



MOTOROLA SOLUTIONS

Non-Proprietary FIPS 140-2 Security Policy: μMACE

Cryptographic module for the Motorola Solutions CRYPTR Micro

Version: 1.3

Date: October 21, 2021

Table of Contents

1	Introduction	4
	Algorithm	4
	Algorithm FW Version	4
	1.1 Module Description and Cryptographic Boundary	6
2	Modes of Operation.....	7
	2.1 Approved Mode Configuration	8
3	Cryptographic Functionality	8
	3.1 Critical Security Parameters	10
	3.2 Public Keys.....	14
4	Roles, Authentication and Services	15
	4.1 Assumption of Roles.....	15
	4.2 Authentication Methods	16
	4.3 Services.....	16
5	Self-Tests	21
6	Physical Security Policy	22
7	Operational Environment	22
8	Mitigation of Other Attacks Policy.....	22
9	Security Rules and Guidance	22
	9.1 Invariant Rules.....	22
10	AES-256 GCM IV Generation Protocol.....	24
11	References and Definitions	25

List of Tables

Table 1 – Cryptographic Module Configuration	4
Table 2 – Approved Mode Drop-in Algorithms.....	4
Table 3 – Non-Approved Mode Drop-in Algorithms.....	4
Table 4 – Historical FIPS 140-2 Validation Status.....	5
Table 5 – Security Level of Security Requirements.....	5
Table 6 – Ports and Interfaces	7
Table 7 – Approved Mode Indicator	7
Table 8 – Approved Algorithms	8
Table 9 – Non-Approved but Allowed Cryptographic Functions	10
Table 10 – Non-Approved Cryptographic Functions.....	10
Table 11 – Critical Security Parameters (CSPs)	10
Table 12 – Public Keys.....	14
Table 13 – Roles Description.....	16
Table 14 – Authenticated Services.....	16
Table 15 – Unauthenticated Services	18
Table 16 – Security Parameters Access by Service	19
Table 17 – References.....	25
Table 18 – Acronyms and Definitions	26

List of Figures

Figure 1 – Module Block Diagram.....	6
Figure 2 – Module	6

1 Introduction

This document defines the Security Policy for the Motorola Solutions μ MACE cryptographic module, hereafter denoted the Module. The Module provides secure key management, and voice/data encryption for the Motorola Solutions CRYPTR Micro.

Table 1 – Cryptographic Module Configuration

Module	HW P/N and Version	Base FW Version
Motorola μ MACE	51009730001, Rev 0x0001	R03.03.09

Algorithms may also optionally be loaded into, or “Drop-in” the Module independent of the Base FW via the Program Update service.

Table 2 – Approved Mode Drop-in Algorithms

Algorithm	Algorithm FW Version	Cert. #
AES128	R01.00.01 (0x52010001)	5076
AES256	R01.00.03 (0x52010003)	5077

Table 3 – Non-Approved Mode Drop-in Algorithms

Algorithm	Algorithm FW Version
ADP	R01.00.00 (0x52010000)
DES-XL	R01.00.00 (0x52010000)
DES-OFB	R01.00.00 (0x52010000)
DES-ECB	R01.00.00 (0x52010000)
DES-CBC	R01.00.00 (0x52010000)
DVI-XL	R01.00.00 (0x52010000)
DVP-XL	R01.00.00 (0x52010000)
Localized Capable	R01.00.00 (0x52010000)

The Module is intended for use by markets that require FIPS 140-2 validated overall Security Level 3 crypto-processors.

The Module was previously FIPS 140-2 validated with the following FW versions.

Table 4 – Historical FIPS 140-2 Validation Status

CMVP Cert#	Base FW Version
3601	R03.01.12
2385	R01.07.01 or R01.07.05

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

Table 5 – Security Level of Security Requirements

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

1.1 Module Description and Cryptographic Boundary

The physical form of the Module is depicted in Figure 1. The Module is a single chip embodiment. The cryptographic boundary is the surface and edges of the chip as shown in Figure 1 and Figure 2 below.

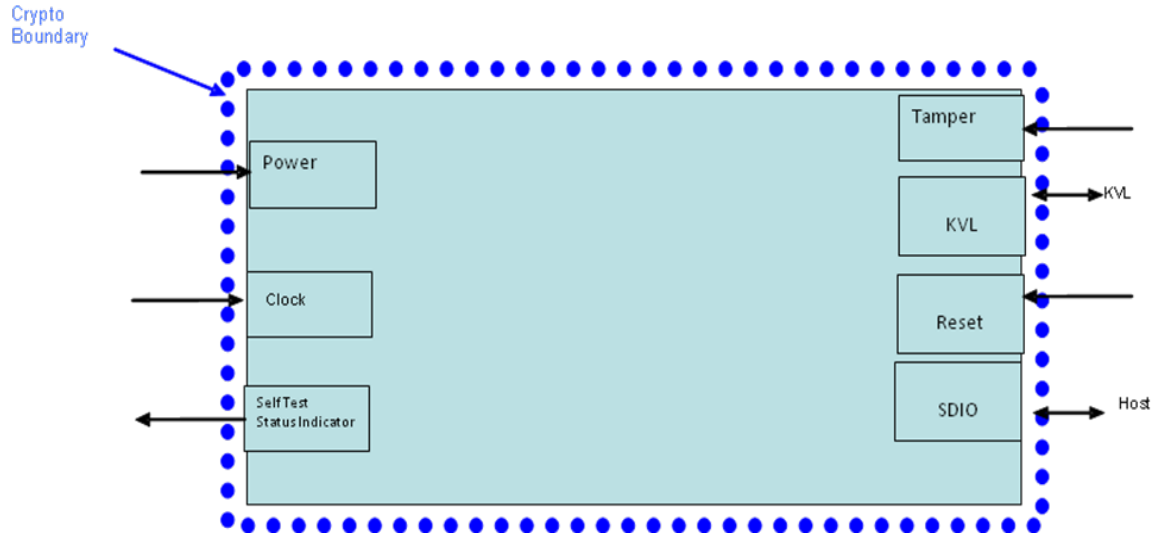


Figure 1 – Module Block Diagram

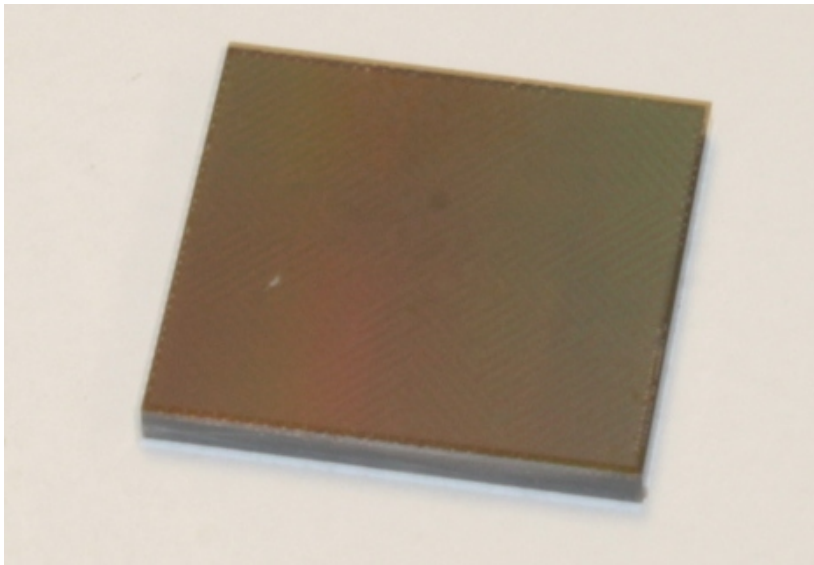


Figure 2 – Module

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

Table 6 – Ports and Interfaces

Port	Description	Logical Interface Type
Power	This interface powers all circuitry. This interface does not support input / output of CSP's.	Power Input
Clock	Clock Input. Not used. This interface does not support input / output of CSP's.	N/A
Tamper	Tamper Input. Not used. This interface does not support input / output of CSP's.	Control Input
KVL	This port is disabled and not used by the Module when configured for overall Security Level 3.	N/A
Self-tests Status Indicator	This interface provides status output to indicate all power-up self-tests completed successfully.	Status Output
Reset	This interface forces a reset of the Module. Not used.	Control Input
SDIO Interface	Provides an interface for factory programming and execution of SDIO commands. All CSPs exchanged over this interface are always encrypted when operating in FIPS Approved mode.	Control Input Status Output Data Output Data Input

2 Modes of Operation

The Module can be configured to operate in a FIPS 140-2 Approved mode of operation at overall Security Level 3 and a non-Approved mode of operation. To transition between FIPS 140-2 Approved and non-Approved modes, an operator must change the value of CSPs via the Program Update service as mentioned in section 3.1; all other CSPs are automatically zeroized by the Module when switching modes. To verify that the Module is in the Approved mode of operation, output from the Version Query service can be used as specified in Table 7. Note that AES-128 and AES-256 drop-in algorithms may or may not be loaded into the Module, however if they are loaded then the output of the Version Query service must also match the values in Table 2 to be in the Approved mode.

Table 7 – Approved Mode Indicator

Item ID	Value	Meaning
0x06 (FIPS)	0x03	FIPS Approved mode at overall Security Level 3
0x06 (FIPS)	0x00	Non-Approved mode

The Version Query service can also be used to verify the firmware version matches an approved version listed on NIST's website: <https://csrc.nist.gov/groups/STM/cmvp/validation.html>

2.1 Approved Mode Configuration

In order to configure the Module into an Approved mode at overall Security Level 3, the Module Configuration service must be used to ensure the following parameters are configured 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

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. #5076) and/ or AES-256 (Cert. #5077).

3 Cryptographic Functionality

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

Table 8 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
5075	AES [197]	ECB [38A]	Key Sizes: 128	Encrypt, Decrypt
5076	AES [197]	CBC [38A]	Key Sizes: 128	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 128	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 128	Encrypt, Decrypt
5077	AES [197]	CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		CFB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
5078	AES [197]	KW [38F]	Forward Key Sizes: 128, 256	Authenticated Encrypt, Authenticated Decrypt
5079	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		GCM [38D]	Key Sizes: 256 Tag Len: 128	Authenticated Encrypt, Authenticated Decrypt
VA	CKG [IG D.12]	[133r2] Section 5.1 Asymmetric signature key generation using unmodified DRBG output		Key Generation
		[133r2] Section 5.2 Asymmetric key establishment key generation using unmodified DRBG output		
		[133r2] Section 6.1 Direct symmetric key generation using unmodified DRBG output		
		[133r2] Section 6.2.1 Derivation of symmetric keys from a key agreement shared secret.		
		[133r2] Section 6.2.2 Derivation of symmetric keys from a pre-shared key		
1636	CVL: TLS [135]	v1.2	SHA (384)	Key Derivation

Cert	Algorithm	Mode	Description	Functions/Caveats
	CVL: SRTP [135]		AES-256	
A657	DRBG [90Ar1]	CTR	AES-256	Deterministic Random Bit Generation
C216	ECDSA [186]		P-384	KeyGen
			P-384 SHA (384)	SigGen
			P-384 SHA (384)	SigVer
3386	HMAC [198]	SHA-384	Key Sizes: 32 $\lambda = 48$	Message Authentication, KDF Primitive, Password Obfuscation
3387	HMAC [198]	SHA-384	Key Sizes: 32 $\lambda = 48$	Message Authentication, KDF Primitive, Password Obfuscation
VA	KAS [56Ar3]	KAS-SSC with KDA, vendor affirmed		key establishment methodology provides 192 bits of encryption strength
VA	KAS-SSC [56Ar3]	ECC (Initiator, Responder), KPG, Partial	P-384 SHA-384	Key Agreement Scheme provides 192 bits of encryption strength
VA	KDA [56Cr1] (§4.1)	SP 800-56Cr1 Section 4.1, Option 1 with SHA-384		Key Derivation
N/A	KTS [38F]	KW	AES (Cert #5078)	Key establishment methodology provides 128 or 256 bits of encryption strength
N/A	KTS [38F]	CBC, ECDSA	AES (Cert. #5077 and ECDSA (Cert. # C216) Authentication	Key establishment methodology provides 256 bits of encryption strength
4132	SHS [180]	SHA-256 SHA-384		Message Digest Generation, Password Obfuscation
4133	SHS [180]	SHA-256 SHA-384		Message Digest Generation, Password Obfuscation

Note: The TLS and SRTP protocol, other than the KDF, have not been tested by the CMVP or CAVP as per FIPS 140-2 Implementation Guidance D.11

Table 9 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
NDRNG	[IG G.13] Non-Deterministic RNG used for seeding the DRBG with 256-bits of security strength; 32 bits per access.

Table 10 – Non-Approved Cryptographic Functions

Algorithm	Description
DIA	Any drop-in algorithm (DIA) other than AES Certs. #5076 and #5077, as described in Section 2.1 of this Security Policy.

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

- ADP
- DES-XL
- DES-OFB
- DES-ECB
- DES-CBC
- DVI-XL
- DVP-XL
- Localized Capable

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

3.1 Critical Security Parameters

All CSPs used by the Module are described in this section. Usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4. It should be noted that Keys/CSPs stored in non-volatile memory/storage are normally preserved during a Program Update. However, all keys/CSPs are zeroized during a Program Update if one or more of the following occurs:

- The key database format/version changes between the resident and upgrade software images.
- The Module’s FIPS status changes, post-upgrade (this indicates that a non-FIPS compliant Drop-in algorithm has been loaded onto the Module)

Table 11 – Critical Security Parameters (CSPs)

CSP	Description / Usage
DRBG Entropy and Nonce Input	256 bits of entropy strength is used in seeding of the CTR_DRBG during DRBG instantiation at power-up. <ul style="list-style-type: none"> • Entry: N/A • Output: N/A • Storage: Plaintext in volatile memory

CSP	Description / Usage
	<ul style="list-style-type: none"> • Zeroization: Power Cycle • Generation: Internally generated using NDRNG
DRBG Internal State (V and Key)	<p>Internal state of SP800-90A CTR_DRBG (V and Key).</p> <ul style="list-style-type: none"> • Entry: N/A • Output: N/A • Storage: Plaintext in volatile memory • Zeroization: Power Cycle • Generation: Internally through SP800-90A CTR_DRBG state modification.
Key Protection Key (KPK)	<p>256-bit AES-CFB8 key used to encrypt TEKs, KEKs, the ECDSA Private Generated Signature Key, and the SRTP/ SRTCP Master Key stored in non-volatile memory.</p> <ul style="list-style-type: none"> • Entry: N/A • Output: N/A • Storage: Encrypted by the UKPPK in non-volatile memory • Zeroization: Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password • Generation: DRBG
Universal Key Protection Protection Key (UKPPK)	<p>A 256-bit AES-OFB key used for encrypting the KPK.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the Image Decryption Key and authenticated with the ECDSA Public Programmed Signature Key via the Program Update service • Output: N/A • Storage: Plaintext in volatile memory, plaintext in non-volatile memory • Zeroized: Program Update • Generation: N/A
Black Keyloading Key (BKK)	<p>256-bit AES KW (SP 800-38F) key used for encrypting keys that are input into the Module and output from the Module via the SDIO interface.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the Image Decryption Key and authenticated with the ECDSA Public Programmed Signature Key via the Program Update service • Output: N/A • Storage: Plaintext in volatile memory, plaintext in non-volatile. • Zeroization: Program Update • Generation: N/A
Image Decryption Key (IDK)	<p>A 256-bit AES-CBC key used to decrypt downloaded images.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the previous Image Decryption Key and authenticated with the ECDSA Public Programmed Signature Key via the Program Update service • Output: N/A • Storage: Plaintext in volatile memory, plaintext split-knowledge in non-volatile memory • Zeroization: Program Update • Generation: N/A

CSP	Description / Usage
Traffic Encryption Keys (TEKs)	<p>128 and 256-bit AES-OFB keys used for enabling secure communication with target devices. These keys could also be used for HMAC Key.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the KEK with AES SP 800-38F KTS • Output: Encrypted by a KEK with AES SP 800-38F KTS • Storage: Stored plaintext in volatile memory, encrypted by the KPK in non-volatile memory • Zeroization: Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete Key Variable • Generation: Established through SP800-56Ar3 KAS
Key Encryption Keys (KEKs)	<p>128 and 256-bit AES-KW keys used for encryption of keys in key transport operation. It could be also used as an HMAC Key.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the KEK with AES SP 800-38F KTS • Output: Encrypted by the KEK with AES SP 800-38F KTS • Storage: Stored plaintext in volatile memory, encrypted by the KPK in non-volatile memory • Zeroization: Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete Key Variable • Generation: Established through SP 800-56Ar3 KAS
Password Encryption Key (PEK)	<p>256-bit AES-CFB8 key used for decrypting passwords during password validation.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the Image Decryption Key and authenticated with the ECDSA Public Programmed Signature Key via the Program Update service • Output: N/A • Storage: Plaintext in non-volatile memory • Zeroization: Program Update • Generation: N/A
User Password	<p>14-32 ASCII printable characters User authentication password. The SHA-384 hash of the decrypted password is compared with the SHA-384 hash value stored in non-volatile memory during password validation</p> <ul style="list-style-type: none"> • Entry: Encrypted by the PEK with AES256-CFB8. • Output: N/A • Storage: Plaintext in volatile memory, SHA-384 hash of the plaintext password is encrypted by the PEK in non-volatile memory • Zeroization: Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password • Generation: N/A
CO Password	<p>14-32 ASCII printable characters CO authentication password. The SHA-384 hash value of the plaintext password is stored encrypted on the PEK in non-volatile memory. The SHA-384 hash of the decrypted password is compared with the SHA-384 hash value stored in non-volatile memory during password validation.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the PEK with AES256-CFB8.

CSP	Description / Usage
	<ul style="list-style-type: none"> • Output: N/A • Storage: Plaintext in volatile memory, SHA-384 hash of the plaintext password is encrypted by the PEK in non-volatile memory • Zeroization: Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password • Generation: N/A
Elliptic Curve Diffie-Hellman Private Key	Random value used to establish a shared secret over an insecure channel. <ul style="list-style-type: none"> • Entry: N/A • Output: N/A • Storage: Plaintext in volatile memory. • Zeroization: Power Cycle, Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete key Variable • Generation: FIPS 186-4 Key Generation on Perform Key Agreement Process service request
Elliptic Curve Diffie-Hellman Shared Secret	The Elliptic Curve Diffie-Hellman Shared Secret is output as part of the Diffie-Hellman key agreement protocol. <ul style="list-style-type: none"> • Entry: N/A • Output: N/A • Storage: Plaintext in volatile memory • Zeroization: Power Cycle, Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete Key Variable • Generation: Established through SP800-56Ar3 KAS
ECDSA Private Generated Signature Key (PGSK)	384-bit ECDSA key used to generate the signature of the input data from the Generate Signature service request. <ul style="list-style-type: none"> • Entry: N/A • Output: N/A • Storage: Plaintext in volatile memory, encrypted by a KPK in non-volatile memory. • Zeroization: Power Cycle, Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete Key Variable • Generation: FIPS 186-4 Key Generation on Generate Key Variable service request
SRTP/SRTCP Master Key	256-bit master key used in the SRTP/SRTCP based derivation of KDF Derived Keys <ul style="list-style-type: none"> • Entry: Encrypted by the KEK with AES SP 800-38F KTS • Output: Encrypted by the KEK with AES SP 800-38F KTS • Storage: Stored plaintext in volatile memory, encrypted by the KPK in non-volatile memory • Zeroization: Power Cycle, Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete Key Variable • Generation: Internally generated using DRBG or derived from SRTP/SRTCP KDF on Generate Key Variable service request

CSP	Description / Usage
SRTP/SRTCP Master Salt	<p>112-bit key used to generate keys using SRTP KDF protocol, or 96-bit key to generate IV internally for AES GCM encryption operation.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the KEK with AES SP 800-38F KTS • Output: Encrypted by the KEK with AES SP 800-38F KTS • Storage: Plaintext in volatile memory • Zeroization: Power Cycle, Program update, Validate CO password, Change CO password, Configure module, Validate User password, Change User password, Delete key variable • Generation: Internally generated using DRBG or derived from SRTP/SRTCP KDF on Generate Key Variable service request
TLS KDF Secret	<p>Secret input used in the TLS-based derivation of KDF Derived Keys. In practice, this input will typically be the Premaster Secret or Master Secret as defined in RFC 5246, but is dependent on the operator.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the KEK with AES SP 800-38F KTS • Output: Encrypted by the KEK with AES SP 800-38F KTS • Storage: Plaintext in volatile memory • Zeroization: Power Cycle, Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete Key Variable • Generation: Internally generated using DRBG or derived from TLS KDF on Generate Key Variable service request
KDF Derived Key	<p>Keys derived using TLS or SRTP KDFs. Module does not have control over the usage of these generated keys, the operator decides the usage. KDF output is always 384 bits, but a key of less length may be derived using a subset of this output.</p> <ul style="list-style-type: none"> • Entry: N/A • Output: Encrypted by the KEK with AES KW SP 800-38F KTS • Storage: Plaintext in volatile memory • Zeroization: Power Cycle, Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete Key Variable • Generation: Internally derived through TLS or SRTP/SRTCP KDF on Generate Key Variable service request

3.2 Public Keys

Table 12 – Public Keys

Key	Description / Usage
ECDSA Public Programmed Signature Key	<p>384-bit ECDSA public key used to validate the signature of the firmware image being loaded before it is allowed to be executed.</p> <ul style="list-style-type: none"> • Entry: Encrypted by the Image Decryption Key and authenticated with the ECDSA Public Programmed Signature Key via the Program Update service. The first key is loaded in manufacturing.

Key	Description / Usage
	<ul style="list-style-type: none"> • Output: N/A • Storage: Plaintext in non-volatile memory • Zeroization: Program Update • Generation: N/A
ECDSA Public Generated Signature Key	<p>384-bit ECDSA key used to verify signatures.</p> <ul style="list-style-type: none"> • Entry: N/A • Output: Plaintext • Storage: Plaintext in volatile memory • Zeroization: Delete Key Variable, Power cycle • Generation: FIPS 186-4 Key Generation on Generate Key Variable service request
Elliptic Curve Diffie-Hellman Public Key	<p>Used to establish a shared secret over an insecure channel.</p> <ul style="list-style-type: none"> • Entry: N/A • Output: Plaintext • Storage: Plaintext in volatile memory • Zeroization: Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete Key Variable • Generation: FIPS 186-4 Key Generation on Perform Key Agreement Process service request
Remote Party Diffie-Hellman Ephemeral Public Key	<p>Used to establish a shared secret over an insecure channel.</p> <ul style="list-style-type: none"> • Entry: Plaintext • Output: N/A • Storage: Plaintext in volatile memory • Zeroization: Program Update, Validate CO Password, Change CO Password, Configure Module, Validate User Password, Change User Password, Delete Key Variable • Generation: N/A

4 Roles, Authentication and Services

4.1 Assumption of Roles

The Module supports a User and Cryptographic Officer (CO) role. Authentication data is initialized to a default value in manufacturing which is sent to the customer along with the module. After authenticating, the CO and User passwords may be changed at any time. The Module enforces the separation of roles using login credentials. Re-authentication is enforced when changing roles.

Table 13 lists all operator roles supported by the Module. The Module does not support a maintenance role or bypass capability. The Module does not support concurrent operators.

Table 13 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Crypto Officer (CO) Role over SDIO interface.	Identity-based	14-32 character ASCII password
User	User Role over SDIO interface.	Identity-based	14-32 character ASCII password

4.2 Authentication Methods

Password Authentication

Since the minimum password length is 14 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in 95^{14} or 1 in 4.8×10^{27} which is less than 1 in 1,000,000.

The Module has a default setting of 15 consecutive failed attempts which is the maximum setting. The worst-case probability of a successful random attempt within a one-minute period is $15/95^{14}$ which is less than 1 in 100,000.

After a configurable number (Default is set to 15) of consecutive failed attempts, the KPK, TEKs and KEKs are zeroized, a new KPK is generated, and the password is reset to the factory default. Note that this makes it very important that physical access to the Module is strictly controlled. The Module is not usable until the factory default password is changed.

4.3 Services

All services implemented by the Module are listed in the tables below. Note that all services listed in Table 14 and Table 15 below are available in both the FIPS Approved and non-Approved mode. The only distinguishing factor between Approved and non-Approved services is whether non-Approved algorithms/ key establishment schemes are available.

Table 14 – Authenticated Services

Service	Description	CO	User
Program Update	Update the Module firmware via the SDIO interface. All keys (stored in volatile and non-volatile memory) and CSPs may be zeroized during a Program Update.	X	X
Validate CO password	Validate the current CO password used to identify and authenticate the CO role via the SDIO interface. Successful authentication will allow access to services allowed for the CO.	X	
Change CO password	Modify the current password used to identify and authenticate the CO Role via SDIO interface.	X	

Service	Description	CO	User
Extract Action Log	Exports a history of actions over the SDIO interface.	X	X
Logout CO Role	Logs out the CO.	X	
Configure Module	Perform configuration of the Module (e.g. time configuration, enable/disable clear key import, enable/disable red keyloading, etc.) via the SDIO interface.	X	
Validate User Password	Validate the current User password used to identify and authenticate the User role via the SDIO interface. Successful authentication will allow access to crypto services allowed for the User.		X
Change User Password	Modify the current password used to identify and authenticate the User Role via the SDIO interface.		X
Algorithm List Query	Provides a list of algorithms over the SDIO interface.		X
Logout User Role	Logs out the User.		X
Export Key Variable	Transfer encrypted key variables (e.g. KEKs, TEKs) out of the Module over the SDIO interface.		X
Import Key Variable	Receive encrypted key variables (e.g. KEKs, and TEKs) over the SDIO interface.		X
Generate Key Variable	Auto-generate Public and Private Generated Signature Keys, SRTP/SRTCP Master Key, SRTP/ SRTCP Master Salt, TLS Master Secret Key and the KPK within the Module.		X
Delete Key Variable	Delete KEKs, TEKs, ECDH Public and Private Keys, ECDH Public and Private Generated Signature Keys, and ECDH Shared Secret.		X
Encrypt	Encrypt plaintext data to be transferred over the SDIO interface.		X
Decrypt	Decrypt ciphertext data received over the SDIO interface.		X
Generate Signature	Generate a Signature and output result over SDIO interface.		X
Verify Signature	Verify a Signature and output result over SDIO interface.		X
Generate Hash	Generate a hash and output result over SDIO interface.		X
Generate MAC	Generate a Message Authentication Code of a block of data to provide data integrity using a shared symmetric key.		X
Perform Key Agreement Process	Perform a key agreement process over SDIO interface		X
Generate Random Number	Generate random data using DRBG and output result over SDIO interface.		X

Service	Description	CO	User
Key Query	Retrieve the metadata for a given key present in the Module.		X

Table 15 – Unauthenticated Services

Service	Description
Perform Self-Tests	Performs module self-tests comprised of cryptographic algorithms test and firmware test. Initiated by a transition from power off state to power on state.
Version Query	Provides module firmware version number and FIPS status over the SDIO interface.

Table 16 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- R = Read: The service reads the CSP.
- W = Write: The service writes to the CSP.
- X = Execute: The service uses the CSP for a cryptographic operation.
- G = Generate: The service generates to the CSP.
- Z = Zeroize: The service zeroizes to the CSP.

Table 16 – Security Parameters Access by Service

Service	CSPs and Public Keys																					
	DRBG Entropy Input	DRBG Internal State (V and Key)	PEK	TEKS	KEKs	KPK	IDK	UKPPK	BKK	CO Password	User Password	ECDSA Private Generated Signature Key	ECDSA Public Programmed Signature Key	ECDSA Public Generated Signature Key	ECDH Private Key	ECDH Shared Secret	ECDH Public Key	Remote Party DHE Public Key	SRTP/SRTCP Master Key	SRTP/SRTCP Master Salt	TLS KDF Secret	KDF Derived Key
Program Update	-	-	RWZ	Z	Z	GWZ	RWXZ	RWXZ	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Configure Module	-	-	RX	Z	Z	GWZ	-	-	-	RWXZ	RWXZ	Z	-	Z	Z	Z	Z	Z	Z	Z	Z	Z
Validate CO Password	-	-	RX	Z	Z	GWZ	-	-	-	RXZ	Z	Z	-	Z	Z	Z	Z	Z	Z	Z	Z	Z
Change CO Password	-	-	RX	Z	Z	GWZ	-	-	-	RWXZ	Z	Z	-	Z	Z	Z	Z	Z	Z	Z	Z	Z
Logout CO Role	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Validate User Password	-	-	RX	Z	Z	GWZ	-	-	-	Z	RXZ	Z	-	Z	Z	Z	Z	Z	Z	Z	Z	Z
Change User Password	-	-	RX	Z	Z	GWZ	-	-	-	Z	RWXZ	Z	-	Z	Z	Z	Z	Z	Z	Z	Z	Z
Logout User Role	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Extract Action Log	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Algorithm List Query	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Export Key Variable	-	-	-	R	R	R	-	-	RX	-	-	R	-	-	R	R	-	-	R	R	R	R
Import Key Variable	-	-	-	W	W	W	-	-	RX	-	-	W	-	-	W	W	-	-	W	W	W	-
Generate Key Variable	-	WX	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	GW	GW	GW	GW
Delete Key Variable	-	-	-	Z	Z	-	-	-	-	-	-	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Encrypt	-	WX	-	RX	-	-	-	-	-	-	-	-	-	-	-	-	-	-	RX	RX	RX	RX

Service	CSPs and Public Keys																						
	DRBG Entropy Input	DRBG Internal State (V and Key)	PEK	TEKs	KEKs	KPK	IDK	UKPPK	BKK	CO Password	User Password	ECDSA Private Generated Signature Key	ECDSA Public Programmed Signature Key	ECDSA Public Generated Signature Key	ECDH Private Key	ECDH Shared Secret	ECDH Public Key	Remote Party DHE Public Key	SRTP/SRTCP Master Key	SRTP/SRTCP Master Salt	TLS KDF Secret	KDF Derived Key	
Decrypt	-	-	-	RX	-	-	-	-	-	-	-	-	-	-	-	-	-	-	RX	RX	RX	RX	
Generate Signature	-	WX	-	-	-	-	-	-	-	-	-	RWX	-	RWX	-	-	-	-	-	-	-	-	
Verify Signature	-	-	-	-	-	-	-	-	-	-	-	-	-	X	-	-	-	-	-	-	-	-	
Generate Hash	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Generate MAC	-	-	-	RX	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Perform Key Agreement Process	-	WX	-	RW	RW	-	-	-	RX	-	-	-	-	-	-	GWX	GWX	GWX	WX	-	-	-	-
Generate Random Number	-	WX	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	
Key Query	-	-	-	R	R	R	-	-	-	-	-	-	-	-	-	-	-	-	R	R	R	R	
Perform Self-Tests	-	-	-	-	-	-	-	-	-	-	-	-	RX	-	-	-	-	-	-	-	-	-	
Version Query	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	

5 Self-Tests

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

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptographic functionality by the Module. The Module toggles the self-test Indicator interface within 2 seconds of power-up to indicate the Firmware Integrity Test, Firmware Load Test, Cryptographic Algorithm Tests, and Critical Functions Test have completed successfully. The Module enters the Critical Error state and does not toggle the self-test Indicator interface if the Firmware Integrity Test, Firmware Load Test, Cryptographic Algorithm Tests, or Critical Functions Test fails. The Critical Error state may be exited by powering the Module off then on.

The Module performs the following algorithm KATs on power-up.

- Firmware Integrity: A digital signature is generated over the base firmware and all Drop-in algorithms code when it is built using SHA-384 (Cert. #4132) and ECDSA P-384 and is stored with the code upon download into the Module. When the Module is powered up the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.
- AES-128 encrypt and decrypt KATS (AES Certs. #5075 (ECB mode) and #5076 (CBC, CTR and OFB modes))
- AES-256 encrypt and decrypt KATS (AES Certs. #5077 (CBC, CFB, CTR and OFB modes) and #5079 (ECB and GCM modes))
- ECDSA P-384 key generation KAT
- ECDSA P-384 signature generation and verification KATs.
- Diffie-Hellman primitive “Z” computation KAT per IG 9.6.
- SHA-256 and -384 KATs (Cert. #4132).
- SHA-256 and -384 KATs (Cert. #4133).
- HMAC-384 KAT (Cert. #3386).
- HMAC-384 KAT (Cert. #3387).
- CTR DRBG (SP 800-90Ar1) KAT.
- AES KW (SP 800-38F) KAT.
- One-Step KDA [56Cr1] (§4.1) KAT.

The Module performs the following critical functions tests as indicated.

- The Module performs a read/write test of the internal RAM at each power up.
- Random Number Generator entropy test. This test runs two RNG statistical tests: a FIPS monobit test, and a FIPS “runs” test as defined in SP 800-22r1a.

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

- ECDSA Pairwise consistency test on ECDSA key pair generation: The ECDSA Public and Private Generated Signature Key pair is tested by the calculation and verification of a digital signature. If the digital signature cannot be verified, the test fails.

- Continuous Random Number Generator test: The continuous random number generator test is performed on the NDRNG and DRBG supported by the Module. An initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. A successive call to NDRNG/DRBG generates a new set of data, which is compared to the comparison data. If a match is detected, this test fails; otherwise the new data is stored as the comparison data and returned to the caller. This testing is done for each 4-byte NDRNG and 16-byte data block generated by the DRBG. The Module enters the Critical Error State if this test fails.
- SP800-90A DRBG health tests.
- Firmware load test: a digital signature is generated over the code when it is built using SHA-384 (Cert. #4132) and ECDSA P-384. Upon download into the Module, the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.

6 Physical Security Policy

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

The Module is covered with a hard, opaque metallic enclosure that provides evidence of attempts to tamper with the Module. Tampering with the Module will cause it to enter a lock-up state in which no cryptographic services will be available.

No maintenance access interface is available.

7 Operational Environment

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

8 Mitigation of Other Attacks Policy

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

9 Security Rules and Guidance

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

9.1 Invariant Rules

1. An operator does not have access to any cryptographic services prior to assuming an authorized role.
2. Power up self-tests do not require any operator action.

3. Data output is inhibited during key generation, self-tests, zeroization, and while in critical error states.
4. The Module does not perform any cryptographic functions while in an error state.
5. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the Module.
6. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
7. The module clears previous authentications on power cycle.
8. The Module does not support manual key entry.
9. The Module does not enter or output plaintext CSPs in the Approved mode.
10. The Module implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
11. The Module conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.

10 AES-256 GCM IV Generation Protocol

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

- TLS: 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. 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 FIPS140-2 IG A.5, Option 1. The fixed field consists of a 16-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 TLS 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 FIPS140-2 IG A.5, 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 FIPS140-2 IG A.5, 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.

11 References and Definitions

The following standards are referred to in this Security Policy.

Table 17 – References

Abbreviation	Full Specification Name
[FIPS140-2]	<i>Security Requirements for Cryptographic Modules, May 25, 2001</i>
[IG]	<i>Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program</i>
[108]	<i>NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009</i>
[131A]	<i>Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, March 2019</i>
[133r2]	<i>NIST Special Publication 800-133 Revision 2, Recommendation for Cryptographic Key Generation, June 2020</i>
[135]	<i>National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.</i>
[186]	<i>National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July 2013.</i>
[197]	<i>National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001</i>
[198]	<i>National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008</i>
[180]	<i>National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015</i>
[22r1a]	<i>National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010</i>
[38A]	<i>National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001</i>
[38B]	<i>National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005</i>
[38D]	<i>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</i>

Abbreviation	Full Specification Name
[38F]	<i>National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012</i>
[52r2]	<i>Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, NIST Special Publication 800-52 Revision 2, Aug 2019</i>
[56Ar3]	<i>NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018</i>
[90Ar1]	<i>National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A Revision 1, June 2015.</i>
[RFC2246]	<i>The TLS Protocol, August 2008</i>
[RFC3711]	<i>The Secure Real-time Transport Protocol (SRTP), March 2004</i>
[RFC5286]	<i>AES Galois Counter Mode (GCM) Cipher Suites for TLS, August 2008</i>
[RFC5246]	<i>The Transport Layer Security (TLS) Protocol, August 2008</i>
[RFC7714]	<i>AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP), December 2015</i>

Table 18 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
BKK	Black Keyloading Key
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CO	Cryptographic Officer
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
FW	Firmware
GCM	Galois/Counter Mode
IDK	Image Decryption Key
IV	Initialization Vector

Acronym	Definition
KDA	Key Derivation Algorithm
KDF	Key Derivation Function
KLK	Key Loss Key
KPK	Key Protection Key
KEK	Key Encryption Key
KVL	Key Variable Loader
PEK	Password Encryption Key
PGSK	Private Generated Signature Key
NDRNG	Non-Deterministic Random Number Generator
SRTP	Secure Real-time Transport Protocol
SRTCP	Secure Real-time Transport Control Protocol
TEK	Traffic Encryption Key
TLS	Transport Layer Security
UKPPK	Universal Key Protection Protection Key