Security Policy: Astro Subscriber Universal Crypto Module (UCM)

Cryptographic module used in Motorola's Astro Spectra Plus, XTL5000, XTS5000, XTL2500, XTS2500 and XTS4000 radios.

Version: R01.02.26

Date: November 17, 2010

Table of Contents

1. Introduction

1.1. Scope

This Security Policy specifies the security rules under which the Astro Subscriber Universal Crypto Module, herein identified as the Astro Subscriber 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. security related data items (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 following Motorola mobile and portable two-way radios:

- Astro Spectra Plus mobile
- XTL5000 mobile
- XTS5000 portable
- XTL2500 mobile
- XTS2500 portable
- XTS4000 portable

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 Hardware / Firmware Version Numbers

Radio Name	**FIPS Validated Cryptographic Module Hardware Kit Numbers**	**FIPS Validated Cryptographic Module Firmware Version Numbers** **(one firmware version should be loaded per hardware kit)**
Astro Spectra Plus	NTN9801B	R05.06.00 R05.06.01 R05.07.10
XTL5000, XTS5000, XTL2500	NTN9738C, NNTN5032D NNTN5032F, NNTN5032G, NNTN5032H, NNTN7427A	R05.06.00 R05.06.01 R05.07.10
XTS2500	0104020J49, 0104020J50, 0104020J51, 0104024J43, 0104024J44, 0104024J45, 0104025J11, 0104025J12, 0104027J01	R05.06.00 R05.06.01 R05.07.10
XTS4000	NNTN7097A	R05.06.00 R05.06.01

		R05.07.10

1.5. Astro Subscriber UCM Cryptographic Boundary

The Astro Subscriber UCM Cryptographic Boundary is described in each Figure's caption below:

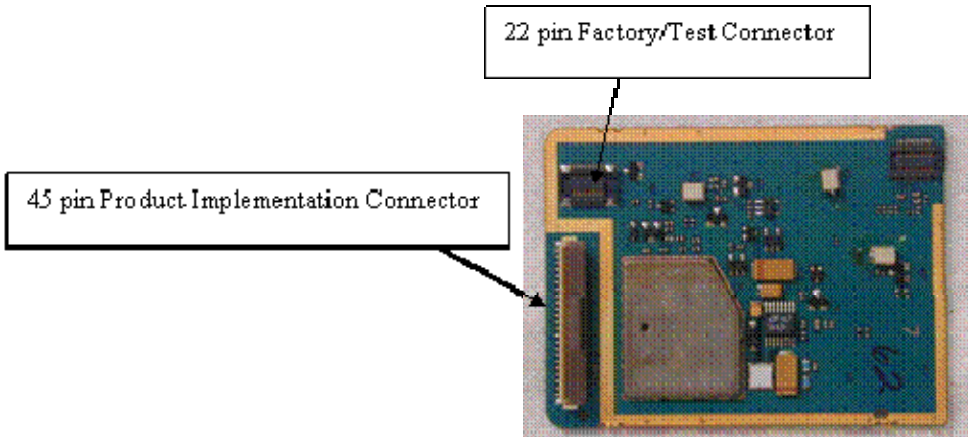

Figure 1: HW kits 0104025J12, 0104025J11, 0104024J45, 0104024J44, 0104024J43, 0104020J49, 0104020J50, 0104020J51, & 0104027J01. The Crypto Boundary is the entire printed circuit board. The Factory/Test connector contains all interface connections to the secure module: SPI (Data, Control, Status, and OTAR Key data), KVL (Key Data, Control, and Status), SCI (factory programming; disabled in firmware outside the factory) and Unswitched and Switched Power Connections. The factory/test connector is not connected when the module is in its intended product. The Product Implementation connector contains all that of the factory/test connecter except for the SCI interface. This interface is used for all secure communications when the module is in its intended product.

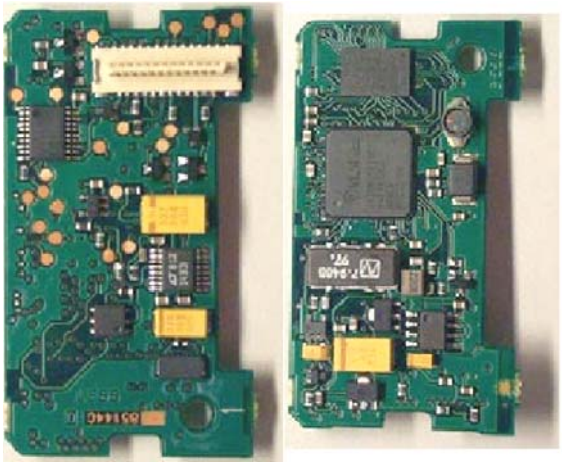

Figure 2: HW kit NTN9801B. The Crypto Boundary is the entire printed circuit board. The 25-pin UCM Module Connector contains all interface connections to the UCM: SPI (Data, Control, Status, OTAR Key data), KVL (Key Data, Control, Status), and Unswitched and Switched Power Connections.

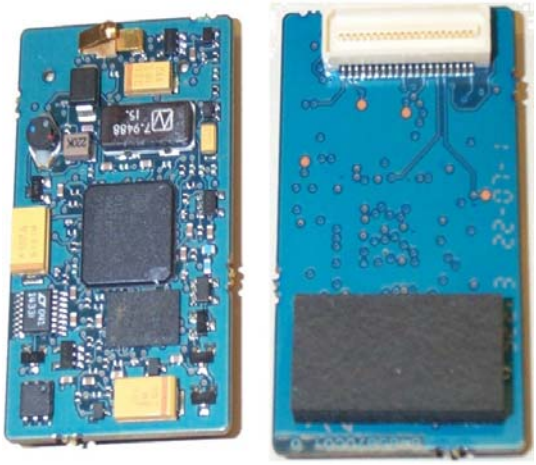

Figure 3: HW kits NTN9738C, NNTN5032D, NNTN5032F and NNTN5032G. The Crypto Boundary is the entire printed circuit board. The 40-pin UCM Module Connector contains all interface connections to the UCM: SPI (Data, Control, Status, OTAR Key data), KVL (Key Data, Control, Status), and Unswitched and Switched Power Connections.

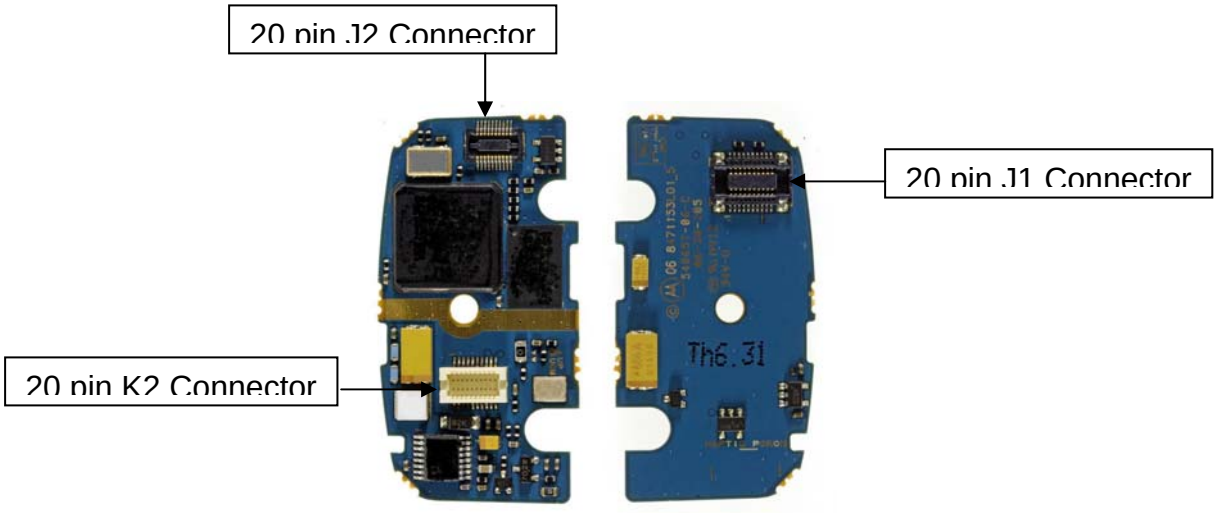

Figure 4: XTS4000 HW kit NNTN7097A. The Crypto Boundary is the entire printed circuit board.
The Module contains three 20–pin connectors named J1, J2 and K2. Connector J1 is used for Factory programming and testing, which contains all interface connections to the secure module: SPI (Data, Control, Status, and OTAR Key data), KVL (Key Data, Control, and Status), SCI (factory programming; disabled in firmware outside the factory), Unswitched and Switched Power Connections and is not connected when the module is in its intended product. Connector K2 is used to interface the XTS4000 to the Radio's main board, which contains all signals of J1 except for the SCI interface. Connector J2 is used for four radio signals only. These are routed internally thru the UCM board from K2 to J2 to avoid wrapping a flex cable around the board. These signals are for the Radio Speaker (Data) (INT_SPKR+, INT_SPKR-), Microphone (Data) (INT_MIC), and Vibrator (Control) (INT_VIBR) and are not security relevant.

2. FIPS 140-2 Security Level

The Astro Subscriber UCM is validated to meet the FIPS 140-2 security requirements for the levels shown below. The overall module is validated to FIPS 140-2 Security Level 1.

Table 1: Astro Subscriber UCM Security Levels

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

3. FIPS 140-2 Approved Operational Modes

The Astro Subscriber UCM includes modes of operation that are FIPS Approved mode of operation and Non-FIPS Approved mode of operation.

3.1. FIPS 140-2 Approved Mode of Operation

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. Motorola Data Communication Over The Air Rekeying (MDC OTAR) disabled. The Download RSS service is used to configure this parameter in the module.
2. Key Loss Key (KLK) generation disabled. The Download RSS service is used to configure this parameter in the module.
3. Infinite UKEK Retention is disabled. The Download RSS service is used to configure this parameter in the module.

   AND/OR

   AES-256 encryption, decryption, and authentication may be used in the following approved modes: OFB, ECB, CBC, and GCM; (authentication, AES MAC, is approved when used for Project 25 OTAR. Note: AES (Cert. #2, key wrapping; key establishment provides 256 bits of encryption strength).
4. The module uses Triple-DES 8-bit CFB mode for symmetric encryption / decryption of keys and parameters stored in the internal database, and Triple-DES CBC mode for symmetric decryption of firmware upgrades, which are approved modes.

3.2. FIPS 140-2 Non Approved Mode of Operation

A non-FIPS 140-2 Approved mode of operation is transitioned to when any of the following is true:

1. The following non-Approved algorithms and modes are installed:
   - DES
   - DES MAC
   - DES-XL
   - DVI-XL
   - DVI-SPFL
   - DVP-XL
   - ADP
   - HCA (Home Country Algorithm)

2. Infinite UKEK Retention feature is enabled. All keys are zeroized including the KEKs when Infinite UKEK Retention feature transitions from enable to disable and also from disable to enable.

All functions that are available in FIPS Approved mode are also available in non-FIPS Approved mode. 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 causes all CSP to be zeroized.

4. 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. Synchronous Serial Interface (SPI) - Plaintext Data, Ciphertext Data, Key Management Data (OTAR), Encrypted Cryptographic Keys (OTAR), Authentication Data
     b. Key Variable Loader (KVL) - Key Management Data, Encrypted Cryptographic Keys, Plaintext Cryptographic Keys
   - Data output interface
     a. Synchronous Serial Interface (SPI) - Plaintext Data, Ciphertext Data, Key Management Data (OTAR)
   - Control input interface
     a. Synchronous Serial Interface (SPI) - Input Commands
     b. Key Variable Loader (KVL) - Input Commands
   - Status output interface
     a. Synchronous Serial Interface (SPI) - Status Codes
     b. Key Variable Loader (KVL) - Status Codes
   - Power interface
     1. Switched - Powers all circuitry except Battery Backed Register
     2. Unswitched - Powers Battery Backed Register
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 in plaintext form.
   AND
   Secret cryptographic keys are entered 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 TEKs and KEKs to be invalidated and the password to be reset to the factory default.
8. The Astro Subscriber UCM provides the following services requiring a role:

- Transfer Key Variable
- Privileged APCO OTAR
- Change Active Keyset
- Change Password
- Encrypt Digital
- Decrypt Digital
- Zeroize Selected Keys
- Show Status

9. The Astro Subscriber UCM provides the following services not requiring a role:
   - Clear Bypass
   - Initiate Self-Tests
   - Validate Password
   - Zeroize all keys
   - Zeroize All Keys and Password
   - Non-Privileged APCO OTAR
   - Reset
   - Shutdown
   - 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 firmware 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:
    - Triple-DES
      - 8-bit CFB for symmetric encryption / decryption of keys and parameters stored in

the internal database
    - CBC for symmetric decryption of firmware upgrades
- AES-256
    - OFB for symmetric encryption / decryption of digital voice and data
    - CBC for MACing of Project 25 OTAR
    - ECB for symmetric decryption of Project 25 OTAR
    - GCM for symmetric encryption / decryption of Encrypted Integrated Data (EID)
- SHA-1
    - Password hashing for internal storage
- ANSI x9.31 RNG
    - IV and KPK generation

17. The Astro Subscriber UCM conforms to all FCC requirements for two-way radios.
18. The Astro Subscriber UCM performs the following self-tests:
    - Power-up and on-demand tests
        - Cryptographic algorithm test: Each algorithm (SHA-1, Triple-DES in the CFB8 and CBC modes, and AES in the OFB, CBC, GCM, 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 decrypted data matches the original plaintext, otherwise it fails.
        - RNG KAT test: the RNG is initialized with a known answer seed, DT counter and Triple-DES key. The RNG is run and the result compared to known answer data. The test passes if the generated data matches the known answer data, otherwise the test fails.
        - Firmware integrity test: The firmware integrity 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, and 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.
        - Clear Bypass test: The output from the module in Clear Bypass mode is redirected to a block of internal RAM. Data is processed using the Clear Bypass mode, and the contents of the RAM block are compared with the data sent. If the contents of the block match the data sent, the test passes, 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
        - Firmware load test: A MAC is generated over the code when it is built using

Triple-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 RNG 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. 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.

19. The Astro Subscriber UCM enters an error state if the Cryptographic Algorithm Test, LFSR Test, Continuous Random Number Generator Test, General Purpose RAM Test, RNG KAT, or the Clear Bypass 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 Firmware Integrity 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 firmware to be loaded.
21. The Astro Subscriber UCM enters an error state if the 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 multiple concurrent operators.
2. All cryptographic module services are suspended during key loading.
3. After a sufficient number (15) of consecutive unsuccessful user login attempts, the module will zeroize all keys from the Key Database.
4. Upon detection of a critically low voltage condition on the switched power supply, the cryptographic module shall erase all plaintext keys.
5. The module shall at no time output any security related data items (CSPs)

5. Crypto-Officer Guidance

5.1. Administration of the Astro Subscriber UCM in a secure manner

The Astro Subscriber 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 via the Download RSS service.

5.2. Assumptions regarding User Behavior

The Astro Subscriber 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. User Guidance

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

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

No Physical Ports or Logical Interfaces are directly available to the Astro Subscriber UCM User, only indirectly through the Subscriber Radio in which the Astro Subscriber 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 Astro Subscriber UCM.

7. 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 at any time. After fifteen consecutive invalid authentication attempts all keys are erased from the Key Database.

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

8. Access Control Policy

8.1. Astro Subscriber UCM Supported Roles

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

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

A user implicitly selects a role based on the service selected.

8.2. 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.
- Validate Password: Validate the current password used to identify and authenticate the User and CO roles. Available without a Role.
- 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.
- Clear Bypass: Allows the clear bypass of voice or data streams. Available without a Role.
- Initiate Self-Tests: Performs module self-tests comprised of cryptographic algorithms test, firmware integrity 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 firmware and Plaintext MAC Key. Firmware upgrades are authenticated using a Triple-DES-CBC MAC. Available without a Role.

Note: The loading of non-validated firmware will invalidate the modules validation.

8.3. Cirtical Security Parameters (CSPs)

Table 2: 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 for encryption of keys in OTAR
Plaintext MAC Key	Key used for authentication of firmware upgrade. Stored in non-volatile memory
Plaintext Password	User password entered during user authentication

8.4. CSP Access Types

Table 3: 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	Encrypts 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 4: 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 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 Digital	X					X	X	
6. Decrypt Digital	X					X	X	
7. Zeroize Selected Keys			X			X	X	
8. Show Status						X	X	
9. Clear Bypass						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

9. Mitigation of Other Attacks Policy

The Astro Subscriber UCM is not designed to mitigate any specific attacks related to power consumption, timing, fault induction, or TEMPEST attacks.

When tamper is enabled through the Download RSS service, the Astro Subscriber UCM uses a tamper-detect circuit that triggers a tamper whenever the UCM is physically separated from the radio, or the Astro Subscriber 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 power up 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