MOTOROLA

Security Policy: Astro Subscriber Encryption Module

Astro Saber, Astro Spectra,
Astro Consolette, XTS3000

Version 01.03.07

8/22/2002

MOTOROLA

1.0 Introduction

1.1 Scope

This Security Policy specifies the security rules under which the Astro Subscriber Encryption Module, herein identified as the Universal Cryptographic Module or UCM, 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 UCM provides secure key management, Over-the-Air-Rekeying (OTAR), and voice and data encryption for the Motorola Astro Saber portable radio, XTS3000 portable radio, Astro Spectra mobile radio, and Astro Consolette.
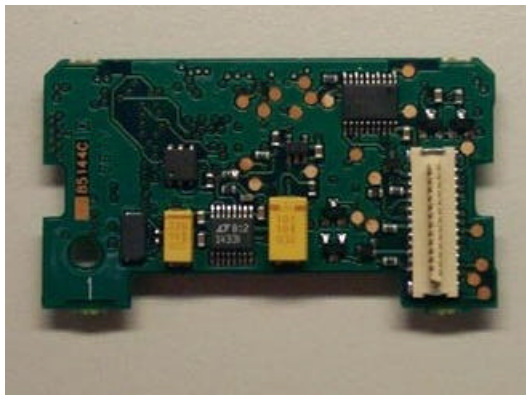

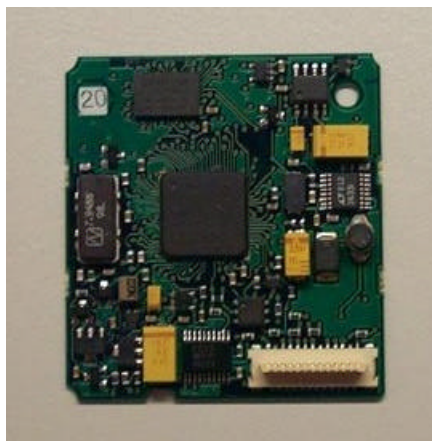**Figure 1 Astro Saber, Astro Spectra, and Astro Consolette UCM**

Figure 2 XTS3000 UCM

1.3 UCM Implementation

MOTOROLA

The UCM is implemented as a multi-chip embedded cryptographic module as defined by FIPS 140-1.

1.4 UCM Cryptographic Boundary

The UCM is defined as the UCM printed circuit board. This includes the Armor IC, flash E^{2}PROM IC, SCI port, SPI port, KVL port, and various support components and circuitry.

2.0 FIPS 140-1 Security Level

The UCM is certified to meet the FIPS 140-1 security requirements for the levels shown in Table 2.1.

Table 2.1
UCM 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
Overall Validation Level	1

3.0 FIPS 140-1 Approved Operational Modes

The UCM 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. MDC OTAR disabled
2. Key Loss Key (KLK) generation disabled
3. Tamper Enabled
4. DES for encryption, decryption, and MACing shall be used in the following approved modes: ECB, OFB, CFB, 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

Use of the following is not FIPS 140-1 approved:
1. Key Loss Key (KLK) generation enabled
2. Tamper disabled
3. MDC OTAR enabled
4. DES-XL, DVI-XL, DVI-SPFL, DVP-XL

4.0 Security Rules

The UCM 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 UCM supports the following interfaces:
   - Data input interface
     a. Serial Communications Interface (SCI) - Plaintext Data, Ciphertext Data
     b. Synchronous Peripheral Interface (SPI) - Key Management Data (OTAR), Encrypted Cryptographic Keys (OTAR), Authentication Data
     c. Key Variable Loader (KVL) - Key Management Data, Encrypted Cryptographic Keys, Plaintext Cryptographic Keys
   - Data output interface
     a. Serial Communications Interface (SCI) - Plaintext Data, Ciphertext Data
     b. Synchronous Peripheral Interface (SPI) - Key Management Data (OTAR)
   - Control input interface
     a. Serial Communications Interface (SCI) - Input Commands
     b. Synchronous Peripheral Interface (SPI) - Input Commands
     c. Key Variable Loader (KVL) - Input Commands
   - Status output interface
     a. Serial Communications Interface (SCI) - Status Codes
     b. Synchronous Peripheral Interface (SPI) - Status Codes
     c. Key Variable Loader (KVL) - Status Codes
   - Power interface
     a. Switched - Powers all circuitry except Battery Backed Register
     b. Unswitched - Powers Battery Backed Register
2. The UCM inhibits all data output via the data output interface whenever an error state exists and during self-tests.
3. The UCM logically disconnects the output data path from the circuitry and processes when performing key generation, manual key entry, or key zeroization.
4. Authentication data (e.g. PINs) and other critical security parameters are entered / output in plaintext form.
   AND
   Secret cryptographic keys are entered / output over a physically separate port.
5. The UCM supports a User role and a Cryptographic Officer role. These two roles have the same set of services.
6. The UCM re-authenticates a role when it is powered-up after being powered-off.
7. The UCM provides the following services requiring a role:
   - Zeroize Selected Keys

MOTOROLA

- Transfer Key Variable
- Privileged APCO OTAR
- Change Active Keyset
- Change Password
- Encrypt Securenet
- Decrypt Securenet
- Encrypt Digital
- Decrypt Digital

8. The UCM provides the following services not requiring a role:
    - Initiate Self Tests
    - Zeroize all keys
    - Non-Privileged APCO OTAR
    - Zeroize All Keys and Password
    - Reset Crypto Module
    - Shutdown Crypto Module
    - Extract Log
    - Clear Log
    - Download RSS

9. The UCM enforces Role-Based authentication.

10. The UCM implements all software using a high-level language, except the limited use of low-level languages to enhance performance.

11. The UCM protects secret keys and private keys from unauthorized disclosure, modification and substitution.

12. The UCM provides a means to ensure that a key entered into, stored within, or output from the UCM is associated with the correct entities to which the key is assigned. Each key in the UCM 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.

13. The UCM denies access to plaintext secret and private keys contained within the UCM.

14. The UCM provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the UCM.

15. The UCM supports the following FIPS approved algorithms:
    - DES
        - OFB for symmetric encryption / decryption of digital voice, data, and Project 25 OTAR
        - 1-Bit CFB for symmetric encryption / decryption of analog voice
        - CBC for MACing of Project 25 OTAR and software upgrades

- ECB for symmetric decryption of Project 25 OTAR
- AES
    - OFB for symmetric encryption / decryption of digital voice, data, and Project 25 OTAR
    - CBC for MACing of Project 25 OTAR and software upgrades
    - ECB for symmetric decryption of Project 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
16. The UCM, when used in the Astro Saber, Astro Spectra, Astro Consolette, and XTS3000 conforms to all FCC requirements for radios.
17. The UCM 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 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 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 RNGs within the module. The first is a hardware RNG which is used to seed the ANSI X9.17 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.

18. The UCM 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 may be exited by powering the module off then on.
19. The UCM enters an error state if the Software/Firmware test fails. This state is exited as soon as an error indicator is output via the status interface.
20. The UCM enters an error state if the Software/Firmware Load test fails. This state is exited as soon as an error indicator is output via the status interface.
21. The UCM outputs an error indicator via the status interface whenever an error state is entered due to a failed self-test.
22. The UCM does not perform any cryptographic functions while in an error state.

4.2 Motorola Imposed Security Rules

1. The UCM does not support a bypass mode.
2. The UCM does not support multiple concurrent operators.
3. The cryptographic module will continue to provide User Role and Crypto Officer Role services until the module has been powered down.
4. All cryptographic module services are suspended during key loading.
5. After a sufficient number (15) of consecutive unsuccessful user login attempts, the module will zeroize all keys from the Key Database.
6. Upon detection of a critically low voltage condition on the switched power supply, the cryptographic module shall erase all plaintext keys.
7. Upon detection of a critically low voltage condition on the unswitched power supply, the cryptographic module shall erase all SRDIs.
8. Upon detection of tamper, the cryptographic module shall erase all SRDIs.
9. The module shall at no time output any security related data items (SRDIs)

5.0 Roles and Services

5.1 UCM Supported Roles

The UCM supports two (2) roles. These roles are defined to be:
- the User Role,
- the Cryptographic Officer (CO) Role

5.2 UCM Services

- Transfer Key Variable: Transfer key variables and/or zeroize key variables to/from the Key Database via a Key Variable Loader (KVL). Available to User and CO Roles.
- Privileged APCO OTAR: Modify and query the Key Database via APCO OTAR Key Management Messages. Available to User and CO Roles.
- Change Active Keyset: Modify the currently active keyset used for selecting keys by PID or CKR. Available to User and CO Roles.
- Change Password: Modify the current password used to identify and authenticate the User and CO Roles. Available to User and CO Roles.

- Encrypt Securenet: Encrypt 12 Kb analog voice. Available to User and CO Roles.
- Decrypt Securenet: Decrypt 12 Kb analog voice. Available to User and CO Roles.
- Encrypt Digital: Encrypt digital voice or data. Available to User and CO Roles.
- Decrypt Digital: Decrypt digital voice or data. Available to User and CO Roles.
- 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. Available without a Role.
- Zeroize Selected Keys: Zeroize selected key variables from the Key Database by Physical ID (PID) or Common Key Reference (CKR). Available to User and CO Roles.
- Zeroize all keys: Zeroize all keys from the Key Database. Available without a Role. (Module can be reinitialized using KVL)
- Zeroize All Keys and Password: Zeroizes all keys and SRDIs in the key database. Resets the password to the factory default. Allows user to gain controlled access to the module if the password is forgotten. Available without a Role. (Module can be reinitialized using KVL)
- Non-Privileged APCO OTAR: Hello and Capabilities Key Management Messages may be performed without a Role.
- Reset Crypto Module: Soft reset of module to remove module from error states. Available without a Role.
- Shutdown Crypto Module: Prepares module for removal of power. Available without a Role.
- Extract Log: Status Request. Provides detailed history of error events. Available without a Role.
- Clear Log: Clears history of error events. Available without a Role.
- Download RSS: Download configuration parameters used to specify module behavior. Examples include enable/disable APCO OTAR, SingleKey or MutliKey mode, etc. Available without a Role.

6.0 Authentication

The UCM uses a 40-bit password to authenticate the User and CO roles. The password is initialized to a default value during manufacturing. After authenticating, the password may be changed at any time. Fifteen consecutive invalid authentication attempts erases all keys from the Key Database.

7.0 Access Control

7.1 Security Relevant Data Items (SRDIs)

MOTOROLA

Table 7.1
SRDI Definition

SRDI Identifier	Description
Key Protection Key (KPK)	Key used to encrypt the database and other non-volatile parameters
Plaintext Traffic Encryption Keys (TEKs)	Keys used for voice and data encryption
Plaintext Key Encryption Keys	Keys used encryption of keys in OTAR
Plaintext MAC Key	Key used for authentication of software upgrade. Stored in non-volatile memory
Plaintext Password	User 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

MOTOROLA

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 Pin	User Role	Crypto Officer Role	No Role Required
1. Transfer Key Variable		X	X			X	X	
2. Privileged APCO OTAR	X	X	X			X	X	
3. Change Active Keyset						X	X	
4. Change Password			X	X	X	X	X	
5. Encrypt Securenet	X					X	X	
6. Decrypt Securenet	X					X	X	
7. Encrypt Digital	X					X	X	
8. Decrypt Digital	X					X	X	
9. Initiate Self Tests						X	X	X

	SRDI Access Operation					Applicable Role		
10. Zeroize Selected Keys			X			X	X	
11. Zeroize All Keys			X			X	X	X
12. Zeroize All Keys and Password			X	X	X	X	X	X
13. Non-Privileged APCO OTAR						X	X	X
14. Reset						X	X	X
15. Shutdown						X	X	X
16. Extract Log						X	X	X
17. Clear Log						X	X	X
18. Download RSS			X	X		X	X	X