Dolby® IMS3-SM FIPS 140-2 Level 2 Validation

Non-proprietary Security Policy

Issue 3

Dolby Laboratories, Inc.

Corporate Headquarters

Dolby Laboratories, Inc.
1275 Market Street
San Francisco, CA 94103-1410 USA
Telephone 415-558-0200
Fax 415-863-1373
http://www.dolby.com

Table of Contents

Introduction

1.1 Purpose

This document is a non-proprietary cryptographic module security policy for the Dolby® IMS3-SM module. It describes how this module meets all the requirements specified in the FIPS (Federal Information Processing Standards) 140-2 publication for security Level 2, and some of the Level 3 requirements. This policy forms a part of the submission package provided to the testing lab.

FIPS 140-2 specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard, go to http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

1.2 References

This security policy describes how the IMS3-SM complies with the 11 sections of the standard.

- For more information on the FIPS 140-2 standard and validation program, go to http://csrc.nist.gov/.
- For more information about Dolby Laboratories solutions, go to http://www.dolby.com/.

IMS3-SM Overview

The IMS3-SM is the module that contains the security manager present in the Dolby® IMS3000 (Product Model: CID1002) for hardware models IMS3-41, IMS3-42 and IMS3-43. The Dolby® IMS3000 can be hosted inside Digital Cinema DLP projectors. It supports the highest JPEG-2000 decoding capabilities and also accepts alternative content.

The figures below show the three IMS3-SM hardware models. All three IMS3-SM hardware models require quantity 4 tamper labels. For details regarding label placement, see **Figure 1** through **Figure 3**.

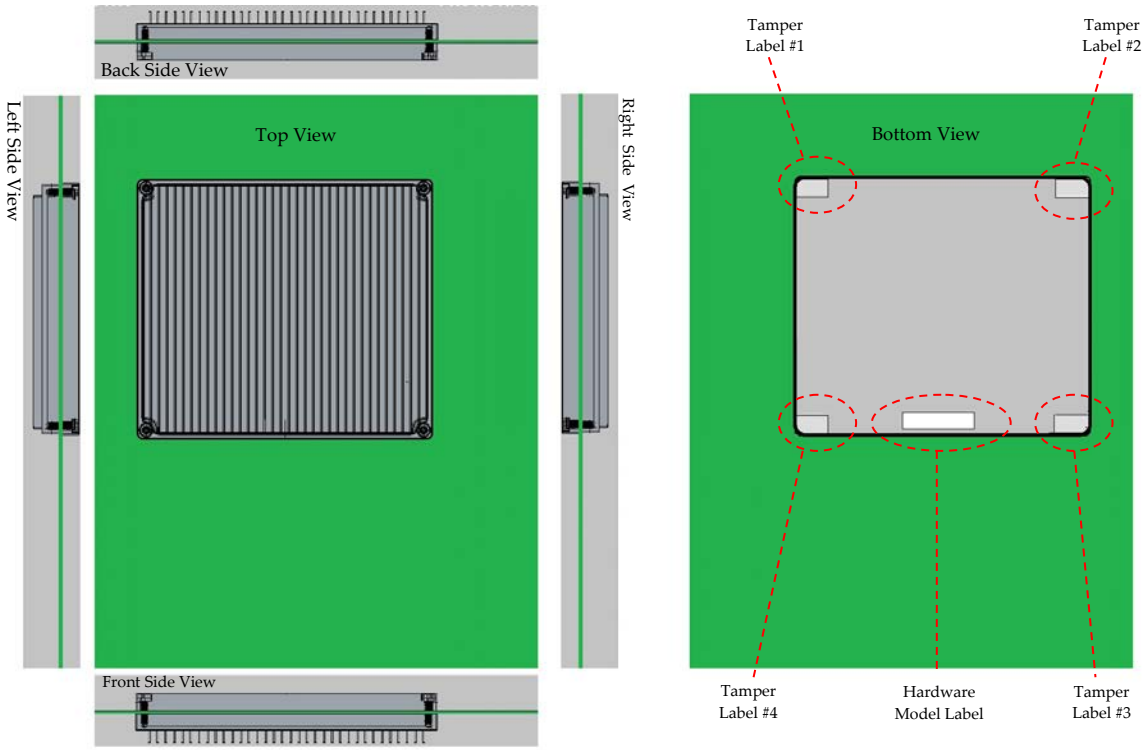

Figure 1 Hardware Model IMS3-41

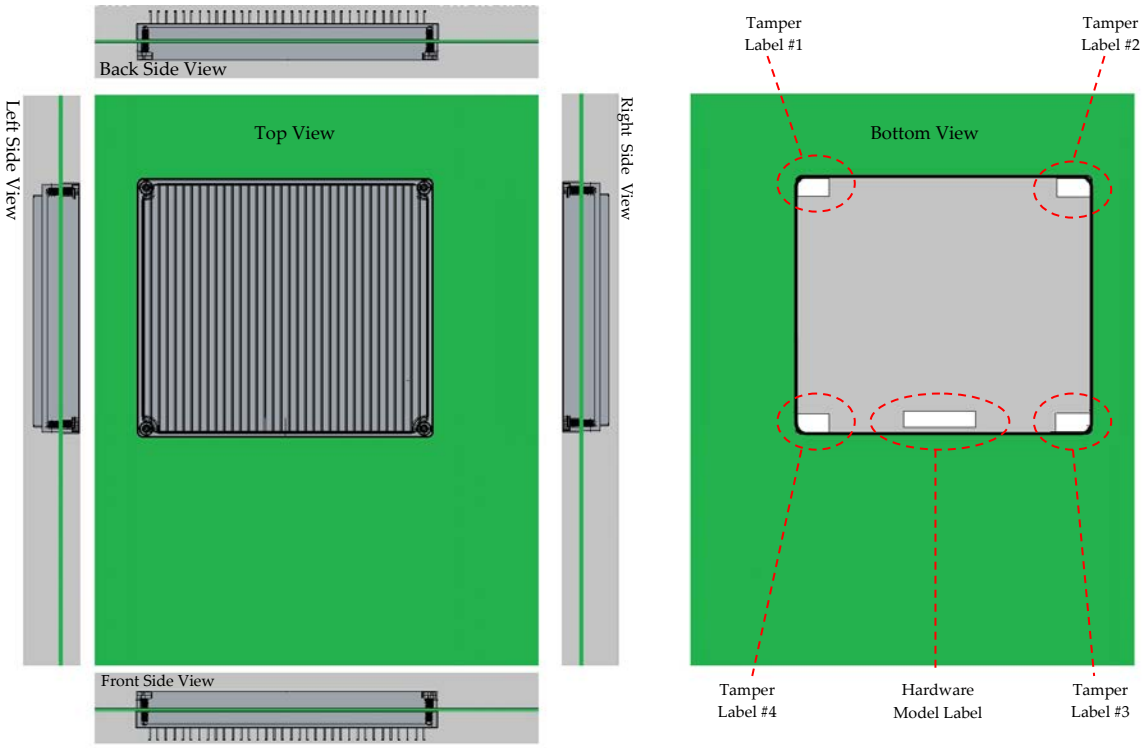

Figure 2 Hardware Model IMS3-42

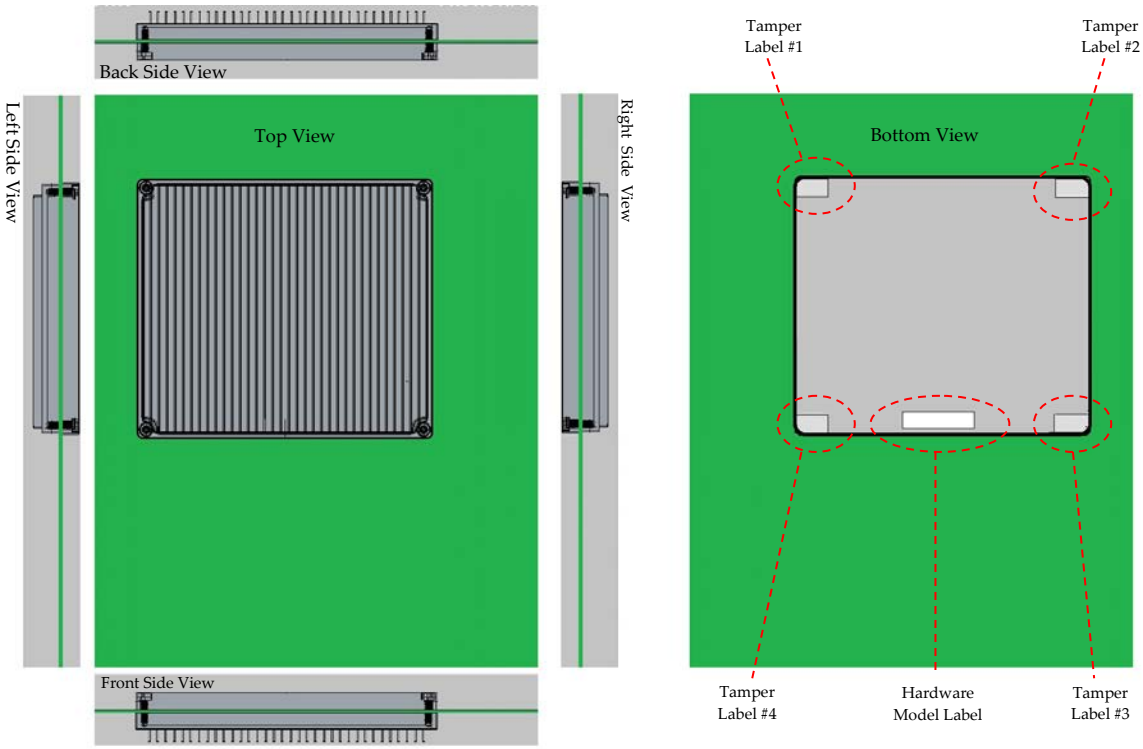

Figure 3 Hardware Model IMS3-43

The IMS3-SM block diagram is presented below:

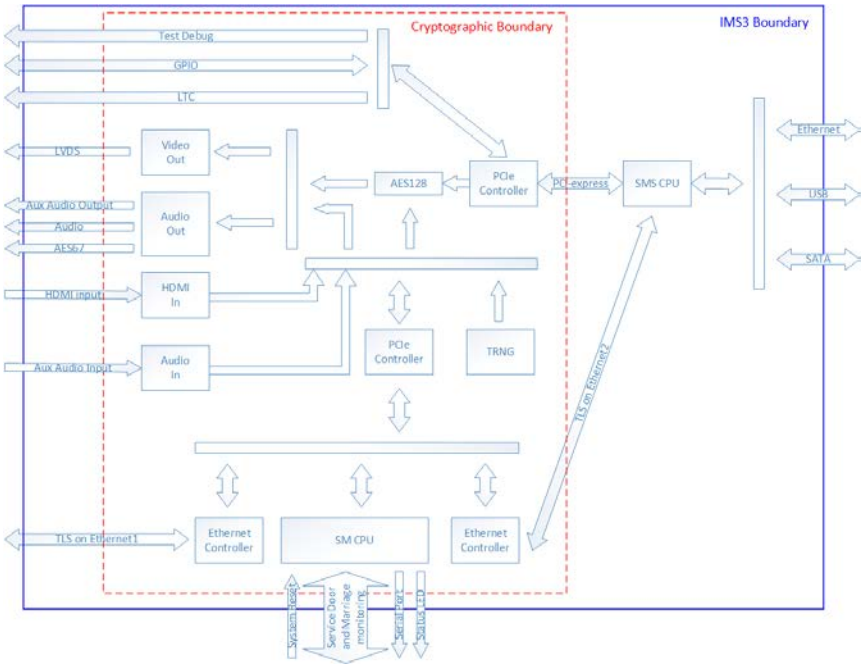

Figure 4 IMS3-SM Block Diagram

FIPS 140-2 Modes of Operation

The IMS3-SM module provides a FIPS Approved mode of operation. This mode of operation makes use of Approved algorithms and also supports non-Approved algorithms that are allowed in a FIPS Approved mode of operation.

At power up, the module enters FIPS Approved mode by default. This is verified by successful completion of the self-tests listed in Chapter 10. Whenever any of the non-Approved services listed in **Table 7-5** are invoked, the module is now in the non-Approved mode of operation.

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed). The resulting generated symmetric key is the unmodified output from SP800-90A DRBG.

3.1 Approved Algorithms

The IMS3-SM supports the following algorithms that are Approved for use in a FIPS mode of operation:

Table 3-1 FIPS Approved Algorithms

CAVP Cert #	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
4418	AES	FIPS 197, SP800-38A	ECB	128, 256	Data Encryption and Decryption [NOTE: AES ECB 256 is not used by any service in FIPS mode; it is used only as a prerequisite for the DRBG]
4419	AES	FIPS 197, SP800-38A	CBC	128	Data Encryption and Decryption
4421	AES	FIPS 197, SP800-38F	KW	128	Key Wrapping /Unwrapping
1427	DRBG	SP 800-90A Rev1	CTR-AES-256	-	Key Generation
2934	HMAC	FIPS 198-1	HMAC-SHA1	160	Firmware Load Test

2407	RSA	FIPS 186-4	SHA-256, PKCS v1.5	2048	Digital Signature Verification
3639	SHS	FIPS 180-4	SHA-1, SHA-256	-	Message Digest

3.2 Non-Approved Algorithms in FIPS Approved Mode

The IMS3-SM also supports the following non-approved algorithms that are allowed for use in the FIPS Approved mode of operation:

Table 3-2 Non-Approved Algorithms Allowed in FIPS Approved Mode

Algorithm	Caveat	Use
NDRNG	-	Seeding for the DRBG
RSA Key Wrapping	Provides 112 bits of encryption strength	Key wrapping; key establishment

3.3 Non-Approved Algorithm in Non-Approved Mode

The IMS3-SM supports the following non-Approved algorithms in the non-Approved mode of operation:

Table 3-3 Non-Approved Algorithms in Non-Approved Mode

Algorithm	Use
AES (non-compliant)	Encryption and Decryption
HMAC-MD5	TLS v1.0 key establishment
NDRNG	RNG seed generation
RNG (ANSI X9.31)	Random Number Generation
RNG (FIPS 186-2)	Random Number Generation
RSA (non-compliant)	Digital Signature Generation and Verification; Asymmetric Key generation
SP800-135 TLS v1.0 KDF (non-compliant)	TLS v1.0 KDF
TI ECDH	Non-security relevant data obfuscation to support interoperability with legacy equipment

Note: Keys that are derived from using the non-compliant TLS cannot be used in the Approved mode of operation.

Security Levels

The IMS3-SM design, development, tests and production has satisfied the requirements to ensure a secure product. It is especially adapted to Digital Cinema security requirements.

The IMS3-SM for hardware models IMS3-41, IMS3-42, and IMS3-43 and firmware versions 1.2.9-0, 1.2.9 -3, 1.2.4-0 is tested to meet the FIPS security requirements for the levels shown in the following table. These configurations are identified as follows:

(*Hardware Versions: IMS3-41 [A], IMS3-42 [A], and IMS3-43 [A]; Firmware Versions: (1.2.9-0, 1.2.9-3, and 1.2.4-0) [A]*; Hardware)

Table 4-1 FIPS 140-2 Security Levels

FIPS 140-2 Security Requirements	Section 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

Module Interfaces

The following table shows the logical interfaces of the IMS3-SM module and how they map to physical ports.

Table 5-1 FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Ports
Data Input Interface	Ethernet1, PCI-express, GPIO, HDMI, Ethernet2, Aux Audio Input
Data Output Interface	LVDS, PCI-express, GPIO, Audio, LTC (time code), Ethernet1, Ethernet2, Aux Audio Output, AES67
Control Input Interface	Ethernet1, Ethernet2, PCI-express, Service door and marriage monitoring, System reset
Status Output Interface	Ethernet1, Ethernet2, PCI-express, Serial Port, Service door and marriage monitoring, Status LED, Test Debug
Power Interface	Power traces

No maintenance access interface is present.

Critical Security Parameters

6.1 Secret and Private Keys and Other CSPs

Following are the secret and private keys that exist within the cryptographic module in the Approved Mode of Operation:

1. Device Secondary Master Key – AES key used to protect the Secondary CSP Secret Key and the AES Binary Update Key.
2. Update Private Key – Private RSA key used for key wrapping.
3. Secondary CSP Secret Key – AES key used to protect the Dolby HMAC Key.
4. AES Binary Update Key – AES key used to decrypt binaries being imported into the module.
5. DRBG Internal State Values – Used by the FIPS Approved DRBG.
6. DRBG Seed Values – Used to seed the FIPS Approved DRBG.
7. Dolby HMAC Key – HMAC key used for Firmware Load Test.

6.2 Public Keys

Public keys are not considered as critical security parameters because of their public status. The public keys contained in the module are listed here for consistency:

1. Update Public Key – Public RSA key used within Digital Certificate.
2. SMS User Public Key – Public RSA key used for TLS and within Digital Certificate.
3. SAS User Public Key – Public RSA key used for TLS and within Digital Certificate.
4. SOS (Crypto-Officer) User Public Key – Public RSA key used for TLS and within Digital Certificate.
5. Cinema Equipment Public Keys – Public RSA keys used for TLS and within Digital Certificate.
6. Signers Public Keys – Public RSA keys used to verify XML files signature and within Digital Certificate.

Roles and Services

The cryptographic module supports four distinct operator roles: PCI User, SMS User, SAS User, and SOS (Crypto-officer) User. No maintenance role is supported. The services for each user are shown in the following tables.

7.1 SMS User Services in FIPS Approved Mode

The following table shows all the services available to the SMS User – *Screen Manager*.

Table 7-1 SMS User Services

Services	Description	CSPs and Public Keys Possibly Involved	Type of access to CSPs and Public Keys
Update	Allows to perform firmware update related operations	AES Binary Update Key	Write
		AES Binary Update Key, Dolby HMAC Key, Update Private Key	Read

7.2 SAS User Services in FIPS Approved Mode

The following table shows all the services available to the SAS User – *Security Agent*.

Table 7-2 SAS User Services

Services	Description	CSPs and Public Keys Possibly Involved	Type of access to CSPs and Public Keys
All the services listed in **Table 7-1** for the SMS User are also available for the SAS User.			
Reset Board	Resets the module	Update private key, Update Public key, Device Secondary Master key, DRBG Internal States values and DRBG Seeds, AES Binary Update Keys	Write

7.3 SOS (Crypto-Officer) User Services in FIPS Approved Mode

The following table shows all the services available to the SOS (Crypto-Officer) User – *Security Officer*.

Table 7-3 SOS (Crypto-Officer) User Services

Services	Description	CSPs and Public Keys Possibly Involved	Type of access to CSPs and Public Keys
All the services listed in **Table 7-2** for the SAS User are also available for the SOS (Crypto-Officer) User.			
Approved Mode Configuration	Performs specific SOS (Crypto-Officer) User configuration operations.	Update Private key, Update Public Key	Read/Write
Zeroization	Zeroizes sensitive data (including all plain text CSPs)	All plaintext CSPs, Update Public key	Write

7.4 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 7-4 Unauthenticated Services

Services	Description	CSPs and Public Keys Possibly Involved	Type of access to CSPs and Public Keys
Get Session ID	Exports the current Session ID of the module	None	None
Show Status	Corresponds to the status information exported automatically through the Serial Port	None	None
Host Reset	Resets the host	None	None
Video Settings	Performs video related settings	None	None
Audio Engine	Executes audio related commands	None	None
Self-Test	The power recycling of the IMS3-SM allows executing the suite of power-up tests required by FIPS 140-2. No other defined service allows executing these power-up tests. It has to be considered as an unauthenticated service as it only requires the IMS3-SM to be powered off and powered on	None	None

7.5 Non-Approved Services

Any operator can invoke the following non-approved services in the non-approved mode of operation:

Table 7-5 Non-Approved Services

Roles	Services	Description	Non-Approved Algorithm(s) Involved
PCI User	Basic Configuration	Sets and retrieves basic configuration parameters.	AES-128-ECB (non-compliant)
PCI User	Configuration	Performs configuration related operations.	SP800-135 TLS v1.0 KDF (non-compliant) RSA (non-compliant) TI-ECDH
PCI User	Advanced Configuration	Sets and retrieves advanced configuration parameters.	AES-128-ECB (non-compliant)
PCI User	Get Status Information	Retrieves status information.	None
PCI User	GPIO Service	Loads and retrieves GPIO data.	None
PCI User	Clear License	Deletes a license file.	SP800-135 TLS v1.0 KDF (non-compliant) RSA (non-compliant)
PCI User, SMS User, SAS User, SOS (Crypto-Officer) User	Get Advanced Information	Retrieves advanced information.	SP800-135 TLS v1.0 KDF (non-compliant) RSA (non-compliant) SHA-256 (non-compliant)
PCI User, SMS User, SAS User, SOS (Crypto-Officer) User	Basic Operations	Performs basic operations.	SP800-135 TLS v1.0 KDF (non-compliant) RSA (non-compliant)
SMS User, SAS User, SOS (Crypto-Officer) User	Basic Settings	Performs some of the module's settings.	SP800-135 TLS v1.0 KDF (non-compliant) RSA (non-compliant)
SMS User, SAS User, SOS (Crypto-Officer) User	Suite Management	Provides suite management operations.	SP800-135 TLS v1.0 KDF (non-compliant) RSA (non-compliant) AES-128-CBC (non-compliant) HMAC-SHA1 (non-compliant)

SAS User, SOS (Crypto-Officer) User	Obsolete Board	Deletes non-sensitive cinema data.	SP800-135 TLS v1.0 KDF (non-compliant) RSA (non-compliant) NDRNG
SOS (Crypto-Officer) User	SOS Configuration	Performs specific SOS (Crypto-Officer) User configuration operations.	SP800-135 TLS v1.0 KDF (non-compliant) AES Key Wrapping (non-compliant) RSA (non-compliant)
SOS (Crypto-Officer) User	Delete	Deletes non-sensitive cinema data.	SP800-135 TLS v1.0 KDF (non-compliant)
All roles	Network Configuration	Performs non-security relevant network related configuration operations.	TI-ECDH
All roles	Setup	Performs non-security relevant setup operations	TI-ECDH

7.6 Authentication Strength

The cryptographic module enforces the separation of roles using identity-based operator authentication. The PCI User role is authenticated through the use of "PCI User Authentication Secrets" – known only by Dolby Laboratories– associated with the current Session Id. Note that data to be compared to authentication secrets are imported encrypted in the module.

SMS, SAS, and SOS (Crypto-Officer) User roles are authenticated through the use of 2048 bits RSA Signatures. Note that these authentications rely on the usage of TLS.

Table 7-6 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Mechanism
PCI User	Identity-based operator authentication	Authentication Secret Verification
SMS User	Identity-based operator authentication	2048 bits RSA Signature Verification
SAS User	Identity-based operator authentication	2048 bits RSA Signature Verification
SOS (Crypto-Officer) User	Identity-based operator authentication	2048 bits RSA Signature Verification

Table 7-7 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Authentication Secret Verification	With 256 possible characters and 8-character Authentication Secret, the probability that a random attempt will succeed or a false acceptance will occur is $5.42 \times 10^{-}(20)$ that is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute with a replay delays of 1s is $3.25 \times 10^{-}(18)$ that is less than 1/100,000.
2048 bits RSA Signature Verification	This verification relies on 2048 bits RSA keys known to provide an equivalent of 112 bits of encryption strength. Therefore, a random attempt has an associated probability of fault acceptance of (1/2)^112, which is less than 1/1,000,000. Given the processing capabilities and the clock speed, the number of consecutive attempts that could be launched in a one minute period is extremely limited. An extremely conservative estimate is that the probability of successfully authenticating in a one minute period would be (1/2)^69, which is much less than 1/100,000.

Physical Security

The IMS3-SM is classified as a multiple-chip embedded module for FIPS purposes. It is comprised of production grade components.

The physical security mechanism employed by the module includes a hard, opaque and tamper-evident metal enclosure that is monitored 24/7 by tamper detection and response mechanisms; any attempt to remove the metal enclosure results in instantaneous active zeroization of all plaintext CSPs. The module also includes tamper evident labels covering each of the mounting hardware for models IMS3-41, IMS3-42, and IMS3-43.These labels are installed by the manufacturer. The PCB itself also provides tamper evidence. The tamper evident metal enclosure, tamper evident labels and tamper evident PCB shall be periodically inspected to ensure that physical security is maintained.

Note: The module hardness testing was only performed at an ambient, single temperature (i.e. 65.3° F) and no assurance is provided for Level 3 hardness conformance at any other temperature.

The cryptographic boundary is the outer perimeter of the module's metal enclosure edge (see Chapter 2) and it includes the hard, opaque and tamper-evident metal enclosure covering all security relevant components.

All the components that reside outside of the metal enclosure are excluded from FIPS 140-2 requirements. Components excluded from the FIPS 140-2 requirements are not security relevant. The excluded components are the non-security relevant data input and data output, filtering components (capacitors, resistors, inductance), voltage regulators, fuses, traces and signals routed to said components, PCB outside metal enclosure, CPU and its memory and connectors.

Table 8-1 Physical Security Inspection

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Metal enclosure with tamper detection and response mechanisms	Upon receiving the module from the manufacturer, and as often as feasible.	Visually inspect all sides of the metal enclosure for visible evidence of tampering (for example, scratches, scrapes, nicks, gouges, and so on). Check the output of the Show Status service on an ongoing basis to confirm that the module has not been tampered with or zeroized.
Tamper evident labels	Upon receiving the module from the manufacturer, and as often as feasible.	Visually inspect the labels for visible evidence of tampering (for example, removal, scratches, scrapes, rips, nicks, replacements, gouges, and so on).
Tamper evident PCB	Upon receiving the module from the manufacturer, and as often as feasible.	Visually inspect the PCB for visible evidence of tampering (for example, scratches, scrapes, nicks, gouges, and so on).

If any tampering with the module is suspected, please remove the module from service and contact Dolby Laboratories Technical Services department immediately at +1-415-645-4900 or email cinemasupport@dolby.com.

Operational Environment

The IMS3-SM supports a limited operational environment that allows only the loading of trusted, validated, and HMACed binary images through authenticated service. Dolby Laboratories maintains sole possession of the corresponding HMAC key needed to validate the uploaded binary into the IMS3-SM.

Self Tests

The IMS3-SM module performs the following self tests:

Power Up Self Tests	Status Output
• BIOS Integrity Test	*"Checking BIOS checksum.. valid" or "Checking BIOS checksum.. invalid"*
• Bootloader Integrity Test	*"Checking bootloader checksum.. valid" or "Checking bootloader checksum.. invalid"*
• Firmware Integrity Test (16 bits and 32 bits CRC)	*"Checking boot checksum.. valid" or "Checking boot checksum.. invalid"*
	"Checking root checksum.. valid" or "Checking root checksum.. invalid"
	"Checking firmware checksum.. valid" or "Checking firmware checksum.. invalid"
	"Checking rootfs" or "rootfs checksum verification failed"
	"Checking linux kernel" or "kernel checksum verification failed"
	"firmware integrity seltest succeeded" or "firmware integrity seltest failed"
• SP800-90a Rev1 DRBG Known Answer Test	*"SP800-90A DRBG selftest succeeded" or "SP800-90A DRBG selftest failed"*
• SHA-1 Known Answer Test	*"SHA1 selftest succeeded" or "SHA1 selftest failed"*
• HMAC Known Answer Test	*"HMAC selftest succeeded" or "HMAC selftest failed"*
• AES Encryption Known Answer Test	*"AES selftest succeeded" or "AES test failed"*
• AES Decryption Known Answer Test	*"AES selftest succeeded" or "AES test failed"*
• RSA Digital Signature Generation Known Answer Test (RSA 2048 SHA-256)	*"RSA selftest succeeded" or "RSA selftest failed"*

• RSA Digital Signature Verification Known Answer Test (RSA 2048 SHA-256)	*"RSA selftest succeeded" or "RSA selftest failed"*
• CRC 32-bit Known Answer Test	*"CRC 32-bit selftest succeeded" or "CRC 32-bit selftest failed"*
• CRC 16-bit Known Answer Test	*"CRC 16-bit selftest succeeded" or "CRC 16-bit selftest failed"*
• AES KeyWrap Known Answer Test	*"KeyWrap selftest succeeded" or "KeyWrap selftest failed"*
Conditional Tests	**Status Output**
• Firmware Load Test (HMAC-SHA1)	*None in case of success; "Error: decipher_body(): checksum incorrect" in case of failure*
• DRBG Continuous Test	*None in case of success; "FIPS Lock" in case of failure*
• NDRNG Continuous Test	*None in case of success; "FIPS Lock" in case of failure.*
• Pair-wise Consistency Test (Digital Signature Generation/Verification; Encryption/Decryption)	*None in case of success; "FIPS Lock" in case of failure.*

The bypass test and the Manual Key Entry Test are N/A.

Note that SHA-1 is used only for HMAC-SHA1 and RSA Digital Signature Verification.

Mitigation of Other Attacks

The IMS3-SM does not mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

Table 11-1 Mitigation of Other Attacks

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

Security Rules

The cryptographic modules design corresponds to the modules security rules. This chapter documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 2 module.

1. The cryptographic module shall provide four distinct operator roles. These are the PCI User role, the SMS User role, the SAS User role, and the SOS (Crypto-Officer) User role.
2. The cryptographic module shall provide identity-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. Data output shall be inhibited during self tests and error states.
5. Data output shall be logically disconnected from the internal process performing key generation and zeroization.
6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The module shall not support a bypass capability or a maintenance interface.
8. The cryptographic module performs the self tests as presented in Chapter 10 above.
9. At any time the operator is capable of commanding the module to perform the power-up self-test by a power cycle.
10. Prior to each use, the SP800-90a Rev1 DRBG and the NDRNG are tested using the conditional test specified in FIPS 140-2 §4.9.2.
11. The module supports concurrent operators.

Appendix A – CSPs and Public Keys

The module's CSPs are listed below:

1) Device Secondary Master Key
- Description: AES KW 128 bits Key used to encrypt/decrypt other CSPs.
- Generation: Generated using the SP800-90A Rev1 DRBG. 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.
- Establishment: N/A
- Storage: Stored in plaintext in the Tamper switch. Temporarily stored in plaintext in SDRAM.
- Entry: N/A
- Output: N/A
- Zeroization: Zeroized by "Zeroization" or "Reset Board" authenticated services. Zeroized when the Tamper switch it is stored in is opened. Also destructed when a tamper event is detected.

2) Update Private Key
- Description: Private 2048 bits RSA key used for key wrapping.
- Generation: N/A. Pre-loaded during manufacturing.
- Establishment: N/A
- Storage: Stored encrypted using AES KW in flash memory. Temporarily stored in plaintext in SDRAM.
- Entry: N/A
- Output: N/A
- Zeroization: Temporary plaintext copies are zeroized by the "Zeroization" authenticated service and when a tamper event or a power shortage happens.

3) Secondary CSP Secret Key
- Description: 128 bits AES KW key used to decrypt other CSPs.
- Generation: N/A. Pre-loaded during manufacturing.
- Establishment: N/A
- Storage: Stored encrypted using AES KW in flash memory and temporarily in plaintext in the SDRAM.
- Entry: N/A
- Output: N/A
- Zeroization: All copies are zeroized by the "Zeroization" authenticated service. Temporary copies stored in RAM are also zeroized at power-off, when a tamper event or a power shortage happens.

4) DRBG Internal State Values

- Description: The internal state values required by the DRBG based on SP800-90A Rev 1 present on the module are the following:
  . K (AES key) – 256 bits
  . V (seed) – 128 bits
- Generation: Initialized and updated through the DRBG processing itself.
- Establishment: N/A
- Storage: Stored in plaintext in SDRAM.
- Entry: N/A
- Output: N/A
- Zeroization: All copies of these internal state values are destructed when the DRBG is uninstantiated.

5) DRBG Seed Values

- Description: Seed values required by the DRBG based on SP800-90A Rev1
- Generation: Initialized by the module's Hardware TRNG.
- Establishment: N/A
- Storage: Stored in plaintext in SDRAM.
- Entry: N/A
- Output: N/A
- Zeroization: All copies of these seeds are zeroized by the "Zeroization" authenticated service and when the DRBG is uninstantiated. Plaintext copies are also zeroized when a tamper event or a power shortage happens.

6) Dolby HMAC Key

- Description: 160 bit HMAC key used to authenticate binaries loaded into the module.
- Generation: N/A. Pre-loaded during manufacturing.
- Establishment: N/A
- Storage: Stored encrypted using AES KW in flash memory and in plaintext in SDRAM.
- Entry: N/A
- Output: N/A
- Zeroization: All plaintext copies of this key are zeroized by the "Zeroization" authenticated service. Plaintext copies of this key stored in RAM are also zeroized at power-off, when a tamper event or a power shortage happens.

7) AES Binary Update Key

- Description: 128 bits AES-CBC Key used for decryption.
- Generation: N/A. Imported wrapped in RSA.
- Establishment: Wrapped with RSA
- Storage: Stored temporarily in plaintext in SDRAM. Otherwise, the RSA wrapped copies are stored encrypted using AES KW in flash memory.
- Entry: Imported wrapped in RSA, through the "Update" authenticated service.
- Output: Exported wrapped in RSA, through the authenticated TLS services "Update".
- Zeroization: All plaintext copies (and non-AES-encrypted, wrapped in RSA or not) of this key are zeroized by the "Zeroization" authenticated service. Copies (wrapped in RSA or not) stored in RAM are also destructed at power-off. Plaintext copies (and non-AES-encrypted RSA wrapped copies) are also destructed when a tamper event or a power shortage happens.

The module supports the following Public Keys:

1) Update Public Key
- Description: 2048 bits Update Public RSA Key used in Digital Certificate
- Generation: N/A. Pre-loaded during manufacturing.
- Establishment: N/A
- Storage: Stored in plaintext in the flash memory. Temporarily stored in plaintext in SDRAM.
- Entry: Imported back in an RSA digitally signed certificate through the "Approved Mode Configuration" authenticated service.
- Output: Exported through the "Approved Mode Configuration" authenticated service.
- Zeroization: Zeroized by the "Zeroization" or "Reset Board" authenticated services.

2) SMS User Public Key
- Description: 2048 bits Public RSA Key used within Digital Certificate for TLS authentication.
- Generation: N/A. Imported during manufacturing.
- Establishment: N/A
- Storage: Stored in plaintext in the flash memory. Temporarily stored in plaintext in SDRAM.
- Entry: Imported in an RSA digitally signed certificate through the "Approved Mode Configuration" authenticated service and during TLS handshake mechanism.
- Output: Exported through the "Approved Mode Configuration" authenticated service.
- Zeroization: Zeroized by the "Zeroization" or "Reset Board" authenticated service.

3) SAS User Public Key
- Description: 2048 bits Public RSA Key used within Digital Certificate for TLS authentication.
- Generation: N/A. Pre-loaded during manufacturing.
- Establishment: N/A
- Storage: Stored in plaintext in the flash memory. Temporarily stored in plaintext in SDRAM.
- Entry: The certificate to be compared against this SAS certificate is imported during TLS handshake mechanism.
- Output: N/A
- Zeroization: N/A

4) SOS User Public Key
- Description: 2048 bits Public RSA Key used within Digital Certificate for TLS authentication.
- Generation: N/A. Pre-loaded during manufacturing.
- Establishment: N/A
- Storage: Stored in plaintext in the flash memory. Temporarily stored in plaintext in SDRAM.
- Entry: The certificate to be compared against this SOS certificate is imported during TLS handshake mechanism.
- Output: N/A
- Zeroization: N/A

5) Cinema Equipment Public Keys

- Description: 2048 bits Public RSA Keys imported within a Digital Certificate when a TLS connection is established.
- Generation: N/A
- Establishment: N/A
- Storage: Stored in plaintext SDRAM.
- Entry: TLS handshake mechanism.
- Output: N/A
- Zeroization: Zeroized at power-off or when the TLS session ends.

6) Signers Public Keys

- Description: 2048 bits Public RSA Keys imported within a Digital Certificate as part of a digitally signed license files import. They are used only to verify digital signatures.
- Generation: N/A
- Establishment: N/A
- Storage: Stored in plaintext SDRAM and in plaintext in the flash memory.
- Entry: Imported through "Update" authenticated service.
- Output: Exported through the "Update" authenticated service.
- Zeroization: Zeroized by the "Reset Board", the "Zeroization" and the "Update" authenticated services. Copies stored in RAM are zeroized at power-off. Also, the expired license files (therefore their signer public keys) are automatically deleted every hour.

Appendix B – CKG as per SP800-133

In accordance with FIPS 140-2 IG D.12, the cryptographic module performs Cryptographic Key Generation (CKG) as per SP800-133 (vendor affirmed). The resulting generated symmetric key is the unmodified output from SP800-90A DRBG. Please see Appendix A – CSPs and Public Keys for more information.

Acronyms

Term	Definition
AES	Advanced Encryption Standard
AES/EBU	Audio Engineering Society/European Broadcasting Union
ANSI	American National Standards Institute
CSP	Critical Security Parameter
DCI	Digital Cinema Initiatives
DRBG	Deterministic Random Bit Generator
DRNG	Deterministic Random Number Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
FPGA	Field-Programmable Gate Array
GPI	General Purpose Input
GPIO	General Purpose Input/Output
GPO	General Purpose Output
HD	High Definition
HMAC	Keyed Hash Message Authentication Code
KAT	Known Answer Test
LTC	Linear Time-Code
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OSD	On Screen Display
PCI	Peripheral Component Interconnect

Term	Definition
PRF	Pseudo Random Function
RNG	Random Number Generator
RSA	Rivest, Shamir and Adelman
RTC	Real Time Clock
SAS	Security Agent System
SDI	Serial Digital Interface
SHA	Secure Hash Algorithm
SMS	Screen Management System
SOS	Security Officer System
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TRNG	True Random Number Generator

Document Revision History

Date	Issue	Description
03/16/2017	1	First version
05/16/2017	2	Second version
06/20/2017	3	Third version