FIPS 140-2 Non-Proprietary Security Policy

for

Gemini

Document Version 1.0.3

Sony Corporation

TABLE OF CONTENTS

1. MODULE OVERVIEW 3

2. SECURITY LEVEL 5

3. MODES OF OPERATION 6

APPROVED MODE OF OPERATION 6

4. PORTS AND INTERFACES 7

5. IDENTIFICATION AND AUTHENTICATION POLICY 8

ASSUMPTION OF ROLES 8

6. ACCESS CONTROL POLICY 9

ROLES AND SERVICES 9
DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 11
DEFINITION OF PUBLIC KEYS: 11
DEFINITION OF CSPS MODES OF ACCESS 12

7. OPERATIONAL ENVIRONMENT 14

8. SECURITY RULES 14

9. PHYSICAL SECURITY POLICY 16

PHYSICAL SECURITY MECHANISMS 16
OPERATOR ACTIONS 16

10. POLICY ON MITIGATION OF OTHER ATTACKS 17

11. DEFINITIONS AND ACRONYMS 18

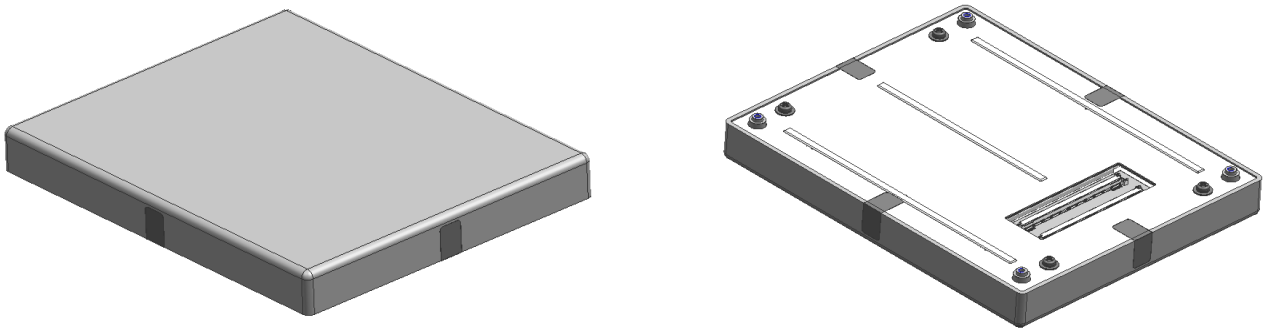
12. REVISION HISTORY 19

1. Module Overview

The Gemini is a multi-chip embedded cryptographic module that is encased in a hard opaque commercial grade metal case. The cryptographic boundary is defined as the entire metal case perimeter, including all hardware, software, and firmware encapsulated within. The interfaces are all traces that cross the cryptographic boundary.

The primary purpose of the Gemini is to provide decryption, decoding/encoding of audio/video data for the digital cinema projector system in which it is used.

The diagram below provides an illustration of the cryptographic module, along with the cryptographic boundary.



Top Side **Bottom Side**

Figure 1 – Image of the Cryptographic Module

The Gemini is validated in the following hardware / firmware versions:

Table 1 – The Validated Module Versions

Hardware version: 1.0.0
Firmware versions: 1.0.0 or 1.0.1

The Gemini firmware configurable hierarchy is as follows:

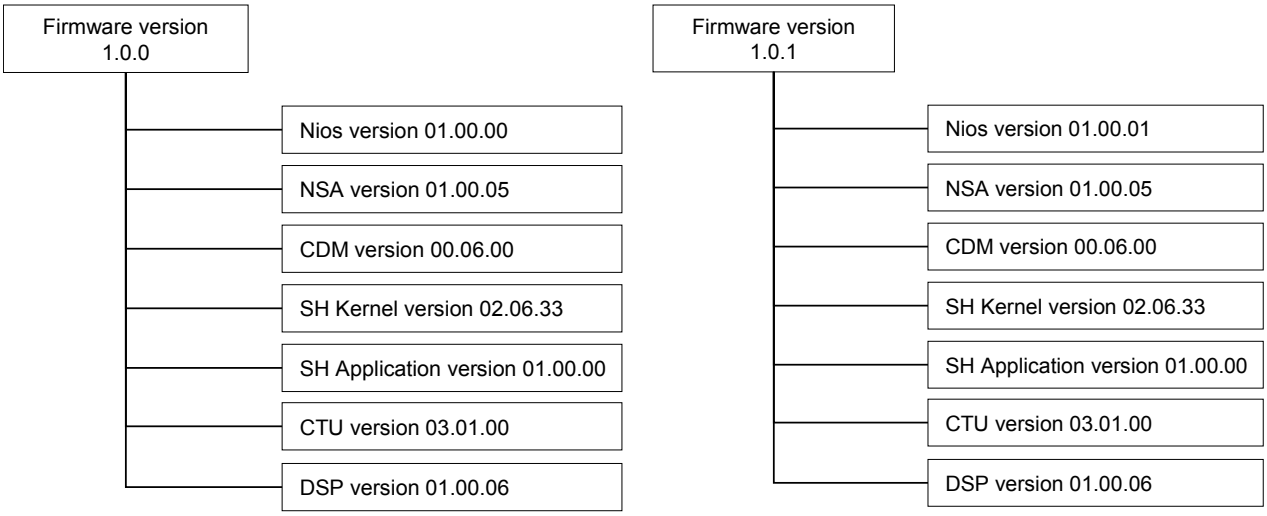


Figure 2 – Gemini firmware configurations.

2. Security Level

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

Table 2 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	2
Roles, Services and Authentication	3
Finite State Model	2
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	2
EMI/EMC	2
Self-Tests	2
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Modes of Operation

Approved mode of operation

The module is designed to continually operate in a FIPS approved mode of operation. A non-FIPS approved mode of operation is not supported. The cryptographic module supports the following FIPS approved cryptographic algorithms:

- AES with 128 bit key (as per FIPS-197)
  - CBC mode of operation - Certificate : #1539
  - CBC mode of operation (Decrypt only) - Certificate : #1541
  - ECB mode of operation - Certificate : #1540
- SHA-1 with 160 bit hash value (as per FIPS 180-3) - Certificate : #1364, #1365, #1367
- SHA-256 with 256 bit hash value (as per FIPS 180-3) - Certificate : #1364, #1365, #1366
- HMAC-SHA-1 with 160 bit MAC value (as per FIPS 198) - Certificate : #901, #902
- RSA Key Generation and Signature Generation/Verification with 2048 bit keys (as per PKCS#1 v1.5) - Certificate : #750, #751
- ANSI X9.31 RNG using AES (as per ANSI X9.31) - Certificate : #829, #830
- FIPS 186-2 RNG using SHA-1 (as per FIPS 186-2) - Certificate : #828

In addition to the above algorithms the module employs the following FIPS non-approved algorithms that are to be used in the FIPS approved mode of operation.

- RSA only for key wrapping. (Key establishment methodology provides 112-bits of encryption strength)
- NDRNG for the seeding of the ANSI X9.31 RNG
- HMAC-MD5 for the pseudo random function in TLS

By verifying that the firmware versions identified using the 'Get Parameter 2' service match each of the validated firmware component versions listed in the Section 1, the operator can be assured that the module is in the Approved mode.

4. Ports and Interfaces

The Gemini's physical interfaces are the traces that cross the perimeter of the physical cryptographic boundary. These traces support the following logical interfaces required by FIPS 140-2:

- Data Input
- Data Output
- Status Output
- Control Input

In addition, the module receives power from an outside source and thus supports a power input interface.

- Power Input

5. Identification and Authentication Policy

Assumption of roles

The Gemini shall support two distinct operator roles (User and Crypto-Officer). The cryptographic module shall enforce the separation of roles using identity-based operator authentication. The Crypto-Officer and User are authenticated using the RSA 2048 signature verification algorithm or an ID and Authentication Secret.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	• RSA Digital Certificate • ID and Authentication Secret Verification
Crypto-Officer	Identity-based operator authentication	• RSA Digital Certificate • ID and Authentication Secret Verification

Table 4 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
RSA Digital Certificate Verification	The authentication is based on RSA 2,048, which has an equivalent strength of 112-bits. Therefore, the probability with which a random attempt will succeed or a false acceptance will occur is 2^{-112} which is less than 1/1,000,000. There is a 10msec delay after each trial which limits the number of attempts per minute. The probability of a random attempt successfully authenticating to the module within one minute is also 1.16E-30 which is less than 1/100,000.
ID and Authentication Secret Verification	The Gemini accepts 64 possible characters and a minimum 8 characters for an authentication secret and the probability with which a random attempt will succeed or a false acceptance will occur is 2^{-48} which is less than 1/1,000,000. There is a 10msec delay after each trial which limits the number of attempts per minute. The probability of a random attempt successfully authenticating to the module within one minute is also 2.13E-11 which is less than 1/100,000.

6. Access Control Policy

Roles and Services

Table 5 – Crypto-Officer Specific Service

Service	Description
Account Management	Manages operator accounts (add and delete).
Critical Security Control	Switches flag of critical security status.
Firmware Update	Updates the firmware of the module.
Initial Configuration	Sets public key certificates and unique product parameters.
Public Key Control	Generates RSA key pair and obtains public keys.
Zeroization	Destroys all plaintext CSPs.

* Note: If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.

Table 6 – User Specific Service

Service	Description
Contents Validation 1	Validates the integrity of audio and video.
CPL Control	Controls DCP and the list of them.
DCP Control	Obtains each parameter which was set in the module.
Get Certificate Data	Obtains RSA public key certificates.
Get Parameter 1	Obtains each parameter which was set in the module.
Get Status 1	Obtains the status of the module and the version number.
KDM Control	Controls KDM (import, read, store, clear).
Log Management	Obtains the log data and tagging.
Playback	Plays back Contents (Video and Audio).
Playback Preparation	Makes the preparation of the playback and obtains the status of playback.
Property Setting	Sets RTC and network parameters.

RAID Operation	Control the data in the RAID configured HDD.
Confirmation Number Change	Changes confirmation number.
Status Initialization	Initializes the marriage status and the tamper status.

Table 7 – Crypto-Officer and User Common Service

Service	Description
Adjust Playback Parameter	Adjusts parameters for the playback and obtains the status of playback.
Certificate Check	Checks integrity RSA public key certificates and obtains them.
Contents Validation 2	Validates the integrity of audio and video.
Get Parameter 2	Obtains each parameter which was set in the module.
Get Random Number	Obtains random number.
Get Status 2	Obtains the status of the module and external devices.
Subtitle Decryption	Decrypts subtitles.
Authentication Secret Change	Changes operator authentication secret. In User Role, a operator can change only own secret.
Playback Control	Controls the playback of Contents (Video and Audio).
Time setting	Obtains/sets the date and the clock time.

Table 8 – Unauthenticated Service

Service	**Description**
Show Status	Obtains the module status.
Self-tests	Performs the power-up self-tests.

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Contents Encryption Key (CEK) – AES key used to decrypt contents.
- Content Integrity Key (CIK) – HMAC-SHA-1 key for integrity check of contents.
- Master Key (MK) – AES key used to protect all CSPs.
- Device Link Key (DLK) – AES key used to protect a channel with external device.
- Temporary Device Link Key (TDLK) – Temporary AES key used to protect a channel with external device.
- TLS Session Key (TSK) – The AES key established in TLS.
- TLS MAC Secret (TMACS) – The HMAC key established in TLS.
- RSA Signing Key (RSK) – RSA private key for the generation of a digital signature for the log data and for processing as TLS server.
- Device Private Key (DPK) – RSA private key used to decrypt wrapped cryptographic keys entered into the module in TLS.
- KDM Private Key (KPK) - RSA private key used for decryption of CEK.
- TLS Premaster Secret (TPS) – The parameter used for key establishment in TLS.
- TLS Master Secret (TMS) – The parameter used for key establishment in TLS.
- PRF State (PS) – The internal state used for key establishment in TLS.
- Seed and Seed Key (SSK) – The secret values necessary for the FIPS approved RNG.
- Authentication Secret (AS) – The operator password used to authenticate the operator.

Definition of Public Keys:

The following are the public keys contained in the module:

- Gemini Manufacturer Public Key – RSASSA 2048 public key used to verify a certificate chain of trust.
- Gemini Trusted Public Key – RSASSA 2048 public key used to verify a certificate chain of trust.
- Device Public Key – RSAES 2048 public key corresponded to the Device Private Key.
- RSA Verifying Key – RSASSA 2048 public key corresponded to the RSA Signing Key.
- KDM Public Key – RSASSA 2048 public key corresponded to the KDM Private Key.
- Public Key for F/W Upgrade – RSASSA 2048 public key used to verify the digital signature over the firmware image to be upgraded.

- Operator Public Key – RSAES 2048 public key used to authenticate operators

Definition of CSPs Modes of Access

Table 9 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- **Generate (*G*)** : the CSP is generated using an approved RNG.
- **Use (*U*)** : the CSP is used to perform cryptographic operations within its corresponding algorithm.
- **Entry (*E*)** : the CSP is entered into the module.
- **Output (*O*)** : the CSP is output from the module.
- **Zeroize (*Z*)** : the CSP is destroyed.

Table 9 – CSP Access Rights within Roles & Services

Role		Service Name	CSP(G, U, E, O, Z)
C.O.	User		
X		Account Management	DLK(U), TDLK(U), AS(U, E, Z)
X		Critical Security Control	DLK(U), TDLK(U)
X		Firmware Update	DLK(U), TDLK(U)
X		Initial Configuration	MK(U, E), DLK(U, E), TDLK(U)
X		Public Key Control	MK(U), DLK(U), TDLK(U), RSK(G, U), DPK(G, U), KPK(G, U), SSK(U)
X		Zeroization	All CSP(Z)
	X	Contents Validation 1	TSK(U), TMACS(U)
	X	CPL Control	TSK(U), TMACS(U)
	X	DCP Control	CEK(Z), TSK(U), TMACS(U)
	X	Get Certificate Data	TSK(U), TMACS(U)
	X	Get Parameter 1	TSK(U), TMACS(U)
	X	Get Status 1	TSK(U), TMACS(U)
	X	KDM Control	CEK(E, O, Z), SSK (E, Z), TSK(U), TMACS(U), KPK(U)
	X	Log Management	TSK(U), TMACS(U), RSK(U)
	X	Playback	TSK(U), TMACS(U)
	X	Playback Preparation	TSK(U), TMACS(U)
	X	Property Setting	TSK(U), TMACS(U)
	X	RAID Operation	TSK(U), TMACS(U)
	X	Confirmation Number Change	TSK(U), TMACS(U)
	X	Status Initialization	TSK(U), TMACS(U)
X	X	Adjust Playback Parameter	CIK(G), DLK(U), TDLK(U)
X	X	Certificate Check	DLK(U), TDLK(O,U)
X	X	Contents Validation 2	DLK(U), TDLK(U)

X	X	Get Parameter 2	DLK(U), TDLK(U)
X	X	Get Random Number	DLK(U), TDLK(U), SSK(U)
X	X	Get Status 2	DLK(U), TDLK(U)
X	X	Subtitle Decryption	DLK(U), TDLK(U), KPK(U)
X	X	Password Change	DLK(U), TDLK(U), AS(U, E, Z)
X	X	Playback Control	CEK(U), CIK(U, Z), DLK(U), TDLK(U)
X	X	Time setting	DLK(U), TDLK(U)
		Show Status	-
		Self-Test	-

* TPS, TMS, and PS are generated, used and zeroized in TLS establishment.

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the module does not contain a modifiable operational environment.

8. Security Rules

The Gemini was designed with the following security rules in mind. These rules are comprised of both those specified by FIPS 140-2 and those derived from Sony's company policy.

1. The cryptographic module shall provide two distinct operator roles. These are the User role, and the Crypto-Officer role.
2. The cryptographic module shall provide identity-based authentication.
3. When the module has not been placed in an authenticated role, the operator shall not have access to any cryptographic services.
4. The cryptographic module shall perform the following tests:

A. Power-up Self-Tests:

1. Cryptographic algorithm tests (for each implementation):
   a. AES 128 CBC Encryption/Decryption Known-Answer Test
   b. AES 128 ECB Encryption/Decryption Known-Answer Test
   c. ANSI X9.31 RNG Known-Answer Test
   d. FIPS 186-2 RNG Known-Answer Test
   e. SHA-1 Known-Answer Test
   f. SHA-256 Known-Answer Test
   g. HMAC-SHA-1 Known-Answer Test
   h. RSA PKCS#1 v1.5 Signature Generation/Verification Known-Answer Test
2. Firmware Integrity Test (CRC-16 and CRC-32)
3. Critical Functions Test:
   a. HMAC-MD5 Known-Answer Test
   b. RSA OAEP Pair-wise Consistency Test
   c. RSA PKCS#1 v1.5 Pair-wise Consistency Test (Encryption/Decryption)

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test
   a. ANSI X9.31 RNG
   b. FIPS 186-2 RNG
   c. NDRNG

   2. RSA Pair-wise Consistency Test
      a. Encryption/Decryption
      b. Signature Generation/Signature Verification
   3. Firmware Load Test (RSA Digital Signature Verification)
5. The operator shall be capable of commanding the module to perform the power-up self-test using recycling power.
6. Data output shall be inhibited during self-tests, zeroization, and error states.
7. Data output shall be logically disconnected from key generation processes.
8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
9. The module supports simultaneous operation up to two operators.
10. The module shall not support a bypass capability or a maintenance interface.
11. If a non-FIPS validated firmware version is loaded onto the module, then the module is ceases to be a FIPS validated module.
12. HMAC-MD5 is only used as the pseudo random function in TLS.
13. The module never outputs any CSPs except Content Encryption Key and Temporary Device Link Key. The Content Encryption Key is output RSA wrapped with KDM public key, and Temporary Device Link Key is transported RSA wrapped with Operator Public Key.

9. Physical Security Policy

Physical Security Mechanisms

The Gemini is a multi-chip embedded cryptographic module with the following physical security mechanisms:

- Production-grade components,
- The enclosure has a removable cover which is put security labels in secure manufacturing facility by Sony. When the cover is removed or the power supply from the outside is lost, all plaintext CSPs within the module are zeroized,
- The enclosure is opaque and provides tamper evidence,
- The enclosure is sufficiently hard, providing tamper detection and response in accordance with FIPS 140-2 level 3 physical security requirements.

Operator Actions

Due to the intended deployment environment for the module, Sony defers the physical inspection criteria to the end user of the cryptographic module. Any such inspection shall be based on the customer security policy, in particular with regards to the inspection frequency.

Table 10 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard Removable Enclosure	Every startup and reboot.	Inspect screw, scratches, or deformation of the metal case. If found such evidences, user should not use the module.
Tamper Evident Seals	Every startup and reboot.	Inspect scratches, prominent words. If found such evidences, user should not use the module and should return it to Sony.
Tamper detection	Every startup and reboot.	If the module was zeroized, user should return it to Sony.

10. Policy on Mitigation of Other Attacks

The module was not designed to mitigate other attacks outside of the specific scope of FIPS 140-2. Therefore, this section is not applicable.

Table 11 – Mitigation of Other Attacks

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

11. Definitions and Acronyms

Term	Definition
AES	**A**dvanced **E**ncryption **S**tandard
CDM	**C**ontents **D**ecryption and **D**ecode **M**odule
CPL	**C**ompositions **P**lay**l**ists
CSP	**C**ritical **S**ecurity **P**arameter
CTU	**C**ounter **T**ampering & **T**amper Detection **U**nit
DCI	**D**igital **C**inema **I**nitiative
DCP	**D**igital **C**inema **P**ackage
DRNG	Deterministic RNG
DSP	**D**igital **S**ignal **P**rocessor
EMI / EMC	**E**lectro**m**agnetic **I**nterference / **E**lectro**m**agnetic **C**ompatibility
HMAC	**H**ash-based **M**essage **A**uthentication **C**ode
KDM	**K**ey **D**elivery **M**essage
Nios	Embedding processer that runs within the PAD (FPGA)
NSA	**N**oise **S**uppressed **A**ccumulation
OAEP	**O**ptimal **A**symmetric **E**ncryption **P**adding
PAD	FPGA that processes video and audio data
PKCS	**P**ublic **K**ey **C**ryptography **S**tandards
PRF	**P**seudo **R**andom **F**unction
RNG	**R**andom **N**umber **G**enerator
RSA	**R**ivest-**S**hamir-**A**dleman
RTC	**R**eal **T**ime **C**lock
SH	Embedded 32-bits RISC
SHA	**S**ecure **H**ash **A**lgorithm
TLS	**T**ransport **L**ayer **S**ecurity

12. Revision History

Date	Version	Description
March 24, 2011	1.0.2	Initial public release.
June 8, 2011	1.0.3	Added firmware version 1.0.1.