IMB-1000 HFR and IMB-1200 HFR Secure Media Blocks Security Policy

USL, Inc.

Version 1.4

March 20, 2013

TABLE OF CONTENTS

1. Module Overview

The IMB-1000 HFR and IMB-1200 HFR Secure Media Blocks (Firmware Version: 02272013; Hardware Version: Rev. 14), hereafter referred to as the cryptographic modules or modules, are Security Processor Blocks designed in accordance with FIPS 140-2 and the Digital Cinema Initiatives (DCI) Digital Cinema System Specification. For FIPS 140-2 purposes, the Secure Media Blocks are defined as multi-chip embedded cryptographic modules encased in metallic enclosures.

The IMB-1200 HFR cryptographic module provides the same ports as the IMB-1000 HFR, but with the addition of two fiber optic ports. The images below depict the IMB-1200 HFR Secure Media Block cryptographic module (see Figures 1 and 2). The boundary is defined as the perimeter of the module's PCB with all components not contained within the metallic enclosure explicitly excluded from the requirements of FIPS 140-2 as they are non-security relevant and have no impact on the overall security of the modules.

Figure 1: IMB-1200 HFR Secure Media Block (Top, Right, Front)

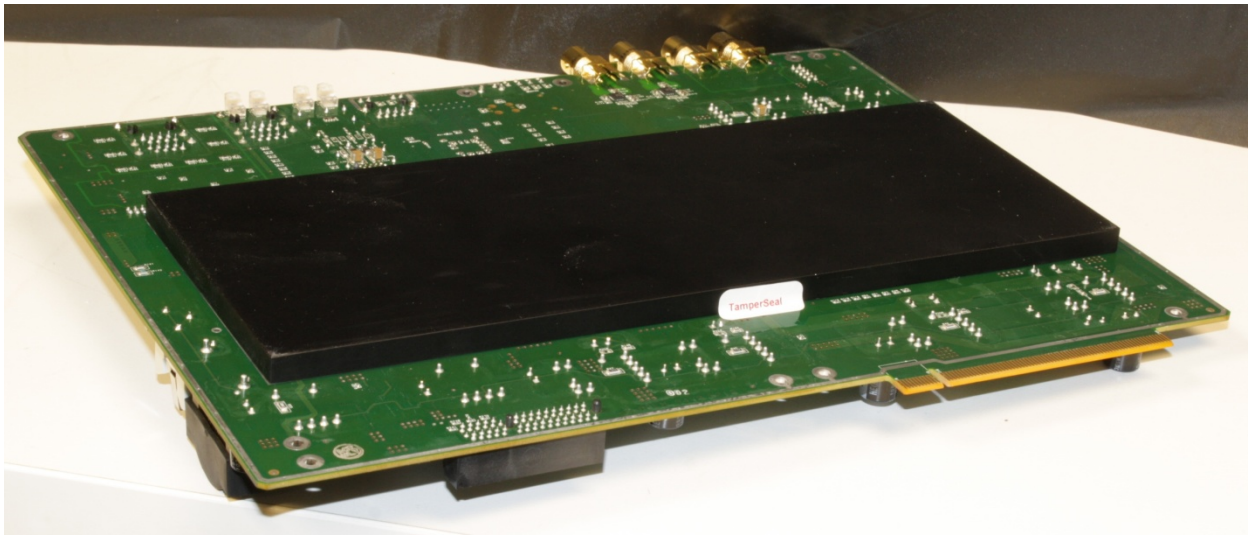

Figure 2: IMB-1200 HFR Secure Media Block (Bottom, Left, Back)

2. Security Level

The cryptographic modules meet the overall requirements applicable to FIPS 140-2 Level 2.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The modules only support an Approved mode of operation, which is specified during power-on with a message to the log, “Operating in FIPS compliant mode”. The modules support the following Approved algorithms:

- HW AES 128CBC (Cert. #1460)
- FPGA AES 128CBC: Video Decryption (Cert. #1964)
- HW HMAC SHA-1 (Cert. #857)
- HW SHA-1 (Cert. #1321)
- AES-128 (Cert. #1459)
- HMAC-SHA-1, HMAC-SHA-256 (Cert. #856)
- SHA-1, SHA-256 (Cert. #1320)
- RNG ANSI X9.31 (Cert. #798)
- RNG FIPS 186-2 (Cert. #1165)
- FIPS 186-2 RSA Sign/Verify PKCS1v1.5, SHA256, 2048-bit keys (Cert. #712)
- SP800-135 KDF (Cert. #52)

The modules support the following non-Approved and allowed algorithms:

- RSA (key wrapping, key establishment methodology provides 112-bits of encryption strength)
- HW NDRNG for seeding the RNGs
- MD5 for use exclusively within TLS
- TI S-BOX (Proprietary algorithm used to facilitate the marriage between a Projector and the module – no security claimed)
- ECDH for facilitating the marriage between a Projector and the module; no-security claimed

4. Ports and Interfaces

The IMB-1000 HFR cryptographic module provides the following physical ports and logical interfaces:

- RJ-45 Ethernet Port (Qty. 2): Data Input, Data Output, Control Input, Status Output
- AES-Audio (Qty. 1): Data Output
- Status LEDs (Qty. 4): Status Output
- Power LEDs (Qty. 6): Status Output
- Boot Status LEDs (Qty. 8): Status Output
- HD-SDI Input (Qty. 2): Data Input
- External Synchronization Input: Data Input
- External Synchronization Output: Data Output
- High-Speed Accessory Port: Data Input
- Accessory Power Port: Power Output
- IRQ-12 Reset for PowerPC: Control Input (Reset)
- PCI-E Card Edge (Qty. 1): Data Input, Data Output, Control Input, Status Output, Power Input
- PCI-E Card Connector (Qty. 1): Data Input, Data Output, Control Input, Status Output
- Battery (Qty. 1): Power Input

The IMB-1200 HFR cryptographic module provides the same ports as the IMB-1000 HFR, but with the addition of two fiber optic ports as follows:

- Fiber Optic Ethernet (Qty. 2): Data Input, Data Output, Control Input, Status Output

5. Identification and Authentication Policy

Assumption of roles

The cryptographic modules support two distinct operator roles, which are the User and Cryptographic-Officer roles.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Method
Cryptographic-Officer	Identity-based operator authentication	2048-bit Digital Signature Verification
User	Identity-based operator authentication	2048-bit Digital Signature Verification

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Digital Signature	The strength of a 2048-bit RSA key (with SHA-256) is known to be 112-bits. Therefore, the strength of a 2048-bit digital signature is 1/2^112, which is less than 1/1,000,000. In a worst case scenario, the module can perform 451 signature verifications per second, which does not include network limitations or timing constraints. Therefore, the probability that multiple attacks within a given minute will be successful is 27,060/2^112, which is less than 1/100,000.

6. Access Control Policy

Roles and Services

The modules support two distinct roles, a User and Cryptographic Officer. The following table describes the services that are allocated to each role:

Table 4 – Services Authorized for Roles

Role	Authorized Services
Cryptographic-Officer	• Upgrade Firmware • Zeroize
User	• End of Transmission • Start Suite • Stop Suite • CPL Validate • KDM Validate • SPL Validate • Decrypt Captions • Validate Ready to Play • Purge CPL • Purge SPL • Purge Suite • Time Adjust • Start Playback • Stop Playback • Pause Playback • Resume Playback

	• Audio Delay • Get Position • Set Position • Get Certificate Request • Product Info • Status • Diagnostic Info • Reset Diagnostic • Security Log Request • Close Log Export • Set Time Zone

Unauthenticated Services:

The cryptographic modules support the following unauthenticated services:

- Show Status: Provides the current status of the module (e.g., temperature, tamper status, date, voltages, serial number, certificates).
- Self-tests: Invoke the power-on self-tests by power cycling the module.

Definition of Critical Security Parameters (CSPs)

The modules contain the following CSPs:

- Device Private Key
- Content Encryption Key
- Content Integrity Key
- TLS Encryption Keys
- TLS Integrity Keys
- RNG Seed Keys
- RNG Seed Values

Definition of Public Keys:

The following are the public keys contained in the modules:

- Device Public Key
- Trusted Root CA Certificates
- USL CA Certificate
- Products Certificate
- Digital Cinema Certificate
- SMS Public Key
- Projector Public Key
- Content Provider Public Keys
- USL Manufacturing Public Key

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different modules' services. The modes of access shown in the table are defined as follows:

- Read
- Write
- Zeroize

Please note that all services are sent through an encrypted TLS tunnel and as such, TLS related CSPs are utilized during each service.

Table 5 – CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
X		Upgrade Firmware	N/A
X		Zeroize	Zeroize All CSPs
	X	End of Transmission	N/A

	X	Start Suite	Read RNG Seed Key and Seed Values
	X	Stop Suite	N/A
	X	CPL Validate	N/A
	X	KDM Validate	Read Device Private Key Write Content Encryption Keys Write Content Integrity Keys
	X	SPL Validate	N/A
	X	Decrypt Captions	Read Content Encryption Keys
	X	Validate Ready to Play	N/A
	X	Purge CPL	N/A
	X	Purge SPL	N/A
	X	Purge Suite	Zeroize Content Encryption Keys and Content Integrity Keys
	X	Time Adjust	N/A
	X	Start Playback	Read Content Encryption Keys Read Content Integrity Keys
	X	Stop Playback	N/A
	X	Pause Playback	N/A
	X	Resume Playback	N/A
	X	Audio Delay	N/A
	X	Get Position	N/A
	X	Set Position	N/A
	X	Get Certificate Request	N/A
	X	Product Info	N/A

	X	Stats	N/A
	X	Diagnostic Info	N/A
	X	Reset Diagnostic	N/A
	X	Security Log Request	Read Device Private Key
	X	Close Log Export	N/A
	X	Set Time Zone	N/A
X	X	Show Status	N/A
X	X	Self-Tests	N/A

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable; the cryptographic modules support a limited operational environment that restricts the loading of firmware by ensuring all firmware being installed is appropriately signed.

8. Security Rules

The cryptographic modules' designs correspond to the cryptographic modules' security rules. This section documents the security rules enforced by the cryptographic modules to implement the security requirements of these FIPS 140-2 Level 2 modules.

1. The modules provide identity-based authentication.
2. The modules will only provide access to cryptographic services if a valid role has been assumed.
3. The cryptographic modules shall perform the following tests:

    A. <u>Power up Self-Tests:</u>

        1. Cryptographic algorithm tests:

            a. HW AES Decrypt KAT
            b. FPGA AES Decryption KAT
            c. HW SHA-1 KAT
            d. HW HMAC SHA-1 KAT
            e. RNG ANSI X9.31 KAT

f. RNG FIPS 186-2 KAT
g. SHA-1, SHA-256 KAT
h. HMAC-SHA-1, HMAC SHA-256 KAT
i. SP800-135 KDF KAT
j. AES Encrypt/Decrypt KAT
k. RSA Sign/Verify KAT
l. RSA Encrypt/Decrypt KAT

2. Firmware Integrity Tests (32-bit CRC, 16-bit CRC)
3. Critical Functions Tests: N/A.

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on the RNGs
2. Firmware Load Test (2048-bit RSA Signature Verification)

4. Data output shall be inhibited during self-tests and error states. In an error state, the modules will restart and re-attempt self-tests.
5. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the modules.
6. Data output shall be logically disconnected to the processes performing zeroization.

9. Physical Security Policy

Physical Security Mechanisms

The IMB-1000 HFR, IMB-1200 HFR Secure Media Blocks are multi-chip embedded cryptographic modules, which include the following physical security mechanisms:

- Production-grade components.
- Tamper-responsive hard, metallic enclosure.
- Two (2) tamper-evident labels (installed during manufacturing).

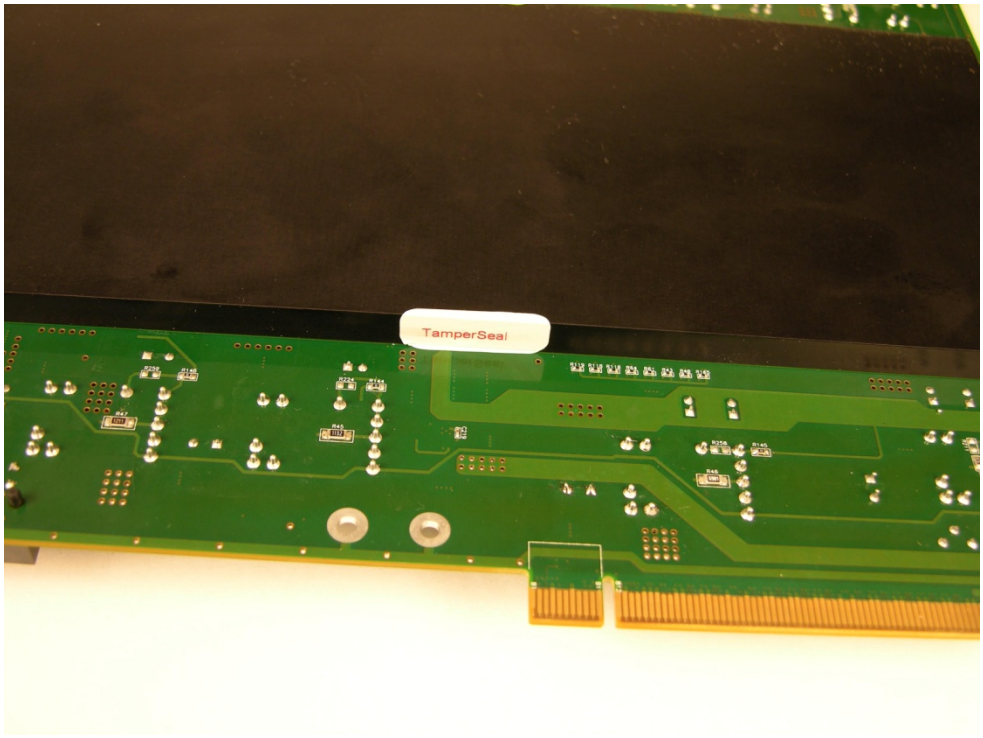

Figure 3 – Tamper Label Placement #1 (Bottom Side)

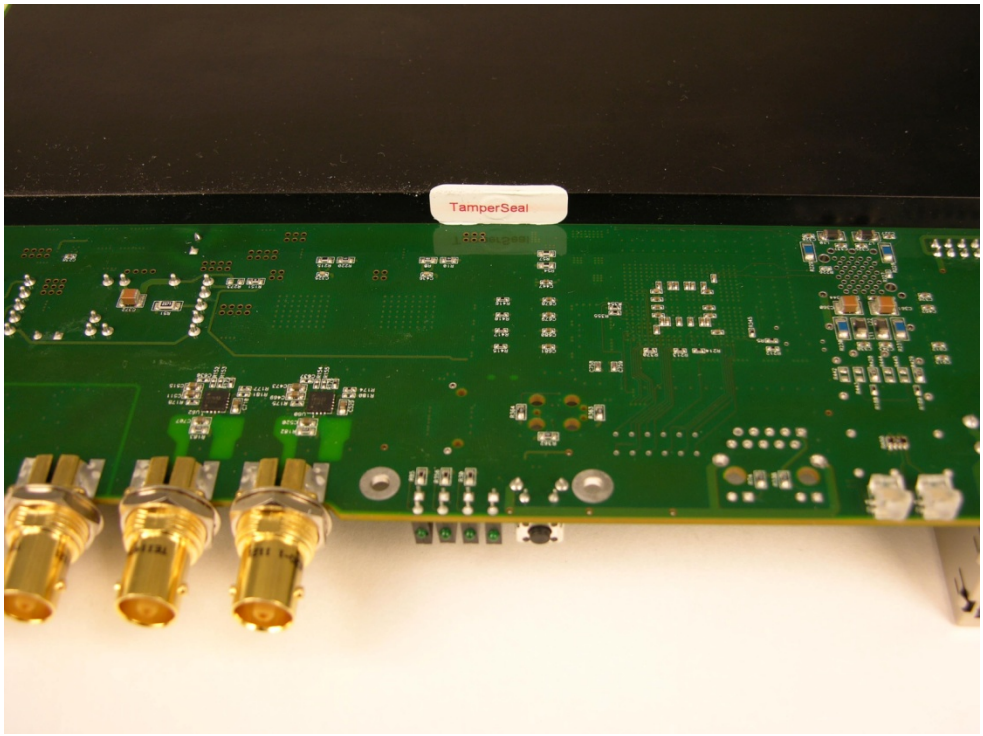

Figure 4 – Tamper Label Placement #2 (Bottom Side)

Operator Required Actions

The operator is required to periodically inspect the modules for evidence of tampering.

Table 7 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper evidence	Annually	Ensure the module does not display any characteristics of an attempted breach.

10. Mitigation of Other Attacks Policy

The modules have not been designed to mitigate attacks beyond the scope of FIPS 140-2 requirements.

11. Definitions and Acronyms

AES	Advanced Encryption Standard
AES-Audio	Audio Engineering Society Audio
ANSI	American National Standards Institute
CO	Cryptographic Officer
CSP	Critical Security Parameter
DCI	Digital Cinema Initiative
DRNG	Deterministic Random Number Generator
CDH	Elliptic Curve Diffie-Hellman
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference

FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
KDM	Key Delivery Message
LDB	Link Decryptor Block
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
PCI-E	Peripheral Component Interconnect Express
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SMS	Screen Management System
SPL	Show Playlist