - KEK: Z - MEK: Z - TEK: Z
OTAR/OTEK Transfer Key	Import or Modify Keys in the Module using AM2.	Approved mode	Ciphertext	Store Keys internal to the Module. Success/Failure Indication.	KTS1	User - KEK: W,E - KPK: E - TEK: W,E
Perform Key Agreement Process	Perform a key agreement process using AM2.	Approved mode	Command in.	Generate Keys stored in the Module. Success/failure status	KeyGen2 KAS	User - DH-CLI-Pub: W,E - DH-Priv: G,E - DH-Pub: G,R - DH-SS: G,E - DRBG-EI/Seed: E - DRBG-State: G,E - KDF-DK: G,E - KEK: W - SRTP-MK: W - SRTP-MS: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- TEK: W - TLS-MS: W
Program Update	Update the MACE HSM 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.	Approved mode	Firmware image	The MACE HSM is upgraded to new firmware.	A5273 Decryption SigVer2	Crypto Officer - BKWK: Z - CO PWD (AM1): Z - DH-CLI-Pub: Z - DH-Priv: Z - DH-Pub: Z - DH-SS: Z - ECDSA-PRIV: Z - ECDSA-PUB: Z - FW-LD-Pub: E,Z - IDK: E,Z - IDK Block: E,Z - IDK ROM: E - KEK: Z - KPK: Z - MEK: Z - PEK: Z - PWD Hash: Z - SRTP-MK: Z - SRTP-MS: Z - TEK: Z - TLS-MS: Z - User PWD (AM2): Z User - BKWK: Z - CO PWD (AM1): Z - DH-CLI-Pub: Z - DH-Priv: Z - DH-Pub: Z - DH-SS: Z - ECDSA-PRIV: Z - ECDSA-

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						PUB: Z - IDK: E,Z - IDK Block: E,Z - IDK ROM: E - KDF-DK: Z - KEK: Z - KPK: Z - MEK: Z - PEK: Z - PWD Hash: Z - SRTP-MK: Z - SRTP-MS: Z - TEK: Z - TLS-MS: Z - User PWD (AM2): Z
Self-Tests	Perform module self-tests comprised of cryptographic algorithm tests and firmware integrity 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.	A5275 Encryption A5275 Decryption A5275 Authenticated Encrypt A5275 Authenticated Decrypt A5274 Encryption A5274 Decryption A5274 Authenticated Encrypt A5274 Authenticated Decrypt A5273 Encryption A5273 Decryption A5273 Authenticated Encrypt A5273	Unauthenticated - FW-LD-Pub: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Authenticated Decrypt IDK-Gen SigGen1 SigVer1 SigVer2 Entropy RNG KAS SHA Common-SHA2 HMAC	
Validate CO Password (AM1)	Validate the current password used to identify and authenticate the CO role using AM1.	Approved mode	Password	Successful authentication will allow access to the services allowed for CO role.	A5273 Encryption A5273 Decryption Common-SHA2	Crypto Officer - CO PWD (AM1): Z - DH-Priv: Z - DH-Pub: Z - DH-SS: Z - ECDSA-PRIV: Z - ECDSA-PUB: Z - KDF-DK: Z - KEK: Z - KPK: G,E,Z - MEK: Z - PEK: E - PWD Hash: W,Z - SRTP-MK: Z - SRTP-MS: Z - TEK: Z - TLS-MS: Z
Validate User Password (AM2)	Validate the current password used to identify and authenticate the User role using AM2.	Approved mode	Password	Successful authentication will allow access to the services allowed for User role.	A5273 Encryption A5273 Decryption Common-SHA2	User - DH-Priv: Z - DH-Pub: Z - DH-SS: Z - ECDSA-PRIV: Z - ECDSA-PUB: Z - KDF-DK: Z - KEK: Z - KPK: G,E,Z - MEK: Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						- PEK: E - PWD Hash: W,Z - SRTP-MK: Z - SRTP-MS: Z - TEK: Z - TLS-MS: Z - User PWD (AM2): Z
Verify Signature	Verify a signature using AM2.	Approved mode	Command In.	Success/failure status.	SigVer1	User - ECDSA-PUB: E

Table 14: Approved Services

4.4 Non-Approved Services

N/A for this module.

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

4.5 External Software/Firmware Loaded

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

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

5 Software/Firmware Security

5.1 Integrity Techniques

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

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

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

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

5.2 Initiate on Demand

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

6 Operational Environment

6.1 Operational Environment Type and Requirements

The MACE HSM has a limited operational environment under the FIPS 140-3 definitions with a Physical Security at Level 2. Therefore, per the FIPS 140-3 Management Manual Section 7.5 Partial validations and non-applicable areas this section in not applicable.

Type of Operational Environment: Limited

7 Physical Security

The MACE HSM 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 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.

7.1 Mechanisms and Actions Required

The MACE HSM is covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the MACE HSM. The security provided from the hardness of the MACE HSM'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 HSM 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 HSM 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 HSM.	Periodically	Look for signs of tampering. Remove from service if tampering found.

Table 15: Mechanisms and Actions Required

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 16: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input encrypted on ephemeral key generated via KAS (I8)	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Manual	Electronic	KTS1
Input encrypted on KEK (I5)	OTAR (outside)	Flash Memory - Encrypted (S3)	Encrypted	Manual	Electronic	KTS1
Input encrypted on TEK or MEK (I7)	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Manual	Electronic	KTS1
Input encrypted on the BKWK (I3)	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Manual	Electronic	A5273 Decryption
Input encrypted on the IDK (I1)	Application Software (outside)	Flash Memory (S2)	Encrypted	Manual	Electronic	A5273 Decryption
Input encrypted on the PEK (I2)	Application Software (outside)	Flash Memory - Encrypted (S3)	Encrypted	Manual	Electronic	A5273 Decryption
Input in plaintext as part of protocol (I4)	Application Software (outside)	Flash Memory (S2)	Plaintext	Manual	Electronic	

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input in plaintext through the KVL (I6)	KVL	Flash Memory (S2)	Plaintext	Manual	Electronic	A5273 Decryption
Output encrypted on ephemeral key generated via KAS (O5)	Flash Memory - Encrypted (S3)	Application Software (outside)	Encrypted	Manual	Electronic	KTS1
Output encrypted on KEK (O3)	Flash Memory - Encrypted (S3)	OTAR (outside)	Encrypted	Manual	Electronic	KTS1
Output encrypted on the BKWK (O1)	Flash Memory - Encrypted (S3)	Application Software (outside)	Encrypted	Manual	Electronic	A5273 Encryption
Output encrypted on the TEK or MEK (O4)	Flash Memory - Encrypted (S3)	Application Software (outside)	Encrypted	Manual	Electronic	KTS1
Output in plaintext public key (O2)	Flash Memory (S2)	Application Software (outside)	Plaintext	Manual	Electronic	

Table 17: 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
Z2	Zeroized by module power cycle or hard reset.*	SSPs in volatile memory zeroized.	Yes
Z3	Zeroized by the "Configure Module" service by overwriting with a fixed pattern of 0s.	CO zeroize module when configuring into an Approved mode.	Yes
Z4	Zeroized by the "Change CO Password (AM1)" service by overwriting with a fixed pattern of 0s.	Old CO password zeroized as new CO password set	Yes

Zeroization Method	Description	Rationale	Operator Initiation
Z5	Zeroized by the "Validate CO Password (AM1)" service by overwriting with a fixed pattern of 0s.	CO password zeroized after too many failed login attempts	Yes
Z6	Zeroized by the "Change User Password (AM2)" service by overwriting with a fixed pattern of 0s.	Old User password zeroized as new CO password set	Yes
Z7	Zeroized by the "Validate User Password (AM2)" service by overwriting with a fixed pattern of 0s.	User password zeroized after too many failed login attempts	Yes

Table 18: 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

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
BKWK	A 256-bit AES OFB (A5273) key used to transfer keys with the Host	256 - 256	Symmetric Key - CSP	Pre-loaded		A5273 Encryption A5273 Decryption
CO PWD (AM1)	8-32 ASCII characters CO password.	N/A - N/A	Authentication - CSP			A5273 Encryption A5273 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		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	384 - 192	Symmetric Key - CSP		KAS	KAS

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	(DH) Shared Secret (SS) is established as a part of DH key agreement scheme.					
DRBG-EI/Seed	Internally generated by the HWRNG	1856 - N/A	N/A - CSP	Entropy		KeyGen1 KeyGen2 SigGen1 RNG
DRBG-nonce	Internally generated by the HWRNG	960 - N/A	N/A - CSP	Entropy		RNG
DRBG-State	CTR_DRBG (A2529) internal state: V (128 bits) and Key (AES 256)	256 - 256	N/A - CSP	RNG		KeyGen1 KeyGen2 SigGen1 RNG
ECDSA-PRIV	384-bit ECDSA Private Key used to generate the signature of the input data from the Generate Signature service request.	384 - 192	Asymmetric Private Key - CSP	KeyGen2		SigGen1
ECDSA-PUB	ECDSA Public key used to validate the signature of the input data from a service request.	768 - 192	Asymmetric Public Key - PSP	KeyGen2		SigVer1
FW-LD-Pub	2048-bit RSA key used to validate the signature of the firmware image during FW integrity	2048 - 112	Asymmetric Public Key - PSP	Pre-Loaded		SigVer2

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	and FW Loading before it is allowed to be executed.					
IDK	A 256-bit AES CBC (A5273) key used to decrypt downloaded firmware images.	256 - 256	Symmetric Key - CSP	IDK-Gen		A5273 Decryption
IDK Block	A 256-bit AES CBC key used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK ROM	256 - 256	Symmetric Key - CSP	Pre-Loaded		IDK-Gen
IDK ROM	A 256-bit AES CBC key used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK Block	256 - 256	Symmetric Key - CSP	Pre-loaded		IDK-Gen
KDF-DK	KDF Derived Key. Keys derived using TLS or SRTP KDFs.	128, 256 - 128, 256	Symmetric Key - CSP	KeyGen1		A5275 Authenticated Encrypt A5275 Authenticated Decrypt A5274 Authenticated Encrypt A5274 Authenticated Decrypt A5273

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
						Authenticated Encrypt A5273 Authenticated Decrypt KDF
KEK	128, 256-bit AES-KW (A2527) keys used for encryption of keys in key transport operation	128, 256 - 128, 258	Symmetric Key - CSP			KTS1
KPK	256 bit AES CFB-8 (A5273) key used to encrypt all TEKs and KEKs stored in the flash.	256 - 256	Symmetric Key - CSP	KeyGen1		A5273 Encryption A5273 Decryption
MEK	256-bit AES key-KW (A2527) used for encryption of keys in key transport operation	256 - 256	Symmetric Key - CSP	KeyGen1		KTS1
PEK	256-bit AES-CFB8 (A5273) key used for decrypting passwords during password validation	256 - 256	Symmetric Key - CSP	Pre-loaded		A5273 Decryption
PWD Hash	256-bit password hash stored in the non-volatile memory.	256 - 128	Authentication - CSP	Common-SHA2		
SRTP-MK	SRTP/SRTCP Master Key. 128 or 256 bit	128, 256 -	Symmetric Key - CSP	KeyGen1		KDF

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
	key used in SRTP KDF.	128, 256				
SRTP-MS	SRTP/SRTCP Master Salt. 112-bit key used in SRTP KDF, or 96-bit key to generate IV internally for AES GCM encryption operation.	96, 112 - 96, 112	Symmetric Key - CSP	KeyGen1		KDF
TEK	128, 256-bit AES-KW (A2527) keys used for enabling secure communication with target devices.	128, 256 - 128, 256	Symmetric Key - CSP			KTS1
TLS-MS	TLS KDF Master Secret. 384 bit secret key material.	384 - 384	Symmetric Key - CSP	KeyGen1		KDF
User PWD (AM2)	8-32 ASCII characters User password.	N/A - N/A	Authentication - CSP			A5273 Encryption A5273 Decryption

Table 19: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
BKWK	Input encrypted on the IDK (I1)	System Memory (S1):Encrypted Flash Memory (S2):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z2 Z3	KPK:Encrypted by KEK:Wraps TEK:Wraps

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
CO PWD (AM1)	Input encrypted on the PEK (I2)	System Memory (S1):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	PEK:Decrypted by PWD Hash:Hashed by
DH-CLI-Pub	Input in plaintext as part of protocol (I4)	System Memory (S1):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	
DH-Priv		System Memory (S1):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	DH-Pub:Paired With DH-SS:Derives
DH-Pub	Output in plaintext public key (O2)	System Memory (S1):Plaintext	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	DH-Priv:Paired With DH-SS:Derives
DH-SS		System Memory (S1):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	DH-Priv:Derived From DH-Pub:Derived From
DRBG-EI/Seed		System Memory (S1):Encrypted	When module is reset	Z2	DRBG-nonce:Used With DRBG-State:Generates
DRBG-nonce		System Memory (S1):Encrypted	When module is reset	Z2	DRBG-EI/Seed:Used With DRBG-State:Generates
DRBG-State		System Memory	When module is reset	Z2	DRBG-EI/Seed:Derived From DRBG-nonce:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
		(S1):Encrypted			
ECDSA-PRIV		System Memory (S1):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	ECDSA-PUB:Paired With
ECDSA-PUB	Output in plaintext public key (O2)	System Memory (S1):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	ECDSA-PRIV:Paired With
FW-LD-Pub		System Memory (S1):Encrypted Flash Memory (S2):Encrypted	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):Encrypted	When module is reset	Z1 Z2	IDK ROM:Used With IDK:Generates
IDK ROM		System Memory (S1):Encrypted Flash Memory (S2):Encrypted	When module is reset	Z1 Z2	IDK Block:Used With IDK:Generates
KDF-DK	Input encrypted on TEK or MEK (I7) Output encrypted	System Memory (S1):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5	SRTP-MK:Used With SRTP-MS:Used With TLS-MS:Used With BKWK:Encrypted by MEK:Encrypted/Decrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	on the BKWK (O1) Output encrypted on the TEK or MEK (O4)			Z6 Z7	
KEK	Input encrypted on the BKWK (I3) Input encrypted on KEK (I5) Input in plaintext through the KVL (I6)	System Memory (S1):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z2	KPK:Encrypted by BKWK:Decrypted by TEK:Decrypted by
KPK		System Memory (S1):Encrypted Flash Memory (S2):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	DRBG-State:Derived From KEK:encrypts in the flash. TEK:encrypts in the flash.
MEK	Input encrypted on ephemeral key generated via KAS (I8) Output encrypted on ephemeral key generated via KAS (O5)	System Memory (S1):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z2	KPK:Encrypted by DH-SS:Encrypted by DH-SS:Decrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
PEK		System Memory (S1):Encrypted Flash Memory (S2):Encrypted	When module is reset	Z1 Z2	CO PWD (AM1):Decrypts User PWD (AM2):Decrypts
PWD Hash		System Memory (S1):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z3 Z4 Z5 Z6 Z7	CO PWD (AM1):Hash of User PWD (AM2):Hash of
SRTP-MK	Input encrypted on the BKWK (I3) Input encrypted on TEK or MEK (I7) Output encrypted on the BKWK (O1) Output encrypted on KEK (O3) Output encrypted on the TEK or MEK (O4)	System Memory (S1):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	KDF-DK:Used With SRTP-MS:Used With BKWK:Encrypted/Decrypted by MEK:Encrypted/Decrypted by
SRTP-MS	Input encrypted on the BKWK (I3) Input encrypted on TEK or MEK (I7)	System Memory (S1):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	KDF-DK:Used With SRTP-MK:Used With SRTP-MS:Used With BKWK:Encrypted/Decrypted by MEK:Encrypted/Decrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	Output encrypted on the BKWK (O1) Output encrypted on KEK (O3) Output encrypted on the TEK or MEK (O4)				
TEK	Input encrypted on the BKWK (I3) Input encrypted on KEK (I5) Input in plaintext through the KVL (I6) Input encrypted on TEK or MEK (I7) Output encrypted on the TEK or MEK (O4)	System Memory (S1):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z2	KPK:Encrypted by BKWK:Decrypted by KEK:Decrypted by MEK:Decrypted by MEK:Encrypted by
TLS-MS	Input encrypted on the BKWK (I3) Input encrypted on TEK or MEK (I7) Output encrypted	System Memory (S1):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	KDF-DK:Used With BKWK:Encrypted/Decrypted by MEK:Encrypted/Decrypted by

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
	on the BKWK (O1) Output encrypted on the TEK or MEK (O4)				
User PWD (AM2)	Input encrypted on the PEK (I2)	System Memory (S1):Encrypted Flash Memory -Encrypted (S3):Encrypted	When module is reset	Z1 Z2 Z3 Z4 Z5 Z6 Z7	PEK:Decrypted by PWD Hash:Hashed by

Table 20: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

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

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware integrity	SHA2-256 (Cert. #817), RSA-2048 (Cert. #A5253)	KAT	SW/FW Integrity	Success or ES2 on failure	When the MACE HSM is powered up, the digital signature is verified. If the digital signature matches then the test passes otherwise it fails.

Table 21: Pre-Operational Self-Tests

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC (A5274) Decryption	AES-128	KAT	CAST	Success or ES1 on failure	AES-CBC Decryption	Bootup
AES-CBC (A5274) Encryption	AES-128	KAT	CAST	Success or ES1 on failure	AES-CBC Encryption	Bootup
AES-CBC (A5275) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-CBC 256 Decryption	Bootup
AES-CBC (A5275) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-CBC 256 Encryption	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CFB8 (A5273) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-CFB8 256 Decryption	Bootup
AES-CFB8 (A5273) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-CFB8 256 Encryption	Bootup
AES-CTR (A5274) Decryption	AES-128	KAT	CAST	Success or ES1 on failure	AES-CTR Decryption	Bootup
AES-CTR (A5274) Encryption	AES-128	KAT	CAST	Success or ES1 on failure	AES-CTR Encryption	Bootup
AES-CTR (A5275) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-CTR 256 Decryption	Bootup
AES-CTR (A5275) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-CTR 256 Encryption	Bootup
AES-ECB (A5274) Decryption	AES-128	KAT	CAST	Success or ES1 on failure	AES-ECB Decryption	Bootup
AES-ECB (A5274) Encryption	AES-128	KAT	CAST	Success or ES1 on failure	AES-ECB Encryption	Bootup
AES-ECB (A5275) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-ECB 256 Decryption	Bootup
AES-ECB (A5275) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-ECB 256 Encryption	Bootup
AES-GCM (A5273) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	256-bit AES-GCM and GMAC Authenticated Decryption	Bootup
AES-GCM (A5273) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	256-bit AES-GCM and GMAC Authenticated Encryption	Bootup
AES-GCM (A5274) Decryption	AES-128	KAT	CAST	Success or ES1 on failure	128-bit AES-GCM and GMAC Authenticated Decryption	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-GCM (A5274) Encryption	AES-128	KAT	CAST	Success or ES1 on failure	128-bit AES-GCM and GMAC Authenticated Encryption	Bootup
AES-GCM (A5275) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	256-bit AES-GCM and GMAC Authenticated Decryption	Bootup
AES-GCM (A5275) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	256-bit AES-GCM and GMAC Authenticated Encryption	Bootup
AES-KW (A2527) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	Message Decryption	Bootup
AES-KW (A2527) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	Message Encryption	Bootup
AES-OFB (A5273) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-OFB 256 Decryption	Bootup
AES-OFB (A5273) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-OFB 256 Encryption	Bootup
AES-OFB (A5274) Decryption	AES-128	KAT	CAST	Success or ES1 on failure	AES-OFB Decryption	Bootup
AES-OFB (A5274) Encryption	AES-128	KAT	CAST	Success or ES1 on failure	AES-OFB Encryption	Bootup
AES-OFB (A5275) Decryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-OFB 256 Decryption	Bootup
AES-OFB (A5275) Encryption	AES-256	KAT	CAST	Success or ES1 on failure	AES-OFB 256 Encryption	Bootup
Counter DRBG (A6380)	AES-256 CTR	KAT	CAST	Success or ES1 on failure	AES-256 CTR_DRBG instantiation and generate KATs performed before the first random	Bootup

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					data generation.	
ECDSA KeyGen (FIPS186-4) (A2532)	ECDSA KeyGen	PWCT	PCT	Success or ES3 on failure	ECDSA P-384 Pair-wise Consistency Test	Bootup
ECDSA SigGen (FIPS186-4) (A2532)	ECDSA P-384 SigGen	KAT	CAST	Success or ES1 on failure	ECDSA P-384 SigGen	Bootup
ECDSA SigVer (FIPS186-4) (A2532)	ECDSA P-384 SigVer	KAT	CAST	Success or ES1 on failure	ECDSA P-384 SigVer	Bootup
Entropy 90B Start-up Adaptive Proportion Test (APT)	Adaptive Proportion Test	APT	CAST	ES4 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	RCT	CAST	ES4 on failure	Designed to quickly detect catastrophic failures that cause the noise source to become "stuck" on a single output value for a long period of time	Bootup
Firmware Load	2048-bit RSA Signature Verification/SHA2-256	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	loading a new firmware image

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
					signature is verified upon download into the MACE HSM.	
HMAC-SHA2-384 (A6378)	HMAC-SHA2-384	KAT	CAST	Success or ES2 on failure	HMAC-SHA2-384	Bootup
KAS-ECC Sp800-56Ar3 (A2533)	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
KDF SRTP (A2534)	SRTP KDF	KAT	CAST	Success or ES1 on failure	SRTP KDF [135]	Bootup
KDF TLS (A2535)	TLS 1.3 KDF	KAT	CAST	Success or ES1 on failure	TLS 1.3 KDF [135]	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.	Bootup
SHA2-256 (A6379)	SHA2-256	KAT	CAST	Success or ES1 on failure	SHA2-256	Bootup
SHA2-256 (SHS 817)	SHA2-256	KAT	CAST	Success or ES2 on failure	SHA2, -256, KAT performed before Pre-Operational FW integrity tests.	Bootup

Table 22: Conditional Self-Tests

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

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 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC (A5274) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CBC (A5274) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CBC (A5275) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CBC (A5275) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CFB8 (A5273) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CFB8 (A5273) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CTR (A5274) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CTR (A5274) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CTR (A5275) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-CTR (A5275) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-ECB (A5274) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-ECB (A5274) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-ECB (A5275) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (A5275) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-GCM (A5273) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-GCM (A5273) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-GCM (A5274) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-GCM (A5274) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-GCM (A5275) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-GCM (A5275) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-KW (A2527) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-KW (A2527) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-OFB (A5273) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-OFB (A5273) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-OFB (A5274) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-OFB (A5274) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-OFB (A5275) Decryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
AES-OFB (A5275) Encryption	KAT	CAST	On Demand/Periodically	Manually/programmatically
Counter DRBG (A6380)	KAT	CAST	On Demand/Periodically	Manually/programmatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
ECDSA KeyGen (FIPS186-4) (A2532)	PWCT	PCT	On Demand/Periodically	Manually/programmatically
ECDSA SigGen (FIPS186-4) (A2532)	KAT	CAST	On Demand/Periodically	Manually/programmatically
ECDSA SigVer (FIPS186-4) (A2532)	KAT	CAST	On Demand/Periodically	Manually/programmatically
Entropy 90B Start-up Adaptive Proportion Test (APT)	APT	CAST	On Demand	Manually
Entropy 90B Start-up Repetition Count Test (RCT)	RCT	CAST	On Demand	Manually
Firmware Load	KAT	SW/FW Load	N/A	N/A
HMAC-SHA2-384 (A6378)	KAT	CAST	On Demand/Periodically	Manually/programmatically
KAS-ECC Sp800-56Ar3 (A2533)	KAT	CAST	On Demand/Periodically	Manually/programmatically
KDF SRTP (A2534)	KAT	CAST	On Demand/Periodically	Manually/programmatically
KDF TLS (A2535)	KAT	CAST	On Demand/Periodically	Manually/programmatically
RSA SigVer (FIPS186-5) (A5253)	KAT	CAST	On Demand	Manually
SHA2-256 (A6379)	KAT	CAST	On Demand/Periodically	Manually/programmatically
SHA2-256 (SHS 817)	KAT	CAST	On Demand/Periodically	Manually/programmatically

Table 24: Conditional Periodic Information

Conditional self–tests are periodically performed by the MACE HSM every X minutes, where X is configured by the operator during module configuration (1 minutes to 720 minutes). The MACE HSM 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 HSM end the periodic self-test executed when the I/O buffer is emptied. The MACE HSM logs the most recent self-test errors to the internal flash; the operator CO) can extract the error logs using Extract Error Log service.

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
ES1	The MACE HSM fails a conditional KAT.	The MACE HSM enters the critical error state. In this state, the MACE HSM 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 HSM fails a firmware loading during program upgrade and/or firmware integrity pre-operational self-test.	The MACE HSM enters the firmware signature validation failure state. In this state, the MACE HSM 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 HSM fails an ECDSA PCT.	The MACE HSM enters a temporary error state. The generated key is discarded.	The error state is automatically cleared and the module resumes normal operation.	The MACE HSM will return an error code (0x01) to the operator.
ES4	The MACE HSM fails to acquire Entropy.	The MACE HSM enters the Fatal Error state.	Automatic	The MACE HSM stores the status into the internal flash memory and resets to attempt recovery.

Table 25: Error States

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

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

1. Upon first access, the operator will use the default passwords for the specified product found on https://support.motorolasolutions.com/.
2. The operator will then change the default passwords based on the requirements in the roles and Authentication Table.
3. The operator will then complete Module configuration using the Module Configuration and Configure OTEK services.
4. Finally, the operator will set the Module to the Approved mode using the Module Configuration Service.

Delivery:

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

11.2 Administrator Guidance

Use vendor provided product specific user guide for secure operations.

11.3 Non-Administrator Guidance

Use vendor provided product specific user guide for secure operations.

11.4 Design and Rules

Rules of Operation

1. The Module provides two distinct operator roles: Cryptographic Officer and User.
2. The Module provides identity-based authentication.
3. The Module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.

6. All self-tests do not require any operator action.
7. Data output is inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
9. There are no restrictions on which keys or SSPs are zeroized by the zeroization service.
10. The Module does support concurrent operators, on the EBI Port, with the following restrictions
    a. The User can only authenticate on Logical Channel 0.
    b. The Crypto Officer can only authenticate on Logical Channel 1.
    c. MEK generation, importing and exporting services require the use of concurrent operators. If only one operator is authenticated then these services will be blocked.
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 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

N/A

11.6 End of Life

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

12 Mitigation of Other Attacks

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

References and Definitions

The following standards are referred to in this Security Policy.

Table 26 References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, October 23, 2024.*
[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*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186-4]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-, July 19, 2013.*
[186-5]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-, February 3, 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*

Abbreviation	Full Specification Name
[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.*
[90B]	*National Institute of Standards and Technology, Recommendation for the Entropy Sources Used for Random Bit Generation, Special Publication 800-90B, January 2018.*
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*
[RFC3686]	*Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP), January 2004*
[RFC3711]	*The Secure Real-time Transport Protocol (SRTP), March 2004*
[RFC5288]	*AES Galois Counter Mode (GCM) Cipher Suites for TLS, August 2008*
[RFC5869]	*HMAC-based Extract-and-Expand Key Derivation Function (HKDF), May 2010*
[RFC5246]	*The Transport Layer Security (TLS) Protocol, August 2008*
[RFC6188]	*The Use of AES-192 and AES-256 in Secure RTP, March 2011*
[RFC7714]	*AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP), December 2015*
[RFC8446]	*The Transport Layer Security (TLS) Protocol Version 1.3, August 2018*

Table 27 Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
BKWK	Black Key Wrap Key
CAST	Cryptographic Algorithm Self-Tests
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CO	Crypto-Officer

Acronym	Definition
CO PWD	Crypto-Officer Password
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
DRBG-EI/Seed	DRNG Entropy Input
DSEK	DRBG Seed Encryption Key
EBI	External Bus Interface
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature
ECDSA-PUB	ECDSA Public Key
FIPS	Federal Information Processing Standards
FW	Firmware
FW-LD-Pub	Firmware Load Public Key
GCM	Galois/Counter Mode
GMAC	Galois Message Authentication Code
HSM	Hardware Security Module
IDK	Image Decryption Key
IV	Initialization Vector
KAT	Known Answer Test
KDA	Key Derivation Algorithm
KDF	Key Derivation Function
KDF-DK	KDF Derived Key
KEK	Key Encryption Key
KPK	Key Protection Key
KYLD	Keyload
KVL	Key Variable Loader
MAC	Message Authentication Code

Acronym	Definition
MACE	Motorola Advanced Crypto Engine
MEK	Multi-HSM Exchange Key
OFB	Output Feedback
OTAR	Over The Air Rekeying
PWD Hash	Password Hash
PEK	Password Encryption Key
PWCT	Pair-Wise Consistency Test
ECDSA-PRIV	ECDSA Private Key
SRTP	Secure Real-time Transport Protocol
SRTP-MK	SRTP/SRTCP Master Key
SRTP-MS	SRTP/SRTCP Master Salt
RSA	Rivest–Shamir–Adleman
SSP	Sensitive Security Parameter
TEK	Traffic Encryption Key
TLS	Transport Layer Security
TLS-MS	TLS Pre-Shared Master Secret
UA	Unauthenticated Service
User PWD	User Password