FIPS 140-2 Non-Proprietary Security Policy

Aspen

Document Version 1.5.0

Sony Corporation

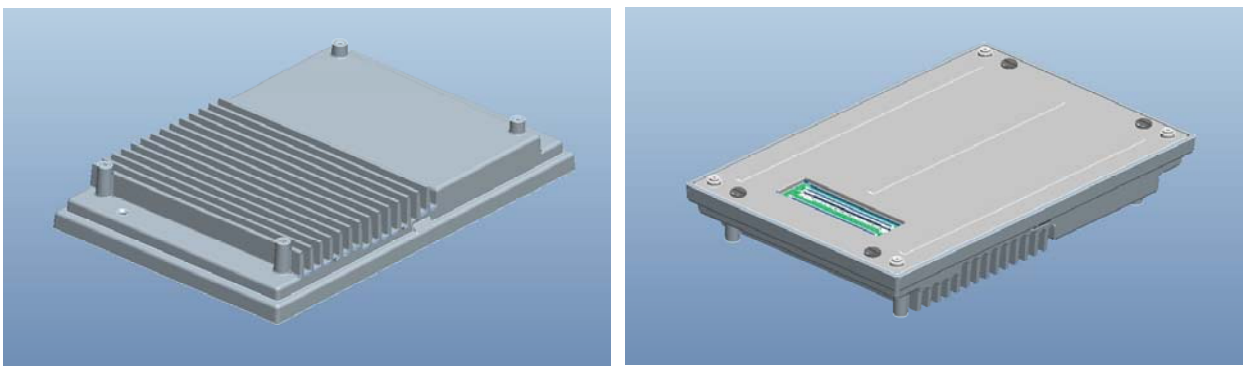
Table of Contents

1. Module Overview

The Aspen 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.

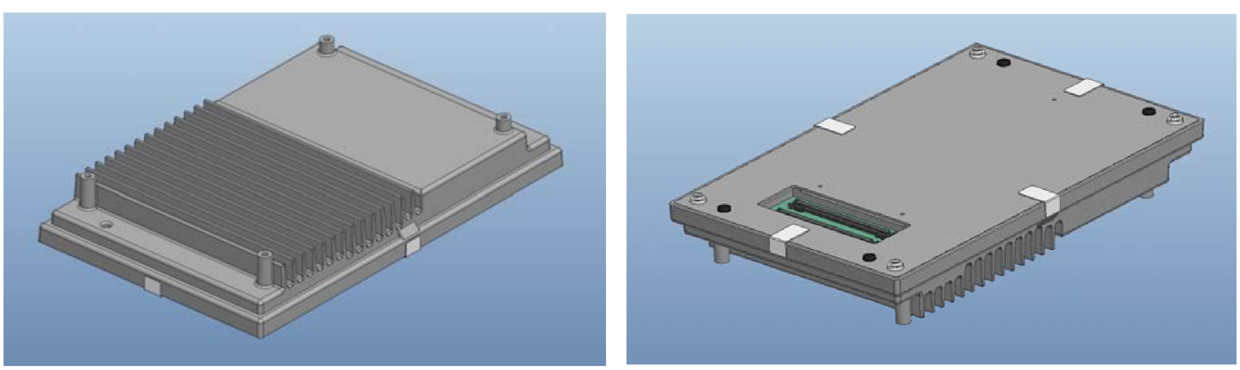
The primary purpose of the Aspen is to provide decryption, decoding/encoding of audio/video data for the digital cinema projector system in which it is used.

The illustration below shows the Aspen, along with the cryptographic boundary.



Top Side **Bottom Side**

Figure 1 - Image of the Aspen Cryptographic Module (Hardware version 1.0.0)



Top Side **Bottom Side**

Figure 2 - Image of the Aspen Cryptographic Module (Hardware version 1.1.0)

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

- Hardware versions: 1.0.0 and 1.1.0
- Firmware versions: 1.3.0, 1.4.0 and 1.5.0

Aspen firmware configuration table is as follows.

Table 1 - Aspen Firmware Configuration

Component	Firmware Component Versions		
	Version 1.3.0	Version 1.4.0	Version 1.5.0
MDC version	01.30.00	01.40.01	01.50.00
NSA version	01.21.00	01.21.00	01.21.00
CDM version	01.30.00	01.30.00	01.30.00
Kernel version	02.06.33	02.06.33	02.06.33
MBA version	01.30.00	01.40.01	01.50.00
CTU version	04.01.01	04.01.01	04.01.01
DSP version	01.00.09	01.00.09	01.00.09
Boot Loader version	01.00.00	01.00.00	01.00.00

Aspen firmware version 1.4.0 was added support for LTC output.

2. Security Level

The Aspen 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 Aspen is designed to continually operate in a FIPS approved mode of operation. The Aspen 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 Signature Generation/Verification with 2,048-bit key using SHA-256 (as per FIPS 186-2) - Certificate: #750
- RSA Signature Generation with 2,048-bit key using SHA-256, Signature Verification with 2,048-bit key using SHA-1 and SHA-256 (as per FIPS 186-2) - Certificate: #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: #1279
- SP 800-135rev1 TLS KDF using SHA-1 (as per SP 800-135rev1) - Certificate: #115

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

- RSA Encryption/Decryption 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

- MD5 for the pseudo random function in TLS
- RSA Signature Generation/Verification with 2,048-bit key using both MD5 and SHA-1 only for TLS 1.0 client authentication

The operator can be assured that the Aspen is in the approved mode by verifying that the firmware versions identified using the 'Get Version' service match each of the validated firmware component versions listed in Section 1.

3.2. Non-Approved Mode of Operation

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

4. Ports and Interfaces

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

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

In addition, the Aspen 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 Aspen supports two distinct operator roles (User and Crypto-Officer). The Aspen enforces the separation of roles using identity-based operator authentication. The Crypto-Officer and User are authenticated using the RSA 2048 signature verification algorithm.

Table 3 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	RSA Digital Certificate
Crypto-Officer	Identity-based operator authentication	RSA Digital Certificate

5.2. Authentication Mechanism

The Aspen supports an authentication mechanism.

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 Aspen within one minute is also $6000 * 2^{-112}$ ($< 2^{10} * 2^{-112} = 2^{-102}$) which is less than 1/100,000.

6. Access Control Policy

6.1. Roles and Services

Table 5 - Crypto-Officer Specific Services

Service	Description
Clear Log	Deletes all logs required by Digital Cinema Initiative (DCI) specification.
Update Start Sequence	Checks a certificate and prepares for firmware update.
Update Module	Receives a firmware image from the operator and perform firmware updating.
Update End Sequence	Ends a firmware update procedure.
Zeroization	Deletes all plaintext CSP.

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

Table 6 - Crypto-Officer and User Common Services

Service	Description
Delete KDM	Deletes Key Delivery Message (KDM) specified with Compositions Play list (CPL) ID.
Delete KDM ID	Deletes KDM specified with KDM ID.
Detail KDM ID	Outputs detailed information of KDM specified with KDM ID.
Get Audio Frequency	Outputs the audio frequency.
Get Audio Muting	Outputs audio mute information.
Get Audio Routing	Outputs the audio routing switch information.
Get Certificate	Outputs information of certificates that the module has.
Get CPL List ID	Outputs CPL playing information buffer ID of the module.
Get Date	Outputs the time and date.
Get Delay	Outputs the audio delay value.
Get LTC Mode	Outputs the Longitudinal Time Code (LTC) mode information. (Available since F/W version 1.4.0)

Service	Description
Get FM ID	Outputs the forensic mark ID.
Get Marriage Status	Outputs the current connection status with an external device.
Get MS Configuration	Outputs the Master/Slave mode of the module.
Get Playback Information	Outputs the current CPL playback status.
Get Root Certificate	Outputs information of root certificates.
Get Security Status	Outputs the current protection status of the module.
Get Status	Outputs information of various statuses.
Get Time-zone	Outputs set time-zone information.
Get Version	Outputs version information of the module.
Get White Point	Outputs the mode of the white point.
Heartbeat	Keeps the current session with an operator.
Initialize Marriage	Initializes the connection status with an external device.
Initialize PCIE Connection*	Sends a signal to an external device to reset its own status.
List KDM ID	Outputs an ID list of stored KDM and keys.
List Root Cert	Outputs a file name list of stored root certificates.
List Security Log	Outputs a file name list of stored security logs.
Play Pause Execution	Pauses playback of the current content.
Play Pause Resume	Resumes playback of the paused content.
Play Prepare Completed	Checks the current playback preparation status of an operator.
Play Prepare CPL	Prepares playback of CPL.
Play Set SPL	Reads the construction of Show Play List (SPL).
Play Step	Plays the paused content frame by frame.
Play Stop	Stops playback of the current content.
Relate KDM ID	Outputs an ID list of KDM specified with CPL ID.
Retrieve Certificate	Outputs stored certificates.
Retrieve Root Cert	Outputs stored root certificates.

Service	Description
Retrieve Security Log	Outputs stored logs required by DCI specification.
Retrieve Security Log 2	Outputs stored logs in the form of XML file.
Set AMB IP	Sets the IP address of Audio Media Block.
Set Audio Frequency	Sets the audio frequency.
Set Audio Muting	Sets the audio muting switch.
Set Audio Routing	Sets the audio routing switch.
Set Date	Sets a time of the module.
Set Date 2	Sets a time of the module.
Set Delay	Sets the audio delay value.
Set LTC Mode	Sets the LTC mode. (Available since F/W version 1.4.0)
Set MS Configuration	Switches the Master/Slave mode of the module.
Set Timed Text Key ID	Sets ID of key used for decrypting encrypted Material eXchange Format (MXF) file.
Set Time-zone	Sets time-zone.
Set White Point	Sets the mode of the white point.
Shutdown	Shuts down or reboots the module.
Snapshot	Outputs logs in the form of ZIP format.
Store KDM	Stores KDM given by an operator.
Verify CPL	Checks whether the specified CPL is playable.
Version	Checks the version of an operator interface.

* Only firmware version 1.2.1 and 1.2.2 support.

Table 7 - Unauthenticated Services

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

6.2. Definition of Critical Security Parameters (CSPs)

The following CSPs are included in the Aspen.

- Contents Encryption Key (CEK) - AES key used to decrypt contents.
- Content Integrity Key (CIK) - HMAC-SHA-1 key for integrity check of contents.
- Aux Data Key (ADK) – AES key used to decrypt Aux data.
- Master Key (MK) - AES key used to protect all stored CSPs.
- 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 used for generation of a digital signature for the log data and TLS session data.
- Device Private Key (DPK) - RSA private key used for decryption of CEK and decryption of wrapped cryptographic keys which are entered into the Aspen 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 RNGs.

6.3. Definition of Public Keys

The following are the public keys contained in the Aspen:

- Aspen Manufacturer Public Key - RSASSA 2048 public key used to verify a certificate chain of trust.
- Aspen Trusted Public Key - RSASSA 2048 public key used to verify a certificate chain of trust.
- RSA Verifying Key - RSASSA 2048 public key corresponding to the RSA Signing Key.

- Device Public Key - RSAES 2048 public key corresponding to the Device 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.
- Aux Data Processor Public Key – RSAES 2048 public key used to authenticate an Aux Data Processor.
- KDM Issuer Public Key - RSASSA 2048 public key used to verify signature of KDM.

6.4. Definition of CSP Access Modes

Table 8 defines the relationship between CSP access modes and module services. The 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 Aspen.
- **Output** (***O***): Outputs the CSP from the Aspen.
- **Zeroize** (***Z***): Removes the CSP.

Table 8 - CSP Access Rights within Roles & Services

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
X		Clear Log	TSK(*U*), TMACS(*U*)
X		Update End Sequence	TSK(*U*), TMACS(*U*)
X		Update Module	TSK(*U*), TMACS(*U*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
X		Update Start Sequence	TSK(*U*), TMACS(*U*)
X		Zeroization	CEK(*Z*), CIK(*Z*), ADK(*Z*), MK(*Z*), RSK(*Z*), DPK(*Z*), TSK(*UZ*), TMACS(*UZ*), TPS(*Z*), TMS(*Z*), PS(*Z*), SSK(*Z*)
X	X	Delete KDM	CEK(*Z*), CIK(*Z*), ADK(*Z*), TSK(*U*), TMACS(*U*)
X	X	Delete KDM ID	CEK(*Z*), CIK(*Z*), ADK(*Z*), TSK(*U*), TMACS(*U*)
X	X	Detail KDM ID	TSK(*U*), TMACS(*U*)
X	X	Get Audio Frequency	TSK(*U*), TMACS(*U*)
X	X	Get Audio Muting	TSK(*U*), TMACS(*U*)
X	X	Get Audio Routing	TSK(*U*), TMACS(*U*)
X	X	Get Certificate	TSK(*U*), TMACS(*U*)
X	X	Get CPL List ID	TSK(*U*), TMACS(*U*)
X	X	Get Date	TSK(*U*), TMACS(*U*)
X	X	Get Delay	TSK(*U*), TMACS(*U*)
X	X	Get LTC Mode	TSK(*U*), TMACS(*U*)
X	X	Get FM ID	TSK(*U*), TMACS(*U*)
X	X	Get Marriage Status	TSK(*U*), TMACS(*U*)
X	X	Get MS Configuration	TSK(*U*), TMACS(*U*)
X	X	Get Playback Information	TSK(*U*), TMACS(*U*)
X	X	Get Root Certificate	TSK(*U*), TMACS(*U*)
X	X	Get Security Status	TSK(*U*), TMACS(*U*)
X	X	Get Status	TSK(*U*), TMACS(*U*)
X	X	Get Time-zone	TSK(*U*), TMACS(*U*)
X	X	Get Version	TSK(*U*), TMACS(*U*)
X	X	Get White Point	TSK(*U*), TMACS(*U*)
X	X	Heartbeat	TSK(*U*), TMACS(*U*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
X	X	Initialize Marriage	RSK(*U*), TSK(*GU*), TMACS(*GU*), TPS(*GOU*), TMS(*GU*), PS(*GU*), SSK(*U*)
X	X	Initialize PCIE Connection	TSK(*U*), TMACS(*U*)
X	X	List KDM ID	TSK(*U*), TMACS(*U*)
X	X	List Root Certificate	TSK(*U*), TMACS(*U*)
X	X	List Security Log	RSK(*U*), TSK(*U*), TMACS(*U*)
X	X	Play Pause Execution	TSK(*U*), TMACS(*U*)
X	X	Play Pause Resume	TSK(*U*), TMACS(*U*)
X	X	Play Prepare Completed	CEK(*U*), CIK(*U*), TSK(*U*), TMACS(*U*)
X	X	Play Prepare CPL	TSK(*U*), TMACS(*U*), ADK(*O*)
X	X	Play Set SPL	TSK(*U*), TMACS(*U*)
X	X	Play Step	TSK(*U*), TMACS(*U*)
X	X	Play Stop	TSK(*U*), TMACS(*U*)
X	X	Relate KDM ID	TSK(*U*), TMACS(*U*)
X	X	Retrieve Certificate	TSK(*U*), TMACS(*U*)
X	X	Retrieve Root Certificate	TSK(*U*), TMACS(*U*)
X	X	Retrieve Security Log	TSK(*U*), TMACS(*U*)
X	X	Retrieve Security Log 2	RSK(*U*), TSK(*U*), TMACS(*U*)
X	X	Set AMB IP	RSK(*U*), TSK(*GU*), TMACS(*GU*), TPS(*GOU*), TMS(*GU*), PS(*GU*), SSK(*U*)
X	X	Set Audio Frequency	TSK(*U*), TMACS(*U*)
X	X	Set Audio Muting	TSK(*U*), TMACS(*U*)
X	X	Set Audio Routing	TSK(*U*), TMACS(*U*)
X	X	Set Date	TSK(*U*), TMACS(*U*)
X	X	Set Date 2	TSK(*U*), TMACS(*U*)

Role		Service Name	CSP (*Access Mode*)
C.O.	User		
X	X	Set Delay	TSK(*U*), TMACS(*U*)
X	X	Set LTC Mode	TSK(*U*), TMACS(*U*)
X	X	Set MS Configuration	TSK(*U*), TMACS(*U*)
X	X	Set Timed Text Key ID	TSK(*U*), TMACS(*U*)
X	X	Set Time-zone	TSK(*U*), TMACS(*U*)
X	X	Set White Point	TSK(*U*), TMACS(*U*)
X	X	Shutdown	TSK(*U*), TMACS(*U*)
X	X	Snapshot	TSK(*U*), TMACS(*U*)
X	X	Store KDM	CEK(*UE*), CIK(*G*), ADK(*UE*), MK(*U*), SPK(*U*), TSK(*U*), TMACS(*U*), SSK(*U*)
X	X	Verify CPL	TSK(*U*), TMACS(*U*)
X	X	Version	TSK(*U*), TMACS(*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 Aspen does not contain a modifiable operational environment.

8. Security Rules

The Aspen 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 Aspen shall provide two distinct operator roles. These are the User role, and the Crypto-Officer role.
2. The Aspen shall provide identity-based authentication.
3. When the Aspen has not been placed in an authenticated role, the operator shall not have access to any cryptographic services.
4. The Aspen 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 (Encryption/Decryption)
            - RSA PKCS#1 v1.5 Pair-wise Consistency Test (Encryption/Decryption)

ii. Conditional Self-Tests:

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

b. Firmware Load Test (RSA Digital Signature Verification)

5. The operator shall be capable of commanding the Aspen 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 Aspen.

9. The Aspen does not support concurrent operators.

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

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

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

13. RSA Signature Generation/Verification using both MD5 and SHA-1 is only used for TLS 1.0 client Authentication.

14. The Aspen only supports the electronic entry form of key establishment.

15. RSA Signing Key is used for TLS establishment when the Aspen behaves as a TLS client in communication with an external device.

16. Device Private Key is used for TLS establishment when the Aspen behaves as a TLS server in communication with an external device.

9. Physical Security Policy

9.1. Physical Security Mechanisms

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

- Production-grade components,
- The enclosure of Aspen hardware version 1.0.0 does not have any removable cover, door or ventilation slits. When the power supply from the outside is lost, all plaintext CSPs within the Aspen are zeroized,
- The enclosure of Aspen hardware version 1.1.0 has a removable cover that four tamper evidence seals (See **Figure 3** and **Figure 4**) are sealed by Sony in secure manufacturing facility. When the cover is removed or the power supply from the outside is lost, all plaintext CSPs within the Aspen 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. Hardness testing was performed at ambient temperature.

Figure 3 – Image of Tamper Evidence Seal

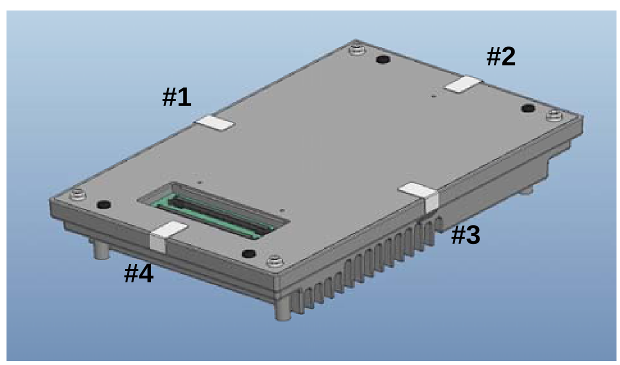


Figure 4 – Seal Location (H/W v1.1.0)

9.2. Operator Actions

Due to the intended deployment environment for the Aspen, 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 (Hardware version 1.0.0)

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Non-Removable Enclosure	Every startup and reboot.	Inspect for scratches or deformation of the metal case. If such evidence is found, user should not use the module.
Tamper detection	Every startup and reboot.	If the module was zeroized, user should return it to Sony.

Table 10 - Inspection/Testing of Physical Security Mechanisms (Hardware version 1.1.0)

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard Removable Enclosure	Every startup and reboot.	Inspect for scratches or deformation of the metal case. If such evidence is found, user should not use the module.
Tamper Evidence Seals	Every startup and reboot.	Inspect for curled corner, peel, rips, or appearance of words “WARRANTY VOID IF REMOVED”. If found such evidences, user should not use the module.
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 Aspen 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 & **T**amper 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
KDF	**K**ey **D**erivation **F**unction
KDM	**K**ey **D**elivery **M**essage
LTC	**L**ongitudinal **(L**iner) **T**ime **C**ode
MBA	**M**edia **B**lock **A**pplication
MDC	**M**edia **D**ecrypt & **D**ecode **C**ontroller
NSA	**N**ios & **A**udio Mapping
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

Term	Definition
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
SHA	**S**ecure **H**ash **A**lgorithm
SPL	**S**how **P**lay **L**ist
TLS	**T**ransport **L**ayer **S**ecurity

12. Revision History

Date	Version	Description
Feb. 09, 2015	1.3.0	Initial public release for firmware version 1.3.0.
Apr. 15, 2015	1.4.0	Added firmware version 1.4.0. (Get/Set LTC Mode services are added.)
Sep. 18, 2015	1.5.0	Added firmware version 1.5.0. (bug fix release)