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

Cryptographic module used in Motorola's Astro PDEG

Version: R01.00.09

Date: May 6, 2011

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. 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
ECB	Electronic Code Book
EI	Ethernet Interface
IPsec	Internet Protocol security
IV	Initialization Vector
KEK	Key Encryption Key
KPK	Key Protection Key
KVL	Key Variable Loader
LED	Light-emitting diode
LFSR	Linear Feedback Shift Register
MACE	Motorola Advanced Crypto Engine
PEK	Password Encryption Key
RAM	Random Access Memory
RNG	Random Number Generator
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.

1.5. ASTRO PDEG MACE Hardware / Firmware Version Numbers

FIPS Validated Cryptographic Module Hardware Kit Numbers	FIPS Validated Cryptographic Module Firmware Version Numbers
5185912Y01	R02.03.01, R02.03.02

1.6. ASTRO PDEG MACE Cryptographic Boundary

The ASTRO PDEG MACE Cryptographic Boundary is drawn around the MACE IC as shown below.

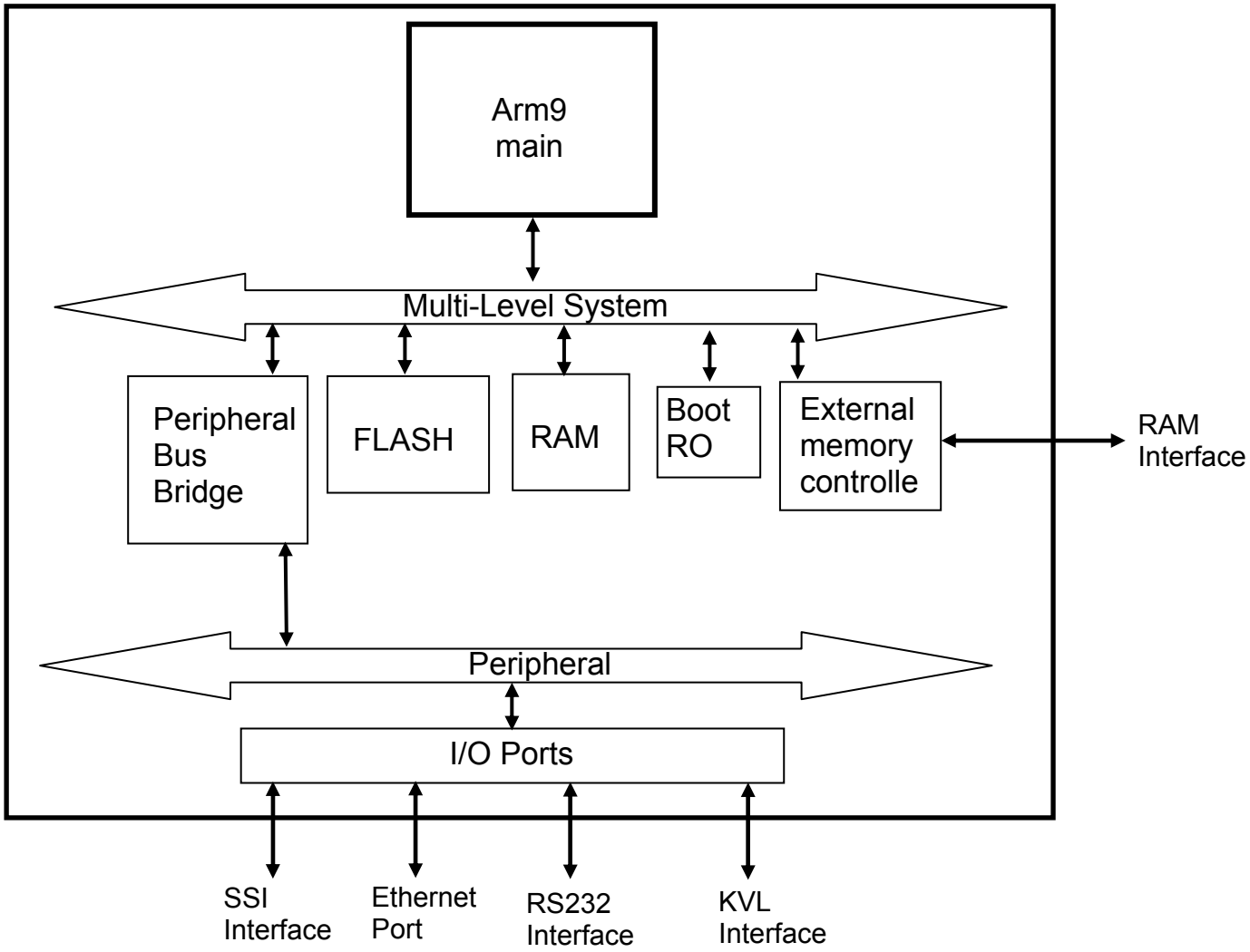

Figure 1: ASTRO PDEG MACE Block Diagram

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.

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
RS232 Interface	1	• Control Input • Status Output • Data Output	Provides an interface for factory programming and execution of RS232 shell commands. This interface does not support output of CSP's.
Serial Synchronous Interface (SSI)	1	• Data Input • Data Output • Control Input • Status Output	Provides an interface to the unprotected network and entry of the User password in encrypted form. This interface does not support output of CSP's.
Ethernet Port (EP)	1	• Data Input • Data Output • Control Input • Status Output	This interface routes packets between subnets. The IP stack of this interface will use the subnet information to determine how to route packets between physical network interfaces. This interface does not support any other input / output of CSP's.
Key Variable Loader (KVL)	1	• Data Input • Data Output • Control Input • Status Output	Provides an interface to the Key Variable Loader. The Traffic Encryption Key (TEK) is entered in encrypted form over the KVL interface. This interface does not support output of CSP's.
RAM	1	• Data Input • Data Output • Control Input • Status Output	This interface provides storage for non-security related stack information. This interface does not support input / output of CSP's.
Power	1	• Power Input • Internal battery-backed RAM	This interface powers all circuitry. This interface does not support input / output of CSP's.

Physical Port	Qty	Logical interface definition	Description
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. 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. 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 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 PDEG Crypto Module is designed to operate in a FIPS 140-2 Approved mode of operation at overall Security Level 3 or in a non-FIPS Approved mode of operation. A serial interface command is used to change the mode and to retrieve the current mode. If a change to the FIPS mode occurs, all TEKs and KEKs are erased.

fips [Enable/Disable]

Disabled: Non-FIPS Mode - Encrypted and Clear keyfill is allowed.
Enabled: FIPS 140-2 Level 3 Keyfill - Only Encrypted keyfill is allowed

If fips mode is not enabled, "fips" command with no parameter displays:

CURRENT STATE:

Encrypted only Keyfill is Disabled
FIPS mode is Not FIPS approved

If fips mode is enabled, "fips" command with no parameter displays:

CURRENT STATE:

Encrypted only Keyfill is Enabled
FIPS mode is Level 3

The RS232 Interface Version Query command will be used to retrieve the current FW and HW version of PDEG Crypto Module

The module supports the following Approved algorithms:
• AES-256 – for symmetric encryption / decryption of keys and parameters stored in the internal database used in the following approved modes: CBC, and 8-bit CFB.
• AES-256 GCM – for high-speed encryption and authentication in the GCM mode.
• SHA-256 – used for password hashing for internal password storage and digital signature verification during firmware integrity test and firmware load test
• RSA-2048 (Cert. #396) – used for digital signature verification during firmware integrity test and firmware load test
• ANSI x9.31 RNG (Cert. #471) – used for IV and KPK generation

The module supports the following non-FIPS Approved algorithms:
• AES MAC (vendor affirmed; P25 AES OTAR); AES (key wrapping; key agreement methodology provides 256 bits of encryption strength)
• Maximal length 64-bit LFSR
• Non-deterministic Hardware Random Number Generator – used to provide random numbers used as Initialization Vectors (IV) and the seeds for the Approved RNG

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.

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, manual key entry, or key zeroization.
3. Authentication data (e.g. passwords) are entered in encrypted form. Authentication data is not output during entry.
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 and a Cryptographic Officer role. Authenticated operators are authorized to assume either supported role. The module does not allow the operator to change roles.
7. The ASTRO PDEG MACE re-authenticates an operator when it is powered-up after being powered-off.
8. The PDEG Crypto Module prevents brute-force attacks on its Crypto-Officer password by using a password that is a minimum of 14 and a maximum of 16 ASCII printable characters in length. The probability of a successful random attempt is at least 1 in 4,876,749,791,155,298,590,087,890,625. It would require at least 48,767,497,911,552,985,900,878 attempts in one minute to lower the random attempt success rate to less than 1 in 100,000. A limit of 10 failed authentication attempts is imposed: 10 consecutive failed authentication attempts will cause the KPK to be zeroized, a new KPK to be generated, and all PSK's to be invalidated (key status is marked invalid).The MACE is not fast enough to perform this many attempts in one minute, even if an attempt took 1 clock cycle (which is doesn't), the mace running at 120Mhz would only be able to process 7,200,000,000 in one minute.

   There are 95 ASCII printable chars
   Password is 14 chars min

   95 ^ 14 = 4,876,749,791,155,298,590,087,890,625

   To get the random success rate to be less than 100,000 per minute, more than 48,767,497,911,552,985,900,878 would need to be entered per minute

   4,876,749,791,155,298,590,087,890,625/100,000 = 48,767,497,911,552,985,900,878.90625

   The mace processor (~120MHz) is not fast enough to process this many entries per minute even if every attempt took just one cycle. Only 7,200,000,000 could be attempted per minute.

120,000,000 * 60 = 7,200,000,000

After 10 incorrect entries, the keys are erased.

9. The PDEG Crypto Module prevents brute-force attacks on its User password by using a password that is 10 hexadecimal digits long. The probability of a successful random attempt is 1 in 1,099,511,627,776 . It would require 10,995,116 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 will cause the KPK to be zeroized, a new KPK to be generated, and all PSK's to be invalidated (key status is marked invalid). The MACE is not fast enough to perform this many attempts in one minute, even if an attempt took 1 clock cycle (which is doesn't), the mace running at 120Mhz would only be able to process 7,200,000,000 in one minute.

   10 hex digits = 40 bits

   2 ^ 40 = 1,099,511,627,776

   To get the random success rate to be less than 100,000 per minute, more than 10,995,116 would need to be entered per minute

   1,099,511,627,776 /100,000 = 10,995,116.27776

   The mace processor (~120MHz) is not fast enough to process this many entries per minute even is every attempt took just one cycle. Only 7,200,000,000 could be attempted per minute

   After 15 incorrect entries, the keys are erased.

10. Authentication data is not output during entry.
11. 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.
12. Authentication data is not output during entry.
13. The ASTRO PDEG MACE implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
14. The ASTRO PDEG MACE protects secret keys from unauthorized disclosure, modification and substitution.
15. 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.

16. The ASTRO PDEG MACE denies access to plaintext secret keys contained within the ASTRO PDEG MACE.
17. The ASTRO PDEG MACE provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the module.
18. The ASTRO PDEG MACE conforms to FCC 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B requirements.
19. 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: Each algorithm (SHA-256, and AES-256 in GCM, CBC, and 8-bit CFB-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: 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.
      - 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 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.
- 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).

20. The ASTRO PDEG 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.
21. 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.
22. 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.
23. The ASTRO PDEG MACE does not perform any cryptographic functions while in an error state.
24. The ASTRO PDEG turns on the “Tx Clear” LED when a rule allowing bypass data exists.

4.2. Motorola Imposed Security Rules

1. The ASTRO PDEG MACE does not support multiple concurrent operators.
2. After a sufficient number (10) of consecutive unsuccessful Crypto-Officer login attempts, the module will zeroize all keys from the Key Database.
3. The module does not support the output of plaintext or encrypted secret keys.

5. Identification and Authentication Policy

The ASTRO PDEG MACE supports a User role and a Crypto-Officer role.

The Crypto-Officer role is authenticated by a digital signature during the Program Update service and a password which is a minimum of 14 and maximum of 16 ASCII printable characters in length for the remaining Crypto-Officer services. After authenticating, the CO password may be changed at any time. After ten consecutive invalid authentication attempts the KPK is zeroized, a new KPK is generated, all TEKs and KEKs are invalidated (key status is marked invalid), the password is reset to the factory default, and the module enters an error state that can only be cleared by power cycling the module.

A 10-digit hexadecimal password is used to authenticate the User role. The User password cannot be changed. After fifteen consecutive invalid authentication attempts the KPK is zeroized, a new KPK is generated, and all TEKs and KEKs are invalidated (key status is marked invalid).

Both Crypto-Officer and User ID's and passwords are initialized to a default value during manufacturing and are sent in encrypted form to the MACE for authentication.

Role	Authentication Type	Identification	Authentication Data Required
Crypto-Officer	Identity-Based	Crypto-Officer ID	Digital signature for Program Update service 14-16 character ASCII password
User	Identity-Based	User ID	10-digit hexadecimal password

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.

7. Access Control Policy

7.1. ASTRO PDEG MACE Supported Roles

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

- User Role and,
- Crypto-Officer (CO) Role.

The ASTRO_PDEG MACE supports only one User ID and one Crypto-Officer ID.

7.2. ASTRO PDEG MACE Services Available to the User Role.

- Transfer Key Variable: Transfer key variables (TEKs and KEKs) to the MACE key database via the KVL interface.
- Key Check: Obtain status information about a specific TEK or KEK via the KVL interface.
- 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).
- Zeroize Keys Via KVL: Zeroize TEKs and KEKs from the key database via the KVL interface.
- Encrypt: Encrypt plaintext data received over the Ethernet port and send ciphertext over SSI.
- Decrypt: Decrypt ciphertext data received over the SSI and send plaintext over Ethernet port.
- OTAR: Decrypt KEKs and TEKs.

7.3. 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. Loading non-FIPS Approved firmware will invalidate the modules validation. All keys and CSPs are zeroized during a Program Update.
- Validate Crypto-Officer Password: Validate the current Crypto-Officer password used to identify and authenticate the Crypto-Officer role via the RS232 interface. Successful authentication will allow entrance to the RS232 shell command interface and access to the RS232 shell command services. Ten consecutive failed attempts causes the KPK to be zeroized, a new KPK to be generated, the TEKs and KEKs to be invalidated (key status is marked invalid), the password to be reset to the factory default, and the module to enter an error state that can only be cleared by power cycling the module.
- Change Crypto-Officer Password: Modify the current password used to identify and authenticate the CO Role via an RS232 shell command.
- Configure ASTRO PDEG: Set configuration parameters used for the Network functionality via an RS232 shell command.
- Extract Error Log: Status request via an RS232 shell command. Provides detailed history of error events.
- Security Association config: Provides the configuration for IPSec via an RS232 shell

command. This service is used to configure bypass.

- Version Query: Provides module firmware and hardware version numbers via an RS232 shell command.
- Red Keyfill (Fips)l: Shell command that is used to enable/disable the ability to perform unencrypted keyload operations. This command has a side affect of reporting out of the rs232 shell whether operating in FIPS 140-2 level 3 mode or not. 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.
- OTAR Configuration: Set configuration parameters used for communication with the KMF for OTAR
- RS232 Shell Help: Shell command to get help on the format of other RS232 shell commands.
- Exit RS232 Shell: Exits the RS232 shell command interface and logs out of the Crypto-Officer role.
- Association Configuration Check: Provides feedback to current configuration including information about whether bypass is enabled.

7.4. ASTRO_PDEG MACE Services Available Without a Role.

- Reset Crypto Module: Toggle the Reset input or a transition from power off to power on state.
- Initiate 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.
- Zeroize All Keys: Zeroizes the TEK, KEK, and KPK, via the Tamper interface.

7.5. Critical Security Parameters (CSPs) and Public Keys

Table 3: CSP Definition

CSP's	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	This is a 128 bit TDES 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)	256 bit AES Key used for decrypting keys entered into the module via a KVL. 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.
Traffic Encryption Keys (TEKs)	256 bit AES-GCM Keys The TEKs are entered in encrypted form via the KVL. Stored in plaintext in RAM and encrypted by the KPK in flash. The TEK is entered wrapped with the BKK and is not output from the module.
Key Encryption Keys (KEKs)	256 bit AES Keys used for encryption of keys in OTAR. KEKs are entered in encrypted form via the KVL and via OTAR. KEKs entered via the KVL are wrapped with the BKK; KEKs received via OTAR are encrypted on another KEK. Stored in plaintext in RAM and encrypted by the KPK in flash. KEKs are not output from the module.
Key Protection Key (KPK)	256 bit AES key used to encrypt TEKs and KEKs. Generated internally by the ANSI X9.31 RNG. Stored in battery-backed RAM. The KPK is not entered into or output from the module.
Password Encryption Key (PEK)	256 bit AES Key used for decrypting passwords during password validation. Loaded via the Program Update service. 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.
User Password	The User password (10 hex digits in length) 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 User Password is entered encrypted with the PEK and is not output from the module.
Crypto-Officer Password	The CO password (14 to 16 ascii characters) 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 User Password is entered encrypted with the PEK and is not output from the module.
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. Stored in volatile memory. Loaded during manufacturing and as part of the boot image during a Program Update service. The Public Programmed Signature Key is loaded during manufacturing and is not output from the module.

7.6. CSP Access Types

Table 5: CSP Access Types

C – Check CSP	Checks status and key identifier information of key.
D – Decrypt CSP	Decrypts KEKs and TEKs retrieved from volatile memory using the KPK. Decrypts KEKs and TEKs entered via the KVL using the Black Keyloading Key. Decrypts KEKs and TEKs entered via OTAR using a KEK. Decrypts entered password with PEK during password validation.
E – Encrypt CSP	Encrypts KEKs and TEKs with KPK prior to storage in volatile memory.
G – Generate CSP	Generates KPK, ANSI X9.31 seed, or ANSI X9.31 seed key
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 volatile and volatile memory. Stores encrypted KEKs and TEKs in non-volatile memory, over-writing any previously invalidated KEK or TEK 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

Service	CSPs										Role		
	ANSI X9.31 seed	ANSI X9.31 seed key	TEK (Traffic Encryption Key)	KEK (Key Encryption Keys)	KPK (Key Protection Key)	PEK (Password Encryption Key	BKK (Black Keyloading Key)	IDK (Image Decryption Key)	User Password	Crypto-Officer Password	User Role	Crypto-Officer Role	No Role Required
Program Update			z	z	z	z,s	z, s	u, z, s				√	
Validate Crypto-Officer Password			i	i	z, g, s	u				d, u, z		√	
Change Crypto-Officer Password			i	i	z, g, s	u				d, u, z		√	
Configure ASTRO_PDEG												√	
OTAR Configuration												√	
Extract Error Log												√	
Association Configuration												√	
Version Query												√	
RS232 Shell Help												√	
Exit RS232 Shell												√	
Transfer Key Variable			d, i, e, z, s	d, i, e, z, s	u		u				√		
Key Check			c	c							√		
Validate User Password			i	i	z, g, s	u			d, u, z		√		
Zeroize Keys Via KVL			i	i							√		
Encrypt			d,u		u						√		
Decrypt			d,u		u						√		

OTAR			d, u, i, e, z, s	d, u, i, e, z, s	u		u				√		
Association Configuration Check												√	
Reset Crypto Module	g, u, z	g, u, z			g, s						√	√	√
Perform Self-Tests											√	√	√
Zeroize All Keys			i	i	z, g, s						√	√	√

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.