Security Policy

No: *010-105847-01 Rev: 2*

REVISION #	ECO #	REVISION #	ECO #
1	15-0450		
2	15-5417		

Title: Christie F-IMB Security Policy

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

Prepared by: **Kevin Draper**

Prep'd Date: **02/02/2015**

Last Updated: **12/18/2015**

Detailed Revision History

Revision	Description of Changes	Date
1	First Revision	08/26/2015
2	Initial Public Release	12/15/2015

This document may only be reproduced in its entirety without revision including this statement.

Copyright ©2015 Christie Digital Systems Canada Inc.

Table of Contents

Table of Figures

List of Tables

1. SCOPE

This document is the Cryptographic Module Security Policy for the Christie F-IMB 4K Integrated Media Block (IMB) (also referred to herein as the Christie F-IMB, the cryptographic module, or simply the module). This policy is a specification of the security rules under which the Christie F-IMB 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 F-IMB 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 “Fusion” Series 3 digital cinema projector (2K or 4K projector). The F-IMB enables playback of encrypted cinema content packaged as an industry standard Digital Cinema Package (DCP). The F-IMB 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
000-105081-01	1.6.0-4217

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 F-IMB 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.

The non-Approved mode of operation uses the TI ECDH algorithm via the "Projector Status" Service. TI ECDH is strictly disallowed in the FIPS Approved mode of operation. Use of the "Projector Status" Service Places the module in the non-Approved mode of operation. Upon completion of the "Projector Status" Service, the module automatically transitions back into the FIPS Approved mode of operation.

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.

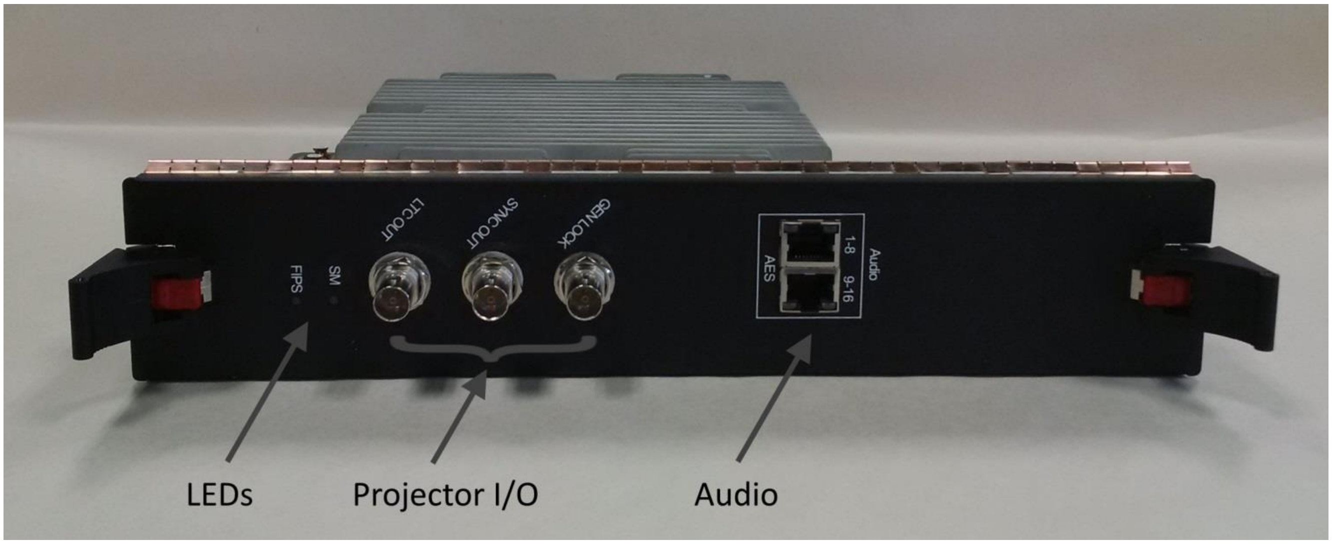


Figure 1 Front view of Christie F-IMB

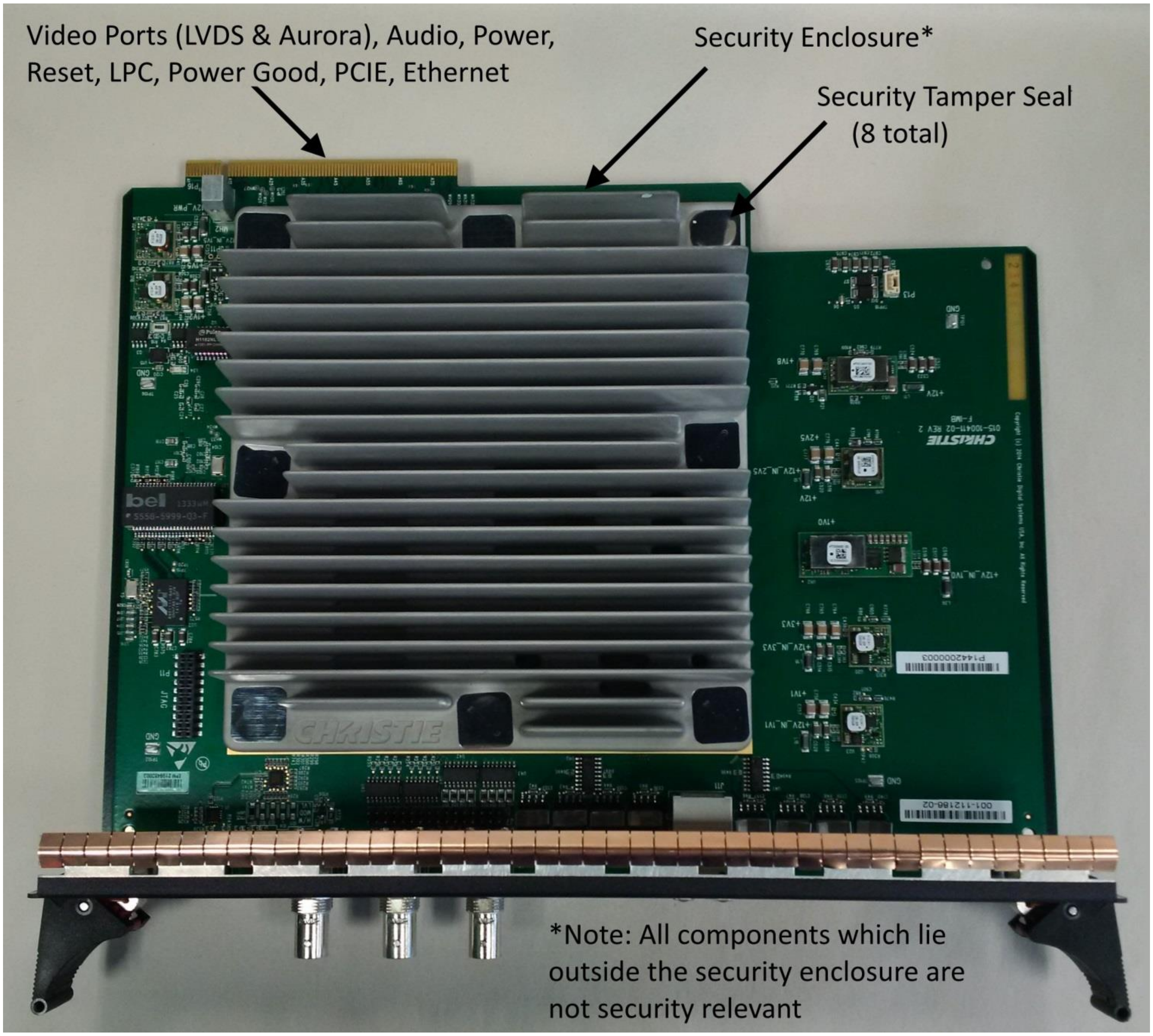
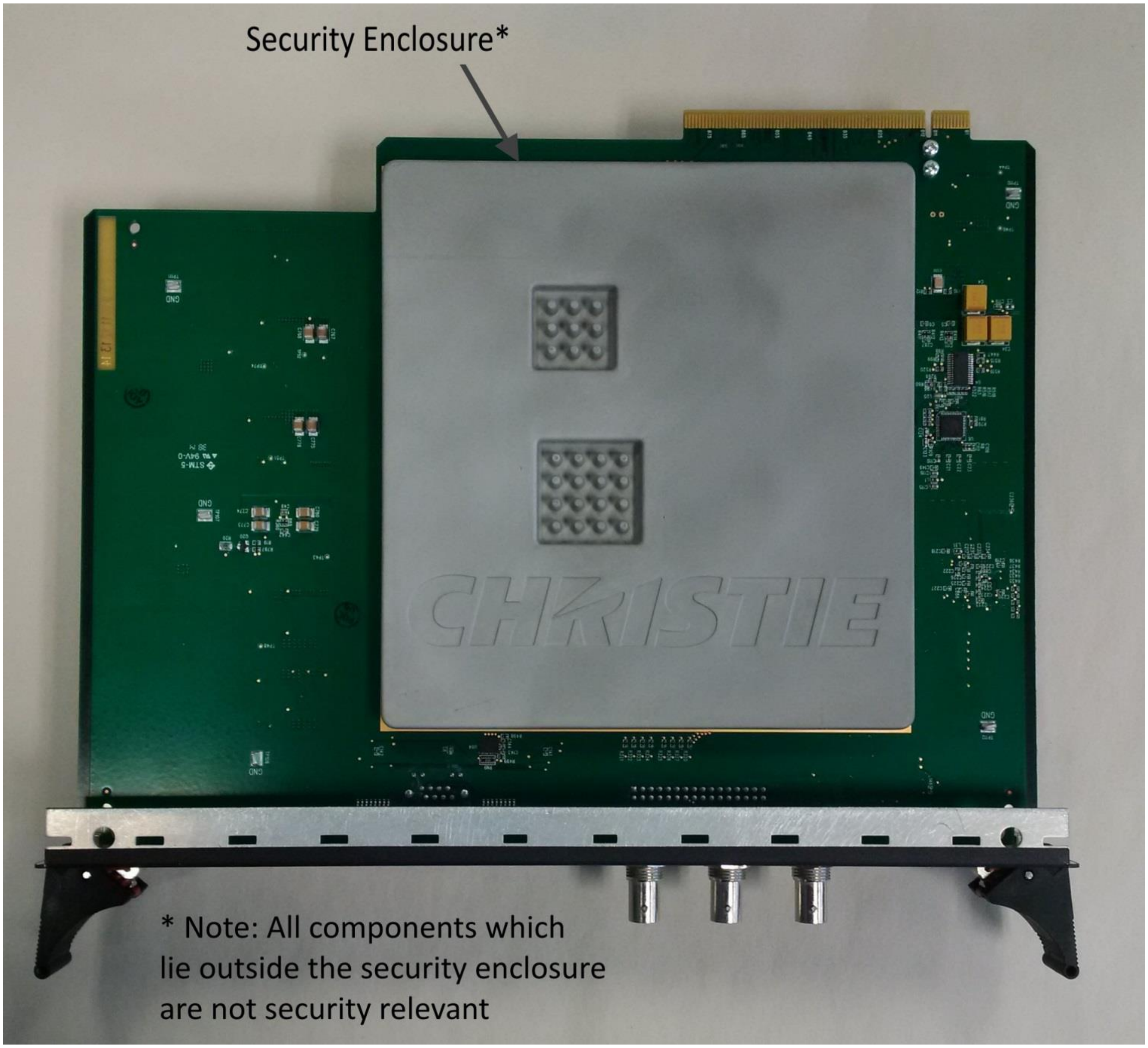

Video Ports (LVDS & Aurora), Audio, Power, Reset, LPC, Power Good, PCIE, Ethernet
Security Enclosure*
Security Tamper Seal (8 total)
*Note: All components which lie outside the security enclosure are not security relevant

Figure 2 Top View of Christie F-IMB



* Note: All components which lie outside the security enclosure are not security relevant

Figure 3 Bottom View of Christie F-IMB

6. BLOCK DIAGRAM

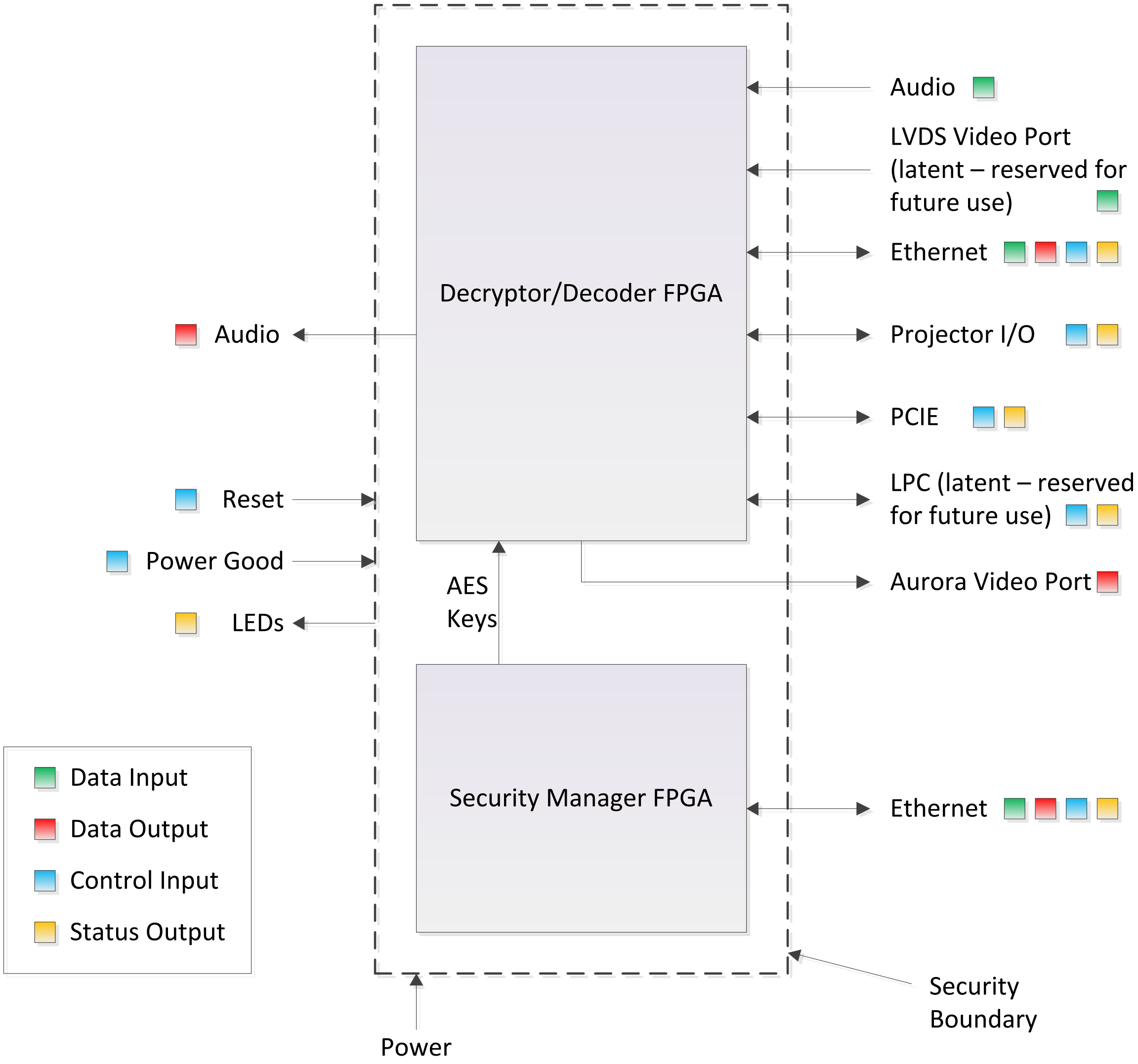


Figure 4 Module Block Diagram

7. 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 (128-bit key) – Cert #1242
  - HMAC-SHA1 – Keyed-Hash Message Authentication Code (160-bit key) – Cert #1241
- Key Derivation
  - KDF - SP 800-135 - Cert #97
    [Note: TLS v1.1 is latent functionality and not directly exposed to any service provided by the module]

The following protocols have not been reviewed or tested by the CAVP and CMVP:

- TLS v1.0
- TLS v1.1 [Note: TLS v1.1 is latent functionality and not directly exposed to any service provided by the module]

8. NON-APPROVED ALGORITHMS IN FIPS MODE

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

- NDRNG
- 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)

9. NON-APPROVED ALGORITHMS

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

- TI ECDH – considered as non-security relevant data obfuscation (plaintext) and only used to interoperate with legacy equipment

10. 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 4 Ports and Interfaces

11. AUTHENTICATION

The Christie F-IMB shall support the following distinct operator roles: Crypto Officer, User and Projector. The Christie F-IMB 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 5 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 6 Strength of Authentication Mechanism

12. ROLES AND SERVICES

12.1 CRYPTO OFFICER SERVICES

Table 7 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	Read, Write

		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)	
KDM Management	Service for managing KDM information	AES Master Key, Device Private Key (SM Key) Content Decryption Keys, DRNG Seed Key (xKey)	Read 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

Table 7 Crypto Officer Services

12.2 USER SERVICES

Table 8 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 8 User Services

12.3 PROJECTOR SERVICES

Table 9 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	Projector Public Key	Read

Table 9 Projector Services

12.4 UNAUTHENICATED SERVICES

Table 10 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

Table 10 Unauthenticated Services

12.5 NON-APPROVED SERVICES

The following services are supported in the non-Approved mode of operation and can be invoked by any operator (unauthenticated):

Services	Description	CSP(s) and Key(s)	Type(s) of Access
* Projector Status	Monitor Projector status	N/A	N/A

Table 11 Non-Approved Services

* Note that the unauthenticated service “Projector Status” is accessible by connecting to the cryptographic module through TI ECDH in the **non-Approved mode of operation**, 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 the Projector Status service is considered to be plaintext with respect to FIPS 140-2, and does not use the Approved security functions, disclose, modify, or substitute CSPs or otherwise affect the security of the module.**

13. CRITICAL SECURITY PARMETERS & PUBLIC KEYS

13.1 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

Table 12 Critical Security Parameters

13.2 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.	Projector Public Key	RSA 2048 – Identity of the projector

Table 13 Public Keys

14. PHYSICAL SECURITY

The Christie F-IMB 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 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.

15. OPERATIONAL ENVIRONMENT

The Christie F-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).

16. 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 / RSA 2048 Signature Verification KAT
        - SHA-1 KAT (executed for SHA (Cert. #1789))
        - AES128 CBC Decrypt KAT (executed for AES (Cert. #2043))
        - HMAC-SHA-1 KAT (using 160 bit HMAC key) (executed for HMAC (Cert. #1242))
        - SP 800-135 KDF 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
        - NDRNG
    - Firmware Load Test (RSA signature verification – RSA 2048 with SHA-256)

17. 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

18. 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.
- 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.

19. 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

20. APPENDIX A: CRITICAL SECURITY PARAMETERS

The Module supports the following critical security parameters:

1. AES Master Key

   Description: used for re-encrypting KDM AES keys to be persisted in Flash.

   Type: AES 128

   Generation: Via Approved ANSI X9.31 DRNG; as per SP800-133 Section 7.1, key generation is performed as per the “Direct Generation” of Symmetric Keys which is an Approved key generation method.

   Storage: Security manager hardware; controlled zeroizeable RAM

   Establishment: N/A

   Entry: N/A

   Output: N/A

   Key-to-entity association: Bound to the process of internal key management, stored at a specific memory location, and via CRC-16.

   Zeroization: Built in function on security manager hardware zeroizes all internal memory on power-down and power-on tamper events. Controlled RAM will be zeroized on power-down and powered-on tamper events.

2. Device Private Key (SM Key)

   Description: RSA private key that device uses to prove its identity and facilitate secure Transport Layer Security (TLS) communications, and to decrypt the KDMs.

   Type: RSA 2048

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

   Storage: Stored in Flash, encrypted with AES Master Key.

   Establishment: N/A

   Entry: N/A

   Output: N/A

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

   Zeroization: Built in function on security manager hardware zeroizes all internal memory on power-down and power-on tamper events.

3. Device Private Key (Log Key)

Description: RSA private key used to sign log data.

Type: RSA 2048

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

Storage: Stored in Flash, encrypted with AES Master Key

Establishment: N/A

Entry: N/A

Output: N/A

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

Zeroization: Built in function on security manager hardware zeroizes all internal memory on power-down and power-on tamper events. Controlled RAM will be zeroized on power-down and powered-on tamper events.

4. Content Decryption Keys

   Description: Key Delivery Message (KDM) AES keys that protect content.

   Type: AES 128 CBC mode (using an IV as specified by SMPTE 429-6)

   Generation: N/A

   Storage: Stored in Flash, encrypted with AES Master Key.

   Establishment: RSA wrapped outside of crypto boundary with Device Public Key and entered into the crypto boundary.

   Entry: Entered in RSA wrapped format

   Output: N/A

   Key-to-entity association: via memory location

   Zeroization: Controlled RAM, and Key Buffer in media decryptor on power-down and power-on tamper events.

5. Content Integrity Keys (MIC key)

   Description: HMAC-SHA-1 keys that protect the integrity of compressed content (integrity pack check parameters)

   Type: HMAC-SHA-1 (128-bit key)

   Generation: Via Approved FIPS 186-2 DRNG; as per SP800-133 Section 7.1, key generation is performed as per the “Direct Generation” of Symmetric Keys which is an Approved key generation method.

   Storage: N/A

Establishment: N/A

Entry: N/A

Output: N/A

Key-to-entity: via memory location

Zeroization: RAM and key buffer in media decyptor zeroized on power-down and power-on tamper events.

6. TLS Pre-Master Secret

   Description: input to TLS PRF

   Type: Session specific TLS secret

   Generation: N/A

   Storage: Plaintext in RAM

   Establishment: generated outside the cryptoboudary by the TLS client; entered into the crypto boundary RSA wrapped with Device Public Key.

   Entry: see Establishment

   Output: N/A

   Key-to-entity: via TLS session identifiers and port number

   Zeroization: Zeroized when TLS session is closed and via tamper.

7. TLS Master Secret

   Description: input to TLS PRF

   Type: Session specific TLS secret

   Generation: N/A

   Storage: RAM

   Establishment: TLS KDF as per SP800-135 Section 4.2.1 and 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4

   Entry: N/A

   Output: N/A

   Key-to-entity: via TLS session identifiers and port number

   Zeroization: Zeroized when TLS session is closed and via tamper.

8. TLS PRF Internal State

   Description: intermediate state variables of PRF

   Type: Session specific TLS secret

   Generation: N/A

   Storage: RAM

   Establishment: TLS KDF as per SP800-135 Section 4.2.1 and 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4

   Entry: N/A

   Output: N/A

   Key-to-entity: via TLS session identifiers and port number

   Zeroization: Zeroized when TLS session is closed and via tamper.

9. TLS AES Session Key

   Description: AES encryption of TLS session data

   Type: AES 128

   Generation: N/A

   Storage: RAM

   Establishment: TLS KDF as per SP800-135 Section 4.2.1 and 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4

   Entry: N/A

   Output: N/A

   Key-to-entity: via TLS session identifiers and port number

   Zeroization: Zeroized when TLS session is closed and via tamper.

10. TLS HMAC Session Key

    Description: HMAC integrity verification of TLS session data

    Type: HMAC-SHA-1 (160-bit key)

    Generation: N/A

    Storage: RAM

    Establishment: TLS KDF as per SP800-135 Section 4.2.1 and 4.2.2; allowed method as per FIPS 140-2 IG D.8 Scenario 4

Entry: N/A

Output: N/A

Key-to-entity: via TLS session identifiers and port number

Zeroization: Zeroized when TLS session is closed and via tamper.

11. DRNG Seed (dt, v) and Seed Key (k)

    Description: seeding inputs in the Approved DRNG (X9.31)

    Type: FIPS 186-2 DRNG

    Generation: via NDRNG from security manager hardware

    Storage: RAM

    Establishment: N/A

    Entry: N/A

    Output: N/A

    Key-to-entity: via data structure and pointer in memory

    Zeroization: Memory location in RAM and security manager hardware zeroized via zeroize command and via tamper.

12. DRNG Internal State

    Description: intermediate state of the DRNG (X9.31)

    Type: X9.31 DRNG

    Generation: inside crypto boundary via X9.31 DRNG

    Storage: RAM

    Establishment: N/A

    Entry: N/A

    Output: N/A

    Key-to-entity: via data structure and pointer in memory

    Zeroization: Memory location in RAM zeroized via zeroize command and via tamper.

13. DRNG Seed Key (xKey)

    Description: seeding input in the Approved DRNG (FIPS 186-2)

    Type: FIPS 186-2 DRNG

Generation: When used for MIC key generation, the xKey is created by padding the AES Content Decryption Keys.

Storage: RAM

Establishment: N/A

Entry: Seed Key is wrapped with Content Decryption Key (RSA 2048)

Output: N/A

Key-to-entity: via data structure and pointer in memory

Zeroization: Memory location in RAM zeroized via zeroize command and via tamper.

14. DRNG Internal State

Description: intermediate state of the DRNG (FIPS 186-2)

Type: FIPS 186-2 DRNG

Generation: inside crypto boundary via FIPS 186-2 DRNG

Storage: RAM

Establishment: N/A

Entry: N/A

Output: N/A

Key-to-entity: via data structure and pointer in memory

Zeroization: Memory location in RAM zeroized via zeroize command and via tamper.

15. Marriage Password

Description: User role authentication password.

Type: Authentication data; minimum 6 characters password, maximum 32 character password.

Generation: N/A

Storage: Stored in Flash, hashed with SHA-256; RAM

Establishment: N/A

Entry: Encrypted via TLS

Output: N/A

Key-to-entity: via memory location

Zeroization: RAM memory is zeroized via tamper. Also zeroized via Zeroization service.

21. 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 Update 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

4. Device Public Key (SM Key)

Description: RSA public key that device uses to prove its identity

Type: RSA 2048

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

Storage: Stored in Flash signed with Christie Certificate Chain; RAM

Establishment: N/A

Entry: N/A - Installed in the secure factory during manufacturing

Output: In X.509 certificate

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

5. Device Public Key (Log Key)

Description: RSA public key that device uses to prove its identity

Type: RSA 2048

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

Storage: Stored in Flash signed with Christie Certificate Chain; RAM

Establishment: N/A

Entry: N/A - Installed in the factory

Output: In X.509 certificate upon request

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

6. SMS Public Key

Description: RSA 2048 - TLS Client Public Key

Type: RSA 2048

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

Storage: Stored in RAM

Establishment: N/A

Entry: Entered into the module during TLS session establishment within a certificate signed by the Certificate Chain

Output: In X.509 certificate

Key-to-entity: via signature verification during projector handshake

7. Projector Public Key

Description: Identity of the projector

Type: RSA 2048

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

Storage: Stored in Flash; RAM

Establishment: N/A

Entry: Entered into the module in X.509 certificate during marriage handshake with projector

Output: In X.509 certificate

Key-to-entity: via signature verification during marriage handshake