# Security Policy: Key Management Facility Crypto Card (KMF CC)

Version 2.19

2/7/2011

# 1.0 Introduction

*1.1 Scope*

This Security Policy specifies the security rules under which the Key Management Facility Cryptographic Card, herein identified as the KMF CC, must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by Motorola. These rules, in total, define the interrelationship between the:

1. module operators,
2. module services,
3. and critical security parameters (CSPs).

*1.2 Overview*

The KMF CC 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 CC combine to provide these cryptographic services for Motorola's APCO-25 compliant Astro ™ radio systems.


**Figure 1 Key Management Facility Crypto Card**

*1.3 KMF CC Hardware / Firmware Version Numbers*

| **FIPS Validated Cryptographic Module Hardware Kit Numbers** | **FIPS Validated Cryptographic Module Firmware Version Numbers** |
|---|---|
| Model T6722A Version CLN7612B, CLN8306C | R01.09 |

*1.4 KMF CC Implementation*

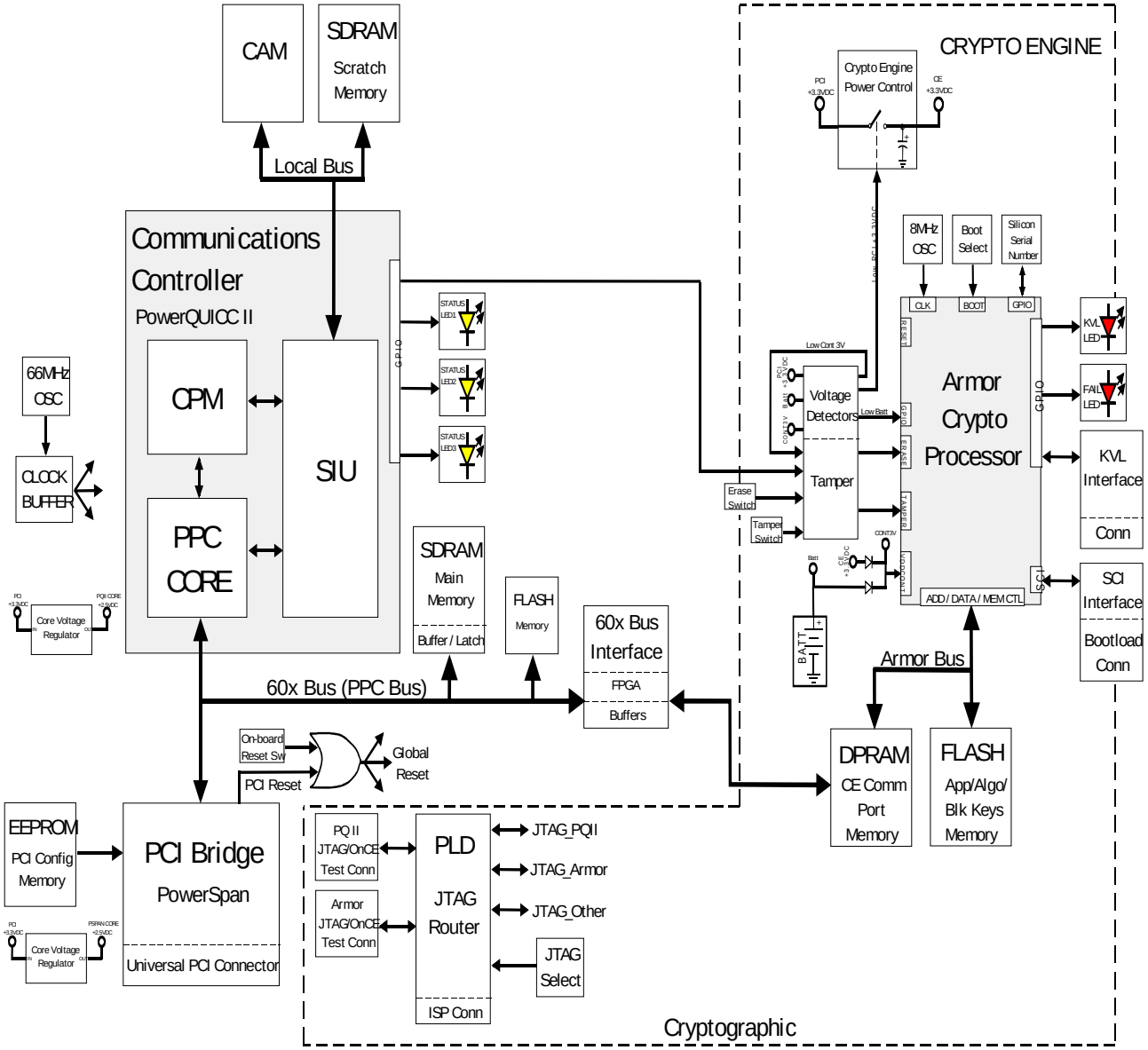
The KMF CC is implemented as a multi-chip embedded cryptographic module as defined by FIPS 140-2. It is comprised of a Crypto Engine, communications controller, and a PCI interface, all housed on a PCI shortcard.

*1.5 KMF CC Cryptographic Boundary*

The Crypto Engine, herein identified as the CE, provides all the KMF CC cryptographic logic and processes. This includes encryption, decryption, and cryptographic key & critical security parameter storage. The cryptographic boundary is defined as the boundary between the CE & JTAG (Joint Test Action Group: IEEE 1149.1)factory interface and all other circuitry on the KMF CC. The CE circuitry is physically grouped together on one corner of the board and is protected by a metal enclosure. All other circuitry on the board that is not part of the CE & JTAG factory interface provides an interface to the host computer where the user interface is implemented.

The CE consists of the Armor cryptographic processor, flash $E^2$PROM, dual port RAM, KVL port, and various support components and circuitry.

**Figure 2 KMF CC Cryptographic Boundary**



# 2.0 FIPS 140-2 Security Level

The KMF CC is validated to meet the FIPS 140-2 security requirements for the levels shown in Table 2.1.

**Table 2.1**
**CE Security Levels**

| FIPS 140-2 Security Requirements Section | Level |
|---|---|
| **Cryptographic Module Specification** | 1 |
| **Cryptographic Module Ports and Interfaces** | 1 |
| **Roles Services and Authentication** | 1 |
| **Finite State Model** | 1 |
| **Physical Security** | 1 |
| **Operational Environment** | N/A |
| **Cryptographic Key Management** | 1 |
| **EMI / EMC** | 3 |
| **Self Tests** | 1 |
| **Design Assurance** | 3 |
| **Mitigation of Other Attacks** | N/A |

# 3.0 FIPS 140-2 Approved Operational Modes

The KMF CC provides modes of operation that are not FIPS 140-2 approved. Below is a list of configuration settings that are required to provide FIPS 140-2 approved operation. To run the KMF CC in approved mode the following three steps must be taken (note: 1 and 2 default to FIPS approved settings at initial power up):

1. Key Loss Key (KLK) generation must be disabled (via download config parameter service).
2. Keyboard Key Entry disabled (via download config parameter service)
3. Encryption keys for non-approved algorithms must not be loaded into the crypto module. A non-approved algorithm may be invoked only when an encryption key for that algorithm has been loaded.

The module supports the following approved algorithms:

- AES-256 for encryption, decryption, and authentication (authentication, AES MAC, is approved when used for Project 25 OTAR. Note: key establishment provides 256 bits of encryption strength) may be used in the following approved modes: OFB, ECB, and CBC.
- TDES for encryption, decryption, and authentication (MAC), shall be used in the following approved modes: 8-bit CFB and CBC
- ANSI x9.31 PRNG for random encryption key and KPK generation.
- SHA-1. Note SHA-1 is not accessible in the KMF CC.

The module supports the following non-approved algorithms:

- AES MAC (P25 AES OTAR)

- DES (ECB, OFB, CFB, and CBC modes)
- DES MAC
- DES-XL
- DVI-XL
- DVP-XL
- HCA
- HW RNG
- LFSR

Approved version numbers:

| | |
|---|---|
| Hardware Version: | CLN7612B, CLN8306C |
| Firmware Version: | R01.09 |
| TDES: | API: R02.01 |
| | ALG: R01.00 |
| | Cert#: 82 |
| AES | API: R02.01 |
| | ALG: R01.00 |
| | Cert#: 2 |
| ANSI x9.31 PRNG | API R02.01 |
| | Alg R01.00 |
| | Cert#: 121 |
| SHA-1 | API: R02.01 |
| | ALG: R01.00 |
| | Cert#: 335 |

# 4.0 Security Rules

The CE on the KMF CC enforces the following security rules. These rules are separated into two categories, 1) those imposed by FIPS 140-2 and, 2) those imposed by Motorola.

### *4.1 FIPS 140-2 Related Security Rules*

1. The CE supports the following interfaces:
   - Data input interface
     a. Dual Port Ram (DPRAM) - Plaintext Data, Ciphertext Data, Encrypted Cryptographic Keys
     b. Serial Communications Interface (SCI) - Encrypted Software Image
     c. Key Variable Loader (KVL) - Key Management Data, Plaintext Cryptographic Keys, Encrypted Software Image
   - Data output interface
     a. Dual Port Ram (DPRAM) - Plaintext Data, Ciphertext Data, Key Management Data (OTAR), Encrypted Cryptographic Keys (OTAR)
   - Control input interface
     a. Dual Port RAM (DPRAM) - Input commands
     b. Serial Communications Interface (SCI) - Input commands
     c. Key Variable Loader (KVL) - Input commands
     d. Key Erase Switch - Manual erase input
     e. Erase Signal from PowerQUICC II
   - Status output interface
     a. Dual Port RAM (DPRAM) - Status codes
     b. Serial Communications Interface (SCI) - Status codes
     c. Key Variable Loader (KVL) - Status codes
     d. KVL & FAIL LEDs - On, off, & flashing codes
   - Power interface
     a. PCI Bus Power - Powers all circuitry except Battery Backed Register and tamper detection circuitry
     b. Continuous (Battery backed) Power - Powers Battery Backed Register and tamper detection circuitry
2. The CE inhibits all data output via the data output interface whenever a fatal error state exists and during self-tests.
3. The CE logically disconnects the output data path from the circuitry and processes when performing key generation, manual key entry, or key zeroization.
4. Plaintext cryptographic keys are entered through the KVL interface only and no plaintext cryptographic keys are ever output from any interface.
5. The CE supports a User role and a Cryptographic Officer role.
6. The CE provides the following services. All services are FIPS approved when executed with an approved algorithm, if applicable, as defined in section 3.0 of this text.
   - Initiate Self Tests (CSPs: KPK; Algs: n/a)
   - Zeroize All Keys (CSPs: KPK; Algs: n/a)
   - Erase/Reset KMF CC (CSPs: none; Algs: n/a)

- Transfer Master Key (CSPs: Master Key; Algs: All approved algs)
- Shutdown KMF CC (CSPs: none; Algs: n/a)
- Inner Layer Encryption (CSPs: KEK, Master Key, KPK; Algs: All approved algs)
- Inner Layer Decryption (CSPs: KEK, Master Key, KPK; Algs: All approved algs)
- Outer Layer Encryption (CSPs: TEK, Master Key, KPK; Algs: All approved algs)
- Outer Layer Decryption (CSPs: TEK, Master Key, KPK; Algs: All approved algs)
- Random Encryption Key Generation (CSPs: Random Encryption Key, Master Key, KPK; Algs: All approved algs)
- Message Authentication Code (MAC) Generation (CSPs: OTAR Plaintext MAC key, Master Key, KPK; Algs: All approved algs excluding AES)
- Encrypt & Forward (CSPs: TEK, KEK, Master Key, KPK; Algs: All approved algs)
- Recrypt (CSPs: Master Key, KPK; Algs: All approved algs)
- Download Configuration Parameter (CSPs: none; Algs: n/a)
- Algorithm Request (CSPs: none; Algs: n/a)
- Post Request (CSPs: none; Algs: n/a)
- Software Version Request (CSPs: none; Algs: n/a)
- Soundoff (CSPs: none; Algs: n/a)
- KVL Programming (CSPs: Software Plain Text MAC Key; Algs: TDES)

7. The CE implements all software using a high-level language, except the limited use of low-level languages to enhance performance.
8. The CE protects secret keys and private keys from unauthorized disclosure, modification and substitution. All keys stored in the module are stored TDES encrypted on the KPK in flash. Keys are only output from the module if they are encrypted on a Master Key. All keys stored in the module contain a CRC checksum over the plain text. The KPK is stored in a battery backed register and is erased on tamper response.
9. The CE provides a means to ensure that a key entered into, stored within, or output from the CE is associated with the correct entities to which the key is assigned. Each key in the CE is entered 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, Common Key Reference (CKR) number, or CKR/Keyset number – Identifiers indicting storage locations.

   Along with the encrypted key data, this information is stored in a key record that includes a CRC over all of the fields to detect data corruption. When used or deleted the keys are referenced by Key ID/Algid, Physical ID, or CKR/Keyset.
10. The CE denies access to plaintext secret and private keys contained within the CE.

11. The CE provides the capability to zeroize the KPK and other unprotected critical security parameters within the CM.
12. The CE supports the following FIPS approved algorithms:
    - TDES
      - 8-bit CFB for symmetric encryption / decryption of keys and parameters stored in the internal database
      - CBC for authentication of upgrades
    - AES
      - OFB for symmetric encryption/decryption of APCO-25 OTAR
      - CBC for authentication of APCO-25 OTAR
      - ECB for symmetric decryption of APCO-25 OTAR
    - ANSI X9.31 PRNG
      - Random Encryption Key Generation
      - KPK Generation
    - SHA-1
      - Note: SHA-1 is not accessible in the KMF CC.

13. The KMF CC, when used in the KMF (Host Computer) conforms to all FCC Class B requirements.
14. The CE of the KMF CC performs the following self-tests:
    - Power-up and on-demand tests
      - Cryptographic algorithm test: Each algorithm (PRNG, Triple-DES in the CFB8 and CBC modes, and AES in the OFB, CBC, and ECB modes) is tested by using a known key, known data, and if required a known IV. The data is then encrypted and compared with known encrypted data; the test passes if the final data matches the known data, otherwise it fails. The encrypted data is then decrypted and compared with the original plaintext; the test passes if the final data matches the original data, otherwise it fails.
      - Software/firmware test: The software firmware test calculates a checksum over the code. The checksum is calculated by summing over the code in 32 bit words. The code is appended with a value that makes the checksum value 0. The test passes if the calculated value is 0; otherwise it fails.
      - Critical Functions test.
        - LFSR Test: The LFSRs (Linier Feedback Shift Register) are tested by setting the feedback taps to a known value, loading them with known data, shifting the LFSR 64 times, then comparing the LFSR data to a known answer. The test passes if the final data matches, otherwise it fails.
        - General Purpose RAM Test: The general purpose RAM is tested for stuck address lines and stuck bits. This is accomplished through a series of operations that write and read the RAM. The test passes if all values read from the RAM are correct; otherwise it fails.
        - Dual Port RAM Test: The DPRAM is tested for stuck address lines and stuck bits. This is accomplished through a series of operations that

write and read the DPRAM. The test passes if all values read from the DPRAM are correct; otherwise it fails.

Powering the module off then on or resetting the module using the Reset service will initiate the power-up and on-demand self tests.

- Conditional tests
  - Software/firmware load test: A MAC is generated over the code when it is built using 3DES-CBC. Upon download into the module, the MAC is verified. If the MAC matches the test passes, otherwise it fails.
  - Continuous Random Number Generator test: The continuous random number generator test is performed on 3 Random Number Generators (RNG) within the module. The first is a non-deterministic hardware RNG which is used to seed the ANSI X9.31 deterministic Pseudo Random Number Generator (PRNG) and the maximal length 64-bit LFSR. The second is an implementation of ANSI X9.31 which is used for key generation, and the third is a maximal length 64-bit LFSR which is used for IV generation. For each RNG, an initial value is generated and stored upon power up. This value is not used for anything other than to initialize comparison data. Successive calls 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 CE enters an error state if the Cryptographic Algorithm Test, LFSR Test, Continuous Random Number Generator Test, or the General-Purpose RAM Test fails. This error state is exited after the erase function is requested & performed or by cycling the power to the KMF CC.
16. The CE enters an error state if the Software/Firmware test fails. This error state is exited after the erase function is requested & performed or by cycling the power to the KMF CC.
17. The CE enters an error state if the Software/Firmware Load test fails. This error state is exited after the erase function is requested & performed or by cycling the power to the KMF CC.
18. The CE outputs an error indicator via the status interface whenever an error state is entered due to a failed self-test.
19. The CE does not perform any cryptographic functions while in an error state.

### *4.2 Motorola Imposed Security Rules*

1. The KMF CC does not support a bypass mode.
2. The KMF CC does not support multiple concurrent operators.
3. All cryptographic module services are suspended during key loading.
4. Upon detection of a critically low voltage condition on the PCI bus power supply, the cryptographic module shall erase all plaintext keys.
5. Upon detection of a critically low voltage condition on the continuous (battery backed) power supply, the cryptographic module shall erase all Critical Security Parameters (CSPs).
6. Upon detection of tamper, the cryptographic module shall erase all CSPs.
7. The module shall at no time output any CSPs.

# 5.0 Roles and Services

*5.1 KMF CC Supported Roles*

The CE supports two (2) roles. These roles are defined to be:

- User Role: Allows user access to the all services short of key entry services.
- Cryptographic Officer (CO) Role: Allows access only to key entry services. The CO role is defined by an operator possessing a KVL and initiating KVL transfers.

*5.2 KMF CC Approved and non-Approved Services*

Associated CSPs can be found in section 4.1 item 6.

- Initiate Self Tests: Performs module self tests comprised of cryptographic algorithms test, software firmware test, and critical functions test. Initiated by module reset or transition from power off state to power on state.
- Zeroize all keys: Zeroize all keys from the Key Database. Available without a Role. (Module can be reinitialized using KVL)
- Erase/Reset KMF CC: Hard signal erase & reset of module to erase plaintext critical security parameters and remove the module from error states.
- Transfer Master Key: Transfer key variables and/or zeroize key variables to/from the Key Database via a Key Variable Loader (KVL).
- Shutdown Crypto Module: Prepares module for removal of power.
- Inner Layer Encryption: Encrypts keys for insertion into Key Management Message (KMM).
- Inner Layer Decryption: Decrypts keys in Key Management Message (KMM).
- Outer Layer Encryption: Encrypts Key Management Message (KMM).
- Outer Layer Decryption: Decrypts Key Management Message (KMM).
- Random Encryption Key Generation: Generates random keys to be used as TEKs or KEKs, encrypts them with the master key and outputs through the DPRAM interface.
- Message Authentication Code (MAC) Generation: Generation of a sophisticated checksum for Key Management Messages (KMM).
- Encrypt & Forward: Encrypt key loaded from KVL with master key & output via DPRAM.
- Recrypt: Decrypt keys with one key and encrypt result with another key.
- Download Configuration Parameter: Provides means to enable/disable configuration parameters.
- Algorithm Request: Provides list of algorithms currently loaded in the CE.
- Post Request: Provides status of KMF CC.
- Software Version Request: Provides version of software currently loaded on KMF CC.
- Soundoff: Provides basic KMF CC on status with simple message response.
- KVL Programming: Places CE in state to accept software updates through the KVL interface.

# 6.0 Access Control

*6.1 Critical Security Parametera (CSPs)*

**Table 6.1**
**CSP Definition**

| CSP Identifier | Description |
|---|---|
| Key Protection Key (KPK) | Key used to encrypt/decrypt the master key. It is internally generated and unique each time generated. |
| Plaintext Traffic Encryption Keys ( TEK) | Keys used for Key Management Message (KMM) encryption/decryption. |
| Plaintext Key Encryption Keys (KEK) | Keys used for encryption of keys in OTAR. |
| Software Plaintext MAC Key | Key used for authentication of software upgrade. |
| Master Key | Key used to encrypt keys in KMF database. It is stored in Flash encrypted with the KPK. |
| OTAR Plaintext MAC Key | Keys used to calculate MAC for Key Management Messages (KMMs) |
| Random Encryption Keys | Random key generated by the module, encrypted on the master key and sent to the output interface. This key can be a key of any algorithm supported by the module. |

*6.2 CSP Access Types*

**Table 6.2**
**CSP Access Types**

| CSP Access Type | Description |
|---|---|
| Retrieve key | Decrypts encrypted Master keys in the database using the KPK and returns plaintext version or returns OTAR Plaintext MAC Key or Software Plaintext MAC Key. |
| Store key | Encypts plaintext Master keys using the KPK and stores the encrypted version in the database |
| Erase Key | Marks encrypted Master keys data in key database as invalid or zeroizes KPK. |
| Create KPK | Generates and stores new KPK |
| Generate Encryption Key | Generates a random key (intended to be used as a KEK or TEK as assigned by the host). |

*6.3 Access Matrix*

**Table 6.3**
**User Service versus CSP Access**

| User Service | Retrieve Key | Store Key | Erase Key | Generate Encryption Key | Create KPK | User Role | Crypto Officer Role | No Role Required |
|---|---|---|---|---|---|---|---|---|
| 1. Initiate Self Tests | | | | | X | X | | |
| 2. Zeroize All Keys | | | X | | | | | X |
| 3. Erase/Reset KMF CC | | | | | | X | | |
| 4. Transfer Master Key | | X | X | | | | X | |
| 5. Shutdown KMF CC | | | | | | X | | |
| 6. Inner Layer Encryption | X | | | | | X | | |
| 7. Inner Layer Decryption | X | | | | | X | | |
| 8. Outer Layer Encryption | X | | | | | X | | |
| 9. Outer Layer Decryption | X | | | | | X | | |
| 10. Random Encryption Key Generation | X | | | X | | X | | |
| 11. MAC Generation | X | | | | | X | | |
| 12. Encrypt & Forward | X | | | | | X | | |
| 13. Recrypt | X | X | X | | | X | | |
| 14. Download Configuration Parameter | | | | | | X | | |
| 15. Algorithm Request | | | | | | X | | |
| 16. Post Request | | | | | | X | | |
| 17. Software Version | | | | | | X | | |
| 18. Soundoff | | | | | | X | | |
| 19. KVL Programming | X | | X | | | | X | |

# 7.0 Authentication Policy

The KMF CC does not support password authentication.