FIPS 140-2 Non-Proprietary Security Policy

Maxar AEDS

Document Version 1.4

October 25, 2023

Prepared For:

Maxar Technologies
3825 Fabian Way
Palo Alto, CA 94303
www.maxar.com

Prepared By:

SafeLogic Inc.
530 Lytton Ave, Suite 200
Palo Alto, CA 94301
www.safelogic.com

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 About FIPS 140

Federal Information Processing Standards Publication 140-2 — Security Requirements for Cryptographic Modules specifies requirements for cryptographic modules to be deployed in a Sensitive but Unclassified environment. The National Institute of Standards and Technology (NIST), Canadian Centre for Cyber Security (CCCS), and Cryptographic Module Validation Program (CMVP) run the FIPS 140 program. National Voluntary Laboratory Accreditation Program (NVLAP) accredits independent testing labs to perform FIPS 140 testing; the CMVP validates modules meeting FIPS 140 validation. *Validated* is the term given to a module that is documented and tested against the FIPS 140 criteria.

More information is available on the CMVP website at https://csrc.nist.gov/groups/STM/cmvp/index.html.

1.2 About this Document

This non-proprietary Cryptographic Module Security Policy for the Maxar AEDS from Maxar Technologies ("Maxar") provides an overview of the product and a high-level description of how it meets the security requirements of FIPS 140-2. This document contains details on the module's cryptographic keys and critical security parameters. This Security Policy concludes with instructions and guidance on running the module in a FIPS 140-2 mode of operation.

Maxar AEDS may also be referred to as the "module" in this document.

1.3 External Resources

The Maxar website (www.maxar.com) contains information on Maxar services and products. The Cryptographic Module Validation Program website contains links to the FIPS 140-2 certificate and Maxar contact information.

1.4 Notices

This document may be freely reproduced and distributed in its entirety without modification.

1.5 Acronyms

The following table defines acronyms found in this document:

Acronym	Term
AEDS	AES Encryption / Decryption System
AES	Advanced Encryption Standard
ANSI	American National Standards Institute
API	Application Programming Interface
AWS	Amazon Web Services
CA	Certificate Authority
CCSDS	Consultative Committee for Space Data Systems
CMVP	Cryptographic Module Validation Program
CO	Crypto Officer
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
DES	Data Encryption Standard
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
EC	Elliptic Curve
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GPC	General Purpose Computer
GUI	Graphical User Interface
HMAC	(Keyed-) Hash Message Authentication Code
HSM	Hardware Security Module
KAT	Known Answer Test
KO	Key Option
MAC	Message Authentication Code
MD	Message Digest
MMI	Machine-to-Machine Interface
NIST	National Institute of Standards and Technology
OS	Operating System
PKCS	Public-Key Cryptography Standards
PKG	Public Key Generation
PKV	Public Key Validation
PRNG	Pseudo Random Number Generator
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, and Adleman
SHA	Secure Hash Algorithm
SDLS	Space Data Link Security
SSL	Secure Sockets Layer
Triple-DES	Triple Data Encryption Algorithm
TLS	Transport Layer Security

Table 1 - Acronyms and Terms

2 Cryptographic Module Specification

The Maxar AEDS provides a dedicated implementation of the CCSDS Space Data Link Security (SDLS) protocol for spacecraft telecommand encryption and telemetry decryption using the Advanced Encryption Standard (AES).

The module is hardware Revision 1, which consists of firmware version 1.0.6.1558.2958 on an AIC TB116-AN server and is classified as a multi-chip standalone cryptographic module. The module also includes the embedded Nuvoton NPCT6XX series TPM 2.0 hardware module with firmware 1.3.0.1 validated to FIPS 140-2 under Cert. #2627 operating in FIPS mode.

The physical cryptographic boundary is defined as the outer case of the AIC TB116-AN server. The module runs on a non-modifiable operating environment. Photos of the AIC TB116-AN with the three (3) tamper-evident seals affixed by the manufacturer are depicted below in Figures 1 &2.

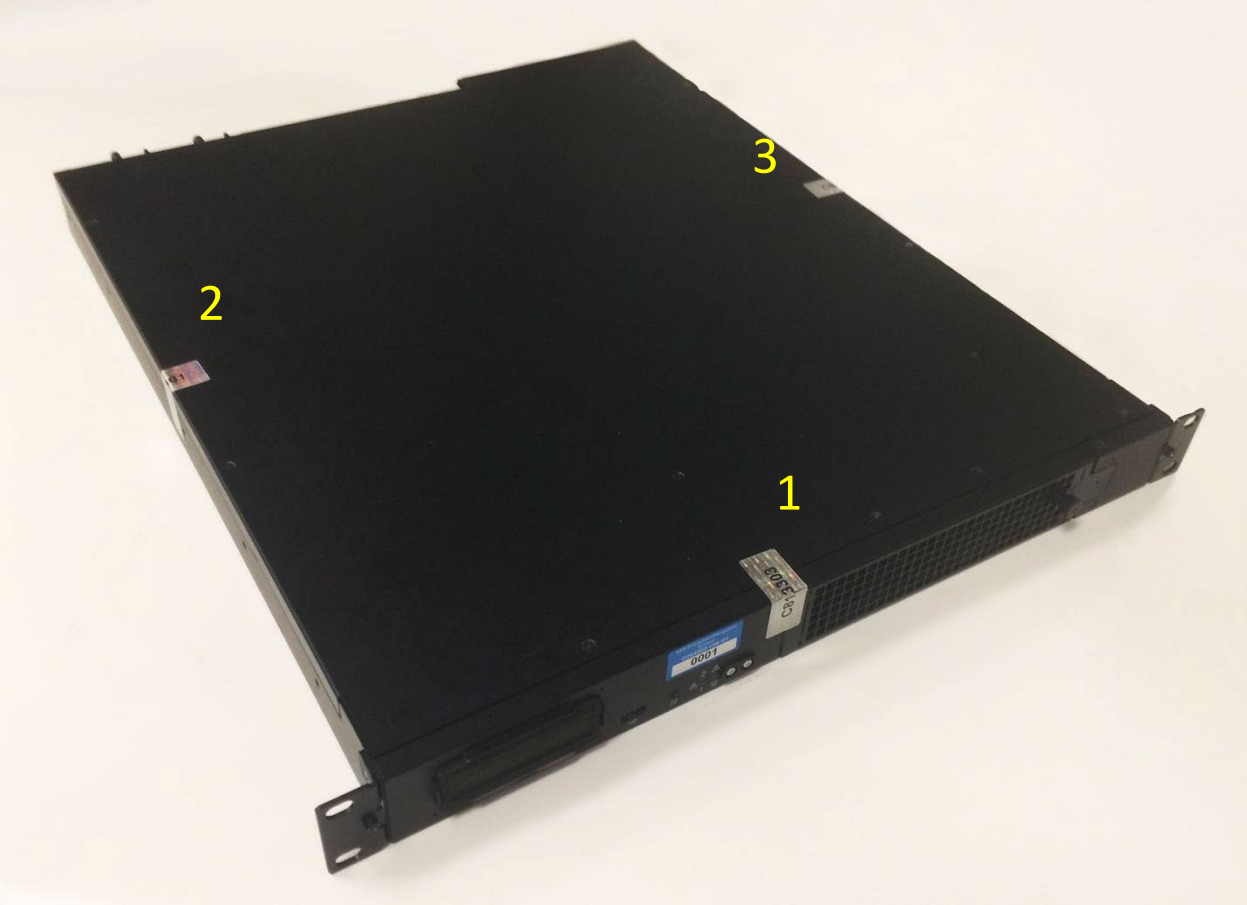

Figure 1 – Maxar AEDS (front) with Tamper-Evident Seals Locations

Figure 2 – Maxar AEDS (back) with Tamper-Evident Seals Locations

2.1 Validation Level Detail

The following table lists the level of validation for each area in FIPS 140-2:

FIPS 140-2 Section Title	Validation Level
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	2
Finite State Model	2
Physical Security	2
Operational Environment	N/A
Cryptographic Key Management	2
Electromagnetic Interference / Electromagnetic Compatibility	2
Self-Tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Table 2 - Validation level by FIPS 140-2 Section

2.2 Approved Cryptographic Algorithms

The following table lists all certificates issued by the Cryptographic Algorithm Validation Program for the module's embedded cryptographic algorithm implementations. Emphasis[1] in Table 3 (only) is added to those algorithms that are employed by the module.

Algorithm	CAVP Certificate
AES **ECB** (e/d; 128, 192, 256) ***CBC** (e/d; 128,* 192*, 256)* **CFB1** (e/d; 128, 192, 256) **CFB8** (e/d; 128, 192, 256) **CFB128** (e/d; 128, 192, 256) **OFB** (e/d; 128, 192, 256) ***CTR** (ext only; 128,* 192*, 256)* **CCM** (KS: 128, 192, 256) **CMAC** (Generation/Verification) (KS: 128, 192, 256) **XTS** (e/d; 128, 256) ***GCM** (KS: AES_128(e/d),* AES_192(e/d)*, AES_256(e/d))*[2] ***GMAC_Supported***	A2061
CVL (ECC CDH KAS) Curves (B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, *P-384*, P-521)	Component 2178
CVL KDF (SP 800-135 for TLS v1.0/1.1, and *TLS v1.2*)	C585
*SP 800-90A DRBG (*Hash_DRBG*,* HMAC_DRBG*, CTR_DRBG)*	A2061
DSA FIPS 186-4 **PQG Gen**: 2048 & 3072 (using SHA-2) **PQG Ver**: 1024, 2048 & 3072 (using SHA-1 and SHA-2) **Key Pair**: 2048-bit & 3072-bit **Sig Gen**: 2048-bit & 3072-bit (using SHA-2) **Sig Ver**: 1024-bit, 2048-bit & 3072-bit (using SHA-1 & SHA-2)	A2061
ECDSA FIPS 186-4 **PKG**: Curves (B-233, B-283, B-409 & B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521) **PKV**: Curves All P, K & B	A2061

[1] Algorithms in-use are *underlined and italic*. If only certain variants of an algorithm are in-use, only those variants will be *italic. [Note: this is only applicable to Table 3.]*

[2] 256 bits of entropy strength is claimed since the IV is generated internally

Sig Gen: (B-233, B-283, B-409 & B-571, K-233, K-283, K-409, K-571, P-224, P-256, P-384, P-521) (SHA-2) **Sig Ver**: Curves (B-163, B-233, B-283, B-409 & B-571, K-163, K-233, K-283, K-409, K-571, P-192, P224, P-256, P-384, P-521) (using SHA-1 and SHA-2)	
HMAC-SHA-1 (160-bit key), HMAC-SHA-224, *HMAC-SHA-256 (256-bit key)*, *HMAC-SHA-384 (384-bit key)*, HMAC-SHA-512	A2061
KAS-SSC ECC Domain Parameter Generation Methods: B-233, B-283, B-409, B-571, K-233, K-283, K-409, K-571, P-224, P-256, *P-384*, P-521 FCC Domain Parameter Generation Methods: FB, FC *CVL Cert. #C585; Key establishment methodology provides 192 bits of encryption strength.*	A2062
KTS *AES-GCM (key establishment methodology provides 128 or 256 bits of encryption strength)*	A2061
KTS *AES-CBC (with HMAC-SHA1, HMAC-SHA-256); key establishment methodology provides 128 or 256 bits of encryption strength)*	A2061
RSA (X9.31, PKCS #1.5, PSS) **FIPS 186-2** **ANSIX9.31** Sig Gen: 4096-bit (SHA-256, SHA-384, SHA-512) Sig Ver: 1024-bit, 1536-bit, 2048-bit, 3072-bit & 4096-bit (any SHA size) **PKCS1 V1 5** Sig Gen: 4096-bit (SHA-224, SHA-256, SHA-384, SHA-512) Sig Ver: 1024-bit, 1536-bit, 2048-bit, 3072-bit & 4096-bit (any SHA size) **PSS** Sig Gen: 4096-bit (SHA-224, SHA-256, SHA-384, SHA-512) Sig Ver: 1024-bit, 1536-bit, 2048-bit, 3072-bit & 4096-bit (any SHA size) **FIPS 186-4** **ANSIX9.31** Sig Gen: 2048-bit (using SHA-256, SHA-384, SHA-512) Sig Ver: 1024-bit, 2048-bit, 3072-bit & 4096-bit (any SHA size) ***PKCS1 V1 5*** *Sig Gen: 2048-bit &* 3072-bit *(SHA-256,* SHA-384, SHA-512*)*	A2061

Sig Ver: 1024-bit, *2048-bit*, 3072-bit & 4096-bit (*SHA-1*, SHA-224, *SHA-256*, *SHA-384*, SHA-512) **PSS** Sig Gen: 2048-bit & 3072-bit (SHA-256, SHA-384, SHA-512) Sig Ver: 1024-bit, 2048-bit, 3072-bit & 4096-bit (any SHA size)	
RSA FIPS 186-4 Key Gen: *2048*, 3072, 4096	A2090
SHA-1 (with HMAC only), SHA-224, *SHA-256*, *SHA-384*, SHA-512	A2061
Triple-DES **TECB** (KO 1 e/d) **TCBC** (KO 1 e/d) **TCFB1** (KO 1 e/d) **TCFB8** (KO 1 e/d) **TCFB64** (KO 1 e/d) **TOFB** (KO 1 e/d) **CMAC** (KS: 3-Key; Generation/Verification; Block Size(s): Full / Partial)	A2061

Table 3 - FIPS Approved Algorithm Certificates

The following Approved cryptographic algorithms are vendor affirmed as part of the validated embedded module.

Algorithm	IG Reference	Use
CKG	Vendor Affirmed IG D.12	[SP 800-133 Rev.2] Sections 5.1, 5.2, 5.3 and Sections 6.1, 6.2.1, 6.2.2, 6.5 The cryptographic module performs Cryptographic Key Generation (CKG) for symmetric keys and asymmetric seeds per NIST SP 800-133rev2 (vendor affirmed). The resulting symmetric key or asymmetric seed is an unmodified output from the Approved DRBG.

Table 4 - Approved Cryptographic Functions with Vendor Affirmations

2.3 Non-Approved but Allowed Algorithms

The module supports the following non-FIPS 140-2 approved but allowed algorithms that may be used in the Approved mode of operation.

Algorithm	Use
NDRNG	The module uses HW NDRNG which generates 384 bits (full entropy) of data to seed the DRBG during instantiation and 256 bits of data to reseed. (This complies with IG 7.14 Section 1.a.)
RSA Key Wrapping, Non-SP 800-56B compliant	Allowed until 2023.12.31 per FIPS140-2_IG - D.9: Key establishment using PKCS#1-v1.5 padding per Section 8.1 of RFC 2313 methodology provides 112 bits of encryption strength. Note: RSA key wrapping is used in TLS protocol implementation.

Table 5 - Non-Approved but Allowed Algorithms

2.4 Module Interfaces

The table below describes the active physical interfaces of the module:

Physical Interface	Description / Use
Gigabit Ethernet Port (6)	● Machine-to-Machine Interface (MMI) provides SDLS cryptographic services via TLS secure TCP/IP connection. Note that only TLS v1.2 is supported. ● Web-based User Interface (WebUI) provides initial module configuration & control via HTTP/2-over-TLS secure TCP/IP connection. Note that only TLS v1.2 is supported.
Power Interfaces (2)	Accept and provide power to the module
LEDs	● Power ● System ID ● System management alert ● Drive activity ● Network activity
USB port (front panel)	Accepts USB flash drive for key loading
USB ports (rear panel)	Accepts USB flash drive for key loading
Serial DB9 Port	Disabled
VGA port	Disabled
IPMI Port	Disabled

Table 6 - Interface Descriptions

The module provides a number of physical and logical interfaces to the device, and the physical interfaces provided by the module are mapped to four FIPS 140-2 defined logical interfaces: data input, data output, control input, and status output. The logical interfaces and their mapping are provided in the following table:

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input	Gigabit Ethernet Ports (6) USB Port
Data Output	Gigabit Ethernet Ports (6)
Control Input	Gigabit Ethernet Port
Status Output	Gigabit Ethernet Port LEDs LCD display
Power	Power Plug On/Off Switch

Table 7 - Logical Interface / Physical Interface Mapping

2.4.1 Interface Security

Communications over both the Machine-to-Machine Interface (MMI) and Web User Interface (WebUI) are secured by Transport Layer Security (TLS) version 1.2. For TLS, the GCM implementation meets Option 1 of IG A.5: it is used in a manner compliant with SP 800-52 and in accordance with Section 4 of RFC 5288 for TLS key establishment (refer to Section 2.4.1.1 for more detail). During operational testing, the module was tested against an independent version of TLS and found to behave correctly.

The TLS cipher suites supported for MMI and WebUI communications (in their IANA canonical forms) are as follows:

MMI

- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256

WebUI

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA

Note that all ECDHE ciphers use Elliptic Curve P-384 as defined in FIPS 186-4.

No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

2.4.1.1 Compliance to IG A.5

The AES GCM IV generation is in compliance with the RFC5288 and RFC5289 and shall only be used for the TLS protocol version 1.2 to be compliant with [FIPS140-2_IG] IG A.5, provision 1 (“TLS protocol IV generation”); thus, the module is compliant with [SP800-52].

The counter portion of the AES GCM IV is set by the module within its cryptographic boundary. When the IV exhausts the maximum number of possible values for a given session key, the first party to encounter this condition shall trigger a handshake to establish a new encryption key in accordance with RFC 5246.

In the event the nonce_explicit part of the IV exhausts the maximum number of possible values for a given session key, either party (the client or the server) that encounters this condition shall trigger a handshake to establish a new encryption key.

2.5 Roles, Services, and Authentication

As required by FIPS 140-2, there are two roles (a Crypto Officer role and User role) in the module that operators may assume. The module supports role-based authentication, and the respective services for each role are described in the following sections. The module does not support a Maintenance role.

2.5.1 Operator Services and Descriptions

The services available to the User and Crypto Officer roles in the module are as follows:

Service	Description	Service Input / Output	Interface	Key/CSP Access	Roles
WebUI TLS Session Init	Provides a protected session for module configuration	TLS Handshake / TLS Session Established	Gigabit Ethernet Port	TLS Session AES/HMAC Keys (WebUI), TLS ECDHE Key (WebUI), TLS Premaster Secret (WebUI), TLS Master Secret (WebUI), TLS Server Cert RSA Private Key (WebUI), Counter DRBG Entropy, Counter DRBG V Value (Seed Length), Counter DRBG Key, Counter DRBG init_seed	Crypto Officer
MMI TLS Session Init	Provides a protected session for SDLS-related cryptographic services	Initiate TLS session / TLS Session Established	Gigabit Ethernet Port	TLS Session AES/HMAC Keys (MMI), TLS Premaster Secret (MMI), TLS Master Secret (MMI), TLS Server Cert RSA Private Key (MMI), Counter DRBG Entropy, Counter DRBG V Value (Seed Length), Counter DRBG Key, Counter DRBG init_seed	User
MMI Channel Enable	Enable use of the MMI TLS Session Init service for User-role connections	Start MMI Channel / MMI Channel Enabled	Gigabit Ethernet Port (WebUI)	TLS Session AES/HMAC Keys (WebUI), SDLS AES Keys, SDLS AES Key Checksums	Crypto Officer

Service	Description	Service Input / Output	Interface	Key/CSP Access	Roles
MMI Channel Disable	Disconnect User-role MMI TLS Sessions and disable the MMI TLS Session Init service for User-role connections	Stop MMI Channel / MMI Channel Disabled	Gigabit Ethernet Port (WebUI)	TLS Session AES/HMAC Keys (WebUI), TLS Session AES/HMAC Keys (MMI), TLS Premaster Secret (MMI), TLS Master Secret (MMI), TLS Server Cert RSA Private Key (MMI)	Crypto Officer
Module Initialization	Performs *Module Integrity Tests* service and initializes the module for FIPS mode of operation	Power on Device / Module Initialization Complete	On/Off Switch	LUKS Partition AES Key	Crypto Officer
Configure	Configure critical security parameters within the module	Configuration Parameters / Module configured	Gigabit Ethernet Port (WebUI), USB Port	TLS Session AES/HMAC Keys (WebUI), TLS Server Cert RSA Private Key (MMI/WebUI), TLS Client Cert RSA Key, TLS Server CA RSA Private Key, SDLS AES Keys, SDLS AES Key Checksums, Counter DRBG Entropy, Counter DRBG V Value (Seed Length), Counter DRBG Key, Counter DRBG init_seed	Crypto Officer
Distribute MMI Credentials	Distribute TLS credentials for User-role MMI access	Initiate Download / Credentials Distributed	Gigabit Ethernet Port (WebUI)	TLS Session AES/HMAC Keys (WebUI), TLS Server Cert RSA Private Key (WebUI), TLS Client Cert RSA Key, TLS Client CA RSA Private Key	Crypto Officer
Module Integrity Tests	Performs integrity tests on module firmware and	Initiate Module Integrity Tests / Module Integrity Tests Completed	On/Off Switch	Firmware Integrity Data	User

Service	Description	Service Input / Output	Interface	Key/CSP Access	Roles
	security features				
SDLS AES Key Select	Loads an SDLS AES Key into RAM to use for cryptographic services	Key Index / Active SDLS AES Key Selected	Gigabit Ethernet Port (MMI)	TLS Session AES/HMAC Keys (MMI), SDLS AES Keys, SDLS AES Key Checksums, Active SDLS AES Key	User
SDLS AES Decrypt	Decrypts a block of SDLS protocol data	Initiate AES decryption / data decrypted	Gigabit Ethernet Port (MMI)	TLS Session AES/HMAC Keys (MMI), Active SDLS AES Key	User
SDLS AES Encrypt	Encrypts a block of SDLS protocol data	Initiate AES encryption/ data encrypted	Gigabit Ethernet Port (MMI)	Active SDLS AES Key, TLS Session AES/HMAC Keys (MMI)	User
Shutdown	Power off module to clear RAM and module state	Initiate Shutdown / Module Powered Down	Power Plug, On/Off Switch, Gigabit Ethernet Port (WebUI)	All CSPs stored in RAM	Crypto Officer
Reboot	Perform *Shutdown* service, power on machine and perform *Module Initialization* service	Initiate Reboot / Module state and RAM cleared	Gigabit Ethernet Port (WebUI)	TLS Session AES/HMAC Keys (WebUI/MMI), TLS Premaster Secret (WebUI/MMI), TLS Master Secret (WebUI/MMI), TLS ECDHE Key (WebUI), TLS Server Cert RSA Private Key (WebUI/MMI), Counter DRBG Entropy, Counter DRBG V Value (Seed Length), Counter DRBG Key, Counter DRBG init_seed	Crypto Officer
Factory Reset	Clear CSPs, restore factory settings, and perform *Reboot* service	Factory Reset Initiated /CSPs cleared from RAM and LUKS partition, new LUKS AES Key derived, module restored to factory settings	Gigabit Ethernet Port (WebUI)	All CSPs on LUKS Partition, All CSPs in RAM	Crypto Officer

Service	Description	Service Input / Output	Interface	Key/CSP Access	Roles
Show Status	Shows status of the module	Show status commands / Module status	Gigabit Ethernet Port (WebUI)	None	Crypto Officer

Table 8 - Operator Services

2.5.2 Crypto Officer Authentication

The Crypto Officer role authenticates via a 1 Gigabit Ethernet. Other than status functions available by viewing LEDs, the services described in the table above are available only to authenticated operators. The operator authenticates via plaintext username/password over a TCP/IP connection secured by TLS version 1.2 (see §3.2.1 for details). Session authorization is provided by a cryptographically signed JSON Web Token. Passwords are stored on the module. The module checks these parameters before allowing access. The module enforces a minimum password length of 12 characters. The password is required to contain at least three of the following four classes of characters: digits, uppercase letters, lowercase letters, and the set of other printable ASCII characters, yielding 95 choices per character. The probability of a successful random attempt is $1/95^{12}$, which is less than 1/1,000,000. The module enforces a 30-minute lockout after five (5) consecutive failed password attempts, so the probability of a success with multiple attempts in a one-minute period is $5/95^{12}$, which is less than 1/100,000.

The Maxar AEDS is delivered with a factory default password for Crypto Office authentication. The first action for the AEDS Crypto Officer will be to change the password in a manner that meets the password requirements in this section.

2.5.3 User Authentication

The module requires certificate-based TLS mutual authentication for the User-role machine-to-machine interfaces. A list of supported TLS cipher-suites is provided in §3.2.1. The module incorporates an internal Public Key Infrastructure (PKI) system with dedicated X509 Certificate Authorities (CA) for issuing and revoking server and client certificates, using 2048-bit RSA keys. A 2048-bit RSA key has 112 bits of equivalent strength. The probability of a successful random attempt is 1/2^112, which is less than 1/1,000,000. The module enforces a limit of 10 incoming connections per second on User-role TCP ports, so the probability of success with multiple consecutive attempts in a one-minute period is 600/2^112 which is less than 1/100,000.

2.6 Physical Security

The module is a multiple-chip standalone module and conforms to Level 2 requirements for physical security. The module's production-grade enclosure is made of a hard metal, and the enclosure contains a removable cover. The tamper-evident seals are affixed by the manufacturer as depicted in the photographs in Section 2.1 of this policy.

The tamper-evident seals must be affixed to the module in the locations as shown in Section 2.1 for the module to operate in the approved mode of operation.

2.7 Operational Environment

The module operates in a limited operational environment and does not implement a General-Purpose Operating System. The module meets Federal Communications Commission (FCC) FCC Electromagnetic Interference (EMI) and Electromagnetic Compatibility (EMC) requirements for business use as defined by 47 Code of Federal Regulations, Part15, Subpart B.

2.8 Cryptographic Key Management

The table below provides a list of Critical Security Parameters and Public Keys that are either inaccessible, or are only accessible with authentication:

Ref#	Keys and CSPs	Storage Locations	Storage Method	Key Establishment	Input Method	Output Method	Zeroization	Access
1	SDLS AES Keys	RAM	Plaintext	See (30)	Disk Read (SDLS AES Key Select, MMI Channel Enable), USB Key (Configure)	None	Shutdown	CO: WD U: WD
2	SDLS AES Key Checksums	RAM	Plaintext	See (31)	Disk Read (SDLS AES Key Select, MMI Channel Enable)	None	Shutdown	CO: WD U: WD
3	Active SDLS AES Key	RAM	Plaintext	See (30)	Disk Read (SDLS AES Key Select)	None	Reboot	CO: D U: WD
4	TLS Session AES/HMAC Keys (MMI)	RAM	Plaintext	[1,3] Derived from (6)	None	None	Reboot, MMI Channel Disable	CO: D U: RW
5	TLS Premaster Secret (MMI)	RAM	Plaintext	[1] Entry	From MMI client, encrypted by (40) (MMI TLS Session Init)	None	Reboot, MMI Channel Disable	CO: D U: RW
6	TLS Master Secret (MMI)	RAM	Plaintext	[1] Derived from (5)	None	None	Reboot, MMI Channel Disable	CO: D U: RW
7	TLS Server Cert RSA Private Key (MMI)**	RAM	Plaintext	See (23)	Disk Read (MMI TLS Session Init)	None	Reboot, MMI Channel Disable	CO: D U: W
8	TLS Session AES/HMAC Keys (WebUI)	RAM	Plaintext	[2,3] Derived from (10)	None	None	Reboot	CO: RWD
9	TLS Premaster Secret (WebUI)	RAM	Plaintext	[2] Derived from (12)	None	None	Reboot	CO: RWD

10	TLS Master Secret (WebUI)	RAM	Plaintext	[2] Derived from (9)	None	None	Reboot	CO: RWD
11	TLS Server Cert RSA Private Key (WebUI)†	RAM	Plaintext	See (24)	Disk Read (WebUI TLS Session Init)	None	Reboot	CO: WD
12	TLS ECDHE Private Key (WebUI)**	RAM	Plaintext	Generated (TLS Handshake)	None	None	Reboot	CO: WD
13	JSON Web Token HMAC Key	RAM	Plaintext	Generated (DRBG)	None	None	Reboot	CO: WD
14	LUKS Partition AES Key	RAM	Plaintext	See (32)	Disk Read	None	Shutdown	CO: WD
15	Firmware Integrity Data	RAM	Plaintext	See (33)	Disk Read (Module Integrity Tests)	None	Module Integrity Tests Completed	CO: WD
16	TLS Client Cert RSA Public Key††	RAM	Plaintext	See (26)	TCP (MMI TLS Session Init), Disk Read (Distribute MMI Credentials)	CO download encrypted by (8)	Shutdown	CO: RWD
17	TLS Client Cert RSA Private Key	RAM	Plaintext	See (25)	Disk Read (Distribute MMI Credentials)	CO download encrypted by (8)	Shutdown	CO: RWD
18	TLS Server CA RSA Private Key†	RAM	Plaintext	See (27)	Disk Read (Configure)	None	Reboot	CO: WD
19	TLS Client CA RSA Private Key†	RAM	Plaintext	See (28)	Disk Read (DistributeMMI Credentials)	None	Reboot	CO: WD
20	TLS Root CA RSA Private Key†	RAM	Plaintext	See (29)	Disk Read (Factory Reset)	None	Reboot	CO: WD
21	TLS Client Cert RSA Public Key	Disk	Plaintext	See (26)	Disk Copy (Distribute MMI Credentials)	None	Factory Reset	CO: WD

22	TLS Client Cert RSA Private Key	Disk	Plaintext	See (24)	Disk Copy (Distribute MMI Credentials)	None	Factory Reset	CO: WD
23	TLS Server Cert RSA Private Key (MMI)	LUKS partition	Encrypted	Generated	None	None	Factory Reset	CO: WD
24	TLS Server Cert RSA Private Key (WebUI)	LUKS partition	Encrypted	Generated	None	None	Factory Reset	CO: WD
25	TLS Client Cert RSA Private Key	LUKS partition	Encrypted	Generated	None	None	Factory Reset	CO: WD
26	TLS Client Cert RSA Public Key	LUKS partition	Encrypted	Generated	None	None	Factory Reset	CO: WD
27	TLS Server CA RSA Private Key	LUKS partition	Encrypted	Generated	None	None	Factory Reset	CO: WD
28	TLS Client CA RSA Private Key	LUKS partition	Encrypted	Generated	None	None	Factory Reset	CO: WD
29	TLS Root CA RSA Private Key	LUKS partition	Encrypted	Generated	None	None	Factory Reset	CO: WD
30	SDLS AES Keys	LUKS partition	Encrypted	Entry	Disk Write (Configure)	None	Factory Reset	CO: WD
31	SDLS AES Key Checksums	LUKS partition	Encrypted	Entry	Disk Write (Configure)	None	Factory Reset	CO: WD
32	LUKS Partition AES Key	TPM	Encrypted	Generated (DRBG)	None	None	Factory Reset	CO: WD
33	Firmware Integrity Data	Disk	Plaintext	Pre-loaded	None	None	None	
34	Counter DRBG Entropy	RAM	Plaintext	Generated (NDRNG)	None	None	Reboot	CO: D U: W
35	Counter DRBG V	RAM	Plaintext	Generated (NDRNG)	None	None	Reboot	CO: D

	Value (Seed Length)							
36	Counter DRBG Key	RAM	Plaintext	Generated (NDRNG)	None	None	Reboot	CO: D U: W
37	Counter DRBG init_seed	RAM	Plaintext	Generated (NDRNG)	None	None	Reboot	CO: D

R = Read W = Write D = Delete

** = RSA/ECDH Decryption Key † = RSA Signature Generation Key †† = RSA Signature Verification Key

[1] See IETF RFC 5246 §8.1.1

[2] See IETF RFC 5246 §8.1.2

[3] See IETF RFC 5288 §4

Table 9 - Module Protected Keys / CSPs

The table below provides a list of Critical Security Parameters that are accessible without authentication:

Ref #	Keys and CSPs	Storage Locations	Storage Method	Key Establishment	Input Method	Output Method	Zeroization
38	TLS Server Cert RSA Public Key (WebUI)	RAM	Plaintext	See (44)	Disk Read	TCP	Reboot
39	TLS ECDHE Public Key (WebUI)	RAM	Plaintext	Generated (TLS Handshake)	None	TCP	Reboot
40	TLS Server Cert RSA Public Key (MMI)	RAM	Plaintext	See (44)	Disk Read	TCP	Reboot
41	TLS Server CA RSA Public Key (MMI)	RAM	Plaintext	See (45)	Disk Read	TCP	Reboot
42	TLS Client CA RSA Public Key (MMI)††	RAM	Plaintext	See (46)	Disk Read	TCP	Reboot
43	TLS Root CA RSA Public Key (MMI)††	RAM	Plaintext	See (47)	Disk Read	TCP	Reboot
44	TLS Server Cert RSA Public Key (MMI,WebUI)	LUKS partition	Encrypted	Generated	None	None	Factory Reset
45	TLS Server CA RSA Public Key	LUKS partition	Encrypted	Generated	None	None	Factory Reset
46	TLS Client CA RSA Public Key	LUKS partition	Encrypted	Generated	None	None	Factory Reset
47	TLS Root CA RSA Public Key	LUKS partition	Encrypted	Generated	None	None	Factory Reset

R = Read W = Write D = Delete

†† = RSA Signature Verification Key

Table 10 - Module Public Keys / CSPs

2.9 Self-Tests

FIPS 140-2 requires the module to perform self-tests to ensure the integrity of the module and the correctness of the cryptographic functionality at start up. In addition, some functions require on-going verification of function, such as the random number generator. All these tests are listed and described in this section. In the event of a self-test error, the module will log the error and will halt. The module must be rebooted to resume function.

The following sections discuss the module's self-tests in more detail.

2.9.1 Power-On Self-Tests

Power-on self-tests are run upon the initialization of the module and do not require operator intervention to run. If any of the tests fail, the module will not initialize. The module will enter an error state and no services can be accessed by the operator. The module implements the following power-on self-tests:

TYPE	DETAIL	PASS/FAIL CRITERIA
Firmware Integrity Check	• SHA-256 •	**Pass** LCD Output: SWINTEGRITY CHECK PASSED **Fail** LCD Output: SWINTEGRITY CHECK FAILED
Known Answer Tests[3]	• AES encrypt/decrypt (all modes) • Triple-DES encrypt/decrypt (all modes) • ECDH P-224 KAT (Shared secret calculation per SP 80056A §5.7.1.2, IG 9.6) HMAC-SHA-1 • HMAC-SHA-224 • HMAC-SHA-256 • HMAC-SHA-384 • HMAC-SHA-512 • RSA sign/verify using 2048 bit key, SHA-256, PKCS#1 • SHA-1 • SP 800-90 DRBG (Hash_DRBG, HMAC_DRBG, CTR_DRBG) (Instantiate, Generate, and Reseed Health Test Functions)	**Pass** LCD Output: FIPS SELFTEST PASSED **Fail** LCD Output: FIPS SELFTEST FAILED
Pair-wise Consistency Tests	• DSA sign/verify using 2048 bit key, SHA-384 • RSA sign/verify using 2048 bit key, SHA-256, PKCS#1 • ECDSA keygen/sign/verify using P-224, K-233 and SHA-512	

Table 11 - Power-On Self Tests

Each module performs all power-on self-tests automatically when the module is initialized. All power-on self-tests must be passed before a User/Crypto Officer can perform services. The Power-on self-tests can be run on demand by rebooting the module in FIPS approved Mode of Operation.

[3] Note that all SHA-X KATs are tested as part of the respective HMAC SHA-X KAT.

2.9.2 Conditional Self-Tests

Conditional self-tests are tests that run on an automatic and on-going basis during operation of the module. If any of these tests fail, the module will enter an error state, where no services can be accessed by the operators. The module can be re-initialized to clear the error and resume FIPS mode of operation. Each module performs the following conditional self-tests:

TYPE	DETAIL
Pair-wise Consistency Tests	• DSA • RSA • ECDSA
Continuous RNG Tests	• Performed on all approved DRBGs (including the NDRNG)
Key Entry Test	• CRC on key load

Table 12 - Conditional Self-Tests

The module does not perform a firmware load test because no additional firmware can be loaded in the module. Please see Section 3 for guidance on configuring and maintaining FIPS mode.

2.10 Mitigation of Other Attacks

The module does not mitigate other attacks.

3 Guidance and Secure Operation

The module only supports FIPS-mode of operation. Beyond initial setup, no specific technical steps are required to configure FIPS-mode of operation. There are no means for a User or the Crypto Officer to take the Maxar AEDS out of FIPS-mode.

3.1 Crypto Officer Guidance

The Crypto Officer must configure and enforce the following initialization procedures in order to operate in FIPS approved mode of operation:

- Verify that the firmware version of the module is Version 1.0.6.1558.2958. No other version can be loaded or used in FIPS mode of operation.
- Users of the module should monitor for evidence of tampering as directed by their local Facility Security Plan or other governing local instructions. If evidence of tampering is noted, users should follow local procedures for reporting possible compromise of cryptographic material.
- Do not disclose passwords and store passwords in a safe location and according to their organization's systems security policies for password storage.

3.2 User Guidance

No additional guidance is required to maintain FIPS mode of operation.