CAT904 Dolby® JPEG2000/MPEG2 Processor Security Policy

Document Version 1.2 September 19, 2008

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 Headquarters

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

Document Version 1.2
S07/17900

Table of Contents

1 Module Overview

The CAT904 Dolby® JPEG2000/MPEG2 Processor 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 CAT904 Dolby® JPEG2000/MPEG2 Processor hardware P/N CAT904Z revisions FIPS_1.0, FIPS_1.0.1, FIPS_1.0.2 and FIPS_1.1 running firmware version 3.1.0.1.

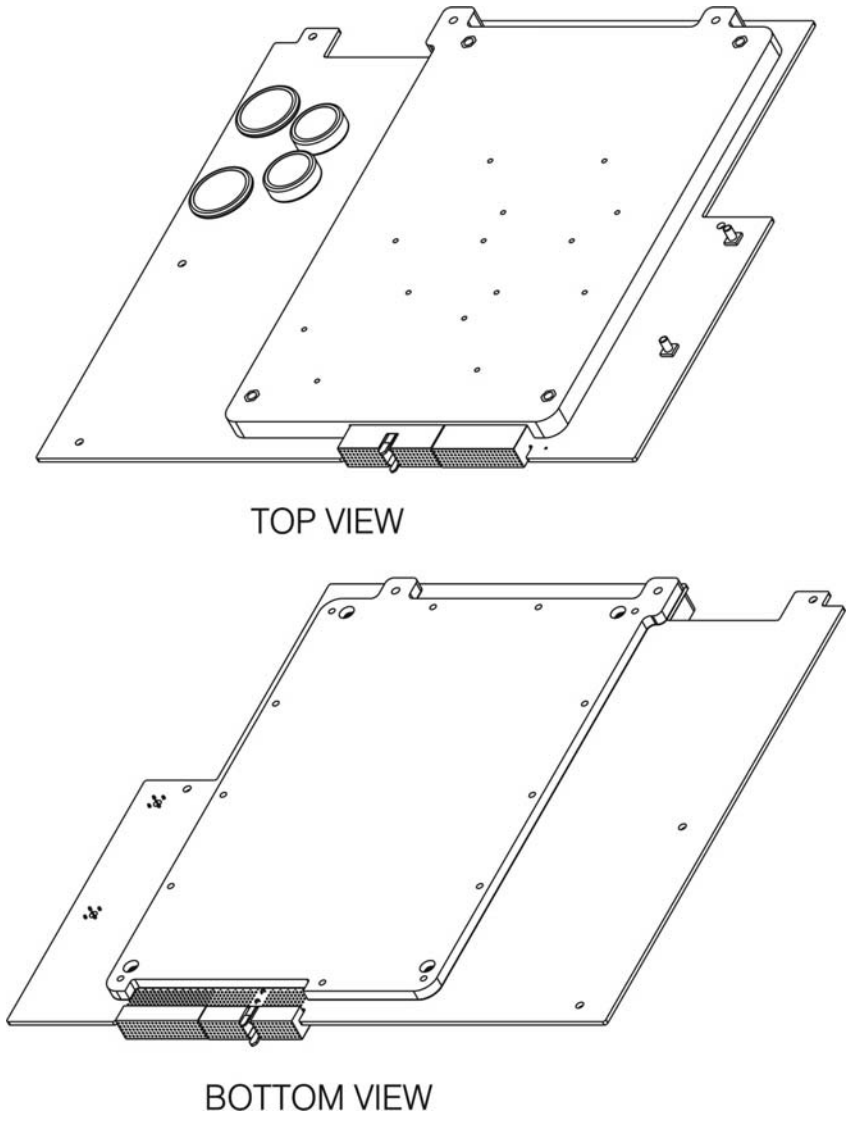

Figure 1 Image of the Cryptographic Module

2 Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 1 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

3 Modes of Operation

The cryptographic module only supports an Approved mode of operation. The Approved mode of operation can be confirmed by verifying the FW version matches the Approved, tested version. The following Approved algorithms are supported:

- AES 128-bit
- AES 256-bit
- SHA-1
- SHA-256
- RSA 2048 Sign/Verify
- HMAC-SHA-1
- HMAC-SHA-256
- ANSI X9.31 DRNG

The cryptographic module supports 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)
- TLS for key establishment (key wrapping; key establishment methodology provides 112 bits of encryption strength)

4 Ports and Interfaces

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

Compact PCI/220-pin interface:	Data Input, Data Output, Control Input, Status Output, Power Input
HD-SDI ports (Qty. 2):	Data Output
Status LEDs (Qty. 13):	Status Output
RS-232	Status Output

5 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 2 Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Digital Signature Verification
Cryptographic-Officer	Identity-based operator authentication	Digital Signature Verification

Table 3 Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Digital Signature with 2048-bit RSA private key	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 is $200/2^{112}$ (due to timing limitations in the module) which is less than 1/100,000.

6 Access Control Policy

Roles and Services

Table 4 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. Playback: Control the playback of content (e.g., Play, Stop, Clear, Mute, Repeat, Step, etc.). Set Time: Sets the current time of the cryptographic module with restrictions. Check License: Verifies the playback license exists and is valid. Clear License: Clears all licenses. 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.
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, and the compact PCI interface.
- Get Time: Retrieves the current time from the cryptographic module.
- Get Public Key Hash: Retrieves the pre-computed hash of the System Public Key.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

1. System Private Key – Used to perform TLS authentication and the key transport of Content Keys.
2. 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.
3. Data Encryption Key – Used to AES encrypt RNG State and firmware images that are to be stored locally.
4. HMAC Key – Used as an HMAC key for authenticating storage of certificates, time adjustment parameters, and the file system.
5. Content Keys – Used to AES decrypt content received from the Show Store.
6. RNG State – The current DRNG state.
7. TLS Encryption Keys – TLS AES session keys used during TLS sessions.
8. TLS HMAC Keys – TLS HMAC keys used during initial TLS handshake.
9. 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:

1. System Public Key – Used to perform the key transport of Content Keys.
2. Show Store Public Key – Used to support TLS operations.
3. Root Public Key – Used to verify a certificate chain of trust.
4. Dolby Maintenance Public Key – Used to verify the digital signature over the firmware image to be loaded.
5. X.509 Certificates – Used when verifying a chain of trust.

Definition of CSPs Modes of Access

Tables 5a and 5b define 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 CSP is RSA unwrapped

Destroy: The CSP is actively destroyed within the module

Table 5a CSP Access Rights within Roles & 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, HMAC Key, TLS Keys (i.e., TLS Encryption Key, TLS HMAC Key), RNG State *Use* Root Public Key, Show Store Public Key, X.509 Certificates
	X	Playback	*Use* Content Key, Key Encryption Key, HMAC Key
	X	Set Time	*Use* TLS Keys, RNG State, HMAC Key *Use* Root Public Key, Show Store Public Key, X.509 Certificates
	X	Check License	*Use* TLS Keys, RNG State, HMAC Key *Use* Root Public Key, Show Store Public Key, X.509 Certificates
	X	Clear License	*Use* TLS Keys, RNG State *Use* Root Public Key, Show Store Public Key, X.509 Certificates
	X	Get Usage Rights	*Use* TLS Keys, RNG State, HMAC Key *Use* Root Public Key, Show Store Public Key, X.509 Certificates
	X	Get All Content IDs	*Use* TLS Keys, RNG State *Use* Root Public Key, Show Store Public Key, X.509 Certificates
	X	Get Number of Keys	*Use* TLS Keys, RNG State *Use* Root Public Key, Show Store Public Key, X.509 Certificates
X		Firmware Upgrade	*Use* Key Encryption Key, Firmware Image Decryption Key, Data Encryption Key *Use* Root Public Key, Dolby Maintenance Public Key, X.509 Certificates
X		Zeroize	*Use* Firmware Image Decryption Key *Use* Root Public Key, Dolby Maintenance Public Key, X.509 Certificates *Destroy* all plaintext CSPs.

Table 5b CSP Access Rights within Roles & Services

Role		Service	Cryptographic Keys and CSPs Access Operation
C.O.	User		
		Self-tests	None
		Get Status	None
		Get Time	None
		Get Public Key Hash	None

7 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.

8 Security Rules

The cryptographic module's design corresponds to the module's 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.

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

   A. Power-up Self-Tests:

      1. Cryptographic algorithm tests:
         a. AES 128-bit Decrypt KAT
         b. AES 256-bit Encrypt/Decrypt KAT
         c. RSA 2048-bit Sign/Verify KAT
         d. RSA 2048-bit Encrypt/Decrypt KAT
         e. HMAC SHA-1 KAT
         f. HMAC SHA-256 KAT

g. SHA-1 KAT (Tested as a part of HMAC)

h. SHA-256 KAT (Tested as a part of HMAC)

i. DRNG KAT

2. Firmware Integrity Test (CRC-32)

3. Critical Functions Tests

a. RAM Write/Read Test

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on DRNG

2. Firmware Load Test (RSA Digital Signature Verification)

5. The operator shall be capable of invoking power-up self-tests by power cycling or resetting the module.
6. Data output shall be inhibited during self-tests, zeroization, and error states.
7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. The module shall not support multiple concurrent operators.
9. 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.

9 Physical Security Policy

Physical Security Mechanisms

The CAT904 Dolby JPEG2000/MPEG2 Processor 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.

10 Mitigation of Other Attacks Policy

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

Table 6 Mitigation of Other Attacks

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

11 Definitions and Acronyms

JPEG	Joint Photographic Experts Group
MPEG	Moving Picture Experts Group
SMPTE	Society of Motion Picture and Television Engineers
PC	Printed Circuit
HD-SDI	High Definition Serial Digital Interface, as defined by the SMPTE 292M standard
PCI	Peripheral Component Interconnect
LED	Light-Emitting Diode
KDM	Key Delivery Message