Shanghai Muge Technology Co., Ltd

GM01 FIPS 140-2 Non-Proprietary SECURITY POLICY

DocumentRevision: 1.0
H.W.Version: 1.0.0
F.W.Version: 1.0.0

REVISION HISTORY

Author(s)	Version	Updates
Chaoyi Ding	**V1.0**	**09.10.2021**

Shanghai MugeTechnology Co., Ltd
Address: J, building 1, No. 2222, Huancheng Road, Jiading District, Shanghai, China 201899
Phone: +86-021-39883510
Website: http://www.screenr-s.com/

Table of Contents

INTRODUCTION

The Shanghai Muge Technology Co., Ltd GM01Cryptographic Module (H.W. Version: 1.0.0; F.W. Version:1.0.0) is a multi-chip embedded cryptographic module designed to decrypt and decode audio/video data for a digital cinema projector.

CRYPTOGRAPHIC BOUNDARY

The cryptographic boundary is defined by the outer perimeter of the main board's PCB. It is outlined in yellow in the below picture. And all security relevant components are enclosed within black metal enclosure in red frame as below:

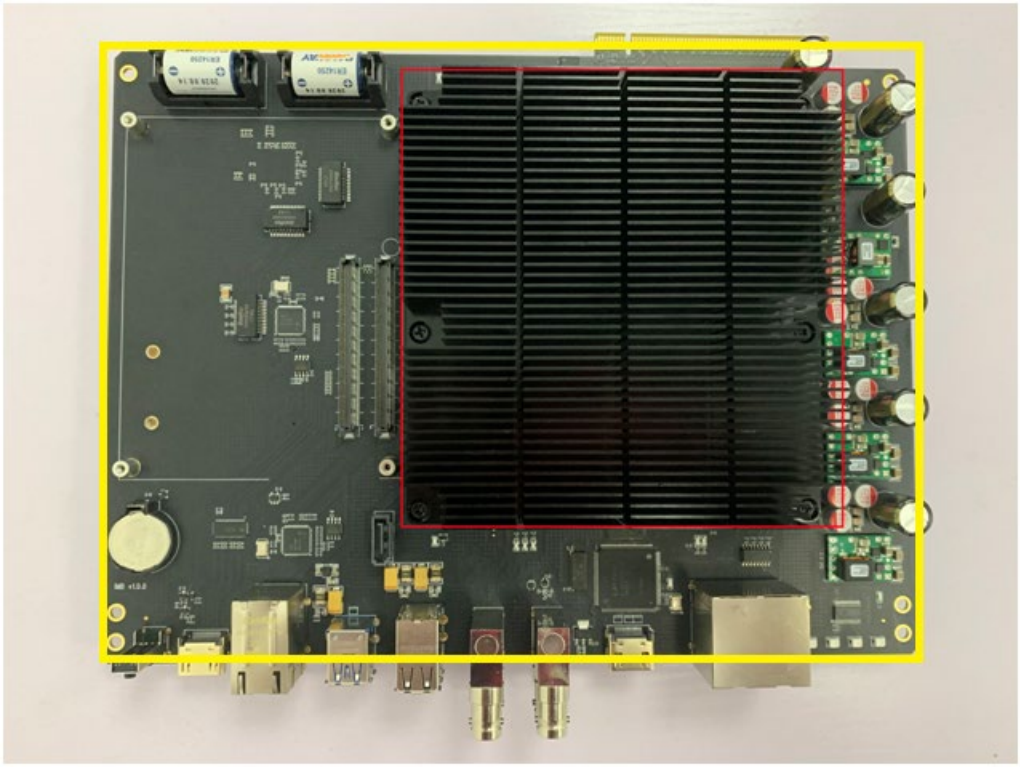

Exhibit 1- Top View of the cryptographic boundary

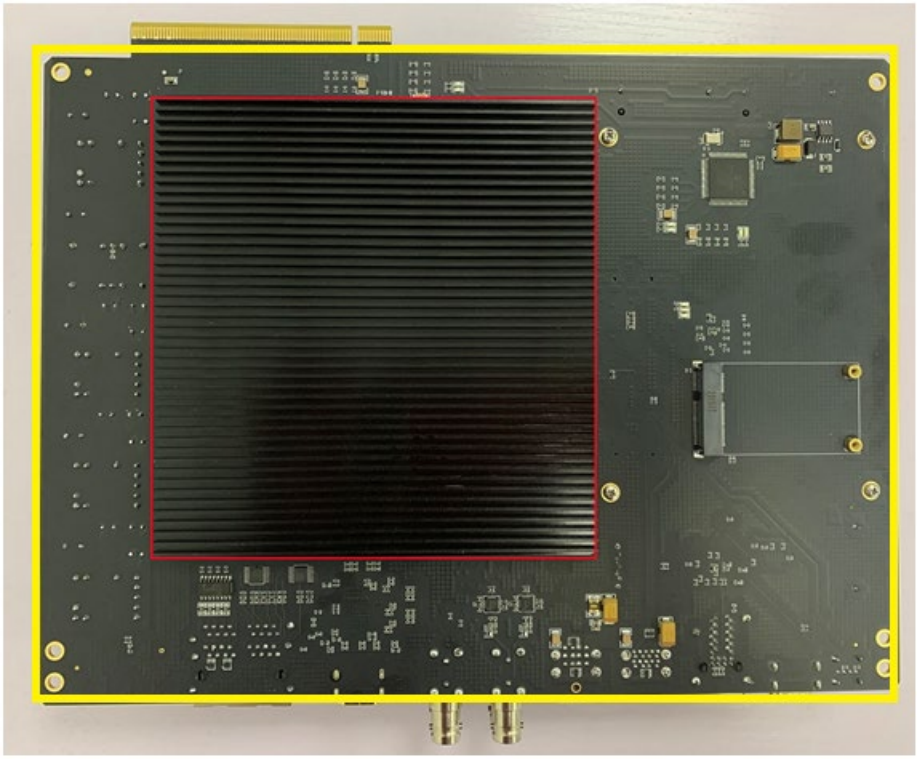

Exhibit 2 – Bottom View of the cryptographic boundary

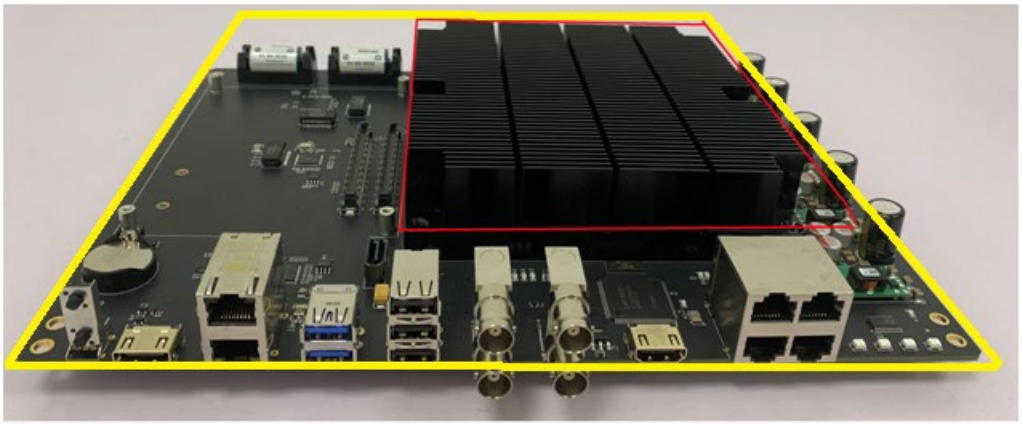

Exhibit 3- Front View of the cryptographic boundary

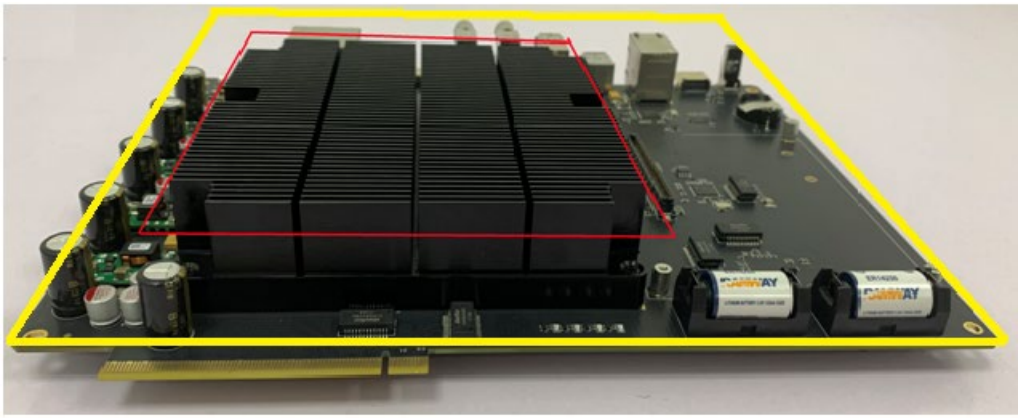

Exhibit 4- Back View of the cryptographic boundary

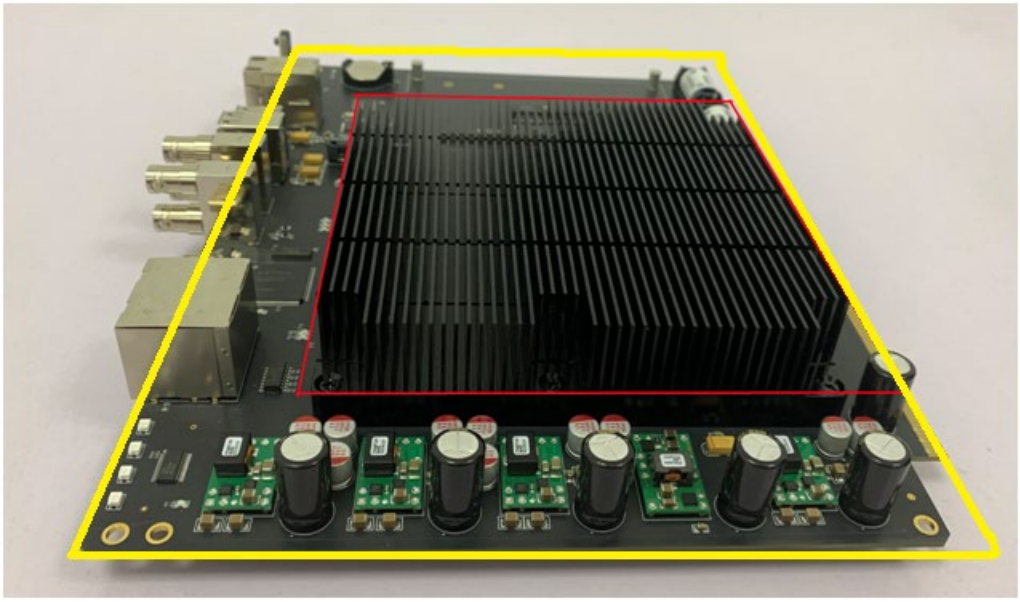

Exhibit 5- Right View of the cryptographic boundary

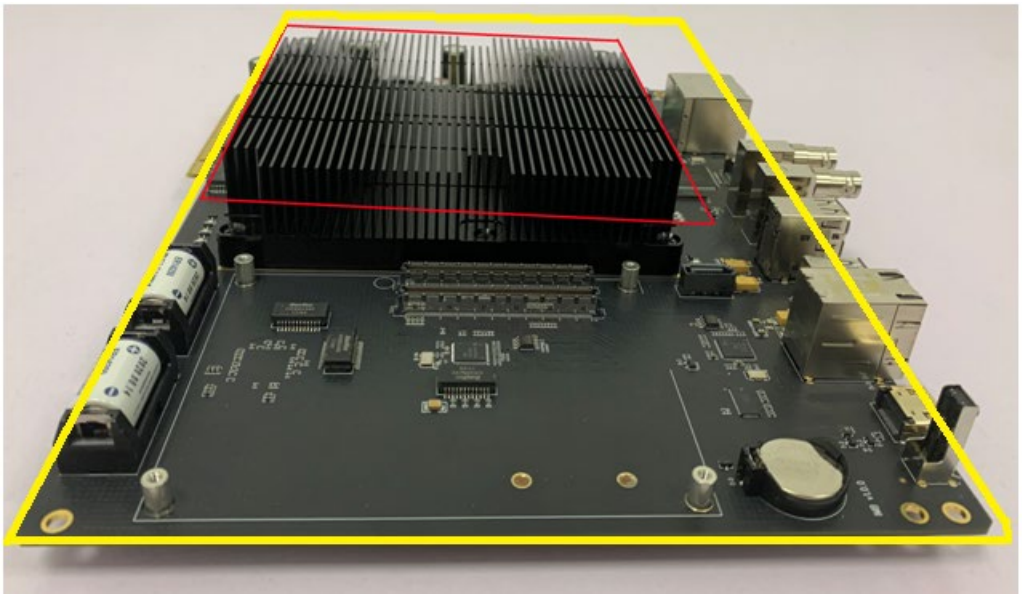

Exhibit 6- Left View of the cryptographic boundary

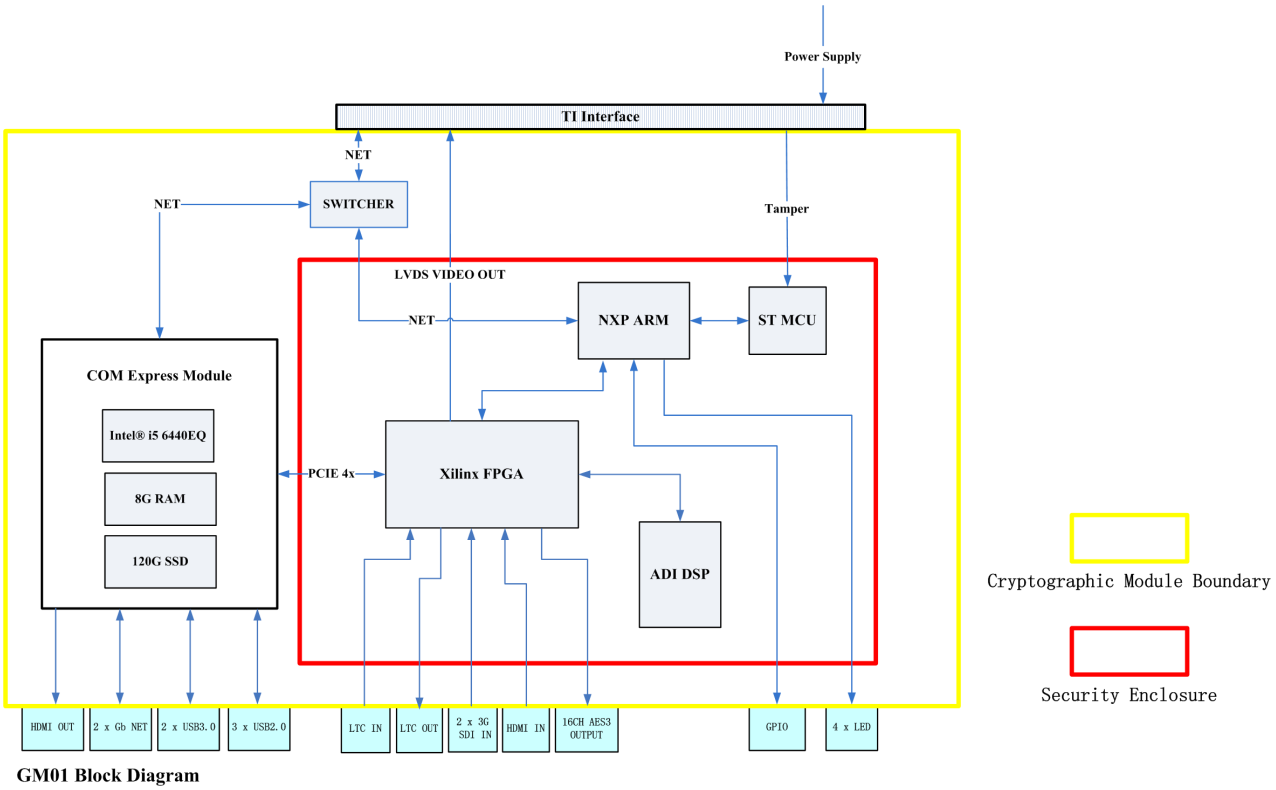

Exhibit 7- Block Diagram of GM01

The excluded components list includes capacitors, resistors, connectors, diodes, inductors, triodes, crystals and fuse, and those components are all outside of security enclosure and not security relevant components. So these excluded components do not harm the security functions of the

module, both from FIPS 140-2 and DCI standpoints. Therefore they are explicitly excluded from FIPS 140-2 requirements.

SECURITY LEVEL SPECIFICATION

The cryptographic module GM01 meets the overall requirements applicable to Level 2 security of FIPS 140-2:

SECURITY REQUIREMENTS AREA	LEVEL
Cryptographic Module Specification	2
Cryptographic Module Ports and Interfaces	2
Roles, Services, and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	3
Self-tests	2
Design Assurance	2
Mitigation of Other Attacks	N/A

Exhibit 8 – GM01 Security Level Table.

PHYSICAL PORTS AND LOGICAL INTERFACES

The module is a multi-chip embedded module with ports and interfaces as shown below:

PHYSICAL PORT	LOGICAL INTERFACE
• eSATA (Qty.1) • USB 3.0 (Qty.2) • USB 2.0 (Qty.3) • HDMI In(Qty.1) • SDI In(Qty.2) • LTC In(Qty.1) • GPI(Qty.1)	Data Input
• Reset Button (Qty.2) • Ethernet (Qty.2)	Control Input
• HDMI Output(Qty.1) • AES3 Audio Output(Qty.2) • LTC out (Qty.1) • GPO(Qty.1) • LVDS (Qty.1)	Data Output
• Status LEDs (Qty.4) • Ethernet (Qty.2)	Status Output
• Battery (Qty.2) • Button Battery (Qty.1) • Power Supply	Power

Exhibit9–Specification of Cryptographic Module Physical Ports and Logical Interfaces

SECURITY RULES

The following specifies the security rules under which the cryptographic module shall operate:

1. The cryptographic module provides two distinct operator roles: User role and the Cryptographic Officer role.
2. The cryptographic module provides identity-based authentication.
3. The cryptographic module clears previous authentications on power cycle.
4. When the module has not been placed in a valid role, the operator does not have access to any cryptographic services.
5. The cryptographic module performs the following tests:

   If the self-test fail, then the 4 LED lights will be:

   LED #1: Green
   LED #2: Red
   LED #3: Off
   LED #4: Off

   A. Power up Self-Tests

      1）Firmware Cryptographic algorithm tests:
      a. RSA 2048-bit Sign/Verify KAT
      b. SHA (SHA-256) KAT

      2）STM32L4A6VG Cryptographic algorithm tests:
      a. RSA 2048-bit SigGen/SigVer/KeyGen KAT
      b. SHA (SHA-256) KAT

      3） Firmware Integrity Test (CRC-32)

   B. Conditional Self-Tests

      1) Firmware Load Test(RSA-2048 Signature Verification)

6. The operator is capable of commanding the module to perform the power-up self-test by cycling power or resetting the module.
7. Power-up self-tests do not require any operator action.
8. Data output is inhibited during key generation, self-tests, zeroization, and error states.
9. There are no restrictions on which keys or CSPs are zeroized by the zeroization service.
10. The module does not support concurrent operators.
11. The module does not support a maintenance interface or role.
12. The module does not support manual key entry.

Modes of Operation

The module provides a FIPS Approved mode of operation and a non-Approved mode of operation. In the FIPS Approved mode of operation, the module only provides the "FW Upgrade" service. The module is in the non-approved mode of operation whenever the Non-Approved Services in exhibit 14 are invoked.

The module will enter FIPS Approved mode of operation following successful power up self-tests, and will signal this via a green LED in the following manner:
LED #1: Green
LED #2: Green
LED #3: Off
LED #4: Off

CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS

The following is a list of Public Keys that are available to each of the authorized roles via the corresponding services. The module does not support CSPs or Private Keys in the FIPS Approved mode.

Public Key

Description	Type	Generation	Storage
CO/User Public Key Public keys used to authenticate Cryptographic Officer and User Roles	RSA2048-bit	N/A – Externally Generated	Plaintext in flash memory and DRAM

Exhibit 10– Public Keys List

IDENTIFICATION AND AUTHENTICATION POLICY

The cryptographic module shall support two distinct operator roles: User and Cryptographic-Officer. The Cryptographic-Officer installs the cryptographic module, and the User is the operator of the module in the field. The cryptographic module shall enforce the separation of roles using identity-based operator authentication by means of RSA 2048 with SHA-256 digital signature verifications.

ROLE	AUTHENTICATION TYPE	AUTHENTICATION DATA
Cryptographic Officer	Identity-based operator authentication	Digital Signature Verification (RSA 2048 with SHA-256)
User	Identity-based operator authentication	Digital Signature Verification (RSA 2048 with SHA-256)

Exhibit11-Roles and Required Identification and Authentication
(FIPS 140-2 Table C1)

Strengths of Authentication Mechanisms

AUTHENTICATION MECHANISM	STRENGTH OF MECHANISM
RSA 2048-bit Digital Signature Verification	The probability that a random attempt will succeed, or a false acceptance will occur, is $1/2^{112}$, which is less than 1/1,000,000. We have measured the performance of the processor and calculated that RSA 2048-bit Digital Signature Verification can be performed 400 times per 1 minute. So the probability of success or false acceptance within a one minute period is $400/2^{112}$, which is less than 1/100,000.

Exhibit12- Strengths of Authentication Mechanisms
(FIPS 140-2 Table C2)

ROLES AND SERVICES

FIPS-Approved mode of service:

R: Read Access

E: Execute Access

ROLE	SERVICE	Descriptions	Key/CSP	Access	Approved Algorithms
Cryptographic Officer/User	FW Update: Updates the firmware of the module.	Upgrade Firmware	CO/User Public key	RE	RSA 2048SHA 256

Exhibit13-Approved mode of service

Below are the list of roles, services and algorithms used in the non-Approved mode of operation:

ROLES	SERVICES	DESCRIPTIONS	NON-APPROVED ALGORITHMS
Cryptographic Officer/User	Role Authentication Login/logout	Login and logout service	DRBG(Non-Compliant) NDRNG (Non-Compliant) RSA 2048(Non-Compliant) AES-128-CBC(Non-Compliant) HMAC-SHA-1(Non-Compliant) SHA-1(Non-Compliant) SP800-135 TLS v1.0 KDF(Non-Compliant)
User	System Management SetConfig/GetConfig GetSMTime/AdjustSMTime GetCert GetIMBVersionInfo GetSMStatusInfo	System Management functions for the module	DRBG(Non-Compliant) NDRNG (Non-Compliant) RSA 2048(Non-Compliant) AES-128-CBC(Non-Compliant) HMAC-SHA-1(Non-Compliant) SHA-1(Non-Compliant) SP800-135 TLS v1.0 KDF(Non-Compliant)
User	KDM Management KDMs Validate Delete KDM	Service for managing KDM information	DRBG(Non-Compliant) NDRNG (Non-Compliant) RSA 2048(Non-Compliant) AES-128-CBC(Non-Compliant) HMAC-SHA-1(Non-Compliant) SHA-1(Non-Compliant) SP800-135 TLS v1.0 KDF(Non-Compliant)

User	CPL Management CPLsValidate PurgeCpl	Service for managing CPL information	DRBG(Non-Compliant) NDRNG (Non-Compliant) RSA 2048(Non-Compliant) AES-128-CBC(Non-Compliant) HMAC-SHA-1(Non-Compliant) SHA-1(Non-Compliant) SP800-135 TLS v1.0 KDF(Non-Compliant)
User	Play Management StartPlay StopPlay CheckKDMValidityPeriod FrameSequencePlay VerifyEssenseFrame GPIOInput GPIOOutput	Service for managing Play	DRBG(Non-Compliant) NDRNG (Non-Compliant) RSA 2048(Non-Compliant) AES-128-CBC(Non-Compliant) HMAC-SHA-1(Non-Compliant) SHA-1(Non-Compliant) SP800-135 TLS v1.0 KDF(Non-Compliant)
User	Log Management GetLog	Service for retrieving log data	DRBG(Non-Compliant) NDRNG (Non-Compliant) RSA 2048(Non-Compliant) AES-128-CBC(Non-Compliant) HMAC-SHA-1(Non-Compliant) SHA-1(Non-Compliant) SP800-135 TLS v1.0 KDF(Non-Compliant)
User	Marriage Management StartMarriage ClearTamper	Verify projector marriage	DRBG(Non-Compliant) NDRNG (Non-Compliant) RSA 2048(Non-Compliant) AES-128-CBC(Non-Compliant) HMAC-SHA-1(Non-Compliant) SHA-1(Non-Compliant) SP800-135 TLS v1.0 KDF(Non-Compliant)
Cryptographic Officer	Zeroization: Actively destroys all CSPs contained within the module in the non-approved mode of operation.	Zeroize CSPs	N/A

Exhibit 14– Non-Approved Services for Roles and algorithms (FIPS 140-2 Table C3, Table C4)

ALGORITHMS

APPROVED ALGORITHMS

The cryptographic module supports the following Approved algorithms in the FIPS approved mode of operation, the following CAVP Certificates test a superset of algorithms, however only those algorithms and modes specified explicitly in Exhibit 15 below are implemented as approved:

CAVP CERT	ALGORITHM	STANDARD	MODE	KEY LENGTHS OR MODULI	USE
Cert. #C1768	RSA	FIPS 186-4	SHA-256 PKCS1 v1.5 SigVer	2048 bits	FW Upgrade(Digital Signature verification)
Cert. #C1768	SHS	FIPS 180-4	SHA-256	N/A	FW Upgrade (Message Digest)

Exhibit 15– Table of Approved Algorithms

Non-APPROVED ALGORITHMS

The following are the non-Approved Algorithms only supported during the non-Approved mode of operation:

ALGORITHM	MODE	KEY LENGTHS, OR MODULI	USE
AES (non-compliant)	CBC	128 bits	Data Decryption
HMAC (non-compliant)	HMAC-SHA-1	112 bits	Message Authentication
AES (non-compliant)	CBC	128 bits	Data Encryption /Decryption
HMAC (non-compliant)	HMAC-SHA-1	112bits	Message Authentication
KDF (non-compliant)	N/A	N/A	Key Derivation
DRBG (non-compliant)	HMAC-SHA-1	N/A	Deterministic Random Bit Generation
HMAC(non-compliant)	HMAC-SHA-1	112bits	Message Authentication
RSA(non-compliant)	N/A	2048bits	Key Transport
NDRNG (non-compliant)	N/A	N/A	Non Deterministic Random Number Generator (NDRNG) used to seed the DRBG

Exhibit 16– Table of non-Approved Algorithms

UNAUTHENTICATED SERVICES

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

• Self-tests: This service executes the suite of self-tests required by FIPS 140-2 and is invoked by power cycling or resetting the device.

• Get Status: This service provides module status via LEDs.

• Zeroization: This service is automatically triggered when the module detects a tamper.

PHYSICAL SECURITY POLICY

Physical Security Mechanisms:

1. The cryptographic module includes the following physical security mechanisms:
2. The entire security module that needs protection is covered by a security enclosure. The top and bottom of the module are covered by this metal rectangular material and respectively pressure twelve micro switches. The security enclosure is fixed with the PCB using screws. The micro switches are connected to microcontroller input signal.
3. Tamper evident seals are located between the security enclosure and the PCB. Cryptographic Officer and User must inspect tamper or destruction of the seals. If such evidence is found, the operator should not use the module.
4. The security protection module mainly consists of the microcontroller unit, button battery and power supply circuit. When the security enclosure is removed or displaced, the micro switch changes will be transferred to the microcontroller unit which triggers the zeroization function. The button cell supplies power to the related circuit when the power supply circuit is not available. The microcontroller unit clears CSPs stored in its internal cache and records this attack (e.g. event, event types, etc.). If the module was zeroized, the user should return it to manufacturer.

PHYSICAL SECURITY MECHANISMS	RECOMMENDED FREQUENCY OF INSPECTION/TEST	INSPECTON/TEST GUIDANCE DETAILS
Hard Opaque Enclosure	At startup or reboot of the module; perform checks as often as defined by vendor's organizational policy.	Inspect for scratches or deformation of the metal enclosure. If such evidence is found, the user should not use the module.
Tamper Evident Seals		Inspect for destruction of the seals. If such evidence is found, the user should not use the module.
Zeroization		If the module was zeroized, the user should return it to manufacturer

Exhibit 17- Inspection/Testing of Physical Security Mechanisms(FIPS 140-2 Table C5)

The module requires quantity 6 tamper labels, and the labels placements are indicated below: TEL

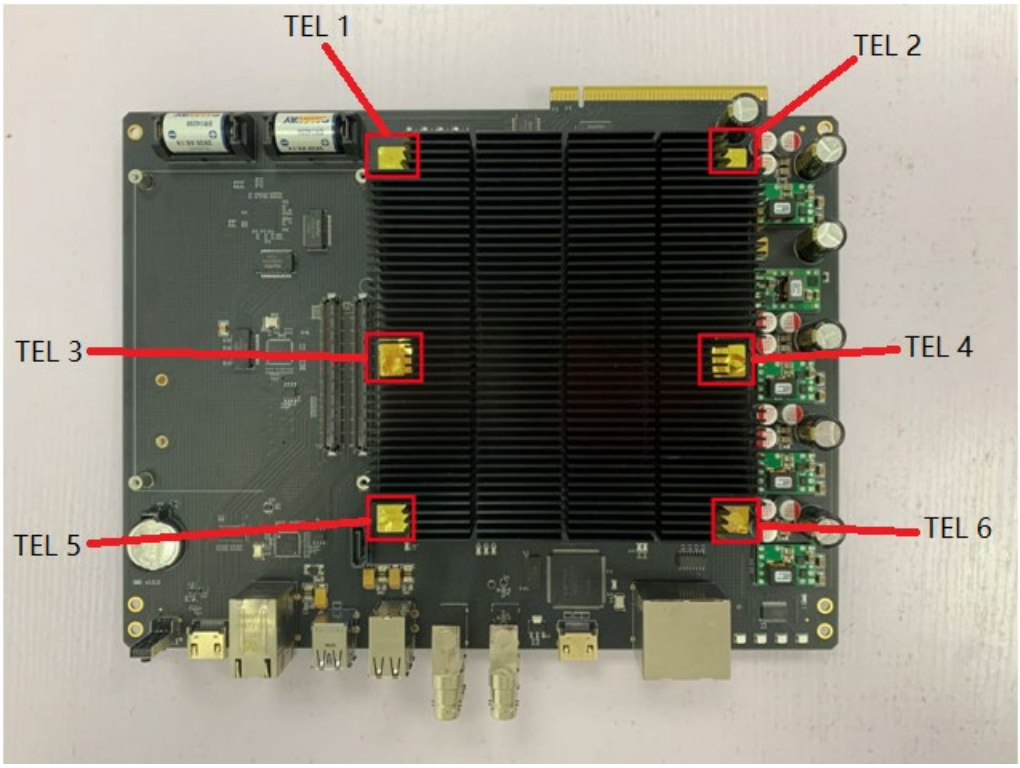

Exhibit 18–Tamper labels placements on GM01 module

MITIGATION OF OTHER ATTACKS POLICY

The module does not support mitigation of other attacks.

OTHER ATTACKS	MITIGATION MECHANISM	SPECIFIC LIMITATIONS
N/A	N/A	N/A

Exhibit 19– Table of Mitigation of Other Attacks (FIPS 140-2 Table C6)