Christie Digital Systems Canada Inc.

Christie IMB-S4 4K Integrated Media Block (IMB)

FIPS 140-3 Non-Proprietary Security Policy

Table of Contents

List of Tables

List of Figures

Author(s)	Title	Date	Version	Description
Ken Wong	Senior Product Developer, Software	2025-11-20	01	Initial Release

1 General

1.1 Overview

This document is the Cryptographic Module Security Policy for the Christie IMB-S4 4K Integrated Media Block (IMB) (also referred to herein as the Christie IMB-S4, the cryptographic module, or simply the module). This policy is a specification of the security rules under which the Christie IMB-S4 operates and meets the requirements of FIPS 140-3 Level 2.

1.2 Security Levels

Section	Title	Security Level
1	General	2
2	Cryptographic module specification	2
3	Cryptographic module interfaces	3
4	Roles, services, and authentication	3
5	Software/Firmware security	3
6	Operational environment	N/A
7	Physical security	2
8	Non-invasive security	N/A
9	Sensitive security parameter management	3
10	Self-tests	2
11	Life-cycle assurance	3
12	Mitigation of other attacks	N/A
	Overall Level	2

Table 1: Security Levels

2 Cryptographic Module Specification

2.1 Description

Purpose and Use:

The Christie IMB-S4 is a multi-chip embedded cryptographic module.

The IMB-S4 enables playback of encrypted cinema content packaged as an industry standard Digital Cinema Package (DCP). The IMB-S4 supports playback of digital cinema content from on-board storage (SSDs) as well as a network attached storage (NAS) device.

Module Type: Hardware

Module Embodiment: MultiChipEmbed

Module Characteristics:

Cryptographic Boundary:

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

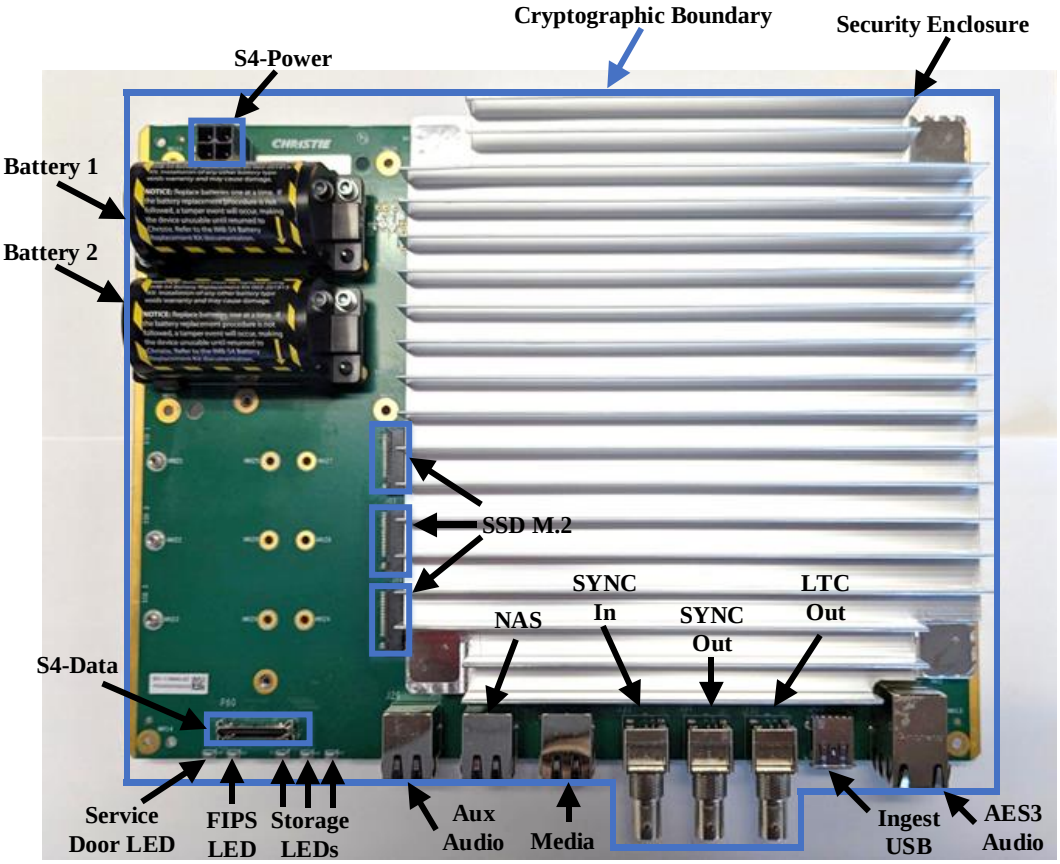

Figure 1 Top View of Christie IMB-S4

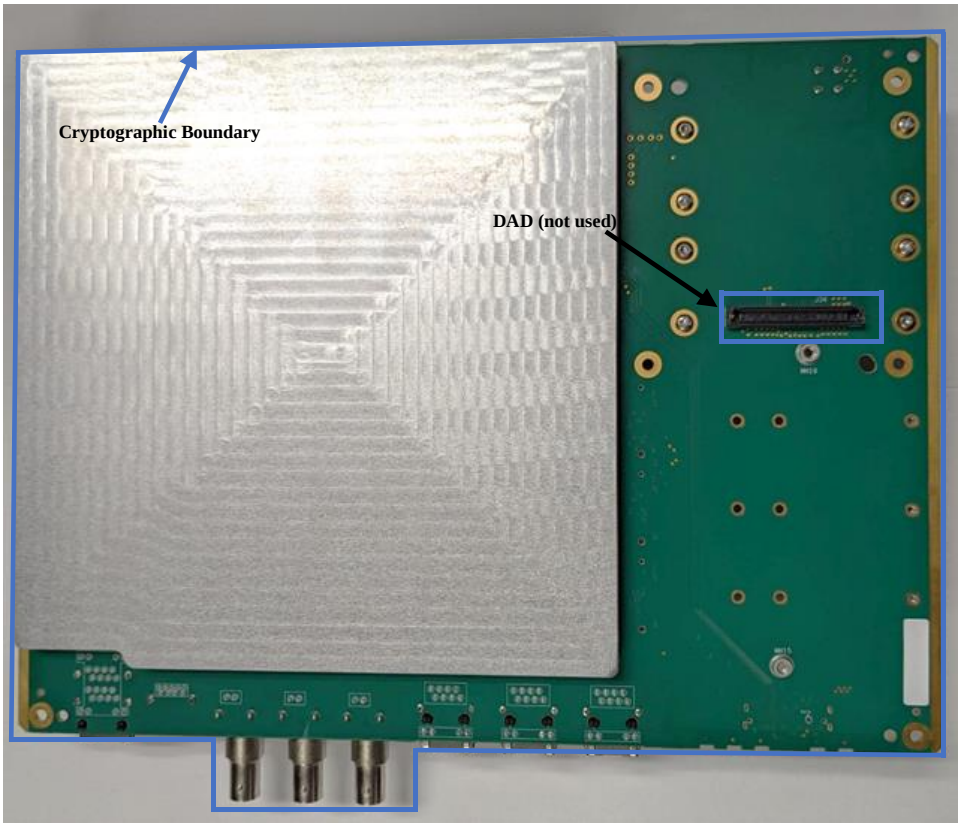

Figure 2 Bottom View of Christie IMB-S4

The cryptographic boundary is the outer physical perimeter of the module's PCB board as represented by the blue boundary in the above photos.

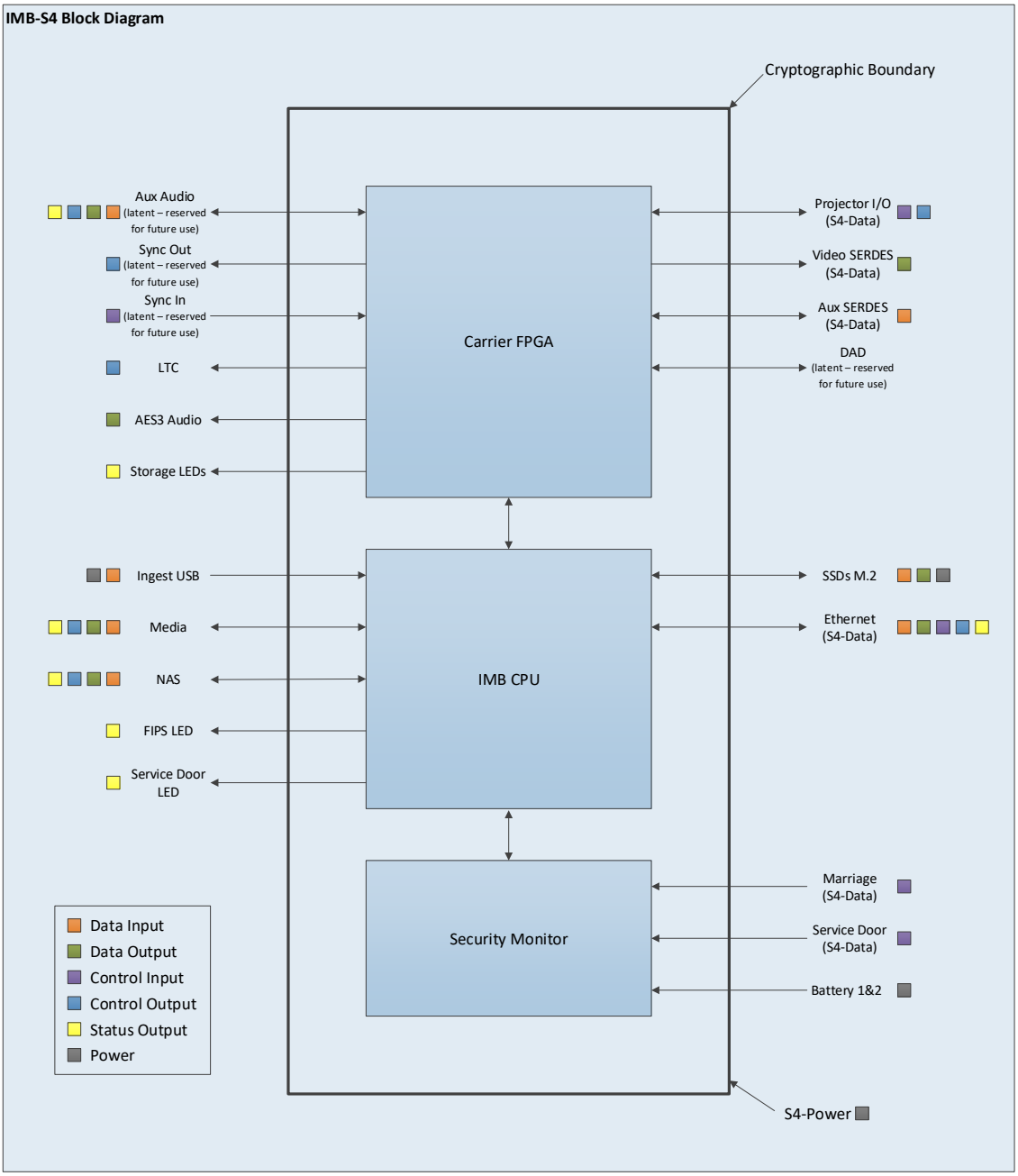

Figure 3 Block Diagram

2.2 Tested and Vendor Affirmed Module Version and Identification

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Christie IMB-S4 4K Integrated Media Block (IMB)	000-201699-01	1.0.0-5494@a	Intel Atom x7-E3950 and SE050 (HW P/N: N7121 B1)	N/A

Table 2: Tested Module Identification – Hardware

The **Get Module Information** approved service listed in section 4.3 Approved Services can be used to retrieve the module name, hardware part number / version, and firmware version. Specifically, each item is mapped to:

Table 3 Get Module Information Service Response Fields

Data	Status Item	Value
Module name	FIPS Model Name	IMB-S4
Hardware part number / version	FIPS Hardware Version	000-201699-01
Firmware Version	IMB Software Version	1.0.0-5494@a

2.3 Excluded Components

The following components are outside the security enclosure and are non-security relevant.

Table 4 Excluded Components

Excluded Component #	Description	Reference Designator
1	Resistor 0Ω	R678
2	Capacitor 47µF	C711
3	Capacitor 47µF	C712

2.4 Modes of Operation

Modes List and Description:

Mode Name	Description	Type	Status Indicator
Non-Approved	Running in non-approved mode of operation	Non-Approved	The module supports a separate indicator for non-approved security services. Module will display Ethernet (S4-Data) Status (FIPS_STATE) == non-approved
Approved	Running in approved mode of operation	Approved	The module supports a separate indicator for approved security services. Module will display Ethernet (S4-Data) Status (FIPS_STATE) == approved

Table 5: Modes List and Description

The module provides both an approved and non-approved mode of operation.

In the approved mode of operation, the module supports a single service (“Upgrade”). Invoking any of the non-approved services of the module directly places the module in a non-approved mode of operation.

As per FIPS 140-3 IG 2.4.A, the non-approved mode services of the module do not share, access, nor use any SSP used by the module in approved mode of operation. The SSPs used by the “Upgrade” service are not used in non-approved mode.

Mode Change Instructions and Status:

The module enters the approved mode of operation immediately after the self-test is completed. The module enters the non-approved mode of operation as soon as the first non-approved service is called.

The module can transition from non-approved to approved mode by rebooting the module and letting the self-test complete.

2.5 Algorithms

Approved Algorithms:

Algorithm	CAVP Cert	Properties	Reference
RSA SigVer (FIPS186-4)	C838	Signature Type - PKCS 1.5, PKCSPSS Modulo - 2048, 3072	FIPS 186-4
SHA-1	A4665	Message Length - Message Length: 8-1024 Increment 8	FIPS 180-4
SHA2-256	A4665	Message Length - Message Length: 8-1024 Increment 8	FIPS 180-4
SHA2-256	C837	Message Length - Message Length: 0-51200 Increment 8	FIPS 180-4

Table 6: Approved Algorithms

Vendor-Affirmed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

Name	Use and Function
MD5	Used as part of the TLS 1.0 implementation.
RSA (non-compliant)	Used as part of the TLS 1.0 implementation and the Ingest, Generate SM Report, Perform Marriage services.
TLS 1.0 KDF (non-compliant)	Used as part of the TLS 1.0 implementation.
AES (non-compliant)	Used as part of the TLS 1.0 implementation and the Ingest, Load Content, Playback services.
HMAC (non-compliant)	Used as part of the TLS 1.0 implementation and the Load Content, Playback services.
SHS (non-compliant)	Used as part of the TLS 1.0 implementation and Generate SM Report, Perform Marriage services.
DRBG (non-compliant)	Used as part of the TLS 1.0 implementation.

Table 7: Non-Approved, Not Allowed Algorithms

2.6 Security Function Implementations

Name	Type	Description	Properties	Algorithms
Digital Signature	DigSig-SigVer	Verification is used during the authentication of the firmware package during upgrade.		RSA SigVer (FIPS186-4): (C838) SHA2-256: (C837)
Secure Hash	SHA	SHA2-256 is used for Firmware Integrity during Upgrade and Self-Test. SHA-1 is only used as a standalone message digest.		SHA-1: (A4665) SHA2-256: (A4665)

Table 8: Security Function Implementations

2.7 Algorithm Specific Information

As per FIPS 140-3 IG C.K, the module supports a FIPS 186-4 algorithm (RSA 2048 SigVer) that was tested in 2019 prior to the Feb 5, 2024, transition. The FIPS 186-4 CAVP test (RSA 2048 SigVer) is mathematically identical to FIPS 186-5 CAVP tests (RSA 2048 SigVer), therefore this module will claim FIPS 186-5 compliance for this test (RSA 2048 SigVer).

Please also note that the SHA-1 algorithm has a transition date of December 31st, 2030. SHA-1 will be disallowed for applying cryptographic protection effective January 1st, 2031.

2.8 RBG and Entropy

N/A for this module.

N/A for this module.

2.9 Key Generation

N/A

2.10 Key Establishment

N/A

2.11 Industry Protocols

N/A

3 Cryptographic Module Interfaces

3.1 Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
Aux Audio	Data Input Data Output Control Output Status Output	Latent - Reserved for future use
Sync Out	Control Output	Latent - Reserved for future use
Sync In	Control Input	Latent - Reserved for future use
LTC	Control Output	Time code information
AES3 Audio	Data Output	Unencrypted Audio
Storage LEDs	Status Output	SSD 1 / 2 / 3 status information
Ingest USB	Data Input	DCP / KDM
Media	Data Input Data Output	DCP / KDM
Media	Status Output	Network Link status, Network Activity Status (via LEDs) Unauthenticated Status Information (TCP port 2000)
FIPS LED	Status Output	FIPS Status
Service Door LED	Status Output	Service Door open / closed
Video SERDES (S4-Data)	Data Output	Unencrypted Video
SSDs M.2	Data Input Data Output	DCP / KDM / Show Playlist
Marriage (S4-Data)	Control Input	Electrical signal indicating open or closed Marriage Ring
Service Door (S4-Data)	Control Input	Electrical signal indicating open or closed Service Door
NAS	Data Input Data Output	DCP / KDM
NAS	Status Output	Network Link status, Network Activity Status (via LEDs) Unauthenticated Status Information (TCP port 2000)
Projector I/O (S4-Data)	Control Input	FPGA handshake signals
Projector I/O (S4-Data)	Control Output	IMB Ready Electrical Signal
Aux SERDES (S4-Data)	Data Input	Audio
Aux SERDES (S4-Data)	Status Output	Latent - Reserved for future use
Ethernet (S4-Data)	Data Input	DCP / KDM
Ethernet (S4-Data)	Data Output	DCP / KDM / Rendered Subtitles
Ethernet (S4-Data)	Control Input	CEP API
Ethernet (S4-Data)	Control Output	FTP control as a client to a server
Ethernet (S4-Data)	Status Output	Unauthenticated Status Information (TCP port 2000)
Ingest USB	Power	N/A
SSDs M.2	Power	N/A
Battery 1 & 2	Power	N/A
S4-Power	Power	N/A
DAD	Status Output	Latent - Reserved for future use

Table 9: Ports and Interfaces

4 Roles, Services, and Authentication

4.1 Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
RSA Digital Signature Verification	Identity-based operator authentication	RSA Digital Signature Verification	The authentication is based on RSA 2048 which provides an equivalent encryption strength of 112 bits. The	There is a 1 second retry delay after each attempt which limits the number of attempts that can be launched per

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
			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.	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 10: Authentication Methods

Authentication for the Ethernet Control Input Interface is accomplished via identity-based operator identification using RSA Digital Signature Verification (using the CAVE SMS Certificate).

4.2 Roles

Name	Type	Operator Type	Authentication Methods
Crypto Officer	Identity	Crypto Officer	RSA Digital Signature Verification

Table 11: Roles

The module supports a single login of the one operator role: Crypto Officer.

4.3 Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Upgrade	Verify authenticity and integrity of firmware package.	Ethernet (S4-Data) Status (FIPS_STATE) == approved	Firmware Package, CAVE SMS Certificate	Ethernet (S4-Data) Upgrade Status == Success	Digital Signature Secure Hash	Crypto Officer - Christie Firmware Update Certificate: E - Christie Firmware Update Public Key: E - Cave SMS Certificate: W - Cave SMS Public Key: W - Christie Root CA Self Signed Certificate: E - Christie Root CA Public Key: E - Christie CA Certificate Chain: E
Get Module Information	Retrieve hardware version and firmware version (Show Version)	Ethernet (S4-Data) Status (FIPS_STATE) == approved	None	Hardware Version, Firmware Version	None	Unauthenticated
Get Status	Retrieve Status (Show Status)	Ethernet (S4-Data) Status (FIPS_STATE) == approved	None	Status of module	None	Unauthenticated

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Perform Self-test (power cycle)	Run pre-operational self-tests	N/A - self-tests are performed at boot-up irrespective of the mode of operation.	None	Ethernet (S4-Data) FIPS_STATE == approved	None	Unauthenticated
Zeroization	Zeroize all SSPs	FIPS Error State	None	FIPS Error State	None	Crypto Officer - Christie Firmware Update Certificate: Z - Christie Firmware Update Public Key: Z - Cave SMS Certificate: Z - Christie Root CA Self Signed Certificate: Z - Christie Root CA Public Key: Z - Christie CA Certificate Chain: Z
Get Upgrade Status	Retrieve status of upgrade	Ethernet (S4-Data) Status (FIPS_STATE) == approved	None	Status Information of upgrade	None	Unauthenticated

Table 12: Approved Services

All approved services are performed via the Crypto Officer role.

As per FIPS 140-3 IG 2.4.C, module supports a separate indicator per approved security service.

4.4 Non-Approved Services

Name	Description	Algorithms	Role
Ingest	Retrieve and store DCP / KDM	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Load Content	Unwrap Content Decryption Keys and perform CPL verification	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant)	Crypto Officer

Name	Description	Algorithms	Role
		DRBG (non-compliant)	
Playback	Decrypt Content, verify frame integrity, and perform playback	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Generate SM Report	Build and sign the SM Report	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Perform Marriage	Perform Electronic Marriage	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
List Remote Device Configurations	List all remote device configurations	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Add Remote Device Configuration	Specify a remote device to ingest content from	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Delete Remote Device Configuration	Delete a remote device configuration	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant)	Crypto Officer

Name	Description	Algorithms	Role
		DRBG (non-compliant)	
Test FTP Server	Confirm connectivity to FTP Server	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
List Ingest Sources	List sources to ingest content from	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Scan for Ingestible Content	Find all ingestible content on local drives	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Cancel Scan for Ingestible Content	Cancel a scan in progress	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
List Ingestible Content	List all ingestible content found from scan	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Cancel Ingest	Cancel an ingest in progress	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant)	Crypto Officer

Name	Description	Algorithms	Role
		DRBG (non-compliant)	
Get Ingest Status	Get Status information about current ingest	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get List of Shared Directories	Retrieve list of shared directories on NAS drive	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
List Content	Retrieve list of content	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Refresh Content	Refresh cached list of content	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get CPL	Retrieve a CPL	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get CPL Details	Retrieve details of a CPL	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant)	Crypto Officer

Name	Description	Algorithms	Role
		DRBG (non-compliant)	
Is CPL Complete	Confirm all assets are available for CPL	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get KDM	Retrieve a KDM	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Delete Content	Remove content from Onboard Storage	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Type of UUID	Retrieve type of content for UUID	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Load Status	Retrieve status of load operation	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get ID of Loaded Content	Retrieve ID of loaded content	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant)	Crypto Officer

Name	Description	Algorithms	Role
		DRBG (non-compliant)	
Enable Looping	Enable content looping	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Unload Content	Unload content from memory	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Module Details / History	Start information collection of Module	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Status of Information Collection	Retrieve status of information collection	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Show Playlists	Retrieve list of show playlists	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Is Show Playlist Complete	Determine if all components of show playlist are present	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant)	Crypto Officer

Name	Description	Algorithms	Role
		DRBG (non-compliant)	
Does Content Exist in Show Playlist	Check if content exists in a playlist	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Confirm KDM Validity for Show Playlist	Confirm that all KDMs for playlist are valid at specified time	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Validate Show Playlist	Validate a specified playlist	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Show Playlist Validation Results	Get the results of the playlist validation	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Enable Scheduler Support	Enable flag indicating that scheduler is active	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Status Item	Retrieve individual status item	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant)	Crypto Officer

Name	Description	Algorithms	Role
		DRBG (non-compliant)	
Get SM Certificate	Retrieve SM Leaf Certificate	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get LS Certificate	Retrieve LS Leaf Certificate	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Stop SM Report Generation	Stop SM Report generation	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Audio Configuration	Retrieve Audio Configuration	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Save Audio Configuration	Save Audio Configuration	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Test NAS Connectivity	Verify connectivity to NAS	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant)	Crypto Officer

Name	Description	Algorithms	Role
		DRBG (non-compliant)	
Get Storage Status	Retrieve status of each storage device	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Save Storage Configuration	Save Storage Configuration	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Storage Configuration	Get Storage Configuration	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Does Show Playlist Exist	Check for an individual show playlist	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Save Show Playlist	Save a show playlist	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Get Show Playlist	Retrieve a saved show playlist	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant)	Crypto Officer

Name	Description	Algorithms	Role
		DRBG (non-compliant)	
Adjust Time	Adjust the Real Time Clock	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer
Is SM Busy	Return True if SM is Busy	MD5 RSA (non-compliant) TLS 1.0 KDF (non-compliant) AES (non-compliant) HMAC (non-compliant) SHS (non-compliant) DRBG (non-compliant)	Crypto Officer

Table 13: Non-Approved Services

4.5 External Software/Firmware Loaded

Any firmware loaded into this module that is not shown on the module certificate, is out of scope of this validation and requires a separate FIPS 140-3 validation.

Loading of External Firmware is performed through the Upgrade Service via the Crypto Officer role. Unauthorized firmware loading is not possible. Additionally, all firmware is digitally signed and checked as per section 5.

Data Output and Control Output is inhibited during firmware load testing. The module also prevents firmware loading during any Data Output and/or Control Output operations. During firmware loading, requests for other services involving Data Output and/or Control Output are prohibited until firmware load is complete and the module is restarted.

The module implements partial image replacement since there is a BIOS firmware component that is not upgradeable in the field and can only be modified by Christie at Christie's secure facility.

5 Software/Firmware Security

5.1 Integrity Techniques

The integrity of the module is verified by comparing the SHA2-256 (SHS Cert. # A4665) value of the firmware calculated at the time of construction of the firmware, with the SHA2-256 value of the currently running firmware. This is performed as part of the Pre-Operational Self-Tests. Please note the SHA2-256 implementation will perform a Cryptographic Algorithm Self-Test using a Known Answer Test, prior to performing the firmware integrity test.

5.2 Initiate on Demand

The operator can initiate firmware integrity test by power-cycling the module.

6 Operational Environment

6.1 Operational Environment Type and Requirements

The module operates in a limited operational environment that only allows the loading of a trusted and validated firmware binary image through an authenticated service. Firmware binary images are signed by an RSA key which is part of the Christie certificate chain.

Type of Operational Environment: Limited

7 Physical Security

7.1 Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Metal Security 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 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: Mechanisms and Actions Required

The Christie IMB-S4 is a multi-chip embedded cryptographic module which is composed of production-grade components. The module satisfies Security Level 2 only for physical security.

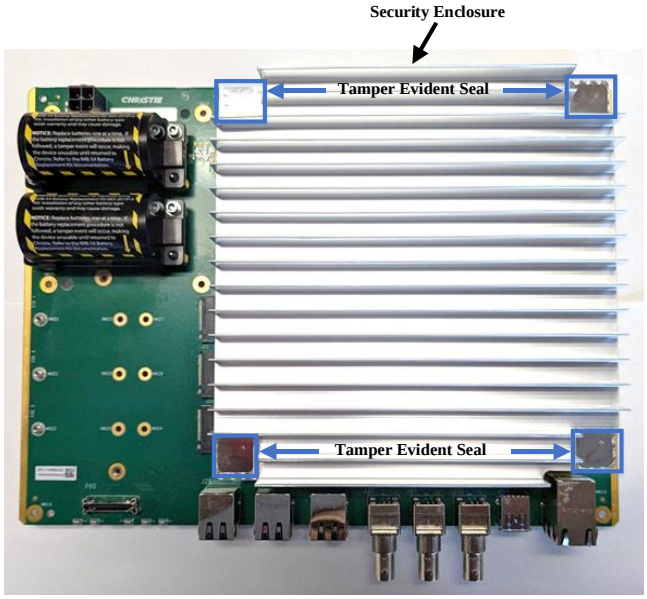

Figure 4 Physical Security Mechanisms

The physical security mechanisms of the module include a hard, opaque and tamper-evident metal security enclosure.

The module includes four tamper evident seals (Figure 4 Physical Security Mechanisms) covering the screws that secure the metal enclosure to the module; said tamper evident seals 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 security enclosure and the tamper-evident seals 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 listed under section 2.3 Excluded Components.

NOTE: Although strictly outside the scope of physical security level 2, the metal security enclosure 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 both batteries become discharged.

8 Non-Invasive Security

N/A

9 Sensitive Security Parameters Management

9.1 Storage Areas

Storage Area Name	Description	Persistence Type
IMB CPU RAM	System Memory	Dynamic
IMB CPU Flash	System Non-Volatile Memory	Static

Table 15: Storage Areas

9.2 SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Factory Installed	Manufacturer	N/A	Plaintext	Automated	Electronic	
Upgrade Service	Ethernet (S4-Data)	IMB CPU RAM	Plaintext	Automated	Electronic	

Table 16: SSP Input-Output Methods

9.3 SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Zeroization Service	Start the zeroization service.		Zeroization Service
Tamper	Security Enclosure Removal or full loss of power		Remove Security Enclosure Remove Both Batteries and main power
Loss of Main Power	Loss of Main Power but battery power is still present		Disconnect power from S4-Power Physical Port
Completion of Service	SSP temporary values are zeroised at the completion of a service		Automatically performed by the module

Table 17: SSP Zeroization Methods

The module explicitly zeroizes SSPs as per the methods above. Please see Section 9.4 for more details.

9.4 SSPs

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Christie Firmware Update Certificate	X.509 Firmware Update Certificate for update package verification	2048 - 112	X.509 - PSP			Digital Signature
Christie Firmware Update Public Key	RSA Public Key for verifying update package signature	2048 - 112	Public - PSP			Digital Signature
Cave SMS Certificate	X.509 Certificate containing the Cave SMS Public Key	2048 - 112	X.509 - PSP			Digital Signature
Cave SMS Public Key	Crypto Officer RSA Public Key	2048 - 112	Public - PSP			Digital Signature
Christie Root CA Self Signed Certificate	X.509 CA Certificate for leaf certificate verification	2048 - 112	X.509 - PSP			Digital Signature
Christie Root CA Public Key	RSA Public Key for leaf certificate verification	2048 - 112	Public - PSP			Digital Signature
Christie CA Certificate Chain	X.509 CA Certificate	2048 - 112	X.509 - PSP			Secure Hash Digital Signature

Table 18: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Christie Firmware Update Certificate	Factory Installed	IMB CPU Flash:Plaintext IMB CPU RAM:Plaintext	N/A	Tamper Zeroization Service	Christie Firmware Update Public Key:Paired With
Christie Firmware Update Public Key	Factory Installed	IMB CPU Flash:Plaintext IMB CPU RAM:Plaintext	N/A	Tamper Zeroization Service	Christie Firmware Update Certificate:Paired With
Cave SMS Certificate	Upgrade Service	IMB CPU RAM:Plaintext	During authentication of Upgrade Service	Loss of Main Power Completion of Service	Cave SMS Public Key:Paired With

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Cave SMS Public Key	Upgrade Service	IMB CPU RAM:Plaintext	During authentication of Upgrade Service	Loss of Main Power Completion of Service	Cave SMS Certificate:Paired With
Christie Root CA Self Signed Certificate	Upgrade Service	IMB CPU Flash:Plaintext IMB CPU RAM:Plaintext	During authentication of Upgrade Service	Loss of Main Power Completion of Service	Christie Root CA Public Key:Paired With
Christie Root CA Public Key	Upgrade Service	IMB CPU RAM:Plaintext IMB CPU Flash:Plaintext	During authentication of Upgrade Service	Loss of Main Power Completion of Service	Christie Root CA Self Signed Certificate:Paired With
Christie CA Certificate Chain	Upgrade Service	IMB CPU RAM:Plaintext IMB CPU Flash:Plaintext	During authentication of Upgrade Service	Loss of Main Power Completion of Service	Christie Root CA Self Signed Certificate:Used With

Table 19: SSP Table 2

10 Self-Tests

10.1 Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Check Security MCU	N/A	N/A	Critical Function	If success, "FIPS_ERROR=None" and FIPS LED will be solid green. If failed, "FIPS_ERROR=SECURITY_MCU_OFFLINE" and FIPS LED will be solid red. If success	Check Security MCU
Check Enclosure Status	N/A	N/A	Critical Function	If success, "FIPS_ERROR=None" and FIPS LED will be solid green. If failed, "FIPS_ERROR=TAMPERED: 1 EN_OPEN: 1" and FIPS LED will be solid red.	Check Enclosure Status
Check NXP SE050	N/A	N/A	Critical Function	If success, "FIPS_ERROR=None" and FIPS LED will be solid green. If failed, "FIPS_ERROR=TPM_FAILURE" and FIPS LED will be solid red.	Check NXP SE050
SHS	SHA2-256	FW Integrity	SW/FW Integrity	If success, "FIPS_ERROR=None" and FIPS LED will be solid green. If failed, "FIPS_ERROR=IMAGE_INTEGRITY" and FIPS LED will be solid red.	Secure Hash

Table 20: Pre-Operational Self-Tests

The NXP SE050 referenced above is synonymous with TPM.

10.2 Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigVer (FIPS186-4) (C838)	2048-bit data, 160-bit digest	KAT	CAST	If success, "FIPS_ERROR=None" and FIPS LED will be solid green. If failed, "FIPS_ERROR=KAT_CHECK" and FIPS LED will be solid red.	Sign, Verify	Power-Up

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
SHA2-256 (A4665)	SHA-256, 256-bit data	KAT	CAST	If success, "FIPS_ERROR=None" and FIPS LED will be solid green. If failed, "FIPS_ERROR=KAT_CHECK" and FIPS LED will be solid red.	Secure Hash	Power-Up
SHA-1 (A4665)	SHA-1	KAT	CAST	If success, "FIPS_ERROR=None" and FIPS LED will be solid green. If failed, "FIPS_ERROR=KAT_CHECK" and FIPS LED will be solid red.	Secure Hash	Power-Up
RSA SigVer (FIPS186-4) (C838)	2048-bit key with SHA2-256 Signature Verification	SW/FW Load	SW/FW Load	If success, "FIPS_ERROR=None" and FIPS LED will be solid green. If failed, "FIPS_ERROR=UPGRADE_FAILURE" and FIPS LED will be solid red.	Verify	Conditional

Table 21: Conditional Self-Tests

The IMB-S4 has one conditional self-test related to firmware loading. Firmware loading requires RSA 2048 for signature verification and SHA-256 for filesystem integrity check. Both algorithms are tested as part of the self-test on boot up and during the periodic self-tests.

10.3 Periodic Self-Test Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Check Security MCU	N/A	Critical Function	7 days	The periodic self-test is performed programmatically at 7 days from when the module is powered on (main power via S4-POWER). Once each periodic self-test is completed, the next self-test will be scheduled at 7 days from that point in time (and so on). If the self-test is to be performed while content is loaded, the self-test will be deferred until content is unloaded. If the maximum 7-day deferment period is hit, the module will force the self-test.
Check Enclosure Status	N/A	Critical Function	7 days	The periodic self-test is performed programmatically at 7 days from when the module is powered on (main power via S4-POWER). Once each periodic self-test is completed,

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				the next self-test will be scheduled at 7 days from that point in time (and so on). If the self-test is to be performed while content is loaded, the self-test will be deferred until content is unloaded. If the maximum 7-day deferment period is hit, the module will force the self-test.
Check NXP SE050	N/A	Critical Function	7 days	The periodic self-test is performed programmatically at 7 days from when the module is powered on (main power via S4-POWER). Once each periodic self-test is completed, the next self-test will be scheduled at 7 days from that point in time (and so on). If the self-test is to be performed while content is loaded, the self-test will be deferred until content is unloaded. If the maximum 7-day deferment period is hit, the module will force the self-test.
SHS	FW Integrity	SW/FW Integrity	7 days	The periodic self-test is performed programmatically at 7 days from when the module is powered on (main power via S4-POWER). Once each periodic self-test is completed, the next self-test will be scheduled at 7 days from that point in time (and so on). If the self-test is to be performed while content is loaded, the self-test will be deferred until content is unloaded. If the maximum 7-

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				day deferment period is hit, the module will force the self-test.

Table 22: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
RSA SigVer (FIPS186-4) (C838)	KAT	CAST	7 days	The periodic self-test is performed programmatically at 7 days from when the module is powered on (main power via S4-POWER). Once each periodic self-test is completed, the next self-test will be scheduled at 7 days from that point in time (and so on). If the self-test is to be performed while content is loaded, the self-test will be deferred until content is unloaded. If the maximum 7-day deferment period is hit, the module will force the self-test.
SHA2-256 (A4665)	KAT	CAST	7 days	The periodic self-test is performed programmatically at 7 days from when the module is powered on (main power via S4-POWER). Once each periodic self-test is completed, the next self-test will be scheduled at 7 days from that point in time (and so on). If the self-test is to be performed while content is loaded, the self-test will be deferred until content is unloaded. If the maximum 7-day deferment period is hit, the module will force the self-test.
SHA-1 (A4665)	KAT	CAST	7 days	The periodic self-test is performed

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
				programmatically at 7 days from when the module is powered on (main power via S4-POWER). Once each periodic self-test is completed, the next self-test will be scheduled at 7 days from that point in time (and so on). If the self-test is to be performed while content is loaded, the self-test will be deferred until content is unloaded. If the maximum 7-day deferment period is hit, the module will force the self-test
RSA SigVer (FIPS186-4) (C838)	SW/FW Load	SW/FW Load	None	Automatically performed by the module during the Upgrade service

Table 23: Conditional Periodic Information

10.4 Error States

Name	Description	Conditions	Recovery Method	Indicator
Tampered	Tampering, Zeroization Service	Full loss of power Security Enclosure Removal Started by Crypto Officer	Return to Factory	FIPS LED will be solid red.
Self-Test Failure	Critical Function Failure	Pre-operational self-test failure	Return to Factory	FIPS LED will be solid red.
Firmware Integrity Failure	Verify Firmware Integrity SHA2-256 checksum	Incorrect checksum	Return to Factory	FIPS LED will be solid red.
Firmware Load Test Failure	Failure during firmware load	Signature Verification or SHA Checksum failure.	Power Cycle	FIPS LED will be solid red.

Table 24: Error States

For more information about each error state, please see the relevant Self-Test section above.

11 Life-Cycle Assurance

11.1 Installation, Initialization, and Startup Procedures

The module is manufactured in a secure facility and placed into the approved mode of operation prior to shipping to the customer. On powering up the module (from battery to main power), the module goes through self-tests and an image integrity check to confirm that the non-modifiable operating environment has not been tampered with.

Any other failure will result in a hard FIPS error state to prevent use of the product in a non-approved mode.

11.2 Administrator Guidance

The module consists of a single Crypto Officer role (see 4.2 Roles) and there are no administrative specific procedures functions required to administer the module while it's in its approved mode of operation.

The module is fully secured and in the approved mode of operation once it is shipped from the factory. There is no additional user behavior expected for secure operation of the module.

Physical Ports and logical Interfaces

Please refer to section 3 Cryptographic Module Interfaces.

Security Events

Please refer to section 2.4 Modes of Operation.

Approved & Non-approved Security Functions

Please refer to section 4.3 Approved Services and section 4.4 Non-Approved Services.

Security Parameters

Please refer to section 9.4 SSPs.

11.3 Non-Administrator Guidance

As defined in section 4.1 Authentication Methods, the module supports identity-based operator authentication and there are no specific procedures required to maintain the operator authentication data and mechanisms functionally independent.

The module enters the approved mode of operation immediately after self-test is completed. The module enters the non-approved mode of operation as soon as the first non-approved service is called.

The module can transition from non-approved to approved mode by rebooting the module and letting the self-test complete.

Please see section 2.4 Modes of Operation for more details.

11.4 Design and Rules

The module supports both battery power and main power by design. Powering up is defined as the process of switching from battery power to main power. All pre-operational self-tests are performed during the powering up sequence and the model automatically transitions to the operational state when the self-tests have passed. Once in this state, the module awaits service requests from the operator.

11.5 Maintenance Requirements

N/A

11.6 End of Life

Procedure for secure sanitization of the IMB-S4 at end-of-life:

1. Remove both battery boards from the IMB-S4.
   This causes tampering and zeroization of the IMB-S4 module.
2. Dispose of the board properly according to local e-waste regulations and laws.
3. Dispose of the batteries, which contain lithium, properly according to local regulations and laws.

Please ensure all components of the IMB-S4 are disposed of properly according to local regulations and laws.

12 Mitigation of Other Attacks

The IMB-S4 module does not mitigate any specific attacks beyond the scope of FIPS140-3.