Motorola Solutions Advanced Crypto Engine (MACE) HSM – Security Level 3

Non-Proprietary FIPS 140-3 Security Policy

Version: 1.5

Date: February 14, 2025

The Motorola Solutions Advanced Crypto Engine (MACE) HSM is used in the Motorola Solutions Micro HSM product.

Table of Contents

List of Tables

List of Figures

1 General

This document defines the non-propriety Security Policy for the Motorola Solutions Advanced Crypto Engine (MACE) HSM – Security Level 3, hereafter denoted as the Module. The MACE is a single-chip cryptographic module to meet FIPS 140-3 Level-3 physical security requirements. The Module provides encryption and decryption services for secure key management, and secure voice/data traffic for Motorola Solutions Micro HSM products.

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

Table 1 – Security Levels

ISO/IEC 24759 Section	Security Requirement	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		**3**

2 Cryptographic Module Specification

The MACE cryptographic module is a single chip hardware cryptographic module. The Module is used in Motorola Solutions, Inc. Micro HSM products. The Module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated overall security level 3.

2.1 Operational Environment

The Module is tested on the following operational environment.

Table 2 – Cryptographic Module Tested Configuration

Model	HW P/N, Version	Base Firmware version	Distinguishing Features
Motorola Solutions Advanced Crypto Engine (MACE) HSM	5185912T05	R04.01.04	Single chip embodiment

The Module supports the following Approved Mode algorithms that may be installed separately from the Module's base firmware using the program update service. While the installation of AES may be done separately, for the purposes of this validation the Module includes this firmware.

Table 3 – Approved Mode Drop-in Algorithms

Algorithm	Algorithm FW Version	Base FW Version	Cert. #
AES128	R01.00.05	R04.01.04	A5274
AES256	R01.00.07	R04.01.04	A5275

2.2 Cryptographic Boundary

Figure 1 and Figure 2 depict the physical form of the MACE cryptographic module. The perimeter of the MACE IC as shown in Figure 3 is the cryptographic boundary.

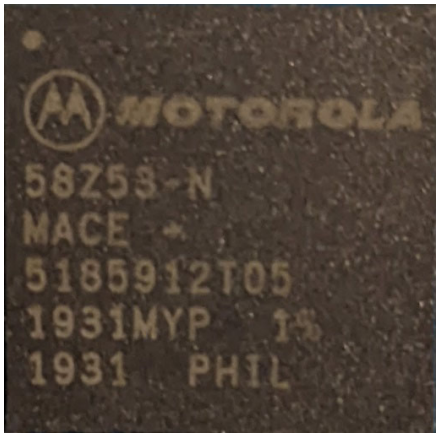

Figure 1: MACE Chip (Top)

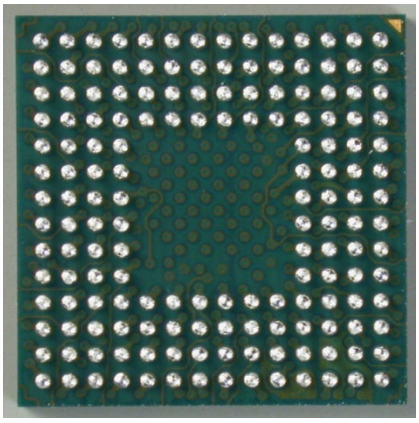

Figure 2: MACE Chip (Interfaces)

The MACE IC has an EBI port, a KVL port when connected to the Motorola Key Variable Loader (KVL), and Power Connections.

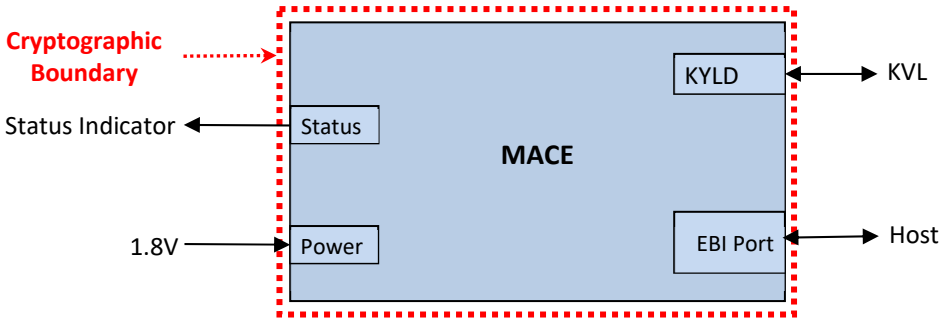

Figure 3: Cryptographic Boundary

2.3 Modes of Operation

The MACE HSM module is originally non-compliant and must be configured to operate in an approved mode of operation. The Module 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 Module to be used in an Approved Mode of operation at overall security level 3. At any given time, use the Module Info service to determine whether the Module is operating at overall security level 3.

Table 4 – Approved Mode Indicator

Item ID	Value	Meaning
0x06 (FIPS)	3	Approved Mode at overall Security Level 3

Note that at least one of the AES-128 and AES-256 drop-in algorithms must be loaded into the Module, however if they are loaded, they must match the values in Table 3 to be in the Approved Mode.

Use Module Info service to verify that the firmware version matches an approved version listed on NIST's website: http://csrc.nist.gov/groups/STM/cmvp/validation.html

Also, the module status service will output the AES DIA versions installed with a display of APCO AES128 Version: R01.00.05 and/or APCO AES256 Version R01.00.07.

2.3.1 Configuration of the Approved Mode of Operation

In order to configure the Module for an Approved Mode at overall Security Level 3, the operator shall use the Module Configuration service to set the following configuration parameters as shown below.

1. Clear Key Import: Disabled
2. Clear Key Export: Disabled
3. Key Loss Key (KLK): Disabled
4. Red Keyloading: Disabled
5. FIPS Security Level 3 compliant key transport: Enabled

The Module will operate in Approved Mode only if it receives external entropy from the operator.

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

2.4 Security Functions

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

Table 5 – Approved Algorithms

Cert #	Algorithm	Mode	Description/ Key Size(s) / Key Strength(s)	Use/Functions
A5273	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CFB8 [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
		GCM/GMAC [38D]	Key Sizes: 256	Authenticated Encrypt, Authenticated Decrypt, Message Authentication

Cert #	Algorithm	Mode	Description/ Key Size(s) / Key Strength(s)	Use/Functions
A5274	AES [197]	ECB [38A]	Key Sizes: 128	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 128	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 128	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 128	Encrypt, Decrypt
		GCM/GMAC [38D]	Key Sizes: 128	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
A5275	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 256	Encrypt, Decrypt
		GCM/GMAC [38D]	Key Sizes: 256	Authenticated Encrypt, Authenticated Decrypt, Message Authentication
A2527	AES [197]	KW [38F]	Forward Key Sizes: 128, 256	Authenticated Encrypt, Authenticated Decrypt for KTS
A2528	AES [197]	KW [38F]	Forward Key Sizes: 256	Authenticated Decrypt for KTS
VA	CKG [IG D.H]	[133] Section 5.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation
		[133] Section 5.2 Asymmetric key establishment key generation using unmodified DRBG output		
		[133] Section 6.1 Direct symmetric key generation using unmodified DRBG output		
		[133] Section 6.3 Symmetric Keys Produced by Combining (Multiple) Keys and Other Data		
A2534	KDF SRTP [135]			AES-128, AES-256

Cert #	Algorithm	Mode	Description/ Key Size(s) / Key Strength(s)	Use/Functions
A2535	KDF TLS [135]	v1.2, v1.3		SHA2(384)
A2529	DRBG [90A]	CTR	Use_df AES-256	Deterministic Random Bit Generation[1]
A2532	ECDSA [186-4]		P-384	KeyGen
			P-384 SHA2(384)	SigGen
			P-384 SHA2(384)	SigVer
A2531	HMAC [198]	HMAC-SHA2-384	Key Sizes: 32 bytes λ = *48 bytes*	Message Authentication
A2533	KAS-ECC [56Arev3]	Ephemeral Unified, (Initiator, Responder), KPG, Partial, oneStepKdf (SP800-56Cr1) IG D.F Scenario 2 path 2	P-384 SHA2-384	Key Agreement Scheme provides 192 bits of encryption strength
A2527	KTS [38F]	KW	AES Cert. #A2527	128 and 256-bit AES-KW keys used for encryption of keys in key transport operation and for enabling secure communication with target devices. Key establishment methodology provides 128 or 256 bits of encryption strength

[1] The entropy for seeding the SP 800-90A DRBG is determined by the operator of the Module that is outside of the module's physical and logical boundary. The operator shall use entropy sources that meet the security strength required for the random number generation mechanism as shown in [SP 800-90A] Table 3 (CTR_DRBG) and set required bits into the module by using Load Entropy service listed in section 4.3. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys.

Cert #	Algorithm	Mode	Description/ Key Size(s) / Key Strength(s)	Use/Functions
A2528	KTS [38F]	KW	AES KW Cert. #2528	256-bit AES KW (SP 800-38F) key used to decrypt the external seed. Key establishment methodology provides 256 bits strength
A5253	RSA [186-5]	PKCS1_v1.5	2048	SigVer
SHS 817	SHA2-256	SHA2		Message Digest Generation, Password Obfuscation
A2530	SHA2-256, SHA2-384	SHA2		Message Digest Generation, Password Obfuscation

Note: No parts of SRTP and TLS, other than the KDF, have been tested by the CAVP and CMVP.

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

Algorithm	Caveat	Use/Function
KTS	Key establishment methodology provides 256 bits strength.	[IG D.G] AES CBC Cert. #A5273 (unwrapping only);

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

Algorithm[2]	Caveat	Use/Function
AES MAC	N/A	[IG 2.4.A] P25 AES OTAR. No Security Claimed. AES MAC is used as part of OTAR but is considered obfuscation. KTS encryption is performed on the OTAR key components using AES KW Cert. #A2527.

[2] These algorithms do not claim any security and are not used to meet FIPS 140-3 requirements. Therefore, SSPs do not map to these algorithms.

2.5 Overall Security Design

1. The Module provides two distinct operator roles: User and Cryptographic 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 Module allows the operator to initiate power-up self-tests by power cycling power or resetting the Module.
6. Power up self-tests do not require any operator action.
7. Data output are 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. The Module does not support manual SSP establishment method.
10. The Module does not have any proprietary external input/output devices used for entry/output of data.
11. The Module does not enter or output plaintext CSPs.
12. The Module does not output intermediate key values.
13. The Module does not provide bypass services for ports/interfaces.
14. The Module does not support a maintenance role and/or bypass capability.

2.6 Rules of Operation

The Module shall be installed in the Motorola Solutions Micro HSM products. After authentication with the default password, the operator shall change the default passwords for Crypto Officer (CO) and User role. The Module is not usable until the factory default passwords are changed.

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

3 Cryptographic Module Interfaces

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

Table 8 – Ports and Interfaces

Physical Port	Logical Interface	Data that passes over port/interface
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.
Self-test Indicator	Status Output	This interface provides status output to indicate all power-up self-tests completed successfully.
Power	Power Input	This interface powers all circuitry.

Note: The module does not have Control Output.

4 Roles, Services, and Authentication

4.1 Assumption of Roles and Related Services

The Module supports two distinct operator roles, User and Cryptographic Officer (CO). Table 9 lists all operator roles supported by the Module and their related services. In addition, the Module supports services which do not require to be authenticated, listed UA in Table 9.

Table 9– Roles, Service Commands, Input and Output

Role			Service	Input	Output
CO	User	UA			
X	X	–	Program Update	Firmware image	The Module is upgraded to new firmware.
X	X	–	Extract Error Logs	Command In	Error logs. Success/failure status.
X	–	–	Extract Action Logs	Command In	Action logs. Success/failure status.
X	–	–	Configure Module	Configuration parameters	The Module is configured as requested. Success/Failure status.
X	–	–	Change CO Password	Password	Updated the CO password. Success/failure status.
X	–	–	Logout CO	Command In	Logout CO role.
–	X	–	Load Entropy	DRBG seed	The DRBG is seeded and initialized. Success/failure status.
–	X	–	Change User Password	Password	Updated the user password. Success/failure status.
–	X	–	Logout User	Command In	Logout the User role.
–	X	–	Algorithm List Query	Command In	List of Drop-In Algorithms (DIAs) available in the Module.
–	X	–	Export Key	Command In	Transfer keys out of the Module. Success/failure status.
–	X	–	Import Key	Encrypted keys	Imports keys into the Module. Success/failure status.
–	X	–	Generate Key	Command In	Generate symmetric [135] keys within the Module. Success/failure status.
–	X	–	Delete Key	Command In	Key is marked for deletion. Success/failure status.
–	X	–	Encrypt	Plaintext	Ciphertext. Success/failure status.
–	X	–	Decrypt	Ciphertext	Plaintext. Success/failure status.
–	X	–	Generate Signature	Command In	Generated signature. Success/failure status.
–	X	–	Verify Signature	Signature	Success/failure status.
–	X	–	Generate Hash	Data	Hash output. Success/failure status.
–	X	–	Generate MAC	Data	Generated MAC. Success/failure status.

Role			Service	Input	Output
CO	User	UA			
–	X	–	Perform Key Agreement Process	Command In	Keys imported into the MACE. Success/failure status.
–	X	–	Generate Random Number	Command In	Generated random numbers. Success/failure status.
–	X	–	Key Query	Command In	Metadata for a given key present in the Module. Success/failure status.
–	–	X	Validate User Password	Password	Successful authentication will allow access to the services allowed for User role.
–	–	X	Validate CO Password	Password	Successful authentication will allow access to the services allowed for CO role.
–	–	X	Perform Self-Tests	Command In	Success/Reset.
–	–	X	Module Info	Command In	Module HW version, version information, and FIPS status.

4.2 Authentication Methods

The Module supports two distinct operator roles (User and Crypto-Officer). The Module uses a minimum 8 ASCII printable characters password to authenticate the User and CO roles. The Module enforces the separation of roles using login credentials and re-authentication is enforced when changing roles.

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

Table 10– Roles and Authentication

Role	Authentication Method	Authentication Strength
CO	Identity-based. 8-32 character ASCII password.	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 $\{(10)*(26^2)*(32)*(95^4)\}$ which is 1 in 17,619,399,200,000 The Module has a default setting of 15 consecutive failed attempts. The module will have to be reinitialized after the 15 consecutive failed attempts. Within a one minute period a successful random attempt is 15 in 17,619,399,200,000

Role	Authentication Method	Authentication Strength
User	Identity-based. 8-32 character ASCII password.	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)*(26^2)*(32)*(95^4)} which is 1 in 17,619,399,200,000. The Module has a default setting of 15 consecutive failed attempts. The module will have to be reinitialized after the 15 consecutive failed attempts. Within a one minute period a successful random attempt is 15 in 17,619,399,200,000.

4.3 Services

All services implemented by the Module are listed in Table 11. The Module does not allow any non-approved service while operating in FIPS 140-3 level 3 mode.

The SSPs modes of access shown in Table 11 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.
- **E** = Execute: The Module uses the SSP in performing a cryptographic operation.
- **Z** = Zeroize: The Module zeroizes the SSP.

Table 11– Approved Services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
Program Update	Upgrade firmware and perform zeroization	RSA [186-5], Cert. #A5253	FW-LD-Pub	CO, User	WZ	Approved Mode
			DSEK		Z	
			BKK		Z	
			IDK-ROM		E	
			IDK-Block		EZ	
			IDK		Z	
			PEK		Z	
			KPK		Z	
			KEK		Z	
			TEK		Z	
			CO PWD		Z	
			User PWD		Z	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
			PWD Hash		Z	
			SRTP-MK		Z	
			SRTP-MS		Z	
			TLS-MS		Z	
			KDF-DK		Z	
			DH-Priv		Z	
			DH-SS		Z	
			ECDSA-PRIV		Z	
			ECDSA-PUB		Z	
			DH-Pub		Z	
			DH-CLI-Pub		Z	
Extract Error Logs	Extract the error logs from the module.	N/A	N/A	CO, User	N/A	Approved Mode
Extract Action Logs	Exports the history of actions performed by the operators.	N/A	N/A	CO	N/A	Approved Mode
Configure Module	Perform configuration of the Module.	N/A	KPK	CO	Z	Approved Mode
			KEK		Z	
			TEK		Z	
			CO PWD		Z	
			User PWD		Z	
			PWD Hash		Z	
			SRTP-MK		Z	
			SRTP-MS		Z	
			TLS-MS		Z	
			KDF-DK		Z	
			DH-Priv		Z	
			DH-SS		Z	
			ECDSA-PRIV		Z	
			ECDSA-PUB		Z	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
			DH-Pub		Z	
Validate CO Password	Validate the current password for CO role.	AES-256, Cert. #A5273 SHS [180], Cert. #A2530	PEK	UA	E	Approved Mode
			KPK		GEZ	
			KEK		Z	
			TEK		Z	
			CO PWD		Z	
			User PWD		Z	
			PWD Hash		Z	
			SRTP-MK		Z	
			SRTP-MS		Z	
			TLS-MS		Z	
			KDF-DK		Z	
			DH-Priv		Z	
			DH-SS		Z	
			ECDSA-PRIV		Z	
			ECDSA-PUB		Z	
			DH-Pub		Z	
Change CO Password	Modify the current CO password.	AES-256, Cert. #A5273 SHS [180], Cert. #A2530	PEK	CO	EZ	Approved Mode
			CO Password		GEZ	
			PWD Hash		GEZ	
Logout CO	Logs out CO role.	N/A	N/A	CO	N/A	Approved Mode
Validate User Password	Validate the current password for User role.	AES-256, Cert. #A5273 SHS [180], Cert. #A2530	PEK	UA	E	Approved Mode
			KPK		GEZ	
			KEK		Z	
			TEK		Z	
			CO PWD		Z	
			User PWD		Z	
			PWD Hash		Z	
			SRTP-MK		Z	
			SRTP-MS		Z	
			TLS-MS		Z	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
			KDF-DK		Z	
			DH-Priv		Z	
			DH-SS		Z	
			ECDSA-PRIV		Z	
			ECDSA-PUB		Z	
			DH-Pub		Z	
Change User Password	Modify the current User password.	CKG, AES-256, Cert. #A5273 SHS [180], Cert. #A2530	PEK	User	E	Approved Mode
			User Password		GEZ	
			PWD Hash		GEZ	
Logout User	Logs out User role.	N/A	N/A	User	N/A	Approved Mode
Load Entropy	Load external entropy used to seed the DRBG.	AES KW #A2528, DRBG [90A] #A2529	DSEK	User	WE	Approved Mode
			DRBG-EI/Seed		G	
			DRBG-State		G	
Algorithm List Query	Provides a list of drop-in algorithms available in the Module.	N/A	N/A	User	N/A	Approved Mode
Export Key	Transfer keys out of the Module.	AES KW #A2527	KEK	User	R	Approved Mode
			TEK		R	
			SRTP-MK		R	
			SRTP-MS		R	
			TLS-MS		R	
			KDF-DK		R	
Import Key	Imports keys into the Module encrypted.	AES KW #A2527	KEK	User	W	Approved Mode
			TEK		W	
			SRTP-MK		W	
			SRTP-MS		W	
			TLS-MS		W	
Generate Key	Generate symmetric	CKG, TLS (#A2535) and	SRTP-MK	User	E	Approved Mode
			SRTP-MS		E	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
	[135] keys within the Module.	SRTP [135] KDF (#A2534)	TLS-MS		E	
			KDF-DK		GW	
			IDK-ROM		EZ	
			IDK-Block		EZ	
			IDK		GZ	
			KPK		GZ	
Delete Key	Mark key for deletion.	N/A	N/A	User	Z	Approved Mode
Encrypt	Encrypt plaintext data.	AES [197] #A5273, AES [197] #A5275, AES [197] #A5274, CKG (VA) TLS (#A2535) and SRTP [135] KDFs (#A2534) DRBG [90A] #A2529	KEK	User	E	Approved Mode
			KPK		E	
			TEK		E	
			KDF-DK		E	
			DRBG-EI/Seed		E	
			DRBG-State		E	
Decrypt	Decrypt ciphertext data.	AES [197] #A5273, AES [197] #A5275, AES [197] #A5274, CKG (VA), TLS (#A2535) and SRTP [135] KDFs (#A2534)	KEK	User	E	Approved Mode
			KPK		E	
			TEK		E	
			KDF-DK		E	
Generate Signature	Generate a signature.	ECDSA [186-4] #A2532, DRBG [90A] #A2529	DRBG-EI/Seed	User	E	Approved Mode
			DRBG-State		E	
			ECDSA-PRIV		GW	
			ECDSA-Pub		GWR	

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
Verify Signature	Verify a signature.	ECDSA [186-4] #A2532	ECDSA-Pub	User	E	Approved Mode
Generate Hash	Generate a hash of a block of data.	SHS [180] #A2530	N/A	User	N/A	Approved Mode
Generate MAC	Generate MAC of a block of data to provide data integrity using a shared symmetric key.	HMAC [198] Cert. #A2531	KEK	User	E	Approved Mode
			TEK		E	
			KDF-DK		E	
Perform Key Agreement Process	Perform a key agreement process.	CKG, DRBG [90A] #A2529, KAS-ECC [56Ar3], Cert. #A2533	KEK	User	W	Approved Mode
			TEK		W	
			SRTP-MK		W	
			SRTP-MS		W	
			TLS-MS		W	
			KDF-DK		W	
			DH-Priv		GE	
			DH-Pub		GRE	
			DH-SS		GE	
			DH-CLI-Pub		WE	
			DRBG-State		GE	
Generate Random Number	Generated random numbers.	DRBG [90A] Cert. #A2529	DRBG-EI/Seed	User	E	Approved Mode
			DRBG-State		E	
Key Query	Retrieve the metadata for a given key present in the Module.	N/A	N/A	User	N/A	Approved Mode
Perform Self-Tests	Performs cryptographic algorithms self-tests.	N/A	N/A	UA	N/A	Approved Mode

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access Rights	Indicator
Module Info	Module HW version, Firmware version, and FIPS status.	N/A	N/A	UA	N/A	Approved Mode

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

5 Firmware Security

The Module has a limited operational environment under the FIPS 140-3 definitions. The Module is composed of base firmware version identified in Table 2. On top of that, customer shall load at least one of the Drop-in algorithms listed in Table 3.

The firmware components are protected with the authentication technique(s) RSA Programmed Signature Key described in Table 19.

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

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

The Module is composed of the following firmware component(s):

- non-modifiable operating system - binary

Firmware versions validated through the FIPS 140-3 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the Module defined by this Security Policy or covered by this validation.

6 Operational Environment

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

7 Physical Security

The Module is a production grade, single-chip cryptographic module 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.

The Module is covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the Module. The security provided from the hardness of the Module's epoxy encapsulate is claimed at ambient temperature (-40 to 85 degrees Celsius) only. No assurance of the epoxy hardness is claimed for this physical security mechanism outside of this range. The Module 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 Module while delivering to operators.

There are two voltage powers that power the MACE. VDDCORE voltage powers all MACE chip functions while VDDBU voltage powers the MACE chip battery. VDDCORE and VDDBU voltages enter the cryptographic boundary of the module separately; and therefore, were tested separately to verify that they both cause the MACE chip to zeroize SSPs.

Table 12 – Physical Security Inspection Guidelines

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

Table 13 – Environmental Failure Protection

	Temperature or Voltage Measurement	Specify EFP or EFT	Results
Low Temperature	-38.1°C	EFP	Shutdown - A tamper flag is raised, a wake-up reset of the product is triggered.
High Temperature	101.4°C	EFP	Shutdown - A tamper flag is raised, a wake-up reset of the product is triggered.
Low Voltage	1.65V VDDCORE : 1.350 VVDBU	EFP	Shutdown - A general reset of the chip is asserted.
High Voltage	2.034V VDDCORE : 2.292V - VVDBU	EFP	Shutdown- A tamper flag is raised, a wake-up reset of the product is triggered.

Table 14 – Coating testing

	Hardness tested temperature measurement
Low Temperature	-40°C
High Temperature	85°C

8 Non-Invasive Security

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

9 Sensitive Security Parameter (SSP) Management

The SSPs access methods are described in Table 15 below:

Table 15– SSP Management Methods

Method	Description
G1	Generated external to the Module and installed during manufacturing.
G2	Derived from the DRBG input per SP800-90Ar1.
G3	FIPS 186-4 compliant ECDSA key generation, using the internal CAVP validated DRBG.
G4	CKG - Symmetric key generated by internal CAVP validated DRBG.
G5	EC Diffie-Hellman shared secret generation using the internal CAVP validated 56Arev3 protocol.
G6	SP 800-135 compliant KDF generated key.
G7	5'ı'õ̂²'¡Õ'õMJfiÍÍ¨öÀÀõÄ-M'u²ßı-âÀ-œÄí¾^-XBL-ß,Ä-ß²˙'õÆ'üÂ-é7, =¨LB?÷̂ı¡÷7, =¨)ªßuÆí
S1	Stored in the volatile memory (RAM).
S2	Stored in the flash in plaintext, associated by memory location (pointer).
S3	Stored in the flash in encrypted, associated by memory location (pointer).
E2	Input electronically using SP800-38F AES key transport by the DSEK using AES KW Cert. # A2528.
E3	Input electronically AES-256 CFB-8 encrypted on the PEK using AES KTS Cert. #A5273.
E4	Input or output electronically using SP800-38F AES key transport on the KEK or TEK using AES KW Cert. # A2527.
E5	Input electronically in plaintext as part of protocol.
E6	Output electronically in plaintext public key.
Z1	Zeroized by the “Program Update” service by overwriting with a fixed pattern 0s.*
Z2	Zeroized by module power cycle or hard reset by overwriting with a fixed pattern 0s.*
Z3	Zeroized by the “Configure Module” service by overwriting with a fixed pattern of 0s.
Z4	Zeroized by the “Change CO Password” service by overwriting with a fixed pattern of 0s.
Z5	Zeroized by the “Validate CO Password” service by overwriting with a fixed pattern of 0s.
Z6	Zeroized by the “Change User Password” service by overwriting with a fixed pattern of 0s.
Z7	Zeroized by the “Validate User Password” service by overwriting with a fixed pattern of 0s.

NOTE: Change and Validate Password services zeroizes when 15 attempts have failed, and the module is reset to factory settings.

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

9.1 Sensitive Security Parameters (SSP)

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

Table 16– SSPs

Key/SSP Name/ Type	Strength (in bits)	Security Function / Cert.	Gene-ration	Import /Export	Establish-ment	Storage	Zeroiza-tion	Use / Related SSPs
CSPs								
DRBG-EI/Seed	N/A	N/A	N/A	E2	N/A	S1	Z2	Externally generated, a minimum of 48 bytes are passively entered into the Module by the User.
DRBG-State	256	DRBG #A2529	G2	N/A	N/A	S1	Z2	CTR_DRBG internal state: V (128 bits) and Key (AES 256).
DSEK	256	AES KW Cert. #A2528	G1	N/A	N/A	S1, S2	Z1	256-bit AES KW (SP 800-38F) key used to decrypt the external seed.
BKK	256	AES CBC Cert. #A5273, RSA Cert. #A5253	G1	N/A	N/A	S1, S2	Z1	A 256-bit AES key used for decrypting Load entropy into the MACE.
IDK-ROM	256	AES CBC Cert. #A5273	G1	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES CBC key used in the õ' ¨ ußıÂ²õïu²' ¡ ÷ß,÷7, =÷ Õ'õMJfiÍ Í ¨õÀÀõÄ÷ êM'u²ßı÷âÂ÷æÄí¾ˆ÷ XBL using IDK-Block
IDK-Block	256	AES CBC Cert. #A2264	G1	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES CBC key used in the õ' ¨ ußıÂ²õïu²' ¡ ÷ß,÷7, =÷ Õ'õMJfiÍ Í ¨õÀÀõÄ÷ êM'u²ßı÷âÂ÷æÄí¾ˆ÷ XBL using IDK-ROM
IDK	256	AES CBC Cert. #A5273, RSA Cert. #A5253	G7	N/A	N/A	S1	Z2	A 256-bit AES CBC key used to decrypt downloaded firmware images.
PEK	256	AES CBC #A5273,	G1	N/A	N/A	S1, S2	Z1, Z2	256-bit AES-CFB8 key used for decrypting passwords during password validation.

Key/SSP Name/ Type	Strength (in bits)	Security Function / Cert.	Gene-ration	Import /Export	Establish-ment	Storage	Zeroiza-tion	Use / Related SSPs
KPK	256	AES CFB-8 Cert. #A5273, DRBG Cert. #A2529	G4	N/A	N/A	S1, S2	Z1, Z2, Z3, Z4, Z5, Z6, Z7	256-bit AES CFB-8 key used to encrypt all TEKs and KEKs stored in the flash.
KEK	128, 256	AES KW #A2527	N/A	E4	N/A	S1, S3	Z1, Z2, Z8	128 and 256-bit AES-KW keys used for encryption of keys in key transport operation.
TEK	128, 256	AES KW Cert. #A2527,	N/A	E4	N/A	S1, S3	Z1, Z2, Z8	128 and 256-bit AES keys used for enabling secure communication with target devices.
CO PWD	256	AES CFB-8 Cert. #A5273	N/A	E3	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7	8-32 ASCII characters CO password.
User PWD	256	AES CFB-8 Cert. #A5273	N/A	E3	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7	8-32 ASCII characters User password.
PWD Hash	192	SHS [180] Cert. #A2530	G1	N/A	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7	384-bit password hash stored in the non-volatile memory.
SRTP-MK	128, 256	CVL SRTP KDF Cert. #A2534	G4	E4	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7	SRTP/SRTCP Master Key. 128 or 256-bit key used in SRTP KDF.
SRTP-MS	96, 112	CVL SRTP KDF Cert. #A2534	G4	E4	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7	SRTP/SRTCP Master Salt. 112-bit key used in SRTP KDF, or 96-bit key to generate IV internally for AES GCM encryption operation.
TLS-MS	384	CVL TLS KDF Cert. #A2535	G4	E4	N/A	S1, S3	Z1, Z2, Z3, Z4, Z5, Z6, Z7	TLS KDF Master Secret. 384-bit secret key material.

Key/SSP Name/ Type	Strength (in bits)	Security Function / Cert.	Gene-ration	Import /Export	Establish-ment	Storage	Zeroiza-tion	Use / Related SSPs
KDF-DK	128, 256	CVL TLS KDF Cert. #A2535 or CVL SRTP KDF Cert. #A2534, AES-GCM Cert. #A5275 and #A5274	G6	E4 (export only)	N/A	S1	Z1, Z2, Z3, Z4, Z5, Z6, Z7	KDF Derived Key. Keys derived using TLS or SRTP KDFs.
DH-Priv	192	KAS Cert. #A2533 DRBG Cert. #A2529	G3	N/A	N/A	S1	Z1, Z2, Z3, Z4, Z5, Z6, Z7	The Elliptic Curve Diffie-Hellman (DH) private key used for establishing a shared secret over an insecure channel.
DH-SS	192	KAS Cert. #A2533	N/A	N/A	G5	S1	Z1, Z2, Z3, Z4, Z5, Z6, Z7	The Elliptic Diffie-Hellman (DH) Shared Secret (SS) is established as a part of DH key agreement scheme.
ECDSA-PRIV	192	ECDSA Cert. #A2532, DRBG Cert. #A2529	G3	N/A	N/A	S1	Z1, Z2, Z3, Z4, Z5, Z6, Z7	384-bit ECDSA Private Key used to generate the signature of the input data from the Generate Signature service request.
PSPs								
FW-LD-Pub	112	AES CBC Cert. #A5273, RSA #A5253	G1	N/A	N/A	S1, S2	Z1, Z2	2048-bit RSA key used to validate the FW Loading before it is allowed to be executed. Note - FW-LD-Pub is also used during FW integrity to validate the signature of the firmware image
DH-Pub	192	KAS Cert. #A2533	G3	E6	N/A	S1	Z1, Z2, Z3, Z4, Z5, Z6, Z7	The Elliptic Curve (EC) Diffie-Hellman (DH) public key, used for establishing a

Key/SSP Name/ Type	Strength (in bits)	Security Function / Cert.	Gene-ration	Import /Export	Establish-ment	Storage	Zeroiza-tion	Use / Related SSPs
								shared secret over an insecure channel.
DH-CLI-Pub	192	KAS Cert. #A2533	N/A	E5	N/A	S1	Z1, Z2, Z3, Z4, Z5, Z6, Z7	The Elliptic Curve (EC) Diffie-Hellman (DH) public key for the other party, used for establishing a shared secret over an insecure channel.
ECDSA-PUB	192	ECDSA Cert. #A2532	G3	E6	N/A	S1	Z1, Z2, Z3, Z4, Z5, Z6, Z7	ECDSA Public key used to validate the signature of the input data from a service request.

Table 17 – Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum number of bits of entropy	Details
External	384 bits of entropy	The Load Entropy service provides the security strength required for the random number generation mechanism Per IG 9.3.A, Example 2A, there is no assurance of the minimum strength of generated SSPs.

10 Self-Tests

The Module performs self-tests to ensure the proper operation of the Module. 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 Module. Pre-operational Cryptographic Algorithm Self-Tests (CAST) are periodically performed by the Module in every X[3] minutes, where X is configured by the operator during module configuration. The Module 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 Module at the end of periodic self-test when the I/O buffer is emptied.

The periodic self-test process should take no more than 2-3 minutes. The Module will reset if any self-tests fails, otherwise it will continue to operate normally.

The Module logs the most recent self-test errors to the internal flash; the operator (UA) can extract the error logs using Extract Error Log service list in section 4.3.

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

Table 18– Error states and indicators

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

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

[3] The operator can configure the periodic self-tests interval to any value between 1 to 712800 minutes.

Table 19– Pre-Operational Self-Test

Security Function	Method	Description	Error state
Firmware integrity	RSA (Cert. #A5253), SHA2-256 (Cert. #817)	A digital signature is generated over the Boot Block, Base firmware and all Drop-in algorithms code when it is built using SHA2-256 (Cert. #817) and RSA-2048 (Cert. #A5253) and is stored with the code upon download into the MACE. When the MACE is powered up, the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.	ES2

The Module performs the following conditional self-tests:

Table 20– Conditional Self-Tests

Security Function	Method	Description	Error state
AES256 – CFB8, CBC, ECB, OFB, and GCM (Cert. #A5273)	KAT	AES-256 encryption KAT.	ES1
AES256 – CFB8, CBC, ECB, OFB, and GCM (Cert. #A5273)	KAT	AES-256 decryption KAT.	ES1
AES256 – CBC, CTR, ECB, OFB, and GCM (Cert. #A5275)	KAT	AES-256 encryption KAT.	ES1
AES256 – CBC, CTR, ECB, OFB, and GCM (Cert. #A5275)	KAT	AES-256 encryption KAT.	ES1
AES128 – CBC, CTR, ECB, OFB, and GCM (Cert. #A5274)	KAT	AES-128 encryption KAT.	ES1
AES128 – CBC, CTR, ECB, OFB, and GCM (Cert. #A5274)	KAT	AES-128 decryption KAT.	ES1
AES KW (Cert. #A2527)	KAT	AES-256 key wrap and key unwrap KAT.	ES1
AES KW (Cert. #A2528)	KAT	AES-256 key unwrap KAT.	ES1
DRBG (Cert. #A2529)	KAT	AES-256 CTR_DRBG instantiation, generate, and reseed KATs performed before the first random data generation.	ES1

Security Function	Method	Description	Error state
KAS-ECC Sp800-56Ar3 (Cert. #A2533)	KAT	Per IG D.F, separately tested KAS Shared Secret generation with P-384 and SP 800-56Cr2 one-step KDA	ES1
ECDSA (Cert. #A2532)	KAT	ECDSA P-384 SigGen KATs.	ES1
ECDSA (Cert. #A2532)	KAT	ECDSA P-384 SigVer KATs.	ES1
HMAC	KAT	HMAC-SHA2-384 KAT.	ES1
SHS (Cert. #A2530)	KAT	SHA2-256, SHA2-384 KAT.	ES1
SRTP KDF [135] (Cert. #2534)	KAT	SRTP KDF KAT.	ES1
TLS 1.2 and TLS 1.3 KDF [135] (Cert. #A2535)	KAT	TLS 1.2 and TLS 1.3 KDF KAT.	ES1
RSA SigVer (Cert. #A5253)	KAT	RSA-2048 SigVer, performed before Pre-Operational FW integrity tests.	ES2
SHS 256-bit (Cert. #817)	KAT	SHA2-256 KAT, performed before Pre-Operational FW integrity tests.	ES2
ECDSA Key Generation (Cert. #A2532)	PWCT	ECDSA P-384 Pair-wise Consistency Test.	ES3
Firmware Load	RSA (Cert. # A5253), SHA2-256 (Cert. #817)	A digital signature is generated over the code when it is built using SHA2-256 and RSA-2048. The digital signature is verified upon download into the Module.	ES2

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Installation and Initialization

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

1. Upon first access, the operator (CO) will use the default password provided by Motorola in a separate communication.
2. The CO will then change the default passwords (user and CO) based on the requirements in the Roles and Authentication table.
3. The CO will then configure the MACE using the Module configuration service as specified in the section 2.3.1.
4. Finally, the CO will set the periodic self-tests timer as part of the Module configuration in every X minutes, where X is a minimum value = 1 minute and maximum value = 712,800 minutes (495 days). Note: the default minimum = 0* but must be changed to a minimum of 1.

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

11.1.2 Delivery

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

During manufacturing, all of the firmware modules are signed by the RSA private Programmed Signature Key and the module is loaded with the RSA public Programmed Signature (FW-LD-Pub) key. The signature of the firmware is verified to ensure the integrity of the module when it is delivered to authorized operators.

The module is embedded into Motorola radio products, and it's put into the radio circuitry during Manufacturing. Hence, the module is directly shipped from the Motorola factory to the end customers through sales and distribution channels.

11.2 Administrator Guidance

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

11.3 Non-Administrator Guidance

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

11.4 Maintenance Requirements

The MACE does not require any special maintenance.

11.5 End of Life

After the end-of-life, the operator should zeroize all SSPs, except those SSPs entered at manufacturing, using the “Configure Module“ 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.

13 AES GCM IV Generation

13.1 Deterministic Construction

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

- TLS 1.2: The Module is compliant with TLS v1.2 and SP800-52 Rev2, Section 3.3.1 in accordance with RFC 5246 for TLS key establishment which implies compliance with TLS v1.2 and SP800-52 Rev2, Section 3.3.1. The AES GCM IV generation is in compliance with RFC 5288 and shall only be used for the TLS protocol version 1.2 to be compliant with FIPS140-3 IG C.H, Option 1. The fixed field consists of a 32-bit salt that is generated internally to the Module and the invocation field consists of a 64-bit nonce_explicit passed into the Module as an input parameter.
    - When the nonce_explicit (counter) part of the IV exhausts the maximum number of possible values for a given session key this condition triggers a handshake to establish a new encryption key per RFC 5246.
    - During operational testing, the Module was tested against an independent version of TLS1.2 and found to behave correctly.

- TLS 1.3: The AES GCM IV is in compliance with RFC 8446 section 5.3. Section 8.1 IV construction and shall only be used for the TLS1.3 protocol to be compliant with FIPS140-3 IG C.H, Option 5. 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.
    - 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.

13.2 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.

14 References and Definitions

The following standards are referred to in this Security Policy.

Table 21– 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, May 16, 2022.*
[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]	*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*
[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*

Abbreviation	Full Specification Name
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*
[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 22– Acronyms and Definitions

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

Acronym	Definition
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
TEK	Key Encryption Key
KYLD	Keyload
KVL	Key Variable Loader
MAC	Message Authentication Code
MACE	Motorola Advanced Crypto Engine
OFB	Output Feedback
OTAR	Over The Air Rekeying
PWD Hash	Password Hash
PEK	Password Encryption Key

Acronym	Definition
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