FIPS 140-2 Security Policy

for

Gemini

Document Version 1.0.2

Sony Corporation

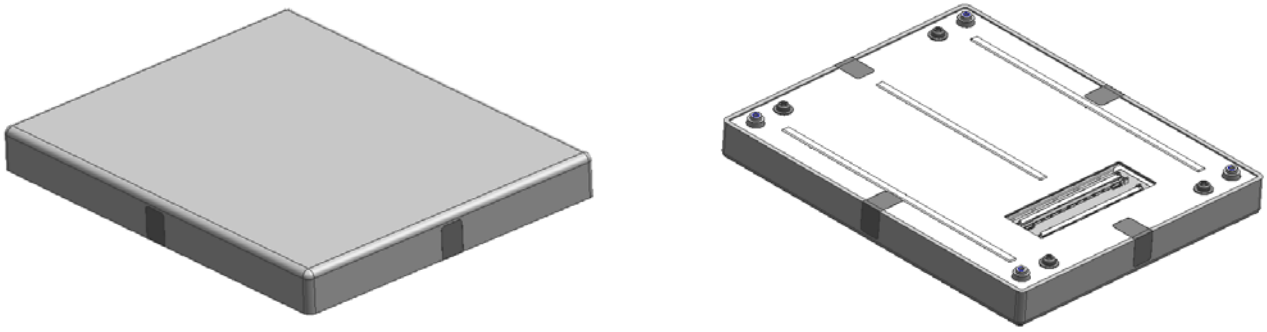
Table of Contents

1. Module Overview

The Gemini cryptographic module is a multi-chip embedded cryptographic module encased in a hard opaque commercial grade metal case. The cryptographic boundary is defined as the entire metal case perimeter, including all hardware 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 illustration below shows the Gemini, along with the cryptographic boundary.



Top Side **Bottom Side**

Figure 1 - Image of the Gemini Cryptographic Module

The Gemini is validated in the following hardware / firmware version.

- Hardware version: 1.0.0
- Firmware version: 2.0.0

Gemini firmware configurable hierarchy is as follows.

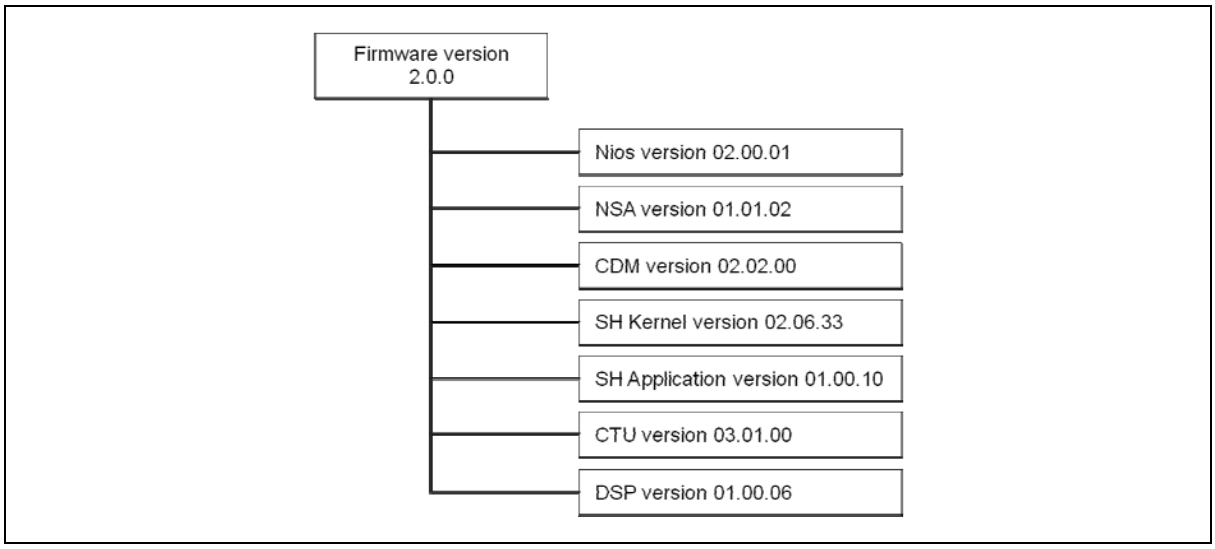


Figure 2 - Gemini Firmware Configuration

2. Security Level

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

Table 1 - 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

3.1. Approved Mode of Operation

The Gemini is designed to continually operate in a FIPS approved mode of operation. The Gemini supports the following FIPS approved cryptographic algorithms:

- AES with 128-bit key (as per FIPS 197)
  - CBC and ECB mode of operation - Certificates: #1539, #1540
  - CBC mode of operation (Decrypt only) - Certificate: #1541
- SHA-1 with 160-bit hash value (as per FIPS 180-3) - Certificates: #1364, #1365, #1367
- SHA-256 with 256-bit hash value (as per FIPS 180-3) - Certificates: #1364, #1365, #1366
- HMAC-SHA-1 with 160-bit MAC value (as per FIPS 198) - Certificates: #901, #902
- RSA Key Generation and Signature Generation/Verification with 2,048-bit key (as per FIPS 186-2) - Certificates: #750, #751
- ANSI X9.31 RNG using AES (as per ANSI X9.31) - Certificates: #829, #830
- FIPS 186-2 RNG using SHA-1 (as per FIPS 186-2) - Certificate: #828

In addition to the above algorithms the Gemini employs the following Allowed non-FIPS approved cryptographic algorithms for use in the FIPS approved mode of operation.

- RSA only for key wrapping. (Key establishment methodology provides 112-bit of encryption strength)
- NDRNG for the seeding of the ANSI X9.31 RNGs
- SP 800-135rev1 TLS KDF
- HMAC-MD5 for the pseudo random function in TLS

The operator can be assured that the Gemini in the approved mode by verifying that the firmware versions

identified using the 'Get Parameter 2' service match each of the validated firmware component versions listed in Section 1.

3.2. Non-Approved Mode of Operation

The Gemini does not support a non-FIPS Approved mode of operation.

4. Ports and Interfaces

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

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

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

- Power Input

5. Identification and Authentication Policy

5.1. Assumption of Roles

The Gemini supports two distinct operator roles (User and Crypto-Officer). The Gemini enforces 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 2 - 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

5.2. Authentication Mechanism

The Gemini supports two authentication mechanisms.

Table 3 - 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-bit. 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 Gemini within one minute is also 6,000 * 2^{-112} (< 2^{10} * 2^{-112} = 2^{-102}) 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} ($=(1/64)^8$) 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 Gemini within one minute is also 6,000 * 2^{-48} ($< 2^{10} * 2^{-48} = 2^{-38}$) which is less than 1/100,000.

6. Access Control Policy

6.1. Roles and Services

Table 4 - Crypto-Officer Specific Services

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 Gemini.
Initial Configuration	Sets public key certificates and unique product parameters.
Public Key Control	Obtains RSA public keys.
Zeroization	Destroys all plaintext CSPs.

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

Table 5 - User Specific Services

Service	Description
Contents Validation 1	Validates the integrity of audio and video.
CPL Control	Controls and lists Digital Cinema Packages (DCP).
DCP Control	Obtains each parameter which was set in the Gemini.
Get Certificate Data	Obtains RSA public key certificates.
Get Parameter 1	Obtains each parameter which was set in the Gemini.
Get Status 1	Obtains the status of the Gemini and the version number.
KDM Control	Controls Key Delivery Message (KDM - import, read, store, clear).
Log Management	Obtains log data and tagging.
Playback	Plays back contents (Video and Audio).
Playback Preparation	Prepares and obtains the status of the playback.
Property Setting	Sets Real Time Clock (RTC) and network parameters.
RAID Operation	Control the data in the RAID configured HDD.

Confirmation Number Change	Changes confirmation number.
Status Initialization	Initializes marriage and tamper status.

Table 6 - Crypto-Officer and User Common Services

Service	Description
Adjust Playback Parameter	Adjusts parameters for playback and obtains the playback status.
Certificate Check	Checks integrity of 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 Gemini.
Get Random Number	Obtains random number.
Get Status 2	Obtains the status of the Gemini and external devices.
Subtitle Decryption	Decrypts subtitles.
Authentication Secret Change	Changes operator authentication secret. In User Role, an 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 7 - Unauthenticated Service

Service	Description
Show Status	Obtains Gemini status.
Self-tests	Performs power-up self-tests.

6.2. Definition of Critical Security Parameters (CSPs)

The following CSPs are included in the Gemini.

- 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 stored 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 (Unused).
- Device Private Key (DPK) - RSA private key (Unused).
- SM Private Key (SPK) - RSA private key used for decryption of CEK, generation of a digital signature for the log data and TLS session data, and decryption of wrapped cryptographic keys which are entered into the Gemini in TLS.
- 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.

6.3. Definition of Public Keys

The following are the public keys contained in the Gemini:

- 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 - RSA 2048 public key corresponded to the Device Private Key (Unused).
- RSA Verifying Key - RSA 2048 public key corresponded to the RSA Signing Key (Unused).
- SM Public Key - RSASSA and RSAES 2048 public key corresponded to the SM 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

6.4. Definition of CSP Access Modes

Table 8 defines the relationship between CSP access modes and module services. The modes of access modes shown in Table 8 are defined as follows:

- **Generate (*G*)**: Generates the Critical Security Parameter (CSP) using an approved Random Number Generator (RNG).
- **Use (*U*)**: Uses the CSP to perform cryptographic operations within its corresponding algorithm.
- **Entry (*E*)**: Enters the CSP into the Gemini.
- **Output (*O*)**: Outputs the CSP from the Gemini.
- **Zeroize (*Z*)**: Removes the CSP.

Table 8 - CSP Access Rights within Roles & Services

Role		Service Name	CSP (*Access Mode*)
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*), DPK(*G*), SPK(*G*, *U*), SSK(*U*)
X		Zeroization	All CSPs(*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*), SPK(*U*)
	X	Log Management	TSK(*U*), TMACS(*U*), SPK(*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*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
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*), SPK(*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*)
Any	Any	Show Status	-
Any	Any	Self-Test	-

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

7. Operational Environment

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

8. Security Rules

The Gemini cryptographic module 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 Gemini shall provide two distinct operator roles. These are the User role, and the Crypto-Officer role.
2. The Gemini shall provide identity-based authentication.
3. When the Gemini has not been placed in an authenticated role, the operator shall not have access to any cryptographic services.
4. The Gemini shall perform the following tests:
    i. Power-up Self-Tests:
        a. Cryptographic algorithm tests (for each implementation):
            - AES 128 CBC Encryption/Decryption Known-Answer Tests
            - AES 128 ECB Encryption/Decryption Known-Answer Test
            - ANSI X9.31 RNG Known-Answer Test
            - FIPS 186-2 RNG Known-Answer Test
            - SHA-1 Known-Answer Test
            - SHA-256 Known-Answer Test
            - HMAC-SHA-1 Known-Answer Test
            - RSA PKCS#1 v1.5 Signature Generation/Verification Known-Answer Test
        b. Firmware Integrity Test (CRC-16 and CRC-32)
        c. Critical Functions Test:
            - HMAC-MD5 Known-Answer Test
            - RSA OAEP Pair-wise Consistency Test
            - RSA PKCS#1 v1.5 Pair-wise Consistency Test (Encryption/Decryption)
    ii. Conditional Self-Tests:

a. Continuous (RNG) test (ANSI X9.31 RNG, FIPS 186-2 RNG, NDRNG)

b. RSA Pair-wise Consistency Test (RSA Encryption/Decryption, RSA Digital Signature Verification)

c. Firmware Load Test (RSA Digital Signature Verification)

5. The operator shall be capable of commanding the Gemini to perform the power-up self-test by 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 Gemini.

9. The Gemini supports simultaneous operation up to two operators.

10. The Gemini shall not support a bypass capability or a maintenance interface.

11. If a non-FIPS validated firmware version is loaded onto the Gemini, then the Gemini ceases to be a FIPS validated module.

12. HMAC-MD5 is only used as the pseudo random function in TLS.

13. The Gemini never outputs any CSPs except the Content Encryption Key and the Temporary Device Link Key. The Content Encryption Key is output RSA wrapped with SM public key, and the Temporary Device Link Key is transported RSA wrapped with the Operator Public Key.

9. Physical Security Policy

9.1. 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 Gemini are zeroized. Refer to Figures 3 and 4 below for the expected placement of the seals and how the tamper seal should look when the module is received from the manufacturer.
- 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.

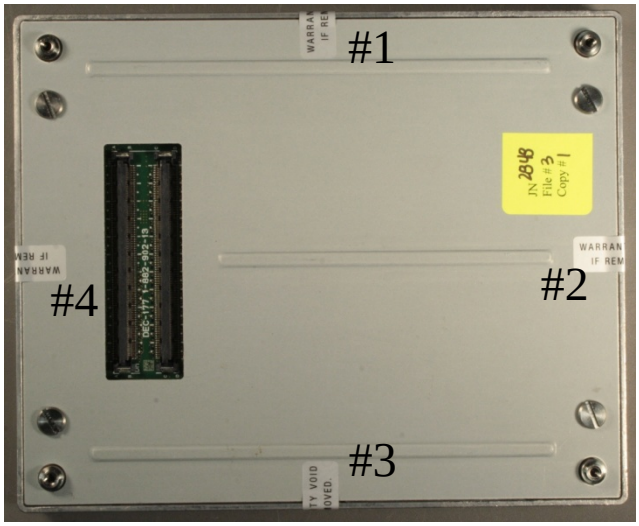


Figure 3: Tamper Evident Seal Locations

Figure 4: Close-up of Un-tampered Seal

9.2. Operator Actions

Due to the intended deployment environment for the Gemini, 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 9 - 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 for screw, scratches, or deformation of the metal case. If such evidence is found, user should not use the module.
Tamper Evident Seals	Every startup and reboot.	Inspect scratches, prominent words. If such evidence is found, 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 Gemini was not designed to mitigate other attacks outside of the specific scope of FIPS 140-2.Therefore, this section is not applicable.

Table 10 - Mitigation of Other Attacks

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

11. Definitions and Acronyms

Table 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
CRC	**C**yclic **R**edundancy **C**ode
CSP	**C**ritical **S**ecurity **P**arameter
CTU	**C**ounter **T**ampering & **Ta**mper Detection **U**nit
DCI	**D**igital **C**inema **I**nitiative
DCP	**D**igital **C**inema **P**ackage
DRNG	**D**eterministic **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 NSA (FPGA)
NSA	**N**io**s** & **A**udio Mapping
OAEP	**O**ptimal **A**symmetric **E**ncryption **P**adding
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
RSA ES/SSA	**RSA E**ncryption **S**tandard / **S**ecure **S**ignature **A**lgorithm
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
.Jun. 15, 2012	1.0.0	Initial public release.
Feb. XX, 2013	1.0.1	Incorporated comments from CST Lab.