GDC Technology Limited

Standalone IMB

Non-Proprietary FIPS 140-2 Security Policy

Document Version: 1.4

Date: April 15, 2019

Table of Contents

1 Overview 4

1.1 Cryptographic Boundary 4
1.2 Mode of Operation 5
1.3 Ports and Interfaces 5

2 Cryptographic Functionality 6

2.1 Critical Security Parameters 7
2.2 Public Keys 8

3 Roles, Authentication and Services 9

3.1 Assumption of Roles 9
3.2 Authentication Method 9
3.3 Services 9

4 Self-tests 12

5 Physical Security Policy 12

6 Operational Environment 13

7 Mitigation of Other Attacks Policy 13

8 Security Rules and Guidance 13

9 References and Definitions 15

List of Tables

Table 1 – Cryptographic Module Configuration 4
Table 2 – Security Level of Security Requirements 4
Table 3 – Ports and Interfaces 5
Table 4 – Approved Algorithms 6
Table 5 – Non-Approved but Allowed Cryptographic Functions 6
Table 6 – Security Relevant Protocols Used in FIPS Mode 7
Table 7 – Critical Security Parameters (CSPs) 7
Table 8 – Public Keys 8
Table 9 – Roles Description 9
Table 10 – Authentication Description 9
Table 11 – Authenticated Services 9
Table 12 – Unauthenticated Services 10
Table 13 – Security Parameters Access Rights within Services 11
Table 14 – Physical Security Inspection Guidelines 13
Table 15 – References 15
Table 16 – Acronyms and Definitions 16

List of Figures

Figure 1 - Image of the GDC-IMB-v4 (Top) 5
Figure 2 - Image of the GDC-IMB-v4 (Bottom) 5
Figure 3 – Tamper Seal Locations 13

1 Overview

The Standalone Image Media Block (IMB) cryptographic module (Firmware Version 3.2, Security Manager Firmware Version 1.7.1; Hardware Version: GDC-IMB-v4), hereafter referred to as the Module or cryptographic module, is a Security Processor Block, Type 1, designed in accordance with FIPS 140-2 and the Digital Cinema System Specification [DCI].

Table 1 – Cryptographic Module Configuration

	Module	HW P/N and Version	FW Version
1	Standalone IMB	GDC-IMB-v4	3.2, Security Manager 1.7.1

The FIPS 140-2 security levels for the Module are as follows:

Table 2 – Security Level of Security Requirements

Security Requirement	Security 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	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A
Overall	2

1.1 Cryptographic Boundary

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 cryptographic boundary is defined as the outer perimeter of the PCB. Figures 1 and 2 below depict the cryptographic module; all components not contained within the metal enclosure (security region) 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-v4 (Top)

Figure 2 - Image of the GDC-IMB-v4 (Bottom)

1.2 Mode of Operation

The Module only supports and operates in an Approved mode. It is not possible to configure the module into a non-Approved mode of operation. To verify that the Module is the FIPS-Approved version, the operator can verify the firmware version and Security Manager version are consistent with those listed in Table 1 above. The version information is logged during power-on.

1.3 Ports and Interfaces

The module's ports and associated FIPS defined logical interface categories are listed in Table 3.

Table 3 – Ports and Interfaces

Port	Description	Logical Interface Type
RS-232 Exposed Header	Status output serial header	Status Out
RS-232/GPIO Module header	Module communication	Not used
I2C header	Header to communicate with an expansion board	Not used
Projector Tamper switch	Marriage and door tamper from projector	Control In
Ethernet (Qty. 4)	Control and data network	Control In |Data In | Data Out | Status Out
GPIO (Qty. 8 in and 8 out)	General purpose input and output	Control In | Data Out | Status Out
AES Audio (2x RJ-45, 8 pairs)	Audio out	Data Out
LVDS Video (1 bus, 22 pairs)	Video out	Data Out
Video Reference Input (Qty. 1)	Reference input	Control in
SDI out (Qty. 2)	Video out	Not used
Reset (Qty. 1)	Reset button	Control In
HDMI (Qty. 2)	Video in	Data In
LED (Qty. 4)	Status LEDs	Status Out
Battery (Qty. 2)	Backup power	Power In

Port	Description	Logical Interface Type
USB 3.0 (Qty. 2)	USB connection	Data In | Data Out
eSATA (Qty. 1)	External SATA connection	Data In | Data Out

2 Cryptographic Functionality

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

Table 4 – Approved Algorithms

Cert	Algorithm	Mode	Description	Functions/Caveats
5122	AES [197]	CBC [38A]	Key Sizes: 128, 256	Encrypt, Decrypt
5123	AES [197]	CBC [38A]	Key Sizes: 128	Decrypt
1650	CVL: TLS [135]	v1.0/1.1	SHA-1	Key Agreement
1651	CVL: RSADP [56B]		n = 2048	Decrypt
1914	DRBG [90A]	CTR	Use_df AES-256	Deterministic Random Bit Generation
3403	HMAC [198]	SHA-1	Key Sizes: 128 – 2048 bit	Message Authentication, KDF Primitive
3404	HMAC [198]	SHA-1	Key Sizes: 512 bit	Message Authentication
N/A	KTS [38F]	CBC, HMAC	AES Cert. #5122 and HMAC Cert. #3403	Key transport (TLS)
2762	RSA [186]	X9.31	n = 2048	KeyGen
		PKCS1_v1.5	n = 2048 SHA(256)	SigGen
		X9.31	n = 2048 SHA(1)	SigVer
		PKCS1_v1.5	n = 2048 SHA(1, 256)	SigVer
4149	SHS [180]	SHA-1 SHA-256		Message Digest Generation
4150	SHS [180]	SHA-1		Message Digest Generation

Table 5 – Non-Approved but Allowed Cryptographic Functions

Algorithm	Description
CKG (no security claimed)	Optional legacy key generation prescribed by [*SMPTE ST 429-6] for checking Message Integrity for the purpose of logging only.*
KAS (no security claimed)	EC Diffie-Hellman prescribed by [DCI] to support authentication of legacy equipment. Not used for transmitting or protecting the modules CSPs.
KTS	RSA based key transport per IG D.9 (2048 bit for use in TLS)[1]. Key establishment methodology provides 112 bits of encryption strength.
MD5	For use in TLS v1.0[1] only [135]

Algorithm	Description
NDRNG	[Annex C] Non-Deterministic RNG; minimum of 128 bytes per access, providing at least 240 bits of entropy for the DRBG. The NDRNG output is used to seed the FIPS Approved DRBG.

Table 6 – Security Relevant Protocols Used in FIPS Mode

Protocol	Key Exchange	Auth	Cipher	Integrity
TLS v1.0[1]	[IG D.8 and SP 800-135] Cipher Suites: TLS_RSA_WITH_AES_128_CBC_SHA	RSA	AES 128	SHA1

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

2.1 Critical Security Parameters

All CSPs used by the Module are described in this section. All usage of these CSPs by the Module (including all CSP lifecycle states) is described in the services detailed in Section 4.

Table 7 – Critical Security Parameters (CSPs)

CSP	Description / Usage
CONT-ENC	Content Encryption Key. AES CBC 128-bit key. Used to decrypt content data.
DRBG-Seed	DRBG entropy input. 128 bytes, only the first 48-bytes are utilized to instantiate the DRBG.
DRBG-State	CTR_DRBG internal state (16-byte V and 32-byte Key – see 800-90A)
MB-PRIV	Media Block Private Key. RSA 2048-bit Private Key. Used to decrypt KDMs, sign security logs, and perform TLS
MB-COMM-PRIV	Media Block Communication Key. RSA 2048-bit Private Key. Used to perform internal TLS.
STOR-AES	Storage Encryption Key. AES CBC 128-bit key. Used to encrypt the MB-PRIV and CONT-ENC for persistent storage.
TLS-MS	(TLS Master Secret) 384-bit secret key material.
TLS-PMS	(TLS Pre-Master Secret) 384-bit secret key material.
TLS-SENC	TLS Session Encryption Keys. AES CBC 128-bit key. Protects TLS session data.
TLS-SMAC	TLS Session Authentication Keys. HMAC-SHA-1 (160-bit). Provide data TLS session data integrity.

2.2 Public Keys

Table 8 – Public Keys

Key	Description / Usage
CONT-PUB	Content Provider Public Keys. RSA 2048-bit Public Key. Used to verify signatures on KDMs and CPLs.
GDC-Root-CA-Chain	Root CA Public Key Certificate Chain. RSA 2048-bit Public Key. Used to verify the validity of SMS-TLS-PUB received during a TLS session.
FW-LOAD-PUB	Firmware Load Public Key. RSA 2048-bit Public Key. Used for firmware signature verification.
MB-PUB	Media Block Public Key. RSA 2048-bit Public Key. Provided to external entities to encrypt KDMs or verify security logs.
MB-COMM-PUB	Media Block Communication Public Key. RSA 2048-bit Public Key. Used to facilitate TLS.
PROJ-CA-Chain	Projector CA Public Key Certificate Chain. RSA 2048-bit Public Key. Used to verify the validity of PROJ-PUB receiving during marriage.
PROJ-PUB	Projector Public Keys. RSA 2048-bit Public Key. Used during the DCI marriage process.
SMS-TLS-PUB	Screen Management System TLS Public Key. RSA 2048-bit Public Key. Used to verify the SMS during a TLS session.

3 Roles, Authentication and Services

3.1 Assumption of Roles

The module supports two distinct operator roles, User and Cryptographic Officer (CO). Table 9 lists all operator roles supported by the module. The Module does not support a maintenance role, changing of roles, or concurrent operators. Operator authentication is performed via digital signature verification; the private keys used to create the signatures are not contained within the module.

Table 9 – Roles Description

Role ID	Role Description	Authentication Type	Authentication Data
CO	Cryptographic Officer – Assumed by GDC Technology Limited	Identity-based	Digital Signature Verification
User	User – Assumed by the SMS	Identity-based	Digital Signature Verification

3.2 Authentication Method

Operators are authenticated via verification of digital signatures created using RSA 2048-keys. 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.

The performance capacities of the module restrict the total number of signature verifications per minute to 142932, which does not include network limitations or timing constraints. Therefore, the probability that multiple attacks within a given minute will be successful is 142932/2^112, which is less than 1/100,000.

Table 10 – Authentication Description

Authentication Method	Probability	Justification
Digital Signature Verification	1/2^112	142932/2^112

3.3 Services

All services implemented by the Module are listed in the tables below.

Table 11 – Authenticated Services

Service	Description	CO	U
Load Firmware	Install firmware	X	
Load File	Install a file	X	
Get Time	Get current time		X
Update Time	Adjust current time		X
Import KDM	Import a new Key Delivery Message (KDM)		X
Purge KDM	Remove one KDM		X
Check KDM	Check availability of a valid KDM for CPL playback		X
Setup CPL	Prepare to playback a Composition Playlist (CPL)		X
Purge All KDM	Remove all KDMs		X

Service	Description	CO	U
Query KDM All	List all currently ingested KDMs		X
Get Logs	Retrieve logs from the Security Manager		X
Get Log Info	Retrieve logging device information (event class, type, and sub-type)		X
Get Log Sig	Retrieve the log report digital signature		X
Install Status	Query installation status		X
Play Control	Notify the Security Manager of playback events		X
SM Status	Retrieve Security Manager status		X
SM Projector Tamper Control	Manage the tamper control of the projector		X
SM Heartbeat	Verify the Security Manager is still active		X
Get Build Info	Retrieve Security Manager version information		X
SM Sys Log	Set logging IP address		X
SM Playerd Log	Request Security Manager to log playback		X
Load Asset Map	Load asset locations required for playback		X
IMB GPIO Output	Trigger hardware GPIO output		X
Reload Config	Reload player configuration		X
Get HW Serial	Get IMB hardware serial number		X
Get SM Pub Cert	Get SM Public Certificate		X
Get SM Mode	Get SM operating mode		X
Get Projector Info	Get status information from projector		X

Table 12 – Unauthenticated Services

Service	Description
Module Reset (Self-test)	Reset the Module by power cycle, which will invoke the Power-On Self-Tests
Show Status	Provides status via the LEDs
Network Configuration	Non-security relevant configuration of the module and establishment of the TLS session.

Table 13 defines the relationship between access to Security Parameters and the different module services. Individual services access to Security Parameters is represented independent of TLS, although all services are performed over a TLS session. The modes of access shown in the table are defined as:

- G = Generate: The service generates the Security Parameter.
- O = Output: The service outputs the Security Parameter.
- E = Execute: The service uses the Security Parameter in an algorithm.

- I = Input: The service inputs the Security Parameter.
- Z = Zeroize: The service zeroizes the Security Parameter. Note that complete zeroization will occur if power and batteries are removed and the module will cease to function.

Table 13 – Security Parameters Access Rights within Services

Service	CSPs and Public Keys																	
	DRBG-Seed	DRBG-State	MB-PRIV	MB-COMM-PRIV	TLS-MS	TLS-PMS	TLS-SENC	TLS-SMAC	STOR-AES	CONT-ENC	MB-PUB	MB-COMM-PUB	SMS-TLS-PUB	GDC-Root-CA-Chain	CONT-PUB	PROJ-PUB	FW-LOAD-PUB	PROJ-CA-Chain
Load Firmware																	E	
Load File																	E	
Get Time																		
Update Time																		
Import KDM			E						E	I					I,E			
Purge KDM										Z								
Check KDM																		
Setup CPL									E						I,E			
Purge All KDM										Z								
Query KDM All																		
Get Logs																		
Get Log Info																		
Get Log Sig			E								E							
Install Status																		
Playback Control																		
SM Status																		
SM Projector Tamper Control					G,E	G,O	G,E	G,E			O					I,E		E
SM Heartbeat																		
Get Build Info																		
SM Sys Log																		
SM Playerd Log																		
Load Asset Map									E	E								
IMB GPIO Output																		
Reload Config																		
Get HW Serial																		
Get SM Pub Cert											O							
Module Reset	G	G			Z	Z	Z	Z										
Get SM Mode																		
Get Projector Info																		
Show Status																		
Network Configuration	G	G	E	E	G,E	I,G,E,O	G,E	G,E			O,E	E	I,E	E		I,E		E

4 Self-tests

The module performs self-tests to ensure the proper operation of the module. Per FIPS 140-2, these are categorized as either power-up self-tests or conditional self-tests. Power up self–tests are available on demand by power cycling the module.

All algorithm Known Answer Tests (KATs) must be completed successfully prior to any other use of cryptography by the Module. If the firmware integrity test fails the module will be unresponsive with no LEDs lit. If one of the KATs fails, the Module enters the error state and outputs status of either a red or orange (top left) LED; otherwise it indicates successful completion by a green (top left) LED.

The module performs the following algorithm KATs on power-up.

- Firmware Integrity (Bootloader): 32 bit CRC performed over all code on NAND.
- Firmware Integrity (Security Manager): HMAC-SHA-1 (Cert. #3403)
- AES-CBC-128 Encrypt/Decrypt KATs (Cert. #5122)
- AES-CBC-128 Decrypt KAT (Cert. #5123
- Security Manager HMAC SHA-1 KAT (HMAC Cert. #3403 and SHA Cert. #4149)
- HMAC SHA-1 KAT (HMAC Cert. #3404 and SHA Cert. #4150)
- SHA-1 KAT (Cert. #4150)
- RSA 2048-bit Signature Generation/Verification KATs (RSA Cert. #2762 and SHA Cert. #4149)
- CTR_DRBG KAT (Cert. #1914)

The module performs the following conditional self-tests as indicated.

- Continuous RNG Test – performed on NDRNG and DRBG
- Firmware Load: RSA 2048 signature verification of SHA-256 based signature.
- SP 800-90A DRBG Health Tests (Instantiate, Reseed)

5 Physical Security Policy

The G2C 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 four (4) tamper-evident seals that are applied during manufacturing. Figure 3 provides the correct locations of the tamper seals.

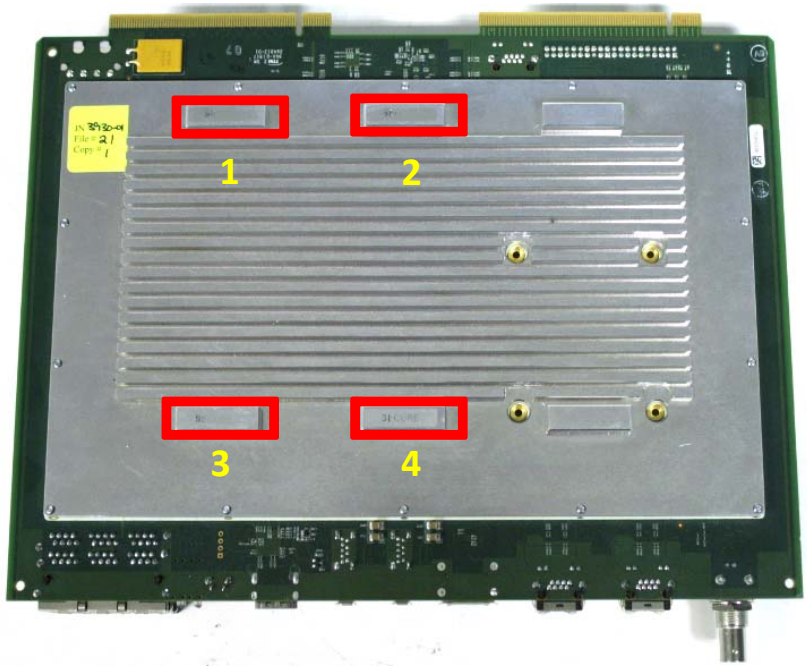

Figure 3 – Tamper Seal Locations

Table 14 – Physical Security Inspection Guidelines

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper-Evident Seals	Monthly	Verify the four seals placed on the bottom heat sink cover show no signs of tamper. If evidence of tamper is identified, notify your organization's Security Administration.

6 Operational Environment

The Module has a non-modifiable operational environment under the FIPS 140-2 definitions. The Module includes a firmware load service to support necessary updates. New firmware versions within the scope of this validation must be validated through the FIPS 140-2 CMVP. Any other firmware loaded into this module is out of the scope of this validation and require a separate FIPS 140-2 validation.

7 Mitigation of Other Attacks Policy

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

8 Security Rules and Guidance

This section documents the security rules for the secure operation of the cryptographic module to implement the security requirements of FIPS 140-2.

1. The module provides two distinct operator roles: User and Cryptographic Officer.
2. The module provides identity-based authentication.
3. The module clears previous authentications on power cycle.
4. An operator does not have access to any cryptographic services prior to assuming an authorized role.
5. The module allows the operator to initiate power-up self-tests by power cycling power or resetting the module.
6. Power up self-tests do not require any operator action.
7. Data output are inhibited during key generation, self-tests, zeroization, and error states.
8. Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module does not support concurrent operators.
10. The module does not support a maintenance interface or role.
11. The module does not support manual key entry.
12. The module does not have any proprietary external input/output devices used for entry/output of data.
13. The module does not enter or output plaintext CSPs.
14. The module does not output intermediate key values.
15. Upon detection of a tamper event, all CSPs are immediately destroyed and the module will cease to function.

9 References and Definitions

The following standards are referred to in this Security Policy.

Table 15 – References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[131A]	*Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, *January 2011*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[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*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[56Br1]	*NIST Special Publication 800-56A Revision 1, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, September 2014*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*
[DCI]	*Digital Cinema Initiatives, LLC, Digital Cinema System Specification, Version 1.2 with Errata as of 30 August 2012 Incorporated*
[SMPTE ST 429-6]	*The Society of Motion Picture and Television Engineers, D-Cinema Packaging – MXF Track File Essence Encryption, October 3, 2006*

Table 16 – Acronyms and Definitions

Acronym	Definition
AES	Advanced Encryption Standard
AES-Audio	Audio Engineering Society Audio
CO	Cryptographic Officer
CPL	Composition Playlist
CSP	Critical Security Parameter
DCI	Digital Cinema Initiative
DRBG	Deterministic Random Bit Generator
EMI/EMC	Electromagnetic Interference/Electromagnetic Compatibility
FIPS	Federal Information Processing Standard
GPIO	General Purpose Input/Output
HMAC	Hash Message Authentication Code
IMB	Image Media Block
KAT	Known Answer Test
KDM	Key Delivery Message
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