Standalone IMB Security Policy
GDC Technology (USA), LLC

Version 1.2

June 14, 2013

TABLE OF CONTENTS

1. Module Overview

The Standalone IMB cryptographic module (Firmware Version 2.0, Security Manager Firmware Version 1.3.0; Hardware Version: GDC- IMB-v2, R8 and R9), hereafter referred to as the cryptographic module or module, is a Security Processor Block, Type 1, designed in accordance with FIPS 140-2 and the Digital Cinema Initiatives (DCI) Digital Cinema System Specification. For FIPS 140-2 purposes, the IMB is defined as a multi-chip embedded cryptographic module encased in a hard, opaque removable enclosure with tamper detection and response circuitry.

The images below depict the cryptographic module; all components not contained within the metal enclosure are explicitly excluded from the requirements of FIPS 140-2 as they are non-security relevant and have no impact on the overall security of the module. Excluded items fall into the following non-security relevant categories:

- Power Supply
- Unconnected Components and Test Points
- Mechanical Connections
- Video and Audio Components

Figure 1 – Image of the GDC-IMB-v2 (Top)

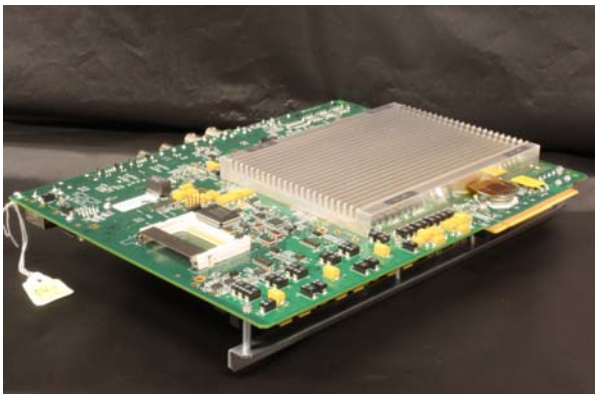

Figure 2 – Image of the GDC-IMB-v2 (Bottom)

2. Security Level

The cryptographic module meets the overall requirements applicable to FIPS 140-2 Level 2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
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	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The module only supports an Approved mode of operation and supports the following Approved algorithms:

- AES-128 CBC, Decrypt only (Cert. #2148)
- AES 128, 192, 256 ECB, CBC, CFB8, CFB128, OFB modes (Cert. #2149)
- SHA-1 (Cert. #1869)
- SHA-1, -224, -256, -384, -512 (Cert. #1870)
- RNG ANSI X9.31 (Cert. #1100)
- FIPS 186-2 RSA Key Gen, Sign/Verify 2048 bit keys (Cert. #1105)
- HMAC-SHA-1 (Cert. #1315)
- HMAC-SHA-1, -224, -256, -384, -512 (Cert. #1316)

The module supports the following non-Approved algorithms allowed for use in the Approved

mode of operation.

- RSA (key wrapping, key establishment methodology provides 112-bits of encryption strength)
- S-Box, proprietary data obfuscation algorithm not utilized to provide FIPS 140-2 cryptographic strength.
- EC-DH
- HW NDRNG, allowed for seeding the RNGs
- MD5, allowed for use exclusively within TLS

An operator can determine the Approved version of the firmware by verifying the firmware version identified in the Security Manager SMPTE log. If the Approved version of the firmware is installed, then the module is constantly in a FIPS-Approved mode of operation.

4. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

• RS-232:	Status Output
• PCIe to SOM:	Data Input, Data Output, Control Input, Status Output, Power Input
• Projector tamper switch input (Qty. 2):	Control Input
• Ethernet (Qty. 3):	Data Input, Data Output, Control Input, Status Output
• GPIO:	Data Output, Control Input
• AES-Audio output:	Data Output
• LVDS video output:	Data Output
• LTC (Linear Time Code) I/O:	Data Input, Data Output
• Video ref in:	Data Input
• SDI In (Qty. 2):	Data Input
• HDMI in:	Data Input
• LED (Qty. 4):	Status Output
• Battery:	Power Input

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports two distinct operator roles, which are the User and Cryptographic-Officer roles.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic-Officer	Identity-based operator authentication	2048-bit Digital Signature
User	Identity-based operator authentication	2048-bit Digital Signature

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Digital Signature	The strength of a 2048-bit RSA key is known to be 112-bits. Therefore, the strength of a 2048-bit digital signature is 1/2^112, which is less than 1/1,000,000. In a worst case scenario, the module can perform 4725 signature verifications per minute, which does not include network limitations or timing constraints. Therefore, the probability that multiple attacks within a given minute will be successful is 4725/2^112.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
Cryptographic-Officer	• Load Firmware • Import MB Private Key
User	• Get Time • Update Time • Import KDM • Purge KDM • Check KDM • Setup CPL • Purge All KDM • Query KDM All • Get Logs • Get Log Info • Get Log Sig • Install Status • Play Control • SM Status • SM Projector Tamper Control • SM Heartbeat

Role	Authorized Services
	• Get Build Info • SM Sys Log • SM Playerd Log • LoadAssetMap • Playback Control • IMB GPIO Output • ReloadConfig

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the module through LEDs.
- Network Configuration: Non-security relevant configuration of the module.
- Self-tests: Invoke the power-on self-tests by power cycling the module.

Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

- Media Block Private Key (RSA 2048-bit) – Used to decrypt KDMs and sign security logs
- IMB TLS Private Key (RSA 2048-bit) – Used to facilitate an internal TLS session
- Protection AES Key (AES 128-bit) – Used to encrypt the Media Block Private Key and Content Encryption Keys for persistent storage
- Content Encryption Key (AES 128-bit) – Used to decrypt content data
- Content Integrity Key (HMAC-SHA-1) – Used to verify integrity of content data
- TLS Encryption Keys (AES 128-bit) – Provides data protection over TLS session
- TLS Integrity Keys (HMAC-SHA-1) – Provides data integrity over TLS session
- RNG Seed Keys – Used to Initialize DRNG
- RNG Seed Values - Used to Initialize DRNG

Definition of Public Keys:

The following are the public keys contained in the module:

- Media Block Public Key (RSA 2048-bit) – Used by external entities as the counterpart to the Media Block Public Key entities
- IMB TLS Public Key (RSA 2048-bit) – Used to facilitate an internal TLS session
- SM TLS Public Key (RSA 2048-bit) – Used to establish TLS connections
- SMS Root CA Certificate (RSA 2048-bit) – Used to verify the validity of SMS public keys received during a TLS session
- GDC FW Public Key (RSA 2048-bit) – Used to verify firmware updates
- Content Provider Public Keys (RSA 2048-bit) – Used to verify digital signatures on KDMs and CPLs
- Projector Public Keys (RSA 2048-bit) – Used during the DCI marriage process
- SMS Public Keys (RSA 2048-bit) – Used to verify authorized SMS during TLS sessions

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Read
- Write

Please note that all authenticated services are sent through an encrypted TLS tunnel and as such, TLS related CSPs are utilized during each service.

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
X		Load Firmware/File	N/A
X		Import MB Private Key	Read, Write MB Private Key Read, Write Protection AES Key

	X	Get Time	N/A
	X	Update Time	N/A
	X	Import KDM	Read MB Private Key Write Content Encryption Key
	X	Purge KDM	Write Content Encryption Key
	X	Check KDM	N/A
	X	Setup CPL	N/A
	X	Purge All KDM	Write Content Encryption Key
	X	Query KDM All	N/A
	X	Get Logs	N/A
	X	Get SM Log Info	N/A
	X	Get SM Log Signature	Read MB Private Key
	X	Install Status	N/A
	X	Play Control	Read Content Encryption Key, Write Content Integrity Key, Read Protection AES Key
	X	SM Status	N/A
	X	SM Projector Tamper Control	N/A
	X	SM Heartbeat	N/A
	X	Get Build Info	N/A
	X	SM Sys Log	N/A
	X	SM Playerd Log	N/A
	X	Load Asset Map	N/A

	X	Playback Control	Read Content Encryption Key, Write Content Integrity Key, Read Protection AES Key
	X	IMB GPIO Output	N/A
	X	Reload Config	N/A
X	X	Self-Tests	N/A
X	X	Show Status	N/A

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable; the cryptographic module supports a limited operational environment that restricts the loading of firmware by ensuring all firmware being installed is appropriately signed.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic module's security rules. This section documents the security rules enforced by the cryptographic module:

1. The module provides identity-based authentication.
2. The module will only provide access to cryptographic services if a valid role has been assumed.
3. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:
      a. AES Encrypt/Decrypt Known Answer Tests (KAT)
      b. HMAC-SHA-1 KAT
      c. SHA-1 KAT (tested as part of the HMAC-SHA-1 KAT)
      d. HMAC-SHA-1, -224, -256, -384, -512 KATs
      e. SHA-1 KAT
      f. SHA-224, -256, -384, -512 (tested as part of the HMAC SHA-224, -256, -384, -512 KATs)
      g. RSA Sign/Verify KAT
      h. ANSI X9.31 RNG KAT
   2. Firmware Integrity Tests (32-bit CRC)
   3. Critical Functions Tests: N/A

   B. Conditional Self-Tests:

   1. Continuous RNG test – performed on NDRNG and DRNG
   2. Firmware Load Test (RSA 2048-bit Signature Verification)

4. Data output shall be inhibited during self-tests and error states. In an error state, the module will restart and re-attempt self-tests.
5. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

9. Physical Security Policy

Physical Security Mechanisms

The Standalone IMB is a multi-chip embedded cryptographic module, which includes the following physical security mechanisms:

- Production-grade components.
- Hard, opaque, removable enclosure with tamper detection and response.
- Tamper evidence is provided by 4 tamper seals that are applied during manufacturing. Figure 3 provides the correct locations of the tamper seals.

Figure 3 – Tamper seal placement

Operator Required Actions

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

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper evidence	Monthly	Physically inspect the tamper seals for visual signs that they have tampered with.
Tamper Status	Annually	Ensure the module does not display any characteristics of

		an attempted breach.

10. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks beyond the scope of FIPS 140-2 requirements.

11. Definitions and Acronyms

AES	Advanced Encryption Standard
AES-Audio	Audio Engineering Society Audio
ANSI	American National Standards Institute
CO	Cryptographic Officer
CPL	Composition Playlist
CSP	Critical Security Parameter
DCI	Digital Cinema Initiative
DRNG	Deterministic Random Number Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
GP I/O	General Purpose Input/Output
HMAC	Hash Message Authentication Code
IMB	Image Media Block
IP	Intellectual Property
KAT	Known Answer Test

KDM	Key Delivery Message
LDB	Link Decryptor Block
LTC	Linear Time Code
LVDS	Low-Voltage Differential Signaling
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
PCI-E	Peripheral Component Interconnect Express
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SM	Security Manager
SMS	Screen Management System