MOTOROLA

Security Policy: Astro Subscriber Encryption Module

Astro Spectra, Astro Saber, Astro Consolette,
and Astro XTS3000

Version 02.00.07

3/22/2004

1.0 Introduction

1.1 Scope

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

1.3 Astro Subscriber UCM Implementation

The Astro Subscriber UCM is implemented as a multi-chip embedded cryptographic module as defined by FIPS 140-2.

1.4 Astro Subscriber UCM Cryptographic Boundary

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

2.0 FIPS 140-2 Security Level

The Astro Subscriber UCM is certified to meet the FIPS 140-2 security requirements for the levels shown in Table 2.1. The overall module is certified FIPS 140-2 Security Level 1.

Table 2.1
Astro Subscriber UCM Security Levels

FIPS 140-2 Security Requirements Section	Level
1. Cryptographic Module Specification	1
2. Module Ports and Interfaces	1
3. Roles, Services, and Authentication	2
4. Finite State Model	1
5. Physical Security	1
6. Operational Environment	N/A
7. Cryptographic Key Management	1
8. EMI / EMC	1
9. Self Tests	1
10. Design Assurance	1
11. Mitigation of Other Attacks	N/A

3.0 FIPS 140-2 Approved Operational Modes

The Astro Subscriber UCM includes modes of operation that are not FIPS 140-2 approved. Documented below are the configuration settings that are required for the module to be used in a FIPS 140-2 approved mode of operation:

1. MDC OTAR disabled
2. Key Loss Key (KLK) generation disabled
3. Tamper Enabled
4. DES for encryption, decryption, and authentication (MAC) shall be used in the following approved modes: ECB, OFB, CFB, and CBC **OR**
5. AES-256 for encryption, decryption, and authentication (authentication, AES MAC, is approved when used for Project 25 OTAR) may be used in the following approved modes: OFB, ECB, and CBC.
6. Use of 3DES 8-bit CFB mode for symmetric encryption / decryption of keys and parameters stored in the internal database, and 3DES CBC mode for symmetric decryption of software upgrades are approved modes

Use of the following algorithms is not FIPS 140-2 approved: DES-XL, DVI-XL, DVI-SPFL, DVP-XL, SHA-1

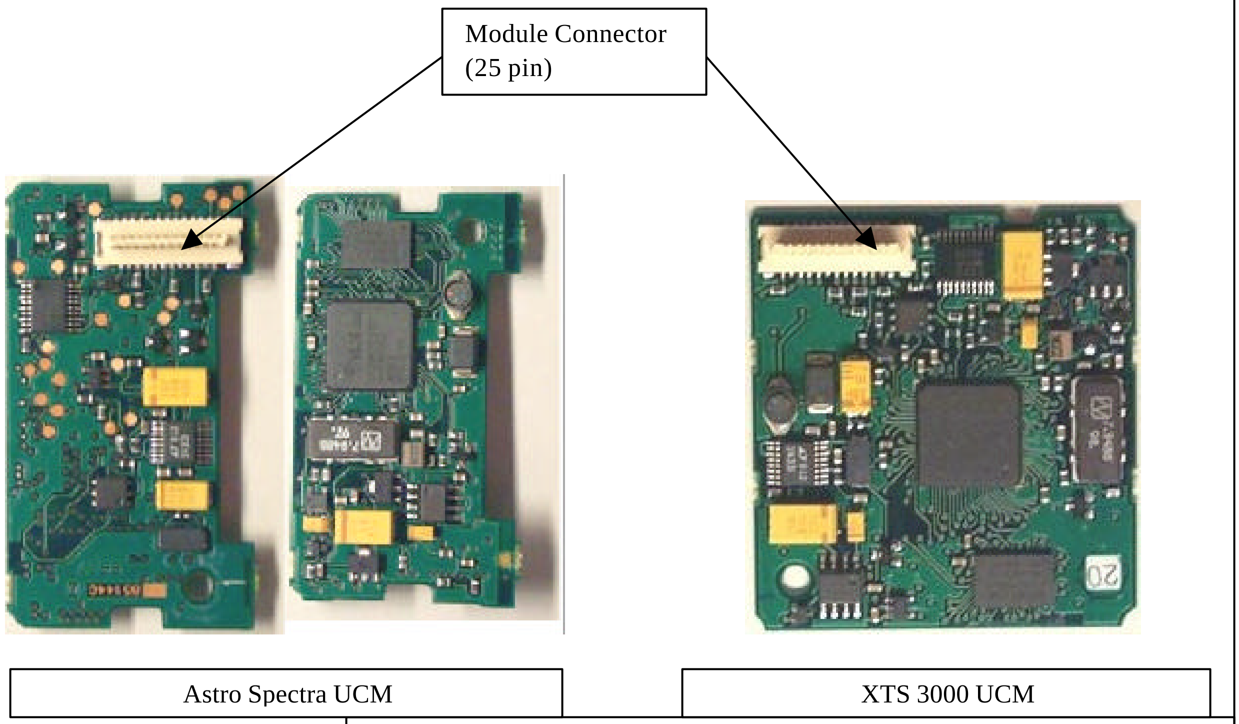
4.0 Security Rules

The Astro Subscriber UCM 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 Astro Subscriber 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



The UCM Module Connector contains all interface connections to the UCM: SPI (Data, Control, Status, OTAR Key data), SCI (Data, Control, Status), KVL (Key Data, Control, Status), and Unswitched and Switched Power Connections. It is also used for tamper detection: If the module is ever disconnected from its host Radio, a tamper will be detected and all security related data items (CSPs) will be erased.

UCM Diagram (Interface Connection)

2. The Astro Subscriber UCM inhibits all data output via the data output interface whenever an error state exists and during self-tests.
3. The Astro Subscriber 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 Astro Subscriber UCM supports a User role and a Cryptographic Officer role. These two roles have the same set of services.
6. The Astro Subscriber UCM re-authenticates a role when it is powered-up after being powered-off.
7. The Astro Subscriber UCM prevents brute-force attacks on its password by using a 40-bit password with more than 1 trillion possible combinations. Also, a limit of 15 failed authentication attempts is imposed; 15 consecutive failed

authentication attempts causes all keys to be erased and the password to be reset to the factory default.

8. The Astro Subscriber UCM provides the following services requiring a role:
   - Zeroize Selected Keys
   - Transfer Key Variable
   - Privileged APCO OTAR
   - Change Active Keyset
   - Change Password
   - Encrypt Securenet
   - Decrypt Securenet
   - Encrypt Digital
   - Decrypt Digital
9. The Astro Subscriber 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
   - Key/Keyset Check
   - Program Update
10. The Astro Subscriber UCM enforces Role-Based authentication.
11. The Astro Subscriber UCM implements all software using a high-level language, except the limited use of low-level languages to enhance performance.
12. The Astro Subscriber UCM protects secret keys and private keys from unauthorized disclosure, modification and substitution.
13. The Astro Subscriber UCM provides a means to ensure that a key entered into, stored within, or output from the Astro Subscriber UCM is associated with the correct entities to which the key is assigned. Each key in the Astro Subscriber 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.
14. The Astro Subscriber UCM denies access to plaintext secret and private keys contained within the Astro Subscriber UCM.

15. The Astro Subscriber UCM provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the Astro Subscriber UCM.
16. The Astro Subscriber 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 authentication of Project 25 OTAR and software upgrades
        - ECB for symmetric decryption of Project 25 OTAR
    - 3DES
        - 8-bit CFB for symmetric encryption / decryption of keys and parameters stored in the internal database
        - CBC for symmetric decryption of software upgrades
    - AES-256
        - OFB for symmetric encryption / decryption of digital voice and data
        - CBC for authentication of Project 25 OTAR
        - ECB for symmetric decryption of Project 25 OTAR
17. The Astro Subscriber UCM, when used in the Astro Spectra, Saber, XTS3000, and Consolette, conforms to all FCC requirements for radios.
18. The Astro Subscriber 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 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 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 X9.31 PRNG and the maximal length 64-bit LFSR. The second is an implementation of Appendix C 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.

19. The Astro Subscriber 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.
20. The Astro Subscriber UCM enters an error state if the Software/Firmware test fails. As soon as an error indicator is output via the status interface, the module transitions from the error state to a state that only allows new software to be loaded.
21. The Astro Subscriber 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.
22. The Astro Subscriber UCM outputs an error indicator via the status interface whenever an error state is entered due to a failed self-test.
23. The Astro Subscriber UCM does not perform any cryptographic functions while in an error state.

4.2 Motorola Imposed Security Rules

1. The Astro Subscriber UCM does not support a Bypass mode.
2. The Astro Subscriber 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 CSPs.
8. Upon detection of tamper, the cryptographic module shall erase all CSPs.
9. The module shall at no time output any critical security parameters (CSPs)

5.0 Crypto Officer Guidance

5.1 Administration of the UCM in a secure manner

The UCM requires no special administration for secure use after it is set up for use in a FIPS approved manner. To do this, set the module's parameters to the settings listed in section 3 of this document.

5.2 Assumptions regarding User Behavior

The UCM 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.

6.0 User Guidance

6.1 Approved Security Functions, Ports, and Interfaces available to Users

All UCM services are available to the UCM User. These are listed in section 9.2 of this document.

No Physical Ports or Logical Interfaces are directly available to the UCM User, only indirectly through the Subscriber Radio in which the UCM is installed. The User need not concern himself with them.

6.2 User Responsibilities necessary for Secure Operation

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

7.0 Identification and Authentication Policy

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

Role	**Authentication Type**	**Authentication Data Required**
User	Role-Based	40-bit Password
Crypto Officer	Role-Based	

8.0 Physical Security Policy

The Astro Subscriber UCM uses a tamper-detect circuit that triggers a tamper whenever the UCM is physically separated from the radio, or the UCM's protective shield is removed. Any detection of a physical intrusion will cause all CSPs to be deleted immediately if the module is still powered up, or at next powerup if it is not powered up. No user maintenance is needed for the physical security mechanisms.

Physical Security Mechanism	**Maintenance Needed**
Tamper Detect Circuit	None

9.0 Access Control Policy

9.1 Astro Subscriber UCM Supported Roles

The Astro Subscriber UCM supports two (2) roles. These roles are defined to be:

- the User Role,
- the Cryptographic Officer (CO) Role

9.2 Astro Subscriber UCM Services

- Show Status: Available through SPI Commands to User and CO roles.
- 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 CSPs 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.
- Key/Keyset Check: Obtain status information about a specific key/keyset. Available without a Role.
- Program Update: Update the module software. Available without a Role.

9.3 Critical Security Parameters (CSPs)

Table 9.3
CSP Definition

CSP 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 (KEKs)	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

9.4 CSP Access Types

Table 9.4
CSP Access Types

CSP 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

Table 9.5
CSP versus CSP Access
(Shaded Services are available to User or CO role only)

	CSP Access Operation					Applicable Role		
User Service	Retrieve Key	Store Key	Erase Key	Create KPK	Store Password	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. Zeroize Selected Keys			X			X	X	
10. Initiate Self Tests						X	X	X
11. Validate Password						X	X	X
12. Zeroize All Keys			X			X	X	X
13. Zeroize All Keys and Password			X	X	X	X	X	X
14. Non-Privileged APCO OTAR (not for key entry)						X	X	X
15. Reset						X	X	X
16. Shutdown						X	X	X
17. Extract Log (Show Status)						X	X	X
18. Clear Log						X	X	X
19. Download RSS			X	X		X	X	X
20. Key/Keyset Check						X	X	X
21. Program Update	X	X	X			X	X	X

10.0 Mitigation of Other Attacks Policy

The UCM is not designed to mitigate any specific attacks outside of those required by FIPS 140-2, including but not limited to power consumption, timing, fault induction, or TEMPEST attacks.