Security Policy

No: *010-103498-12 Rev: 1*

REVISION #	ECO #	REVISION #	ECO #
1	15-3805		

Title: Christie IMB-S2 Security Policy

Product(s): **Christie IMB-S2 4K Integrated Media Block (IMB)**

Prepared by: **Kevin Draper**

Prep'd Date: **08/11/2015**

Last Updated: **08/25/2015**

Detailed Revision History

Revision	Description of Changes
1	Initial public release.

Table of Contents

Table of Figures

List of Tables

1. SCOPE

This document is the Cryptographic Module Security Policy for the Christie IMB-S2 4K Integrated Media Block (IMB) (also referred to herein as the Christie IMB-S2, the cryptographic module, or simply the module). This policy is a specification of the security rules under which the Christie IMB-S2 operates and meets the requirements of FIPS 140-2 Level 2.

1.1 REFERENCE DOCUMENTS

Document No.	Description
FIPS PUB 140-2	Security Requirements For Cryptographic Modules [FIPS PUB 140-2] (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

Table 1 Reference Documents

2. PRODUCT OVERVIEW

The Christie IMB-S2 is a multi-chip embedded cryptographic module. It is a DCI-compliant integrated media block solution to enable the playback of the video, audio and timed text essence on a Christie "Solaria" Series 2 digital cinema projector (2K or 4K projector). The IMB-S2 enables playback of encrypted cinema content packaged as an industry standard Digital Cinema Package (DCP). The IMB-S2 supports playback of digital cinema content from a network attached storage (NAS) or direct attach storage (DAS) device.

2.1 VALIDATED MODULE VERSIONS

The validated module consists of the following:

Hardware version	Firmware version
000-102675-01	1.0.1-2641
000-102675-01	1.0.3-3047
000-102675-01	1.1.0-3271
000-102675-01	1.2.0-3400
000-102675-01	1.2.1-3546
000-102675-01	1.3.0-3704
000-102675-01	1.3.2-3709
000-102675-01	1.5.0-3848
000-102675-01	1.5.2-3897

000-102675-02	1.6.0-3934
000-102675-02	1.7.0-4209

Table 2 Validated module versions

3. SECURITY LEVELS

The IMB is tested to meet the FIPS security requirements shown in Table 3.

FIPS 140-2 Security Requirements	Security Level
1. Cryptographic Module Specification	3
2. Cryptographic Module Ports and Interfaces	2
3. Roles, Services and Authentication	3
4. Finite State Model	2
5. Physical Security	3
6. Operational Environment	N/A
7. Cryptographic Key Management	2
8. EMI/EMC	2
9. Self-Tests	2
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A
FIPS Overall Level	2

Table 3 FIPS 140-2 Security Levels

4. CRYPTOGRAPHIC BOUNDARY

The illustrations below indicate the cryptographic boundary and the physical ports defined on the boundary. Unlabelled connectors are not interfaces on the cryptographic boundary.

Figure 1 Front view of Christie IMB-S2

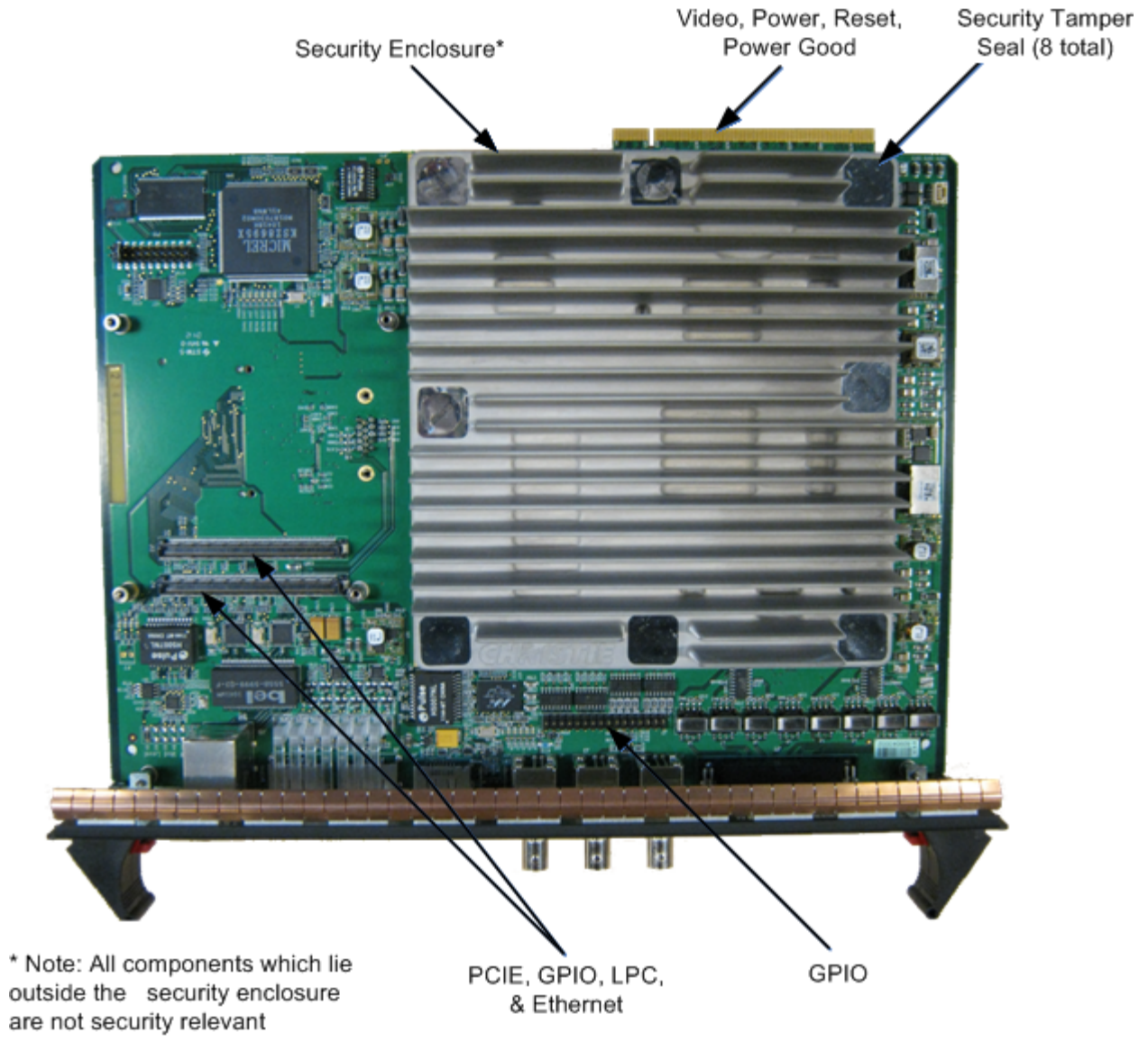

Figure 2 Top View of Christie IMB-S2

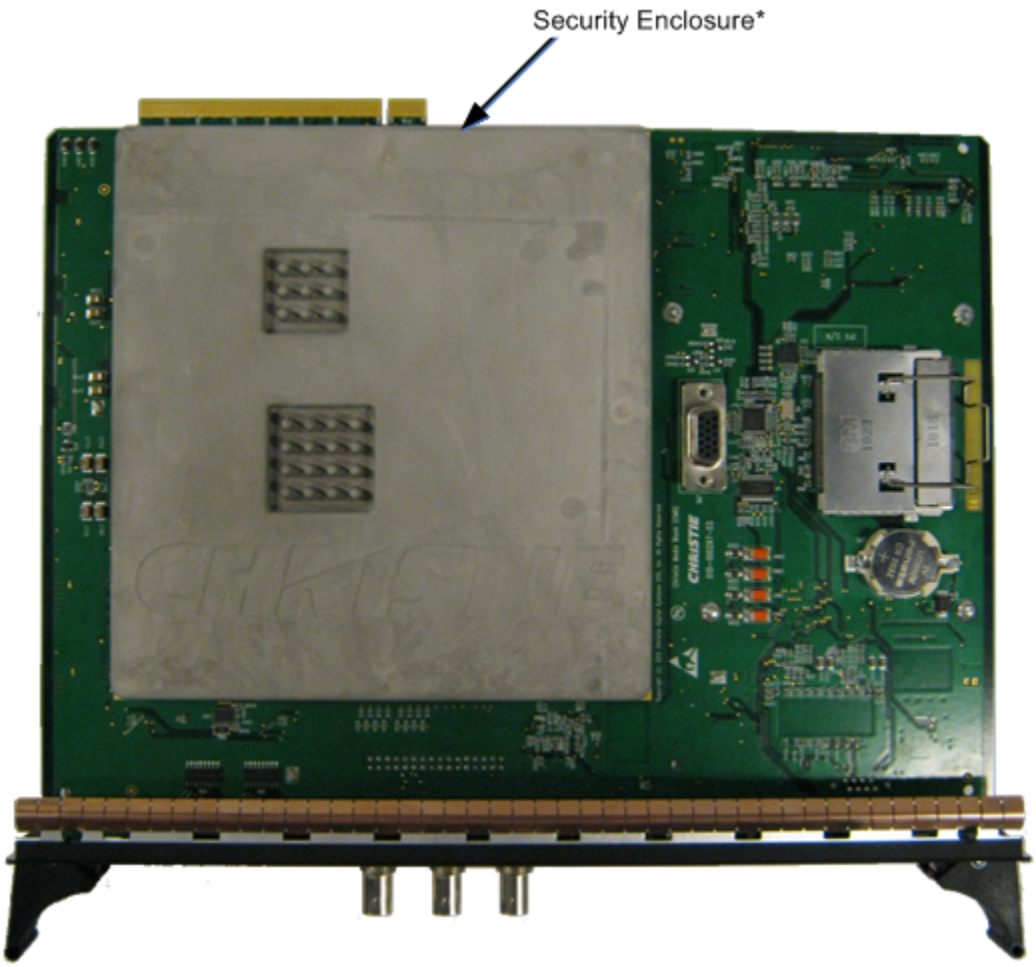

Figure 3 Bottom View of Christie IMB-S2

5. BLOCK DIAGRAM

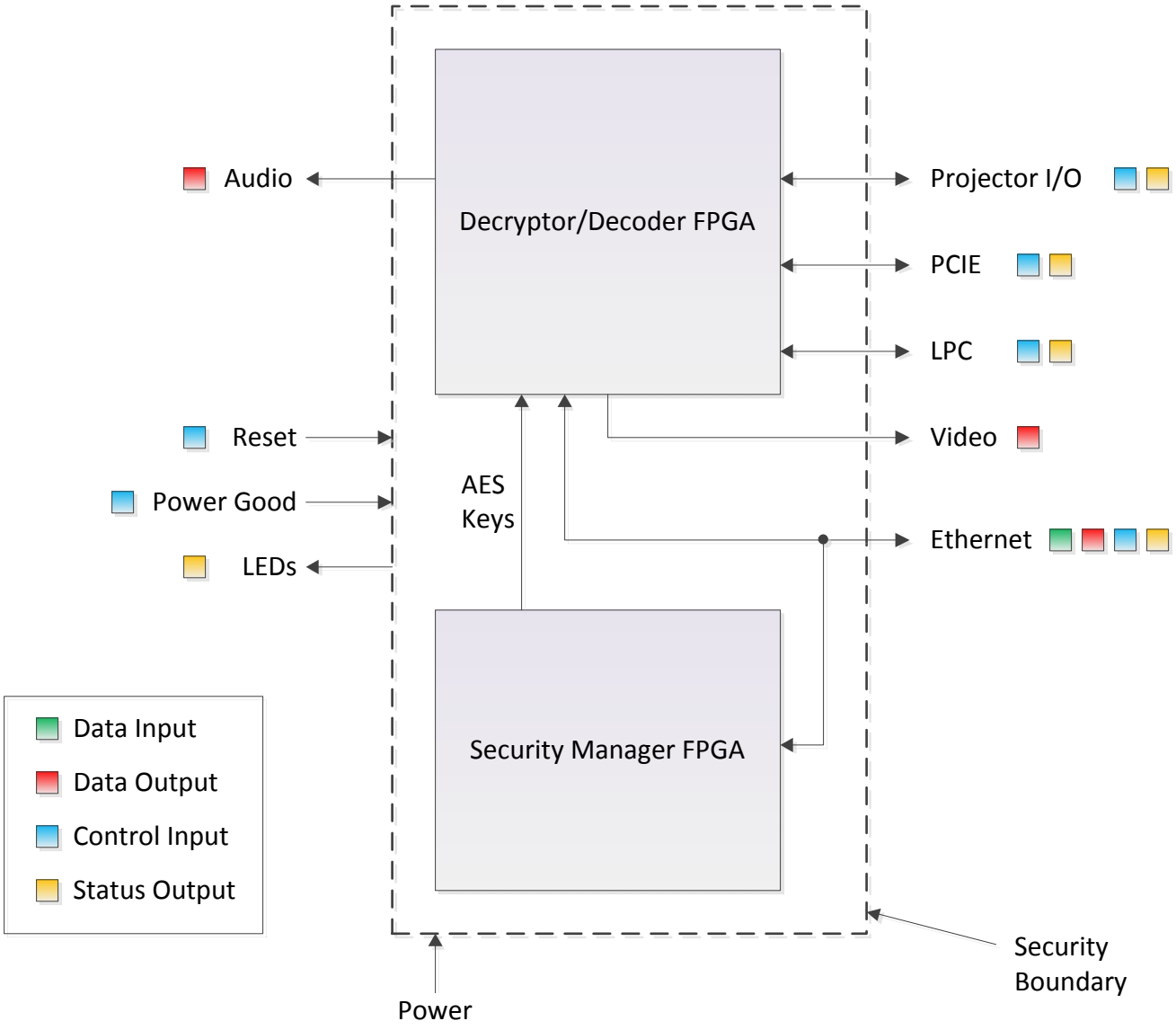

Figure 4 Module Block Diagram

6. APPROVED ALGORITHMS

The cryptographic module supports the following Approved algorithms:

- Symmetric Key Encryption/Decryption
  - Advanced Encryption Standard (AES) – Cert #2043 [CBC Mode]
  - Advanced Encryption Standard (AES) – Cert #2042 [CBC/ECB Mode]
- Asymmetric Key Signature Generation & Verification
  - RSA (2048 bits) – Cert #1062
- Secure Hash Standard (SHS)
  - SHA-1 – Cert #1789
  - SHA-1 – Cert #1788
  - SHA-256 – Cert #1788
- Random Number Generators (DRNG)
  - DRNG – ANSI X9.31 – Cert #1066, 1230
  - DRNG - FIPS 186-2 – Cert #1066
- Message Authentication
  - HMAC-SHA1 – Keyed-Hash Message Authentication Code – Cert #1242
  - HMAC-SHA1 – Keyed-Hash Message Authentication Code – Cert #1241
- Key Derivation
  - KDF - SP 800-135 - Cert #97

7. NON-APPROVED ALGORITHMS

The cryptographic module supports the following non-Approved algorithms:

- Hardware RNG
- MD5 (as used in TLS)
- RSA Key unwrapping of KDMs allowed as a commercially available key establishment technique (key wrapping; key establishment methodology provides 112 bit of encryption strength)
- TI ECDH – considered as non-security relevant data obfuscation (plaintext) and only used to interoperate with legacy equipment
- TI S-box - considered as non-security relevant data obfuscation (plaintext) and only used to interoperate with legacy equipment

8. PORTS AND INTERFACES

The following table maps the logical interfaces to the physical ports:

Logical Interface	Physical Ports
Data Input	Ethernet, PCIE
Data Output	Ethernet, PCIE, Audio, Video
Control Input	Ethernet, Projector I/O, PCIE, LPC, Reset (Manual), Reset (Automatic), Power Good
Status Output	Ethernet, Projector I/O, LPC, LEDs
Power	Power

9. AUTHENTICATION

The Christie IMB-S2 shall support the following distinct operator roles: Crypto Officer, User and Projector. The Christie IMB-S2 does not support a Maintenance role. The cryptographic module shall enforce the separation of roles using identity-based operator identification.

Role	Type of Authentication	Authentication Data
Crypto Officer	Identity-based operator authentication	RSA Digital Signature Verification
User	Identity-based operator authentication	ID and Password
Projector	Identity-based operator authentication	RSA Digital Signature Verification

Table 4 Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
RSA Digital Signature Verification	The authentication is based on RSA 2048 which provides an equivalent encryption strength of 112 bits. 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. There is a 1 second retry delay after each attempt which limits the number of attempts that can be launched per minute. The probability that a random attempt will successfully authenticate to the module within one minute is $60/2^{112}$ which is less than 1/100,000.
ID and Password Verification	The module accepts 63 possible characters and a minimum 6 characters for an authentication secret. The probability that a random attempt will succeed or a false acceptance will occur is 1/(63^6) which is less than

	1/100,000,000. There is a 1 second retry delay after each attempt which limits the number of attempts that can be launched per minute. The probability that a random attempt will successfully authenticate to the module within one minute is 60/(63^6) which is less than 1/100,000.

Table 5 Strength of Authentication Mechanism

10. ROLES AND SERVICES

10.1 CRYPO OFFICER SERVICES

Table 6 summarizes the services that are only available to the Crypto Officer role.

Services	Description	CSP(s) and Key(s)	Type(s) of Access
Upgrade	Update the firmware via RSA signature verification	Christie Root CA Key, Certificate Chain, Christie Firmware Update Key	Read
Zeroization	Zeroizes all sensitive data including plaintext CSPs	AES Master Key, Device Public Key (SM Key), Device Public Key (Log Key), Content Description Keys, Content Integrity Keys (MIC key), TLS Pre-master secret, TLS Master Secret, TLS PRF Internal State, TLS AES Session Key, TLS HMAC Session Key, DRNG Seed (dt, v) and Seed Key (k), DRNG Internal State (X9.31), DRNG Seed Key (xKey), DRNG Internal State (FIPS 186-2), Marriage Password	Write
System Management	System Management functions for the module	TLS Pre-master secret, TLS Master Secret, TLS PRF Internal State, TLS AES Session Key, TLS HMAC Session Key, Marriage Password	Write

Crypto Officer Authentication	Authenticate Crypto Officer	TLS Pre-master secret, SMS Public Key	Read
		TLS Master Secret, TLS PRF Internal State, TLS AES Session Key, TLS HMAC Session Key, DRNG Seed (dt,v) and Seed Key (k), DRNG Internal State (X9.31), Device Public Key (SM Key)	Read, Write
KDM Management	Service for managing KDM information	AES Master Key, Device Private Key (SM Key)	Read
		Content Decryption Keys, DRNG Seed Key (xKey)	Read, Write
CPL Management	Service for managing CPL information	Device Private Key (SM Key)	Read
Encrypted Playback	Service for decrypting encrypted content	AES Master Key, Content Integrity Keys (MIC key), Content Decryption Keys, DRNG Seed Key (xKey), DRNG Internal State (FIPS 186-2)	Read
Log Management	Service for retrieving log data (secure get status)	Device Private Key (Log Key), Device Public Key (Log Key)	Read
Atmos Management	Service for managing decryption keys on Atmos server	TLS Master Secret, TLS PRF Internal State, TLS AES Session Key, TLS HMAC Session Key, DRNG Seed (dt,v) and Seed Key (k), DRNG Internal State (X9.31), Device Public Key (Log Key), Content Decryption Keys	Read, Write

Table 6 Crypto Officer Services

10.2 USER SERVICES

Table 7 summarizes the services that are only available to the User role.

Services	Description	CSP(s) and Key(s)	Type(s) of Access
Suite Management	Initiate, monitor and manage projector suite	Marriage Password	Read, Write

Table 7 User Services

10.3 PROJECTOR SERVICES

Table 8 summarizes the services that are only available to the projector role.

Services	Description	CSP(s) and Key(s)	Type(s) of Access
Marriage Verification	Verify projector marriage	ICP Public Key	Read

Table 8 Projector Services

10.4 UNAUTHENICATED SERVICES

Table 9 summarizes the unauthenticated services that are available.

Services	Description	CSP(s) and Key(s)	Type(s) of Access
Power On Self-Tests	Self-tests performed at Power On	N/A	N/A
Status	Status Output	N/A	N/A
* ICP Status	Monitor ICP status	N/A	N/A

Table 9 Unauthenticated Services

* Note that the unauthenticated service “ICP Status” is accessible by connecting to the cryptographic module through TI ECDH and TI S-box, the use of which is considered non-security relevant data obfuscation from FIPS 140-2 perspective as related to this cryptographic module; this does not provide any security relevant functions and is not used to protect sensitive unclassified data. The I/O therein is obfuscated to support interoperability with existing legacy equipment and is only used to set and retrieve non-security relevant items. **Note that all said service is considered to be plaintext with respect to FIPS 140-2, and do not use the Approved security functions, disclose, modify, or substitute CSPs or otherwise affect the security of the module.**

11. CRITICAL SECURITY PARMETERS & PUBLIC KEYS

11.1 CRITICAL SECURITY PARAMETERS (CSPS)

#	Name	Description
1.	AES Master Key	AES 128 bits - used for key management.
2.	Device Private Key (SM Key)	RSA 2048 – RSA private key that device uses to prove its identity and facilitate secure Transport Layer Security (TLS) communications, and for key transport.
3.	Device Private Key (Log Key)	RSA 2048 - RSA private key used to sign log data.
4.	Content Decryption Keys	AES 128 CBC mode - AES keys that protect encrypted content.
5.	Content Integrity Keys (MIC key)	HMAC-SHA-1 (128-bit key) – content integrity key
6.	TLS Pre-Master Secret	Session specific TLS secret
7.	TLS Master Secret	Session specific TLS secret
8.	TLS PRF Internal State	Session specific TLS secret
9.	TLS AES Session Key	AES 128 CBC mode - AES encryption/decryption of TLS session data
10.	TLS HMAC Session Key	HMAC-SHA-1 (160-bit key) - HMAC integrity of TLS session data
11.	DRNG Seed (dt, v) and Seed Key (k)	X9.31 DRNG - seeding inputs in the Approved DRNG
12.	DRNG Internal State (ANSI X9.31)	X9.31 DRNG - intermediate state of the DRNG
13.	DRNG Seed Key (xKey)	FIPS 186-2 DRNG - seeding inputs in the Approved DRNG
14.	DRNG Internal State (FIPS 186-2)	FIPS 186-2 DRNG - intermediate state of the DRNG
15.	Marriage Password	User role authentication data; 6-32 characters password

11.2 PUBLIC KEYS

#	Name	Description
1.	Christie Root CA Key	RSA 2048 – Christie Root CA key
2.	Certificate Chain	RSA 2048 – Christie Certificate Chain
3.	Christie Firmware Update Key	RSA 2048 – Christie firmware verification key
4.	Device Public Key (SM Key)	RSA 2048 - RSA public key that device uses to prove its identity and facilitate secure Transport Layer Security (TLS) communications, and for key transport.
5.	Device Public Key (Log Key)	RSA 2048 - RSA public key used to verify log signatures.
6.	SMS Public Key	RSA 2048 – TLS Client Public Key
7.	ICP Public Key	RSA 2048 – Identity of the projector
8.	Atmos Public Key	RSA 2048 – Identity of the Dolby Atmos server

12. PHYSICAL SECURITY

The Christie IMB-S2 is a multi-chip embedded cryptographic module which is composed of production-grade components.

The physical security mechanisms of the module includes a hard, opaque and tamper-evident metal enclosure that is monitored 24/7 by battery backed-up tamper detection and response mechanisms. Any attempt to remove the metal enclosure results in instantaneous active zeroization of all plaintext CSPs. Zeroization also occurs if the battery becomes discharged. The module includes tamper-evident labels covering the screws that secure the metal enclosure to the module; said tamper-evident labels are installed as part of the manufacturing process and shall not be removed (i.e. maintenance role is not supported, maintenance interface is not supported).

The tamper-evident metal enclosure and the tamper-evident labels shall be periodically inspected to ensure the physical security of the module is maintained.

All components which lie outside the metal enclosure are not security relevant and are excluded from the FIPS 140-2 requirements. The excluded components are the non-security relevant data input and data output, passive components (capacitors, resistors, inductors), voltage regulators, traces and signals routed to these components, the PCB lying outside the metal enclosure, connectors and the faceplate.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Metal enclosure	Upon receipt of module and as often as feasible.	Visually inspect metal enclosure for scratches, gouges, deformation and other signs of visible signs of tamper.
Tamper Responsive Switches	N/A	N/A
Tamper Evident Seals	Upon receipt of module and as often as feasible.	Visually inspect the tamper evident seals for scratches, gouges, deformation or other physical signs of tampering.

Table 10 Inspection/Testing of Physical Security Mechanisms

If any tampering of the module is observed or suspected, remove the module from service and return it to Christie Digital.

13. OPERATIONAL ENVIRONMENT

The IMB operates in a limited operational environment that only allows the loading of trusted and validated firmware binary images through an authenticated service. Firmware binary images are signed by an RSA key which is part of the Christie certificate chain. The RSA signature verification algorithm has been validated (RSA Cert. #1062).

14. SELF-TESTS

The module performs the following self-tests:

- Power Up Self-Tests
  - Cryptographic algorithm tests:
    - ANSI X9.31 DRNG KAT
    - FIPS 186-2 DRNG KAT
    - AES 128 CBC Encrypt/Decrypt KAT
    - SHA-1 KAT
    - SHA-256 KAT
    - HMAC-SHA-1 KAT (using 160 bit HMAC key)
    - RSA 2048 Signature Generation (using SHA-1)/ RSA 2048 Signature Verification KAT
    - SHA-1 KAT
    - AES128 CBC Decrypt KAT
    - HMAC-SHA-1 KAT (using 160 bit HMAC key)
    - KDF 800 KAT
  - Firmware Integrity Test - EDC that meets requirements of AS09.24
  - Critical Functions Tests:
    - RSA 2048 Encrypt/Decrypt KAT
- Conditional Self-Tests
  - Continuous Random Number Generator (RNG) tests:
    - ANSI X9.31 RNG
    - FIPS 186-2 RNG
    - Hardware RNG
  - Firmware Load Test (RSA signature verification)

15. MITIGATION OF OTHER ATTACKS

The cryptographic module does not mitigate any specific attacks beyond the scope of FIPS 140-2.

Other Attacks	Mitigation Mechanism	Specific Limitations
N/A	N/A	N/A

Table 11 Mitigation of Other Attacks

16. SECURITY RULES

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

- The module does not support a bypass capability or a maintenance interface.
- The module supports concurrent operators. However, the module does not support more than one operator per role. The operators may not switch roles without re-authenticating.
- The operator must re-authenticate on each power-up event.
- The module inhibits data output during an error state, zeroization, key generation and during the power-up self-tests.
- The module shall enforce identity-based authentication.
- The module does not provide feedback of authentication data.
- The module does not support a non-FIPS mode of operation. The module only operates in an Approved mode of operation. The module is initialized for FIPS mode of operation from the factory.
- The operator may verify that the module is running in an approved mode of operation by verifying the FIPS LED status (Note: the FIPS LED is in position #4):
    - Orange – module is running power-up self-tests
    - Green – module has successfully performed self-tests and is running in FIPS mode
    - Red – module has entered an error state; all cryptographic operations are inhibited.
- An error state may be cleared by power-cycling the module.
- The module provides logical separation between all the data input, control input, data output and status output interfaces.
- The module protects all CSPs from unauthenticated disclosure and unauthorized modification. The module protects all public keys from unauthorized modification and unauthorized substitution.
- The module does not support manual key entry. A manual key entry test is not implemented.
- The module does not support split-knowledge processes.
- The operator may perform on-demand power-on self-test by recycling power to the module.
- The status output does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.

17. ACRONYMS

Acronym	Definition
AES	Advanced Encryption Standard
CSP	Critical Security Parameter
DAS	Direct Attached Storage
DCI	Digital Cinema Initiatives, LLC
DCP	Digital Cinema Package
DRNG	Deterministic Random Number Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standards
FPGA	Field Programmable Gate Array
HMAC	Hashed Message Authentication Code
ICP	Integrated Cinema Processor
IMB	Image Media Block
KAT	Known Answer Test
MAC	Media Access Control
NAS	Network Attached Storage
RSA	Rivest-Shamir-Adleman
SHA	Secure Hash Algorithm
TI	Texas Instruments Incorporated
TI ECDH	Considered as non-security relevant data obfuscation (plaintext) and only used to interoperate with legacy equipment
TI S-box	Considered as non-security relevant data obfuscation (plaintext) and only used to interoperate with legacy equipment
TLS	Transport Layer Security