Security Policy

No: *010-107949-01 Rev: 3*

REVISION #	ECO #	REVISION #	ECO #
1	18-2103	3	19-0509
2	18-3663		

Title: Christie IMB-S3 4K Integrated Media Block (IMB) Security Policy

Product(s): Christie IMB-S3 4K Integrated Media Block (IMB)

Prepared by: Kevin Draper

Prep'd Date: 05/11/2017

Last Updated: 02/05/2019

Detailed Revision History

Revision	Description of Changes	Date
1	Initial Public Release	05/11/2018
2	Updated for firmware versions 2.1.5-4575 & 2.1.5-4582	10/03/2018
3	Updates to clarify security details	02/05/2019

Table of Contents

Table of Figures

List of Tables

1. SCOPE

This document is the Cryptographic Module Security Policy for the Christie IMB-S3 4K Integrated Media Block (IMB) (also referred to herein as the Christie IMB-S3, the cryptographic module, or simply the module). This policy is a specification of the security rules under which the Christie IMB-S3 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-S3 is a multi-chip embedded cryptographic module. In the FIPS Approved mode of operation, the module only provides the "Upgrade" service.

In the non-Approved mode of operation the module is a DCI-compliant integrated media block solution to enable the playback of the video, audio and timed text essence on a Christie "Fusion" Series 3 digital cinema projector (2K or 4K projector). The IMB-S3 enables playback of encrypted cinema content packaged as an industry standard Digital Cinema Package (DCP). The IMB-S3 supports playback of digital cinema content from a network attached storage (NAS) device.

2.1 VALIDATED MODULE VERSIONS

The validated module consists of the following:

Hardware version	Firmware version
000-105081-03	2.1.5-4575
000-105081-03	2.1.5-4582

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	2
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. MODES OF OPERATION

The Christie IMB-S3 provides a FIPS Approved mode of operation and a non-Approved mode of operation.

To determine that the module is running in a FIPS Approved mode of operation, the operator shall verify the FIPS LED status:

- 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.

In the FIPS Approved mode of operation, the module only provides the "Upgrade" service. The module is in the non-Approved mode of operation whenever any of the disallowed services in Section 11.4, Table 12 Non-Approved Services, are invoked.

5. CRYPTOGRAPHIC BOUNDARY

The illustrations below indicate the cryptographic boundary and the physical ports defined on the boundary.

The cryptographic boundary is the outer physical perimeter of the module's PCB board; the effective security boundary is the physical perimeter of the module's metal Security Enclosure.

Everything outside the metal Security Enclosure is excluded from FIPS 140-2 Requirements. Unlabelled connectors are not interfaces on the cryptographic boundary.

Figure 1 Front view of Christie IMB-S3

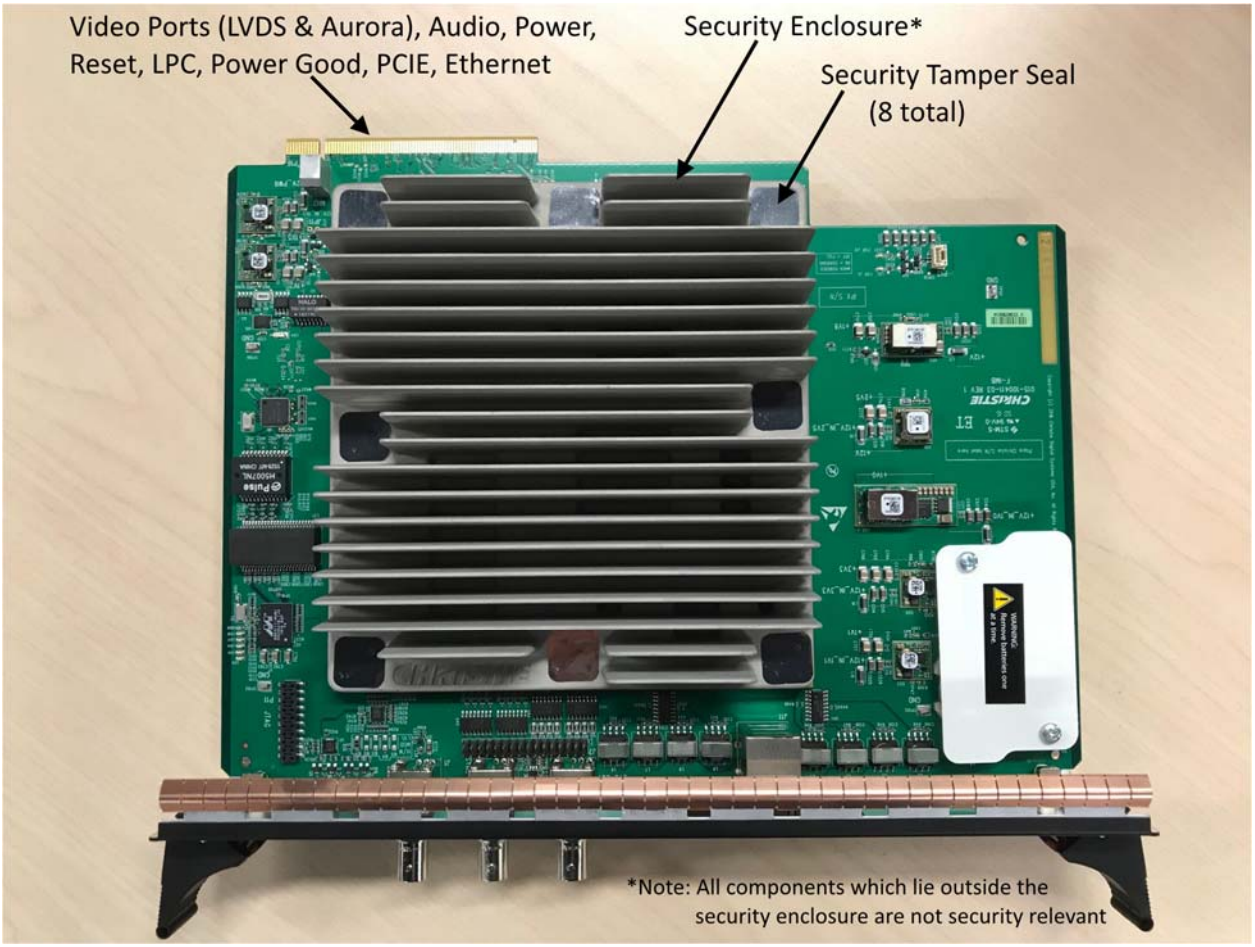

Figure 2 Top View of Christie IMB-S3

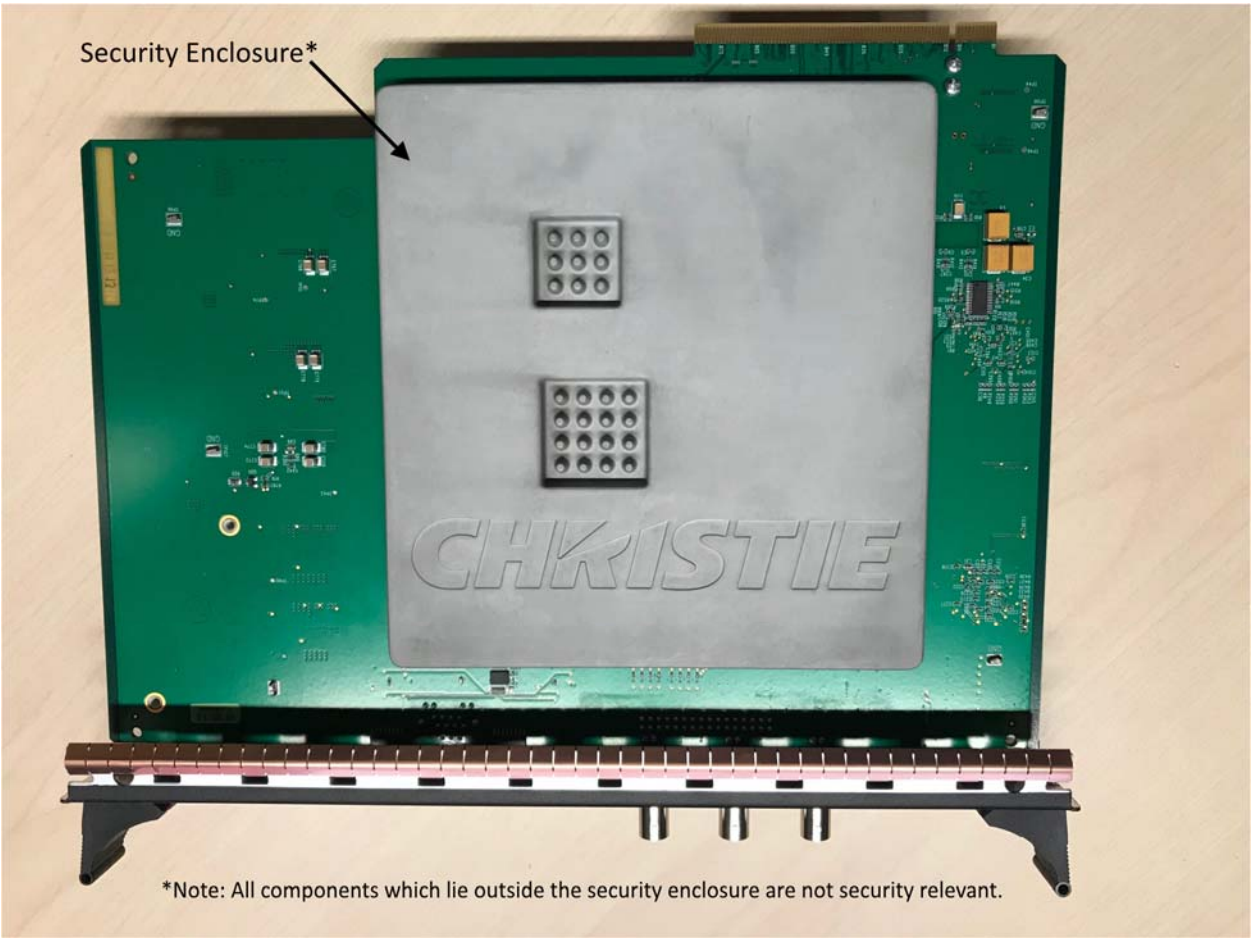

Figure 3 Bottom View of Christie IMB-S3

6. BLOCK DIAGRAM

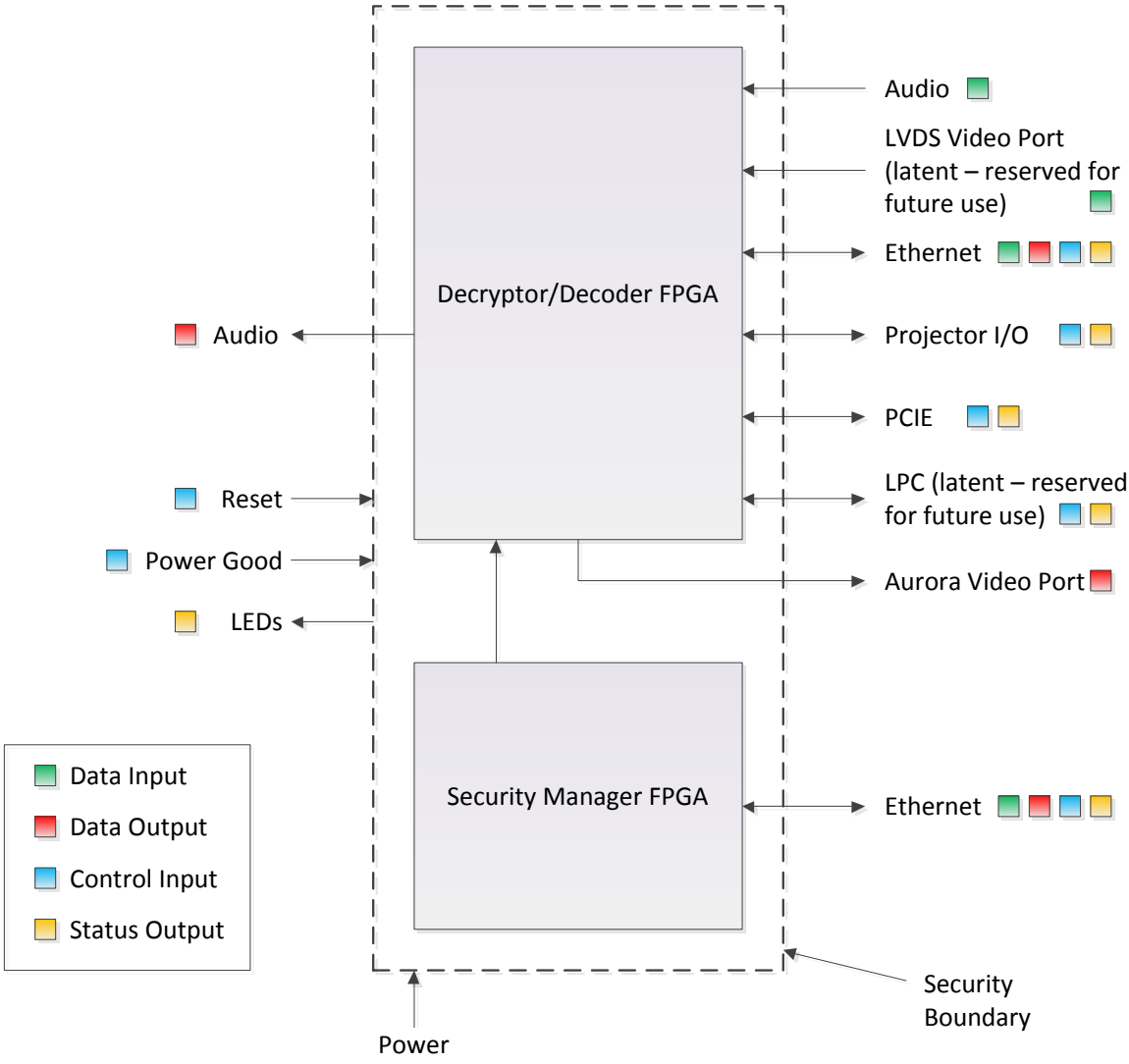

Figure 4 Module Block Diagram

7. APPROVED ALGORITHMS

The cryptographic module only supports the following Approved algorithms in the FIPS Approved mode of operation:

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
1062	RSA	FIPS 186-2	PKCS1.5 with SHA-256	2048	Digital Signature Verification
1788	SHS	FIPS 180-4	SHA-256	N/A	Message Digest

Note: CAVP certificates contain many other algorithms/modes that are not supported by the Module in the FIPS Approved Mode

Table 4 FIPS Approved Algorithms

8. NON-APPROVED ALGORITHMS

The cryptographic module supports the following non-Approved algorithms in the non-Approved mode of operation:

Algorithm	Use
AES-128-CBC (non-compliant)	Encryption / Decryption
AES-128-ECB (non-compliant)	Encryption / Decryption
ANSI X9.31 DRNG	Random Number Generation
FIPS 186-2 DRNG	Random Number Generation
HMAC-SHA-1 (non-compliant)	Message Authentication
MD5	Message digest in TLS 1.0 / 1.1
NDRNG	Seeding for the DRNG
RSA 2048 (non-compliant)	Digital Signature Generation: RSA-2048 with SHA-1 and RSA-2048 with SHA-256; Digital Signature Verification: RSA-2048 with SHA-1; RSA-2048 Decryption
SP800-135 TLS v1.0 KDF (non-compliant)	TLS 1.0 / 1.1 Key derivation
SHA-1 (non-compliant)	Message Digest
TI ECDH	Considered as non-security relevant data obfuscation (plaintext) and only used to interoperate with legacy equipment

Table 5 Non-Approved Algorithms

9. PORTS AND INTERFACES

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

Logical Interface	Physical Ports
Data Input	Ethernet, Audio, LVDS Video Port (latent – reserved for future use)
Data Output	Ethernet, Audio, Aurora Video Port
Control Input	Ethernet, Projector I/O, PCIE, LPC (latent – reserved for future use), Reset, Power Good
Status Output	Ethernet, Projector I/O, PCIE, LPC (latent – reserved for future use), LEDs
Power	Power

Table 6 Ports and Interfaces

10. AUTHENTICATION

The Christie IMB-S3 shall support the following distinct operator roles: Crypto Officer and User.The Christie IMB-S3 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	RSA Digital Signature Verification

Note: See Table 4 for applicable Modes and Key Lengths

Table 7 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.

Table 8 Strength of Authentication Mechanism

11. ROLES AND SERVICES

11.1 CRYPTO OFFICER SERVICES

Table 9 summarizes the services that are available to the Crypto Officer role.

Services	Description	Public 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

Table 9 Crypto Officer Services

11.2 USER SERVICES

Table 10 summarizes the services that are available to the User role.

Services	Description	Public 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

Table 10 User Services

11.3 UNAUTHENTICATED SERVICES

Table 11 summarizes the unauthenticated services that are available to the module. The services are implicitly allocated to each authorized role, since both the Crypto Officer and User can invoke Power On Self-Tests by power-cycling the module and similarly observe Status output via the LEDs.

Services	Description	Public 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

Table 11 Unauthenticated Services

11.4 NON-APPROVED SERVICES

The following services are supported only in the non-Approved mode of operation:

Roles	Services	Description	Non-Approved Algorithms
Crypto Officer/ User	Projector Status	Monitor Projector status	TI-ECDH
Crypto Officer/ User	Zeroization	Zeroizes keys used in the non-Approved mode of Operation	N/A
Crypto Officer/ User	System Management	System Management functions for the module	ANSI X9.31 DRNG NDRNG MD5 RSA 2048 (non-compliant) AES-128-CBC (non-compliant) HMAC-SHA-1 (non-compliant) SHA-1 (non-compliant) SP800-135 TLS v1.0 KDF (non-Compliant)
Crypto Officer/ User	Digital Cinema Authentication	Authenticate Digital Cinema	ANSI X9.31 DRNG NDRNG MD5 RSA 2048 (non-compliant) AES-128-CBC (non-compliant) HMAC-SHA-1 (non-compliant) SHA-1 (non-compliant) SP800-135 TLS v1.0 KDF (non-Compliant)
Crypto Officer/ User	KDM Management	Service for managing KDM information	MD5 HMAC-SHA-1 (non-compliant) SHA-1 (non-compliant) SP800-135 TLS v1.0 KDF (non-

			Compliant) RSA 2048 (non-compliant) AES-128-CBC (non-compliant) AES-128-ECB (non-compliant) ANSI X9.31 DRNG FIPS 186-2 DRNG NDRNG
Crypto Officer/ User	CPL Management	Service for managing CPL information	ANSI X9.31 DRNG NDRNG MD5 RSA 2048 (non-compliant) AES-128-CBC (non-compliant) HMAC-SHA-1 (non-compliant) SHA-1 (non-compliant) SP800-135 TLS v1.0 KDF (non-Compliant)
Crypto Officer/ User	Encrypted Playback	Service for decrypting encrypted content	ANSI X9.31 DRNG NDRNG MD5 RSA 2048 (non-compliant) AES-128-CBC (non-compliant) HMAC-SHA-1 (non-compliant) SHA-1 (non-compliant) SP800-135 TLS v1.0 KDF (non-Compliant)
Crypto Officer/ User	Log Management	Service for retrieving log data	ANSI X9.31 DRNG NDRNG MD5 RSA 2048 (non-compliant) AES-128-CBC (non-compliant)

			HMAC-SHA-1 (non-compliant) SHA-1 (non-compliant) SP800-135 TLS v1.0 KDF (non-Compliant)
Crypto Officer/ User	Suite Management	Initiate, monitor and manage projector suite	ANSI X9.31 DRNG NDRNG MD5 RSA 2048 (non-compliant) AES-128-CBC (non-compliant) HMAC-SHA-1 (non-compliant) SHA-1 (non-compliant) SP800-135 TLS v1.0 KDF (non-Compliant)
Crypto Officer/ User	Marriage Verification	Verify projector marriage	ANSI X9.31 DRNG NDRNG MD5 RSA 2048 (non-compliant) AES-128-CBC (non-compliant) HMAC-SHA-1 (non-compliant) SHA-1 (non-compliant) SP800-135 TLS v1.0 KDF (non-Compliant)

Table 12 Non-Approved Services

12. CRITICAL SECURITY PARMETERS & PUBLIC KEYS

12.1 CRITICAL SECURITY PARAMETERS (CSPS)

The module does not contain secret, private keys and/or CSPs in the Approved mode of operation.

12.2 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

Table 13 Public Keys

13. PHYSICAL SECURITY

The Christie IMB-S3 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. 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. Periodic inspection will occur each time the module is inserted or removed from the projector.

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.

Note: The module hardness testing was only performed at a single temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.

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 14 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.

14. OPERATIONAL ENVIRONMENT

The Christie IMB-S3 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).

Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation.

15. SELF-TESTS

The module performs the following self-tests:

- Power Up Self-Tests
  - Cryptographic algorithm tests:
    - SHA-256 KAT
    - RSA 2048 Signature Verification KAT
  - Firmware Integrity Test - EDC that meets requirements of AS09.24
  - Critical Functions Tests: N/A
- Conditional Self-Tests
  - Firmware Load Test (RSA signature verification – RSA 2048 with SHA-256)

16. 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 15 Mitigation of Other Attacks

17. 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 and during the power-up self-tests.
- The module shall enforce identity-based authentication.
- The module does not provide feedback of authentication data.
- An error state may be cleared by power-cycling the module.
- Failure of Power Up Self-Tests, described in Section 15, will result in a “Red” FIPS LED Status. The module will enter the error state; all cryptographic operations are inhibited.
- Failure of conditional Self-Tests, described in Section 15, will result in a “soft” error. The error is indicated via the Status service as follows:

  [ERR][16384] [SM UPGRADE] Signature verification failed.
  [ERR][16384] [SM UPGRADE] Upgrade package integrity check failed.

- The module provides logical separation between all the data input, control input, data output and status output interfaces.
- 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.

18. 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
IMB	Image Media Block
KAT	Known Answer Test
KDM	Key Delivery Message – as per SMPTE 430-1
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
TLS	Transport Layer Security

19. APPENDIX A: CRITICAL SECURITY PARAMETERS

The module does not contain secret, private keys and CSPs in the Approved mode of operation.

20. APPENDIX B: PUBLIC KEYS

The module supports the following public keys:

1. Christie Root CA Key

   Description: digitally signed and thus authorizes other public keys to be used by the module for a defined purpose

   Type: RSA 2048

   Generation: N/A - Installed into the module within the secure factory during manufacturing

   Storage: Stored in Flash in self-signed certificate; RAM

   Entry: N/A - Installed into the module within the secure factory during manufacturing

   Output: In X.509 certificate upon request

   Establishment: N/A

   Key-to-entity: via memory location and CRC-16

2. Certificate Chain

   Description: digitally verify public keys

   Type: RSA 2048

   Generation: N/A - Installed into the module within the secure factory during manufacturing

   Storage: Stored in Flash in certificate signed by Christie Root CA Key; RAM

   Establishment: N/A

   Entry: N/A - Installed into the module within the secure factory during manufacturing

   Output: In X.509 certificate upon request

   Key-to-entity: via memory location and CRC-16

3. Christie Firmware Update Key

   Description: Used to securely update the firmware via RSA signature verification via the Upgrade service.

   Type: RSA 2048

   Generation: N/A - generated outside of the crypto boundary by Christie

   Storage: RAM

   Establishment: N/A

   Entry: Entered into the module via a certificate signed by the Certificate Chain

   Output: In X.509 certificate upon request

   Key-to-entity: via memory location and CRC