Sony Security Module

Security Policy

Document Version 1.0.0

Sony Corporation

FIPS 140-2 Non-Proprietary

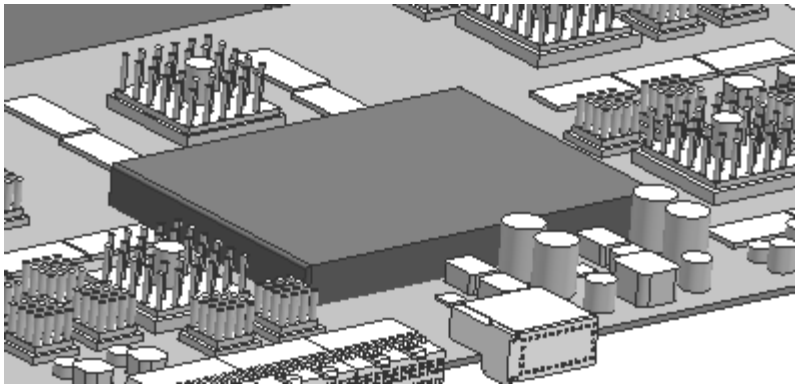
TABLE OF CONTENTS

1. Module Overview

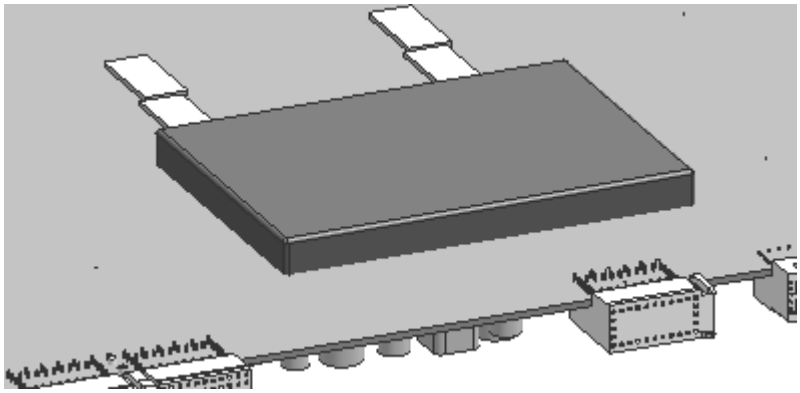
The Sony Security Module (SSM) is a multi-chip embedded cryptographic module that is encased in a hard opaque commercial grade metal case. The cryptographic boundary is defined as the entire metal case perimeter, including all hardware, software, and firmware encapsulated within. The interfaces are all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

The primary purpose of the Sony Security Module 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 intended cryptographic boundary.



Top



Bottom

Figure 1 – Image of the Cryptographic Module

The SSM is validated hardware version 1.0.1 / firmware version 1.0.1.

The SSM firmware configurable hierarchy is as follows:

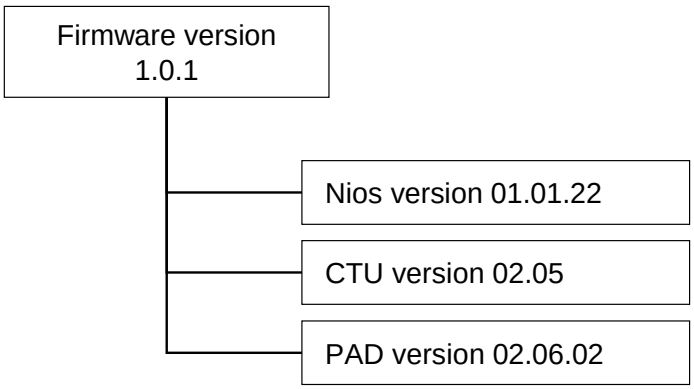


Figure 2 – SSM firmware configuration

2. Security Level

The cryptographic module 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
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 FIPS non-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 - Certificates : #901 and #1470
  - ECB mode of operation - Certificate : #902
- SHA-1 with 160 bit hash value (as per FIPS 180-3) - Certificates : #882 and #1330
- SHA-256 with 256 bit hash value (as per FIPS 180-3) - Certificate : #882
- RSA Key Generation and Signature Generation/Verification with 2,048 bit keys (as per PKCS#1 v1.5) - Certificate : #724
- ANSI X9.31 RNG using TDES-2Key (as per ANSI X9.31) - Certificate : #517
- FIPS 186-2 RNG using SHA-1 (as per FIPS 186-2) - Certificate : #804
- HMAC-SHA-1 with 160 bit key (as per FIPS 198) - Certificates : #865 and #866

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)
- HMAC-MD5 for the pseudo random function in TLS 1.0.
- NDRNG for the seeding of the above RNG

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

4. Ports and Interfaces

The SSM'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
- Power Input

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

The module has six status output interfaces. The operator can identify the status of the SSM by monitoring those interfaces.

5. Identification and Authentication Policy

Assumption of roles

The SSM 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 operator is authenticated using the RSA 2048 signature verification algorithm or an ID and password.

Table 2 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User (Field)	Identity-based operator authentication	• RSA Digital Certificate • ID and Password
Crypto-Officer (Factory)	Identity-based operator authentication	• RSA Digital Certificate • ID and Password

Table 3 - Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
RSA Digital Certificate Verification	The authentication is based on RSA 2048, which has an equivalent strength of 112-bits[1]. 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 Password Verification	The SSM accepts 64 possible characters and a minimum 8-characters for a Password, 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.

[1] Reference SP800-57

6. Access Control Policy

Roles and Services

Table 4 - Crypto-Officer Specific Service

Service	Description
Control Data	Sets AES shared key and Public Key Certificate
Firmware Update	Updates the firmware of the module*
User Control	Edits a user ID and Password
Generate RSA Key	Generates a RSA Key pair
Zeroization	Destroys all Critical Security Parameters

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

Table 5 - Crypto-Officer and User Common Service

Service	Description
KDM Control	Controls KDM (import, Clear)
Playback	Controls the playback of Contents (Video and Audio)
Set Time	Sets the RTC time
Get Time	Obtains the RTC time
Get Status	Obtains the status of the module as well as the version number
External Security Control	Obtains the status of external devices connected to SSM.
Sign Data	Signs data
Get Session Data	Decrypts the data needed to establish a TLS session
Get Random Number	Provides a random number
Get Certificate	Obtains a certificate
Set Log	Sets external log data

Service	Description
Get Log	Obtains log data
Change Password	Changes the personal password (C.O. can change all user passwords)
Contents Validate	Validates DCP

Table 6 - Unauthenticated Service

Service	Description
Show Status	Obtains the module status

Definition of Critical Security Parameters (CSPs)

The following are CSPs contained in the module:

- Contents Encryption Keys (CEK) – AES key used to decrypt media data.
- Content Integrity Key(CIK) – The HMAC seed key used to check the integrity of contents.
- Key Encryption Key (KEK) – AES key used to protect RSK, DPK, and TPK.
- Device Link Key (DLK) – AES key used to protect a channel with the SSM Control Procedure.
- Temporary Device Link Key (TDLK) – Temporary AES key used to protect a channel with the SSM Control Procedure.
- 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.
- Device Private Key (DPK) – RSA private key used to decrypt wrapped cryptographic keys entered into the module.
- TLS Private Key (TPK) – RSA private key for 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.
- Authentication Secrets (AS) – The User and Crypto-Officer password used to authenticate the operator.
- Seed and Seed Key (SSK) – The secret values necessary for the FIPS approved RNG.

Definition of Public Keys:

The following are the public keys contained in the module:

- SSM Manufacturer Public Key – RSASSA 2048 public key used to verify a certificate chain of trust.
- SSM Trusted Public Key – RSASSA 2048-bit public key used to verify a certificate chain of trust.
- RSA Verifying Key – RSASSA public key corresponded to the RSA Signing Key.

- Public Key for F/W Upgrade – RSASSA public key used to verify the digital signature over the firmware image to be upgraded.
- Operator Public Key – RSAES public key used to authenticate operators.
- Device Public Key – RSAES public key corresponded to the Device Private Key.
- TLS Public Key – RSAES public key corresponded to the TLS Private Key.

Definition of CSPs Modes of Access

Table 7 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 the 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 7 - CSP Access Rights within Roles & Services

Role		Service	CSPs
C.O.	User		
X		**Control Data**	KEK(E), DLK(E,U), TDLK(U), TSK(U), TMACS(U), RSK(U), DPK(U), TPK(U)
X		**Firmware Update**	DLK(U), TDLK(U), TSK(U), TMACS(U)
X		**User Control**	DLK(U), TDLK(U), TSK(U), TMACS(U), AS(E,Z)
X		**Generate RSA Key**	KEK(U), DLK(U), TDLK(U), TSK(U), TMACS(U), RSK(G), DPK(G), TPK(G), SSK(U)
X		**Zeroization**	CEK(Z), CIK(Z), KEK(Z), DLK(Z), TDLK(Z), TSK(Z), TMACS(Z), RSK(Z), DPK(Z), TPK(Z), TPS(Z), TMS(Z), PS(Z), SSK(Z)
X	X	**KDM Control**	CEK(E,Z), DLK(E,U), TDLK(U), DPK(U), TSK(U), TMACS(U), SSK(U)

Role		Service	CSPs
C.O.	**User**		
X	X	**Playback**	CEK(U), CIK(G,U,Z), DLK(U), TDLK(U), TSK(U), TMACS(U), SSK(U)
X	X	**Set Time**	DLK(U), TDLK(U), TSK(U), TMACS(U)
X	X	**Get Time**	DLK(U), TDLK(U), TSK(U), TMACS(U)
X	X	**Get Status**	DLK(U), TDLK(U), TSK(U), TMACS(U)
X	X	**External Security Control**	DLK(U), TDLK(U), TSK(U), TMACS(U)
X	X	**Sign Data**	DLK(U), TDLK(U), TSK(U), TMACS(U), RSK(U)
X	X	**Get Session Data**	DLK(U), TDLK(U), TSK(U), TMACS(U)
X	X	**Get Random Number**	DLK(U), TDLK(U), TSK(U), TMACS(U), SSK(U)
X	X	**Get Certificate**	DLK(U), TDLK(U), TSK(U), TMACS(U)
X	X	**Set Log**	DLK(U), TDLK(U), TSK(U), TMACS(U)
X	X	**Get Log**	DLK(U), TDLK(U), TSK(U), TMACS(U)
X	X	**Change Password**	DLK(U), TDLK(U), TSK(U), TMACS(U), AS(E,U)
X	X	**Contents Validate**	DLK(U), TDLK(U), TSK(U), TMACS(U)
-	-	**Show Status**	

* 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 Sony Security 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 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
   i. RSA OAEP Pair-wise Consistency Test
   j. RSA PKCS#1 v1.5 Pair-wise Consistency Test
2. Firmware Integrity Test (CRC-32)
3. Critical Functions Test:
   a. RAM Check (SD-RAM, DP-RAM)

B. Conditional Self-Tests:

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

   2. RSA Pair-wise Consistency Test (if internal generation is being done)
   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 multiple concurrent operators of 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. 2-key TDES is used in DRNG only, and is not used to encrypt data.
13. HMAC-MD5 is only used in TLS, and is not used to verify any other data.

9. Physical Security Policy

Physical Security Mechanisms

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

- Production-grade components,
- The enclosure does not have a removable cover, door or ventilation slits,
- The enclosure is opaque and provides tamper evidence,
- The enclosure is sufficiently hard, providing tamper resistance 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 8 - Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard Non-Removable Enclosure	To be determined by the end user	Unexpected chips, scratches, or deformation of the metal case

10. Policy on Mitigation of Other Attacks

The module was not designed to mitigate other attacks. Therefore, this section is not applicable.

Table 9 - Mitigation of Other Attacks

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

11. Definitions and Acronyms

Term	Definition
AES	Advanced Encryption Standard
CSP	Critical Security Parameter
CTU	Counter Tampering & Tamper Detection Unit
DCI	Digital Cinema Initiative
DCP	Digital Cinema Package
DRNG	Deterministic RNG
EMI / EMC	Electromagnetic Interference / Electromagnetic Compatibility
HMAC	Hash-based Message Authentication Code
KDM	Key Delivery Message
Nios	Embedding processer that runs within the PAD (FPGA)
OAEP	Optimal Asymmetric Encryption Padding
PAD	FPGA that processes video and audio data
PKCS	Public Key Cryptography Standards
PRF	Pseudo Random Function
RNG	Random Number Generator
RSA	Rivest-Shamir-Adleman
RTC	Real Time Clock
SHA	Secure Hash Algorithm
SSM	Sony Security Module
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security

12. Revision History

Date	Version	Description
Sep. 28, 2010	1.0.0	Initial release