FIPS 140-2 Security Policy

for

Gemini

Document Version 1.0.4

Sony Corporation

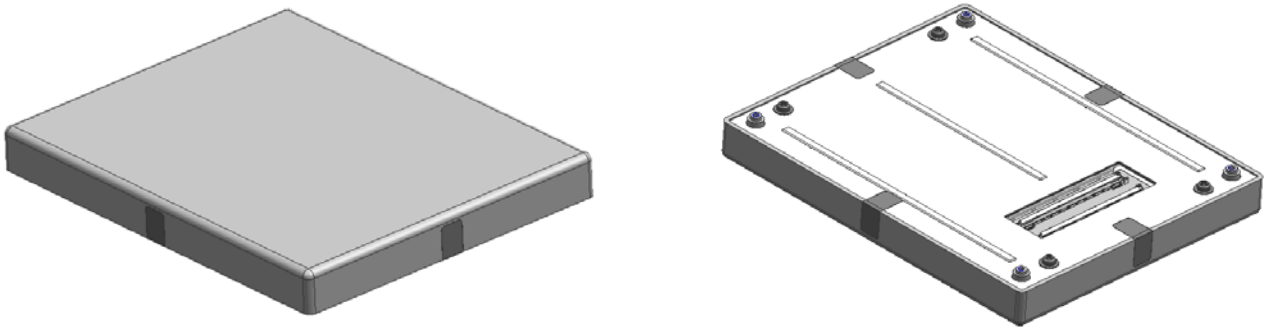
Table of Contents

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 and 2.1.0

Gemini firmware configuration table is as follows.

Table 1 – Gemini Firmware Configuration

Firmware Component	Firmware Version 2.0.0	Firmware Version 2.1.0
Nios	02.00.01	02.01.02
NSA	01.01.02	01.01.03
CDM	02.02.00	02.02.01
SH Kernel	02.06.33	02.06.33
SH Application	01.00.10	01.00.11
CTU	03.01.00	03.01.00
DSP	01.00.06	01.00.08

2. Security Level

The Gemini 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

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
- SP 800-135rev1 TLS KDF using SHA-1 (as per SP 800-135rev1)- Certificate: #115

  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 encryption only for key encapsulation. (Key establishment methodology provides 112-bit of encryption strength)
- NDRNG for the seeding of the ANSI X9.31 RNGs
- 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 Version Info' or ‘Get Detail Version Info’ 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 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

5.2. Authentication Mechanism

The Gemini supports two authentication mechanisms.

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-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 5 - Crypto-Officer Specific Services

Service	Description
Get User List	Outputs the List of User ID.
Initialize User	Initializes User account.
User Addition	Adds User account (up to 10 accounts)）
User Deletion	Deletes User account.
Initialize Critical Security Status	Initializes Critical Security Status.
Software Update	Performs firmware updating.
Check Factory Data	Checks whether each of initial data is set up.
Clear Log	Deletes log.
Set Factory Data	Sets up initial data.
Set Version	Sets up the version of DC Block.
Generate RSA Key	Generates the specified RSA key pair (ANSI X9.31) and outputs a public key.
Get Certificate Signing Request	Outputs RSA public key in CSR form.
Get RSA Public Key	Outputs the specified RSA public key.
Zeroization	Deletes all plaintext CSP.

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

Table 6 - User Specific Services

Service	Description
Delete Root Certificate	Deletes the specified root certificate.
Get Certificate Info	Outputs the detailed information of the specified certificate.
Get Root Certificate	Outputs the detailed information of the specified root certificate.

Service	Description
List Root Certificate	Outputs the file name list of stored root certificates.
Retrieve Certificate	Outputs a certificate specified by the certificate number.
Retrieve Root Certificate	Outputs the root certificate specified by the file name.
Store Root Certificate	Stores the root certificate specified by the file name.
User Password	Changes User password.
Validation Cancel	Cancels validation.
Validate DCP	Validates DCP specified by ID.
Validate Progress	Outputs the progress of DCP/CPL validation.
Validate 2	Validates DCP/CPL specified by ID.
Detail CPL 2	Outputs the detailed information of CPL stored in RAID block.
Detail CPL 3	Outputs the detailed information of CPL stored in RAID block.
Detail CPL 4	Outputs the detailed information of CPL stored in RAID block.
Detail CPL 5	Outputs the detailed information of CPL stored in RAID block.
Detail CPL 6	Outputs the detailed information of CPL stored in RAID block.
List CPL	Outputs the ID list of CPL stored in RAID block.
Relate CPL	Outputs the list of CPL relating to a specified PLID.
Retrieve CPL	Outputs a CPL file and stores it in RAID block.
Store PREPWI Begin	Starts import of DCP files associated to a specified Packing List.
Store PREPWI Cancel	Cancels import of CPL via networks.
Store PWI Begin	Starts import of CPL via networks.
Store PWI Cancel	Cancels import of CPL via networks.
Verify CPL	Verifies the CPL specified by CPL ID.
Delete DCP	Deletes DCP in RAID block.
Get DCP Deletion Count	Outputs the number of times that DCP in RAID block was deleted.
List DCP	Outputs the list of DCP registered in RAID block.
List DCP 2	Outputs the list of playable DCP registered in RAID block.
Refresh DCP	Refreshes a DCP area.

Service	Description
Refresh PWI DCP	Refreshes a DCP area specified by CPL and PKL.
Retrieve PL	Outputs a PKL file.
Set Title	Sets a title to DCP stored in RAID block.
Store DCP Begin	Starts import of DCP.
Store DCP End	Ends import of DCP.
Store S2S Begin	Starts import of S2S DCP.
Store S2S Cancel	Cancels import of S2S DCP.
Verify PL	Verifies the PL specified by PL ID.
Get Date	Outputs the clock of Gemini.
Get Time-zone	Outputs the time zone information of Gemini.
Get Time-zone 2	Outputs the time zone information of the environment.
Get Version	Outputs version information including each module version of Gemini and RAID block.
Get Version 2	Outputs the version information of a RAID block in addition to Get Version.
Ger Version 3	Outputs the version information of projector in addition to Get Version 2.
Get Audio Frequency	Outputs the MT's Audio frequency.
Get LED	Outputs the status of LED.
Get LED 2	Outputs the status and the color of LED.
Get Marriage Status	Outputs the status of marriage with projector.
Get PWI Transfer Status	Outputs the current PWI transfer status or result.
Get Rebuilding	Outputs the progress of the RAID rebuilding.
Get Status	Outputs device status information.
Get Status 2	Outputs RAID information in addition to Get Status.
Get Status 3	Outputs projector information in addition to GET Status 2.
Get Tamper Status	Outputs the tampering status..
Get Transfer Status	Outputs the current S2S transfer status or result.
Get Whitepoint	Outputs the status of whitepoint.
Heartbeat	Transmits a heartbeat.

Service	Description
Delete KDM	Deletes KDM specified by CPL ID or KDM ID.
Detail CPL	Outputs the detailed information of CPL stored in RAID block.
Detail KDM	Outputs the detailed information of KDM specified by CPL ID or KDM ID.
List KDM	Outputs the list of the registered KDM specified by KDM or KDM ID.
Relate KDM	Outputs the list of KDM related to CPL ID or KDM ID.
Retrieve KDM	Outputs the KDM file stored in RAID block.
Store KDM	Stores KDM.
Get Event Log	Outputs the event log information stored in RAID block.
Get Event Log 2	Outputs the event log information stored in RAID block.
List Security Log	Outputs the file name list of the security log stored in Gemini.
Retrieve Security Log	Outputs the security log stored in Gemini.
Retrieve Security Log 2	Outputs the security log specified by the file name.
Snapshot	Logs service snapshot.
Get Playback Status	Outputs the playback status.
Get Reel	Outputs the reel number playing back.
Play Pause Execution	Pauses playback.
Play Pause Resume	Resumes playback.
Playback CPL Start	Start playback of CPL.
Playback SPL Start	Start playback of SPL.
Playback 3D CPL Start	Starts playback of CPL.
Playback 3D SPL Start	Starts playback of SPL.
Playback Step	Performs frame-by-frame playback.
Playback Stop	Stops playback.
Get CC Delay	Outputs the delay of Closed Caption.
Get Delay	Outputs the delay of AV.
Get Muting	Outputs the current routing switch status of audio.
Get Muting Mask	Outputs the information of current audio muting mask.

Service	Description
Get Playback Type	Outputs the current playback type.
Get Position	Outputs the position where playback was stopped last time.
Get SPL	Outputs SPL stored in RAID block.
Set Audio Frequency	Sets the MT's audio frequency.
Set CC Delay	Sets the delay of Closed Caption.
Set Delay	Sets the delay of AV.
Set Muting	Sets information of audio routing switch.
Set Muting Mask	Sets information of muting mask.
Set Playback Type	Set playback type.
Set SPL	Sets SPL to a specified GPI channel.
Set Subtitle box	Sets the subtitle box size information.
Set Date	Sets up the clock of Gemini.
Set Date 2	Sets up the clock of Gemini.
Set External IP	Sets the IP address and port of external SMS.
Set LED Off	Turns off the external LED.
Set Network Configuration	Sets the network configuration information.
Set Time-zone	Sets up the time zone.
Set Time-zone 2	Sets up the time zone.
Delete Any	Deletes a file specified by file name.
DF	Outputs the information about RAID block.
Get Network Configuration	Outputs the current network configuration information.
List Any	Outputs the list of files.
Retrieve Any	Outputs a file specified by file name.
Store Any	Stores a file specified by file name.
Initialize Marriage	Resets the status of marriage with projector.
Initialize Security	Resets the security status of external equipment.

Table 7 - Crypto-Officer and User Common Services

Service	Description
Get Audio Status	Outputs the current status of audio.
Get Video Status	Outputs the current status of video.
Initialize Audio	Sets the parameters about Audio MXF.
Initialize Video	Sets the parameters about Video MXF.
Remap Audio	Sets up which channel of Sound Track is assigned to every channel.
Set Audio Lip Sync	Sets the delay to adjust to lip sync.
Set Audio Reel Information	Sets the audio reel information.
Set Video Reel Information	Sets the video reel information.
Get Certificate	Outputs the specified RSA public key certificate.
Initialize Validation Audio	Initializes validation of audio.
Initialize Validation Video	Initializes validation of video.
Start Validation	Starts validation of video/audio.
Stop Validation	Stops validation of video/audio.
Get Detail Version Information	Outputs detailed version of each component.
Get FM Serial Number	Outputs the FM serial number.
Get Gemini Version	Outputs the version of Gemini.
Get Serial Number	Outputs the serial number of Gemini.
Get Version Information	Outputs version information.
Get Random Number	Generates and outputs a random number.
Get Critical Security Status	Output the critical security status.
Get External Device Status	Outputs the status of the external device connected to Gemini.
Get Gemini Status	Outputs the current status of Gemini.
Change User Password	Changes own password.
Mute Audio	Mutes the sound of the specified channel.
Mute Video	Turns a video plain black.
Pause Playback	Pauses playback of video/audio.

Service	Description
Start Playback	Starts playback of video/audio.
Stop Playback	Stops playback of video/audio.
Initialize Subtitle Decryption	Initializes subtitle for decryption.
Set/Get Date	Sets/Outputs date and time.

Table 8 - 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 - RSASSA 2048 public key used to authenticate operators.
- Projector Public Key - RSAES 2048 public key used to authenticate an external device.
- KDM Issuer Public Key - RSASSA 2048 public key used to verify signature of KDM.

6.4. Definition of CSP Access Modes

Table 9 defines the relationship between CSP access modes and module services. The modes of access modes shown in Table 9 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 9 - CSP Access Rights within Roles & Services

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
X		Get User List	DLK(*U*), TDLK(*U*)
X		Initialize User	DLK(*U*), TDLK(*U*), AS(*UZ*)
X		User Addition	DLK(*U*), TDLK(*U*), AS(*E*)
X		User Deletion	DLK(*U*), TDLK(*U*), AS(*Z*)
X		Initialize Critical Security Status	DLK(*U*), TDLK(*U*)
X		Software Update	DLK(*U*), TDLK(*U*)
X		Check Factory Data	MK(*U*), DLK(*U*), TDLK(*U*)
X		Clear Log	DLK(*U*), TDLK(*U*)
X		Set Factory Data	MK(*E*), DLK(*E*), TDLK(*U*)
X		Set Version	DLK(*U*), TDLK(*U*)
X		Generate RSA Key	MK(*U*), DLK(*U*), TDLK(*U*), RSK(*G,E*), DPK(*G,E*), SPK(*G,E*), SSK(*U*)
X		Get Certificate Signing Request	MK(*U*), DLK(*U*), TDLK(*U*), SPK(*U*)
X		Get RSA Public Key	DLK(*U*), TDLK(*U*)
X		Zeroization	All CSPs(*Z*)
X	X	Get Audio Status	DLK(*U*), TDLK(*U*)
X	X	Get Video Status	DLK(*U*), TDLK(*U*)
X	X	Initialize Audio	DLK(*U*), TDLK(*U*)
X	X	Initialize Video	DLK(*U*), TDLK(*U*)
X	X	Remap Audio	DLK(*U*), TDLK(*U*)
X	X	Set Audio Lip Sync	DLK(*U*), TDLK(*U*)
X	X	Set Audio Reel Information	CEK(*U*), CIK(*G*), DLK(*U*), TDLK(*U*)
X	X	Set Video Reel Information	CEK(*U*), CIK(*G*), DLK(*U*), TDLK(*U*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
X	X	Get Certificate	DLK(*U*), TDLK(*U*)
X	X	Initialize Validation Audio	DLK(*U*), TDLK(*U*)
X	X	Initialize Validation Video	DLK(*U*), TDLK(*U*)
X	X	Start Validation	DLK(*U*), TDLK(*U*)
X	X	Stop Validation	DLK(*U*), TDLK(*U*)
X	X	Get Detail Version Information	DLK(*U*), TDLK(*U*)
X	X	Get FM Serial Number	DLK(*U*), TDLK(*U*)
X	X	Get Gemini Version	DLK(*U*), TDLK(*U*)
X	X	Get Serial Number	DLK(*U*), TDLK(*U*)
X	X	Get Version Information	DLK(*U*), TDLK(*U*)
X	X	Get Random Number	DLK(*U*), TDLK(*U*), SSK(*U*)
X	X	Get Critical Security Status	DLK(*U*), TDLK(*U*)
X	X	Get External Device Status	DLK(*U*), TDLK(*U*)
X	X	Get Gemini Status	DLK(*U*), TDLK(*U*)
X	X	Change User Password	DLK(*U*), TDLK(*U*), AS(*E*,*U*,*Z*)
X	X	Mute Audio	DLK(*U*), TDLK(*U*)
X	X	Mute Video	DLK(*U*), TDLK(*U*)
X	X	Pause Playback	DLK(*U*), TDLK(*U*)
X	X	Start Playback	CEK(*U*), CIK(*U*), DLK(*U*), TDLK(*U*)
X	X	Stop Playback	CIK(*Z*), DLK(*U*), TDLK(*U*)
X	X	Initialize Subtitle Decryption	DLK(*U*), TDLK(*U*)
X	X	Set/Get Date	DLK(*U*), TDLK(*U*)
	X	Delete Root Certificate	TSK(*U*), TMACS(*U*)
	X	Get Certificate Info	TSK(*U*), TMACS(*U*)
	X	Get Root Certificate	TSK(*U*), TMACS(*U*)
	X	List Root Certificate	TSK(*U*), TMACS(*U*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
	X	Retrieve Certificate	TSK(*U*), TMACS(*U*)
	X	Retrieve Root Certificate	TSK(*U*), TMACS(*U*)
	X	Store Root Certificate	TSK(*U*), TMACS(*U*)
	X	User Password	TSK(*U*), TMACS(*U*)
	X	Validation Cancel	TSK(*U*), TMACS(*U*)
	X	Validate DCP	TSK(*U*), TMACS(*U*)
	X	Validate Progress	TSK(*U*), TMACS(*U*)
	X	Validate 2	TSK(*U*), TMACS(*U*)
	X	Detail CPL 2	TSK(*U*), TMACS(*U*)
	X	Detail CPL 3	TSK(*U*), TMACS(*U*)
	X	Detail CPL 4	TSK(*U*), TMACS(*U*)
	X	Detail CPL 5	TSK(*U*), TMACS(*U*)
	X	Detail CPL 6	TSK(*U*), TMACS(*U*)
	X	List CPL	TSK(*U*), TMACS(*U*)
	X	Relate CPL	TSK(*U*), TMACS(*U*)
	X	Retrieve CPL	TSK(*U*), TMACS(*U*)
	X	Store PREPWI Begin	TSK(*U*), TMACS(*U*)
	X	Store PREPWI Cancel	TSK(*U*), TMACS(*U*)
	X	Store PWI Begin	TSK(*U*), TMACS(*U*)
	X	Store PWI Cancel	TSK(*U*), TMACS(*U*)
	X	Verify CPL	TSK(*U*), TMACS(*U*)
	X	Delete DCP	CEK(*Z*), TSK(*U*), TMACS(*U*)
	X	Get DCP Deletion Count	TSK(*U*), TMACS(*U*)
	X	List DCP	TSK(*U*), TMACS(*U*)
	X	List DCP 2	TSK(*U*), TMACS(*U*)
	X	Refresh DCP	TSK(*U*), TMACS(*U*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
	X	Refresh PWI DCP	TSK(*U*), TMACS(*U*)
	X	Retrieve PL	TSK(*U*), TMACS(*U*)
	X	Set Title	TSK(*U*), TMACS(*U*)
	X	Store DCP Begin	TSK(*U*), TMACS(*U*)
	X	Store DCP End	TSK(*U*), TMACS(*U*)
	X	Store S2S Begin	TSK(*U*), TMACS(*U*)
	X	Store S2S Cancel	TSK(*U*), TMACS(*U*)
	X	Verify PL	TSK(*U*), TMACS(*U*)
	X	Get Date	TSK(*U*), TMACS(*U*)
	X	Get Time-zone	TSK(*U*), TMACS(*U*)
	X	Get Time-zone 2	TSK(*U*), TMACS(*U*)
	X	Get Version	TSK(*U*), TMACS(*U*)
	X	Get Version 2	TSK(*U*), TMACS(*U*)
	X	Ger Version 3	TSK(*U*), TMACS(*U*)
	X	Get Audio Frequency	TSK(*U*), TMACS(*U*)
	X	Get LED	TSK(*U*), TMACS(*U*)
	X	Get LED 2	TSK(*U*), TMACS(*U*)
	X	Get Marriage Status	TSK(*U*), TMACS(*U*)
	X	Get PWI Transfer Status	TSK(*U*), TMACS(*U*)
	X	Get Rebuilding	TSK(*U*), TMACS(*U*)
	X	Get Status	TSK(*U*), TMACS(*U*)
	X	Get Status 2	TSK(*U*), TMACS(*U*)
	X	Get Status 3	TSK(*U*), TMACS(*U*)
	X	Get Tamper Status	TSK(*U*), TMACS(*U*)
	X	Get Transfer Status	TSK(*U*), TMACS(*U*)
	X	Get White Point	TSK(*U*), TMACS(*U*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
	X	Heartbeat	TSK(*U*), TMACS(*U*)
	X	Delete KDM	CEK(*Z*), TSK(*U*), TMACS(*U*)
	X	Delete KDM Specified by ID	CEK(*Z*), TSK(*U*), TMACS(*U*)
	X	Detail CPL	TSK(*U*), TMACS(*U*)
	X	Detail KDM	TSK(*U*), TMACS(*U*)
	X	Detail KDM Specified by ID	TSK(*U*), TMACS(*U*)
	X	List KDM	TSK(*U*), TMACS(*U*)
	X	List KDM specified by ID	TSK(*U*), TMACS(*U*)
	X	Relate KDM	TSK(*U*), TMACS(*U*)
	X	Relate KDM ID	TSK(*U*), TMACS(*U*)
	X	Retrieve KDM	TSK(*U*), TMACS(*U*)
	X	Store KDM	CEK(*E*,*U*), TSK(*U*), TMACS(*U*), SPK(*U*)
	X	Get Event Log	TSK(*U*), TMACS(*U*)
	X	Get Event Log 2	TSK(*U*), TMACS(*U*)
	X	List Security Log	TSK(*U*), TMACS(*U*)
	X	Retrieve Security Log	TSK(*U*), TMACS(*U*), SPK(*U*)
	X	Retrieve Security Log 2	TSK(*U*), TMACS(*U*)
	X	Snapshot	TSK(*U*), TMACS(*U*)
	X	Get Playback Status	TSK(*U*), TMACS(*U*)
	X	Get Reel	TSK(*U*), TMACS(*U*)
	X	Play Pause Execution	TSK(*U*), TMACS(*U*)
	X	Play Pause Resume	TSK(*U*), TMACS(*U*)
	X	Playback CPL Start	TSK(*U*), TMACS(*U*)
	X	Playback SPL Start	TSK(*U*), TMACS(*U*)
	X	Playback 3D CPL Start	TSK(*U*), TMACS(*U*)
	X	Playback 3D SPL Start	TSK(*U*), TMACS(*U*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
	X	Playback Step	TSK(*U*), TMACS(*U*)
	X	Playback Stop	TSK(*U*), TMACS(*U*)
	X	Get CC Delay	TSK(*U*), TMACS(*U*)
	X	Get Delay	TSK(*U*), TMACS(*U*)
	X	Get Muting	TSK(*U*), TMACS(*U*)
	X	Get Muting Mask	TSK(*U*), TMACS(*U*)
	X	Get Playback Type	TSK(*U*), TMACS(*U*)
	X	Get Position	TSK(*U*), TMACS(*U*)
	X	Get SPL	TSK(*U*), TMACS(*U*)
	X	Set Audio Frequency	TSK(*U*), TMACS(*U*)
	X	Set CC Delay	TSK(*U*), TMACS(*U*)
	X	Set Delay	TSK(*U*), TMACS(*U*)
	X	Set Muting	TSK(*U*), TMACS(*U*)
	X	Set Muting Mask	TSK(*U*), TMACS(*U*)
	X	Set Playback Type	TSK(*U*), TMACS(*U*)
	X	Set SPL	TSK(*U*), TMACS(*U*)
	X	Set Subtitle box	TSK(*U*), TMACS(*U*)
	X	Set Date	TSK(*U*), TMACS(*U*)
	X	Set Date 2	TSK(*U*), TMACS(*U*)
	X	Set External IP	TSK(*U*), TMACS(*U*)
	X	Set LED Off	TSK(*U*), TMACS(*U*)
	X	Set Network Configuration	TSK(*U*), TMACS(*U*)
	X	Set Time-zone	TSK(*U*), TMACS(*U*)
	X	Set Time-zone 2	TSK(*U*), TMACS(*U*)
	X	Delete Any	TSK(*U*), TMACS(*U*)
	X	DF	TSK(*U*), TMACS(*U*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
	X	Get Network Configuration	TSK(*U*), TMACS(*U*)
	X	List Any	TSK(*U*), TMACS(*U*)
	X	Retrieve Any	TSK(*U*), TMACS(*U*)
	X	Store Any	TSK(*U*), TMACS(*U*)
	X	Initialize Marriage	TSK(*U*), TMACS(*U*)
	X	Initialize Security	TSK(*U*), TMACS(*U*)
		Show Status	
		Self-tests	

* 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
            - SP 800-135rev1 TLS KDF 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 encapsulated 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.

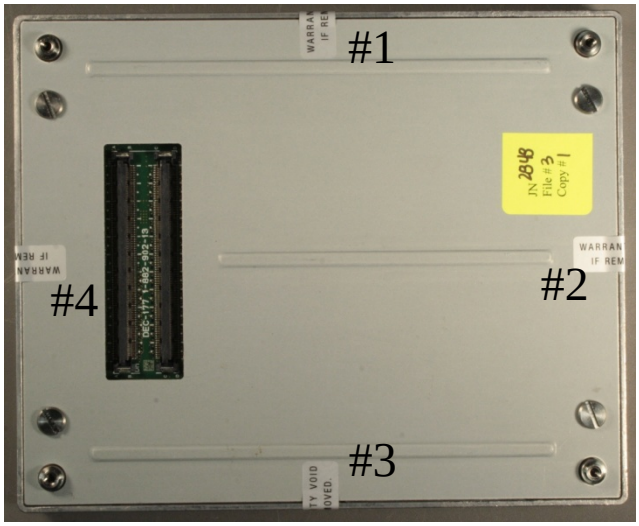


Figure 2: Tamper Evident Seal Locations

Figure 3: 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 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 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 11 - Mitigation of Other Attacks

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

11. Definitions and Acronyms

Table 12 -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.
Nov. 19, 2013	1.0.2	Added KDF as the allowed non-FIPS approved algorithm
Apr. 2, 2014	1.0.3	Added the self-test of KDF and a firmware version. Changed the name of services.
Sep. 11, 2014	1.0.4	Corrected the Nios version.