MOTOROLA

Security Policy: Digital Interface Unit Crypto Module (DIU CM)

Version 2.0

6/10/02

1.0 Introduction

1.1 Scope

This Security Policy specifies the security rules under which the Digital Interface Unit Cryptographic Module, herein identified as the DIU CM, must operate. Included in these rules are those derived from the security requirements of FIPS 140-1 and additionally, those imposed by Motorola. These rules, in total, define the interrelationship between the:

1. module operators,
2. module services,
3. and security related data items (SRDIs).

1.2 Overview

The DIU CM provides secure voice and Over-the-Air-Rekeying (OTAR) advanced key management for Motorola's Digital Interface Unit (DIU). The DIU and DIU CM combine to provide these cryptographic services for Motorola's APCO-25 compliant Astro ™ family of console and base station radio infrastructure equipment.

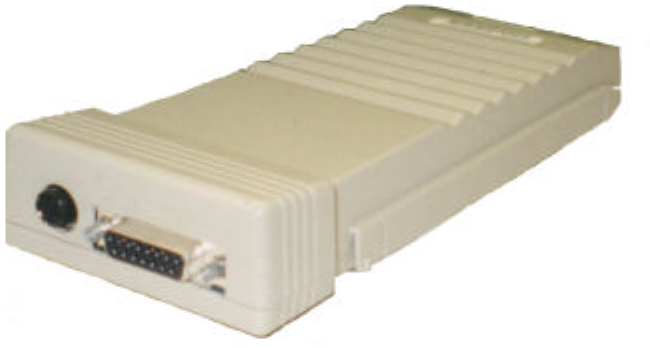


Figure 1 Digital Interface Unit Cryptographic Module

1.3 DIU CM Implementation

The DIU CM is implemented as a multi-chip embedded cryptographic module as defined by FIPS 140-1. It is comprised of the Armor Cryptographic Processor, Flash memory, key zeroization circuitry, tamper circuitry, power regulation, and on board back-up battery all enclosed in a tamper protected housing.

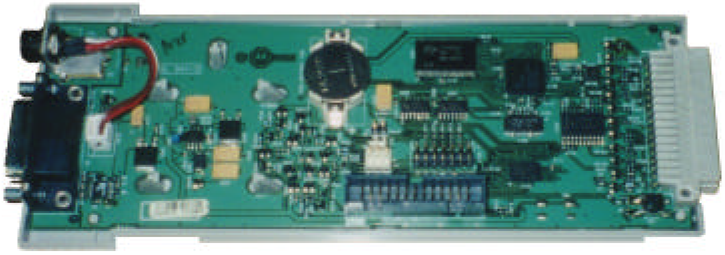


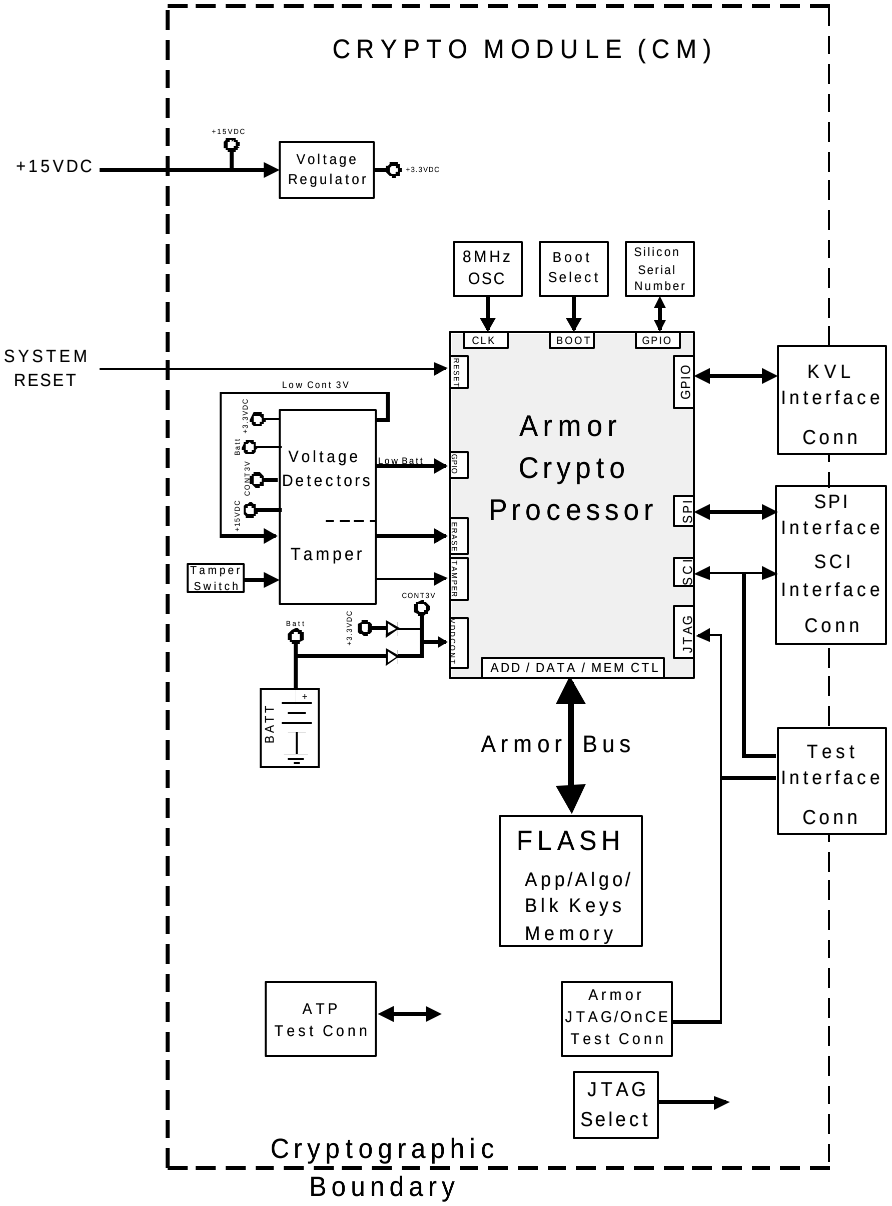
Figure 2 Digital Interface Unit Cryptographic Module (Cover Removed)

1.4 DIU CM Cryptographic Boundary

The DIU CM provides all the cryptographic logic and processes required by the DIU. This includes encryption, decryption, and cryptographic key & critical security parameter storage. The cryptographic boundary is defined as the boundary that encompasses all of the CM circuitry which is bounded by a tamper protected physical enclosure.

The DIU CM consists of the Armor cryptographic processor, flash E^2PROM, SCI port, SPI port, KVL port, Test port, and various support components and circuitry.

Figure 3 DIU CM Cryptographic Boundary



2.0 FIPS 140-1 Security Level

The DIU CM is validated to meet the FIPS 140-1 security requirements for the levels shown in Table 2.1.

Table 2.1
DIU CM Security Levels

FIPS 140-1 Security Requirements Section	Level
1. Cryptographic Module	1
2. Module Interfaces	1
3. Roles and Services	2
4. Finite State Machine Model	1
5. Physical Security	1
6. Software Security	3
7. Operating System Security	N/A
8. Key Management	1
9. Cryptographic Algorithms	1
10. EMI / EMC	1
11. Self Tests	1

3.0 FIPS 140-1 Approved Operational Modes

The DIU CM includes modes of operation that are not FIPS 140-1 approved. Documented below are the configuration settings that are required for the module to be used in a FIPS 140-1 approved mode of operation:

1. FIPS mode enabled
2. MDC OTAR disabled
3. Key Loss Key (KLK) generation disabled
4. DES for encryption, decryption, and MACing shall be used in the following approved modes: ECB, OFB, and CBC
5. AES for encryption, decryption, and MACing shall be used in the following approved modes: ECB, OFB, and CBC
6. Use of TDES 8-bit CFB mode for symmetric encryption / decryption of keys and parameters stored in the internal database, and TDES CBC mode for symmetric decryption of software upgrades are approved modes

Note: Use of the following is not FIPS 140-1 approved: DES-XL, DVI-XL, DVP-XL, and HCA.

4.0 Security Rules

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

4.1 FIPS 140-1 Related Security Rules

1. The CM supports the following interfaces:
   - Data input interface
     a. Serial Peripheral Interface (SPI) - Bypass Digital Voice, Ciphertext Digital Voice, Key Management Data (OTAR), Encrypted Cryptographic Keys (OTAR), Authentication Data
     b. Serial Communications Interface (SCI) - Plaintext Digital Voice
     c. Key Variable Loader (KVL) - Key Management Data, Encrypted Cryptographic Keys, Plaintext Cryptographic Keys, Encrypted Software Image
   - Data output interface
     a. Seria l Peripheral Interface (SPI) - Bypass Digital Voice, Ciphertext Digital Voice, Key Management Data (OTAR)
     b. Serial Communications Interface (SCI) - Plaintext Digital Voice
   - Control input interface
     a. Serial Peripheral Interface (SPI) - Input commands
     b. Serial Communications Interface (SCI) - Input commands
     c. Key Variable Loader (KVL) - Input commands
     d. CM System Reset Signal
   - Status output interface
     a. Serial Peripheral Interface (SPI) - Status codes
     b. Serial Communications Interface (SCI) - Status codes
     c. Key Variable Loader (KVL) - Status codes
   - Power interface
     a. Power (+15VDC & GND) - Powers all CM circuitry. Internal battery supplies power to battery backed register and tamper detection circuitry when +15VDC not available.
2. The CM inhibits all data output via the data output interface whenever a fatal error state exists and during self-tests.
3. The CM 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. Authentication data (e.g. passwords) and other critical security parameters are entered in plaintext form and are never output from any interface.
   AND
   plaintext cryptographic keys are entered over a physically separate port.
6. The CM supports a user role and two categories of cryptographic officer roles. These roles have different sets of services.
7. The CM re-authenticates a role when it is powered-up after being powered-off.
8. The CM provides the following services for the Crypto Officer (Initialization) role:
   - Download RSS
   - Initialize passwords

9. The CM provides the following services for the Crypto Officer (Standard) role:
   - Transfer Key Variables
   - All services available in the User role
10. The CM provides the following services for the User role:
    - Privileged APCO OTAR
    - Change Active Keyset
    - Change Password
    - Logout
    - Encrypt Digital Voice
    - Decrypt Digital Voice
    - Clear Bypass
    - Zeroize Selected Keys
    - Software Update
    - All services available without a role
11. The CM provides the following services not requiring a role:
    - Login (Validate Password)
    - Algorithm Request
    - Software Version/Soundoff/Keep Alive
    - Initiate Self Tests
    - Zeroize all keys
    - Non-Privileged APCO OTAR
    - Zeroize All Keys and Passwords
    - Extract / Clear Error Log
    - Key Status
    - Reset Crypto Module
12. The CM enforces Role-Based authentication.
13. The CM implements all software using a high-level language, except the limited use of low-level languages to enhance performance.
14. The CM protects secret keys and private keys from unauthorized disclosure, modification and substitution.
15. The CM provides a means to ensure that a key entered into or stored within the CM is associated with the correct entities to which the key is assigned. Each key in the CM 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.
16. The CM denies access to plaintext secret and private keys contained within the CM.
17. The CM provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the CM.
18. The CM supports the following FIPS approved algorithms:

- DES
  - OFB for symmetric encryption / decryption of digital voice and APCO-25 OTAR
  - CBC for MACing of APCO-25 OTAR and software upgrades
  - ECB for symmetric decryption of APCO-25 OTAR
- TDES
  - 8-bit CFB for symmetric encryption / decryption of keys and parameters stored in the internal database
  - CBC for symmetric decryption of software upgrades
- AES
  - OFB for symmetric encryption / decryption of digital voice and APCO-25 OTAR
  - CBC for use in APCO-25 OTAR and software upgrades
  - ECB for symmetric decryption of APCO-25 OTAR

19. The DIU CM, when used in the DIU, conforms to all FCC Class A requirements.
20. The CM performs the following self-tests:

- Power-up and on-demand tests
  - Cryptographic algorithm test: Each algorithm is tested by using a known key, known data, and if required a known IV. The data is then encrypted; the encrypted data is then decrypted. The test passes if the final data matches the known 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 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.

  Powering the module off then on or resetting the module using the CM Reset signal 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 DES-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 X9.17 deterministic Pseudo Random Number Generator (PRNG) and the maximal length 64-bit LFSR. The second is an implementation of Appendix C ANSI X9.17 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.

21. The CM 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 CM reset signal is activated or by cycling the power to the CM. The CM performs power-up self tests when its reset signal is activated or its power is cycled. The CM will again enter an error state if these tests continue to fail upon each subsequent power-up self test.
22. The CM enters an error state if the Software/Firmware test fails. This error state is exited after the CM reset signal is activated or by cycling the power to the CM. The CM performs power-up self tests when its reset signal is activated or its power is cycled. The CM will again enter an error state if the Software/Firmware test continues to fail upon each subsequent power-up self test.
23. The CM enters an error state if the Software/Firmware Load test fails. This error state is exited after the CM reset signal is activated or by cycling the power to the CM.
24. The CM outputs an error indication via the status interface whenever an error state is entered due to a failed self-test.
25. The CM does not perform any cryptographic functions while in an error state.

4.2 Motorola Imposed Security Rules

1. The DIU CM does not support multiple concurrent operators.
2. The cryptographic module will continue to provide User role and Crypto Officer role services until the module has been powered down or until logged out of the role.
3. All cryptographic module services are suspended during key loading.
4. After more than ten (10) consecutive unsuccessful user login attempts, the module will zeroize all passwords and keys from the key database.
5. Upon detection of a critically low voltage condition on the CM's +15VDC power supply, the cryptographic module shall erase all plaintext keys.
6. Upon detection of a critically low voltage condition on the CM's +3.3VDC internal operating power supply, the cryptographic module shall erase all plaintext keys.
7. Upon detection of a critically low voltage condition on the CM's continuous +3VDC battery backed power supply, the cryptographic module shall erase all Security Related Data Items (SRDIs).
8. Upon detection of tamper, the cryptographic module shall erase all SRDIs.
9. The module shall at no time output any SRDIs.

5.0 Roles and Services

5.1 DIU CM Supported Roles

The CM supports three (2) main roles as defined by FIPS 140-1 of which the Crypto Officer role has two (2) different categories. These roles are defined to be:

- Cryptographic Officer roles (2)
    - Crypto Officer (Initialization)
    - Crypto Officer (Standard)
- User role

5.2 DIU CM Services

Services available in Crypto Officer (Initialization) role:

- Download RSS: Download configuration parameters used to specify module behavior. Examples include enable/disable FIPS mode, enable/disable KLK generation, etc.
- Initialize passwords for each role: Initialize passwords for the two (2) individual Crypto Officer (Standard) roles and the ten (10) individual User roles. Modify the default password for the one (1) individual Crypto Officer (Initialization) role.

Services available in Crypto Officer (Standard) role:

- Transfer key variables: Transfer key variables to the CM's key database via a Key Variable Loader (KVL).
- All services available in the user role (see below).

Services available in User role:

- Privileged APCO OTAR: Modify and query the Key Database via APCO OTAR Key Management Messages.
- Change Active Keyset: Modify the currently active keyset used for selecting keys by PID or CKR.
- Change Password: Modify the current password used to identify and authenticate the assumed role.
- Logout: Leave the assumed role and deny access to services associated with that role
- Encrypt Digital Voice: Encrypt digital voice.
- Decrypt Digital Voice: Decrypt digital voice.
- Clear Bypass: Bypass encryption/decryption and allow plaintext to pass through CM.
- Zeroize Selected Keys: Zeroize selected key variables from the Key Database by Physical ID (PID) or Common Key Reference (CKR).
- Software Update: Update the CM software via the KVL.
- All services available without a role (see below).

Services available without a role:

- Login (Validate Password): Validate the entered password and authenticate the assumed role.
- Algorithm Request: Provides list of algorithms currently loaded in the CM.
- Software Version/Soundoff/Keep Alive: Provides basic CM keep alive status with simple message response containing version of software currently loaded on CM.
- Initiate Self Tests: Performs module self tests comprised of cryptographic algorithms test, software firmware test, and critical functions test. Initiated by CM reset or transition from power off state to power on state.
- Zeroize All Keys: Zeroize all keys from the Key Database (Module can be reinitialized using KVL).
- Non-Privileged APCO OTAR: Hello and Capabilities Key Management Messages processed.

- Zeroize All Keys and Password: Zeroizes all SRDIs. Clears all User and Crypto Officer (Standard) role passwords and resets the Crypto Officer (Initialization) password to the factory default. Allows access to the module if password(s) are forgotten.
- Extract / Clear Error Log: Provides history of error events (Error & software module where occurred) and provides option to clear history of error events.
- Key Status: Provides status of all keys residing in module (Location, ID, algorithm used with).
- Reset Crypto Module: Hardware signal reset of module to remove CM from error states.

6.0 Authentication

The DIU CM uses 40-bit passwords to authenticate the Crypto Officer (Initialization) role, the two (2) Crypto Officer (Standard) roles, and the ten (10) User roles. The Crypto Officer (Initialization) role password is initialized to a default value during manufacturing and after a tamper activation has occurred. The Crypto Officer (Standard) and User role passwords are initialized while in the Crypto Officer (Initialization) role. After authenticating to an individual role, the password for that role may be changed at any time.

More than ten (10) consecutive invalid authentication attempts activates the tamper response; all critical security parameters (all keys from the Key Database & all passwords) are zeroized. In addition, the Crypto Officer (Initialization) role password is reset to its default value.

7.0 Access Control

7.1 Security Relevant Data Items (SRDIs)

Table 7.1
SRDI Definition

SRDI Identifier	Description
Key Protection Key (KPK)	Key used to encrypt/decrypt the key database and other non-volatile parameters. It is internally generated and unique each time generated.
Plaintext Traffic Encryption Keys (TEK)	Keys used for voice and Key Management Message (KMM) encryption/decryption.
Plaintext Key Encryption Keys (KEK)	Keys used to encrypt/decrypt keys in OTAR KMMs.
Plaintext MAC Key	Key used for authentication of software upgrade.
Plaintext Password	Operator password entered during user authentication.

7.2 SRDI Access Types

Table 7.2
SRDI Access Types

SRDI Access Type	Description
Retrieve key	Decrypts encrypted TEKs or KEKs in the database using the KPK and returns plaintext version.
Store key	Encypts plaintext TEKs or KEKs using the KPK and stores the encrypted version in the database.
Erase Key	Marks encrypted TEK or KEK data in key database as invalid.
Create KPK	Generates and stores new KPK.
Store Password	Hashes user password and stores it in the database.

7.3 Access Matrix

Table 7.3
SRDI versus SRDI Access

User Service	SRDI Access Operation					Applicable Role			
	Retrieve Key	Store Key	Erase Key	Create KPK	Store Password	Crypto Officier (Initialization)	Crypto Officier (Standard)	User	No Role Required
1. Download RSS (Enable FIPS mode & Initialize CM parameters)						X			
2. Initialize passwords					X	X			
3. Transfer key variables		X	X				X		
4. Privileged APCO OTAR	X	X	X				X	X	
5. Change Active Keyset							X	X	
6. Change Password			X	X	X	X	X	X	
7. Login (Validate Password)						X	X	X	X
8. Logout						X	X	X	
9. Encrypt Digital Voice	X						X	X	
10. Decrypt Digital Voice	X						X	X	
11. Clear Bypass							X	X	
12. Zeroize Selected Keys			X				X	X	
13. Algorithm Request							X	X	X
14. Software Version/Soundoff/Keep Alive							X	X	X
15. Software Update	X						X	X	
16. Initiate Self Tests							X	X	X
17. Zeroize All Keys			X				X	X	X
18. Non-Privileged APCO OTAR							X	X	X
19. Zeroize All Keys and Password			X	X	X		X	X	X
20. Extract / Clear Error Log						X	X	X	X
21. Key Status						X	X	X	X
22. Reset Crypto Module							X	X	X