Non-Proprietary Security Policy

CHN-II Integrated Media Block

Digicine Oristar Technology Development(Beijing) Co., Ltd

VERSION: **1.1**
DATE: **2015-04-09**

Table of Contents

1 Introduction 3
1.1 Purpose 4
1.2 Revisions 4
1.3 Security Levels 5
1.4 Approved Mode of Operation 5
2 Ports and Interfaces 6
3 Security Functions 8
3.1 Approved Security Functions 8
3.2 Allowed Key Establishment and Key Transport Protocols 8
3.3 Non-Approved Security Functions 8
4 Cryptographic Keys and CSPs 9
4.1 Public Keys 9
5 Self-Tests 10
5.1 Power-Up Self-Tests 10
5.2 Conditional Tests 10
6 Security 11
6.1 Operational Environment 11
7 Physical Security Policy 12
7.1 Physical Security 12
7.2 Zeroization 13
8 Identification and Authentication Policy 14
8.1 Authentication 14
9 Access Control Policy 15
9.1 Services for Authorized Roles 15
9.2 Services for Unauthorized Roles 15
9.3 Access Rights within Services 16
10 Mitigation of Other Attacks Policy 19
11 Appendix 20
11.1 Acronyms 20

1 Introduction

The Digicine Oristar Technology Development (Beijing) Co., Ltd ("Oristar") CHN-II cryptographic module is a multi-chip embedded hardware Digital Cinema decoder.

The CHN-II complies with the Digital Cinema System Specification V1.2 released on March 07, 2008 by the Digital Cinema Initiative (DCI). The whole Image Media Block (IMB) functionality is integrated in the CHN-II, making it a very strong and intrinsically secure component in terms of content protection. It meets the requirements of FIPS 140-2 Security Level 3.

The CHN-II is a printed circuit board (PCB) designed for integration into a Texas Instruments (TI) Series 2 DLP Cinema projector. The module's cryptographic boundary is the outer edge of the PCB. All parts outside the physically protected area on the board are excluded from the requirements of FIPS 140-2 because they are non-security relevant and cannot be used to compromise the security of the module.

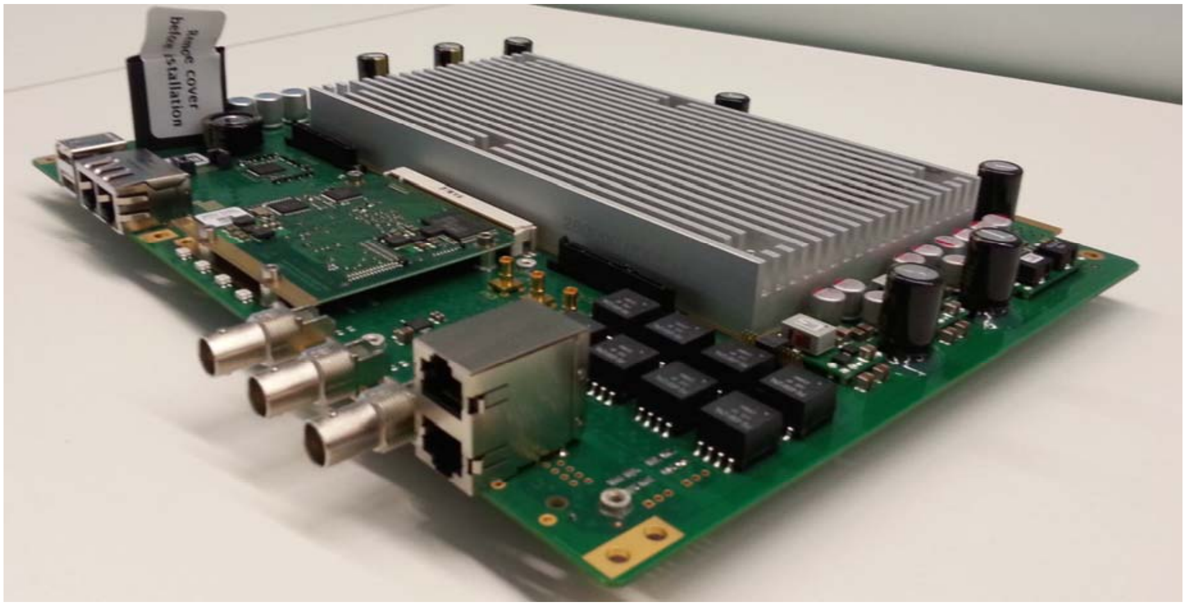

Figure 1 – CHN-II – Front

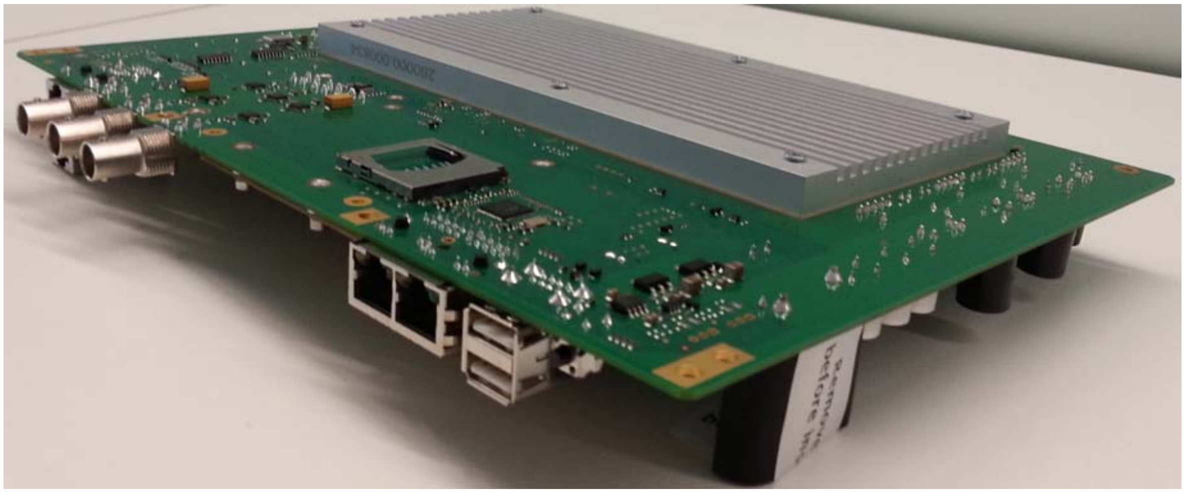

Figure 2 – CHN-II - Back

1.1 Purpose

This document is the security policy for the CHN-II cryptographic module. It describes the security behavior of the module and how it meets the requirements of FIPS Publication 140-2 Security Level 3.

The FIPS PUB 140-2 is a U.S. government computer security standard used to validate cryptographic modules. The security level 3 describes a “production grade” module, which is physically and logically tamper-resistant and has the functionality to protect and in case of an attack to erase all secure content.

1.2 Revisions

The module has been validated with the following version information:

Hardware:	1.0
Firmware:	1.0.0 and 1.2.0
Bootloader:	1.0

1.3 Security Levels

The CHN-II is designed, developed and tested to meet the requirements of DCI Digital Cinema System Specification V1.2 as well as the requirements of FIPS 140-2 Security Level 3, which is requested by the DCI. The following table lists the compliance level of each section:

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
Operating Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 1 - Levels of Security Requirements

1.4 Approved Mode of Operation

The module only provides the FIPS 140-2 approved mode of operation. This mode is invoked automatically at boot up of the cryptographic module.

To verify that the module is in approved mode of operation, the operator shall check for version numbers matching those listed on the validation certificate (refer to Section 1.2) using the Show Status service.

2 Ports and Interfaces

The CHN-II cryptographic module has several physical ports, i.e., connectors, which are used for single or multiple purposes.

The CHN-II provides the following physical ports:

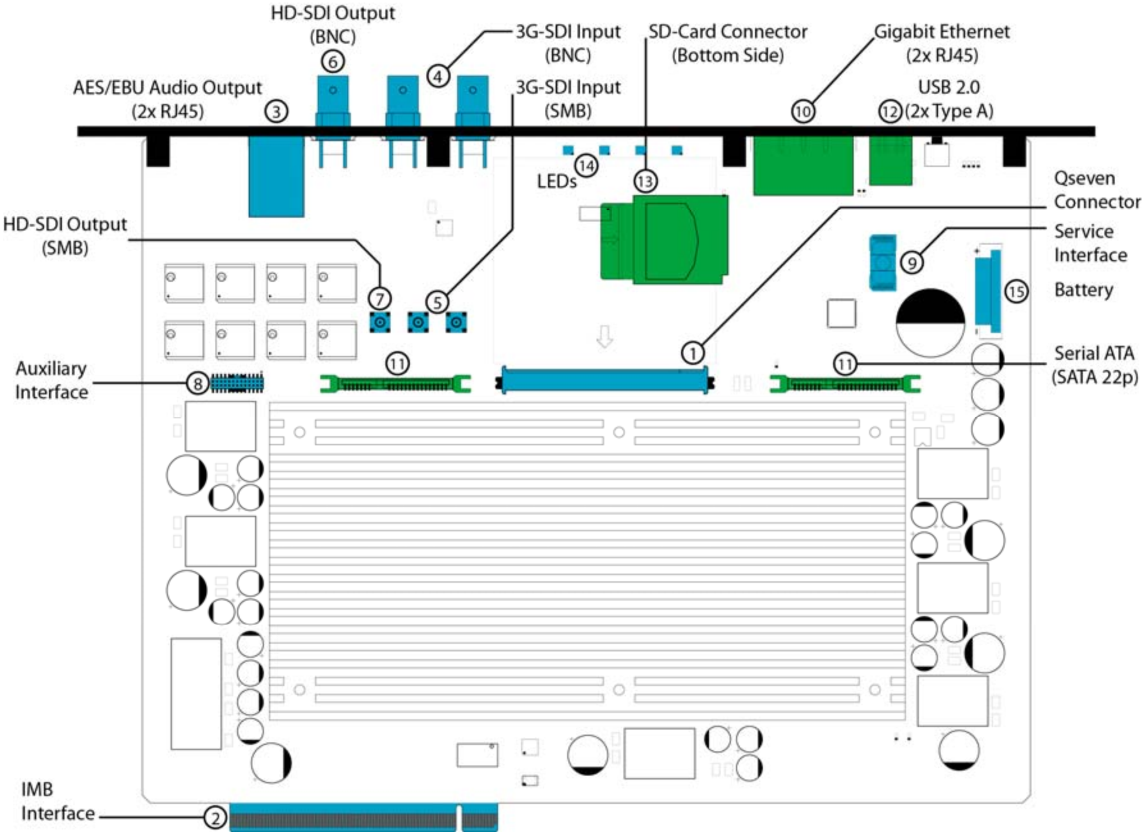

Figure 3 – Physical Connectors

The following table describes how the physical ports relate to logical interfaces.

Location	Physical Port	Protocol	Quantity	Logical Interface
1	PCI Express (Qseven connector)	PCI Express Base Specification Revision 1.1	1	Data input, Control input, Data output, Status output,
2	IMB interface	TI proprietary	1	Data output, Control input, Status output, Power input
3	AES/EBU Audio (RJ45)	AES3	2	Data output
4	3G-SDI input (BNC)	SMPTE424M SMPTE425M	2	Data input
5	3G-SDI input (SMB)	SMPTE424M SMPTE425M	2	Data input
6	HD-SDI output (BNC)	SMPTE292M	1	Data output
7	HD-SDI output (SMB)	SMPTE292M	1	Unused. Legacy component
8	Auxiliary interface (Pin Header)	Proprietary GPIO	1	Unused. Legacy component
9	Service interface (contact pads)	UART	1	Status output,
10	Gigabit Ethernet (RJ45)	IEEE 802.3ab	2	Data input, Control input, Data output, Status output
11	Serial ATA	SATA Revision 1.0a	2	Data input
12	USB 2.0	USB Specification Revision 2.0	2	Data input
13	SD-Card	SDIO	1	Data input
14	LEDs	N/A	4	Status output
15	Battery	N/A	1	Power input

Table 2 - Relation of Ports and Interfaces

No maintenance access interface is present.

3 Security Functions

The CHN-II cryptographic module supports FIPS 140-2 approved cryptographic algorithms, allowed key establishment protocols and other approved and non-approved security functions.

3.1 Approved Security Functions

1. **RSA-2048**, used for sign/verify (RSA Cert. #1498)
2. **AES-128, -256**, in CBC mode (encryption/decryption) (AES Cert. #2858)
3. **AES-128,** in CBC mode (decryption only) (AES Certs. #2880, and #2882)
4. **AES-256,** in CBC mode (decryption only) (AES Cert. #2881)
5. **RNG**, ANSI X9.31 RNG using AES (RNG Cert. #1281)
6. **HMAC-SHA-1** (HMAC Certs. #1798 and #1816)
7. **SHA-1** (SHS Cert. #2401 and #2421)
8. **SHA-256** (SHS Certs. #2401 and #2422)

3.2 Allowed Key Establishment and Key Transport Protocols

1. Key transport using RSA (key wrapping, uses key size 2048 bit, key establishment methodology provides 112 bits of encryption strength.

3.3 Non-Approved Security Functions

1. Hardware RNG is the non-deterministic RNG (physical hardware) utilized for seeding the DRNG
2. TI S-Box, proprietary algorithm used for projector communication and is not relied upon to provide FIPS 140-2 cryptographic strength
3. EC Diffie-Hellman, used to establish communication channel with the projector and is not relied upon to provide FIPS 140-2 cryptographic strength
4. SP 800-135rev1 KDF within TLS (not CAVP tested)
5. MD5 within TLS

4 Cryptographic Keys and CSPs

The CHN-II cryptographic module contains the following CSPs:

- **Master Key (AES-256):** System Master Key used as key encrypting key for CSP decryption. The used key size is 256 bits.
- **Decryption Key (RSA-2048):** System Private Decryption Key, used for content key unwrapping. The used key size is 2048 bits.
- **Signature Key (RSA-2048):** System Private Signature Key used to sign log messages, for TLS authentication and projector marriage. The used key size is 2048 bits.
- **Content Key (AES-128):** Content Keys, used to decrypt content. The used key size is 128 bits.
- **Firmware Key (AES-128):** Firmware image decryption key. The used key size is 128 bits.
- **TLS Pre-master Secret:** The parameter used for the generation of TLS Master Secret.
- **TLS Master Secret:** The parameter used for the generation of TLS Session Key and TLS Integrity Key.
- **TLS Session Key (AES-128):** The AES key used to protect TLS connection.
- **TLS Integrity Key (160 bit HMAC key):** The HMAC-SHA-1 key used to check integrity of TLS connection.
- **Seed and Seed Key:** Used to initialize the DRNG.
- **Message Integrity Key (HMAC-SHA-1):** Message Integrity Check Keys. The used key size is 160 bits.

4.1 Public Keys

The cryptographic module contains the following public keys:

- **Oristar Cert (X.509v3):** Oristar certificates used to verify the signature of firmware and feature update images.
- **TSP Cert (X.509v3):** TSP certificate chain used to verify other certificates.
- **SMS Cert (X.509v3):** SMS certificate used by the IMB to authenticate TLS session between IMB and SMS.
- **IMB Decryption Cert (X.509v3):** IMB decryption certificate.
- **IMB Sign Cert (X.509v3):** IMB certificate used by the SMS to authenticate TLS session between IMB and SMS. Also used by the projector for marriage.
- **Projector Cert (X.509v3):** Projector certificate used by the IMB for projector marriage. This certificate is verified using a Trusted Device List.
- **DCP Provider Certi (X.509v3):** DCP provider certificate chain used to verify the signature of Extra-Theater Messages like KDMs.

5 Self-Tests

The CHN-II cryptographic module performs all below mentioned power-up self-tests on boot-up and only enters FIPS 140-2 approved mode of operation if all tests passed successfully. The conditional tests are executed every time the corresponding algorithm is used.

5.1 Power-Up Self-Tests

- Firmware integrity test (32-bit CRC and SHA-256)
- RSA Signature Generation and Signature Verification known answer tests
- AES CBC (128 and 256) Decrypt known answer tests
- AES CBC (128 and 256) Encrypt and Decrypt known answer tests
- SHA-1 known answer tests
- SHA-256 known answer tests
- ANSI X9.31 RNG known answer test
- HMAC-SHA-1 known answer tests

5.2 Conditional Tests

- Firmware load test (RSA 2048-bit signature verification)
- Continuous Random Number Generator Test on Hardware RNG
- Continuous Random Number Generator Test on RNG

6 Security

6.1 Operational Environment

The whole firmware of the CHN-II cryptographic module is stored persistently inside the module. During power-up the integrity of the stored firmware is checked before it is loaded and the module enters FIPS 140-2 approved mode of operation and no further firmware can be loaded.

All functions stored persistently in the module are static, non-modifiable, and do not use an underlying general purpose operating system. Thus the requirements of FIPS 140-2 Chapter 4.6.1 (Operational Environment) are not applicable because of the limited operational environment.

7 Physical Security Policy

7.1 Physical Security

The CHN-II cryptographic module is a multiple-chip embedded cryptographic module protected by a tamper-resistant metal cover on the upper and on the lower side of the board (see Figure 1 and Figure 2). Both cover shells are mounted stationary and are protected by a tamper detection mechanism as well as tamper-evident coating over the screws, which must be checked periodically (refer to Table 3).

During normal operation, the operator only has access to the front panel interfaces of the module, because it is integrated in the projector. It is protected against removal by the projector's physical and electrical arrangements

A maintenance service for the CHN-II is neither required nor allowed.

Physical Security Mechanisms	Recommended Frequency of Inspection	Inspection Guidance Details
Metal cover	Before projector marriage	Both cover shells shall not be damaged
Cover fixing bolts	Before projector marriage	All bolts shall not be damaged
Tamper evident coating over screws	Before with projector marriage	The coating shall not be damaged or look tampered. Please refer to Figure 5 for a picture of untampered coating.

Table 3 - Physical Security Inspection Guidance

The seal-protected cover also acts as a heat sink and forms a hard enclosure in means of FIPS 140-2.

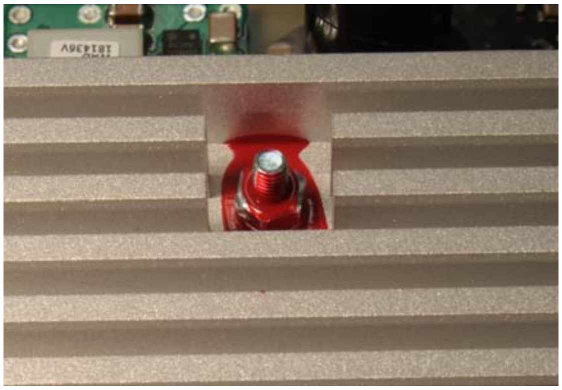

Figure 4 – Coating Over Screw

As soon as a cover is removed the tamper detection response is triggered, automatically forcing active zeroization of all cryptographic keys as described in Section 0below.

7.2 Zeroization

After tamper detection, secret and private cryptographic keys and CSPs are actively and immediately deleted.

When an attack is detected and the system is inactive (power-off) only the key encrypting key ZK is zeroized by the tamper detection device and thus also the IMBPrDecK, IMBPrSignK, and FWSymK immediately become unusable.

If the system is active (power-on) while being attacked additionally all temporary cryptographic keys and CSPs of the module are zeroized.

The module also contains a Zeroize service allocated to the User role. This service zeroizes all secret and private cryptographic keys and CSPs within the module.

8 Identification and Authentication Policy

8.1 Authentication

The following table describes the roles and how they are authenticated:

Role	Type of Authentication	Authentication Data
User	Identity-based authentication	2048-bit digital signature verification
Crypto Officer	Identity-based authentication	2048-bit digital signature verification

Table 4 – Authentication Types

Authentication Mechanism	Strength of Mechanism
Digital Signature Verification	The RSA private key used to generate the digital signature is 2048-bits. The strength of a 2048-bit RSA key (with SHA-256) is known to be 112 bits. Therefore, the strength of a 2048-bit digital signature is 1/2^112, which is less than one in 1,000,000. The module can perform RSA signature verifications in approximately 900ms, which is approximately 67 verifications per minute. The probabilty that a brute force attack will be successful given a minute of time is 67/(2^112), which is less than the required 1/100,000.

Table 5 - Strength of Authentication

9 Access Control Policy

9.1 Services for Authorized Roles

The CHN-II cryptographic module supports two authorized roles. The User role covers general security related services, including cryptographic and other approved security functions. The Crypto Officer (CO) role covers secure firmware update.

User Role	CO Role	Service	Service Description
	x	SystemUpdate	Update IMB firmware
x		StartSuite	Query the SM to check the auditorium equipment (e.g., marriage status) and start operation
x		StopSuite	Query the SM to stop operation
x		UploadCPL	Upload a Composition Play List to the SM for validation
x		UploadKDM	Upload a Key Delivery Message to the SM for validation and key decryption
x		PurgeCPL	Remove a CPL and all the associated data (CPL, KDMs, keys, etc.)
x		PlayBack	Play a show, send encrypted data and control playback
x		PlayShow	Prepare a show (as a list of CPLs) for playback
x		StopShow	Reject a prepared show
x		CheckShow	Check that a show (as a list of CPLs) is ready for playback at a given time
x		GetCertificates	Retrieve the IMB certificates
x		GetCPLList	Retrieve the list of currently available CPLs
x		GetKDMList	Retrieve the list of available KDMs for a specific CPL
x		QuerySM	Query the SM status
x		AdjustTime	Allow the auditorium operator to adjust the SM clock
x		GetLogReport	Retrieve security logs maintained by the SM
x		InitiateMarriage	Initiate projector marriage procedure
x		ClearTamper	Clear pending service door tamper
x		Zeroize	Zeroize all module cryptographic keys and CSPs

Table 6 – Authenticated Services

9.2 Services for Unauthorized Roles

The module provides the following unauthenticated services:

Service	Service Description
EstablishConnection	Start TLS session between the SM and the external SMS
ProjectorInterface	Query status, initiate marriage and clear service door tamper
Playback Plaintext	Play a show, send plaintext data and control playback
Restart	Restart of the IMB causing a reset and reboot. This causes the suite of self-tests to be run.

Service	Service Description
ShowStatus	Output the current status of the cryptographic module.

Table 7 - Unauthenticated Services

9.3 Access Rights within Services

Service	Cryptographic Keys and CSPs	Types of Access generate/read/write/modify/zeroize
SystemUpdate	Oristar Cert	read
	Firmware Key	read
StartSuite	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
StopSuite	DCP Provider Cert	zeroize
	Content Key	zeroize
	Message Integrity Key	zeroize
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
UploadCPL	DCP Provider Cert	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
UploadKDM	DCP Provider Cert	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
	Content Key	write
	Message Integrity Key	write
	Decryption Key	read
PurgeCPL	DCP Provider Cert	zeroize
	Content Key	zeroize
	Message Integrity Key	zeroize
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
Playback	Content Key	read
	Message Integrity Key	read
PlayShow	Content Key	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
StopShow	TLS Pre-Master Secret	read
	TLS Master Secret	read

Service	Cryptographic Keys and CSPs	Types of Access generate/read/write/modify/zeroize
	TLS Session Key	read
	TLS Integrity Key	read
CheckShow	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
GetCertificates	IMB Dec Cert	read
	IMB Sign Cert	read
	Oristar Cert	read
	TSP Cert	read
	Projector Cert	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
GetCPLList	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
GetKDMList	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
QuerySM	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
AdjustTime	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
GetLogReport	Signature Key	read
	TSP Cert	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
InitiateMarriage	Projector Cert	read/write
	IMB Sign Cert	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
ClearTamper	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
Zeroize	Master Key	zeroize

Service	Cryptographic Keys and CSPs	Types of Access generate/read/write/modify/zeroize
	Decryption Key	zeroize
	Signature Key	zeroize
	Firmware Key	zeroize
	Content Key	zeroize
	Message Integrity Key	zeroize
	TLS Pre-Master Secret	zeroize
	TLS Master Secret	zeroize
	TLS Session Key	zeroize
	TLS Integrity Key	zeroize
	DRNG State	zeroize
EstablishConnection	Signature Key	read
	IMB Sign Cert	read
	TSP Cert	read
	SMS Cert	read/write
	TLS Pre-Master Secret	generate
	TLS Master Secret	generate
	TLS Session Key	generate
	TLS Integrity Key	generate
	DRNG State	generate
ProjectorInterface	Projector Cert	read/write
	IMB Sign Cert	read
Playback Plaintext	-	n/a
Restart	Decryption Key	zeroize
	Signature Key	zeroize
	Firmware Key	zeroize
	Content Key	zeroize
	Message Integrity Key	zeroize
	DCP Provider Cert	zeroize
	SMS Cert	zeroize
	TLS Pre-Master Secret	zeroize
	TLS Master Secret	zeroize
	TLS Session Key	zeroize
	TLS Integrity Key	zeroize
	DRNG State	zeroize
ShowStatus	-	n/a

Table 8 - Access Right Mapping

10 Mitigation of Other Attacks Policy

Mitigation of other attacks in the meaning of FIPS PUB 140-2 is not claimed. The module has not been designed to mitigate other attacks outside of the scope of FIPS 140-2.

11 Appendix

11.1 Acronyms

Acronym	Description
AES	Advanced Encryption Standard
AES3	Digital audio interface specified by Audio Engineering Society in standard AES3
CBC	Cipher Block Chaining – Block Cipher Mode
CPL	Composition Play List
CSP	Critical Security Parameters
CTR	Counter – Block Cipher Mode
DCI	Digital Cinema Initiative
DES	Data Encryption Standard
PRNG	Deterministic RNG
ECB	Electronic Codebook – Block Cipher Mode
FPGA	Field Programmable Gate Array
HD-SDI	High Definition Serial Digital Interface
HRNG	Non-deterministic RNG (physical hardware)
IMB	Image Media Block
JPEG	Joint Photographic Experts Group
KDM	Key Delivery Message
MPEG	Moving Picture Experts Group
PCB	Printed Circuit Board
PCI	Peripheral Component Interconnect
RNG	Random Number Generator
RSA	Asymmetric Cryptographic Algorithm published by Ron Rivest, Adi Shamir and Leonard Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SM	Security Manager
SMPTE	Society of Motion Picture and Television Engineers
SMS	Screen Management System (not part of the validation)
TLS	Transport Layer Security
TSP	Theatre System Provider

Table 9 - Acronyms