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

Nonproprietary Security Policy

Version: 4

Dolby Laboratories, Inc.

Corporate Headquarters

Dolby Laboratories, Inc.
100 Potrero Avenue
San Francisco, CA 94103-4813 USA
Telephone 415-558-0200
Fax 415-863-1373
www.dolby.com/

European Licensing Liaison Office

Dolby International AB
Apollo Building, 3E
Herikerbergweg 1-35
1101 CN Amsterdam Zuidoost
The Netherlands
Telephone 31-20-651-1800
Fax 31-20-651-1801

Table of Contents

Introduction

1.1 Purpose

This document is a nonproprietary cryptographic module security policy for the Dolby® IMS-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 IMS-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/.

IMS-SM Overview

The IMS-SM is the security manager module present in the Dolby® IMS1000 (for hardware models IMS-SM-C1, IMS-SM-C2, IMS-SM-E1 and IMS-SM-E2) or IMS2000 (for hardware models IMS2-SM-C1, IMS2-SM-C2 and IMS2-SM-C3) that 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 seven IMS-SM hardware models. Figure 2 through Figure **7** have the same orientation depicted in Figure **1.** All seven IMS-SM hardware models require quantity 4 tamper labels. For details regarding label placement, see Figure 2 through Figure 7.

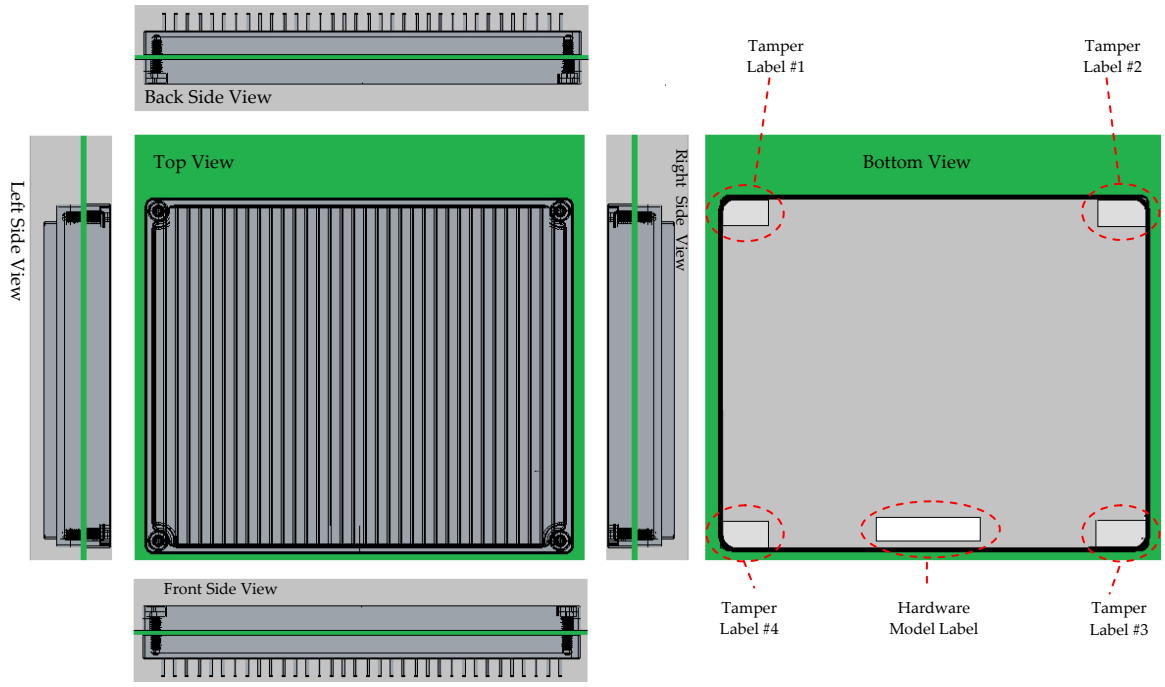

Figure 1 Hardware Model IMS-SM-C1

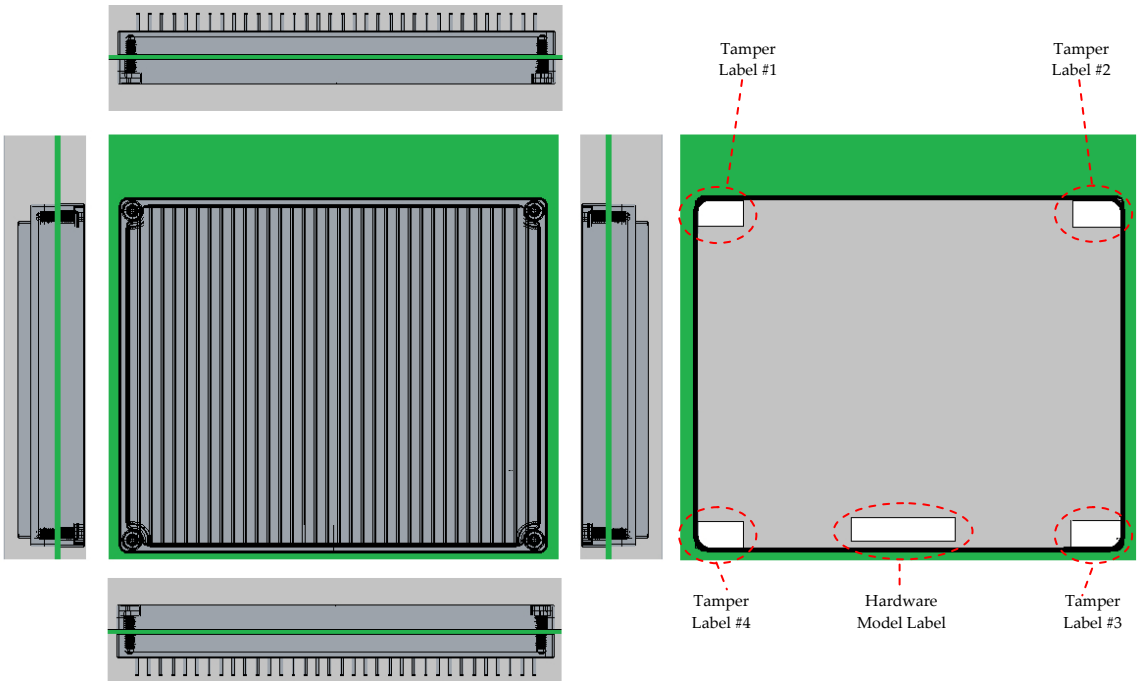

Figure 2 Hardware Model IMS-SM-C2

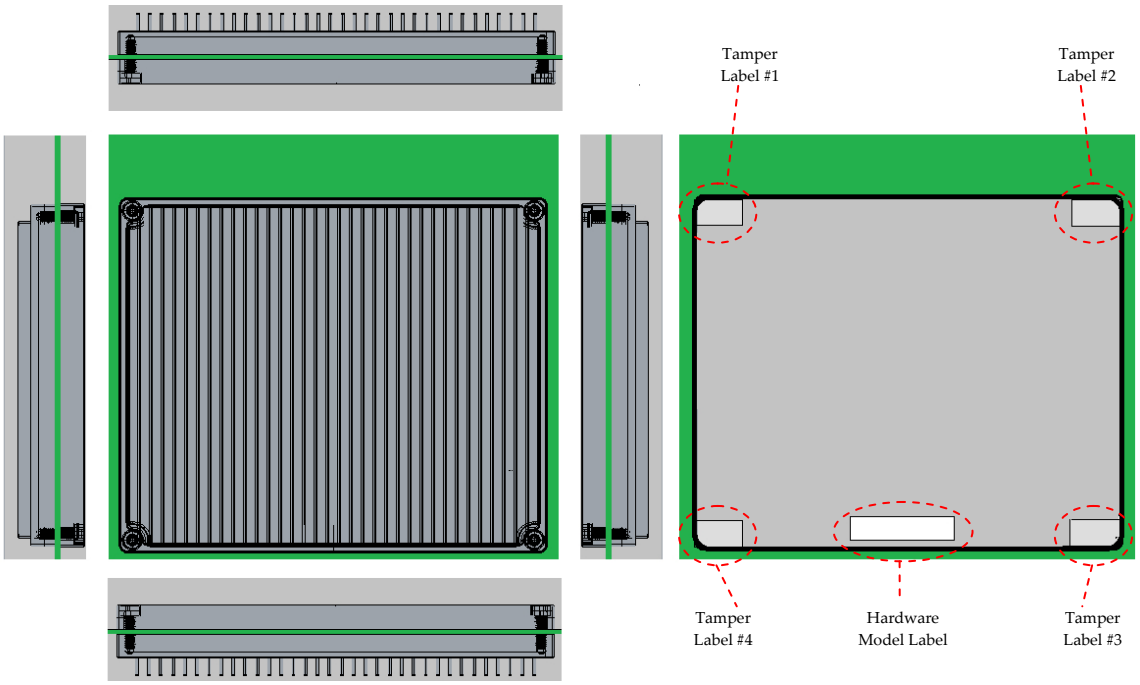

Figure 3 Hardware Model IMS-SM-E1

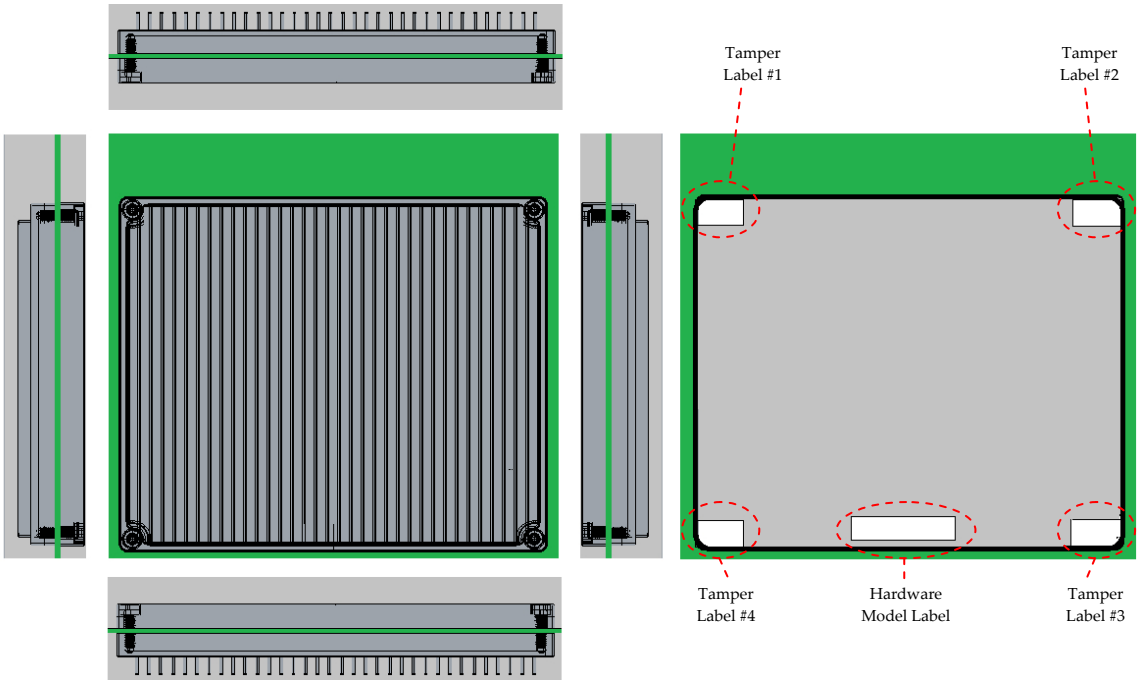

Figure 4 Hardware Model IMS-SM-E2

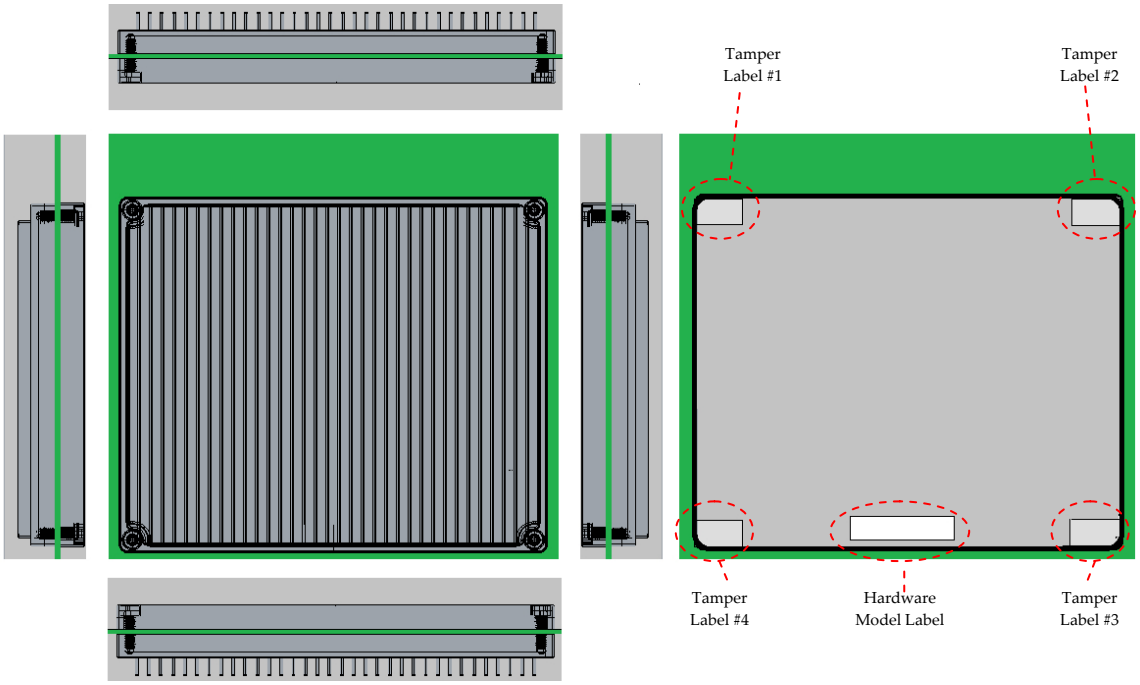

Figure 5 Hardware Model IMS2-SM-C1

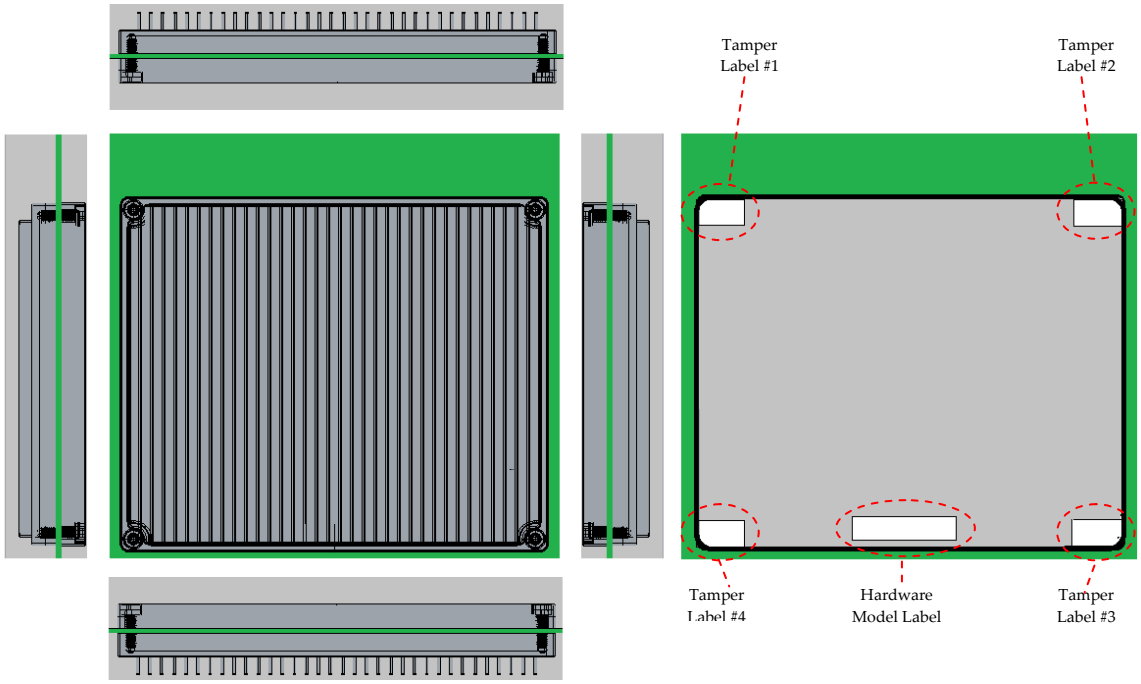

Figure 6 Hardware Model IMS2-SM-C2

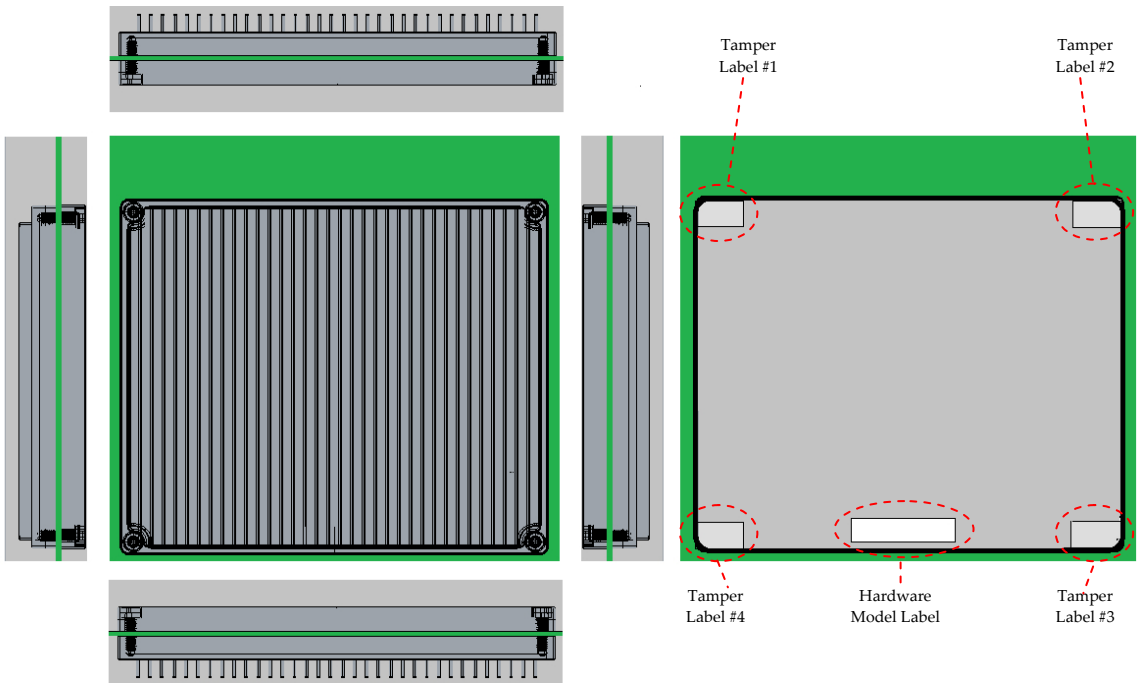

Figure 7 Hardware Model IMS2-SM-C3

The IMS-SM block diagram is presented below:

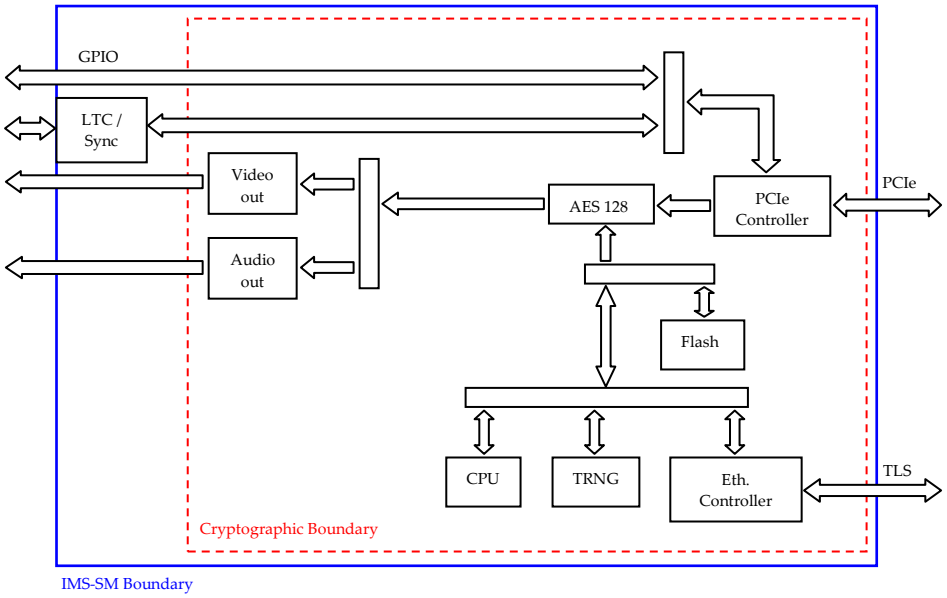

Figure 8 IMS-SM Block Diagram

FIPS 140-2 Modes of Operation

The IMS-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.

To determine that the module is running in FIPS mode, invoke the "Get Advanced Information" service and check that the firmware versions are the same as those written in this security policy document. Also, check that the hardware version written on the modules sticker matches the one specified in this security policy document. The operator shall also ensure that all self-tests pass and that the module transitions into operational mode as indicated by the following status available via the Show Status service: FIPS Check … SUCCESS All Good.

The IMS-SM module also provides a non-approved mode of operation that makes use of TI ECDH that "is not" allowed in the FIPS Approved mode of operation. Use of the Network Configuration Service places the module in the non-approved mode of operation. Upon completion of the Network Configuration Service, the module automatically transitions back into the FIPS Approved mode of operation.

3.1 Approved Algorithms

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

- AES (FPGA implementation) with 128 bit keys decryption in CBC mode – see Certificate #2974
- AES with 128 bit keys for encryption and decryption in CBC mode – see Certificate #2975
- AES with 128 bit keys for encryption and decryption in ECB mode – see Certificate #2976
- KTS (AES Certificate #2996; key establishment methodology provides 128 bits of encryption strength)
- HMAC-SHA1 – see Certificate #1897
- SHA-1 and SHA-256, used by other algorithms (such as, HMAC-SHA1, FIPS 186-2 RNG or RSA Digital Signature) – see Certificate #2500. Note: SHA-1 is used only for HMAC-SHA1 and RSA Digital Signature Verification.
- ANSI X9.31 RNG, using TDES-2Keys – see Certificate #1300
- FIPS 186-2 RNG – see Certificate #1301

- RSA Digital Signature Generation/Verification – see Certificate #1569
- RSA Digital Signature Verification – see Certificate #1567
- RSA Key Generation – see Certificate #1568
- CVL (SP800-135 TLS KDF) – see Certificate #365

3.2 Non-approved Algorithms in FIPS Approved Mode

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

- RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- NDRNG (Non Deterministic Random Number Generator) – used to seed the Approved ANSI X9.31 RNG presented in paragraph 3.1
- MD5 – used for TLS key establishment (that is, in TLS KDF only)
- HMAC-MD5 used for TLS key establishment (that is, in TLS KDF only)

3.3 Non-approved Algorithm in Non-approved Mode

The IMS-SM supports the following non-approved algorithm in the non-approved mode of operation:

- TI ECDH: non-security relevant data obfuscation to support interoperability with legacy equipment

Security Levels

The IMS-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 IMS-SM for hardware models IMS-SM-C1, IMS-SM-C2, IMS-SM-E1, IM-SM-E2, IMS2-SM-C1, IMS2-SM-C2 and IMS2-SM-C3 and firmware versions 4.4.1-0, 4.2.0-3, 6.0.12d-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: IMS-SM-C1 [A], IMS-SM-C2 [A], IMS-SM-E1 [A], IMS-SM-E2 [A], IMS2-SM-C1 [A], IMS2-SM-C2 [A] and IMS2-SM-C3 [A]; Firmware Versions: (4.4.1-0, 4.2.0-3 and 6.0.12d-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 IMS-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	LVDS trace, PCI-express trace, GPIO traces, SDI dual HD input traces, HDMI input trace, LTC (time code) input connector, Ethernet traces
Data Output Interface	LVDS trace, PCI-express trace, GPIO connectors, Audio traces, LTC (time code) output connector, Ethernet traces
Control Input Interface	LVDS trace, PCI-express trace, Service door and marriage monitoring traces, Video sync input traces, System reset trace
Status Output Interface	LVDS trace, PCI-express trace, Serial Port, Clock output, Service door and marriage monitoring traces, Status LED traces
Power Interface	PCI-express trace, 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.

1. Device Master Key – AES key used to protect the Device Private Key, the External Private Key, the CSP Secret Key and the AES Binary Update Key.
2. Device Private Key – Private RSA key used for key wrapping and TLS.
3. External Private Key – Private RSA key used for key wrapping.
4. Extra Private Key – Private RSA key, used for digital signature generation and TLS client operations.
5. Reset Private Key – Private RSA key used for key wrapping and TLS.
6. Reset Secret Key – AES key used to protect the Reset Private Key.
7. CSP Secret Key – AES key used to protect the Reset Secret Key, the Dolby HMAC Key, the AES Shared knowledge Key, the AES Wrapping Key and the PCI User Authentication Secrets.
8. AES Wrapping Key – AES key used for AES Key Wrapping.
9. AES Content Encryption Keys – AES keys that protect content.
10. AES Binary Update Key – Used to decrypt binaries being imported into the module.
11. Seed Values – Used to seed the FIPS Approved RNGs.
12. AES Shared Knowledge Key – AES key used to secure import/export of CSPs.
13. Dolby HMAC Key – HMAC key used for Firmware Load Test.
14. Content Integrity Keys – HMAC keys used to verify the integrity of HMAC content.
15. TLS AES Session Keys – AES keys used for TLS communication.
16. TLS HMAC Sessions Keys – HMAC keys used for TLS communication.
17. TLS PRF Data – Used for TLS session key establishment.
18. TLS Master Secret – Used for TLS session key establishment.
19. TLS Pre-Master Secret – Used for TLS session key establishment.
20. PCI User Authentication Secrets – PCI User Authentication Secrets used by the module (eight characters).

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. Device Public Key – Public RSA key used for TLS and within Digital Certificate.
2. External Public Key – Public RSA key used within Digital Certificate.
3. Extra Public Key – Public RSA key used for TLS client mode and within digital certificate.
4. Reset Public Key – Public RSA key used for TLS and within Digital Certificate.
5. SMS User Public Key – Public RSA key used for TLS and within Digital Certificate.
6. SAS User Public Key – Public RSA key used for TLS and within Digital Certificate.
7. SOS (Crypto-Officer) User Public Key – Public RSA key used for TLS and within Digital Certificate.
8. Cinema Equipment Public Keys – Public RSA keys used for TLS and within Digital Certificate.
9. Signers Public Keys – Public RSA keys used to verify XML files signature and within Digital Certificate.
10. ICP Public Keys – Public RSA keys used within Digital Certificate for TLS and Digital Signature verification.

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 PCI User Services In FIPS Approved Mode

The following table summarizes specific services available to the PCI Users only.

Table 7-1 PCI User Services

Services	Description	CSPs and Public Keys Possibly Involved	Type of access to CSPs and Public Keys
Basic Configuration	Sets and retrieves basic configuration parameters.	AES Shared Knowledge Key, AES Content Encryption Keys	Read
		Content Integrity Keys	Read/Write
Advanced Configuration	Sets and retrieves advanced configuration parameters.	Device Master Key, Dolby HMAC Key, AES Binary Update Key, External Private Key, CSP Secret Key, AES Shared Knowledge Key, External Public Key	Read
		AES Content Encryption Keys	Read/Write
Get Status Information	Retrieves status information.	None	None
GPIO	Loads and retrieves GPIO data.	None	None
Get Advanced Information	Retrieves advanced information.	Device Master Key, Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, Reset Public Key, External Public Key, Extra Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		Cinema Equipment Public Keys	Write

Services	Description	CSPs and Public Keys Possibly Involved	Type of access to CSPs and Public Keys
Basic Operations	Performs basic operations.	Device Master Key, Device Private Key, Extra Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, AES Wrapping Key, Device Public Key, Reset Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		AES Binary Update Key, AES Content Encryption Keys, Content Integrity Keys, Seed Values, Signers Public Keys, Cinema Equipment Public Keys, ICP Public Keys	Write
		External Private Key, External Public Key	Read/Write
Configuration	Performs configuration related operations	TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret	Read

7.2 SMS User Services in FIPS Approved Mode

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

Table 7-2 SMS User Services

Services	Description	CSPs and Public Keys Possibly Involved	Type of access to CSPs and Public Keys
Get Advanced Information	Retrieves advanced information.	Device Master Key, Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, Reset Public Key, External Public Key, Extra Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		Cinema Equipment Public Keys	Write

Services	Description	CSPs and Public Keys Possibly Involved	Type of access to CSPs and Public Keys
Basic Operations	Performs basic operations.	Device Master Key, Device Private Key, Extra Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, AES Wrapping Key, Device Public Key, Reset Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		AES Binary Update Key, AES Content Encryption Keys, Seed Values, Signers Public Keys, Cinema Equipment Public Keys, ICP Public Keys	Write
		External Private Key, External Public Key	Read/Write
Basic Settings	Performs some of the module's settings.	Device Master Key, Device Private Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		AES Binary Update Key, Dolby HMAC Key, Signers Public Keys	Read/Write
Suite Management	Provides suite management operations.	Device Master Key, Device Private Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key, External Private Key	Read
		AES Binary Update Key, AES Content Encryption Keys, Content Integrity Keys, Signers Public Keys	Read/Write

7.3 SAS User Services in FIPS Approved Mode

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

Table 7-3 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 7-2 for the SMS User are also available for the SAS User.			
Reset Board	Resets the module.	Device Master Key, Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, Reset Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		Device Private Key, Device Public Key, External Private Key, External Public Key, Extra Private Key, Extra Public Key, Content Integrity Keys, Seed Values, AES Content Encryption Keys, AES Binary Update Key, Signers Public Keys, ICP Public Keys	Write

7.4 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 7-4 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 7-3** for the SAS User are also available for the SOS (Crypto-Officer) User.			
SOS Configuration	Performs specific SOS (Crypto-Officer) User configuration operations.	Device Master Key, Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, AES Wrapping Key, Device Public Key, Reset Public Key, SOS (Crypto-Officer) User Public Key	Read
		Device Private Key, Device Public Key, External Private Key, External Public Key, Extra Private Key, Extra Public Key, SMS User Public Key	Read/Write
Zeroization	Zeroizes sensitive data (including all plain text CSPs)	Device Master Key, Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, Reset Public Key, SOS (Crypto-Officer) User Public Key	Read
		All plaintext CSPs, Device Public Key, External Public Key, Extra Public Key, SMS User Public Key, Signers Public Keys, ICP Public Keys	Write

7.5 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 7-5 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
Setup	Performs non-security relevant setup operations	None	None
Video Settings	Performs video related settings	None	None
Self-Test	The power recycling of the IMS-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 IMS-SM to be powered off and powered on	None	None

7.6 Non-approved Service

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

Service	Description
Network Configuration	Performs non-security relevant network related configuration operations

Note that the Network Configuration unauthenticated service is accessible to any operator 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 a 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 used only to set and retrieve non-security relevant items. Note that the Network Configuration 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.

7.7 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 IMS-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 IMS-SM-C1, IMS-SM-C2, IMS-SM-E1, IMS-SM-E2, IMS2-SM-C1, IMS2-SM-C2 and IMS2-SM-C3.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.

The cryptographic boundary is the outer perimeter of the module's 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, 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 + 1-866-484-4004 or email doremisupport@dolby.com.

Operational Environment

The IMS-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 IMS-SM.

Self Tests

The IMS-SM module performs the following self tests:

- Power Up Self Tests
  - Firmware Integrity Test (32 bits CRC)
  - AES Encryption Known Answer Test
  - AES Decryption Known Answer Test
  - HMAC-SHA-1 Known Answer Test
  - SHA-1 Known Answer Test
  - RSA Digital Signature Generation Known Answer Test (RSA 2048 SHA-256)
  - RSA Digital Signature Verification Known Answer Test (RSA 2048 SHA-256)
  - ANSI X9.31 RNG Known Answer Test
  - FIPS186-2 RNG Known Answer Test
  - Critical Functions Tests:
    - CRC 32-bit Known Answer Test
    - RSA Encryption/Decryption Pair-wise Consistency Test
- Conditional Tests
  - Continuous ANSI X9.31 RNG Test
  - Continuous FIPS 186-2 RNG Test
  - Continuous NDRNG Test
  - Firmware Load Test (HMAC-SHA-1)
  - Pair-wise Consistency Test (RSA Keys Generation: Digital Signature Generation/Verification; Encryption/Decryption)

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 IMS-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 ANSI X9.31 RNG, FIPS 186-2 RNG, and the NDRNG are tested using the conditional test specified in FIPS 140-2 §4.9.2.
11. The module supports concurrent operators.

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
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
PRF	Pseudo Random Function
RNG	Random Number Generator

Term	Definition
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	Version	Description
05/26/2015	Version 1	First version
06/02/2015	Version 2	Second version
07/10/2015	Version 3	Third version
11/16/2015	Version 4	Initial public release