# Security Policy: ASTRO PDEG Motorola Advanced Crypto Engine (MACE)

Cryptographic module used in Motorola Solutions Astro PDEG

Version: R01.00.17

Date: July 12, 2018

## Table of Contents

# 1. Introduction

## 1.1. Scope

This Security Policy specifies the security rules under which the ASTRO PDEG Motorola Advanced Crypto Engine, herein identified as the ASTRO PDEG 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. These rules, in total, define the interrelationship between the:

- Module Operators,
- Module Services, and
- Critical Security Parameters (CSPs).

## 1.2. Definitions

| | |
|---|---|
| ALGID | Algorithm Identifier |
| CBC | Cipher Block Chaining |
| CFB | Cipher Feedback |
| CKR | Common Key Reference |
| CO | Crypto-Officer |
| CSP | Critical Security Parameter |
| DES | Data Encryption Standard |
| DRBG | Deterministic Random Bit Generator |
| ECB | Electronic Code Book |
| EI | Ethernet Interface |
| IC | Integrated Circuit |
| IPsec | Internet Protocol security |
| IV | Initialization Vector |
| KEK | Key Encryption Key |
| KPK | Key Protection Key |
| KVL | Key Variable Loader |
| LED | Light-emitting diode |
| MACE | Motorola Advanced Crypto Engine |
| NDRNG | Non-Deterministic Random Number Generator |
| PEK | Password Encryption Key |
| RAM | Random Access Memory |
| TEK | Traffic Encryption Key |

## 1.3. Overview

The ASTRO PDEG MACE provides secure key management and data encryption for the Astro System.

## 1.4. ASTRO PDEG MACE Implementation

The ASTRO PDEG MACE is implemented as a single-chip cryptographic module as defined

by FIPS 140-2.


**Figure 1: MACE Chip (Top)**

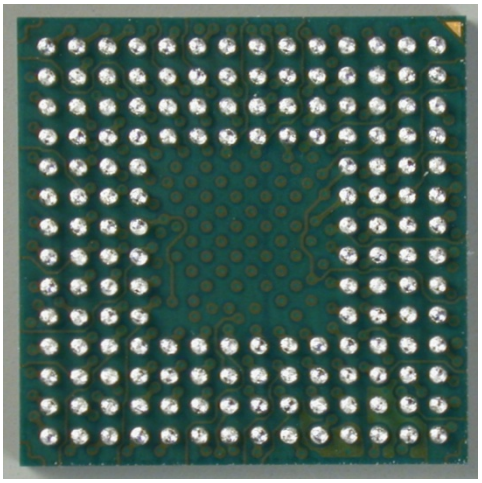

**Figure 2: MACE Chip (Interfaces)**

### 1.5. ASTRO PDEG MACE Hardware / Firmware Version Numbers

| FIPS Validated Cryptographic Module Hardware Kit Numbers | FIPS Validated Cryptographic Module Firmware Version Numbers |
|---|---|
| 5185912Y01, 5185912Y03, 5185912Y05, or 5185912T05 | R02.05.00, R02.05.01 |

### 1.6. ASTRO PDEG MACE Cryptographic Boundary

The Crypto Boundary is drawn around the ASTRO PDEG MACE IC which is responsible for all key storage and generation and performs all crypto processing for the ASTRO PDEG MACE.

The Cryptographic Boundary is shown in Figure 3 below.

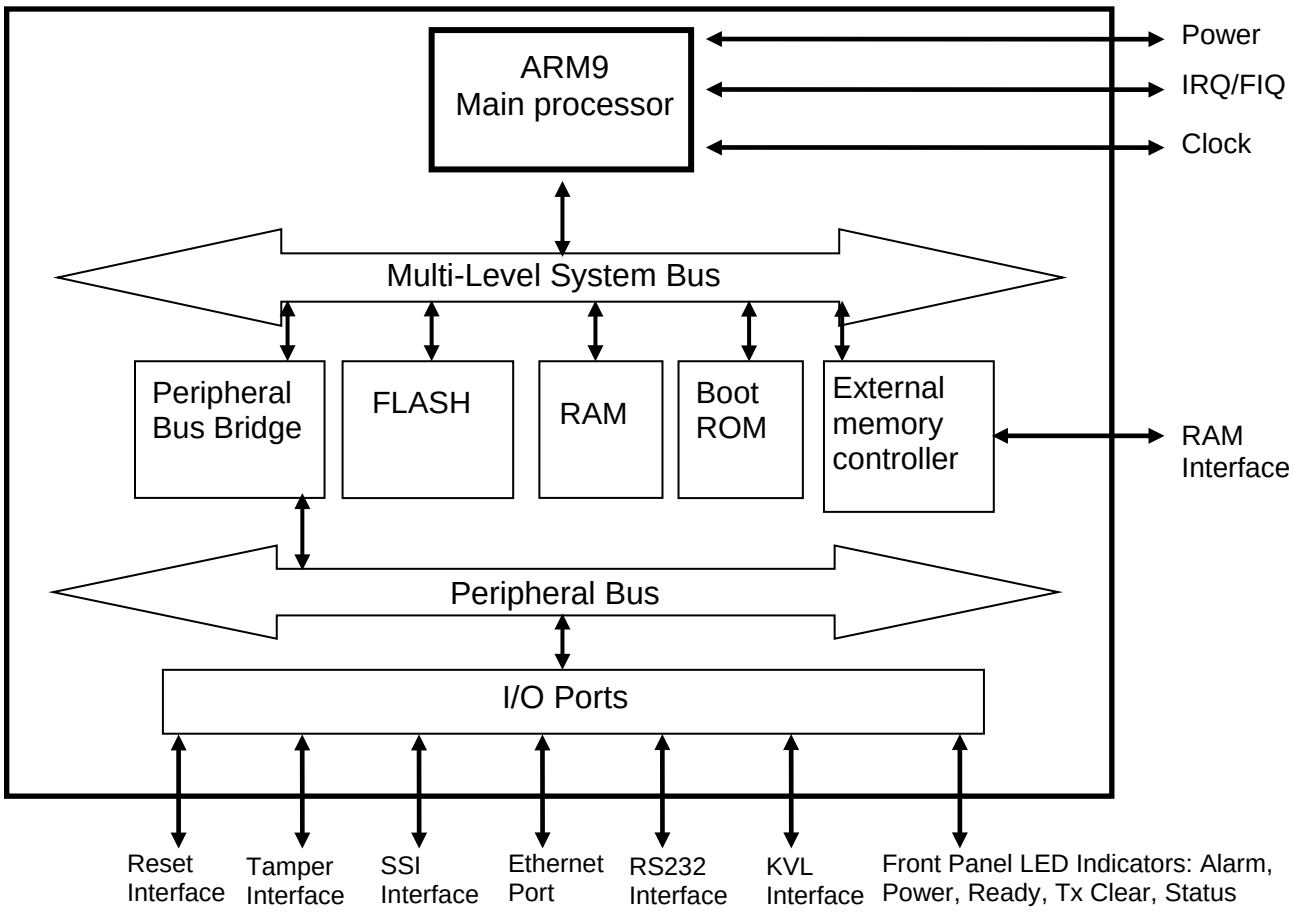


**Figure 3: ASTRO PDEG Block Diagram**

### 1.7. Ports and Interfaces

The ASTRO PDEG 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<br>• Data Output<br>• Control Input<br>• Status Output | Provides an interface to the unprotected network and entry of the User password in encrypted form.<br>This interface does not support output of CSP's. |
| Ethernet Port (EP) | 1 | • Data Input<br>• Data Output<br>• Control Input<br>• Status Output | This interface routes packets between subnets.<br>The IP stack of this interface will use the subnet information to determine how to route packets between physical network interfaces.<br>This interface does not support any other input / output of CSP's. |
| RS232 Interface | 1 | • Control Input<br>• Status Output<br>• Data Output | Provides an interface for factory programming and execution of RS232 shell commands.<br>This interface does not support output of CSP's. |
| Key Variable Loader (KVL) | 1 | • Data Input<br>• Data Output<br>• Control Input<br>• Status Output | Provides an interface to the Key Variable Loader. The Traffic Encryption Key (TEK) is entered in encrypted form over the KVL interface.<br>This interface does not support output of CSP's. |

| Physical Port | Qty | Logical interface definition | Description |
|---|---|---|---|
| RAM | 1 | • Data Input<br>• Data Output<br>• Control Input<br>• Status Output | This interface provides storage for non-security related stack information.<br>This interface does not support input / output of CSP's. |
| Power | 1 | • Power Input<br>• Internal battery-backed RAM | This interface powers all circuitry.<br>This interface does not support input / output of CSP's. |
| Tamper Interface | 1 | Control Input | The interface is used for zeroization of Traffic Encryption Keys (TEKs), KPK. |
| Reset Interface | 1 | Control Input | This interface forces a reset of the module. |
| Alarm LED output | 1 | Status Output | The Alarm LED output is used to drive the external Alarm LED red to indicate a fatal error has been detected. |
| Power LED output | 1 | Status Output | The Power LED output is used to drive the external Power LED green when power is supplied to the module. |
| Ready LED output | 1 | Status Output | The Ready LED output is used to drive the external Ready LED green when the module is ready to communicate with a KVL. |
| TX Clear LED output | 1 | Status Output | The TX Clear LED output is used to drive the external TX Clear LED orange when a "Bypass Rule" is programmed. |
| Status LED output | 1 | Status Output | The Status LED output is used to drive the external Status LED green to indicate a good battery, and a Traffic Encryption Key (TEK) has been loaded.<br>The Status LED output is used to drive the external Status LED yellow to indicate a good battery, but no Traffic Encryption Key (TEK) has been loaded.<br>The Status LED output is used to drive the external Status LED red to indicate a low or dead battery. |
| IRQ/FIQ | 2 | Control Input | External interrupts. |
| Clock | 1 | Control Input | Clock input |

## 2. FIPS 140-2 Security Levels

The ASTRO PDEG MACE is designed 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 PDEG 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 PDEG MACE can be configured to operate in a FIPS 140-2 Approved mode of operation and a non-FIPS Approved mode of operation. 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, and vice versa, causes all CSPs to be zeroized. The FIPS mode is indicated by issuing the "fips" command on the serial command shell. The result from this command will display whether or not the module is in FIPS approved operating mode. The Version Query service should be used to verify that the firmware version matches an approved version listed on NIST's website: https://csrc.nist.gov/projects/cryptographic-module-validation-program/module-validation-lists. This can be done via the serial interface.

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

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.

1. Disable Red Keyfill. The Configure Module service, issued from the ASTRO PDEG MACE command line, is used to configure this parameter in the module.
2. Only Approved and Allowed algorithms used. The module supports the following Approved algorithms:
   - AES-256 8-bit CFB (Cert. #819) – used for symmetric encryption/ decryption of keys and parameters stored in the internal database
   - AES-256 OFB (Cert #819) – for symmetric encryption/decryption of keys
   - AES-256 ECB (Cert. #819) – used for inner layer encryption
   - AES-256 CBC (Cert. #819) - during firmware upgrades and OTAR
   - AES-256 GCM (Cert. #1295) – for high-speed encryption/authentication in GCM mode.
   - AES-256 KW (Cert. #5358, key unwrapping; key establishment methodology provides 256 bits of encryption strength)
   - SHA-256 (Cert. #817) – used for digital signature verification during firmware integrity test and firmware load test. Used for password hashing for internal password storage.
   - SP800-90A DRBG (Cert. #505) - used for IV and key generation.
     The minimum number of bits of entropy generated by the module for key generation is at least 384 bits.
   - RSA-2048 (Cert. #396) – used for digital signature verification during firmware integrity test and firmware load test.
3. The module supports the following non-FIPS Approved algorithms, allowed in FIPS Approved mode:
   - AES MAC (AES Cert. #819, vendor affirmed; P25 AES OTAR);
   - Non-deterministic Hardware Random Number Generator (NDRNG) – used to provide seeds for the FIPS approved DRBG.

### 3.2. Non Approved Mode of Operation

A non-FIPS Approved mode of operation is transitioned to when the following condition is met:

1. Red Keyfill is enabled. This is disabled since it allows for keys to be sent in plaintext which is not allowed at FIPS Level 3.

All services available in the Approved mode are also available in the non-Approved mode of operation. The TEK and KEK keys can be entered in plaintext in the non-Approved mode.

# 4. Security Rules

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

### 4.1. FIPS 140-2 Imposed Security Rules

1. The ASTRO PDEG MACE inhibits all data output via the data output interface whenever an error state exists and during self-tests.
2. The ASTRO PDEG MACE logically disconnects the output data path from the circuitry and processes when performing key generation, or key zeroization.
3. Authentication data (e.g. passwords) are entered in encrypted form.
4. Secret cryptographic keys are entered in encrypted form over a physically separate port.
5. The ASTRO PDEG MACE enforces Identity-Based authentication.
6. The ASTRO PDEG MACE supports a User role, Cryptographic Officer role and a KVL role. Authenticated operators are authorized to assume either supported role. The module does not allow the operator to change roles.
7. The module does support bypass.
8. The ASTRO PDEG MACE uses RSA-2048 to prevent brute-force attacks on the digital signature used to verify 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.
9. Authentication data is displayed during entry.
10. After a sufficient number (10) of consecutive unsuccessful Crypto-Officer login attempts, the module will zeroize all CSP's stored in non-volatile storage.
11. The module does not support the output of plaintext or encrypted secret keys.
12. The ASTRO PDEG MACE implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
13. The ASTRO PDEG MACE protects secret keys from unauthorized disclosure, modification and substitution.
14. The ASTRO PDEG MACE provides a means to ensure that a key entered into or stored within the ASTRO PDEG MACE is associated with the correct entities to which the key is assigned. Each key in the ASTRO PDEG MACE is entered encrypted 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 fields to protect against data corruption. When used or deleted the keys are referenced by CKR / Key ID / Algid, Key ID / Algid, Physical ID, or CKR / Keyset.
15. The module denies access to plaintext secret keys contained within the ASTRO PDEG MACE.

16. The ASTRO PDEG MACE provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the module.
17. The ASTRO PDEG MACE conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.
18. The ASTRO PDEG MACE performs the following self-tests. Powering the module off then on or resetting the module using the Reset service will initiate the power up self-tests.
    - Power up and on-demand tests
      - Cryptographic algorithm test:
      - SHA-256 KAT
      - AES-256 KATs (all supported operational modes): 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.
      - DRBG (RNG) KAT test: the DRBG is initialized with a known, predetermined seed value. The DRBG 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. This KAT is an implementation of the procedure outlined in the "Deterministic Random Bit Generator Validation System (DRBGVS)" found at http://csrc.nist.gov/groups/STM/cavp/documents/drbg/DRBGVS.pdf
      - SP 800-90A Section 11.3 Health Tests
      - 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.
      - Critical Functions Test: External indicators test: Upon every power up, the MACE will assert and de-assert each signal connected to an external indicator, so that the User may verify that the indicators are functioning and controlled by the MACE.
      - Bypass test: Upon power up, the MACE will verify that the method for verifying bypass conditionally is working. A temporary configuration will be set up, data will be passed into the testing mechanism and the expected result will be verified. If the expected result is not reported, the test fails.
    - Conditional tests
      - 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 both of the RNG's supported by the module - the DRBG, as well as the NDRNG. 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.

- Bypass test: All data shall be passed into the bypass validation functionality which will determine if it meets the requirements for bypass (matching IP addresses, etc). If the data does not match a “”data bypass rule”, it is either thrown out or encrypted (if an “encrypt” rule is satisfied).

19. The ASTRO PDEG MACE enters an error state if the Cryptographic Algorithm Test, Continuous Random Number Generator Test, or DRBG KAT fails. This error state may be exited by powering the module off then on.
20. The ASTRO PDEG MACE enters an error state if the Firmware Integrity test or Firmware Load 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 PDEG MACE outputs an error indicator by turning the Alarm LED output red whenever an error state is entered due to a failed self-test. If all power up self-tests pass, the Alarm LED output will be clear.
22. The ASTRO PDEG MACE does not perform any cryptographic functions while in an error state.
23. The ASTRO PDEG turns on the “Tx Clear” LED when a security association rule allowing bypass data exists.
24. The ASTRO PDEG MACE does not support multiple concurrent operators.

# 5. Identification and Authentication Policy

The ASTRO PDEG MACE supports a User role, a Crypto-Officer role, and a KVL role. The identification, and authentication policy for each of these roles is detailed in the table below:

The Crypto-Officer and User roles are authenticated with passwords. The Crypto-Officer and User passwords are initialized to a default value during manufacturing and are sent in encrypted form to the module for authentication. After authenticating, the Crypto-Officer and User passwords may be changed at any time. The KVL role is authenticated using an AES key.

**Table 3: Roles and Authentication Mechanisms**

| Role | Authentication Type | Authentication Mechanism | Strength of Authentication |
|---|---|---|---|
| Crypto-Officer | Identity-Based | Identity: a 4-byte identifier is used to identify the identity and role. The ASTRO PDEG MACE supports a single identity.<br><br>Crypto-Officer Password: a password that is a minimum of 14-16 ASCII (printable) characters password is authenticated to gain access to all Crypto-Officer services. It should be noted that after authenticating, this password may be changed at any time. | Since the minimum password length is 14 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in 95 ^ 14 or 1 in 4,876,749,791,155,298,590,087,890,625.<br><br>The module limits the number of authentication attempts to in one minute to 10. The probability of a successful random attempt during a one-minute period is 10 in 95 ^ 14 or 1 in 2.050546e+27 |
| | | RSA signature verification: In the case of the Program Update service, the CO provides a digital signature to assume the CO role. (This is the only service in which an operator provides authentication data other than the Operator ID and password.) | The RSA key size is 2048 bits. The probability that a random attempt will succeed or a false acceptance will occur is approximately 1/2^112, which is less than 1/1,000,000.<br><br>The module will only accept a maximum of 1 authentication attempt per minute using the RSA digital signature technique. The probability of a successful random attempt during a one-minute period is approximately 1/2^112, which is less than 1/100,000. |

| Role | Authentication Type | Authentication Mechanism | Strength of Authentication |
|---|---|---|---|
| User | Identity-Based | Identity: a 4-byte identifier is used to identify the identity and role. The ASTRO PDEG MACE supports a single identity.<br><br>User Password: a 10 hexadecimal digit (5 bytes) long password is authenticated to gain access to all User services. It should be noted that after authenticating, this password may be changed at any time. | Since the minimum password length is 5 bytes long printable characters and there are 40 bits, the probability of a successful random attempt is 1 in 2 ^40 or 1 in 1,099,511,627,776.<br><br>The module limits the number of authentication attempts in one minute to 15. The probability of a successful random attempt during a one-minute period is 15 in 2 ^40 or 1 in 1.364242e+11. |
| KVL | Identity-Based | Identity: a 1-byte identifier is used to identify the identity and role. The ASTRO PDEG MACE supports a single identity.<br><br>BKK: a 256-bit AES key is authenticated to gain access to the services performed over the KVL interface. This CSP is used as the method of authentication in the following KVL-centric services:<br><br>• "Configure Module via KVL Interface"<br>• "Zeroize Keys via KVL Interface"<br>• "Store & Forward" | The probability of a successful random attempt is 1 in 2 ^ 256.<br><br>The maximum number of authentication attempts that can be performed over the KVL interface with the BKK in one minute is 745. Therefore the probability of a successful random attempt during a one-minute period is 745 in 2 ^ 256 or 1 in 1.55425e+74. |

# 6. Physical Security Policy

The ASTRO PDEG 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 PDEG MACE is covered with a hard opaque metallic coating that provides evidence of attempts to tamper with the module. Tampering with the module will cause it to enter a lock-up state in which no crypto services will be available. The ASTRO PDEG MACE does not contain any doors, removable covers, or ventilation holes or slits. No maintenance access interface is available.

Note: Motorola Solutions did not provide operating and storage temperature ranges to the test lab so module hardness testing was only performed at ambient temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.

The operator is required to periodically inspect the module for tamper evidence.

# 7. Access Control Policy

## 7.1. ASTRO PDEG Supported Roles

The module supports the following roles:

- User Role
- Crypto-Officer Role
- KVL Role

## 7.2. ASTRO PDEG MACE Services Available to the Crypto-Officer Role.

- Program Update: Update the module firmware via the KVL interface. Firmware upgrades are authenticated using a digital signature. The following points should be noted regarding the Program Update
    - The Program Update image is AES256 encrypted
    - The Program Update image is RSA-2048 signed
    - Keys/CSPs stored in non-volatile memory/storage are normally preserved during a Program Update. However all keys /CSPs are zeroized during a Program Update if one or more of the following occurs:
        - The key database format changes between the resident and upgrade software images
        - The key database version changes between the resident and upgrade software images
- Validate Crypto-Officer Password: Validate the role's current password via the RS232 interface. Successful authentication will allow entry/access to the RS232 shell command services. Fifteen consecutive failed validation attempts will cause the KPK to be zeroized, a new KPK to be generated, and the TEKs and KEKs to be invalidated (key status is marked invalid).
- Change Crypto-Officer Password: Modify the current password used to identify and authenticate this role via an RS232 shell command.
- Logout Crypto-Officer: Exits the RS232 shell command interface and logs out of the Crypto-Officer role.
- Configure Module:
    - Set configuration to toggle between FIPS 140-2 Level 3, or the non-FIPS compliant mode. Toggling this option causes the KPK to be zeroized, a new KPK to be generated, the TEKs and KEKs to be invalidated (key status is marked invalid), and the module to enter an error state that can only be cleared by power cycling the module.
    - Security Association Configuration: Provides the configuration for IPSec via an RS232 shell command. This service is used to configure bypass.
    - Set general configuration parameters used for the network functionality via an RS232 shell command.
- OTAR Configuration: Set configuration parameters used for communication with the KMF for OTAR
- Association Configuration Check: Provides feedback to current configuration including information about whether bypass is enabled.
- Extract Action Log: Status request via an RS232 shell command. Provides detailed history of error events.

- Version Query: Provides module firmware and hardware version numbers via an RS232 shell command.

### 7.3. ASTRO PDEG MACE Services Available to the User Role.

- Decrypt: Decrypt ciphertext data received (over the SSI) and send plaintext (over Ethernet) back.
- Encrypt: Encrypt plaintext data (received over the Ethernet) and send ciphertext (over SSI) back.
- Validate User Password: Validate the current User password used to identify and authenticate the User role via the SSI interface. Fifteen consecutive failed validation attempts will cause the KPK to be zeroized, a new KPK to be generated, and the TEKs and KEKs to be invalidated (key status is marked invalid).
- OTAR: Decrypt KEKs and TEKs.

### 7.4. ASTRO PDEG MACE Services Available to the KVL Role

- Configure Module via KVL interface: Perform configuration of the module (e.g. OTAR configuration) via the KVL interface.
- Store & Forward: Modify and query the KEKs and TEKs stored internally via the KVL interface.
- Transfer Key Variable: Transfer key variables (TEKs and KEKs) to the MACE key database via the KVL interface.
- Delete Key Variable: Zeroize KEKs and TEKs via the KVL interface.
- Key Check: Obtain status information about a specific TEK or KEK via the KVL interface.
- Version Query via KVL interface: Provides module firmware version numbers via the KVL UI.
- Algorithm List Query: Provides module firmware version numbers via the KVL UI.
- Key Query: Provides key metadata present on the device at the time of query via the KVL UI.

### 7.5. ASTRO PDEG MACE Services Available Without a Role.

- Perform Self-Tests: Performs module self-tests comprised of cryptographic algorithms test and firmware test. Initiated by module reset or transition from power off state to power on state.
- Reset Crypto Module: Toggle the Reset input or a transition from power off to power on state.
- Erase Crypto Module: Zeroizes the TEK, KEK, and KPK, via the Tamper interface.

## 7.6. Critical Security Parameters (CSPs) and Public Keys

**Table 4: CSP Definition**

| CSP Identifier | Description |
|---|---|
| SP800-90A DRBG seed | This is a 384-bit seed value used within the SP800-90A DRBG.<br>Entry - n/a<br>Output - n/a<br>Storage – temporarily in plaintext in volatile memory<br>Zeroization - on power off<br>Generation - Non-deterministic Hardware Random Number Generator |
| SP800-90A DRBG internal state (“V” and “Key”) | This is the internal state of the SP800-90A DRBG during initialization.<br>Entry - n/a<br>Output - n/a<br>Storage – temporarily in plaintext in volatile memory<br>Zeroization - on power off<br>Generation - internal to the SP800-90A DRBG |
| Key Protection Key (KPK) | This is a 256-bit AES key used to encrypt the TEK and KEKkeys stored in non volatile memory.<br>Entry - n/a<br>Output - n/a<br>Storage – stored in plaintext in non volatile memory<br>Zeroization - on Program Update, Erase Crypto Module service request<br>Generation - internally using the SP800-90A DRBG |
| Black Keyloading Key (BKK) | 256 bit AES Key used for decrypting the TEK and KEK keys entered into the module via a KVL.<br>Entry - on Program Update service request<br>Output - n/a<br>Storage – stored in plaintext in non-volatile memory<br>Zeroization - on Program Update service request<br>Generation - n/a |
| Image Decryption Key (IDK) | A 256-bit AES key used to decrypt downloaded images.<br>Entry - on Program Update service request<br>Output - n/a<br>Storage - in plaintext in non volatile memory<br>Zeroization - on Program Update service request<br>Generation - n/a |
| Traffic Encryption Keys (TEKs) | 256-bit AES GCM Keys used for enabling secure communication with target devices and for encryption and authentication of Key Management Messages in OTAR.<br>Entry – input encrypted with the BKK using AES Key Wrap over the Ethernet Interface<br>Output - n/a<br>Storage – stored encrypted with KPK (AES256-CFB8) in non volatile memory; stored in plaintext in RAM only as long as needed<br>Zeroization - on Delete Key Variable, Erase Crypto Module, and Program Update service requests<br>Generation: n/a |

| CSP Identifier | Description |
|---|---|
| Key Encryption Keys (KEKs) | 256 bit AES Keys used for encryption of keys in OTAR.<br>Entry – input encrypted with BKK using AES Key Wrap over either the KVL (wrapped the BKK) or Ethernet Interface (wrapped with a previously entered KEK stored in the module, entered via KVL)<br>Output - n/a<br>Storage – stored encrypted either in plaintext in RAM, or encrypted by the KPK (AES256-CFB8) in non volatile memory<br>Zeroization - on Delete Key Variable, Erase Crypto Module, and Program Update service requests<br>Generation: n/a |
| Password Encryption Key (PEK) | This is a 256-bit AES Key used for decrypting passwords during password validation.<br>Entry - on Program Update service request<br>Output - n/a<br>Storage - in plaintext in non volatile memory; encrypted by the KPK in non volatile memory<br>Zeroization - on Program Update, Erase Crypto Module service request<br>Generation - n/a |
| User Password | The User Password is a 10-digit hexadecimal value used to authenticate the User role.<br>Entry – entered encrypted with the PEK (AES256-CFB8)<br>Output - n/a<br>Storage – temporarily exists in volatile memory; a SHA-256 hash of the User Password is stored in non-volatile memory<br>Zeroization – on Program Update service request or power cycle<br>Generation - n/a |
| Crypto-Officer Password | The Crypto-Officer password is a 14-16 ASCII character password used to authenticate the Crypto-Officer role.<br>Entry - entered encrypted with the PEK (AES256-CFB8)<br>Output - n/a<br>Storage - temporarily exists in volatile memory; a SHA-256 hash of the plaintext password is stored in non volatile memory<br>Zeroization – on Program Update service requests or power cycle<br>Generation - n/a |

**Table 5: Public Key(s)**

| Public Keys | Description |
|---|---|
| Public Programmed Signature Key | 2048 bit RSA key used to validate the signature of the firmware image being loaded before it is allowed to be executed.<br>Entry – loaded during manufacturing and as part of the boot image during a Program Update service<br>Output - n/a<br>Storage - Stored temporarily in volatile memory and persistently in Flash<br>Generation - n/a |

### 7.7. CSP Access Types

**Table 6: CSP Access Types**

| CSP Access Type | Description |
|---|---|
| **C** – Check CSP | Checks status of the CSP. |
| **D** – Decrypt CSP | Decrypts entered KEKs and TEKs using the BKK during CSP entry over the KVL interface.<br>Decrypts KEKs and TEKs entered via OTAR using a KEK.<br>Decrypts entered passwords using the PEK during entry over the serial interface. |
| **E** – Encrypt CSP | Encrypts KEKs and TEKs prior to output over the Ethernet or KVL interface using another KEK. |
| **G** – Generate CSP | Generates KPK, SP800-90A seed, or SP800-90A internal state. |
| **I** – Invalidate CSP | Marks encrypted KEKs and TEKs stored in volatile memory as invalid. KEKs and TEKs marked invalid can then be over-written when new KEKs and/or TEKs are stored. |
| **S** – Store CSP | Stores KPK in non-volatile and volatile memory.<br>Stores encrypted KEKs and TEKs in non-volatile memory, over-writing any previously invalidated KEK or TEK in that location.<br>Stores plaintext BKK, PEK, or IDK in non-volatile memory.<br>Stores Hash of the User and Crypto-Officer password in non volatile memory (encrypted on PEK). |
| **U** – Use CSP | Uses CSP internally for encryption / decryption services. |
| **Z** – Zeroize CSP | Zeroizes a CSP. |

**Table 7: CSP versus CSP Access**

| Service | CSP | | | | | | | | | | Role | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | SP800-90A DRBG seed | SP800-90A DRBG internal state | PEK | TEKs | KEKs | KPK | BKK | IDK | User Password | Crypto-Officer Password | User Role | Crypto-Officer Role | KVL Role | No Role Required |
| Program Update | | | z,s | z | z | z | z, s | u, z, s | | | | √ | | |
| Validate Crypto-Officer Password | | | u | i | i | z, g, s | | | | d, u, z | | √ | | |
| Change Crypto-Officer Password | | | u | i | i | z, g, s | | | | d, u, z,s | | √ | | |
| Logout Crypto-Officer Role | | | | | | | | | | | | √ | | |
| Configure Module | | | | | | z | | | | | | √ | | |
| Extract Action Log | | | | | | | | | | | | √ | | |
| Version Query (serial console) | | | | | | | | | | | | √ | | |
| Association Configuration Check | | | | | | | | | | | | √ | | |
| OTAR Configuration | | | | | | | | | | | | √ | | |
| Encrypt | | | d,u | | u | | | | | | √ | | | |
| Decrypt | | | d,u | | u | | | | | | √ | | | |
| Validate User Password | | | u | i | i | z, g, s | | | d, u, z | | √ | | | |
| OTAR | | | | d, u, i, e, z, s | d, u, i, e, z, s | u | | u | | | √ | | | |
| Configure Module via KVL Interface | | | | | | | u | | | | | | √ | |
| Store & Forward | | | | d, u, i, e, z, s | d, u, i, e, z, s | u | u | | | | | | √ | |
| Transfer Key Variable | | | | d, i, e, z, s | d, i, e, z, s | u | u | | | | | | √ | |
| Delete Key Variable | | | | i | i | z | u | | | | | | √ | |
| Key Check | | | | c | c | | u | | | | | | √ | |
| Version Query via KVL interface | | | | | | | u | | | | | | √ | |
| Algorithm List Query | | | | | | | u | | | | | | √ | |
| Key Query | | | | d | d | u | u | | | | | | √ | |
| Perform Self-Tests | g | g | | | | | | | | | | | | √ |
| Reset Crypto Module | | | | i | i | z, g, s | | | | | | | | √ |
| Erase Crypto Module | g, u, z | g, u, z | z | z | | g, s, z | | | | | | | | √ |

## 8. Mitigation of Other Attacks Policy

The ASTRO PDEG 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.