FIPS 140-2 Security Policy for

Eastman Kodak Company® Secure Module 3000

Version 0.14
September 27, 2009

Table of Contents

Overview 3
Ports and Interfaces 4
Roles, Services and Authentication 4
  Roles 4
  Services 4
    RSA-based Authentication 6
Operational Environment 6
Cryptographic Key Management 6
Self Tests 8
    Power-Up Self Tests 8
    Conditional Self Tests 9
Mitigation of Other Attacks 9
Physical Security Policy 9
Secure Installation 12

Overview

The Kodak Secure Module 3000 (herein referred to as “the module” or “Secure Module”) provides the cryptographic functions used during the playback of digital cinema content. The Secure Module converts the packaged, compressed and encrypted data into raw image, sound, subtitles and auxiliary data used in exhibition and performs security functions such as media decryption, link encryption, and key management.

The Kodak Secure Module 3000 is a multi-chip, embedded cryptographic module and is intended to meet the overall DCI specification, version 1.2 requirements. This equates to an overall FIPS 140-2 Level 2. The following table summarizes the individual FIPS 140-2 sections as well as the level required by DCI for the module, for each section.

Table 1 – Intended Level Per FIPS 140-2 Section

Section	Section Title	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	3
4	Finite State Model	2
5	Physical Security	3
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

The Secure Module supports Security Management, Media Decryption and Link Encryption. The module only implements an Approved mode of operation.

The Secure Module consists of the following FIPS approved algorithms:

- AES – Certs. #1071, #1072 and #1076
- SHA-1 – Certs. #1012 and #1013
- SHA-256 – Cert. #1013
- HMAC SHA-1 – Certs. #603 and #604
- RSA – Cert. #508
- RNG – Cert. #606

The Secure Module also supports the following non-FIPS approved algorithms:

- RSA – key wrapping; key establishment mechanism provides 112-bits of encryption strength.

- MD5[1]
- HMAC-MD5[1]

The following sections demonstrate how the Secure Module meets the requirements of FIPS 140-2 Level 3. The evaluated platform consists of the following:

- Kodak Secure Module 3000
    - Hardware P/N 4F6138 Version – A
    - Firmware Version – 1.0-068

This document details the security policy for the module.

Ports and Interfaces

The Secure module has the following physical ports and interfaces.

Table 2 – Secure module Interface Mapping

Logical Interface	Physical Interface Mapping
Data Input Interface	Parallel Bus Port, Ethernet Port
Data Output Interface	Ethernet Port, Serial Video Port, Serial Audio Port
Control Input Interface	Ethernet Port, Parallel Bus Port
Status Output Interface	Ethernet Port, LED Pins, Parallel Bus Port
Power Interface	Power Pins

Roles, Services and Authentication

Roles

The module supports two roles: a User role and a Crypto Officer role. The User role and the Crypto Officer role can only access the module after authenticating themselves on a TLS session. The module supports identity-based authentication using digital certificates for both User and Crypto Officer Roles. The User role and the Crypto Officer role are mutually exclusive from one-another.

The module does not support a maintenance role.

Services

[1] This algorithm is allowed for use in FIPS mode as the HMAC MD5 part of the pseudo-random function in TLS v1.0.

In order to invoke the services associated with each role, the operator must first establish TLS communication on the appropriate port. Each role is authenticated via a certificate exchange over TLS sessions.

The services provided are summarized in Table 3.

Table 3 – Module Services

Role	Service	Service Inputs	Service Outputs
User Role	KDM Validate	Key Delivery Message	None
User Role	Prep Suite	Media to be played	None
User Role	Play	None	Encrypted content playback
User Role	Purge Suite	None	None
Crypto Officer Role	Upgrade	Upgrade Authorization Message	None
Any	Operator Authentication	Operator Authentication Certificate	Established TLS Session
Any	Perform Self-tests	None	Self-tests Results
Any	Show Status	None	Module Status

Table 4 – Access Rights within Services

Service	Cryptographic Keys and CSPs	Type(s) of Access
KDM Validate	Device Private Key	Read
	Master Key	Read
	Content Encryption Key	Write
Prep Suite	X9.31 RNG Seed Key	Read
	X9.31 RNG Seed	Read
	Link Encryption Key	Write
Play	Master Key	Read
	Content Encryption Key	Read
	Link Encryption Key	Read
Purge Suite	Content Encryption Key	Delete
	Link Encryption Key	Delete
Upgrade	Device Private Key	Read
Operator Authentication	Kodak Authorized User Root Cert.	Read
	TLS Pre-master Secret	Write
	TLS Encryption Key	Write
Perform Self-tests	None	None
Show Status	None	None

The module does not support a bypass capability in the approved mode of operations.

RSA-based Authentication

The User and Crypto Officer authenticate to the module using an RSA key pair. The RSA key pair has modulus size of 2048 bit, which has an equivalent symmetric key strength of 112-bits. An attacker would have a 1 in 2^112 chance of randomly obtaining the key, which is much stronger than the one in a million chance required by FIPS 140-2. To exceed a one in 100,000 probability of a successful random key guess in one minute, an attacker would have to be capable of approximately 5.19x10^28 attempts per minute, which far exceeds the operational capabilities of the module to support.

Operational Environment

The module operates in a limited operational environment. There is no way for an operator to load/execute firmware that has not been placed on the Secure Module by the Crypto Officer via the authenticated path.

Candidate firmware will be accompanied by an RSA digitally signed upgrade authorization message. This signed message includes a manifest file of cryptographic hashes for all components of the candidate firmware. The Crypto Officer is the only operator that can initiate the upgrade procedure and can only do so via the authenticated TLS session. Once the upgrade action is initiated and the signature and hashes are verified then the firmware images can be loaded for use.

In order to maintain the FIPS 140-2 validation of the module, only firmware that has been validated against FIPS 140-2 may be used.

Cryptographic Key Management

Key/CSP Entry/Output:

Entry of Content Encryption keys is performed when these keys are delivered in asymmetrically encrypted key delivery messages that are transmitted over an AES-128 protected and authenticated TLS session.

Key Generation

The Master Key and Link Encryption Keys are generated via the ANSI X9.31 DRNG supported in the Secure Module.

Symmetric key generation is used in the creation TLSv1.0 sessions with clients.

The Device Private Key and the public keys used by the module are installed in the factory and there is no User or Crypto Officer command to change them, thus no modification or substitution is possible.

Key Storage/Zeroization:

Content Encryption Keys are kept in a key cache in the module's flash disk. The key cache is encrypted using the Master Key. The Master Key is destroyed as a part of the module's tamper response strategy.

The TLS session keys are stored in the Secure Module's memory during the TLS handshake and are destroyed at the end of the TLS session.

Table 5 – Secret and Private Cryptographic Keys and CSPs

Keys/CSPs	Description	Algorithm	Storage/Location	Zeroization	Generation
Device Private Key	RSA 2048-bit private key that is used to decrypt messages intended for the Secure Module and for signing digital signatures	2048 bit RSA key	Stored encrypted on flash disk. The key is encrypted using the Master Key. When in use, the key is decrypted into DDR2 RAM	Under normal power, the key is zeroized by DDR clear.	Generated outside the module and entered during manufacturing.
Master Key	AES-128 key used to protect the Device Private Key and Content Encryption Key cache.	AES-CBC (128 bit)	Security Supervisor battery backed RAM Persistent Plaintext	Zeroized by tamper switch when enclosure opened by operator[2]	Generated in the module using ANSI X9.31 DRNG.
Content Encryption Keys	AES-128 keys used to protect data sent to the Secure Module-also used in HMAC-SHA-1 calculations	AES-CBC (128 bit)	Persistently stored to Flash Disk Encrypted	Not zeroized as they are encrypted with Master key	N/A - These keys are entered into the module asymmetrically encrypted with RSA keys.
Content Integrity Keys	HMAC-SHA-1 message integrity code used to ensure the integrity of the data sent into the Secure Module	HMAC-SHA-1	Security Manager (FPGA) Ephemeral Encrypted	Register Reset	Not generated in the Secure Module.
Link Encryption Keys	AES-128 key used to encrypt outgoing video data	AES-CTR (128 bit)	Link Encryptor (FPGA) Ephemeral Plaintext	Register Reset	Generated in the module using ANSI X9.31 DRNG.
TLS Pre master secret	Shared secret created using asymmetric cryptography from which new TLS session keys can	Shared secret	Security Manager (FPGA) Ephemeral Plaintext	Zeroized when the TLS session is closed.	Negotiated during TLS handshake.

[2] See Physical Security Policy section for details for operator zeroization procedure

	be created.				
TLS Encryption Key	AES 128 keys used to encrypt session data during TLS session.	AES-CBC (128 bit)	Security Manager (FPGA) Ephemeral Plaintext	Zeroized when the TLS session is closed.	Negotiated during the TLS handshake.
X9.31 RNG Seed Key	Two-Key Triple-DES value used by the ANSI X9.31 RNG	ANSI X9.31 RNG	Security Manager (FPGA) Ephemeral Plaintext	Zeroized when module restarted	Generated from output of the non-approved RNG
X9.31 RNG Seed	8-byte seed value (V) used by ANSI X9.31 RNG	ANSI X9.31 RNG	Security Manager (FPGA) Ephemeral Plaintext	Zeroized when module restarted	Generated from output of the non-approved RNG.

Register Reset: This method involves an FPGA register reset action and can only be taken when the Secure Module is running under primary power.

There are a few public keys and certificates stored within the Secure Module. They are as follows:

- Device Public Key – used to establish TLS sessions and used by entities external to the Secure module to encrypt messages intended for it – companion to the Device Private Key
- Device Certificate – contains a copy of the Device Public Key – used to identify the Secure module uniquely
- Kodak Authorized User root cert – X509 certificate containing an RSA 2048-bit public key. All certificates that get issued to authorized users (SMS) will be signed by this root certificate. The root certificate can be used to check the authenticity of a user that connects to the Secure module.
- Authorized Upgrade Public Key – RSA 2048-bit public key used to authenticate the firmware upgrade.

Self Tests

Power-Up Self Tests

The following power-up self tests are performed by the module:

- Firmware integrity tests using CRC-32
- Known Answer Tests for each implementation of the approved algorithms: AES, SHA-1, SHA-256, HMAC SHA-1, RSA, and RNG
- A self-test that checks for an enclosure breach
- Check on private key integrity

Conditional Self Tests

The following conditional self tests are performed by the module:

- Continuous Random Number Generator Test for both approved and non-approved RNGs
- Firmware Load Test using RSA digital signature whenever firmware is loaded into the module.

Mitigation of Other Attacks

The module does not implement mechanisms to mitigate any other specific attacks.

Physical Security Policy

The Kodak Secure Module 3000 is a multiple-chip embedded module and validated at Level 3. The module is made of commercially available, production grade components meeting commercial specifications for power, temperature, reliability, shock and vibration. All integrated circuit chips have standard passivation techniques applied to them.

The cryptographic security boundary is defined by the unit's strong opaque metal enclosure. Access to the circuitry is restricted through the use of tamper-evidence labels applied to the removable cover showing visible evidence if the unit has been opened after shipment. The only way to get to the cover is to break the tamper seals.

Tamper response and zeroization circuitry is also present to destroy plaintext critical security parameters (CSP) upon removal of the cover. Tamper response and zeroization is active when power is applied - either main (primary) power or battery back-up. Loss of both also results in zeroization. NOTE - the battery is located on the Carrier Board external to the module's cryptographic boundary.

An operator of the module can use the tamper response and zeroization circuitry to perform the procedural zeroization of the module's Master Key value. The two methods available to the operator are:

1. While power is still applied to the module, the operator can remove the case causing one of the switches to be triggered and actively zeroizing the value.
2. The operator can remove the module from the computer system it is installed into and disconnect the carrier board from the module. This will remove power from the module causing the Master Key to be passively zeroized since there is no power available to maintain the value in RAM.

Attempts to enter the module without removing the cover will cause visible damage to the module.

The Kodak Secure Module 3000 is 1.1 inches high by 5.5 inches wide by 10.5 inches deep.

To ensure physical security, make the following checks regularly:

- examine the enclosure for obvious signs of damage,
- examine the enclosure for removal of tamper seals.

The following table outlines the recommended inspection and/or testing of the physical security mechanisms:

Physical Security Mechanism	**Recommended Frequency of Inspection/Test**	**Inspection/Test Guidance Details**
Tamper Switch	No direct inspection or test is required.	The module enters the tamper error state when the switch is tripped. Once in this state, the destruction of all CSPs due to tamper will render the module un-usable even if switches are reset
Tamper Evidence	In accordance with organization's Security Policy.	Inspect the enclosure and tamper evident tape for physical signs of tampering or attempted access to the cryptographic module.

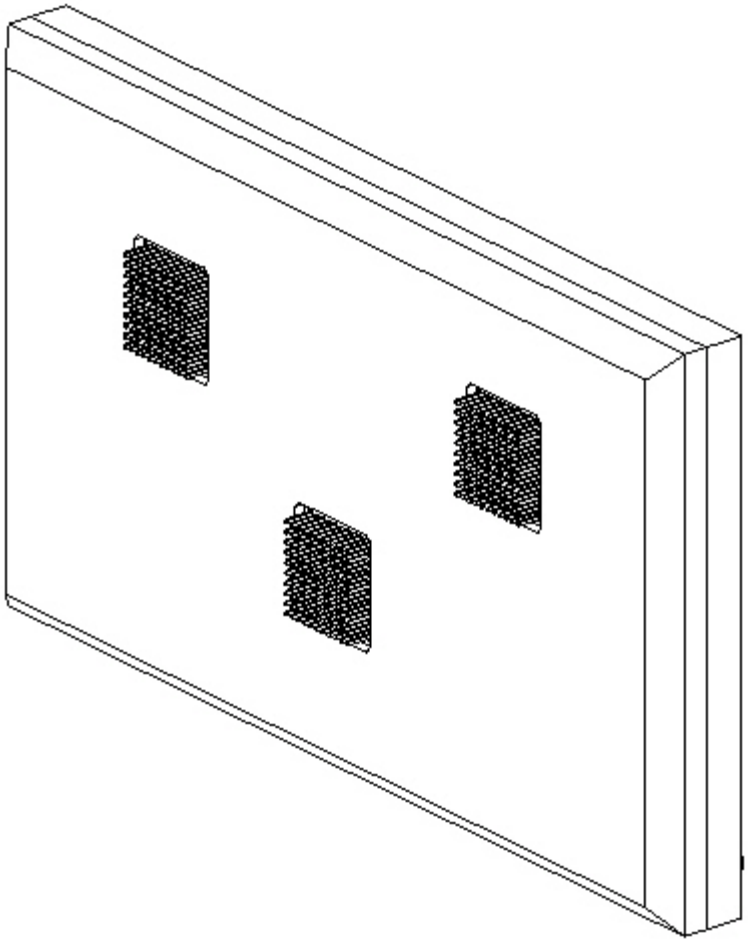

Figure 1 - Front view

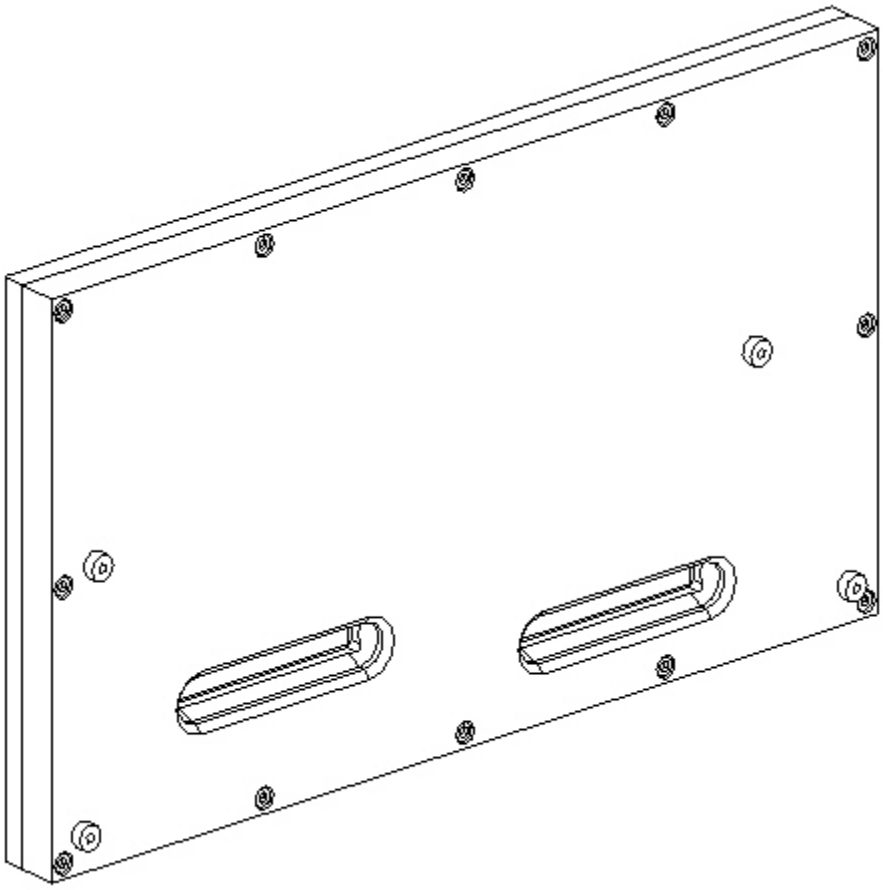

Figure 2 - Back view

Secure Installation

The operator(s) assuming the Crypto-Officer role receives the module from Kodak via a secure delivery mechanism. The module is shipped in a box sealed with tape. The Crypto-Officer should examine the box and tape used to seal the box for evidence of tampering. Additionally, the Crypto-Officer should carefully examine the shipping container containing the module for signs of tampering, which can include tears, scratches, and other irregularities in packaging.

Before the initial configuration of the module, the Crypto-Officer must maintain control of the module and restrict any access to the module until configuration is completed and the module is fully initialized for FIPS 140-2 compliant operations.

Periodically, the Secure Module should be inspected to verify that its enclosure has not been tampered with and the device is physically secure. The module is housed in a FIPS 140-2 Level 3 compliant case and is shipped from the factory in a secure condition. Access to the module's internal components can only be gained by removing the module's cover. Tamper-evident labels are placed across the module's removable covers. Any attempt to access the module's

internal components will result in the tamper evident labels being damaged. Tamper response and zeroization circuitry is also present to destroy plaintext critical security parameters (CSP) upon removal of the cover. The module enclosure should be regularly inspected for signs of tampering, including deep scratches on the surface, cracks, and any physical damage to the appearance of the module. Verify that the tamper-evident labels are fully intact.