Astro PDEG Motorola Advanced Crypto Engine (MACE)

Non-Proprietary FIPS 140-3 Security Policy

Document Version: 1.2

Date: November 01, 2024

Table of Contents

List of Tables

List of Figures

1 General

This document defines the Security Policy for the Astro Packet Data Encryption Gateway (PDEG) Motorola Advanced Crypto Engine (MACE), hereafter denoted the ASTRO PDEG MACE or the Module. The ASTRO PDEG MACE is implemented as a single-chip cryptographic module to meet FIPS 140-3 level 3 physical security requirements as defined by FIPS 140-3. The ASTRO PDEG MACE provides secure key management, Over-the-Ethernet-Keying (OTEK), and data encryption for the Motorola Solutions PDEG Encryption Unit.

The FIPS 140-3 security levels for the ASTRO PDEG MACE are as follows:

Table 1 – Security Levels

ISO/IEC 24759 Section 6 [Number below]	FIPS 140-3 Section Title	Security Level
1	General	3
2	Cryptographic Module Specification	3
3	Cryptographic Module Interfaces	3
4	Roles, Services and, Authentication	3
5	Software/Firmware Security	3
6	Operational Environment	N/A
7	Physical Security	3
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	3
10	Self-Tests	3
11	Life-Cycle Assurance	3
12	Mitigation of Other Attacks	N/A
Overall		**3**

2 Cryptographic Module Specification

The ASTRO PDEG MACE cryptographic module is a single chip hardware cryptographic module. The ASTRO PDEG MACE is used in the Motorola Solutions PDEG Encryption Unit. The ASTRO PDEG MACE cryptographic module is intended for use by US Federal agencies or other markets that require FIPS 140-3 validated overall security level 3.

2.1 Operational Environment

The ASTRO PDEG MACE cryptographic module is tested on the following operational environment.

Table 2 – Cryptographic Module Tested Configuration

Model	HW P/N, Version	Base Firmware version	Distinguishing Features
Astro PDEG Motorola Advanced Crypto Engine (MACE) Identifier: PDEG_RED_MODULE_ID 0x32	5185912Y03, 5185912Y05, 5185912T05	R02.07.04	Single chip embodiment

2.2 Cryptographic Boundary

The physical form of the ASTRO PDEG MACE cryptographic module is depicted in Figure 1 and Figure 2. The ASTRO PDEG MACE is a single chip embodiment. The cryptographic boundary of the ASTRO PDEG MACE IC as shown in Figure 3.

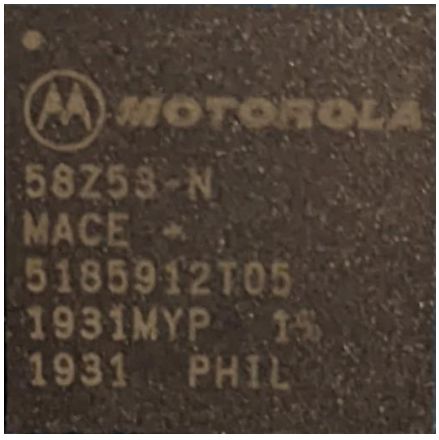

Figure 1: MACE Chip (Top)

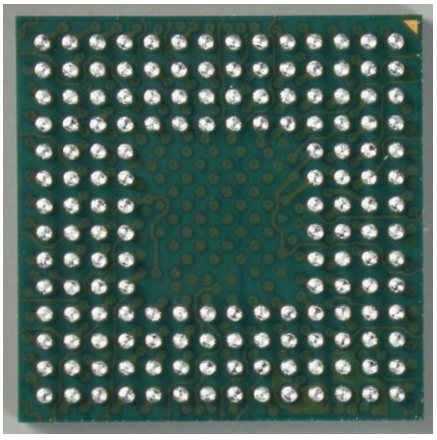

Figure 2: MACE Chip (Interfaces)

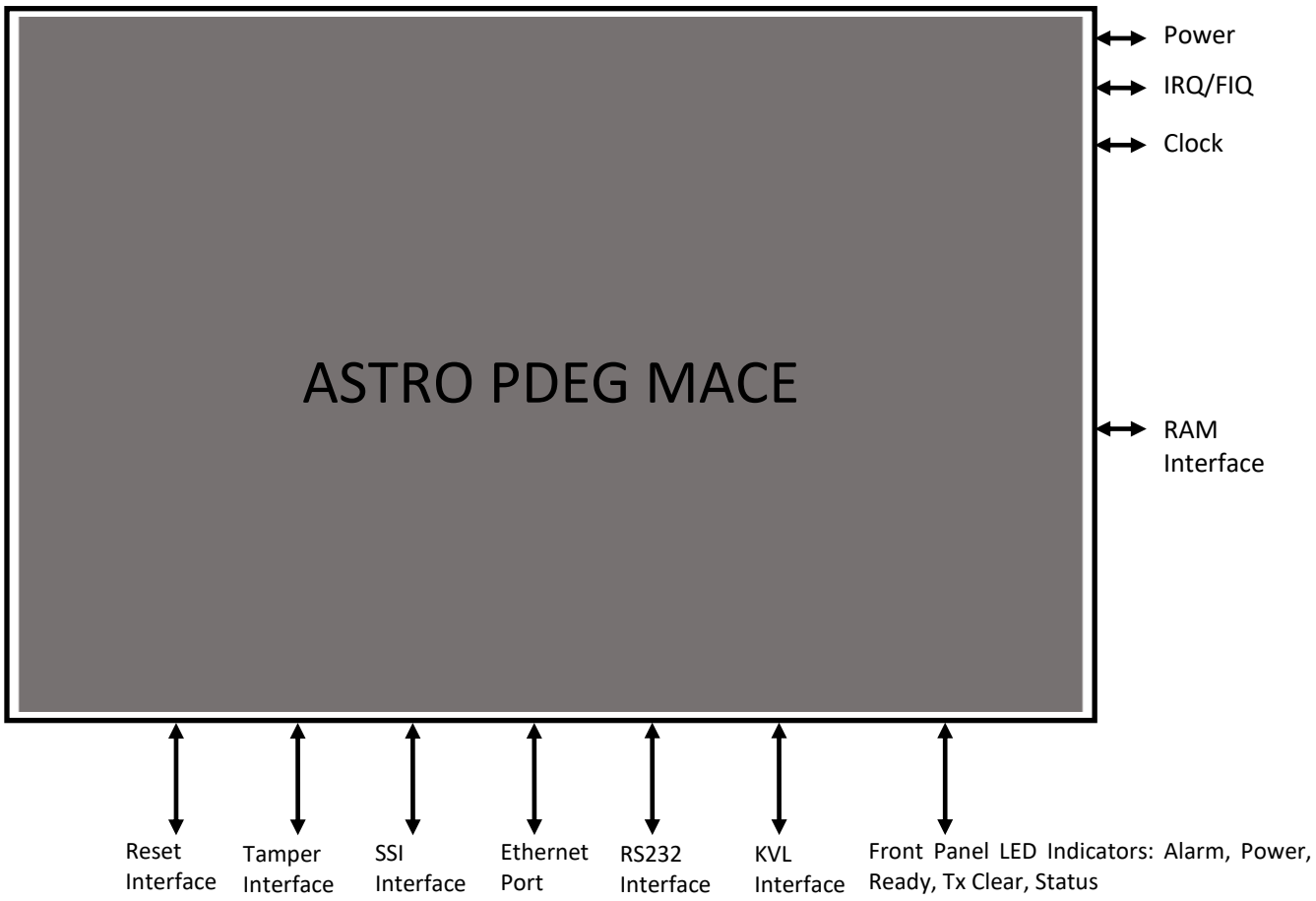

Figure 3: Cryptographic Boundary

2.3 Modes of Operation

The ASTRO PDEG MACE can be configured to operate in a an approved mode of operation and a non-approved mode of operation. CSPs are not shared between approved mode and non-approved mode. The transition from a approved mode to a non- approved mode, and vice-versa, causes all CSPs to be zeroized except hardcoded CSPs. All hardcoded CSPs are unique between approved and non-approved mode and therefore are exclusive between approved and non-approved services and modes of operation.

When the module is in approved mode. The “Module Status” service can be used to verify the firmware version matches an approved version listed on NIST’s website:
https://csrc.nist.gov/projects/cryptographic-module-validation-program/validated-modules

2.3.1 Configuration of the Approved Mode of Operation

The module can be configured to operate in a FIPS 140-3 Approved mode of operation at overall Security Level 3. To configure the module to operate in approved mode, the operator must log in as the CO using the default password and:

1. Change the default password.
2. Activate and configure the periodic self-test timer.
3. Type the command "`fips enable`" to configure the Module into Approved mode (level 3).

The Approved mode is indicated by using the "Set FIPS Mode" service. The result from this service will display:

- Encrypted only Keyfill is Enabled
- FIPS mode is Level 3

The operator shall configure the periodic self-tests timer as part of the Module configuration, refer to Section 11 for further details.

2.3.2 Configuration of the Non-Approved Mode of Operation

To configure the device to a non-Approved mode, the operator as the CO can type the command "fips disable". The result is indicated by using the "Set FIPS Mode" service. The result from this service will display:

- Encrypted on Keyfill is Disabled
- FIPS mode is Not FIPS approved

The loading of non-validated firmware within the validated cryptographic module invalidates the module's validation and zeroizes all CSPs.

2.4 Security Functions

The MACE implements the Approved and Non-Approved but Allowed cryptographic functions listed in the tables below.

Table 3 – Approved Algorithms

Cert #	Algorithm	Mode	Description	Functions/Caveats
AES 819	AES [197]	CBC [38A]	Key Sizes: 256	Encrypt, Decrypt
		CFB8 [38A]	Key Sizes: 256	Encrypt, Decrypt
		ECB [38A]	Key Sizes: 256	Encrypt, Decrypt
		OFB [38A]	Key Sizes: 256	Encrypt, Decrypt
AES 1295	AES [197]	GCM [38D][1]	Key Sizes: 256	Encrypt, Decrypt
AES 5358	AES [197]	KW [38F]	Forward Key Sizes: 256	Authenticated Decrypt for KTS
VA	CKG [IG D.H]	[133] Section 4 and Section 6.1 (example 1) - Direct symmetric key generation using unmodified DRBG output		Key Generation, IV

[1] Per IG C.H Scenario 2, the MACE generates GCM IVs randomly with a length of 96-bits as specified in SP800-38D section 8.2.2 using approved DRBG (Cert # A2935).

Cert #	Algorithm	Mode	Description	Functions/Caveats
		[133] Section 6.3 (#2) Symmetric Keys Produced by Combining (Multiple) Keys and Other Data		
A2935	DRBG [90A]	CTR with derivation function	AES-256	Deterministic Random Bit Generation[2]
AES 5358	KTS	Key Unwrap	AES-256	AES KW Cert. #5358
A5253	RSA [186-5]	PKCS1_v1.5	2048	SigVer
SHS 817	SHS [180]	SHA-256		Message Digest Generation, Password Obfuscation

Table 4 – Non-Approved Algorithms Allowed in the Approved Mode of Operation

Algorithm	Description
KTS (AES Key Unwrap)	[IG D.G] AES Cert. #AES 819, key unwrapping; Key establishment methodology provides 256 bits strength.

Table 5 – Non-Approved Algorithms Allowed in the Approved Mode of Operation with No Security Claimed

Algorithm	Description
AES MAC	[IG 2.4.A] P25 AES OTAR. No Security Claimed. AES MAC is used as part of OTAR but is considered obfuscation. KTS encryption is performed on the OTAR key components and decrypted within the module using AES KW Cert. #AES 5358

Note: All Security Functions are available in Approved and Non-Approved mode.

Note: The module does not implement any Non-Approved Algorithms and Not Allowed Cryptographic Functions in the Approved Mode of Operation.

2.5 Overall Security Design

1. The Module provides identity based authentication.
2. The Module inhibits all data output via the data output interface whenever an error state exists, zeroization, firmware loading, key generation and during self-tests.
3. The Module logically disconnects the output data path from the circuitry and processes when performing key generation, or key zeroization.
4. Authentication data (e.g., passwords) are entered in encrypted form.
5. Secret cryptographic keys are entered in encrypted form over a physically separate port.
6. The Module supports a Cryptographic Officer role and User role. Authenticated operators are authorized to assume either supported role.
7. The module supports alternating bypass.

[2] The entropy for seeding the SP 800-90A DRBG is determined by the operator of the MACE which is outside of the module's physical and logical boundary. The operator shall use entropy sources that meet the security strength required for the random Number generation mechanism as shown in [SP 800-90A] Table 3 (CTR_DRBG) and set required bits into the module by using Load Entropy service listed in section 4.3. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys. The MACE will not operate in an approved mode if the module is not seeded by the external entropy.

8. Authentication data is not displayed during entry.
9. After a sufficient number of consecutive unsuccessful attempts (10 for Crypto Officer, 15 for User), the module will zeroize all CSP's stored in non-volatile storage, except the User password.
10. The Module does not support the output of plaintext or encrypted secret keys.
11. The Module implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
12. The ASTRO PDEG MACE protects secret keys from unauthorized disclosure, modification and substitution.
13. The Module provides a means to ensure that a key entered into or stored within the Module is associated with the correct entities to which the key is assigned.
14. The Module denies access to plaintext secret keys contained within the Module.
15. The Module provides the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the Module.
16. The Module enters an error state if the Cryptographic Algorithm Test, Continuous Random Number Generator Test, or DRBG KAT fails. This error state may be excited by powering the module off then on.
17. The Module enters a state that only allows new firmware to be loaded if Firmware Integrity test or Firmware Load test fails.
18. The Module outputs an error indicator by turning the Alarm LED output red whenever an error state is entered due to a failed self-test.
19. The Module does not perform any cryptographic functions while in an error state.
20. The Module turns on the "Tx Clear" LED when a security association rule allowing bypass data exists.
21. The Module does not support multiple concurrent operators.

2.6 Rules of Operation

The ASTRO PDEG MACE shall operate within a Motorola Solutions PDEG Encryption Unit. After authentication with the default password, the operator shall change the default password for User role. The ASTRO PDEG MACE is not usable until the factory default password is changed for the User role.

Likewise, before any CO operations can be performed, the CO password must be changed from the factory default upon first login of the CO.

3 Cryptographic Module Interfaces

The MACE's ports and associated defined logical interface categories are listed in Table 6.

Table 6 – Ports and Interfaces

Physical Port	Logical Interface	Data that passes over port/interface
Serial Synchronous Interface (SSI)	Data Input Data Output Control Input Status Output	Provides an interface to the unprotected network and entry of the User password in encrypted form.
Ethernet Port (EP)	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.
RS232 Interface	Control Input Status Output Data Output	Provides an interface for factory programming and execution of RS232 shell commands.
Key Variable Loader (KVL)	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.
RAM	Data Input Data Output Control Input Status Output	This interface provides storage for non-security related stack information.
Power	Power Input Internal battery-backed RAM	This interface powers all circuitry.
Tamper Interface	Control Input	The interface is used for zeroization of Traffic Encryption Keys (TEKs), KPK.
Reset Interface	Control Input	This interface forces a reset of the module.
Alarm LED output	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	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	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	Status Output	The TX Clear LED output is used to drive the external TX Clear LED orange when a "Bypass Rule" is programmed.

Physical Port	Logical Interface	Data that passes over port/interface
Status LED output	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	Control Input	External interrupts
Clock	Control Input	Clock input

NOTE: The module does not have Control Output

4 Roles, Services and Authentication

4.1 Assumption of Roles and Related Services

The ASTRO PDEG MACE supports two distinct operator roles, Cryptographic Officer (CO) and User. Table 7 lists all operator roles supported by the ASTRO PDEG MACE and their related services. In addition, the ASTRO PDEG MACE supports services which do not require to be authenticated, listed as "UA" in Table 7. The ASTRO PDEG MACE does not support a maintenance role.

Table 7 – Roles, Service Commands, Input and Output

Role			Service	Input	Output
CO	User	UA			
X	–		Program Update	Firmware image	The ASTRO PDEG MACE is upgraded to new firmware.
–	X	–	Load Entropy	DRBG seed	The DRBG is seeded and initialized. Success/failure status.
–	X	–	OTEK	Encrypted keys	Decrypted keys that were imported encrypted into the ASTRO PDEG MACE. Success/failure status.
–	X	–	Generate Random Number	Command In	Generated random numbers. (KPK, IV) Success/failure status.
X	–	–	Change CO Password	Password	Updated the CO password. Success/failure status.
–	X	–	Change User Password	Password	Updated the User password. Success/failure status.
X	–	–	Validate CO Password	Password	Successful authentication will allow access to the services allowed for CO role.
–	X	–	Validate User Password	Password	Successful authentication will allow access to the services allowed for User role.
X	–	–	Logout CO	Command In	Logout CO/Exits command shell interface
–	X	–	Logout User	Reboot/Command In	Logout User
–	X	–	Encrypt	Plaintext	Ciphertext. Success/failure status.
–	X	–	Decrypt	Ciphertext	Plaintext. Success/failure status.
–	X	–	Bypass	Plaintext	Plaintext. Success/failure status.
X	-	–	Module Status	Command in	Module HW version, version information, and FIPS status.
X	-	X	Self-Tests	Power on/Command In	Success/Reset.
X	–	–	Configure Module	Configuration parameters	Updated module configuration. Success/failure status.

Role			Service	Input	Output
CO	User	UA			
X	–	–	Set FIPS Mode	Configuration parameters	Updated module FIPS mode/Display current FIPS mode
X	–	–	Configure Security Association	Configuration parameters	Updated module security association configuration. Success/failure status.
X	–	–	Check Security Association	Command In	Security association configuration.
X	–	–	Configure OTEK	Configuration parameters	Updated OTEK configuration. Success/failure status.
X	–	–	Version Query	Command In	Show module version info
–	X	–	Delete Key	Command In	Key is marked for deletion. Success/failure status.
–	X	–	Perform Key Transport Process	Command In	Keys imported into the MACE. Success/failure status.
–	X	–	KVL Transfer Key[3]	Encrypted Keys	Keys imported into the ASTRO PDEG MACE. Success/failure status.
–	X	–	KVL Delete Key	Command In	Keys deleted from the ASTRO PDEG MACE. Success/failure status.
–	X	–	KVL Check Key	Command In	Show key status
–	X	–	KVL Query Algorithm List	Command In	Show list of supported algorithms
X	–	–	Extract Error Log	Command In	Error logs out. Success/Failure status.
–	–	X	Reset Crypto Module	Reset Button press/Cycle power.	Reset the MACE
–	–	X	Erase Crypto Module	Erase Button press	Zeroize all CSPs

4.2 Authentication Methods

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

[3] In Non-Approved Mode of Operation, Keys imported into the ASTRO PDEG MACE using the KVL Transfer Key are in plaintext.

Table 8 – Roles and Authentication

Role	Authentication Type	Authentication Method	Authentication Strength
CO	Identity-Based	Crypto-Officer Password: a 15-16 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.	The password requires a minimum of 1 Upper case, 1 Lower case, 1 Numerical and 1 special character. Since the minimum password length is 15 ASCII printable characters and there are 95 ASCII printable characters, the probability of a successful random attempt is 1 in $\{(10)*(26^2)*(32)*(95^{11})\}$. After the CO password has been incorrectly entered 10 consecutive times, the Module will erase all CSPs, reset the CO password back to the default and set an alarm, at which time the module must be power cycled to become operational again.
User	Identity-Based	User Password: a 10 hexadecimal digit 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 10 hex digits, the probability of successful random attempt is 1 in 16^10. After the User password has been incorrectly entered 15 consecutive times, the Module will erase all CSPs, reset the CO password back to the default and set an alarm, at which time the module must be power cycled to become operational again. Note the User password is NOT reset in this instance.

4.3 Services

All services implemented by the ASTRO PDEG MACE are listed in Table 9. The ASTRO PDEG MACE does not allow any non-approved services while operating in FIPS 140-3 level 3 mode. The Note that all services listed in Table 9 below are available in both the approved and non-approved mode.

The SSPs modes of access shown in Table 9 are defined as:

- **G** = Generate: The ASTRO PDEG MACE generates or derives the SSP.
- **R** = Read: The SSP is read from the ASTRO PDEG MACE (e.g., the SSP is output).
- **W** = Write: The SSP is updated, imported, or written to the ASTRO PDEG MACE.
- **E** = Execute: The ASTRO PDEG MACE uses the SSP in performing a cryptographic operation.
- **Z** = Zeroize: The ASTRO PDEG MACE zeroizes the SSP

The approved security service indicator of the module is compliant to the example scenario #2 of [IG] 2.4.C.

Table 9 – Approved Services

Service	Description	Approved Security Functions	Keys and/or SSP	Roles	Access Rights to Keys and/or SSPs	Indicator
Program Update	Update the ASTRO PDEG MACE firmware. Firmware upgrades are authenticated using a digital signature. The Program Update Public Signature Key is used to validate the signature of the firmware image being loaded before it is allowed to be executed.	RSA [186-5], Cert. #A5253	FW-LD-Pub	CO	Z	Approved Mode
			IDK		Z	
			IDK-ROM		E	
			IDK-Block		EZ	
			BKK		Z	
			EDK		Z	
			PEK		Z	
			KPK		Z	
			UKKPK		Z	
Load Entropy	Load entropy into the ASTRO PDEG MACE.	AES Key Unwrap, AES Cert. #AES 5358, DRBG [90A] Cert. #A2935	DRBG-EI/SEED	User	WE	Approved Mode
			DRBG-State		G	
			EDK		E	
Generate Random Number	Generated random numbers.	AES-256, Cert. #AES 819, CKG (VA), DRBG [90A] #A2935	DRBG-EI/SEED	User	E	Approved Mode
			DRBG-State		E	
			KPK		G	
			UKKPK		E	
OTEK	Load Keys into the ASTRO PDEG MACE.	AES Key Unwrap, AES Cert. #AES 5358	KEK	User	E	Approved Mode
			TEK		E	
			PEK	CO	E	

Service	Description	Approved Security Functions	Keys and/or SSP	Roles	Access Rights to Keys and/or SSPs	Indicator
Change CO Password	Modify the current password used to identify and authenticate the CO role.	AES-256, Cert. #AES 819, SHS [180], Cert. #SHS 817	KPK		GEZ	Approved Mode
			KEK		Z	
			TEK		Z	
			CO Password		GEZ	
			PWD Hash		GEZ	
			UKKPK		E	
Change User Password	Modify the current password used to identify and authenticate the User role.	AES-256, Cert. #AES 819 SHS [180], Cert. #SHS 817	PEK	User	E	Approved Mode
			KPK		GEZ	
			KEK		Z	
			TEK		Z	
			User Password		GEZ	
			PWD Hash		GEZ	
			UKKPK		E	
Validate CO Password	Validate the current password used to identify and authenticate the CO role.	AES-256, Cert. # AES 819, SHS [180], Cert. #SHS 817	PEK	CO	E	Approved Mode
			KPK		GEZ	
			KEK		Z	
			TEK		Z	
			CO Password		Z	
			User Password		Z	
			PWD Hash		Z	
			UKKPK		E	
Validate User Password	Validate the current password used to identify and authenticate the User role.	AES-256, Cert. # AES 819 SHS [180], Cert. #SHS 817	PEK	User	E	Approved Mode
			KPK		GEZ	
			KEK		Z	
			TEK		Z	
			CO Password		Z	
			User Password		Z	
			PWD Hash		Z	
			UKKPK		E	
Logout CO	Exits command shell interface	N/A	N/A	CO	N/A	Approved Mode
Encrypt	Encrypt data.	AES [197], Certs. #AES 819 or #AES 1295, CKG (VA), DRBG [90A] #A2935	PEK	User	E	Approved Mode
			TEK		E	
			KEK		E	
			KPK		E	
			DRBG-EI/SEED		E	
			DRBG State		E	
			PEK	User	E	

Service	Description	Approved Security Functions	Keys and/or SSP	Roles	Access Rights to Keys and/or SSPs	Indicator
Decrypt	Decrypt data.	AES [197], Certs. #AES 819 or #AES 1295, CKG (VA), DRBG [90A] # A2935	TEK		E	Approved Mode
			KEK		E	
			KPK		E	
			BKK		E	
			IDK		E	
Bypass	Bypass encryption/decryption services	N/A	N/A	User	N/A	Approved Mode
Module Status	Provide firmware version, current FIPS status	N/A	N/A	CO	N/A	Approved Mode
Self-Tests	Perform module self-tests comprised of cryptographic algorithm tests, firmware integrity test, and critical functions test. Initiated by module reset or transition from power off state to power on state.	N/A	FW-LD-Pub	CO/UA	E	Approved Mode
Module Configuration	Set configuration parameters used to specify module behavior.	N/A	KPK	CO	GEZ	Approved Mode
			KEK		Z	
			TEK		Z	
			Password		WZ	
			PWD Hash		WZ	
			UKKPK		E	
Set FIPS Mode	Update module FIPS mode.	N/A	N/A	CO	N/A	Approved Mode
Configure Security Association	Update module security association configuration.	N/A	N/A	CO	N/A	Approved Mode
Check Security Association	Display Security association configuration.	N/A	N/A	CO	N/A	Approved Mode
Configure OTEK	Set configuration parameters used for communication with the KMF for OTEK	N/A	N/A	CO	N/A	Approved Mode

Service	Description	Approved Security Functions	Keys and/or SSP	Roles	Access Rights to Keys and/or SSPs	Indicator
Version Query	Provides module firmware and hardware version numbers	N/A	N/A	CO	N/A	Approved Mode
Delete Key	Mark key for deletion.	N/A	KPK	User	N/A	Approved Mode
Perform Key Transport Process	Perform a key transport process for OTEK service.	AES KW Key Unwrap, AES Cert. #AES 5358	KEK	User	W	Approved Mode
			TEK		W	
KVL Transfer Key	Imports keys to the ASTRO PDEG MACE via KVL.	AES KW Key Unwrap, AES Cert. #AES 5358	BKK	User	E	Approved Mode
			KPK		E	
			KEK		W	
			TEK		W	
KVL Delete Key	Zeroize selected key variables from the ASTRO PDEG MACE.	N/A	KEK	User	Z	Approved Mode
			TEK		Z	
KVL Check Key	Obtain status information about a specific key/keyset.	N/A	BKK	User	E	Approved Mode
KVL Query Algorithm List	Provides algorithm version numbers	N/A	N/A	User	E	Approved Mode
Extract Error Log	Provide the history of error events.	N/A	N/A	CO	N/A	Approved Mode
Reset Crypto Module	Reset/power cycle the ASTRO PDEG MACE.	N/A	DRBG-EI/SEED	UA	Z	Approved Mode
			DRBG-State		Z	
Erase Crypto Module	Zeroize 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.	N/A	KPK	UA	GZ	Approved Mode
			KEK		Z	
			TEK		Z	
			Password		Z	
			PWD Hash		Z	
			UKKPK		E	

Note: All services in Table 9 are available in Non-Approved Mode with the KVL Transfer Key importing keys in plaintext.

5 Firmware Security

The ASTRO PDEG MACE is composed of base firmware version identified in Table 2.

The firmware components are protected with the authentication technique(s) RSA Programmed Signature Key described in Table 17.

The Module includes a firmware verification and load service to support necessary updates.

The operator can initiate the firmware integrity test on demand by power cycling the ASTRO PDEG MACE.

6 Operational Environment

The ASTRO PDEG MACE has a limited operational environment under the FIPS 140-3 definitions with a Physical Security at Level 3 therefore this section in not applicable.

7 Physical Security

The ASTRO PDEG MACE is a production grade, single-chip cryptographic module as defined by FIPS 140-3 and is designed to meet level 3 physical security requirements. The information below is applicable to cryptographic module hardware kit numbers 5185912Y03, 5185912Y05, and 5185912T05, which have identical physical security characteristics.

The ASTRO PDEG MACE is covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the ASTRO PDEG MACE. The security provided from the hardness of the ASTRO PDEG MACE's epoxy encapsulate is claimed at ambient temperature (-40 to 85 degrees Celsius) only. No assurance of the epoxy hardness is claimed for this physical security mechanism outside of this range. The ASTRO PDEG 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 ASTRO PDEG MACE while delivering to operators.

There are two voltage powers that power the MACE. VDDCORE voltage powers all MACE chip functions while VDDBU voltage powers the MACE chip battery. VDDCORE and VDDBU voltages enter the cryptographic boundary of the module separately; and therefore, were tested separately to verify that they both cause the MACE chip to zeroize SSPs

Table 10 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Covered with a hard-opaque epoxy coating that provides evidence of attempts to tamper with the ASTRO PDEG MACE.	Periodically	Look for signs of tampering. Remove from service if tampering found.

Table 11 – EFP/EFT

	Temperature or Voltage Measurement	EFP Description	Results
Low Temperature	-38.1°C	A tamper flag is raised, a wake-up reset of the product is triggered.	Shutdown
High Temperature	101.4°C	A tamper flag is raised, a wake-up reset of the product is triggered.	Shutdown
Low Voltage	1.65V 65V VDDCORE : 1.350 VVDBU	A general reset of the chip is asserted.	Shutdown
High Voltage	2.034V VDDCORE : 2.292V - VVDBU	A tamper flag is raised, a wake-up reset of the product is triggered.	Shutdown

Table 12 – Hardness testing temperature ranges

	Hardness tested temperature measurement
Low Temperature	-40°C
High Temperature	85°C

8 Non-Invasive Security

The ASTRO PDEG MACE does not implement any mitigation method against non-invasive attack.

9 Sensitive Security Parameter (SSP) Management

The SSPs access methods are described in Table 13 below:

Table 13 – SSP Management Methods

Method	Description
G1	Generated external to the MACE and installed during manufacturing.
G2	Derived from the DRBG input per SP800-90Ar1.
G3	Symmetric key generated by internal CAVP validated DRBG.
G4	Generated per SP800-133r2 (Section 6.3 #2) via XOR of 2 other keys (IDK-ROM and IDK-Block)
S1	Stored in the volatile memory (RAM).
S2	Stored in the flash in plaintext, associated by memory location (pointer).
S3	Stored in the flash in encrypted, associated by memory location (pointer).
E1	Electronically input, AES-256 CBC encrypted by the IDK-Block and ROM using AES KTS (Cert. #AES 819)
E2	Electronically input, AES-256 OFB encrypted by the BKK using AES KTS (Cert. #AES 819)
E3	Electronically input, AES-256 CFB-8 encrypted by the PEK using AES KTS (Cert. #AES 819)
E4	Electronically input, AES-256 ECB encrypted by the EDK using AES KTS (Cert. #AES 819).
E5	Electronically input using SP800-38F AES key transport on the KEK or TEK using AES KW (Cert. #AES 5358).
Z1	Zeroized by program update service by overwriting with a fixed pattern of “0s”.
Z2	Zeroized in RAM by module power cycle or hard reset by overwriting with a fixed pattern of “0s”.
Z3	Zeroized by the “KVL Delete Key” service by overwriting with a fixed pattern of “0s”.
Z4	Zeroized by the “Erase Crypto Module service by overwriting with a fixed pattern of “0s”.
Z5	Zeroized by the “validate password” service by overwriting with a fixed pattern “0s”.
Z6	Zeroized by the “change password” service by overwriting with a fixed pattern “0s”.
Z7	Zeroized by the “module configuration” service by overwriting with a fixed pattern “0s”.
Z8	Zeroized by the “OTEK” service by overwriting with a fixed pattern “0s”.
Z9	Zeroized by the “KVL Transfer Keys” service by overwriting with a fixed pattern “0s”.

NOTE: Zeroization is implicit and is considered complete either after the boot sequence is complete or when CO initiates zeroization via Erase Crypto Module service and the module provides success/fail status.

9.1 Sensitive Security Parameters (SSPs)

All SSPs (CSPs and PSPs) used by the ASTRO PDEG MACE are described in this section. All usage of these CSPs by the ASTRO PDEG MACE is described in the services detailed in 4.3.

Table 14 – SSPs

Key/SSP Name/ Type	Strength (in bits)	Security Function/Cert.	Gener-ation	Import (I) /Export (E)	Establish-ment	Storage	Zeroiza-tion	Use/Related SSPs
CSPs								
DRBG-EI/Seed	N/A	N/A	N/A	E4	N/A	S1	Z2	Externally generated, a minimum of 48 bytes are passively entered into the MACE by the CO.
DRBG-State	256	DRBG Cert. #A2935	G2	N/A	N/A	S1	Z2	CTR_DRBG internal state: V (128 bits) and Key (AES 256) and derived from DRBG-EI/Seed
IDK-ROM	256	AES CBC Cert. #AES 819	G1	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES CBC key used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK Block.
IDK-Block	256	AES CBC Cert. #AES 819	G1	E1	N/A	S1, S2	Z1, Z2	A 256-bit AES CBC key used in the re-construction of IDK per SP800-133r2 (Section 6.3 #2) via XOR using IDK-ROM.
IDK	256	AES CBC Cert. #AES 819, RSA Cert. #A5253	G4	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES CBC key used to decrypt downloaded images.
BKK	256	AES OFB Cert. #AES 819, RSA Cert. #A5253	G1	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES key used for decrypting the keys entered into the MACE through KVL interface.
EDK	256	AES CBC Cert. #AES 819, AES ECB Cert. #AES 819, RSA Cert. #A5253	G1	N/A	N/A	S1, S2	Z1, Z2	A 256-bit AES key used for decrypting the external entropy seed
PEK	256	AES CFB-8 Cert. #AES 819, RSA Cert. #A5253	G1	N/A	N/A	S1, S2	Z1, Z2	256-bit AES CFB-8 key used for decrypting passwords.

Key/SSP Name/ Type	Strength (in bits)	Security Function/Cert.	Gener-ation	Import (I) /Export (E)	Establish-ment	Storage	Zeroiza-tion	Use/Related SSPs
KPK	256	AES CFB-8 Cert. #AES 819, DRBG Cert. #A2935	G3	N/A	N/A	S1, S3	Z2, Z4, Z5, Z7	256-bit AES CFB-8 key used to encrypt all TEKs and KEKs stored in the flash.
UKKPK	256	AES CBC Cert #AES819, AES CFB8 Cert #AES819, RSA Cert #A5253	G1	N/A	N/A	S1, S2	Z1, Z2	256-bit AES Key used for encrypting the KPK in flash
KEK	256	AES KW Cert. #AES 5358, AES OFB Cert. #AES 819	N/A	E2, E5	N/A	S1, S3	Z2, Z3, Z4, Z5, Z7, Z8, Z9	256-bit AES Keys used for decrypting keys in the OTEK service.
TEK	256	AES KW #AES 5358, AES OFB Cert. #AES 819, AES GCM #AES 1295	N/A	E2, E5	N/A	S1, S3	Z2, Z3, Z4, Z5, Z7, Z8, Z9	256-bit AES key used for data encryption.
CO Password	N/A	AES CFB-8 Cert. #AES 819	N/A	E3	N/A	S1	Z2, Z5, Z6, Z7	15-16-digit ASCII (printable) characters password.
User Password	N/A	AES CFB-8 Cert. #AES 819	N/A	E3	N/A	S1	Z2, Z5, Z6, Z7	10-digit hexadecimal number user authentication password.
PWD Hash	128	SHS [180] Cert. #SHS 817	G1	N/A	N/A	S1, S2	Z2, Z5, Z6, Z7	256-bit password hash stored in the non-volatile memory.
PSPs								
FW-LD-Pub	112	AES CBC Cert. #AES 819, RSA Cert. #A5253	G1	N/A	N/A	S1, S2	Z1, Z2	FW Load: 2048-bit RSA key used to validate the signature of the firmware image before it is allowed to be executed.

Table 15– Non-Deterministic Random Number Generation Specification

Entropy Sources	Minimum number of bits of entropy	Details
External	384 bits of entropy	The entropy for seeding the SP 800-90A DRBG is determined by the host application using the Module and is outside of the module's physical. The operator shall use entropy sources that meet the security strength required for the random number generation mechanism as shown in [SP 800-90A] Table 3 (CTR_DRBG) and set required bits into the module by using Load Entropy service listed in section 4.3. Since entropy is loaded passively into the module, there is no assurance of the minimum strength of generated keys.

10 Self-Tests

The ASTRO PDEG MACE performs self-tests to ensure the proper operation. Per FIPS 140-3 these are categorized as either pre-operational self-tests or conditional self-tests.

Pre-operational and Conditional self-tests are available on demand by power cycling the MACE. Conditional self–tests are periodically performed by the MACE as configured by the operator during module configuration as shown in Section 11.1.1. The MACE will not accept any commands when a periodic self-test is required; the commands still in the I/O buffer will be processed by the MACE at the end of periodic self-test when the I/O buffer is emptied. The MACE will reset if any self-tests fail, otherwise it will continue to operate normally. The MACE logs the most recent self-test errors to the internal flash; the operator (UA) can extract the error logs using Extract Error Log service list in section 4.3.

The self-tests error states and status indicator are described in table below:

Table 16 – Error States and Indicators

Error state	Description	Indicator
ES1	The ASTRO PDEG MACE fails a KAT.	The ASTRO PDEG MACE enters the critical error state and sets the status alarm LED. In this state, the ASTRO PDEG MACE stores the status into the internal flash memory and then halts all further operation by entering an infinite loop. The operator may correct this state by power cycling the ASTRO PDEG MACE.
ES2	The ASTRO PDEG MACE fails a firmware loading during program upgrade and/or firmware integrity pre-operational self-test.	The ASTRO PDEG MACE enters the firmware signature validation failure state and sets the status alarm LED. In this state, the ASTRO PDEG MACE halts all further operations by entering the flash programming mode. The operator may correct the issue by power cycle and/or re-flashing a new image.

The ASTRO PDEG MACE performs the following pre-operational self-tests:

Table 17 – Pre-Operational Self-Test

Security Function	Method	Description	Error state
Firmware integrity	RSA (Cert. #A5253), SHA-256 (Cert. #SHS 817)	A digital signature is generated over the Boot Block and Base firmware when it is built using SHA-256 (Cert. #SHS 817) and RSA-2048 (Cert. #A5253) and is stored with the code in the ASTRO PDEG MACE. When the ASTRO PDEG MACE is powered up, the digital signature is verified. If the digital signature matches, then the test passes, otherwise it fails.	ES2
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.	ES1

The MACE performs the following conditional self-tests:

Table 18 – Conditional Self-Tests

Security Function	Method	Description	Error state
AES – ECB (Cert. #AES 819)	KAT	AES-256 ECB encryption KAT – Inclusive to AES CBC and OFB testing with 256-bit key per IG 10.3.A.	ES1
AES – ECB (Cert. #AES 819)	KAT	AES-256 ECB decryption KAT – Inclusive to AES CBC and OFB testing with 256-bit key per IG 10.3.A.	ES1
AES – CFB8 (Cert. #AES 819)	KAT	AES-256 CFB-8 encryption KAT – Inclusive to AES-256 OFB testing with 256-bit key per IG 10.3.A.	ES1
AES – CFB8 (Cert. #AES 819	KAT	AES-256 CFB-8 decryption KAT – Inclusive to AES-256 OFB testing with 256-bit key per IG 10.3.A.	ES1
AES – GCM (Cert. #AES 1295)	KAT	AES-256 GCM encryption and decryption KAT as per IG 10.3.A	ES1
AES – GCM (Cert. #AES 1295)	KAT	AES-256 GCM encryption and decryption KAT as per IG 10.3.A	ES1
AES KW (Cert. #AES 5358)	KAT	AES-256 key unwrap KAT.	ES1
DRBG (Cert. # A2935)	KAT	AES-256 CTR_DRBG Health Tests (instantiation, generate, and reseed) KATs performed before the first random data generation.	ES1
Firmware Load	RSA-2048 SigVer	A digital signature is generated over the code when it is built using SHA-256 (Cert. #SHS 817) and RSA-2048 (Cert. #A5253). The digital signature is verified upon download into the ASTRO PDEG MACE.	ES2
RSA SigVer (Cert. #A5253)	KAT	RSA-2048 SigVer, performed before FW integrity tests.	ES2
SHS 256-bit (Cert. #SHS 817)	KAT	SHA-256 KAT, performed before FW integrity tests.	ES2
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).	ES1
Bypass Integrity Test	SHA-256 Hash	The IP source/destination addresses (table of associations) is stored with an associated hash value that is checked each time the table is accessed and updated with a new hash value when the table is modified by the authenticated CO via the Security Association Configuration service.	ES2

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

11.1.1 Installation and Initialization

The Module is originally a non-compliant module and must be initialized to be in approved mode. There is no non-approved mode. During initialization the operator shall configure the MACE from the instructions below:

1. Upon first access, the operator will use the default password provided by Motorola in a separate communication.
2. The operator will then change the default password based on the requirements in Table 8 – Roles and Authentication
3. The operator will then configure the MACE using the Module configuration service as specified in the section 2.3.1.
4. Finally, the operator will set the periodic self-tests timer as part of the Module configuration in every X minutes, where X is a minimum value = 1 minute and maximum value = 712,800 minutes (495 days). Note: the default minimum = 0* but must be changed to a minimum of 1.

   * periodic self-tests will not perform if minimum = 0

11.1.2 Delivery

The MACE is embedded in multiple Motorola Solutions, Inc. radios (aka, subscribers). Motorola uses commercially available courier systems such as UPS, FedEx, and DHL with a tracking number and requires a signature at the end by an authorized client.

11.2 Administrator Guidance

Use radio specific user guide available on the www.motorolasolutions.com website for secure operations.

11.3 Non-Administrator Guidance

Use radio specific user guide available on the www.motorolasolutions.com website for secure operations.

11.4 Maintenance Requirements

The MACE does not require any special maintenance.

11.5 End of Life

After the end-of-life, the operator should zeroize all SSPs using the “Zeroize all keys and password“ service listed in the Section 4.3 followed by shredding the MACE chip.

12 Mitigation of Other Attacks

The ASTRO PDEG MACE does not implement any mitigation method against other attacks.

13 References and Definitions

The following standards are referred to in this Security Policy.

Table 19 – References

Abbreviation	Full Specification Name
[FIPS140-3]	*Security Requirements for Cryptographic Modules*, March 22, 2019
[ISO19790]	*International Standard, ISO/IEC 19790, Information technology — Security techniques — Test requirements for cryptographic modules, Third edition, March 2017*
[ISO24759]	*International Standard, ISO/IEC 24759, Information technology — Security techniques — Test requirements for cryptographic modules, Second and Corrected version, 15 December 2015*
[IG]	*Implementation Guidance for FIPS PUB 140-3 and the Cryptographic Module Validation Program, October 7, 2022.*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, Revision 2, March 2019*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, Revision 2, June 2020*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-5, February 2023.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38D]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, Special Publication 800-38D, November 2007*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, Revision 1, June 2015.*
[OTAR]	*Project 25 – Digital Radio Over-The-Air-Rekeying (OTAR) Messages and Procedures [TIA-102.AACA-A], September 2014*

Table 20 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
BKK	Black Keyloading Key
CBC	Cipher Block Chaining
CFB	Cipher Feedback
CKG	Cryptographic Key Generation
CSP	Critical Security Parameter
DRBG	Deterministic Random Bit Generator
DRBG-EI	DRBG Entropy Input
ECB	Electronic Code Book
EDK	Entropy Decryption Key
FIPS	Federal Information Processing Standards
FW	Firmware
FW-LD-Pub	Firmware Load Public Key
GCM	Galois/Counter Mode
HSM	Hardware Security Module
IC	Integrated Circuit
IDK	Image Decryption Key
IV	Initialization Vector
KAT	Known Answer Test
KPK	Key Protection Key
KEK	Key Encryption Key
KVL	Key Variable Loader
MAC	Message Authentication Code
MACE	Motorola Advanced Crypto Engine
OFB	Output Feedback
OTAR	Over The Air Rekeying
PDEG	Packet Data Encryption Gateway
PEK	Password Encryption Key
PWD Hash	Password Hash
RSA	Rivest–Shamir–Adleman
SSI	Synchronous Serial Interface
SSP	Sensitive Security Parameter
TEK	Traffic Encryption Key
UA	Unauthenticated Service
UKKPK	Universal Key for Key Protection Key