FIPS 140-2 Non-Proprietary Security Policy

Granada

Document Version 1.0.1

Sony Imaging Products & Solutions Inc.

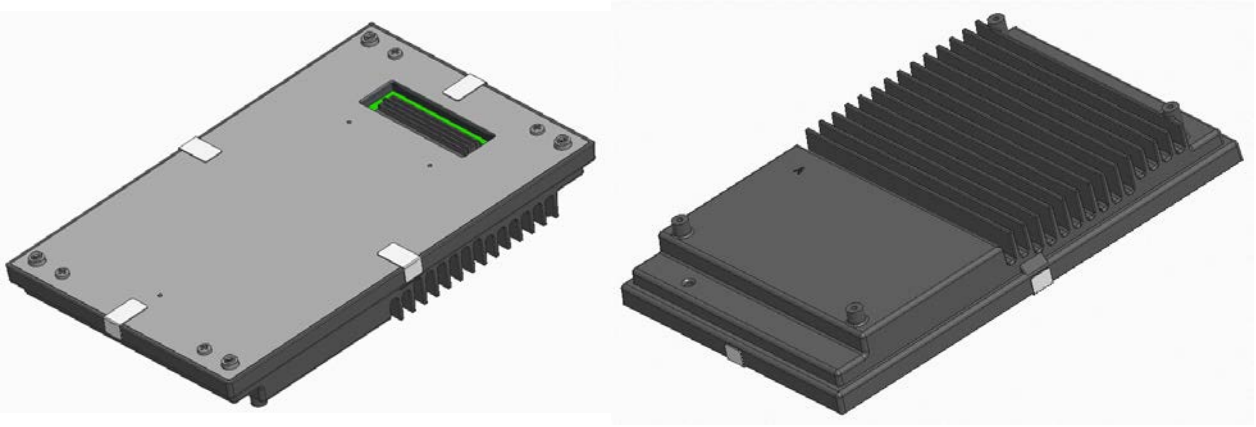
Table of Contents

1. Module Overview

The Granada 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 Granada 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 Granada, along with the cryptographic boundary.



Top Side **Bottom Side**

Figure 1 - Image of the Granada Cryptographic Module

This document is written about the following validated hardware / firmware version of Granada:

- Hardware version: 1.0.0
- Firmware version: 1.0.0

Granada firmware configuration table is as follows.

Table 1 - Granada Firmware Configuration

Firmware Version	Component Versions							
	MDC	DSP	NSA	MAGU	CTU	Kernel	MBA	Boot Loader
1.0.0	02.00.11	01.00.09	01.21.00	01.00.02	04.01.02	02.06.33	02.00.04	01.00.00

2. Security Level

The Granada 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	2
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 Granada is designed to continually operate in a FIPS approved mode of operation. The Granada supports the following FIPS approved cryptographic algorithms:

Table 3 – Approved Mode of Operation

Cert	Algorithm	Imp.	Mode	Description	Use / Caveats
5639	AES [197]	SH	ECB, CBC [38A]	Key size: 128 bit	Encrypt, Decrypt
5640		KU1	ECB, CBC [38A]	Key size: 128 bit	Encrypt, Decrypt
5642		KU2	CBC [38A]	Key size: 128 bit	Decrypt
5641		KU1	KW [38F]	Key size: 128 bit	Encrypt, Decrypt
VA	CKG [IG D.12]		[133] Section 7.3 Derivation of symmetric keys from a shared secret.		Key Generation
2037	CVL: TLS[1] [135]	SH	V1.0/1.1	SHA-1	Key Derivation
2275	DRBG [90A]	SH	Hash	SHA-256	Random Bit Generation
3756	HMAC [198]	SH	SHA-1	Key size = 160 bit	Message Authentication
3757		KU	SHA-1	Key size = 128 bit	Message Authentication
5639 3756	KTS: AES and HMAC [38F]	SH	key establishment methodology provides 112-bit of encryption strength		Key establishment
3034	RSA [186]	KU	PKCS1_v1.5	n=2048 SHA-256	Signature Generation, Signature Verification
3033		SHKU	Appendix B.3.3	n=2048 fixed e	Key Generation
			PKCS1_v1.5	n=2048 SHA-256	Signature Generation
				n=2048 SHA-1, SHA-256	Signature Verification
1365	SHS [180]	C	SHA-1 SHA-256		Message Digest Gen
4522		SH	SHA-1 SHA-256		Message Digest Gen

4524		KU1	SHA-256		Message Digest Gen
4523		KU2	SHA-1		Message Digest Gen

[1] No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP. The module uses the TLS_RSA_WITH_AES_128_CBC_SHA cipher suite.

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

- RSA Encryption/Decryption (Key wrapping; key establishment methodology provides 112-bit of encryption strength)
- NDRNG for the seeding of the DRBG. 64 bits per access used to provide > 128 bits of entropy to seed the Hash DRBG.
- MD5 (no security claimed) for the pseudo random function in TLS [IG 1.23 example 2aD.2]
- RSA Signature Generation/Verification with 2048-bit key using both MD5 and SHA-1 only for TLS 1.0 client authentication

The operator can be assured that the Granada 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 Granada does not support a non-FIPS Approved mode of operation.

4. Ports and Interfaces

The physical interfaces for Granada 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 Granada 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 Granada supports two distinct operator roles (User and Crypto-Officer). The Granada 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 4 - 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 Granada supports authentication via TLS client based certificates.

Table 5 - 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. 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 Granada within one minute is $6000 * 2^{-112}$ ($< 2^{13} * 2^{-112} = 2^{-99}$) which is less than 1/100,000.

6. Access Control Policy

6.1. Roles and Services

Table 6 - 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 performs firmware updating.
Update End Sequence	Ends a firmware update procedure.
Zeroization	Deletes all plaintext CSPs.

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

Table 7 - 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.
Detail KDM ID CPC	Obtains detailed information of KDM linking CPL ID.
Establish TLS session	Authenticates and establishes secure TLS session.
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.

Service	Description
Get Delay	Outputs the audio delay value.
Get LTC Mode	Outputs the Longitudinal Time Code (LTC) mode information.
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.
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.

Service	Description
Retrieve Root Cert	Outputs stored root certificates.
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.
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.

Table 8 - 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 Granada.

- Contents Encryption Key (CEK) - AES 128-bit key used to decrypt contents.
- Content Integrity Key (CIK) - HMAC-SHA-1 128-bit key for integrity check of contents.
- Aux Data Key (ADK) - AES 128-bit key used to decrypt Aux data.
- Master Key (MK) - AES 128-bit key used to protect all stored CSPs.
- License Key (LK) - AES 128-bit key used for decryption of KDM.
- TLS Session Key (TSK) - AES 128-bit key established in TLS.
- TLS MAC Secret (TMACS) - HMAC-SHA-1 160-bit key established in TLS.
- RSA Signing Key (RSK) - RSA 2048-bit private key used for generation of a digital signature for the log data and TLS session data.
- Device Private Key (DPK) - RSA 2048-bit private key used for decryption of CEK and decryption of wrapped cryptographic keys which are entered into the Granada in TLS.
- Reserved Private Key (RPK) - RSA 2048-bit private key which is not used in the module.
- TLS Premaster Secret (TPS) - The 48-Byte parameter used for key establishment in TLS.
- TLS Master Secret (TMS) - The 48-Byte parameter used for key establishment in TLS.
- PRF State (PS) - The 24-Byte internal state used for key establishment in TLS.
- Entropy Input (EI) - The entropy input used to seed the FIPS approved Hash_DRBG.
- DRBG State (DS) - The V and C values of the internal working state of the Hash_DRBG.

6.3. Definition of Public Keys

The following are the public keys contained in the Granada:

- Granada Manufacturer Public Key (GMPK) - RSASSA 2048 public key used to verify a certificate chain of trust.
- Granada Trusted Public Key (GTPK) - RSASSA 2048 public key used to verify a certificate chain of

trust.

- RSA Verifying Key (RVK) - RSASSA 2048 public key corresponding to the RSA Signing Key.
- Device Public Key (DPBK) - RSAES 2048 public key corresponding to the Device Private Key.
- Public Key for F/W Upgrade (FWUK) - RSASSA 2048 public key used to verify the digital signature over the firmware image to be upgraded.
- Operator Public Key (OPK) - RSASSA 2048 public key used to authenticate operators.
- Projector Public Key (PPK) - RSAES 2048 public key used to authenticate an external device.
- Aux Data Processor Public Key (ADPPK) – RSAES 2048 public key used to authenticate an Aux Data Processor.
- KDM Issuer Public Key (KIPK) - RSASSA 2048 public key used to verify signature of KDM.
- Reserved Public Key (RPBK) – RSA 2048 public key which is not used.

6.4. Definition of CSP Access Modes

Table 9 defines the relationship between CSP access modes and module services. The 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 Granada.
- **Output (*O*)**: Outputs the CSP from the Granada.
- **Zeroize (*Z*)**: Removes the CSP.

All authenticated services are accessed via TLS and therefore include TMACS(*U*) and TSK(*U*).

Table 9 - CSP Access Rights within Roles & Services

Role		Service Name	CSP and Key (*Access Mode*)
C.O.	User		
X		Clear Log	
X		Update End Sequence	
X		Update Module	FWUK(*U*)
X		Update Start Sequence	FWUK(*E*)
X		Zeroization	CEK(*Z*), CIK(*Z*), ADK(*Z*), MK(*Z*), LK(*Z*), RSK(*Z*), DPK(*Z*), RPK(*Z*)TSK(*Z*), TMACS(*Z*), TPS(*Z*), TMS(*Z*), PS(*Z*) , EI(*Z*), DS(*Z*)
X	X	Delete KDM	CEK(*Z*), CIK(*Z*), ADK(*Z*)
X	X	Delete KDM ID	CEK(*Z*), CIK(*Z*), ADK(*Z*)
X	X	Detail KDM ID	
X	X	Detail KDM ID CPC	
X	X	Establish TLS session	DS(*GUZ*), DPBK(*O*), OPK(*EU*), GMPK(*U*), GTPK(*U*), DPK(*U*), TPS(*EUZ*), TMS(*GUZ*), PS(*GUZ*), TSK(*G*), TMACS(*G*)
X	X	Get Audio Frequency	
X	X	Get Audio Muting	
X	X	Get Audio Routing	
X	X	Get Certificate	
X	X	Get CPL List ID	
X	X	Get Date	
X	X	Get Delay	
X	X	Get FM ID	
X	X	Get LTC Mode	
X	X	Get Marriage Status	
X	X	Get MS Configuration	

Role		Service Name	CSP and Key (*Access Mode*)
C.O.	User		
X	X	Get Playback Information	
X	X	Get Root Certificate	GTPK*(U)*
X	X	Get Security Status	
X	X	Get Status	
X	X	Get Time-zone	
X	X	Get Version	
X	X	Get White Point	
X	X	Heartbeat	
X	X	Initialize Marriage	RSK(*U*), TSK(*GU*), TMACS(*GU*), TPS(*GOU*), TMS(*GU*), PS(*GU*), EI*(U)*, DS(*U*), RVK(*OU*), PPK(*EU*)
X	X	Initialize PCIE Connection	
X	X	List KDM ID	
X	X	List Root Certificate	GTPK(*U*)
X	X	Play Pause Execution	
X	X	Play Pause Resume	
X	X	Play Prepare Completed	CEK(*U*), CIK(*U*)
X	X	Play Prepare CPL	ADK(*O*)
X	X	Play Set SPL	
X	X	Play Step	
X	X	Play Stop	
X	X	Relate KDM ID	
X	X	Retrieve Certificate	RVK(*O*), DPBK(*O*)
X	X	Retrieve Root Certificate	GTPK(*O*)
X	X	Retrieve Security Log 2	RSK(*U*), TSK(*U*), TMACS(*U*) , RVK(*O*)

Role		Service Name	CSP and Key (*Access Mode*)
C.O.	User		
X	X	Set AMB IP	RSK(*U*), TSK(*GU*), TMACS(*GU*), TPS(*GOU*), TMS(*GU*), PS(*GU*), EI*(U)*, DS(*U*) , ADPPK(*EU*)
X	X	Set Audio Frequency	
X	X	Set Audio Muting	
X	X	Set Audio Routing	
X	X	Set Date	
X	X	Set Date 2	
X	X	Set Delay	
X	X	Set LTC Mode	
X	X	Set MS Configuration	
X	X	Set Timed Text Key ID	
X	X	Set Time-zone	
X	X	Set White Point	
X	X	Shutdown	
X	X	Snapshot	
X	X	Store KDM	CEK(*UE*), CIK(*UE*), ADK(*UE*), MK(*U*), LK(*UEZ*), DPK(*U*), EI(*U*), DS(*U*), KIPK(*EU*)
X	X	Verify CPL	
X	X	Version	
Any	Any	Show Status	
Any	Any	Self-Test	

7. Operational Environment

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

8. Security Rules

The Granada 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 Granada shall provide two distinct operator roles. These are the User role, and the Crypto-Officer role.
2. The Granada shall provide identity-based authentication.
3. When the Granada has not been placed in an authenticated role, the operator shall not have access to any cryptographic services.
4. The Granada shall perform the following tests:
    i. Power-up Self-Tests:
        a. Cryptographic algorithm tests (for each implementation):
            - AES 128 CBC Encrypt and Decrypt Known-Answer Tests
            - AES 128 ECB Encrypt and Decrypt Known-Answer Test
            - AES Key Wrap and Unwrap Known-Answer Test
            - Hash DRBG Known-Answer Test and Health Testing
            - SHA-1 Known-Answer Test
            - SHA-256 Known-Answer Test
            - HMAC-SHA-1 Known-Answer Test
            - RSA PKCS#1 v1.5 2048 Signature Generation and Verification using SHA-256 Known-Answer Test
            - SP 800-135rev1 TLS KDF Known-Answer Test
        b. Firmware Integrity Test (CRC-16 and CRC-32)
        c. Critical Functions Test:
            - RSA PKCS#1 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 (Hash DRBG, NDRNG)

b. Firmware Load Test (RSA Digital Signature Verification)

5. The operator shall be capable of commanding the Granada 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 and zeroization processes.

8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the Granada.

9. The Granada does not support concurrent operators.

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

11. If a non-FIPS validated firmware version is loaded onto the Granada, then the Granada 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 Granada only supports the electronic entry form of key establishment.

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

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

9. Physical Security Policy

9.1. Physical Security Mechanisms

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

- Production-grade components,
- The enclosure of Granada has a removable cover with four tamper evidence seals (See Figure 2 and Figure 3) applied by Sony in a secure manufacturing facility. When the cover is removed or the power supply from the outside is lost, all plaintext CSPs within the Granada 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 2 – Image of Tamper Evidence Seal

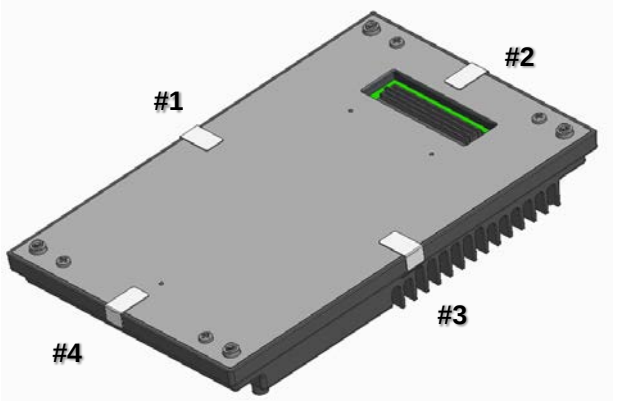


Figure 3 – Seal Location

9.2. Operator Actions

Due to the intended deployment environment for the Granada, 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 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 Granada 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. References

Table 12 - References

Abbreviation	Full Specification Name
[FIPS140-2]	*Security Requirements for Cryptographic Modules*, May 25, 2001
[IG]	*Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program*
[133]	*NIST Special Publication 800-133, Recommendation for Cryptographic Key Generation, December 2012*
[135]	*National Institute of Standards and Technology, Recommendation for Existing Application-Specific Key Derivation Functions, Special Publication 800-135rev1, December 2011.*
[186]	*National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-4, July, 2013.*
[197]	*National Institute of Standards and Technology, Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, November 26, 2001*
[198]	*National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July, 2008*
[180]	*National Institute of Standards and Technology, Secure Hash Standard, Federal Information Processing Standards Publication 180-4, August, 2015*
[38A]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001*
[38F]	*National Institute of Standards and Technology, Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping, Special Publication 800-38F, December 2012*
[90A]	*National Institute of Standards and Technology, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, June 2015.*

12. Definitions and Acronyms

Table 13 -Definitions and Acronyms

Term	Definition
AES	**A**dvanced **E**ncryption **S**tandard
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**io**s** & **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
DRBG	**D**eterministic **R**andom **B**it **G**enerator
RSA	**R**ivest-**S**hamir-**A**dleman

Term	Definition
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

13. Revision History

Date	Version	Description
Sep. 14, 2018	1.0.0	Initial release for firmware version 1.0.0 and hardware version 1.0.0
Mar 13, 2019	1.0.1	Updated to address comments from CMVP