JPG2K
Security Policy
Document Version 1.3

AJA Video Systems, Inc.

October 11, 2011

TABLE OF CONTENTS

1. Module Overview

The JPG2K (HW P/N 102387-00, 102387-02, and 102387-03; FW Version 1.0, 1.5, and 1.6) is a multi-chip embedded cryptographic module. The JPG2K is a JPEG-2000 decoder board designed to be an OEM solution compliant with the DCI specification for a Secure Processing Block Type-1 and the FIPS 140-2 requirements. The module's primary purpose is to secure content essence from a server to a projector; however, the module will require the installation of a Security Manager application, which is not included as part of this evaluation, to fully comply with DCI specifications. Note: The Security Manager application or any other application to be loaded on the JPG2K module is outside the scope of this validation. For the module running an application to be a FIPS validated module, it must successfully undergo revalidation testing.

The cryptographic boundary of the module is the entire board. The security relevant sub-region of the module is encased in a hard, opaque encapsulate (see Figures 1 and 2 below). The components not encapsulated within the epoxy are excluded from the requirements of FIPS 140-2 as they are non-security relevant and do not affect the overall security of the module.

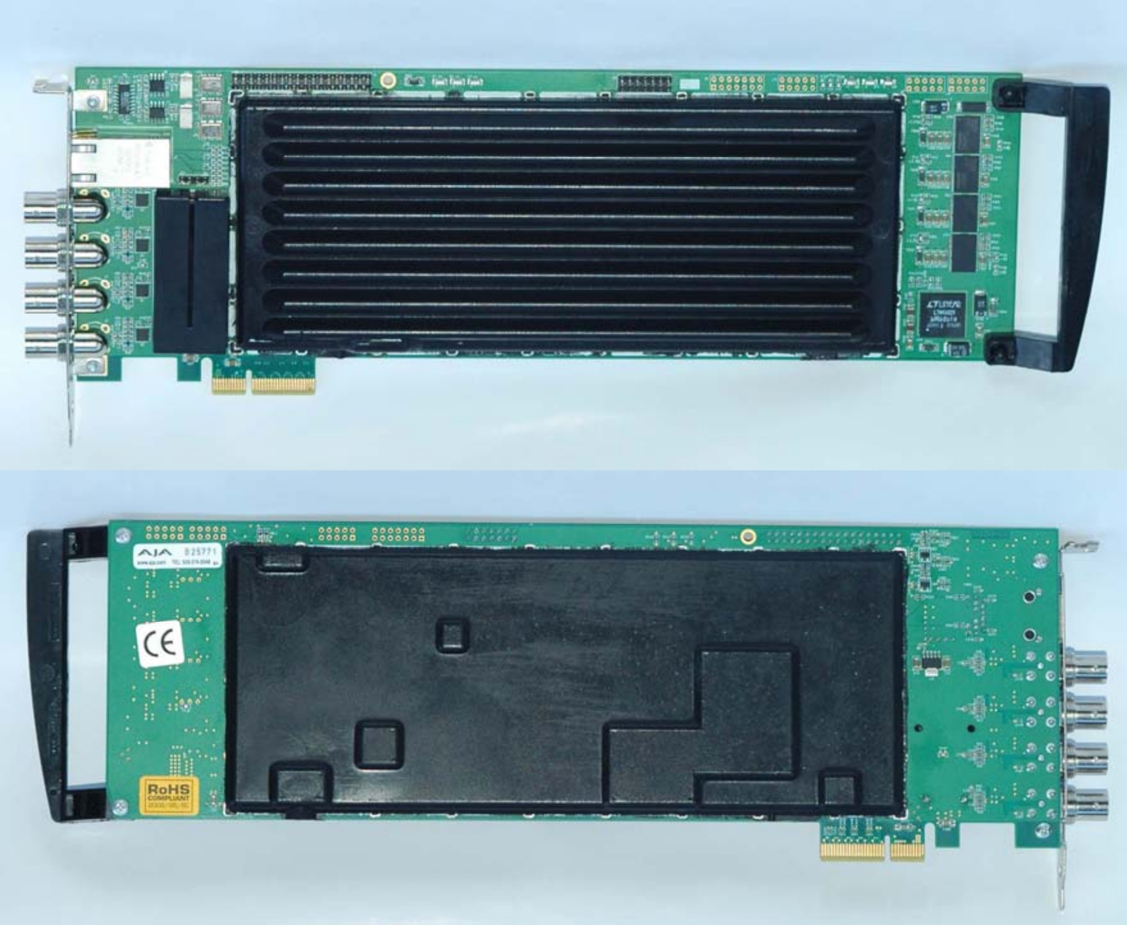

Figure 1 – Images of the 102387-00 (Top & Bottom)

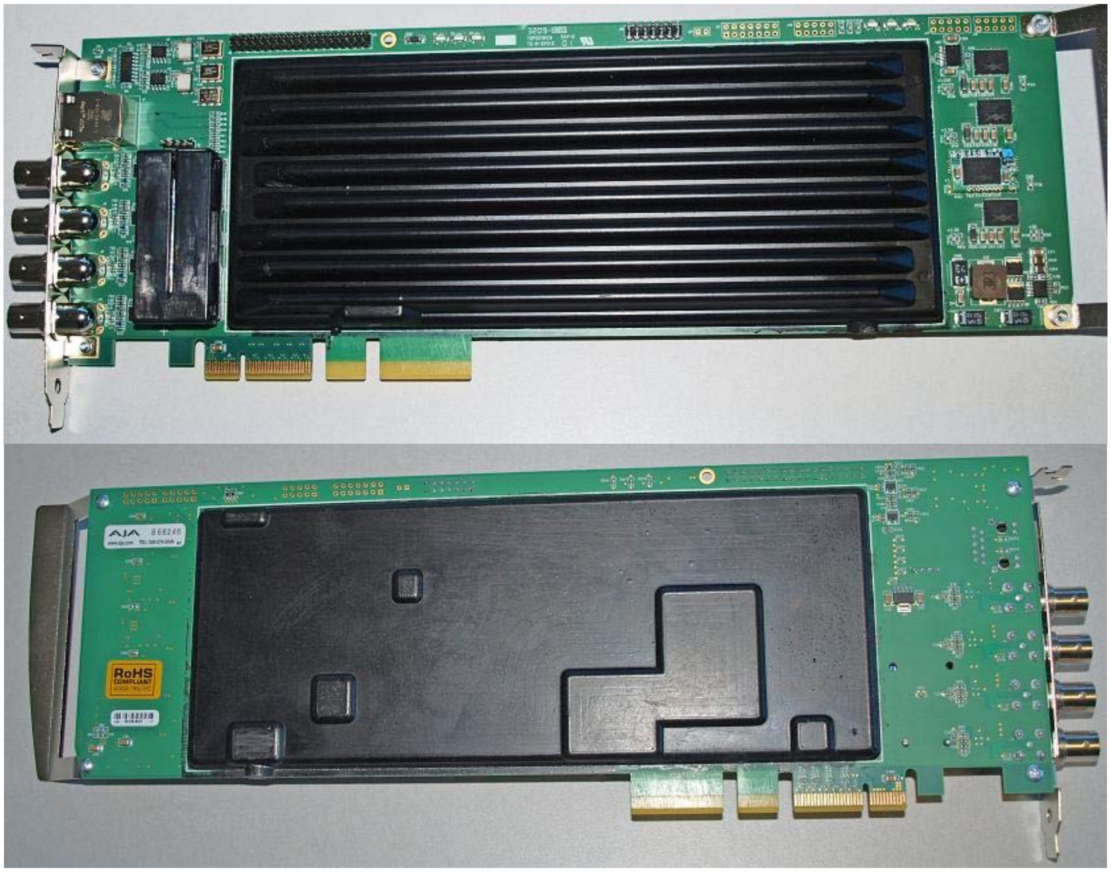

Figure 2 – Image of the 102387-02 (Top & Bottom)

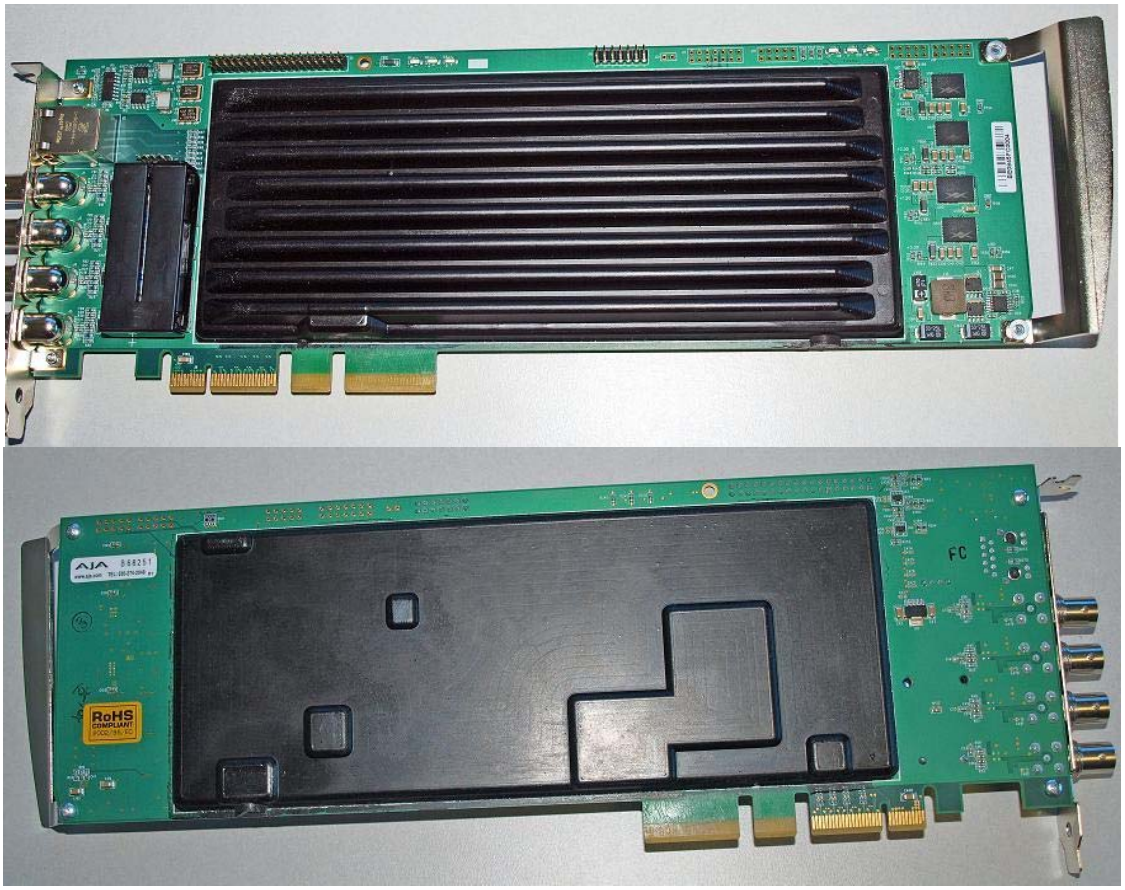

Figure 3 – Image of the 102387-03 (Top & Bottom)

2. Security Level

The cryptographic module meets the overall requirements applicable to Security Level 3 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

Approved mode of operation

The module only supports an Approved mode of operation. An operator can determine the Approved version of the firmware by verifying that the firmware version identified during power-up matches the validated version listed on the CMVP Validated FIPS 140-2 Cryptographic Modules website.

The following FIPS Approved algorithm is used by the module as configured for this validation (i.e., without a Security Manager installed):

- RSA Verify ANSI X9.31, 2048-bit keys (Cert. #392)

The module also supports the following latent algorithms, which are available for use after a Security Manager application is installed:

- Latent FIPS Approved algorithms:
  - RSA Sign ANSI X9.31, 2048-bit keys (Cert. #392)
  - AES ECB and CBC, 128-bit keys (Cert. #812)
  - HMAC-SHA-1 (Cert. #450)

  - DRNG ANSI X9.31 (Cert. #467)
  - SHA-1 FPGA (Cert. #809)
  - SHA-1 DS5250 (Cert. #810)
  - SHA-1 Power PC (Cert. #811)
- Latent non-FIPS Approved but allowed algorithms:
  - RSA Encrypt/Decrypt for Key Transport Only (key wrapping; key establishment methodology provides 112 bits of encryption strength)
  - HW NDRNG

4. Ports and Interfaces

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

• 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):	Control Input
• Reset Jumper (Qty. 1):	Control input
• PCI-E Card edge (Qty. 1):	Data input/output, Control input, Status output, Power input

The following ports are physically available, but are only used when a Security Manager application is installed:

• Analog Reference Input (Qty. 1):	Control input
• HD-SDI Output (Qty. 4):	Data output
• AES-Audio (Qty. 8):	Data output

5. Identification and Authentication Policy

Assumption of roles

The JPG2K cryptographic module only supports a single operator, who assumes both the User and Cryptographic-Officer roles.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
Cryptographic-Officer/User	Identity-based operator authentication via the Firmware Load service (see Table 4)	2048-bit Digital Signature

Table 3 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Digital Signature	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 four firmware signature verifications per minute, due to timing constraints. Therefore, the probability that multiple attacks within a given minute will be successful is 4/2^112, which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 4 – Services Authorized for Roles

Role	Authorized Services
Cryptographic-Officer/User	Firmware Load: Load an external firmware image. Note: Any external firmware image or application that is loaded on the module is outside the scope of this validation.

Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

- Show Status: Provides the current status of the module through LEDs.
- Self-tests: Invoke the power-on self-tests by power cycling the module.

Latent Services:

The following services are only available when a Security Manager is installed, which is not within the scope of this validation. The services are listed here for reference only:

- RSA Encrypt/Decrypt Key Transport
- AES Decrypt (FPGA)
- HMAC-SHA-1
- Generate Random Number
- Generate Key Pair
- SHA-1
- RSA Sign ANSI X9.31
- Zeroize

Definition of Critical Security Parameters (CSPs)

The module does not contain any CSPs.

Definition of Public Keys:

The following are the public keys contained in the module:

- Firmware Load Key: Verifies the authenticity of firmware images to be loaded from an external source, and verifies operator authentication.

Definition of CSPs Modes of Access

Table 5 defines the relationship between access to CSPs and the different module services.

Table 5 – CSP Access Rights within Roles & Services

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

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable; the JPG2K supports a limited operational environment that restricts the loading of firmware by ensuring all firmware being installed is appropriately signed.

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. <u>Power up Self-Tests:</u>

      1. Cryptographic algorithm tests:
         a. AES Decrypt Known Answer Test
         b. DRNG Known Answer Test
         c. HMAC SHA-1 Known Answer Test
         d. SHA-1 DS5250 Known Answer Test
         e. SHA-1 PowerPC Known Answer Test
         f. SHA-1 FPGA Known Answer Test (Tested as part of HMAC SHA-1)
         g. RSA Sign/Verify Known Answer Test
         h. RSA Encrypt/Decrypt Pairwise Consistency Test
      2. Firmware Integrity Test
      3. Critical Functions Tests: N/A.

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on NDRNG and DRNG
2. RSA Pairwise Consistency Test (Sign/Verify and Encrypt/Decrypt)
3. Firmware Load Test (RSA Signature Verification)

4. Data output shall be inhibited during self-tests and error states.
5. The module does not support key generation or zeroization without a Security Manager, which is not included in this validation.
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 concurrent operators.
8. The module shall not support bypass or maintenance states.

9. Physical Security Policy

Physical Security Mechanisms

The JPG2K 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.

Operator Required Actions

The operator is required to periodically inspect the module for evidence of tampering.

Table 7 – 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 beyond the scope of FIPS 140-2 requirements.

11. Definitions and Acronyms

AES	Advanced Encryption Standard
AES-Audio	Audio Engineering Society Audio
ANSI	American National Standards Institute
CBC	Cipher Block Chaining
CO	Cryptographic Officer
CSP	Critical Security Parameter
DCI	Digital Cinema Initiatives
DRNG	Deterministic Random Number Generator
ECB	Electronic Codebook
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FSM	Finite State Model
HD-SDI	High-Definition Serial Digital Interface
HMAC	Keyed-Hash Message Authentication Code
KAT	Known Answer Test
LED	Light Emitting Diode
MAC	Message Authentication Code
NDRNG	Non-Deterministic Random Number Generator
OEM	Original Equipment Manufacturer
PCI-E	Peripheral Component Interconnect Express
RNG	Random Number Generator
RSA	Rivest Shamir Adelman
SHA	Secure Hash Algorithm