Non-Proprietary FIPS 140-2 Security Policy:

KMF/Wave/Traffic CryptR

Document Version: 1.3

Date: October 3, 2022

Table of Contents

1 Introduction

This document defines the Security Policy for the Motorola Solutions KMF/WAVE/Traffic CryptR module, hereafter denoted the Module. The Module is a production grade, multi-chip standalone cryptographic module as defined by FIPS 140-2 and is designed to meet Level 2 Physical Security requirements. The Module provides encryption and decryption services for secure key management, Over-the-Air-Rekeying (OTAR), and secure voice/data traffic for Motorola's Key Management Facility (KMF) and Motorola's Wave System. In the Wave System, the Module is referred to as the Wave CryptR/Traffic CryptR. In the Astro System, the Module is referred to as the KMF CryptR. The KMF and KMF CryptR combine to provide cryptographic services for Motorola's APCO-25 compliant Astro™ radio systems.

Table 1 – Cryptographic Module Configuration

Module	HW P/N* and Version	Base FW Version
KMF/Wave/Traffic CryptR	CLN8566A, Rev. 0x1 CLN1875A, Rev. 0x1	R03.07.04

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)	C489
AES256	R01.00.03 (0x52010003)	C491

Table 3 – Non-Approved Mode Drop-in Algorithms

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

The Module is intended for use by the markets that require FIPS 140-2 validated overall security level 2.

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

Table 4 – Security Level of Security Requirements

Security Requirement	Security Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall	**2**

1.1 Module Description and Cryptographic Boundary

The module's cryptographic boundary is drawn around the entire product which includes the housing, various IC's, FLASH, RAM, and Printed Circuit Board as shown in Figure 1.

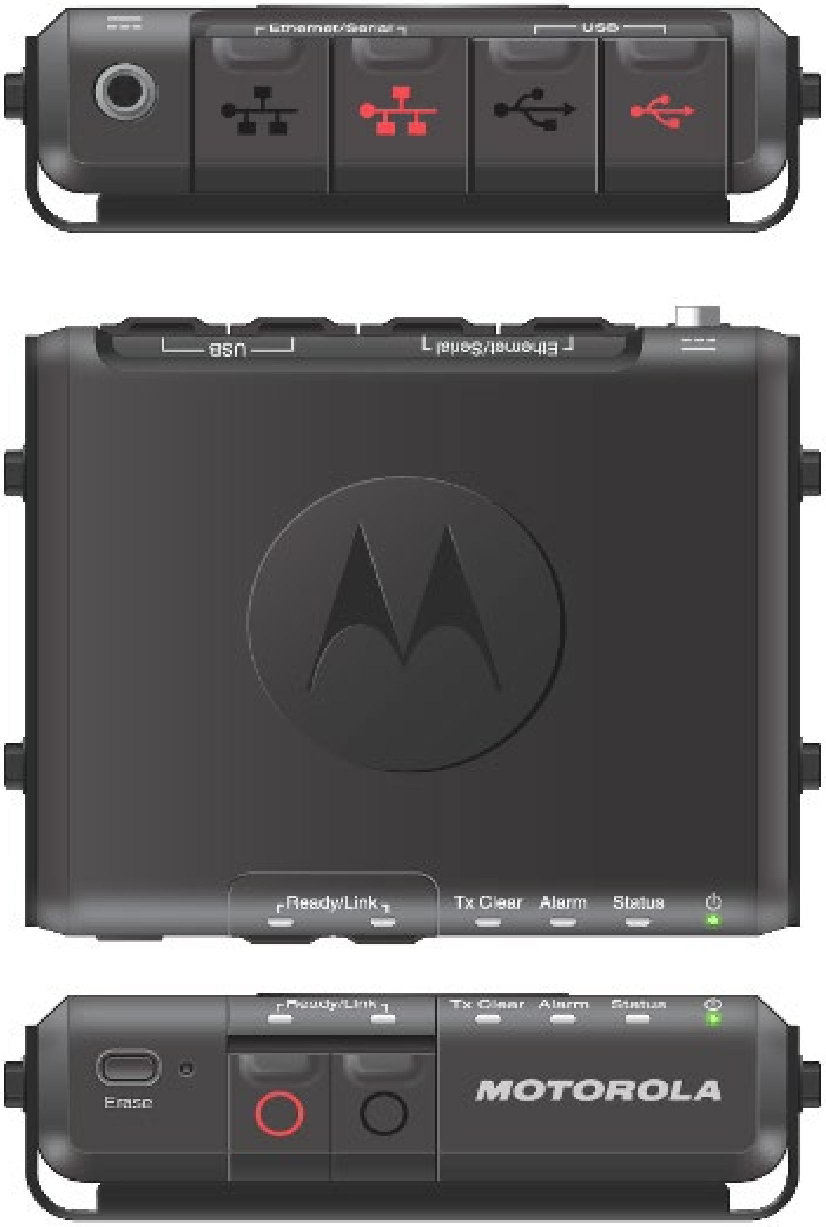

Figure 1: The Module – Rear, Top and Front View

The Module's ports and associated FIPS defined logical interface categories are listed in Table 5. The module consists of two (2) areas. The Black ports and Red ports, as seen in Figure 1. The black ports are only available for use on HW P/N CLN8566A with limited functionality and they do not allow any crypto functions.

Table 5 – 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
Key Variable Loader (KVL) Interface (RED)	Provides an interface to the Key Variable Loader. The TEK/KEKs are entered in encrypted form over the KVL interface.	Data Input Data Output Control Input Status Output
Key Variable Loader (KVL) Interface (BLACK)	Only used for version information and program update.	Data Input Status Output
RS-232 Serial to Ethernet Interface (RED)	Provides an interface for execution of RS-232 shell commands. This interface does not support output of CSP's.	Data Output Control Input Status Output
Mini-Universal Serial Bus (mini-USB) Interface	Provides an interface for execution of RS-232 shell commands. This interface does not support output of CSP's.	Data Output Control Input Status Output
USB Interfaces (RED and BLACK)	These ports are not used by the Module	N/A
Ethernet Interface (RED)	This interface routes packets to the Host. All CSPs exchanged over this interface are always encrypted when operating in FIPS Approved mode. This interface also supports the input of encrypted passwords for operator authentication.	Data Input Data Output Control Input Status Output
Ethernet Interface (BLACK)	Only used for displaying power-up status.	Status Output
Erase Switch	This interface is used for zeroization of KEKs, TEKs.	Control Input
Reset Switch	This interface forces a reset of the Module.	Control Input
Alarm LED Output	The Alarm LED output turns solid red to indicate an unrecoverable error has been encountered and flashing red to indicate a security condition has been detected that requires operator intervention.	Status Output
Power LED Output	The Power LED output turns steady green after power is applied, flashes five times on power-up, and flashing green to indicate a low or dead battery.	Status Output
Ready LED Output (RED)	The Ready LED (red) output turns solid green to indicate an Ethernet link has been established and is flashing green when there is activity on the link. This LED will turn red if the KVL or serial shell interface is enabled; if there is a failure on the KVL or serial interface the LED will flash red twice and turn off (note if the Ethernet interface is also enabled the LED will be orange for these operations).	Status Output
Ready LED Output (BLACK)	The Ready LED output is not used and remains off other than at power-up or programming.	Status Output

Port	Description	Logical Interface Type
TX Clear LED Output	The TX Clear LED output turns orange during a firmware upgrade failure. Otherwise, it is not used and remains off other than during power-up self-test when the LED turns green momentarily.	Status Output
Status LED Output	The Status LED output is steady red when no key has been loaded and green when a key has been loaded.	Status Output

2 Modes of Operation

The Module can be configured to operate in a FIPS 140-2 Approved mode of operation 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 6. Note that AES-128 and/or AES-256 drop-in algorithms may or may not be loaded into the Module, however if they are loaded, they must match the values in Table 2 to be in the Approved mode.

Table 6 – Approved Mode Indicator

Item ID	Value	Meaning
0x06 (FIPS)	0x02	FIPS Approved mode
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: http://csrc.nist.gov/groups/STM/cmvp/validation.html

2.1 Approved Mode Configuration

Certain requirements must be met in order for the module to operate in an Approved mode. First, the Module Configuration service must be used to ensure that the following parameters are disabled:

1. Clear Key Import
2. Clear Key Export
3. Key Loss Key (KLK)

Enabling any of the above parameters will force the Module to transition into a non-Approved mode. Additionally, the operator is responsible for seeding the Module's DRBG [90A] using the Load Entropy service listed in Table 13. If the Module does not receive external entropy, the Module will not operate in an Approved mode. Furthermore, 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. However, in order to remain in the Approved mode, only Approved algorithms may be loaded into the Module; in particular AES-128 (Cert. #C489) and/or AES-256 (Cert. #C491).

Finally, an operator must also adhere to the procedural enforcement requirements documented in Section 9.2 of this Security Policy.

3 Cryptographic Functionality

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

Table 7 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
C489	AES [197]	ECB [38A]	Key Sizes: 128	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 128	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 128	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 128	Encrypt, Decrypt
C490	AES [197]	OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CFB8 [38A]	Key Sizes: 256	Encrypt, Decrypt
C491	AES [197]	ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		CTR [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
		GCM [38D]	Key Sizes: 256 Tag Len: 128	Authenticated Encrypt, Authenticated Decrypt
C492	AES [197]	KW [38F]	Forward Key Sizes: 128, 256	Authenticated Encrypt, Authenticated Decrypt
VA	CKG [IG D.12]	[133rev2] Section 4 and 6.1 Direct symmetric key generation using unmodified DRBG output		Key Generation
C496	CVL: TLS [135]	v1.2	SHA (384)	Key Derivation
	CVL: SRTP [135]		AES-256	
C494	DRBG [90A]	CTR	Use_df AES-256	Deterministic Random Bit Generation[1]
C495	ECDSA [186]		P-384	KeyGen
			P-384 SHA (384)	SigGen
			P-384 SHA (384)	SigVer
C493	HMAC [198]	SHA-384	Key Sizes: 32 $\lambda = 48$	Message Authentication, KDF Primitive, Password Obfuscation
A1761	KAS [56Ar3]	ECC (Initiator, Responder), KPG, Partial with oneStepKdf.	P-384 SHA-384	Key Agreement Scheme provides 192 bits of encryption strength

[1] The entropy for seeding the SP 800-90A DRBG is determined by the user of the module which is outside of the module's physical boundary. The target application 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 calling module defined API function. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys.

Cert	Algorithm	Mode	Description	Functions/Caveats
N/A	KTS [38F]	KW	AES Cert. #C492	Key Establishment methodology provides 128 or 256 bits of encryption strength
N/A	KTS [IG D.9]	GCM	AES Cert. #C491	Key Establishment
N/A	KTS [IG D.9]	CBC, ECDSA	AES Cert. #C491 and ECDSA Cert. #C495	
C493	SHS [180]	SHA-256 SHA-384		

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 8 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
AES Key Unwrap	[IG D.9] AES-OFB (Cert. #C489) key unwrapping for use in key transport; provides 128 bits of encryption strength.
AES Key Unwrap	[IG D.9] AES-OFB (Cert. #C490) key unwrapping for use in key transport; provides 256 bits of encryption strength.
AES Key Unwrap	[IG D.9] AES-OFB (Cert. #C491) key unwrapping for use in key transport; provides 256 bits of encryption strength.
AES MAC	[IG G.13] AES Cert. #C492, vendor affirmed; P25 AES OTAR

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

- ADP
- AES-OFB Key Wrap
- DES-CBC
- DES-ECB
- DES-OFB
- DES-XL
- DVI-XL
- DVP-XL

Note that all of the above are "drop-in" algorithms, except AES-OFB Key Wrap.

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 9 – Critical Security Parameters (CSPs)

CSP	Description / Usage
Input String	384-2048-bit string entered into the module from an external source for input into the DRBG Seed. The input string is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. • Entry: Encrypted entropy supplied from an external source. • Output: N/A • Storage: Plaintext in volatile memory • Zeroization: on power cycle • Generation: N/A
SP800-90A DRBG Seed	384-bit seed value used within the SP800-90A DRBG. This seed is derived using the Input String as external entropy (between 384-2048 bits and an internally generated personalization string (256-bits). The seed is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. • Entry: N/A • Output: N/A • Storage: Plaintext in the volatile memory • Zeroization: Power cycle • Generation: Internally by combining entropy from an external source and an internally generated personalization string
DRBG Internal State (V and Key)	Internal state of SP800-90A CTR_DRBG (V and Key). • Entry: N/A • Output: N/A • Storage: Plaintext in the volatile memory • Zeroization: Power cycle • Generation: SP800-90A CTR_DRBG state modification.
DRBG Seed Encryption Key (DSEK)	256-bit AES-KW key used to decrypt the external entropy seed (input string). • 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
Key Protection Key (KPK)	256-bit AES-CFB8 key used to encrypt all other keys (except KVL-BKK, PEK, UKPPK, and IDK) stored in non-volatile memory. • Entry: N/A • Output: N/A

CSP	Description / Usage
	• Storage: Encrypted by the UKPPK in non-volatile memory (flash) and/ or stored in plaintext in non-volatile memory (BB-RAM) • Zeroization: Program Update • Generation: DRBG
Universal Key Protection Protection Key (UKPPK)	256-bit AES-OFB key used for encrypting the KPK. • 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 • Zeroization: Power cycle, Program Update • Generation: N/A
Key Variable Loader Black Keyloading Key (KVL-BKK)	256-bit AES-OFB key used for encrypting keys that are input into the Module when connected to the KVL. • 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 • Zeroization: Power cycle, Program Update • Generation: N/A
Image Decryption Key (IDK)	A 256-bit AES-CBC key used to decrypt downloaded images. • 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 • Zeroization: Power cycle, Program Update • Generation: N/A
Traffic Encryption Keys (TEKs)	128 and 256-bit AES-OFB keys used for enabling secure communication with target devices. It could be also used for HMAC Key, encryption and authentication of Key Management Messages in OTAR. • Entry: Encrypted by the KVL-BKK with AES256 OFB key unwrap or plaintext when authenticated to the KVL role. Encrypted with KEK with AES SP 800-38F KTS, when authenticated to the User role. • Output: Encrypted by a KEK with AES SP 800-38F KTS (KW or OTAR format) over the Ethernet Interface. • Storage: Stored plaintext in volatile memory, AES256-CFB8 encrypted by the KPK in non-volatile memory • Zeroization: Delete Key Variable, Power cycle, OTAR, Store & Forward, and Program Update • Generation: Established through SP 800-56Ar3 KAS
Key Encryption Keys (KEKs)	128 and 256-bit AES-KW or AES-OFB keys used for enabling secure communication with target devices. It could be also used as an HMAC Key.

CSP	Description / Usage
	• Entry: Encrypted by the KVL-BKK with AES256 OFB key unwrap or plaintext when authenticated to the KVL. Encrypted by the KEK with AES SP 800-38F KTS when authenticated to the User role. • Output: Encrypted by a KEK with AES SP 800-38F KTS (KW or OTAR format) over the Ethernet Interface. • Storage: Stored plaintext in volatile memory, AES256-CFB8 encrypted by the KPK in non-volatile memory • Zeroization: Delete Key Variable, Power cycle and Program Update • Generation: Established through SP 800-56Ar3 KAS
Password Encryption Key (PEK)	256-bit AES-CFB8 key used for decrypting passwords during password validation. • 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	8-32 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 • 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: Power cycle, Program Update, Change User Password • Generation: N/A
Crypto-Officer Password	8-32 ASCII printable characters Crypto-Officer 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. • 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: Power cycle, Program Update, Change Crypto-Officer Password • Generation: N/A
Elliptic Curve Diffie-Hellman Private Key	Random value used to establish a shared secret over an insecure channel. • Entry: N/A • Output: N/A • Storage: Plaintext in volatile memory. • Zeroization: Delete Key Variable, Power cycle, Program Update • Generation: Power cycle, FIPS 186-4 Key Generation on Perform Key Agreement service request

CSP	Description / Usage
Elliptic Curve Diffie-Hellman Shared Secret	The Elliptic Curve Diffie-Hellman Shared Secret is established as part of the Diffie-Hellman key agreement protocol. • Entry: N/A • Output: N/A • Storage: Plaintext in volatile memory • Zeroization: Power cycle, Program Update • 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. • Entry: N/A • Output: N/A • Storage: Plaintext in volatile memory, encrypted by a KPK in non-volatile memory. • Zeroization: Delete Key Variable, Power cycle, Program Update • 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 • Entry: Encrypted by the KVL-BKK with AES256 OFB mode when authenticated to the KVL role. Encrypted by a KEK with AES SP 800-38F KTS or AES OFB key unwrap, depending on host selection when authenticated to the User role. • Output: Encrypted by a KEK (User Role only) with AES SP 800-38F KTS (KW or OTAR format) or AES OFB mode over the Ethernet Interface • Storage: Stored plaintext in volatile memory, encrypted by the KPK in non-volatile memory • Zeroization: Delete Key Variable, Power cycle, Program Update • Generation: Internally generated using DRBG or externally generated and pushed from the KVL
SRTP/SRTCP Master Salt	112-bit key used to generate keys using SRTP KDF protocol, or 96-bit key to generate IV internally for AES GCM encryption operation. • Entry: Encrypted by a KEK (User Role only) with AES SP 800-38F KTS (KW or OTAR format) or AES OFB key unwrap over the Ethernet Interface • Output: Encrypted by a KEK (User Role only) with AES SP 800-38F KTS (KW or OTAR format) over the Ethernet Interface • Storage: Plaintext in volatile memory • Zeroization: Delete Key Variable, Power cycle • Generation: Internally generated using DRBG or externally generated and pushed from the KVL
TLS KDF Secret	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. • Entry: Encrypted by a KEK (User Role only) with AES SP 800-38F KTS (KW or OTAR format) or AES OFB key unwrap over the Ethernet Interface

CSP	Description / Usage
	- Output: N/A - Storage: Plaintext in volatile memory - Zeroization: Delete Key Variable, Power cycle - Generation: Internally generated using DRBG or externally generated and pushed from the KVL
KDF Derived Key	Keys derived using TLS or SRTP/SRTCP 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. - Entry: N/A - Output: Encrypted by a KEK (User Role only) with AES SP 800-38F KTS (KW or OTAR format) over the Ethernet Interface - Storage: Plaintext in volatile memory - Zeroization: Delete Key Variable, Power cycle - Generation: Internally derived through TLS or SRTP/ SRTCP KDF on Generate Key Variable service request

3.2 Public Keys

Table 10 – Public Keys

Key	Description / Usage
ECDSA Public Programmed Signature Key	384-bit ECDSA public key used to validate the signature of the firmware image being loaded before it is allowed to be executed. - 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. - Output: N/A - Storage: Plaintext in non-volatile memory - Zeroization: Program Update - Generation: N/A
ECDSA Public Generated Signature Key	384-bit ECDSA key used to verify signatures. - Entry: N/A - Output: Plaintext over the Ethernet interface - 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	Used to establish a shared secret over an insecure channel. - Entry: N/A - Output: Plaintext over the Ethernet interface - Storage: Plaintext in volatile memory - Zeroization: Delete Key Variable, Power cycle

Key	Description / Usage
	• Generation: FIPS 186-4 Key Generation on Perform Key Agreement Process service request
Remote Party Diffie-Hellman Ephemeral Public Key	Used to establish a shared secret over an insecure channel. • Entry: Plaintext over Ethernet interface • Output: N/A • Storage: Plaintext in volatile memory • Zeroization: Delete Key Variable, Power cycle • Generation: N/A

4 Roles, Authentication and Services

4.1 Assumption of Roles

The Module supports a User, KVL and Cryptographic Officer (CO) role. Authentication data is initialized to a default value in manufacturing and are sent in encrypted form to the Module for authentication. After authenticating, the Crypto-Officer 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.

The KVL role is authenticated by the KVL-BKK to configure the Module via KVL Interface, Zeroize Keys via KVL Interface, Key Query, and Store & Forward services.

Table 11 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 11 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer Role over Ethernet interface.	Identity-based	8-32 character ASCII password
User	User Role over Ethernet interface.	Identity-based	8-32 character ASCII password
KVL	When a User or CO is connected to the Module through a Motorola KVL device.	Role-based	256-bit AES key (KVL-BKK)

4.2 Authentication Methods

Password Authentication

Since the minimum password length is 8 (default is 15) ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in 95^8 which is less than 1 in 1,000,000.

The Module limits the number of consecutive failed authentication attempts to a configurable number (factory default 10, maximum 15). The worst-case probability of a successful random attempt within a one-minute period is $15/95^8$, which is less than 1 in 100,000.

If the Module's retry counter is set to zero, infinite retries are allowed. In this case, the Module takes approximately 48ms to authenticate CO/User logging message over Ethernet interface. The worst-case probability of a successful random attempt within a one-minute period is $1250/95^8$ which is less than 1 in 100,000

After a configurable number of consecutive failed attempts, the KPK, TEKs and KEKs are zeroized, a new KPK is generated, and the passwords are 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.

KVL-BKK Authentication:

Communications between the Module and a KVL device are encrypted with the 256-bit KVL-BKK. A KVL device is authenticated by having possession of the key needed to decrypt communications. The probability of a successful random attempt is 1 in 2^{256}, which is less than 1 in 1,000,000.

It takes approximately 80.5 milliseconds for each encrypted data packet to be sent between the Module and KVL. Therefore, the maximum number of authentication attempts that can be performed as a KVL Role with the KVL-BKK in one minute is 745 and the probability of a successful random attempt during a one-minute period is 745 in 2^{256} or 1 in 1.55425e+74, which is less than 1 in 100,000.

Table 12 – Authentication Description

Authentication Method	Probability	Probability over a One-Minute Period
Password	$1/95^8$	$15/95^8$ or $1250/95^8$, depending on configuration
KVL-BKK	$1/2^{256}$	$745/2^{256}$

4.3 Services

All services implemented by the Module are listed in the tables below. Note that all services listed in Table 13 and Table 14 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 13 – Authenticated Services

Service	Description	CO	User	KVL
Load Entropy	Load external entropy used to seed the DRBG.		X	

Service	Description	CO	User	KVL
Program Update	Update the Module firmware via the Ethernet interface. All keys (stored in volatile and non-volatile memory) and CSPs may be zeroized during a Program Update.	X	X	X
Validate Crypto-Officer password	Validate the current Crypto-Officer password used to identify and authenticate the Crypto-Officer role via the Ethernet interface. Successful authentication will allow access to services allowed for the Crypto Officer.	X		
Change Crypto-Officer password	Modify the current password used to identify and authenticate the Crypto-Officer Role via Ethernet interface.	X		
Extract Action Log	Exports a history of actions over the Ethernet interface.	X	X	
Logout Crypto-Officer Role	Logs out the Crypto-Officer.	X		
Configure Module via Ethernet interface	Perform configuration of the Module (e.g. password length, time configuration, enable/disable clear key import, enable/disable red keyloading, etc.) via the Ethernet interface.	X		
Validate User Password	Validate the current User password used to identify and authenticate the User role via the Ethernet 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 Ethernet interface.		X	
Algorithm List Query	Provides a list of algorithms over the Ethernet 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 Ethernet interface. Transfer clear key variables out of the Module over Ethernet interface is supported when the Module is running in non-FIPS mode.		X	
Import Key Variable	Receive encrypted key variables (e.g., KEKs, and TEKs) over the Ethernet and KVL interfaces. Receive clear key variables over Ethernet interface is supported when the Module is running in non-FIPS mode.		X	X
Generate Key Variable	Auto-generate Public and Private Generated Signature Keys, SRTP/SRTCP Master Key, SRTP/ SRTCP Master Salt, TLS KDF 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 Ethernet interface.		X	

Service	Description	CO	User	KVL
Decrypt	Decrypt ciphertext data received over the Ethernet interface.		X	
Generate Signature	Generate a Signature and output result over Ethernet interface.		X	
Verify Signature	Verify a Signature and output result over Ethernet interface.		X	
Generate Hash	Generate a hash and output result over Ethernet 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 to create an ECDH Shared Secret, and ECDH Public and Private Keys in volatile memory.		X	
Generate Random Number	Generate random data using DRBG and output result over Ethernet interface.		X	
Key Query	Retrieve the metadata for a given key present in the Module.		X	
OTAR	Modify and query the TEKs and KEKs in the Module via APCO OTAR Key Management Messages.		X	
Store & Forward via KVL Interface	Modify and query the KEKs and TEKs stored internally via the KVL interface.			X
Zeroize Keys via KVL interface	Zeroize KEKs and TEKs when connected to the KVL.			X
Configure Module via KVL interface	Perform configuration of the Module (e.g., OTAR configuration) when connected to the KVL.			X

Table 14 – 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 Ethernet interface.
Erase	Zeroization of CSPs and public keys as listed in Table 15.
Reset	Reset the Module.

Table 15 defines the relationship between access to Security Parameters and the different module services. The modes of access shown in the table are defined as:

- C = Check CSP: Check status of the CSP (i.e., existence, size, format, etc.).
- D = Decrypt: Decrypts entered key using other KEK during CSP entry over the Ethernet interface or using the KVL-BKK during CSP entry over the KVL interface. In the case of the Program Update service, decryption will occur using the IDK.
- I = Plaintext entry: only applies to public keys, with the exception of TEKs and KEKs, which may be loaded in plaintext over the KVL interface.
- O = Plaintext output: only applies to public keys
- E = Encrypt: Encrypts key prior to output over the Ethernet interface using a KEK.
- G = Generate CSP: Generates key or establishes over KAS.
- S = Store CSP: Stores CSP in volatile or non-volatile memory.
- U = Use CSP: Uses key internally to perform services.
- Z = Zeroize: The service zeroizes the CSP.
- - = No access: the service does not access the CSP.

Table 15 – Security Parameters Access by Service

Service	CSPs and Public Keys																						
	Input String	SP800-90A DRBG Seed	DRBG Internal state (V and Key)	PEK	DSEK	TEKs	KEKs	KPK	KVL-BKK	IDK	UKPPK	Crypto-Officer 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	ECDH Ephemeral Public Key	SRTP/SRTCP Master Key	SRTP/SRTCP Master Salt	TLS KDF Secret Key	KDF Derived Key
Program Update	-	-	-	D,Z,S	D,Z,S	Z	Z	Z	D,Z,S	U,Z,S	D,Z	Z	Z	Z, U	Z, U	Z, U	Z,U	Z	Z	Z	Z	Z	Z	Z
Validate Crypto-Officer password	-	-	-	U	-	-	-	D	-	-	U	D,U,Z	-	-	-	-	-	-	-	-	-	-	-	-
Change Crypto-Officer password	-	-	-	U	-	-	-	D,S,E, G	-	-	U	D,U,Z, S	-	-	-	-	-	-	-	-	-	-	-	-
Logout Crypto-Officer Role	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Extract Action Log	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Configure Module via Ethernet interface	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Validate User Password	-	-	-	U	-	-	-	D	-	-	U	-	D,U,Z	-	-	-	-	-	-	-	-	-	-	-
Change User Password	-	-	-	U	-	-	-	-	-	-	U	-	D,U,Z, S	-	-	-	-	-	-	-	-	-	-	-
Logout User Role	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Load Entropy	U	S	-	-	U	Z	Z	Z	-	-	-	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z	Z
Algorithm List Query	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Export Key Variable	-	-	-	-	-	D,E,U	D,E,U	U	-	-	-	-	-		-	-	-	D,E,U	-	-	D,E,U	D,E,U	D,E,U	D,E,U
Import Key Variable	-	-	-	-	-	D,E,S, U,I	D,E,S, U,I	U	U	-	-	-	-	-	-	-	U	-	-	-	D,E,S, U	D,E,S, U	D,E,S,U	D,E,S, U
Generate Key Variable	-	U	G,U,Z	-	-	E,S	E,S	U	-	-	-	-	-	E,G,S	-	O	E,G,S	-	-	-	E,G,S	E,G,S	E,G,S	E,G,S

Service	CSPs and Public Keys																						
	Input String	SP800-90A DRBG Seed	DRBG Internal state (V and Key)	PEK	DSEK	TEKs	KEKs	KPK	KVL-BKK	IDK	UKPPK	Crypto-Officer 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	ECDH Ephemeral Public Key	SRTP/SRTCP Master Key	SRTP/SRTCP Master Salt	TLS KDF Secret Key	KDF Derived Key
Delete Key Variable	-	-	-	-	-	Z	Z	-	-	-	-	-	-	Z	-	-	Z	Z	-	-	Z	Z	Z	Z
Encrypt	-	-	-	-	-	C,U	C,U	C,U	C,U	-	-	-	-	-	-	-	-	-	-	-	C,U	C,U	C,U	C,U
Decrypt	-	-	-	-	-	C,U	C,U	C,U	C,U	-	-	-	-	-	-	-	U	-	-	-	C,U	C,U	C,U	C,U
Generate Signature	-	-	U	-	-	-	-	U	-	-	-	-	-	D,U	-	-	U	U	-	-	-	-	-	-
Verify Signature	-	-	-	-	-	-	-	U	-	-	-	-	-	-	-	U	-	-	-	-	-	-	-	-
Generate Certificate	-	-	-	-	-	-	-	U	-	-	-	-	-	G,U	-	G	-	-	-	-	-	-	-	-
Generate Hash	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Generate MAC	-	-	-	-	-	D,U,C	-	U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U
Perform Key Agreement Process	-	-	U	-	-	-	G	-	-	-	-	-	-	-	-	-	E,G,S	G	G,U,O	U,I	-	-	-	-
Generate Random Number	-	G,U	G,U,Z	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Key Query	-	-	-	-	-	D	D	U	-	-	-	-	-	-	-	-	-	-	-	-	U	U	U	U
OTAR	-	-	-	-	-	D,E,S,U	D,E,S,U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Store & Forward via KVL Interface	-	-	-	-	-	D,E,S,U	D,E,S,U	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Zeroize Keys via KVL interface	-	-	-	-	-	Z	Z	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Perform Self-Tests	-	-	-	-	-	-	-	-	-	-	-	-	-	-	U	U	-	U	-	-	-	-	-	-
Version Query	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
Erase		-	-	Z	-	Z	Z	Z	-	-	-	Z	Z	Z	-	Z	Z	Z	Z	Z	Z	Z	Z	Z
Reset		Z	Z	-	-	Z	Z	-	Z	-	Z	Z	Z	Z	-	Z	Z	Z	Z	Z	Z	Z	Z	Z

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 "Status LED" lights (red if no keys present on the Module, green if keys are present in the Module) indicate that 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 light the "Status LED" 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. The AES KATS are inclusive of the drop-in algorithms.

- Firmware Integrity: A digital signature is generated over the base firmware and all Drop-in algorithms code when it is built using SHA-384 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 for CBC, CTR, ECB and OFB modes (Cert. #C489)
- AES-256 encrypt and decrypt KATs for CFB8 and OFB modes (Cert. #C490)
- AES-256 encrypt and decrypt KATs for CBC, CTR, ECB, GCM and OFB modes (Cert. #C491)
- AES-128 and 256 KW encrypt and decrypt (SP800-38F) KAT (Cert. #C492)
- ECDSA P-384 key generation KAT
- ECDSA P-384 signature generation and verification KATs
- EC Diffie-Hellman primitive "Z" computation KAT per IG D.8
- SHA-256 and -384 KATs
- HMAC-384 KAT
- CTR DRBG KAT (instantiate, reseed and generate)
- One-Step KDF [56Cr2] (§4.1) KAT
- SRTP KDF KAT
- TLS KDF 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.
- External indicator tests - upon every power- up, the Module will assert and de-assert each signal connected to an external indicator, so that the User may verify that the indicators are functioning and controlled by the Module.

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.
- SP800-90A DRBG Continuous Test: The continuous random number generator test is performed on the 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 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 16 byte DRBG data block, generated by the DRBG. The Module enters the Critical Error State if this test fails.

- Firmware load test: a digital signature is generated over the code when it is built using SHA-384 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, multi-chip standalone cryptographic module as defined by FIPS 140-2 and is designed to meet Level 2 Physical Security requirements. The Module is entirely contained within a hard-plastic production-grade removable enclosure. The enclosure is opaque within the visible spectrum. The removable cover is protected with two (2) tamper-evident seals. The tamper-evident labels are visible on both sides of the enclosure exterior as shown in Figure 3, Figure 4 and Figure 5 below.

The two (2) tamper seals are installed during manufacturing and serve to inform the user if the Module has been tampered with. These seals should be checked periodically by the operator for signs of tamper. If signs of tamper are detected, the Module is rendered inoperable. If this is the case, the tamper can then be addressed by the operator as described below.

Here are some facts about how the operator can address the tamper state:

1. The Crypto Officer is the only role authorized to bring the Module out of tamper.
2. Only certain tamper states are operator-recoverable.
    a. Non-recoverable tamper states are over/under voltage, over/under temperature.
    b. If the tamper is non-recoverable the Module should be returned to the factory for diagnosis/reprogramming.
3. Operator recoverable tamper states can be resolved using the Module's serial console (instructions to clear the tamper conditions are provided on the serial console, the operator should follow said instructions).
4. It should also be noted that if the operator is unconfident about the state of their device, after discovering the tamper labels have been broken, they have the option to send the Module to the factory for diagnosis/reprogramming. Similarly, the factory can re-apply new tamper labels to the device.
5. No maintenance access interface is available.

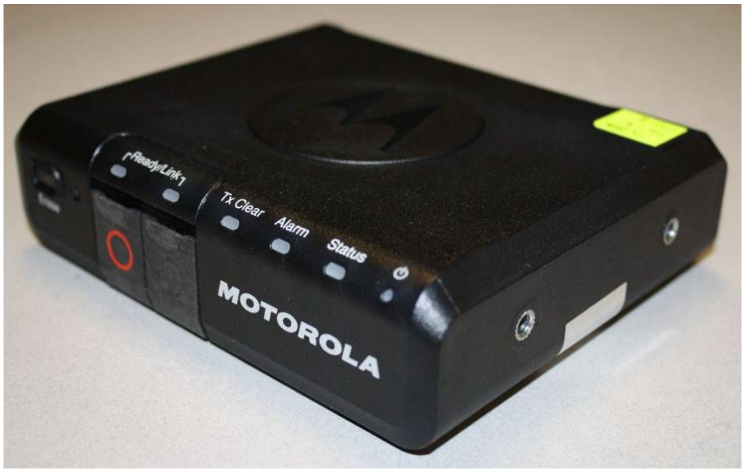

Figure 2: Top/Front/Right view

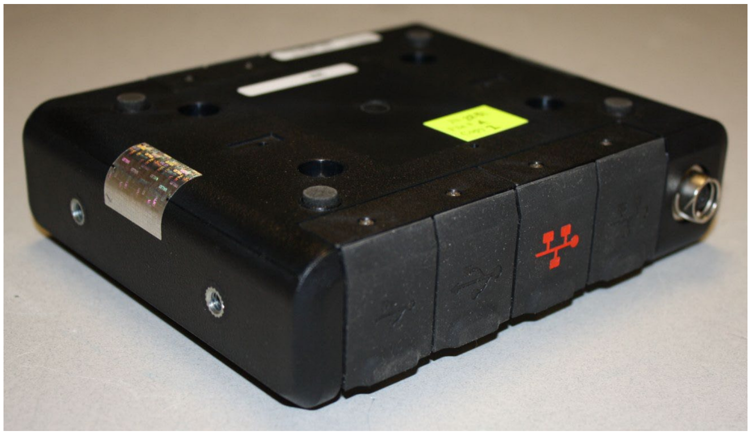

Figure 3: Underside/Rear/Left view

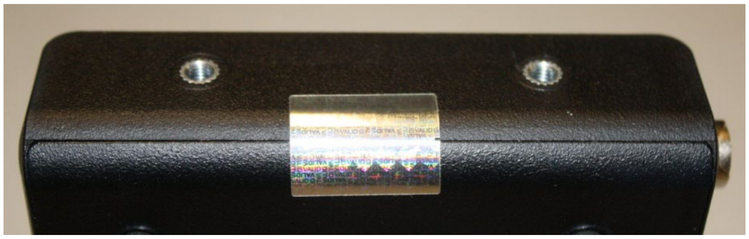

Figure 4: Right Side Tamper Label Placement

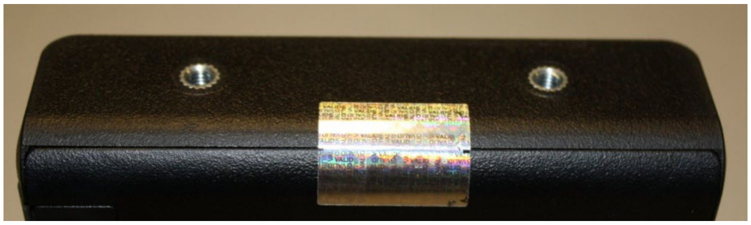

Figure 5: Left Side Temper Label Placement

7 Operational Environment

The Module has a limited 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, specifically Program Update.
7. The Module does not support manual key entry.
8. The Module does not enter or output plaintext CSPs in the Approved mode.
9. The Module implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
10. The Module conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.

9.2 Procedural Enforcement

1. An operator shall ensure that the security strength of the TLS KDF Secret is at least as strong as the length of the resulting KDF Derived Key.
2. An operator shall ensure KDF Derived Keys used in the FIPS Approved mode have at least 112 bits of security strength.
3. An operator shall ensure KDF Derived Keys used for key transport have at least the security strength of the key(s) being transported.
4. An operator shall ensure KDF Derived keys are only used within the context of the TLS or SRTP/ SRTCP protocols, dependent on which protocol KDF was used to derive the key.
5. An operator shall not output a KDF Derived Key in plaintext.
6. If the module fails the FW integrity test, an operator shall ship the module to a Motorola service center for recovery.
7. The module is capable of outputting keys encrypted with non-Approved key wrapping (AES-OFB encryption without an Approved MAC authentication) as follows:
   TEKs, KEKs, SRTP/ SRTCP Master Key, SRTP/ SRTCP Master Salt, KDF Derived Key
   An operator shall ensure that non-Approved key wrapping is not used in the Approved mode of operation.

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 compliant 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 compliant 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 consists of a 0 bit and 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 16 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[108]	*NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions (Revised), October 2009*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, January 2011*
[133rev2]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, 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 186-4, July, 2013.*
[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*
[22r1a]	*National Institute of Standards and Technology, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, April 2010*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38B]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, May 2005*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*

Abbreviation	Full Specification Name
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56Ar3]	*NIST Special Publication 800-56A Revision 3, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, April 2018*
[56Cr2]	*NIST Special Publication 800-56C Revision 2, Recommendation for Key-Derivation Methods in Key-Establishment Schemes, August 2020*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*
[RFC2246]	*The TLS Protocol, August 2008*
[RFC3711]	*The Secure Real-time Transport Protocol (SRTP), March 2004*
[RFC5286]	*AES Galois Counter Mode (GCM) Cipher Suites for TLS, August 2008*
[RFC5246]	*The Transport Layer Security (TLS) Protocol, August 2008*
[RFC7714]	*AES-GCM Authenticated Encryption in the Secure Real-time Transport Protocol (SRTP), December 2015*

Table 17 – Acronyms and Definitions

Acronym	Definition
ADP	Advanced Digital Privacy
AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DSEK	DRBG Seed Encryption Key
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

Acronym	Definition
IV	Initialization Vector
KDF	Key Derivation Function
KLK	Key Loss Key
KMF	Key Management Facility
KPK	Key Protection Key
KEK	Key Encryption Key
KVL	Key Variable Loader
KVL-BKK	KVL - Black Keyloading Key
OTAR	Over The Air Rekeying
PEK	Password Encryption Key
PGSK	Private Generated Signature Key
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