DCI Board Security Policy
GDC Technology (USA) LLC

Version 1.2

December 9, 2011

TABLE OF CONTENTS

1. Module Overview

The DCI Board (Firmware Versions 1.0 and 1.1; Security Manager Firmware Version 1.2.11; Hardware Versions: Z-OEM-DCI-R0, Z-OEM-DCI-R2, Z-OEM-DCI-R3), 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 DCI board is defined as a multi-chip embedded cryptographic module encased in a hard, opaque potting material.

The images below depict the cryptographic module; all components not encapsulated within the potting material 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

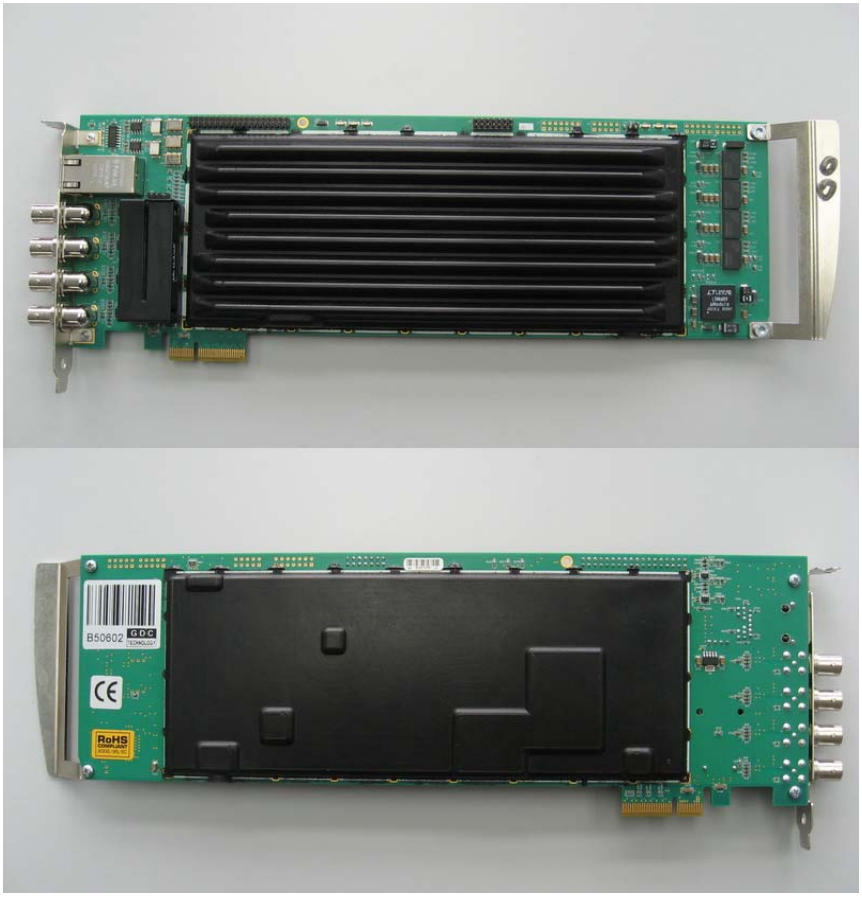

Figure 1 – Image of the Z-OEM-DCI-R0 (Top & Bottom)

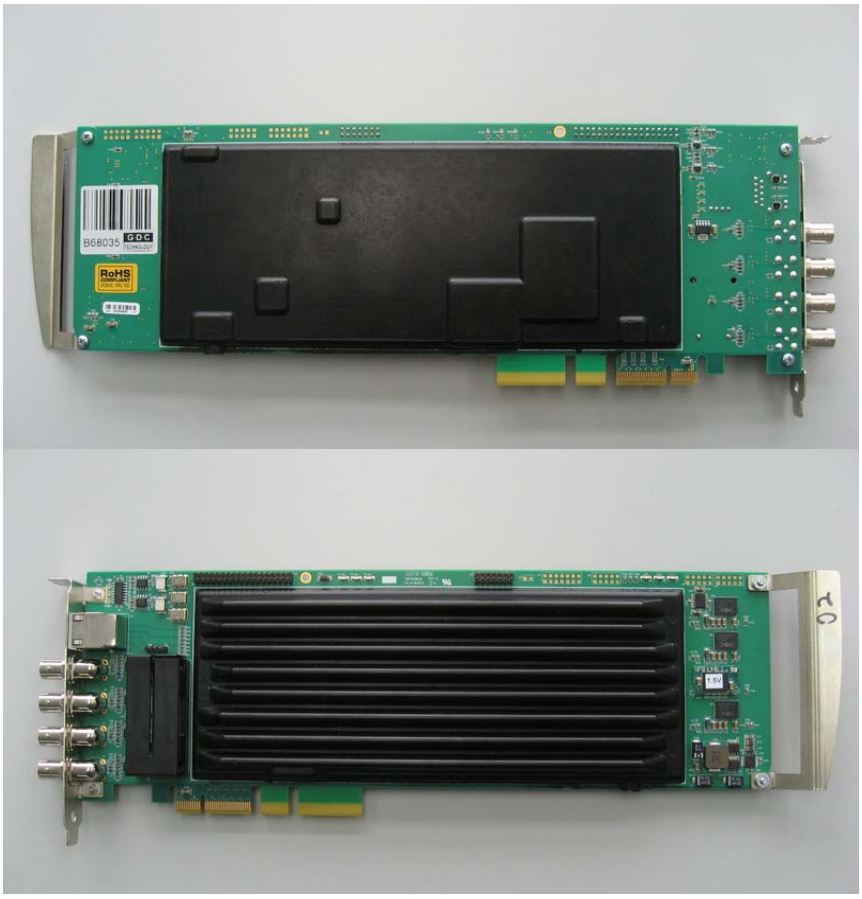

Figure 2 – Image of the Z-OEM-DCI-R2 (Top & Bottom)

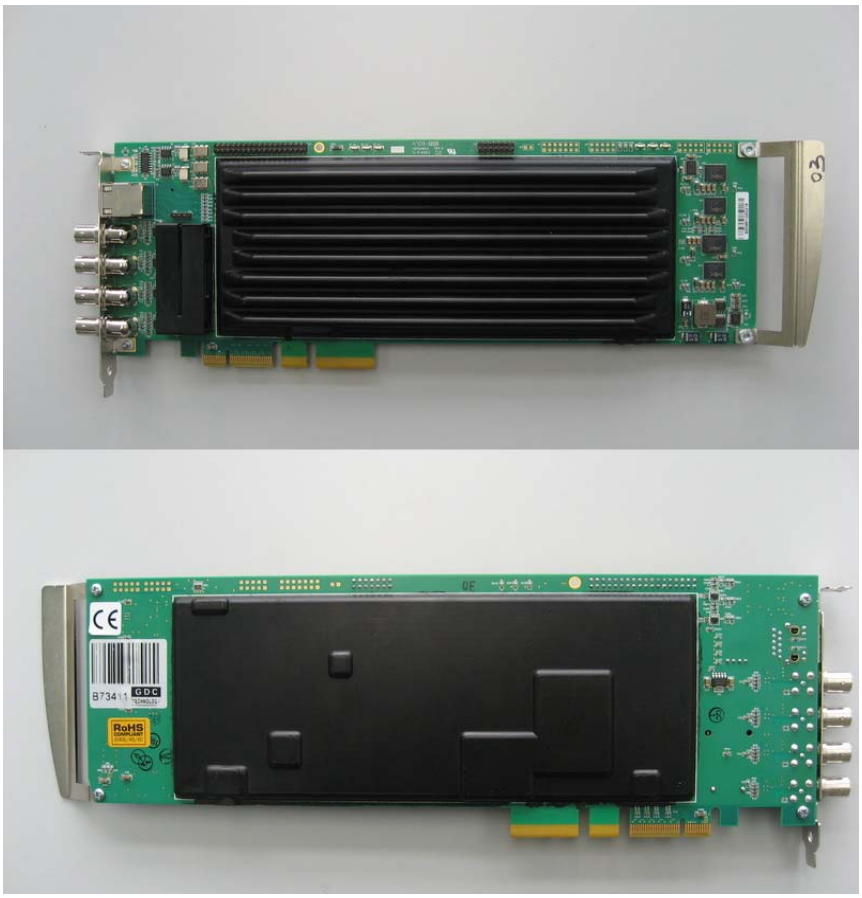

Figure 3 – Image of the Z-OEM-DCI-R3 (Top & Bottom)

2. Security Level

The cryptographic module meets the overall requirements applicable to FIPS 140-2 Level 3.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
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 (Certs. #1278 and #1286)
- SHS (Certs. #1176, #1178, #1179 and #1180)
- RNG ANSI X9.31 (Certs. #713 and #716)
- RSA Sign/Verify ANSI X9.31, 2048 bit keys (Certs. #610 and #613)
- HMAC-SHA-1 (Certs. #743 and #747)

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)
- 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 during power-up. If the Approved version of the firmware is installed, then the module is constantly in a FIPS-Approved mode of operation. The module will start-up and output “FIPS mode: 1”.

4. Ports and Interfaces

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

- Analog Reference Input (Qty. 1): Control Input
- Ethernet (Qty. 1): Data Input, Data Output, Control Input, Status Output (status output in the form of return codes and status messages to other devices)
- Ethernet LEDs (Qty. 5) Status Output (manual status output)
- Status LEDs (Qty. 3) Status Output (manual status output)
- RS-232 (Qty. 1): Control Input
- Reset Jumper (Qty. 1): Control Input
- HD-SDI Output (Qty. 4): Data Output
- AES-Audio (Qty. 8): Data Output
- PCI-E Card edge (Qty. 1): Data Input, Data Output, Control Input, Status Output, Power Input (status output in the form of return codes and status messages to other devices)

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 18 signature verifications per second, which does not include network limitations or timing constraints. Therefore, the probability that multiple attacks within a given minute will be successful is 1080/2^112.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
Cryptographic-Officer	• Upgrade SM • Import MB Private Key
User	• Get Time • Update Time • Import KDM • Query KDM All • Install Status • Play Reel • Setup CPL • Play Control • SM Status • Set LDB IP

Role	Authorized Services
	• Get LDB Status • Get Logs • Get SM Log Info • Get SM Log Signature • Purge KDM • Purge All KDM • Check KDM

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the module through LEDs. The status LEDs indicate whether the module is powering up, in an operational state, or in the error state. If the Power-on Self-tests pass successfully, all status LEDs will turn green. If the module has entered the error state, one LED will blink while the others remain lit.
- Self-tests: Invoke the power-on self-tests by power cycling the module.
- Zeroize: Actively overwrites all contents of key memory.

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
- TLS Private Key (RSA 2048-bit) – Used to facilitate TLS operations
- 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
- CineLink II Key (CineLink II Proprietary Link Obfuscation) – Obfuscates communication with Projector
- 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 Deterministic RNG
- RNG Seed Values - Used to Initialize Deterministic RNG

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
- 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 integrity at power on as well as 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 to verify authorized projectors during TLS sessions
- 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
- Zeroize

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		Upgrade SM	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 All KDM	Zeroize Content Encryption Key
	X	Query KDM All	N/A
	X	Install Status	N/A
	X	Play Reel	Read Content Encryption Key,

			Write Content Integrity Key, Write CineLink II Key, Read Protection AES Key
	X	Setup CPL	N/A
	X	Play Control	N/A
	X	SM Status	N/A
	X	Set LDB IP	N/A
	X	Get LDB Status	N/A
	X	Get Logs	N/A
	X	Get SM Log Info	N/A
	X	Get SM Log Signature	Read MB Private Key
	X	Purge KDM	Zeroize Content Encryption Key
	X	Check KDM	N/A
X	X	Self-Tests	N/A
X	X	Zeroize	Zeroize MB Private Key, Protection AES Key, TLS Private Key, Content Encryption Key, Content Integrity Key, CineLink II Key, RNG Seed Key, RNG Seed Values
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 to implement the security requirements of this FIPS140-2 Level 3 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. <u>Power up Self-Tests:</u>

1. Cryptographic algorithm tests:
    a. AES Encrypt/Decrypt KATs
    b. HMAC SHA-1 KATs
    c. SHA-1 KATs

d. RSA Sign/Verify KATs
e. RSA Encrypt/Decrypt Pairwise Consistency Test & KAT
f. ANSI X9.31 RNG KATs

2. Firmware Integrity Tests (2048-bit RSA Signature Verifications)
3. Critical Functions Tests: N/A

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on NDRNG and RNGs
2. Firmware Load Test (RSA 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 DCI Board is a multi-chip embedded cryptographic module, which includes the following physical security mechanisms:

- Production-grade components.
- Hard potting encapsulation with removal/penetration attempts rendering the module inoperable. **Note: The vendor did not provide operating and storage temperature ranges to the test lab so module hardness testing was only performed at ambient temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.**

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
Encapsulate	6 months	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
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
HMAC	Hash Message Authentication Code
IP	Intellectual Property
KAT	Known Answer Test
KDM	Key Delivery Message
LDB	Link Decryptor Block
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