Secure Media Block

Security Policy

Version 0.3

Qube Cinema, Inc.

September 21, 2011

TABLE OF CONTENTS

1. Module Overview

The Secure Media Block (Firmware Version 1.0.1.0; Hardware Versions: Z-OEM-DCI-Q-R0, Z-OEM-DCI-Q-R2, Z-OEM-DCI-Q-R3) is a multi-chip embedded cryptographic module encapsulated in a hard opaque potting material. The module has been designed to meet the requirements of both FIPS 140-2 Level 3, as well as Digital Cinema Initiative (DCI) requirements for a Secure Processing Block Type 1.

The Secure Media Block primarily provides services necessary for securing content essence from external storage servers to projection. The cryptographic boundary is defined as the perimeter of the PC board with components outside of the potting material excluded from the requirements of FIPS 140-2 as they are non-security relevant and cannot cause the security of the module to be compromised (see Figures 1 through 3). The excluded components are non-security relevant and can be described as follows:

- Power Supply (including the battery and all other power related components)
- Unconnected Components and Test Points
- Mechanical Connections
- Video and Audio Components

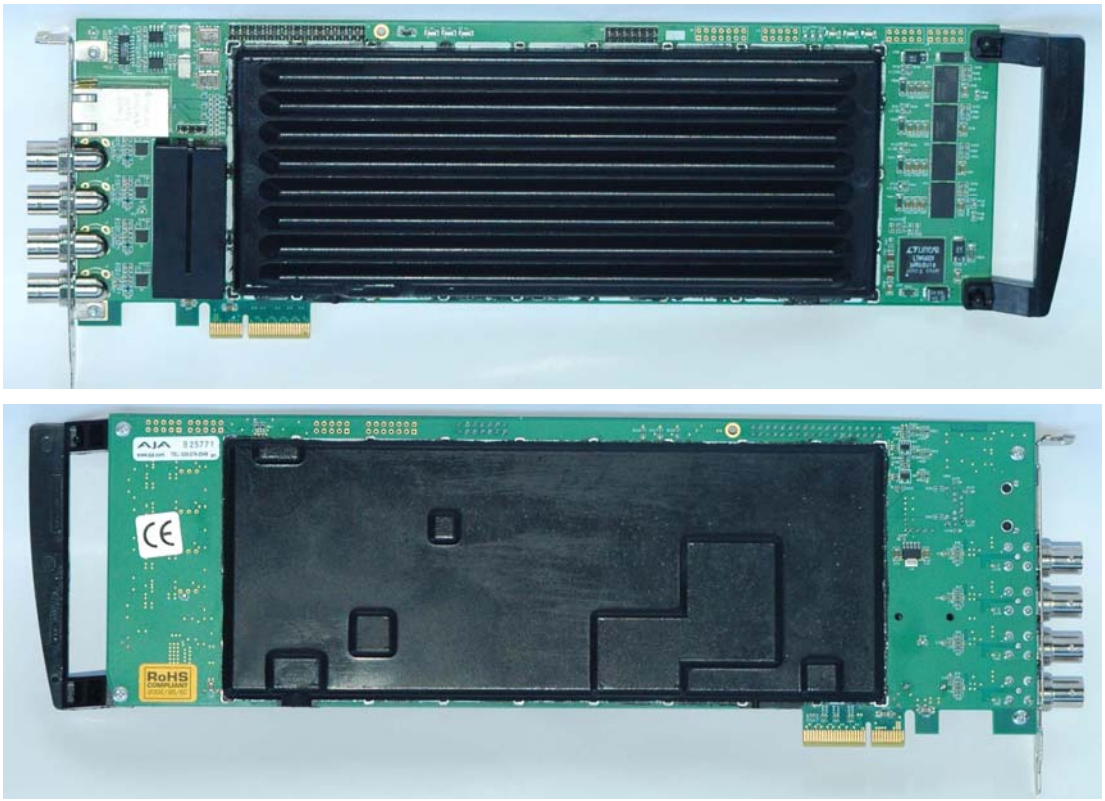

Figure 1 – Image of the Z-OEM-DCI-Q-R0 (Top & Bottom)

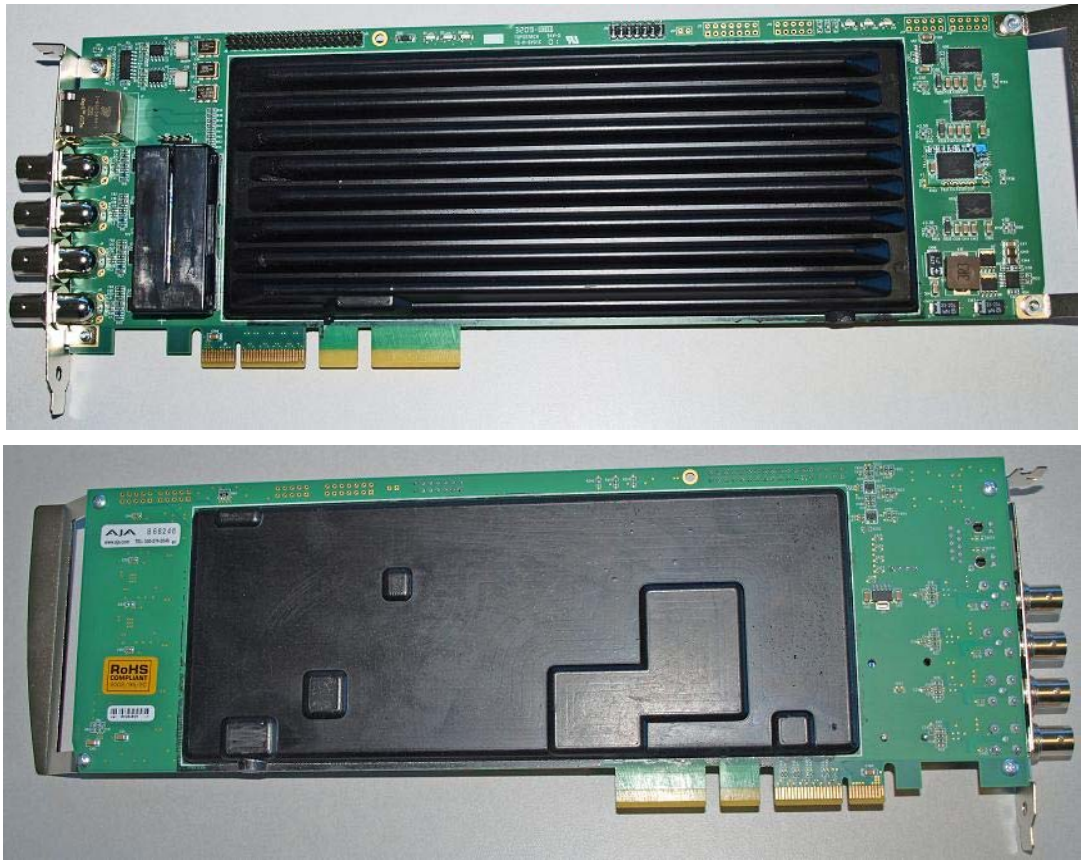

Figure 2 – Image of the Z-OEM-DCI-Q-R2 (Top & Bottom)

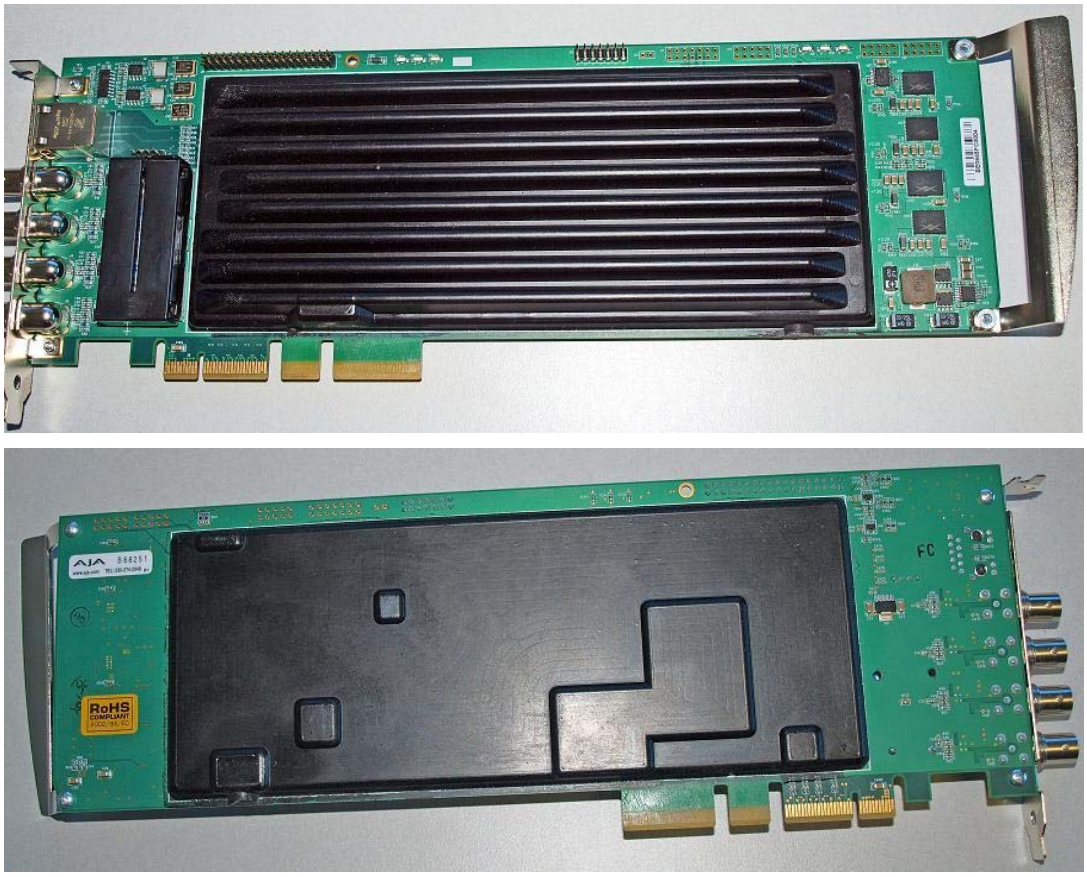

Figure 3 – Image of the Z-OEM-DCI-Q-R3 (Top & Bottom)

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 module only supports an Approved mode of operation and cannot be configured otherwise. The Approved mode can be verified by issuing the "Query Info" service, which will display the installed firmware version. The firmware version can then be verified to match the version listed on the validation certificate. The module supports the following Approved algorithms, which have been tested and validated:

- AES ECB and CBC, 128-bit keys (Cert. #812)
- AES ECB, CBC, OFB, CFB8, and CFB128 modes QubeCryptoLib (Cert. #1455)
- HMAC-SHA-1 (Cert. #450)
- HMAC SHA-1 QubeCryptoLib (Cert. #854)
- RNG ANSI X9.31 (Cert. #467)
- RNG ANSI X9.31 QubeCryptoLib (Cert. #797)
- SHA-1, SHA-256 QubeCryptoLib (Cert. #1318)
- SHA-1 (Certs. #809, #810, #811)
- RSA Sign/Verify ANSI X9.31, 2048-bit keys (Cert. #392)
- RSA Sign/Verify QubeCryptoLib, 1024, 2048, 3072, 4096-bit keys (Cert. #711)

The module supports the following non-Approved algorithms/functions:

- RSA for Key Transport Only (key wrapping; key establishment methodology provides 112 bits of encryption strength)
- Hardware NDRNG
- MD-5 within TLS
- CineLink II Processing

4. Ports and Interfaces

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

• Analog Reference Input (Qty. 1):	Control input
• Ethernet (Qty. 1):	Data input/output, Control input, Status output
• Ethernet LEDs (Qty. 5)	Status output
• Status LEDs (Qty. 3)	Status Output
• RS-232 (Qty. 1):	Status Output (COM)
• Reset Jumper (Qty. 1):	Control input
• HD-SDI Output (Qty. 4):	Data output
• AES-Audio (Qty. 8):	Data output
• PCI-E Card edge (Qty. 1):	Data input/output, Control input, Status output, Power input

5. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports two distinct operator roles (User and Cryptographic-Officer). The cryptographic module shall enforce the separation of roles using identity-based operator authentication. Upon power cycle, all authenticated states are cleared and operators must re-authenticate.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Screen Management System (User)	Identity-based operator authentication	Digital Signature Verification
Qube Cinema (Cryptographic-Officer)	Identity-based operator authentication	Digital Signature Verification

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Digital Signature Verification	The strength of a 2048-bit RSA key is known to be 112-bits. Therefore, the strength of a 2048-bit digital signature is 1/2^112, which is less than 1/1,000,000. The module can only perform 120 signature verifications per minute, due to performance and network constraints. Therefore, the probability that multiple attacks within a given minute will be successful is 120/2^112, which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
Screen Management System (User)	Get Time: Returns current date and time. Adjust Time: Adjusts the clock with the given time offset. Get Current Year Adjustments: Returns the sum of the clock adjustments performed in the current calendar year. Get Certificate: Returns the Security Manager's leaf certificate. Get Certificate Chain: Returns the Security Manager's certification chain and leaf certificate. Prep Suite: Establishes the TLS sessions between the module and remote SPBs, such as a projector. Purge Suite: Terminate TLS sessions with remote SPBs. Validate KDM: Checks the validity of a Key Delivery Message. Get Timed Text Key: Returns the content decryption keys for subtitles and captions. Validate CPL: Check the validity of a Composition Playlist. Get Show: Returns information about the currently loaded show. Prep Show: Instructs the Security Manager to prepare the loaded show for playback. Play Show: Instructs the Security Manager to initiate playback of the loaded show. Stop Show: Instructs the Security Manager to stop playback of a playing show. Purge Show: Instructs the Security Manager to purge all elements of the loaded show. Validate Certificate: Instructs the Security Manager to validate a Digital Cinema Certificate. Validate Certificate Chain: Instructs the Security Manager to validate a chain of Digital Cinema Certificates. Get Security Log Report: Returns a security log report for the date/time range provided. Query Info: Returns a collection of identification elements regarding the module, such as version information. ShutDown: Instructs the Security Manager to shut down.

Role	Authorized Services
Qube Cinema (Cryptographic Officer)	Start Firmware Upgrade: Initiate a firmware upgrade operation. Upload Firmware Bytes: Import a firmware chunk for an upgrade operation. Finish Firmware Upgrade: Complete the previously initiated firmware upgrade operation and validate the firmware signature. Zeroize: Destroy all plaintext CSPs contained within the module. Note: All services available to the User are also available to the CO.

Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

- Show status: Provides the current status of the module through the console output.
- Self-tests: Executes the suite of self-tests required by FIPS 140-2 and is invoked by power cycling the module.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Master Key: AES 128-bit encryption key used to protect persistently stored CSPs.
- Device Private Key: RSA 2048-bit private key that uniquely identifies the module to external entities and facilitates key wrap.
- TLS Encryption Keys: AES 128-bit encryption key that provides data confidentiality for TLS sessions.
- TLS Integrity Keys: HMAC SHA-1 keys that provide data integrity for TLS sessions.
- Content Encryption Keys: AES 128-bit encryption keys that provide data confidentiality for content received from an external entity.
- Content Integrity Keys: HMAC SHA-1 keys used to provide data integrity for the content received from external entities.
- CineLink II Key: Obfuscates data transmitted to the Projector
- RNG State: Internal state of the RNG that's used to generate random numbers.

Definition of Public Keys

The following are the public keys contained in the module:

- Device Public Key: RSA 2048-bit key used by external entities.
- Qube Verification Public Key: RSA 2048-bit key used to verify the digital signatures applied over firmware upgrade packages.
- Chain-of-Trust Verification Certificates: X.509 certificates used to verify the validity of certificates received from external entities.

- Projector Certificate: X.509 certificates used to identify the projector, as well as to assist in establishing the TLS session between the module and the projector.
- Issuer Certificates: X.509 certificates used to identify the issuer of KDMs, CPLs, and PKLs.
- SMS Certificate: X.509 certificate used to identify the SMS during the TLS handshake.
- CO Certificate: X.509 certificate used to identify the CO during the TLS handshake.

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Read: Access the value without modification.
- Write: Modify the value.
- Zeroize: Destroy the value by overwriting with zeroes.

Table 5 – CSP Access Rights within Roles & Services

C.O. Role	User Role	U/A*	Service	Cryptographic Keys and CSPs Access Operation
X	X		Get Time	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Adjust Time	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Get Current Year Adjustment	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Get Certificate	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Get Certificate Chain	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Prep Suite	Read, Write TLS Encryption Keys Read, Write TLS Integrity Keys Read, Write RNG State Read Device Private Key
X	X		Purge Suite	Zeroize TLS Encryption Keys Zeroize TLS Integrity Keys
X	X		Validate KDM	Read TLS Encryption Keys Read TLS Integrity Keys Read Device Private Key Write Content Encryption Keys Write Content Integrity Keys

C.O. Role	User Role	U/A*	Service	Cryptographic Keys and CSPs Access Operation
X	X		Get Timed Text Key	Read TLS Encryption Keys Read TLS Integrity Keys Read Content Encryption Keys Read Content Integrity Keys
X	X		Validate CPL	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Get Show	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Prep Show	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Play Show	Read TLS Encryption Keys Read TLS Integrity Keys Read Content Encryption Keys Read Content Integrity Keys Read, Write CineLink II Key
X	X		Stop Show	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Purge Show	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Validate Certificate	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Validate Certificate Chain	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Get Security Log Report	Read TLS Encryption Keys Read TLS Integrity Keys Read Device Private Key
X	X		Query Info	Read TLS Encryption Keys Read TLS Integrity Keys
X	X		Shutdown	Read TLS Encryption Keys Read TLS Integrity Keys
X			Start Firmware Upgrade	Read TLS Encryption Keys Read TLS Integrity Keys
X			Upload Firmware Bytes	Read TLS Encryption Keys Read TLS Integrity Keys
X			Finish Firmware Upgrade	Read TLS Encryption Keys Read TLS Integrity Keys
X			Zeroize	Read TLS Encryption Keys Read TLS Integrity Keys Zeroize All Plaintext CSPs

C.O. Role	User Role	U/A*	Service	Cryptographic Keys and CSPs Access Operation
		X	Show Status	N/A
		X	Self-Tests	N/A

*** U/A = Unauthenticated (no role required)**

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module contains a limited operational environment, which only allows for the loading of trusted firmware signed by Qube Cinema.

8. Security Rules

The cryptographic module's design corresponds to the cryptographic 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 module provides identity-based authentication.
2. The module will only provide access to cryptographic services if a valid role has been assumed.
3. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

      1. Cryptographic algorithm tests:
         a. AES Known Answer Tests
         b. RNG Known Answer Tests
         c. HMAC SHA-1 Known Answer Tests
         d. SHA-1, SHA-256 Known Answer Tests
         e. RSA Known Answer Tests
      2. Firmware Integrity Test (2048-bit RSA Signature Verification)
      3. Critical Functions Tests: N/A.

   B. Conditional Self-Tests:

      1. Continuous Random Number Generator Tests – performed on NDRNG and RNGs
      2. Firmware Load Test (RSA Signature Verification)

Note: Upon successful completion of power up self-tests, the module will become responsive to service requests. In addition, the module will output a status message to the console indicating that self-tests have passed successfully.

4. Data output shall be inhibited during self-tests and error states.

5. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. The module shall not support concurrent operators, maintenance operators/interfaces, manual key entry, or bypass capabilities.

9. Physical Security Policy

Physical Security Mechanisms

The Qube Secure Media Block is a multi-chip embedded cryptographic module, which includes the following physical security mechanisms:

- Production-grade components.
- Hard potting encapsulation with removal/penetration attempts rendering the module inoperable. No operating and storage temperature ranges had been specified, so the encapsulate hardness was only tested at ambient temperature and no assurance is provided at any other temperature.

Operator Required Actions

The operator is required to periodically inspect the exterior of the module.

Table 6 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Encapsulate	6 months	Ensure the module does not display any characteristics of an attempted breach.

10. Mitigation of Other Attacks Policy

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

11. Acronyms

AES	Advanced Encryption Standard
AES-Audio	Audio Engineering Society Audio
CPL	Composition Playlist
CSP	Critical Security Parameter
FIPS	Federal Information Processing Standard
HD-SDI	High Definition Serial Digital Interface
HMAC	Hash-based Message Authentication Code
JPEG	Joint Photographic Experts Group
KDM	Key Delivery Message
LED	Light-Emitting Diode
MD	Message Digest
MPEG	Moving Picture Experts Group
NDRNG	Non-deterministic Random Number Generator
PC	Printed Circuit
PCI	Peripheral Component Interconnect
PKL	Packaging List
RNG	Random Number Generator
RSA	Rivest Shamir Algorithm
SHA	Shamir Hashing Algorithm
SMPTE	Society of Motion Picture and Television Engineers
SPB	Secure Processing Block
TLS	Transport Layer Security

