CAT862 Dolby® JPEG 2000/MPEG-2 Media Block IDC Security Policy

Version 3 June 30, 2010

Dolby Laboratories Licensing Corporation

Corporate Headquarters

Dolby Laboratories, Inc.
Dolby Laboratories Licensing Corporation
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 Laboratories, Inc.
Wootton Bassett
Wiltshire SN4 8QJ England
Telephone (44) 1793-842100
Fax (44) 1793-842101

Asia

Dolby Laboratories International Services, Inc.
Japan Branch
NBF Higashi-Ginza Square 3F
13–14 Tsukiji 1-Chome, Chuo-ku
Tokyo 104-0045 Japan
Telephone (81) 3-3524-7300
Fax (81) 3-3524-7389
www.dolby.co.jp

Dolby Laboratories International Services, Inc.
Hong Kong Branch
RM5407 Central Plaza
18 Harbour Road
Wanchai, Hong Kong
Telephone (852) 2519-0888
Fax (852) 2519-8988

Dolby Laboratories International Services Co., Ltd.
03–07a, Floor 18
The Center
989 ChangLe Road
Shanghai 200031 China
Telephone (86) 21-6113-3456
Fax (86) 21-6113-3400
www.dolby.com.cn

S10/22048/22963
Version 3

Contents

1 Module Overview

The CAT862 Dolby® JPEG 2000/MPEG-2 Media Block IDC is a multi-chip embedded cryptographic module partially encased in a hard opaque commercial grade metal case. The primary purpose of the module is to decrypt, decode, and encode audio/video data for a digital cinema player. The cryptographic boundary is defined as being the perimeter of the printed circuit board. The components and areas of the printed circuit board not covered by the metallic case are excluded from the requirements of FIPS 140-2, because they are non-security relevant.

This document refers specifically to the CAT862 Dolby JPEG 2000/MPEG-2 Media Block IDC hardware P/N CAT862Z revision FIPS_1.0, FIPS_1.1, and FIPS_1.2 running firmware version 4.1.4_FIPS.

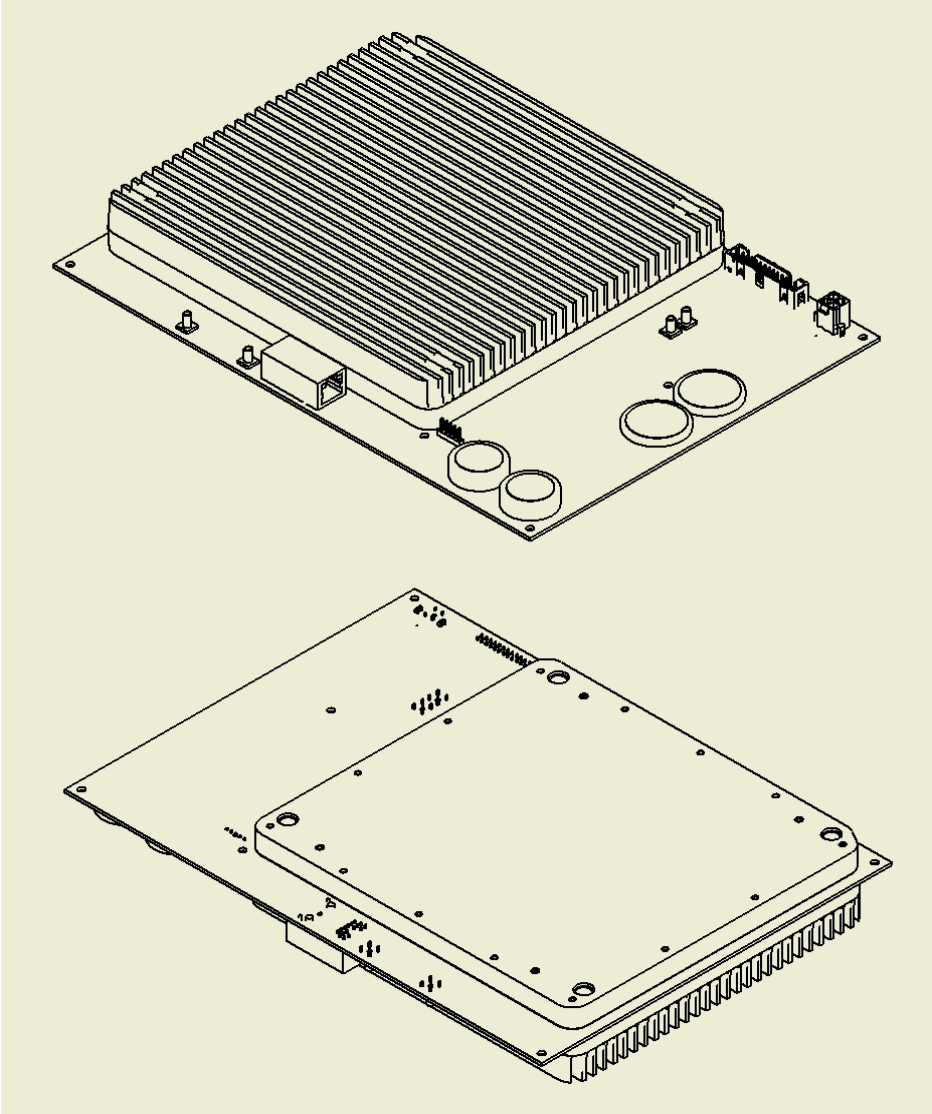

Figure 1 Image of the Cryptographic Module

2 Acronyms and Definitions

Table 1 shows acronyms used in this document and their definitions.

Table 1 Acronyms and Definitions

Acronym	Definition
CPL	Composition Play List
HD-SDI	High Definition Serial Digital Interface, as defined by the SMPTE 292M standard
JPEG	Joint Photographic Experts Group
KDM	Key Delivery Message
LED	Light-Emitting Diode
LTC	Linear Time Code
MPEG	Moving Picture Experts Group
SMPTE	Society of Motion Picture and Television Engineers
TMS	Theatre Management System

3 Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2. Table 2 shows the specific requirements sections and associated security level.

Table 2 Module Security Level Specification

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

4 Modes of Operation

The cryptographic module only supports an Approved mode of operation. The Approved mode of operation can be confirmed by verifying that the firmware version matches the Approved, tested version. The firmware version number can be retrieved using the Get Status service.

When the cryptographic module is installed in a Dolby Digital Cinema system, the Dolby TMS software "Decoder FIPS 140-2 Validated Mode" device property indicates **true** when the module is in the Approved mode of operation. If the "Decoder FIPS 140-2 Validated Mode" device property indicates **false**, the module is not in the Approved mode and will not function. This device property can be found within the TMS software interface under the **system** mode on the **theatre devices** tab.

The following Approved algorithms are supported:

- AES 128-bit – certificates #519, #520, #1067
- AES 256-bit – certificate #520
- SHA-1 – certificates #592, #1086
- SHA-256 – certificate #592
- RSA 2048 Key Gen and Sign/Verify – certificate #233
- HMAC-SHA-1 – certificates #270, #676
- HMAC-SHA-256 – certificate #270
- FIPS 186 GP RNG – certificate #650
- ANSI X9.31 RNG – certificate #296

The cryptographic module supports TLS v1.0 with AES, as well as the following non-FIPS-approved algorithms:

- MD5 within TLS
- RSA 2048 Encrypt/Decrypt for Key Transport (key wrapping; key establishment methodology provides 112 bits of encryption strength)

5 Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

Table 3 Module Port and Interface Specification

Port	Interface
1000BASE-T Ethernet port	Data Input, Data Output, Control Input, Status Output
USB port	Data Input, Control Input, Status Output
HD-SDI ports (Qty: 2)	Data Output
Audio port	Data Output
LTC port	Status Output
Vref port	Status Output, Control Input

Port	Interface
Status LEDs (Qty: 4)	Status Output
RS232 ports (Qty: 2)	Status Output
ATX 2x2 port	Power Input
Reset ports (Qty: 3)	Control Input

6 Identification and Authentication Policy

Assumption of Roles

The cryptographic module shall support two distinct operator roles: User and Cryptographic Officer. The Cryptographic Officer is assumed by Dolby Laboratories and the User is assumed by the Show Store. The cryptographic module shall enforce the separation of roles using identity-based operator authentication by means of digital signatures.

Table 4 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Digital Signature Verification using Show Store Root Public Key
Cryptographic Officer	Identity-based operator authentication	Digital Signature Verification using Dolby Maintenance Public Key

Table 5 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
RSA 2048-bit Digital Signature verification	The probability that a random attempt will succeed or a false acceptance will occur is $1/2^{112}$ which is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute through random attempts is $200/2^{112}$ (due to timing limitations in the module) which is less than 1/100,000.

7 Access Control Policy

Roles and Services

Table 6 Services Authorized for Roles

Role	Authorized Services
User: Assumed by the Show Store	Execute Key Delivery Message (KDM): Execute KDM, which includes the loading of an RSA wrapped Content Key. Start Suite: Initializes the playback suite. Prep Suite: Prepares the playback suite for playback of content Stop Suite: Terminates the playback suite. Purge Suite: Purges the playback suite and begins projector log extraction. CPL Validate: Validates a content play list. Playback: Control the playback of content (e.g., Play, Stop, Clear, Mute, Repeat, Step, etc.). Set Time: Sets or adjusts the current time of the cryptographic module with restrictions. Get Time Status: Retrieves the current time and adjustment settings. Check License: Verifies the playback license exists and is valid. Clear Licenses: Clears all licenses. Delete License: Deletes a single license. Get Usage Rights: Retrieves usage rights. Get All Content IDs: Retrieves all content IDs. Get Number of Keys: Retrieves the total number of keys present in a KDM. Get Audit Logs: Retrieves audit logs. ASM Send: Sends an Auditorium Security Message (ASM) to the projector. Decrypt Subtitle: Decrypts a subtitle file using a Content Key obtained from a KDM.
Cryptographic Officer: Assumed by Dolby Laboratories	Firmware Upgrade: Updates the firmware of the module. Zeroize: This service actively destroys all plaintext critical security parameters.

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Self-tests: This service executes the suite of self-tests required by FIPS 140-2 and is invoked by power cycling or resetting the device.
- Get Status: This service provides module status via LEDs, the RS-232 port, USB port, and the Ethernet port.
- Get Time: Retrieves the current time from the cryptographic module.
- Get Public Key Hash: Retrieves the pre-computed hash of the System Public Key.
- Set Configuration: This service sets audio and video parameters (e.g., video format, output enable, AV mute, 3D coefficients, etc.).

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- System Private Key: Used to perform TLS authentication, the key transport of Content Keys, and to sign audit logs.
- Key Encryption Key: Used to AES encrypt the System Private Key, Data Encryption Key, HMAC Key, and Content Keys that are stored locally. The Key Encryption Key is used automatically at system boot time to decrypt the System Private Key, Data Encryption Key and HMAC Key.
- Data Encryption Key: Used to AES encrypt RNG State and firmware images that are to be stored locally.
- HMAC Key: Used as an HMAC key for authenticating storage of certificates, time adjustment parameters, and the file system.
- Content Keys: Used to AES decrypt content received from the Show Store.
- Content Integrity Keys: Used as an HMAC key for verifying content integrity.
- CineLink™ Keys: AES keys used in the CineLink processor.
- RNG State: The current ANSI X9.31 DRNG state.
- FIPS 186-2 RNG State: The current FIPS 186-2 GP DRNG state.
- TLS Session Parameters Used in Support of TLS Session Establishment:
  - TLS Random Number
  - TLS PreMaster Secret
  - TLS Master Secret
- TLS Encryption Keys: TLS AES session keys used during TLS sessions.
- TLS HMAC Keys – TLS HMAC keys used during initial TLS handshake.
- Firmware Image Decryption Key – Used to AES decrypt firmware images during firmware upgrade.

Definition of Public Keys

The following are the public keys contained in the module:

- System public Key: Used to perform the key transport of Content Keys.

- Show Store Public Key: Used to support TLS operations.
- Show Store Root Public Key: Used to verify Show Store certificates.
- Root Public Key: Used to verify a certificate chain of trust.
- Dolby Maintenance Public Key: Used to verify the digital signature over the firmware image to be loaded.
- X.509 Certificates – Used when verifying a chain of trust.

Definition of CSPs Modes of Access

Table 7 defines the relationship between access to CSPs and the different module services. The modes of access shown in the tables are defined as follows:

- Generate: The CSP is generated.
- Use: The CSP is used.
- Import: The CSP is entered into the module.
- Export: The CSP is output from the module.
- Wrap: The CSP is RSA wrapped.
- Unwrap: The CS is RSA unwrapped.
- Destroy: The CSP is actively destroyed within the module.

Table 7 CSP Access Rights within Roles and Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
	X	Execute KDM	*Import & Unwrap* Content Key. *Use* System Private Key, Key Encryption Key, Data Encryption Key, HMAC Key, TLS Keys (i.e., TLS Session Parameters, TLS Encryption Key, TLS HMAC Key), RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Start Suite	*Use* TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Prep Suite	*Generate* CineLink Key. *Use* HMAC Key, TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates. *Output* CineLink Key.
	X	Stop suite	*Use* TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Purge Suite	*Use* TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
	X	CPL Validate	*Use* HMAC Key, TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Playback	*Generate* Content Integrity Key. *Use* Content Key, Key Encryption Key, HMAC Key, Content Integrity Key, CineLink Key, FIPS 186-2 RNG State. *Output* CineLink Key.
	X	Set time	*Use* TLS Keys, Data Encryption Key, RNG State, HMAC Key. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Get Time Status	*Use* HMAC Key, TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Check License	*Use* TLS Keys, Data Encryption Key, RNG State, HMAC Key. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Clear Licenses	*Use* HMAC Key, TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Delete License	*Use* HMAC Key, TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Get Usage Rights	*Use* TLS Keys, Data Encryption Key, RNG State, HMAC Key. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Get All Content IDs	*Use* TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Get Number of Keys	*Use* TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	Get Audit Logs	*Use* System Private Key, TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
	X	ASM Send	*Use* TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
	X	Decrypt Subtitle	*Use* Content Key, Key Encryption Key, TLS Keys, Data Encryption Key, RNG State. *Use* Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.
X		Firmware Upgrade	*Import & Unwrap* Firmware Image Decryption Key. *Use* Key Encryption Key, Firmware Image Decryption Key, Data Encryption Key. *Use* Root Public Key, Dolby Maintenance Public Key, X.509 Certificates.
X		Zeroize	*Import & Unwrap* Firmware Image Decryption Key. *Use* Firmware Image Decryption Key. *Use* Root Public Key, Dolby Maintenance Public Key, X.509 Certificates. *Destroy* all plaintext CSPs.
		Self-tests	None
		Get Status	None
		Get Time	None
		Get Public Key Hash	None
		Set Configuration	None

8 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module supports a limited operational environment; only validated and trusted software can be loaded by means of a 2048-bit RSA digital signature.

9 Security Rules

The cryptographic module design corresponds to the module security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

- The cryptographic module shall provide two distinct operator roles. These are the User role and the Cryptographic-Officer role.
- The cryptographic module shall provide identity-based authentication.
- The cryptographic module shall not support a maintenance interface.
- The cryptographic module shall perform the following tests for each implemented cryptographic algorithm:

Power-up Self Tests

1) Cryptographic algorithm tests:
    a. AES 128-bit Encrypt/Decrypt KAT, 3 implementations – certificates #519, #520, #1067
    b. AES 256-bit Encrypt/Decrypt KAT – certificate #520
    c. RSA 2048-bit Sign/Verify KAT – certificate #233
    d. RSA 2048-bit Encrypt/Decrypt KAT
    e. HMAC SHA-1 KAT, 2 implementations – certificates #270, #676
    f. HMAC SHA-256 KAT – certificate #270
    g. SHA-1 KAT (Tested as a part of HMAC), 2 implementations – certificates #592, #1086
    h. SHA-256 KAT (Tested as a part of HMAC) – certificate #592
    i. RNG KATs – certificates #296, #650
2) Firmware Integrity Test (CRC-32)
3) Critical Functions Tests
    a. RAM Write/Read Test

Conditional Self-Tests

1) Continuous Random Number Generator (RNG) test - performed on ANSI X9.31 RNG and FIPS 186-2 GP RNG
2) Firmware Load Test (RSA Digital Signature Verification)

- The operator shall be capable of invoking power-up self-tests by power cycling or resetting the module.
- Data output shall be inhibited during self-tests, zeroization, and error states.
- Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
- The module shall not support multiple concurrent operators.
- When the cryptographic module is powered off and subsequently powered on, the results of previous authentications shall not be retained and the module shall require the operator to be re-authenticated.

10 Physical Security Policy

Physical Security Mechanisms

The CAT862 Dolby JPEG 2000/MPEG-2 Media Block IDC includes the following physical security mechanisms:

- Production-grade components and production-grade opaque metal enclosure.
- Metal enclosure with automatic zeroization when enclosure is opened via tamper detection and zeroization circuitry.
- Enclosure cover screws are protected with tamper-evident expansion plugs.

11 Mitigation of Other Attacks Policy

The module has not been designed to mitigate specific attacks beyond the scope of FIPS 140-2 requirements.