# 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 being employed.

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

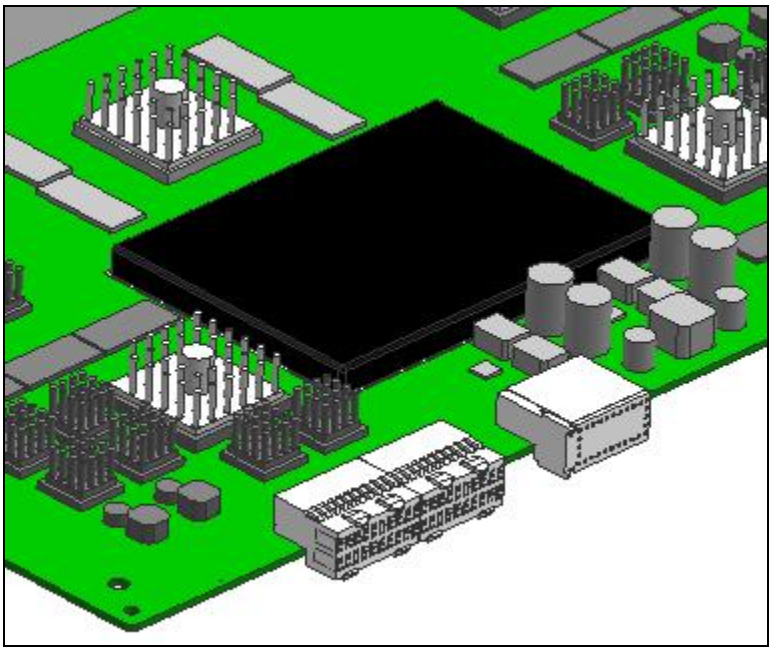

**Figure 1 – Image of the Cryptographic Module**

The SSM is validated in the following hardware / firmware version;

| Hardware version | Firmware version |
|---|---|
| 1.0.0 | 1.0.0 |

The SSM firmware configurable hierarchy is as follows;

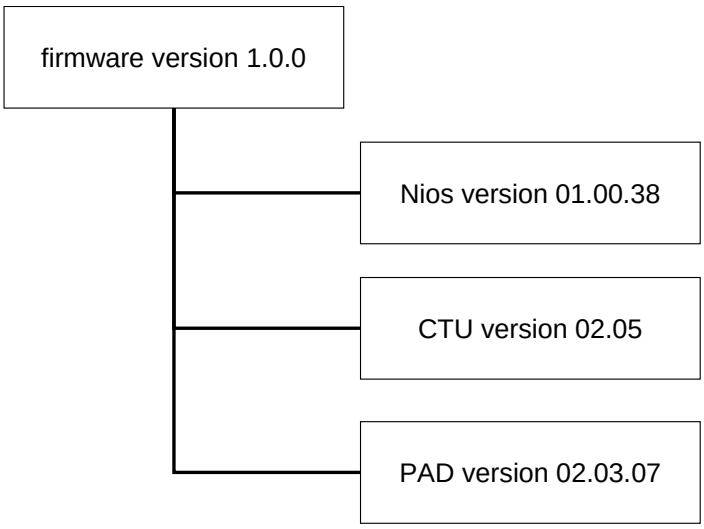


**Figure 2 – SSM firmware configuration.**

# 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 | 3 |
| Roles, Services and Authentication | 3 |
| Finite State Model | 2 |
| Physical Security | 3 |
| Operational Environment | N/A |
| Cryptographic Key Management | 3 |
| 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 always 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 (Decrypt only) - Certificate : #901
  - ECB mode of operation - Certificate : #902
- SHA-1 with 160 bit hash value (as per FIPS 180-2) - Certificate : #882
- SHA-256 with 256 bit hash value (as per FIPS 180-2) - Certificate : #882
- RSA Signature Generation/Verification with 2048 bit keys (as per PKCS#1 v1.5) - Certificate : #437
- ANSI X9.31 RNG using TDES-2Key (as per ANSI X9.31) - Certificate : #517

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 above RNG

By verifying that the firmware versions identified using the 'Get Status' 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 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 status output interfaces are connected to seven LEDs (three onboard LEDs and four Front Panel LEDs) on the board which SSM is put on and the status of SSM are indicated by them.

# 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 Crypto-Officer is authenticated using the RSA 2048 signature verification algorithm or the ID and password.

**Table 2 - Roles and Required Identification and Authentication**

| Role | Type of Authentication | Authentication Data |
|---|---|---|
| User | Identity-based operator authentication | ID and Password |
| Crypto-Officer | Identity-based operator authentication | • RSA Digital Certificate<br>• 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.<br><br>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 minimum 8-digits 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.<br><br>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 a 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 |

| Service | Description |
|---|---|
| Set Log | Sets a external log data |
| Get Log | Obtains a log data |
| Change Password | Change the own password (C.O. can change the all user password) |

**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.
- Key Encryption Key (KEK) – AES Key used to protect RSK, DPK, and TPK.
- Device Link Key for SSM CtrlProc (DLKC) – AES key used to protect a channel with the SSM Control Procedure.
- Temporary Device Link Key for SSM CtrlProc (TDLKC) – Temporary AES key used to protect a channel with the SSM Control Procedure.
- 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.
- Authentication Secrets (AS) – The secret information necessary 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.
- 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.
- C.O. Public Key – RSAES public key used to authenticate the C.O.
- 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 | | CEK | KEK | DLKC | TDLKC | RSK | DPK | TPK | AS | SSK |
| X | | **Control Data** | | *E* | *E,U* | *E,U* | *G,U* | *G,U* | *G,U* | | |
| X | | **Firmware Update** | | | *U* | *U* | | | | | |
| X | | **User Control** | | | *U* | *U* | | | | *E,Z* | |
| X | | **Generate RSA Key** | | *U* | | | *G* | *G* | *G* | | *U* |
| X | | **Zeroization** | *Z* | *Z* | *Z* | *Z* | *Z* | *Z* | *Z* | | *Z* |
| X | X | **KDM Control** | *E,Z* | | *U* | *U* | | *U* | | | *U* |
| X | X | **Playback** | *U* | | *U* | *U* | | | | | |
| X | X | **Set Time** | | | *U* | *U* | | | | | |
| X | X | **Get Time** | | | *U* | *U* | | | | | |
| X | X | **Get Status** | | | *U* | *U* | | | | | |
| X | X | **External Security Control** | | | *U* | *U* | | | | | |
| X | X | **Sign Data** | | | *U* | *U* | *U* | | | | *U* |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| X | X | **Get Session Data** | | | *U* | *U* | | | *U* | | *U* |
| X | X | **Get Random Number** | | | *U* | *U* | | | | | *U* |
| X | X | **Get Certificate** | | | *U* | *U* | | | | | |
| X | X | **Set Log** | | | *U* | *U* | | | | | |
| X | X | **Get Log** | | | *U* | *U* | | | | | |
| X | X | **Change Password** | | | *U* | *U* | | | | *E,U* | |
| | | **Show Status** | | | | | | | | | |

# 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:
   a. AES 128 CBC Decryption Known-Answer Test
   b. AES 128 ECB Encryption/Decryption Known-Answer Test
   c. RNG Known-Answer Test
   d. SHA-1 Known-Answer Test
   e. SHA-256 Known-Answer Test
   f. RSA PKCS#1 v1.5 Signature Generation/Verification Known-Answer Test
   g. RSA OAEP 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
   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 by recycling power.
6. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. The module shall not support multiple concurrent operators.
9. The module shall not support a bypass capability or a maintenance interface.
10. If a non-FIPS validated firmware version is loaded onto the module, then the module is no longer a FIPS validated module.

# 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 any removable cover, door and 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 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 end user | Unexpected chips, scratches, or deformation of the metal case |

# 10. Mitigation of Other Attacks Policy

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

**Table 9 – Mitigation of Other Attack**

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

# 11. Definitions and Acronyms

| Term | Definition |
|---|---|
| **CFG** | Configuration |
| **CTU** | Counter Tampering & Tamper Detection Unit |
| **EPCS** | Serial configuration device, FPGA configuration ROM |
| **LVDS** | Low Voltage Differential Signaling. A communication protocol |
| **MFP** | Mix Finger Print. A module that provides the MIX function for subtitles and pictures (superimposing the subtitles onto the video) and video finger print function |
| **Nios** | Embedding processer that runs within the PAD (FPGA) |
| **OAEP** | Optimal Asymmetric Encryption Padding |
| **PAD** | FPGA that processes video and audio data |
| **DCI** | Digital Cinema Initiative |
| **DCP** | Digital Cinema Package |
| **SSM** | Sony Security Module |
| **SMS** | Screen Management System |
| **DMX** | Demultiplexer |
| **AES/EBU** | AES/EBU (Audio Engineering Society / European Broadcasting Union) is one of the standards of digital audio. |
| **RTC** | Real Time Clock |

# 12. Revision History

| Date | Version | Description |
|---|---|---|
| July 8, 2009 | 1.0.0 | Initial release |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |