Security Policy: Astro Subscriber Motorola Advanced Crypto Engine (MACE)

Cryptographic module used in Motorola Solutions Astro XTL5000, XTS5000, APX2000, SRX2200, APX4000, APX6000, APX6000XE, APX6500, APX7000, APX7000XE, and APX7500 radios.

Version: R01.01.03

Date: June 12, 2012

Table of Contents

1. INTRODUCTION 3
1.1. SCOPE 3
1.2. DEFINITIONS 3
1.3. OVERVIEW 4
1.4. ASTRO SUBSCRIBER MACE IMPLEMENTATION 4
1.5. ASTRO SUBSCRIBER MACE HARDWARE / FIRMWARE VERSION NUMBERS 4
1.6. ASTRO SUBSCRIBER MACE CRYPTOGRAPHIC BOUNDARY 5
1.7. PORTS AND INTERFACES 5
2. FIPS 140-2 SECURITY LEVELS 7
3. FIPS 140-2 APPROVED OPERATIONAL MODES 8
3.1. CONFIGURATION SETTINGS FOR OPERATION AT FIPS 140-2 OVERALL SECURITY LEVEL 3 8
3.2. NON APPROVED MODE OF OPERATION 9
4. CRYPTO OFFICER AND USER GUIDANCE 10
4.1. ADMINISTRATION OF THE ASTRO SUBSCRIBER MACE IN A SECURE MANNER (CO) 10
4.2. ASSUMPTIONS REGARDING USER BEHAVIOR (CO) 10
4.3. APPROVED SECURITY FUNCTIONS, PORTS, AND INTERFACES AVAILABLE TO USERS 10
4.4. USER RESPONSIBILITIES NECESSARY FOR SECURE OPERATION 10
5. SECURITY RULES 11
5.1. FIPS 140-2 IMPOSED SECURITY RULES 11
5.2. MOTOROLA IMPOSED SECURITY RULES 13
6. IDENTIFICATION AND AUTHENTICATION POLICY 14
7. PHYSICAL SECURITY POLICY 15
8. ACCESS CONTROL POLICY 16
8.1. ASTRO SUBSCRIBER MACE SUPPORTED ROLES 16
8.2. ASTRO SUBSCRIBER MACE SERVICES 16
8.3. KEY MANAGEMENT 17
8.4. CSP ACCESS TYPES 19
9. MITIGATION OF OTHER ATTACKS POLICY 21

1. Introduction

1.1. Scope

This Security Policy specifies the security rules under which the Astro Subscriber Motorola Advanced Crypto Engine, herein identified as the Astro Subscriber MACE, must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and those imposed additionally by Motorola Solutions, Inc.. These rules, in total, define the interrelationship between the:

1. Module Operators,
2. Module Services, and
3. Critical Security Parameters (CSPs).

1.2. Definitions

ALGID		Algorithm Identifier
CBC		Cipher Block Chaining
CFB		Cipher Feedback
CKR		Common Key Reference
CO		Cryptographic Officer or Crypto-Officer
CODEC		Coder/Decode
CPS		Customer Programming Software
CPLD		Complex Programmable Logic Device
CSP		Critical Security Parameter
DES		Data Encryption Standard
ECB		Electronic Code Book
IV		Initialization Vector
KEK		Key Encryption Key
KID		Key Identifier
KLK		Key Loss Key
KMM		Key Management Message
KPK		Key Protection Key
KVL		Key Variable Loader
LFSR		Linear Feedback Shift Register
MAC		Message Authentication Code
MACE		Motorola Advanced Crypto Engine
OFB		Output Feedback
OMAP		Open Multimedia Applications Platform
OTAR		Over The Air Rekeying
RNG		Random Number Generator
TEK		Traffic Encryption Key

1.3. Overview

The Astro Subscriber MACE provides secure key management, Over-the-Air-Rekeying (OTAR), and voice and data encryption for the following Motorola Solutions mobile and portable two-way radios:

- APX2000 (portable)
- SRX2200 (portable)
- APX4000 (portable)
- APX6000 (portable)
- APX6000XE (portable)
- APX6500 (mobile)
- APX7000 (portable)
- APX7000XE (portable)
- APX7500 (mobile)

1.4. Astro Subscriber MACE Implementation

The Astro Subscriber MACE is implemented as a single-chip cryptographic module as defined by FIPS 140-2.

1.5. Astro Subscriber MACE Hardware / Firmware Version Numbers

FIPS Validated Cryptographic Module Hardware Kit Numbers	FIPS Validated Cryptographic Module Firmware Version Numbers
5185912Y01 or 5185912Y03	D01.03.08, or R07.11.08

Note: The Astro Subscriber MACE may operate in FIPS Approved mode with Module Firmware Version number R01.02.00, R01.02.01, R01.02.02, (previously validated under FIPS 140-2 Cert. #1535) D01.03.08, or R07.11.08.

The Astro Subscriber MACE supports the following FIPS Approved algorithms which may be installed separately from MACE firmware using the Program Update service. While the installation of AES may be done separately, for the purposes of this validation the module includes this firmware.

Approved Algorithm	Certificate Number	Part Number	Algorithm Firmware Version Numbers
AES-256 (ECB, CBC, OFB)	819	5185912 Family	R01.00.00
AES-256 (GCM)	1295	5185912 Family	R02.00.00

Note: Either AES Firmware Version R01.00.00 or both R01.00.00 and R02.00.00 must be loaded for the Astro Subscriber MACE to be in FIPS Approved mode.

1.6. Astro Subscriber MACE Cryptographic Boundary

The Astro Subscriber MACE Cryptographic Boundary is drawn around the MACE IC as shown below.

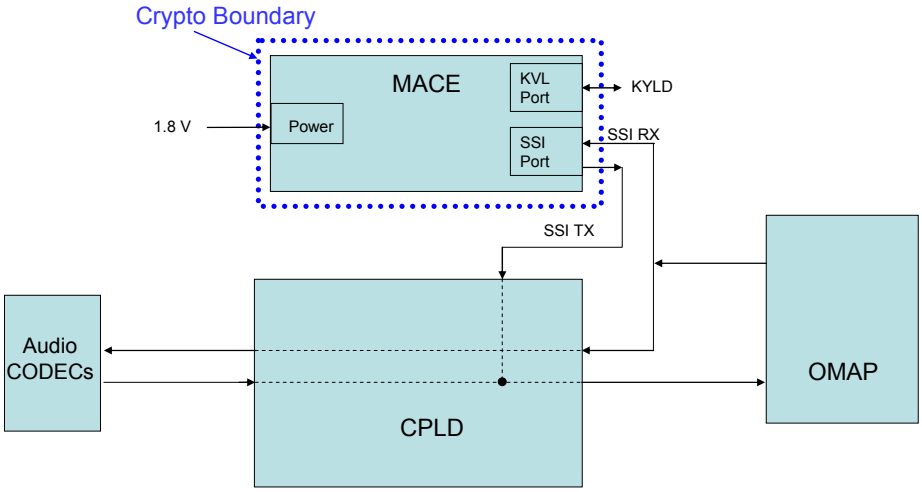

Figure 1: The Crypto Boundary is drawn around the MACE IC which has an SSI port (used for Data, Control, Status, and OTAR Key data), a KVL port (used for Key Data, Control, and Status), and Power Connections.

1.7. Ports and Interfaces

The Astro Subscriber MACE provides the following physical ports and logical interfaces:

Table 1: Ports and Interfaces

Physical Port	Qty	Logical interface definition	Description
Serial Synchronous Interface (SSI)	1	- Data Input - Data Output - Control Input - Status Output	The main physical port provided by the module. It provides access to the majority of the supported interfaces. This port is not used by firmware version R07.11.08.
Serial Peripheral Interface (SPI)	1	- Data Input - Data Output - Control Input - Status Output	The main physical port provided by the module. It provides access to the majority of the supported interfaces. This port is only used by firmware version R07.11.08.

Physical Port	Qty	Logical interface definition	Description
Key Variable Loader (KVL)	1	- Data Input - Control Input - Status Output	This interface provides the input and output to a Key Variable Loader (KVL).
Self-test Indicator Interface	1	- Status Output	This interface provides status output to indicate all power-up self-tests completed successfully.
Power	1	- Power Input	This interface powers all circuitry.

2. FIPS 140-2 Security Levels

The Astro Subscriber MACE can be configured to operate at FIPS 140-2 overall Security Level 3. The table below shows the FIPS 140-2 Level of security met for each of the eleven areas specified within the FIPS 140-2 security requirements.

Table 2: Astro Subscriber MACE Security Levels

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

3. FIPS 140-2 Approved Operational Modes

The Astro Subscriber MACE can be configured to operate in a FIPS Approved mode of operation and a Non-FIPS 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 at overall Security Level 3.

At any given time, the FIPS Status service can be used to determine whether the module is operating at overall Security Level 3 or in a non-FIPS Approved mode. Status is indicated by the FIPS STATUS RESPONSE message: Non-FIPS Compliance Mode or Level 3 FIPS Approved Mode.

3.1. Configuration Settings for operation at FIPS 140-2 overall Security Level 3

Documented below are the actions and configuration settings required to enable FIPS 140-2 overall Security Level 3.

1. Disable Motorola Data Communication Over The Air Rekeying (MDC OTAR). The Download Configuration Parameters service is used to configure this parameter in the module.
2. Disable Key Loss Key (KLK) generation. The Download Configuration Parameters service is used to configure this parameter in the module.
3. Disable Red Keyfill. When Red Keyfill is disabled, the module will not allow keys to be entered in plaintext form; all keys entered into the module must be encrypted. The Download Configuration Parameters service is used to configure this parameter in the module.
4. Only Approved and Allowed algorithms installed. The module supports the following Approved algorithms:
    - AES-256 (Cert. #819) –Used for encryption and decryption in the following Approved modes: OFB, ECB, CBC, and 8-bit CFB.
    - AES-256 GCM (Cert. #1295) – Used for symmetric encryption / decryption of Encrypted Integrated Data (EID)
    - SHA-256 (Cert. #817) – used for password hashing for internal password storage and digital signature verification during software/firmware integrity test and software/firmware load test
    - RSA-2048 (Cert. #396) – used for digital signature verification during software/firmware integrity test and software/firmware load test
    - ANSI x9.31 RNG (Cert. #471) – used for IV and KPK generation
5. The module supports the following Allowed algorithm:
    - AES MAC (Cert. #819) – Used to provide authentication within APCO OTAR. AES MAC as used within APCO OTAR has been vendor affirmed and is approved when used for Project 25 APCO OTAR.
6. Zeroize default security parameters: The Program Update service should be used to ensure all default CSP's are zeroized. The Program Update service is invoked in the factory at programming time and can be invoked in the field either by a FLASHPort Upgrade through CPS or a FLASHPort Upgrade with a KVL and PCMCIA card.
7. Infinite UKEK Retention is disabled. The Download Configuration Parameters service is used to configure this parameter in the module.

3.2. Non Approved Mode of Operation

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

1. MDC OTAR is enabled.
2. KLK generation is enabled.
3. Infinite UKEK Retention feature is enabled. All keys are zeroized including the KEKs when the Infinite UKEK Retention feature transitions from enable to disable and also from disable to enable.

The module maintains FIPS mode status and will provide this upon operator request.

4. Crypto Officer and User Guidance

4.1. Administration of the Astro Subscriber MACE in a secure manner (CO)

The Astro Subscriber MACE 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 Configuration Parameters service.

Note that all keys will be zeroized after the Program Update service has completed.

4.2. Assumptions regarding User Behavior (CO)

The Astro Subscriber MACE 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.

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

Astro Subscriber MACE services available to the Astro Subscriber MACE User are listed in section 8.2.

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

4.4. User Responsibilities necessary for Secure Operation

No special responsibilities are required of the User for secure operation of the Astro Subscriber MACE.

5. Security Rules

The Astro Subscriber MACE enforces the following security rules. These rules are separated into those imposed by FIPS 140-2 and those imposed by Motorola.

5.1. FIPS 140-2 Imposed Security Rules

1. The Astro Subscriber MACE inhibits all data output via the data output interface whenever an error state exists and during self-tests.
2. The Astro Subscriber MACE logically disconnects the output data path from the circuitry and processes when performing key generation, manual key entry, or key zeroization.
3. Authentication data (e.g. PINs) are entered in encrypted form. Authentication data is not output during entry.
4. At FIPS 140-2 overall Security Level 3, secret cryptographic keys are entered in encrypted form over a physically separate port.
5. The Astro Subscriber MACE enforces Identity-Based authentication.
6. The Astro Subscriber MACE supports a User role and a Crypto-Officer role. Authenticated operators are authorized to assume either supported role.
7. The Astro Subscriber MACE reauthenticates an operator when it is powered-up after being powered-off.
8. The Astro Subscriber MACE prevents brute-force attacks on its password by using a 10-digit password that reduces the probability of a successful random attempt to one in 10,000,000,000. It would require 100,000 attempts in one minute to lower the random attempt success rate to less than 1 in 100,000. A limit of 15 failed authentication attempts is imposed; 15 consecutive failed authentication attempts causes all TEKs and KEKs to be invalidated (key status is marked invalid) and the password to be reset to the factory default.
9. The Astro Subscriber MACE uses RSA-2048 to prevent brute-force attacks on the digital signature used to verify software/firmware integrity during a Program Update. As the Program Update service requires more than one minute to complete the random attempt success rate during a one minute period cannot be lowered to less than 1 in 100,000.
10. Authentication data is not output during entry.
11. The Astro Subscriber MACE provides the following services requiring a role:
    - Program Update
    - Transfer Key Variable
    - Privileged APCO OTAR
    - Change Active Keyset
    - Change Password
    - Encrypt Digital
    - Decrypt Digital
    - Zeroize Selected Keys
    - Key/Keyset Check
12. The Astro Subscriber MACE provides the following services not requiring a role:
    - FIPS Status
    - Initiate Self Tests

- Validate Password
- Zeroize All Keys
- Zeroize All Keys and Password
- Non-Privileged APCO OTAR
- Reset
- Shutdown
- Extract Error Log
- Clear Error Log
- Download Configuration Parameters

13. The Astro Subscriber MACE implements all software using a high-level language, except the limited use of low-level languages to enhance performance.
14. The Astro Subscriber MACE protects secret keys and private keys from unauthorized disclosure, modification, and substitution.
15. The Astro Subscriber MACE provides a means to ensure that a key entered into or stored within the Astro Subscriber MACE is associated with the correct entities to which the key is assigned. Each key in the Astro Subscriber MACE 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, and Keyset number – Identifiers indicating 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 CKR/Key ID/Algid, Key ID/Algid, Physical ID, or CKR/Keyset.
16. The Astro Subscriber MACE denies access to plaintext secret and private keys contained within the Astro Subscriber MACE.
17. The Astro Subscriber MACE provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the Astro Subscriber MACE.
18. The Astro Subscriber MACE provides the following non-FIPS Approved Random Number Generators to provide random numbers used as Initialization Vectors (IV) and the seeds for the Approved RNG.
    - Maximal length 64-bit LFSR.
    - Non-deterministic Hardware Random Number Generator
19. The Astro Subscriber MACE conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.
20. The Astro Subscriber MACE performs the following self-tests:
    - Power up and on-demand tests
      - Cryptographic algorithm test: Each algorithm (SHA-256, AES-256 in the OFB, CBC, ECB, 8-bit CFB, and GCM 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.
- Software/firmware Integrity test: A digital signature is generated over the code when it is built using SHA-256 and RSA-2048 and is stored with the code upon download into the module. When the module is powered up the digital signature is verified. If the digital signature matches 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
  - Software/firmware Load test: A digital signature is generated over the code when it is built using SHA-256 and RSA-2048. Upon download into the module, the digital signature is verified. If the digital signature matches the test passes, otherwise it fails.
  - Continuous Random Number Generator test: The continuous random number generator test is performed on all RNGs supported by the module. 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.

21. The Astro Subscriber MACE enters an error state if the Cryptographic Algorithm Test, Continuous Random Number Generator Test, or RNG KAT fails. This error state may be exited by powering the module off then on.
22. The Astro Subscriber MACE enters an error state if the Software/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 software to be loaded.
23. The Astro Subscriber MACE enters an error state if the Software/Firmware Load test fails. This error state may be exited by powering the module off then on which will start the download and validation process over.
24. The Astro Subscriber MACE outputs a status indicator via the Self-test Indicator interface to indicate all self-tests passed. A status indicator is not output via the Self-test Indicator interface whenever an error state is entered due to a failed self-test.
25. The Astro Subscriber MACE does not perform any cryptographic functions while in an error state.

5.2. Motorola Imposed Security Rules

1. The Astro Subscriber MACE 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. The module does not support the output of plaintext or encrypted keys.

6. Identification and Authentication Policy

The Astro Subscriber MACE supports two distinct operator roles (User and Crypto-Officer). The Astro Subscriber MACE uses a 10-digit password to authenticate the User and an RSA-2048 digital signature to authenticate the Crypto-Officer. The role of the operator is specified by selecting which physical port will be used to authenticate and access module services.

The authentication data for the Program Update service is the digital signature of the downloaded software.

Role	Authentication Type	Authentication Data Required
User	Identity-Based	User ID and 10-digit Password
Crypto-Officer	Identity-Based	RSA-2048 digital signature for Program Update service

7. Physical Security Policy

The Astro Subscriber MACE is a production grade, single-chip cryptographic module as defined by FIPS 140-2 and is designed to meet Level 3 physical security requirements.

The Astro Subscriber MACE is covered with a hard opaque epoxy coating that provides evidence of attempts to tamper with the module. The security provided from the hardness of the module's epoxy encapsulate is claimed at ambient temperature (20 to 25 degrees Celsius) only. No assurance of the epoxy hardness is claimed for this physical security mechanism outside of this range. The Astro Subscriber MACE does not contain any doors, removable covers, or ventilation holes or slits. No maintenance access interface is available. No special procedures are required to maintain physical security of the module while delivering to operators.

The figures below are applicable to Cryptographic Module hardware kit number 5185912Y01 and 5185912Y03. Cryptographic Module hardware kit number 5185912Y01 and 5185912Y03 have identical physical security characteristics.

Figure 1: MACE Chip (Top)

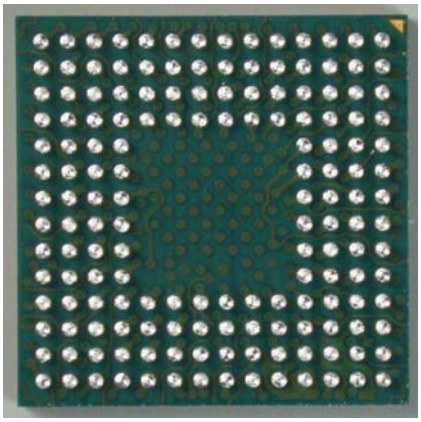

Figure 2: MACE Chip (Interfaces)

8. Access Control Policy

8.1. Astro Subscriber MACE Supported Roles

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

- User role and,
- Cryptographic Officer (Crypto-Officer or CO) role.

8.2. Astro Subscriber MACE Services

- Program Update: Update the module software. Software upgrades are authenticated using a digital signature. The Program Update Public Signature Key (a 2048 bit public RSA key) is used to validate the signature of the firmware image being loaded before it is allowed to be executed. All keys and CSPs are zeroized during a Program Update. To maintain validation, only validated software should be loaded. Loading non-validated software will invalidate the modules validation. Available to CO role.
- Transfer Key Variable: Transfer key variables to the MACE Key Database via a Key Variable Loader (KVL). If the Red Keyfill configuration parameter is enabled then keys will be transferred from the KVL in plaintext. If Red Keyfill is disabled, all keys transferred from the KVL will be encrypted. The Red Keyfill configuration parameter can be changed using the Download Configuration Parameters service. Available to User role. Any modification of the Red Keyfill parameter will zeroize all keys; therefore the operator shall reinitialize the module in accordance with the instructions provided in Section 3.1 of this document.
- Privileged APCO OTAR: Modify and query the Key Database via APCO OTAR Key Management Messages. This service has access to non-Approved algorithms if those algorithms are installed and selected. Only Approved algorithms should be installed to remain in an Approved mode of operation. Available to User role.
- Change Active Keyset: The active keyset is used to store a group of keys for current use while inactive keysets are used to store keys for future use. This service modifies the currently active keyset used for selecting keys for encryption / decryption services. Available to User role.
- Change Password: Modify the current password used to identify and authenticate the User role. Fifteen consecutive failed attempts causes the KPK to be zeroized, a new KPK to be generated, all TEKs and KEKs to be invalidated (key status is marked invalid), and the password to be reset to the factory default. Available to User role.
- Encrypt Digital: Encrypt digital voice or data. This service has access to non-Approved algorithms if those algorithms are installed and selected. Only Approved algorithms should be installed to remain in an Approved mode of operation. Available to User role.
- Decrypt Digital: Decrypt digital voice or data. This service has access to non-Approved algorithms if those algorithms are installed and selected. Only Approved algorithms should be installed to remain in an Approved mode of operation. Available to User role.
- Zeroize Selected Keys: Zeroize selected key variables from the Key Database by Physical ID (PID) or Common Key Reference (CKR). Available to User role.
- Key/Keyset Check: Obtain status information about a specific key/keyset. Available to User role.
- FIPS Status: Provides current FIPS status about whether the module is operating at

overall Security Level 3, or in a non-Approved mode of operation. Available without a role.

- Initiate Self Tests: Performs module self-tests comprised of cryptographic algorithm tests, software / 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.
- Validate Password: Validate the current password used to identify and authenticate the User role. Fifteen consecutive failed attempts causes the KPK to be zeroized, a new KPK to be generated, all TEKs and KEKs to be invalidated (key status is marked invalid), and the password to be reset to the factory default. Available without a role.
- Zeroize All keys: Zeroize all keys from the Key Database. Available without a role. (Module can be reinitialized using a Key Variable Loader.)
- Zeroize All Keys and Password: Zeroizes the KPK and all keys and CSPs in the key database and causes a new KPK to be generated. 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 a Key Variable Loader.)
- 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 or a transition from power off to power on state. Available without a role.
- Shutdown (Crypto Module): Prepares module for removal of power. Available without a role.
- Extract Error Log: Status Request. Provides detailed history of error events. Available without a role.
- Clear Error Log: Clears history of error events. Available without a role.
- Download Configuration Parameters: Download configuration parameters used to specify module behavior. Examples include enable/disable APCO OTAR, SingleKey, or MutliKey mode, etc. If the Tamper configuration parameter changed the module will zeroize the KPK and all keys and CSPs in the key database and will generate and store a new KPK. Available without a role.

8.3. Key Management

CSPs: The following table provides a list and description of all CSPs managed by the module.

Table 3: CSP Definition

CSP Identifier	Description
ANSI X9.31 Seed	A 64-bit seed value used within the ANSI X9.31 RNG. The seed is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The seed is not entered into or output from the module.
ANSI X9.31 Seed Key	Key used to seed the ANSI X9.31 RNG during initialization. The seed key is not stored but temporarily exists in volatile memory and is zeroized by power cycling the module. The seed key is not entered into or output from the module.

Black Keyloading Key (BKK)	A 256 bit AES key used for decrypting keys entered into the module via a KVL when the Red Keyfill configuration parameter is disabled. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The BKK is entered using the Program Update service and is not output from the module.
Image Decryption Key (IDK)	A 256-bit AES key used to decrypt downloaded images. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The IDK is entered using the Program Update service and is not output from the module.
Key Encryption Keys (KEKs)	256 bit AES key used for encryption of other keys in OTAR. Stored encrypted on KPK in non-volatile memory. Entered through the KVL or APCO OTAR. KEK's are not output from the module.
Key Protection Key (KPK)	256 bit AES key used to encrypt TEKs and KEKs stored in non-volatile memory. The KPK is not entered into or output from the module.
Password	The 10-digit password is entered encrypted on the PEK. After decryption the plaintext password is not stored but temporarily exists in volatile memory. The SHA-256 hash of the decrypted password is compared with the hash value stored in non-volatile memory during password validation. The password is not output from the module.
Password Encryption Key (PEK)	256 bit AES key used for decrypting password during password validation. Stored in plaintext in non-volatile memory and zeroized through the Program Update service. The PEK is entered using the Program Update service and is not output from the module.
Traffic Encryption Keys (TEKs)	256 bit AES key used for voice and data encryption. Stored encrypted on KPK in non-volatile memory. Entered through the KVL or APCO OTAR. TEK's are not output from the module.

Public Keys: The following table lists and describes all Public Keys managed by the module.

Table 4: Public Key Definition

Public Key Name	Description
Programmed Signature Key	2048 bit RSA key used to validate the signature of the firmware image being before it is allowed to be executed and is also used for authentication of the Crypto-Officer role. Loaded during manufacturing. The Programmed Signature Key is not output from the module.

8.4. CSP Access Types

Table 5: CSP Access Types

CSP Access Type	Description
c - Check CSP	Checks status and key identifier information of key.
d - Decrypt CSP	Decrypts TEK or KEK retrieved from non-volatile memory using the KPK. Decrypts TEKs or KEKs entered via the KVL when the Red Keyfill configuration parameter is disabled using the Black Keyloading Key. Decrypts entered password with PEK during password validation.
e - Encrypt CSP	Encrypts TEK or KEK with KPK prior to storage in non-volatile memory.
g - Generate CSP	Generates KPK, ANSI X9.31 seed, or ANSI X9.31 seed key.
i - Invalidate CSP	Marks encrypted TEKs or KEKs stored in non-volatile memory as invalid. TEKs or KEKs marked invalid can then be over-written when new TEKs or KEKs are stored.
s - Store CSP	Stores KPK in volatile and non-volatile memory. Stores encrypted TEKs or KEKs in non-volatile memory, over-writing any previously invalidated TEK or KEK in that location. Stores plaintext BKK, PEK, or IDK in non-volatile memory.
u - Use CSP	Uses CSP internally for encryption / decryption services.
z - Zeroize CSP	Zeroizes key.

Table 6: CSP versus CSP Access

	CSP									Role		
User Service	ANSI X9.31 seed	ANSI X9.31 seed key	BKK (Black Keyloading Key)	IDK (Image Decryption Key)	KEK (Key Encryption Key)	KPK (Key Protection Key)	Password	PEK (Password Encryption Key)	TEK (Traffic Encryption Key)	User Role	Crypto-Officer Role	No Role Required
1. Program Update			z, s	u, z, s	z	z		z, s	z		√	
2. Transfer Key Variable			u		i, e, z, s	u			i, e, z, s	√		
3. Privileged APCO OTAR			u		d, u, i, e, z, s	u			d, u, i, e, z, s	√		
4. Change Active Keyset										√		
5. Change Password					i	z, g, s	d, u, z	u	i	√		
6. Encrypt Digital									d, u	√		
7. Decrypt Digital									d, u	√		
8. Zeroize Selected Keys					i				i	√		
9. Key/Keyset Check					c				c	√		
10. FIPS Status					c				c	√	√	√
11. Initiate Self Tests										√	√	√
12. Validate Password					i	z, g, s	d, u, z	u	i	√	√	√
13. Zeroize All Keys					i				i	√	√	√
14. Zeroize All Keys and Password					i	z, g, s			i	√	√	√
15. Non-Privileged APCO OTAR (not for key entry)										√	√	√
16. Reset	g, u, z	g, u, z				g, s				√	√	√
17. Shutdown										√	√	√
18. Extract Error Log										√	√	√
19. Clear Error Log										√	√	√
20. Download Configuration Parameters					i	z, g, s			i	√	√	√

9. Mitigation of Other Attacks Policy

The Astro Subscriber MACE 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.