Contents

1 Module Overview ............................................................................................................. 1
2 Acronyms and Definitions ............................................................................................... 2
3 Security Level .................................................................................................................. 2
4 Modes of Operation ......................................................................................................... 3
5 Ports and Interfaces ........................................................................................................ 3
6 Identification and Authentication Policy ........................................................................ 4
7 Access Control Policy ..................................................................................................... 5
8 Operational Environment ............................................................................................... 9
9 Security Rules .................................................................................................................. 9
10 Physical Security Policy ............................................................................................... 11
11 Mitigation of Other Attacks Policy ............................................................................... 11
1 Module Overview

The CAT904 Dolby® JPEG 2000/MPEG-2 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 JPEG 2000/MPEG-2 Processor hardware P/N CAT904Z revision FIPS_1.0, FIPS_1.0.1, FIPS_1.0.2 and FIPS_1.1 running firmware version 1.3.4.21.

Figure 1 Image of the Cryptographic Module
2 Acronyms and Definitions

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

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

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

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)
- SP 800-135rev1 TLS KDF for key establishment (not CAVP tested)

5 Ports and Interfaces

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

<table>
<thead>
<tr>
<th>Port</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compact PCI/220-pin interface</td>
<td>Data Input, Data Output, Control Input, Status Output, Power Input</td>
</tr>
<tr>
<td>Board Reset (Jumper 15)</td>
<td>Control Input</td>
</tr>
<tr>
<td>HD-SDI ports (Qty: 2)</td>
<td>Data Output</td>
</tr>
<tr>
<td>Status LEDs (Qty: 13)</td>
<td>Status Output</td>
</tr>
<tr>
<td>RS232 ports (Qty: 1)</td>
<td>Status Output</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Role</th>
<th>Type of Authentication</th>
<th>Authentication Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Identity-based operator authentication</td>
<td>Digital Signature Verification using Show Store Root Public Key</td>
</tr>
<tr>
<td>Cryptographic Officer</td>
<td>Identity-based operator authentication</td>
<td>Digital Signature Verification using Dolby Maintenance Public Key</td>
</tr>
</tbody>
</table>

Table 5 Strengths of Authentication Mechanisms

<table>
<thead>
<tr>
<th>Authentication Mechanism</th>
<th>Strength of Mechanism</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA 2048-bit Digital Signature verification</td>
<td>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 $1/100,000$.</td>
</tr>
</tbody>
</table>
# Access Control Policy

## Roles and Services

### Table 6 Services Authorized for Roles

<table>
<thead>
<tr>
<th>Role</th>
<th>Authorized Services</th>
</tr>
</thead>
</table>
| 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.  
                                | Get ShowPlayer Certificate: Retrieves the Media Block certificate chain.             
                                | Get Projector Certificate and Thumbprint: Retrieves the Projector certificate chain and certificate thumbprint. |
| Cryptographic Officer: Assumed by Dolby Laboratories | Firmware Upgrade: Updates the firmware of the module.                             
                                | Zeroize: This service actively destroys all plain text 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 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.
- **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**: Authenticates 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 to verify content integrity.
- **Cinelink™ Keys**: AES keys used in the CineLink processor.
- **RNG State**: The ANSI X9.31 seed and seed key.
- **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 CSP is RSA unwrapped.
- **Destroy**: The CSP is actively destroyed within the module.

#### Table 7 CSP Access Rights within Roles and Services

<table>
<thead>
<tr>
<th>Role</th>
<th>Service</th>
<th>Cryptographic Keys and CSPs Access Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>C.O.</td>
<td>User</td>
<td></td>
</tr>
<tr>
<td>X</td>
<td>Execute KDM</td>
<td><em>Import &amp; Unwrap Content Key.</em>&lt;br&gt; <em>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.</em>&lt;br&gt; <em>Use Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.</em></td>
</tr>
<tr>
<td>X</td>
<td>Start Suite</td>
<td><em>Use TLS Keys, Data Encryption Key, RNG State.</em>&lt;br&gt; <em>Use Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.</em></td>
</tr>
<tr>
<td>X</td>
<td>Prep Suite</td>
<td><em>Generate CineLink Key.</em>&lt;br&gt; <em>Use HMAC Key, TLS Keys, Data Encryption Key, RNG State.</em>&lt;br&gt; <em>Use Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.</em>&lt;br&gt; <em>Export CineLink Key.</em></td>
</tr>
<tr>
<td>X</td>
<td>Stop suite</td>
<td><em>Use TLS Keys, Data Encryption Key, RNG State.</em>&lt;br&gt; <em>Use Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.</em></td>
</tr>
<tr>
<td>X</td>
<td>Purge Suite</td>
<td><em>Use TLS Keys, Data Encryption Key, RNG State.</em>&lt;br&gt; <em>Use Root Public Key, Show Store Public Key, Show Store Root Public Key, X.509 Certificates.</em></td>
</tr>
<tr>
<td>Role</td>
<td>Service</td>
<td>Cryptographic Keys and CSPs Access Operation</td>
</tr>
<tr>
<td>------</td>
<td>--------------</td>
<td>---------------------------------------------</td>
</tr>
<tr>
<td>C.O.</td>
<td>User</td>
<td></td>
</tr>
</tbody>
</table>
| 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.  
Export CineLink Key. |
| X    | Set time     | 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 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.  
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.  
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. |
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 provides two distinct operator roles. These are the User role and the Cryptographic-Officer role.
- The cryptographic module provides identity-based authentication.
- The cryptographic module does not support a maintenance interface.
- The cryptographic module performs the following tests for each implemented cryptographic algorithm:
Power-up Self Tests

1) Cryptographic algorithm tests:
   a. AES 128-bit Decrypt KAT – certificate #519
   b. AES 128-bit and 256-bit Encrypt KAT – certificate #520
   c. AES 128-bit and 256-bit Decrypt KAT – certificate #520
   d. AES 128-bit Encrypt KAT – certificate #1067
   e. RSA 2048-bit Sign KAT – certificate #233
   f. RSA 2048-bit Verify KAT – certificate #233
   g. RSA 2048-bit Encrypt KAT
   h. RSA 2048-bit Decrypt KAT
   i. HMAC SHA-1 KAT, 2 implementations – certificates #270, #676
   j. HMAC SHA-256 KAT – certificate #270
   k. SHA-1 KAT (Tested as a part of HMAC), 2 implementations – certificates #592, #1086
   l. SHA-256 KAT (Tested as a part of HMAC) – certificate #592
   m. 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 is capable of invoking power-up self-tests by power cycling or resetting the module.
   • Data output is inhibited during self-tests, zeroization, and error states.
   • Status information does not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
   • The module does not support multiple concurrent operators.
   • When the cryptographic module is powered off and subsequently powered on, the results of previous authentications is not retained and the module requires the operator to be re-authenticated.
   • The module uses the FIPS validated nShield module to generate randomness that is injected during manufacturing. Three 64-bit random values are provided during manufacturing to account for a maximum of 192-bits of uncertainty.
10 Physical Security Policy

Physical Security Mechanisms

The CAT904 Dolby JPEG 2000/MPEG-2 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.

11 Mitigation of Other Attacks Policy

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