Security Policy: KMF CryptR

Version: R01.00.17

Date: December 3, 2012

Table of Contents

1. Introduction

1.1. Scope

This Security Policy specifies the security rules under which the KMF CryptR must operate. In addition to the security requirements derived from FIPS 140-2 are those imposed by Motorola. These rules, in total, define the interrelationship between the:

- Module Operators,
- Module Services, and
- Critical Security Parameters (CSPs).

1.2. Definitions

ALGID	Algorithm Identifier
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CSP	Critical Security Parameter
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECB	Electronic Code Book
ECDSA	Elliptic Curve Digital Signature Algorithm
IV	Initialization Vector
KLK	Key Loss Key
KMF	Key Management Facility
KPK	Key Protection Key
KVL	Key Variable Loader
LED	Light-emitting diode
LFSR	Linear Feedback Shift Register
OTAR	Over-the-Air-Rekeying
PEK	Password Encryption Key
RAM	Random Access Memory
RNG	Random Number Generator

1.3. Overview

The KMF CryptR provides encryption and decryption services for secure key management and Over-the-Air-Rekeying (OTAR) for Motorola's Key Management Facility (KMF). The KMF and KMF CryptR combine to provide these cryptographic services for Motorola's APCO-25 compliant Astro™ radio systems.

1.4. KMF CryptR Implementation

The KMF CryptR is implemented as a Multi-chip standalone cryptographic module as defined by FIPS 140-2.

1.5. KMF CryptR Hardware / Firmware Version Numbers

The KMF CryptR has the following FIPS validated hardware and firmware version numbers:

Table 1: FIPS Validated Version Numbers

FIPS Validated Cryptographic Module Hardware Kit Numbers	FIPS Validated Cryptographic Module Firmware Version Numbers
P/N CLN8566A	R01.02.10, R01.05.00

1.6. KMF CryptR Cryptographic Boundary

The KMF CryptR cryptographic boundary is drawn around the entire product which includes the housing, various IC's, FLASH, RAM, and Printed Circuit Board as shown below.

Figure 1: KMF CryptR

1.7. Ports and Interfaces

The KMF CryptR provides the following physical ports and logical interfaces:

Table 3: Ports and Interfaces

Physical Port	Qty	Logical interface definition	Description
Power	1	Power Input	This interface powers all circuitry. This interface does not support input / output of CSP's.
Key Variable Loader (KVL) Interface	1	Data Input Data Output Control Input Status Output	Provides an interface to the Key Variable Loader. The KEKs are entered in encrypted form over the KVL interface. The hash of the boot block is output over the KVL interface if the Firmware Integrity Test is successful on power up.
Key Variable Loader (KVL) Auxiliary Interface	1	N/A	This port is not used by the KMF CryptR.
RS-232 Serial Interface	1	N/A	This port is not used by the KMF CryptR.
Mini-Universal Serial Bus (mini-USB) Interface	1	Control Input Status Output Data Output	Provides an interface for execution of RS-232 shell commands. This interface does not support output of CSP's.
Ethernet Interface (RED)	1	Data Input Data Output Control Input Status Output	This interface routes packets to the Host. This interface supports the output of TEKs encrypted on a KEK. This interface also supports the input of encrypted passwords for operator authentication.
Ethernet Interface (BLACK)	1	N/A	This port is not used by the KMF CryptR.
Erase Switch	1	Control Input	This interface is used for zeroization of KEKs, TEKs.
Reset Switch	1	Control Input	This interface forces a reset of the KMF CryptR.
Alarm LED Output	1	Status 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.
Power LED Output	1	Status 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.
Ready LED Output (red)	1	Status Output	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).
Ready LED Output (black)	1	Status Output	The Ready LED output (black) is not used and remains off other than at power up self-test or programming.
TX Clear LED Output	1	Status 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 LED Output	1	Status Output	The Status LED output is steady red when no key has been loaded and green when a key has been loaded.

2. FIPS 140-2 Security Levels

The KMF CryptR can be configured to operate at FIPS 140-2 overall Security Level 2. The table below shows the FIPS 140-2 Level of security met for each of the eleven areas specified within the FIPS 140-2 security requirements.

Table 4: KMF CryptR Security Levels

FIPS 140-2 Security Requirements Section	Validated Level at overall Security Level 2
Cryptographic Module Specification	2
Module Ports and Interfaces	2
Roles, Services, and Authentication	3
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

3. FIPS 140-2 Approved Operational Modes

The KMF CryptR can be configured to operate in a FIPS 140-2 Approved mode of operation and a non-FIPS Approved mode of operation. CSPs are not shared between FIPS Approved mode and non-FIPS Approved mode. The transition from a FIPS Approved mode to a non-FIPS Approved mode, and vice versa, causes all CSPs to be zeroized. 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

3.1. Configuration Settings for operation at FIPS 140-2 overall Security Level 2

Documented below are the configuration settings that are required for the module to be used in a FIPS 140-2 Approved mode of operation at overall Security Level 2.

1. Disable Clear Key Import. The Module Configuration service is used to configure this parameter in the module. When this configuration setting is disabled, clear key import will be disallowed.
2. *Disable Clear Key Export.* The Module Configuration service is used to configure this parameter in the module. When this configuration setting is disabled, clear key export will be disallowed.
3. Disable Key Loss Key (KLK). The Module Configuration service is used to configure this parameter in the module.
4. Only Approved and Allowed algorithms used. The module supports the following Approved algorithms:
   - AES-256 8-bit CFB (Cert. #1901) – used for symmetric encryption / decryption of keys and parameters stored in the internal database
   - AES-256 OFB (Cert #1901) – for symmetric encryption / decryption of keys
   - AES-256 ECB (Cert. #1901) – used for inner layer encryption
   - AES-256 CBC (Cert. #1901) - for firmware upgrades and OTAR
   - AES256 CTR (Cert. #1901) - for use with the SP800-90 DRBG
   - SHA-384 (Cert. #1670) – used for digital signature verification during firmware integrity test and firmware load test. Used for password hashing for internal password storage.
   - SP800-90 DRBG (Cert. #159) - used for IV and key generation in Firmware version R01.02.10 only.
   - FIPS 186-3 ECDSA-384 (Cert. #268) – used for digital signature verification

The following non-Approved algorithms and protocols are allowed within the Approved mode of operation:

- AES (Cert. #1901, key wrapping; key establishment methodology provides 256 bits of encryption strength) – used for key encryption
- Non-deterministic Hardware Random Number Generator
  - Used to provide random numbers used as Initialization Vectors (IV) and the seeds for the Approved DRBG in Firmware version R01.02.10 only
  - Used to provide random numbers used as IVs and key generation in Firmware version R01.05.00 only
- AES MAC (AES Cert. #1901, vendor affirmed; P25 AES OTAR)
- Maximal length 64-bit LFSR

3.2. Non Approved Mode of Operation

A non-FIPS Approved mode of operation is transitioned to when any of the following is true:

1. Clear Key Import is enabled.
2. Clear Key Export is enabled.
3. KLK generation is enabled.
4. Non-Approved algorithms are used.

The module supports the following non-Approved algorithms:

- FIPS 186-3 ECDSA-384 Key Generation and Signature Generation (non-compliant) – not used in operation with the KMF.
- SP800-56A KAS (not tested; non-compliant) – not used in operation with the KMF.
- SHA1 / SHA256 (not tested; non-compliant) – not used in operation with the KMF.
- DES-XL
- DES-OFB
- DES-ECB
- DES-CBC
- DVI-XL
- DVP-XL
- AME Localized Capable

4. Crypto Officer and User Guidance

4.1. Administration of the KMF CryptR in a secure manner (CO)

The KMF CryptR requires no special administration for secure use after it is set up for use in a FIPS Approved manner. To do this, configure the module as described in Section 3 of this document.

Note that all keys will be zeroized after the Program Update service has completed.

4.2. Assumptions regarding User Behavior (CO)

The KMF CryptR has been designed in such a way that no special assumptions regarding User Behavior have been made that are relevant to the secure operation of the unit.

4.3. Approved Security Functions, Ports, and Interfaces available to Users

KMF CryptR services available to the User role are listed in section 8.2.

4.4. User Responsibilities necessary for Secure Operation

No special responsibilities are required of the User for secure operation of the KMF CryptR.

5. Security Rules

The KMF CryptR enforces the following security rules.

1. The KMF CryptR inhibits all data output via the data output interface whenever an error state exists and during self-tests.
2. The KMF CryptR logically disconnects the output data path from the circuitry and processes when performing key generation or key zeroization.
3. Authentication data (e.g. passwords) are entered in encrypted form. Authentication data is not output during entry.
4. The KMF CryptR does not support manual key entry.
5. The KMF CryptR enforces Identity-Based authentication.
6. The KMF CryptR supports a User role and a Crypto-Officer role. The module will verify the authorization of the operator to assume each role.
7. The KMF CryptR re-authenticates an operator when it is powered-up after being powered-off.
8. The KMF CryptR implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
9. The KMF CryptR protects secret keys and private keys from unauthorized disclosure, modification, and substitution.
10. The KMF CryptR provides a means to ensure that a key entered into or stored within the module is associated with the correct entities to which the key is assigned. Each key in the KMF CryptR is entered encrypted and stored with the following information:
    - Key Identifier – 16 bit identifier
    - Algorithm Identifier – 8 bit identifier
    - Key Type – Traffic Encryption Key or Key Encryption Key
    - Physical ID – Identifier indicating storage locations.

    Along with the encrypted key data, this information is stored in a key record that includes a CRC over all fields to protect against data corruption.
11. The KMF CryptR denies access to plaintext secret and private keys contained within the module.
12. The Program Update service can be used to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the module.
13. The KMF CryptR conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class A requirements.
14. The KMF CryptR performs the following self-tests. Powering the module off then on will initiate the power up self-tests.
    - Power up and on-demand tests
      - Cryptographic algorithm test: A cryptographic algorithm test using a known answer is conducted for all cryptographic functions (e.g., encryption, decryption, authentication, random number generation, and hashing) for each Approved algorithm listed below. The test passes if the final data matches the known data, otherwise it fails.
        - AES-256 (8-bit CFB, ECB, CBC, OFB, and CTR modes) encrypt / decrypt
        - SHA-384
        - SP800-90 DRBG

        - ECDSA-384 (signature generation and verification) (this is performed as a Pairwise Consistency test on powerup)
    - Firmware integrity test: A digital signature is generated over the code when it is built using SHA-384 and ECDSA-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.
    - Critical functions test: The module performs a read/write test of the internal RAM at each power up. The module also performs an external indicators test: 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.
- Conditional tests
    - Firmware load test: A digital signature is generated over the code when it is built using SHA-384 and ECDSA-384. Upon download into the module, the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.
    - Continuous Random Number Generator test: The continuous random number generator test is performed on all RNGs supported by the module (SP800-90 DRBG, NDRNG, and 64-bit LFSR). For each RNG, an initial 64-bit 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 any one of the RNGs 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.

15. The KMF CryptR enters the Critical Error state if the Cryptographic Algorithm Test, Critical Functions Test, or Continuous Random Number Generator Test fails. An error indicator is output by turning the Alarm LED red while in the Critical Error state. The Critical Error state may be exited by powering the module off then on.
16. The KMF CryptR outputs a hash of the boot block over the KVL interface to indicate the Firmware Integrity Test or Firmware Load Test has completed successfully. The KMF CryptR enters the Signature Validation Failure state if the Firmware Integrity test or Firmware Load test fails. A hash of the boot block is not output over the KVL interface to indicate the Firmware Integrity test or Firmware Load test failed. While in this state the module will wait to be programmed and will not perform any other operations.
17. The KMF CryptR does not perform any cryptographic functions while in an error state.

6. Identification and Authentication Policy

The KMF CryptR supports a User role and a Crypto-Officer role.

The Crypto-Officer and User roles are authenticated with passwords. The Crypto-Officer and User passwords are initialized to a default value during 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.

Table 5: Roles and Authentication

Role	Authentication Type	Authentication Mechanism	Strength of Authentication
Crypto-Officer	Identity-Based	Identity: a 4-byte identifier is used to identify the identity and role. The KMF CryptR supports a single identity. Crypto-Officer Password: a 14-32 character ASCII password is authenticated to gain access to all Crypto-Officer services.	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 4,876,749,791,155,298,590,087,890,625. The module limits the number of authentication attempts in one minute to 15. The probability of a successful random attempt during a one-minute period is 15 in 95 ^ 14 or 1 in 3.25117e+26.
User	Identity-Based	Identity: a 4-byte identifier is used to identify the identity and role. The KMF CryptR supports a single identity. User Password: a 14-32 character ASCII password is authenticated to gain access to all User services.	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 4,876,749,791,155,298,590,087,890,625. The module limits the number of authentication attempts in one minute to 15. The probability of a successful random attempt during a one-minute period is 15 in 95 ^ 14 or 1 in 3.25117e+26.

7. Physical Security Policy

The KMF CryptR 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 KMF CryptR 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 tamper-evident tape. The tamper-evident tape is visible on both side of the enclosure exterior.

Two tamper labels are installed during manufacturing and should be checked periodically by the user for signs of tamper.

No maintenance access interface is available.

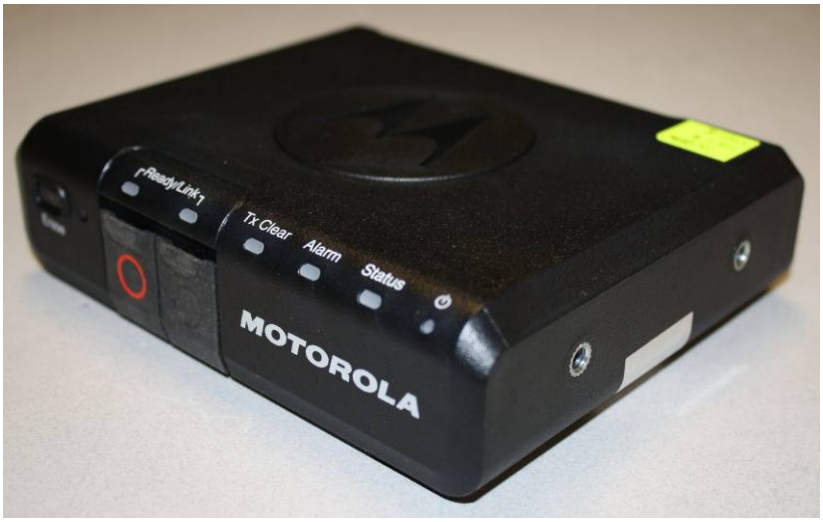

Figure 2: KMF CryptR (Top/Front/Right)

Figure 3: KMF CryptR (Underside/Rear/Left)

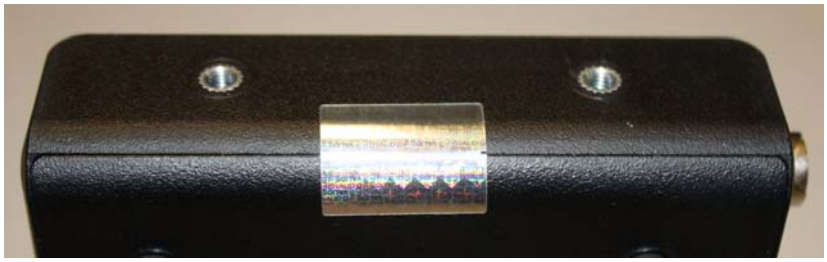

Figure 4: Right Side Tamper Seal Placement

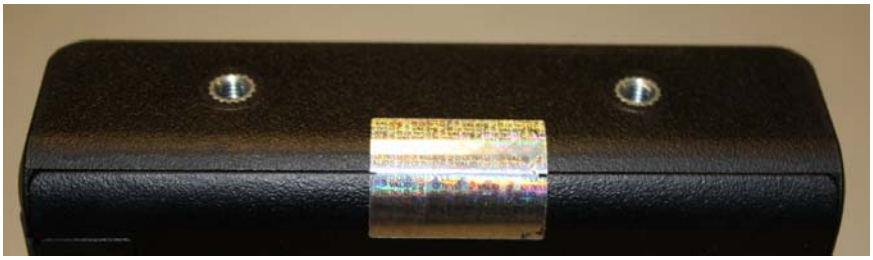

Figure 5: Left Side Tamper Seal Placement

8. Access Control Policy

8.1. KMF CryptR Supported Roles

The KMF CryptR supports two (2) roles. These roles are defined to be the:

- User Role
- Crypto-Officer Role

8.2. KMF CryptR Services Available to the User Role.

- 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.
- Change User Password: Modify the current password used to identify and authenticate the User Role via the Ethernet interface.
- Algorithm List Query: Provides a list of algorithms over the Ethernet interface.
- Logout User Role: Logs out the User.
- Export Key Variable: Transfer key variables (KEKs, TEKs) out of the module over the Ethernet interface.
- Import Key Variable: Receive encrypted key variables (KEKs) over the KVL or Ethernet interface.
- Generate Key Variable: Auto-generate KEKs, TEKs, and the KPK within the module.
- Delete Key Variable: Delete KEKs, and TEKs stored in the module.
- Edit Key Variable: Edit KEKs and TEKs managed by the module.
- Key Check: Validate the correctness of a Key based on algorithm properties.
- Encrypt: Encrypt plaintext data to be transferred over the Ethernet interface.
- Decrypt: Decrypt ciphertext data received over the Ethernet interface.
- Transfer Key Variable: Internally transfer key variables (KEKs, TEKs) between volatile and non-volatile memory.
- Generate Hash: Generate a hash and output result over Ethernet interface.
- Generate Random Number: Generate random data using the SP800-90 DRBG and output result over Ethernet interface.
- Key Query: Retrieve the metadata for a given key present in the module.
- Generate AES MAC: Generate an AES MAC.

8.3. KMF CryptR Services Available to the Crypto-Officer Role.

- Program Update: Update the module firmware via the Ethernet interface. All keys (stored in RAM and non-volatile memory) and CSPs are zeroized during a Program Update.
- 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.
- Change Crypto-Officer password: Modify the current password used to identify and authenticate the Crypto-Officer Role via Ethernet interface.
- Extract Action Log: Exports a history of actions over the Ethernet interface.
- Logout Crypto-Officer Role: Logs out the Crypto-Officer.
- Configure Module: Perform configuration of the module (e.g. time configuration, enable/disable clear key import, etc.).

8.4. KMF CryptR Services Available Without a Role.

- Perform Self-Tests: Performs module self-tests comprised of cryptographic algorithms test and firmware integrity test. Initiated by a transition from power off state to power on state.
- Version Query: Provides module firmware version number.
- Erase: zeroization of KEKs, TEKs**.**
- Reset: resets the KMF CryptR.

8.5. Critical Security Parameters (CSPs) and Public Keys

Table 6: CSP Definition

CSP Identifier	Description
SP800-90 seed	This is a 384-bit seed value used within the SP800-90 DRBG. The seed is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The seed is not entered into or output from the module. Entry - n/a Output - n/a Storage – in plaintext in volatile memory Zeroization - on power off Generation - Non-deterministic Hardware Random Number Generator
SP800-90 internal state ("V" and "Key")	This is the internal state of the SP800-90 DRBG during initialization. The internal state is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The internal state is not entered into or output from the module. Entry - n/a Output - n/a Storage – in plaintext in volatile memory Zeroization - on power off Generation - Internal to the SP800-90 DRBG
Key Protection Key (KPK)	This is a 256-bit AES key used to encrypt all other keys stored in non volatile memory. Generated internally using the SP800-90 DRBG. Stored in plaintext in non volatile memory. The KPK is not entered into or output from the module. Entry - n/a Output - n/a Storage – stored in plaintext in non volatile memory Zeroization - on Program Update service request Generation - SP800-90 DRBG
Black Keyloading Key (BKK)	This is a 256-bit AES Key used for encrypting keys that are input into the module and output from the module via the Ethernet interface. It is also used to wrap KEKs that are input over the KVL interface. Stored unencrypted in RAM while in use; stored in plaintext in non-volatile memory and zeroized through the Program Update service. Also stored encrypted on

CSP Identifier	Description
	the KPK in non volatile memory. The BKK is entered using the Program Update service (encrypted using AES-CBC) and is not output from the module. Entry - on Program Update service request Output - n/a Storage - in plaintext in non volatile memory Zeroization - on Program Update service request Generation - n/a
Image Decryption Key (IDK)	A 256-bit AES key used to decrypt downloaded images. The IDK is not output from the module. Entry - on Program Update service request Output - n/a Storage - in plaintext in non volatile memory Zeroization - on Program Update service request Generation - n/a
Traffic Encryption Keys (TEKs)	256-bit AES Keys used for enabling secure communication with target devices and for encryption and authentication of Key Management Messages in OTAR. TEKs are entered encrypted (AES Key Wrapping) over the Ethernet interface. The TEKS are stored encrypted on the KPK (AES256-CFB8) in non volatile memory. TEKs are stored in plaintext in RAM only as long as needed. TEKs are output from the module encrypted (AES Key Wrapping) via the Ethernet interface. Entry – input encrypted with AES Key Wrap over the Ethernet Interface Output – output encrypted with AES Key Wrap over the Ethernet Interface Storage – stored encrypted on KPK with AES256-CFB8 in non volatile memory Zeroization - on Delete Key Variable, Erase, and Program Update service requests Generation – SP800-90 DRBG
Key Encryption Keys (KEKs)	256-bit AES Keys used for encryption of keys in OTAR. KEKs are entered encrypted (AES Key Wrapping) over the Ethernet interface or via the KVL interface. The KEKS are stored encrypted on the KPK (AES256-CFB8) in non volatile memory. KEKs are stored in plaintext in RAM only as long as needed. KEKs are output encrypted with AES Key Wrap via the Ethernet interface. Entry – input encrypted with AES Key Wrap over the Ethernet Interface or over the KVL Interface Output - output encrypted with AES Key Wrap over the Ethernet Interface Storage – stored encrypted on KPK with AES256-CFB8 in non volatile memory Zeroization - on Delete Key Variable, Erase, and Program Update service requests Generation – SP800-90 DRBG
User Password	The User Password is entered encrypted on the PEK (AES256-CFB8). The User Password is not stored in the module or

CSP Identifier	Description
	output from the module. Entry – entered encrypted on the PEK with AES256-CFB8 Output - n/a Storage – a hash of the User Password is stored in non-volatile memory Zeroization – on Program Update service request Generation - n/a
Crypto-Officer Password	The Crypto Officer password is entered encrypted on the PEK (AES256-CFB8). After decryption the plaintext password is not stored but temporarily exists in volatile memory. 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 - entered encrypted on the PEK with AES256-CFB8 Output - n/a Storage - SHA-384 hash of the plaintext password is encrypted on the PEK in non volatile memory Zeroization – on Program Update service requests Generation - n/a
Password Encryption Key (PEK)	This is a 256-bit AES Key used for decrypting passwords during password validation. Loaded via the Program Update service. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. Also stored encrypted on the KPK in non volatile memory. The PEK is not output from the module. Entry - on Program Update service request Output - n/a Storage - in plaintext in non volatile memory; encrypted on the KPK in non volatile memory Zeroization - on Program Update service request Generation - n/a

Table 7: Public Keys

Key	Description
ECDSA Public Programmed Signature Key	A 384-bit ECDSA public key used to validate the signature of the firmware image being loaded before it is allowed to be executed. Stored in non volatile memory. Loaded during manufacturing and as part of the boot image during a Program Update service. The Public Programmed Signature Key is not output from the module. Entry - on Program Update service request Output - n/a Storage - in plaintext in non volatile memory Zeroization - on Program Update service request Generation - n/a

8.6. CSP Access Types

Table 8: CSP Access Types

CSP Access Type	Description
C – Check CSP	Checks status of the CSP.
D – Decrypt CSP	Decrypts entered KEKs and TEKs using the BKK during CSP entry over the Ethernet interface. Decrypts entered passwords using the PEK during entry over the Ethernet interface.
E – Encrypt CSP	Encrypts KEKs and TEKs prior to output over the Ethernet or KVL interface using another KEK.
G – Generate CSP	Generates TEK, KEK, KPK, SP800-90 seed, or SP800-90 internal state.
S – Store CSP	Stores KPK in plaintext in non volatile memory. Stores plaintext BKK, PEK, or IDK in volatile and non-volatile memory (encrypted except IDK). Stores SHA-384 Hash of the User and Crypto-Officer password in non volatile memory (encrypted on PEK).
U – Use CSP	Uses CSP internally for encryption / decryption services.
Z – Zeroize CSP	Zeroizes CSP.

Table 9: CSP versus CSP Access

Service	CSP										Role		
	SP800-90 seed	SP800-90 seed internal state	PEK	TEKs	KEKs	KPK	BKK	IDK	User Password	Crypto-Officer Password	User Role	Crypto-Officer Role	No Role Required
1. Program Update			z,s	z	z	z	z, s	u, z, s	z	z		√	
2. Validate Crypto-Officer Password			u							d, u, z		√	
3. Change Crypto-Officer Password			u							d, u, z, s		√	
4. Validate User Password	u	u	u			z, g, s			d, u, z		√		
5. Change User Password			u						d, u, z, s		√		
6. Extract Action Log												√	
7. Version Query													√
8. Algorithm List Query											√		
9. Logout User Role											√		
10. Logout Crypto-Officer Role												√	
11. Export Key Variable				d,e,u	d,e,u	u	u				√		
12. Import Key Variable				d,e,s, u	d,e,s, u	u	u				√		
13. Generate Key Variable	u	u		e,g,s	e,g,s	u					√		
14. Delete Key Variable				z	z						√		
15. Edit Key Variable				d,e,u, s	d,e,u, s	u					√		
16. Key Check				c	c	u					√		
17. Encrypt				u	u	u					√		
18. Decrypt				u	u	u					√		
19. Perform Self-Tests	g	g											√
20. Transfer Key Variable				d,e,u, s	d,e,u, s	u					√		
21. Generate HASH						u					√		
22. Configure Module												√	
23. Generate Random Number	u	u									√		
24. Key Query				d	d	u					√		
25. Erase				z	z								√
26. Reset													√
27. Generate AES MAC											√		

9. Mitigation of Other Attacks Policy

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