MVC201

Non-Proprietary Security Policy

Date: 2017-5-26
Document Revision: 1.3

MikroM GmbH
Darwinstr. 17
10589 Berlin
Germany

Phone: +49 30 398839 0
Fax: +49 30 398839 29
Web: www.mikrom.com

Table of Contents

1 Introduction

The MikroM MVC201 cryptographic module is a high-end multi-chip hardware decoder targeting the professional application Digital Cinema. Based on re-programmable (FPGA) hardware and a powerful on-board microprocessor the MVC201 represents a solution for real-time decoding of JPEG2000 and MPEG-2 MP@HL video streams.

The MVC201 complies with the Digital Cinema System Specification V1.2 with Errata as of 30 August 2012 Incorporated, dated 10 October 2012. The whole Image Media Block (IMB) functionality is integrated in the MVC201, making it a very strong and intrinsically secure component in terms of content protection. It meets the requirements of FIPS 140-2 Security Level 3 (Ref. [FIPS 140-2]).

The validation of the whole MVC201 only maintains if the version numbers correspond to those listed under Section 1.2.

The MVC201 is a printed circuit board (PCB) designed for integration into a Texas Instruments (TI) Series 2 DLP Cinema projector. The module's cryptographic boundary is the outer edge of the PCB. All parts outside the physically protected area on the board are excluded from the requirements of FIPS 140-2 because they are non-security relevant and cannot be used to compromise the security of the module.

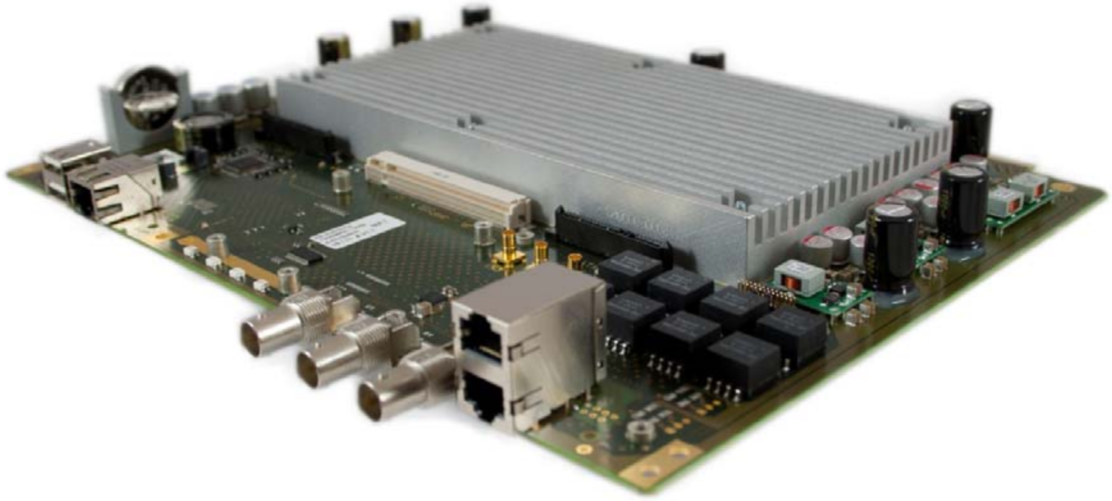

Figure 1 – MVC201 – front

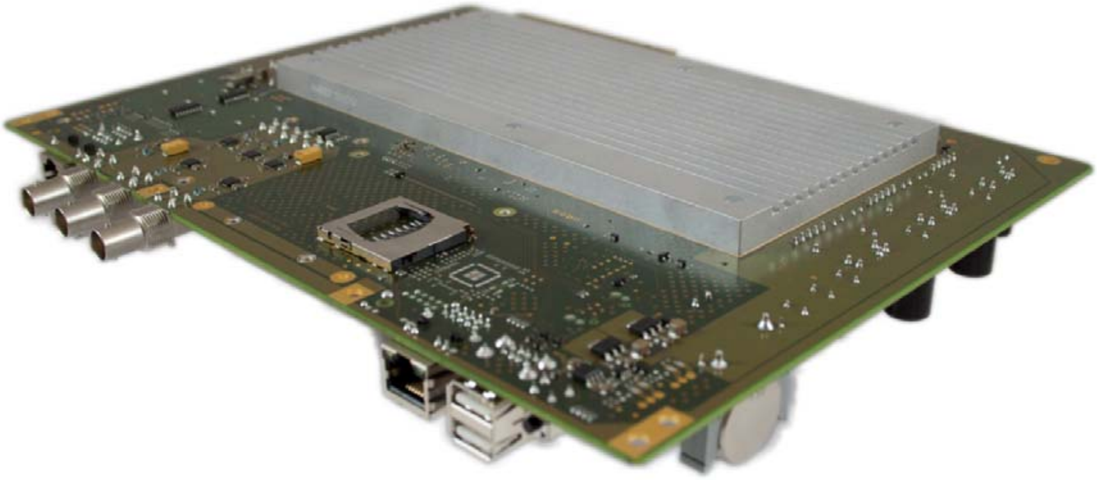

Figure 2 – MVC201 - back

1.1 Purpose

This document is the security policy for the MVC201 cryptographic module. It describes the security behavior of the module and how it meets the requirements of FIPS Publication 140-2 Security Level 3.

The FIPS PUB 140-2 is a U.S. government computer security standard used to validate cryptographic modules. The security level 3 describes a “production grade” module, which is physically and logically tamper-resistant and has the functionality to protect and in case of an attack to erase all secure content.

1.2 Revisions

Six configurations of the MVC201 are included in this validation, as follows:

1. MVC201-IS1 rev.1.1
2. MVC201-IF1 rev.1.1
3. MVC201-MS1 rev.1.1
4. MVC201-MF1 rev.1.1
5. MVC201-RS1 rev.1.1
6. MVC201-RS2 rev.1.1

All components within the physically protected security region are identical for all six configurations; the only difference is in the available ports.

Please see Table 2 for a listing of the ports available for each configuration.

The PCB revision can be validated by visual inspection of the bottom side of the board, where it is etched in the copper layer. The PCB revision is also denoted on the serial number label which is located on the top side of the board. Both items are shown in Figure 3. Furthermore a function is provided which can be used to obtain the PCB version.

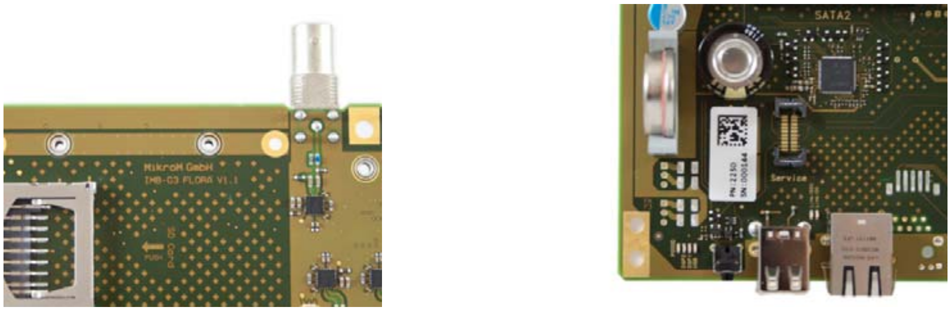

Figure 3 - Etched revision and S/N label

The validated firmware version is equal to:

Firmware Version:	1.23.157.20779
Bootloader Version:	1.3.7.18217

The driver’s API provides a function which can be used to obtain the overall firmware revision as well as the revisions of the different firmware modules contained in this revision.

1.3 Security Levels

The MVC201 is designed, developed and tested to meet the requirements of DCI Digital Cinema System Specification V1.2 as well as the requirements of FIPS 140-2 Security Level 3, which is requested by the DCI (Ref. [DCI DCSS]). The following table lists the compliance level of each section:

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operating Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

Table 1 - Levels of security requirements

1.4 Approved Mode of Operation

The module only provides the FIPS 140-2 approved mode of operation. This mode is invoked automatically at boot up of the cryptographic module.

To verify that the module is in approved mode of operation, the operator shall check for version numbers matching those listed on the validation certificate (refer to Section 1.2) using the Show Status service. Upon successful completion of self-tests and entering the Approved mode, the module will output “FIPS mode active”.

2 Ports and Interfaces

The MVC201 cryptographic module has several physical ports, i.e., connectors, which are used for single or multiple purposes.

The MVC201 provides the following physical ports:

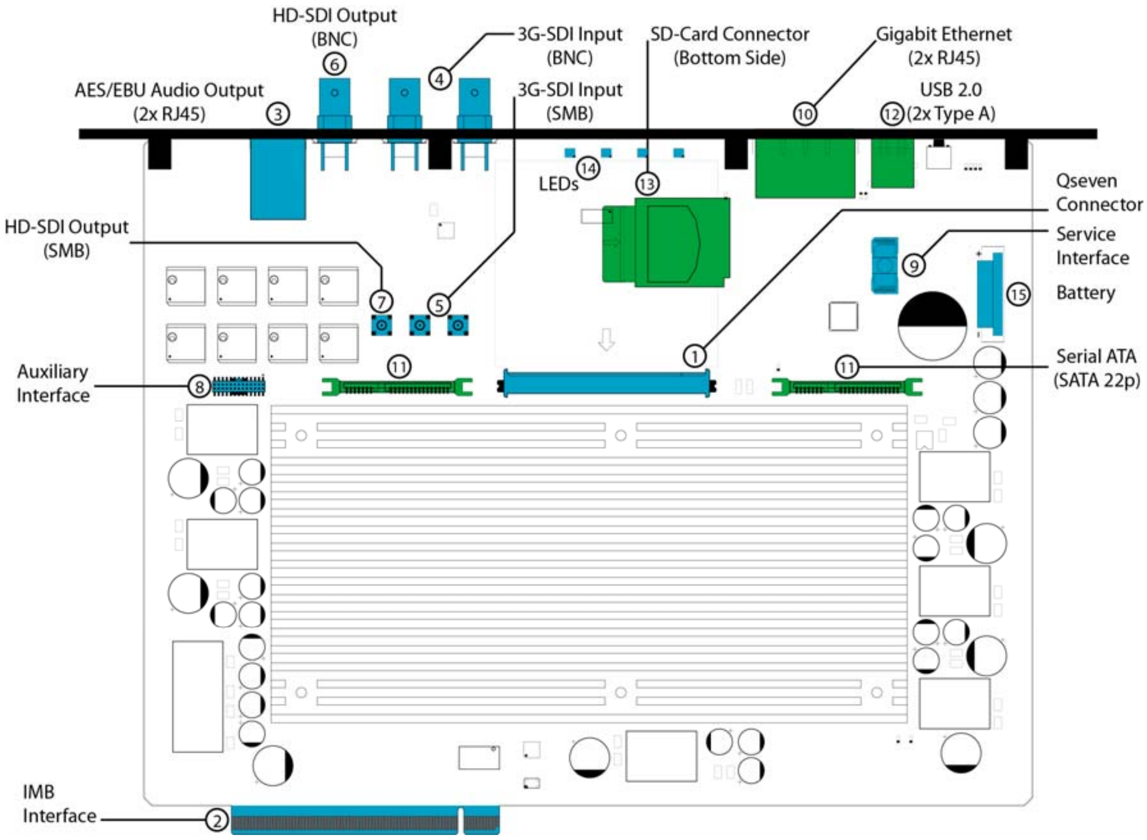

Figure 4 – Physical connectors

The following table describes how the physical ports relate to logical interfaces.

Location	Physical Port	Protocol	Quantity per HW Version						Logical Interface
			IS1	IF1	MS1	MF1	RS1	RS2	
1	PCI Express (Qseven connector)	PCI Express Base Specification Revision 1.1	1	1	1	1	1	1	Data input, Control input, Data output, Status output,
2	IMB interface	TI proprietary	1	1	1	1	1	1	Data output, Control input, Status output, Power input
3	AES/EBU Audio (RJ45)	AES3	2	2	2	2	2	2	Data output
4	3G-SDI input (BNC)	SMPTE424M SMPTE425M	0	2	0	2	0	0	Data input
5	3G-SDI input (SMB)	SMPTE424M SMPTE425M	0	2	0	2	2	2	Data input
6	HD-SDI output (BNC)	SMPTE292M	0	1	0	1	0	0	Data output
7	HD-SDI output (SMB)	SMPTE292M	0	1	0	1	0	0	Unused. Legacy component
8	Auxiliary interface (Pin Header)	Proprietary GPIO	1	1	1	1	1	1	Unused. Legacy component
9	Service interface (contact pads)	UART	1	1	1	1	1	1	Status output
10	Gigabit Ethernet (RJ45)	IEEE 802.3ab	2	2	1	1	1	1	Data input, Control input, Data output, Status output
11	Serial ATA	SATA Revision 1.0a	2	2	2	2	2	2	Data input

Location	Physical Port	Protocol	Quantity per HW Version						Logical Interface
			IS1	IF1	MS1	MF1	RS1	RS2	
12	USB 2.0	USB Specification Revision 2.0	2	2	2	2	2	2	Data input
13	SD-Card	SDIO	0	1	1	1	0	0	Data input
14	LEDs	N/A	4	4	4	4	4	4	Status output
15	Battery	N/A	1	1	1	1	1	1	Power input

Table 2 - Relation of ports and interfaces

No maintenance access interface is present.

3 Security Functions

The MVC201 cryptographic module supports FIPS 140-2 approved cryptographic algorithms and allowed key establishment protocols.

3.1 Approved Security Functions

1. **AES** (Certs. #1995, #1996 and #2898), AES-128, -256 in CBC mode (decryption only) (Ref. [FIPS 197])
2. **AES** (Cert. #4129), AES-128, -256 in CBC mode (Encryption/decryption) (Ref. [FIPS 197])
3. **AES** (Cert. #4130), AES-128 in ECB mode (Encryption only) (Ref. [FIPS 197])
4. **CVL** (Cert. #940), TLS KDF (Ref. [SP800-135rev1]); No parts of the TLS protocol have been reviewed or tested by the CAVP or CMVP.
5. **DRBG** (Cert. #1249), Hash DRBG SP800-90A DRBG (Ref. [SP800-90A])
6. **HMAC** (Certs. #2702 and #1833) HMAC-SHA-1 (Ref. [FIPS 180-4])
7. **RSA** (Cert. #2248), RSA-2048 used for sign/verify (Ref. [FIPS 186-4])
8. **SHA** (Certs. #3399 and #1749), SHA-256 (Ref. [FIPS 180-4])
9. **SHA** (Certs. #3399 and #1750) SHA-1 (Ref. [FIPS 180-4])

3.2 Allowed Key Establishment and Key Transport Protocols

1. Key transport using **RSA** (key wrapping, uses key size 2048 bit, ref. [FIPS 140-2 IG, 7.1]) key establishment methodology provides 112 bits of encryption strength.

3.3 Non-Approved, but Allowed Security Functions

1. **Hardware RNG** is the non-deterministic RNG (physical hardware) utilized for seeding the **DRBG**
2. MD5 within TLS

4 Cryptographic Keys and CSPs

The MVC201 cryptographic module contains the following CSPs:

- **ZK (AES-256):** System Master Key used as key encrypting key for CSP decryption. The used key size is 256 bits.
- **IMBPrDecK (RSA-2048):** System Private Decryption Key, used for content key unwrapping. The used key size is 2048 bits.
- **IMBPrSignK (RSA-2048):** System Private Signature Key, used to sign log messages, for TLS authentication and projector marriage. The used key size is 2048 bits.
- **CONTKi (AES-128):** Content Keys, used to decrypt content. The used key size is 128 bits.
- **FWSymK (AES-128):** Firmware image decryption key.
  The used key size is 128 bits.
- **TLS Pre-master Secret:** The parameter used for the generation of TLS Master Secret.
- **TLS Master Secret:** The parameter used for the generation of TLS Session Key and TLS Integrity Key.
- **TLS Session Key (AES-128):** The AES key used to protect TLS connection.
- **TLS Integrity Key (160 bit HMAC key):** The HMAC-SHA-1 key used to check integrity of TLS connection.
- **DRBG Secrets:** V and C secret values pertaining to the Hash DRBG.
- **MICKi (HMAC-SHA-1):** Message Integrity Check Keys.
  The used key size is 160 bits.

4.1 Public Keys

The cryptographic module contains the following public keys:

- **MIKCerti (X.509v3):** MikroM certificates used to verify the signature of firmware and feature update images.
- **TSPCerti (X.509v3):** TSP certificate chain used to verify SMSCert, IMBDecCert and IMBSignCert.
- **SMSCert (X.509v3):** SMS certificate used by the IMB to authenticate TLS session between IMB and SMS. Can be verified with TSPCerti.
- **IMBDecCert (X.509v3):** IMB decryption certificate. Can be verified with TSPCerti.
- **IMBSignCert (X.509v3):** IMB certificate used by the SMS to authenticate TLS session between IMB and SMS. Also used by the projector for marriage. Can be verified with TSPCerti.

- **PROJCert (X.509v3):** Projector certificate used by the IMB for projector marriage. This certificate is verified using a Trusted Device List.
- **DCPProvCerti (X.509v3):** DCP provider certificate chain used to verify the signature of Extra-Theater Messages like KDMs.
- **RSPBCerti (X.509v3)**: Certificates used to establish TLS sessions with remote SPBs.

5 Self-Tests

The MVC201 cryptographic module performs all below mentioned power-up self-tests on boot-up and only enters FIPS 140-2 approved mode of operation if all tests passed successfully. The conditional tests are executed every time the corresponding algorithm is used.

5.1 Power-Up Self-Tests

- Firmware integrity test (32-bit CRC and SHA-256)
- RSA Signature Generation and Signature Verification known answer tests
- AES CBC (128 and 256) Decrypt known answer tests
- AES CBC (128 and 256) Encrypt and Decrypt known answer tests
- AES ECB (128) Encrypt known answer test
- SHA-1 known answer tests
- SHA-256 known answer tests
- DRBG known answer test
- HMAC-SHA-1 known answer tests
- TLS KDF known answer tests

5.2 Conditional Tests

- Firmware load test (RSA 2048-bit signature verification)
- Continuous Random Number Generator Test on Hardware RNG
- Continuous Random Number Generator Test on DRBG
- SP800-90A Health Tests

6 Security

6.1 Operational Environment

The whole firmware of the MVC201 cryptographic module is stored persistently inside the module. During power-up the integrity of the stored firmware is checked before it is loaded and the module enters FIPS 140-2 approved mode of operation and no further firmware can be loaded.

All functions stored persistently in the module are static, non-modifiable and do not use an underlying general purpose operating system. Thus the requirements of FIPS 140-2 chapter 4.6.1 (Operational Environment) are not applicable because of the limited operational environment.

7 Physical Security Policy

7.1 Physical Security

The MVC201 cryptographic module is a multiple-chip embedded cryptographic module protected by a tamper-resistant metal cover on the upper and on the lower side of the board (see Figure 1 and Figure 2). Both cover shells are mounted stationary and are protected by a tamper detection mechanism as well as tamper-evident coating over the screws which must be checked periodically (refer to Table 3).

During normal operation the operator only has access to the front panel interfaces of the module, because it is integrated in the projector. It is protected against removal by the projector's physical and electrical arrangements

A maintenance service for the MVC201 is neither required nor allowed.

Physical Security Mechanisms	Recommended Frequency of Inspection	Inspection Guidance Details
Metal cover	Together with projector marriage	Both cover shells shall not be damaged
Cover fixing bolts	Together with projector marriage	All bolts shall not be damaged
Tamper evident coating over screws	Together with projector marriage	The coating shall not be damaged or look tampered. Please refer to Figure 5 for a picture of untampered coating.

Table 3 - Physical security inspection guidance

The seal-protected cover also acts as a heat sink and forms a hard enclosure in means of FIPS 140-2.

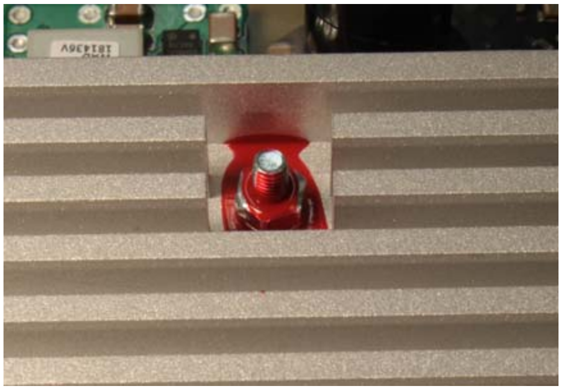

Figure 5 – Coating over screw

As soon as a cover is removed the tamper detection response is triggered, automatically forcing active zeroization of all cryptographic keys as described in Section 7.2 below.

7.2 Zeroization

After tamper detection, secret and private cryptographic keys and CSPs are actively and immediately deleted.

When an attack is detected and the system is inactive (power-off) only the key encrypting key ZK is zeroized by the tamper detection device and thus also the IMBPrDecK, IMBPrSignK, and FWSymK immediately become unusable.

If the system is active (power-on) while being attacked additionally all temporary cryptographic keys and CSPs of the module are zeroized.

The module also contains a Zeroize service allocated to the User role. This service zeroizes all secret and private cryptographic keys and CSPs within the module.

8 Identification and Authentication Policy

8.1 Authentication

The following table describes the roles and how they are authenticated:

Role	Type of Authentication	Authentication Data
User	Identity-based authentication	2048-bit RSA digital signature verification
Crypto Officer	Identity-based authentication	2048-bit RSA digital signature verification

Table 4 – Authentication types

Authentication Mechanism	Strength of Mechanism
Digital Signature Verification	The RSA private key used to generate the digital signature is 2048-bits. The strength of a 2048-bit RSA key (with SHA-256) is known to be 112 bits. Therefore, the strength of a 2048-bit digital signature is 1/2^112, which is less than one in 1,000,000. The module can perform RSA signature verifications in approximately 900ms, which is approximately 67 verifications per minute. The probability that a brute force attack will be successful given a minute of time is 67/(2^112), which is less than the required 1/100,000.

Table 5 - Strength of Authentication

9 Access Control Policy

9.1 Services for Authorized Roles

The MVC201 cryptographic module supports two authorized roles. The User role covers general security related services, including cryptographic and other approved security functions. The Crypto Officer (CO) role covers secure firmware update.

User Role	CO Role	Service	Service Description
	x	SystemUpdate	Update IMB firmware or feature set
x		StartSuite	Query the SM to check the auditorium equipment (e.g., marriage status) and start operation. May also establish a TLS connection with a remote SPB.
x		StopSuite	Query the SM to stop operation
x		UploadCPL	Upload a Composition Play List to the SM for validation
x		UploadKDM	Upload a Key Delivery Message to the SM for validation and key decryption
x		PurgeCPL	Remove a CPL and all the associated data (CPL, KDMs, keys, etc…).
x		PlayBack	Play a show, send encrypted data and control playback
x		PlayShow	Prepare a show (as a list of CPLs) for playback
x		StopShow	Reject a prepared show
x		CheckShow	Check that a show (as a list of CPLs) is ready for playback at a given time
x		GetCertificates	Retrieve the IMB certificates
x		GetCPLList	Retrieve the list of currently available CPLs
x		GetKDMList	Retrieve the list of available KDMs for a specific CPL
x		QuerySM	Query the SM status
x		AdjustTime	Allow the auditorium operator to adjust the SM clock
x		GetLogReport	Retrieve security logs maintained by the SM
x		InitiateMarriage	Initiate projector marriage procedure
x		ClearTamper	Clear pending service door tamper
x		Zeroize	Zeroize all module cryptographic keys and CSPs

Table 6 – Authenticated Services

9.2 Services for Unauthorized Roles

The module provides the following unauthenticated services:

Service	Service Description
EstablishConnection	Start TLS session between the SM and the external SMS
ProjectorInterface	Query status, initiate marriage and clear service door tamper
Playback Plaintext	Play a show, send plaintext data and control playback
Restart	Restart of the IMB causing a reset and reboot. This causes the suite of self-tests to be run.
ShowStatus	Output the current status of the cryptographic module.

Table 7 - Unauthenticated Services

9.3 Access Rights within Services

Service	Cryptographic Keys and CSPs	Types of Access generate/read/write/modify/zeroize
SystemUpdate	MIKCerti	read
	FWSymK	read
StartSuite	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
StopSuite	DCPProvCerti	zeroize
	CONTKi	zeroize
	MICKi	zeroize
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
UploadCPL	DCPProvCerti	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
UploadKDM	DCPProvCerti	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
	CONTKi	write
	MICKi	write
	IMBPrDecK	read

Service	Cryptographic Keys and CSPs	Types of Access generate/read/write/modify/zeroize
PurgeCPL	DCPProvCerti	zeroize
	CONTKi	zeroize
	MICKi	zeroize
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
Playback	CONTKi	read
	MICKi	read
PlayShow	CONTKi	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
StopShow	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
CheckShow	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
GetCertificates	IMBDecCert	read
	IMBSignCert	read
	MIKCerti	read
	TSPCerti	read
	PROJCert	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
GetCPLList	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
GetKDMList	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
QuerySM	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read

Service	Cryptographic Keys and CSPs	Types of Access generate/read/write/modify/zeroize
AdjustTime	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
GetLogReport	IMBPrSignK	read
	TSPCerti	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
InitiateMarriage	PROJCert	read/write
	IMBSignCert	read
	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
ClearTamper	TLS Pre-Master Secret	read
	TLS Master Secret	read
	TLS Session Key	read
	TLS Integrity Key	read
Zeroize	ZK	zeroize
	IMBPrDecK	zeroize
	IMBPrSignK	zeroize
	FWSymK	zeroize
	CONTKi	zeroize
	MICKi	zeroize
	TLS Pre-Master Secret	zeroize
	TLS Master Secret	zeroize
	TLS Session Key	zeroize
	TLS Integrity Key	zeroize
	DRBG Secrets	zeroize
EstablishConnection	IMBPrSignK	read
	IMBSignCert	read
	TSPCerti	read
	SMSCert	read/write
	TLS Pre-Master Secret	generate
	TLS Master Secret	generate
	TLS Session Key	generate
	TLS Integrity Key	generate
	DRBG Secrets	generate
ProjectorInterface	PROJCert	read/write
	IMBSignCert	read
Playback Plaintext	-	n/a

Service	Cryptographic Keys and CSPs	Types of Access generate/read/write/modify/zeroize
Restart	IMBPrDecK	zeroize
	IMBPrSignK	zeroize
	FWSymK	zeroize
	CONTKi	zeroize
	MICKi	zeroize
	DCPProvCerti	zeroize
	SMSCert	zeroize
	TLS Pre-Master Secret	zeroize
	TLS Master Secret	zeroize
	TLS Session Key	zeroize
	TLS Integrity Key	zeroize
	DRBG Secrets	zeroize
ShowStatus	-	n/a

Table 8 - Access Right Mapping

10 Mitigation of Other Attacks Policy

Mitigation of other attacks in the meaning of FIPS PUB 140-2 is not claimed. The module has not been designed to mitigate other attacks outside of the scope of FIPS 140-2.

11 Appendix

11.1 Acronyms

Acronym	Description
AES	Advanced Encryption Standard
AES3	Digital audio interface specified by Audio Engineering Society in standard AES3
CBC	Cipher Block Chaining – Block Cipher Mode
CPL	Composition Play List
CSP	Critical Security Parameters
CTR	Counter – Block Cipher Mode
DCI	Digital Cinema Initiative
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook – Block Cipher Mode
FPGA	Field Programmable Gate Array
HD-SDI	High Definition Serial Digital Interface
HRNG	Non-deterministic RNG (physical hardware)
IMB	Image Media Block
JPEG	Joint Photographic Experts Group
KDM	Key Delivery Message
MPEG	Moving Picture Experts Group
PCB	Printed Circuit Board
PCI	Peripheral Component Interconnect
RNG	Random Number Generator
RSA	Asymmetric Cryptographic Algorithm published by Ron Rivest, Adi Shamir and Leonard Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SM	Security Manager
SMPTE	Society of Motion Picture and Television Engineers
SMS	Screen Management System (not part of the validation)
TLS	Transport Layer Security
TSP	Theatre System Provider

Table 9 - Acronyms

11.2 References

Reference	Description
DCI DCSS	Digital Cinema System Specification V1.1, 2007
FIPS 140-2	FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 2001, with Change Notices 2002
FIPS 140-2 DTR	Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 2004 Draft
FIPS 140-2 IG	Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, 2009
FIPS 180-3	FIPS PUB 180-3, Secure Hash Standard (SHS), 2008
FIPS 186-4	FIPS PUB 186-4, Digital Signature Standard (DSS), 2013
FIPS 197	FIPS PUB 197, Announcing the Advanced Encryption Standard (AES), 2001
FIPS 198	FIPS PUB 198, The Keyed-Hash Message Authentication Code (HMAC), 2002
PKCS #1 v2.1	RSA Cryptography Standard, RSA Laboratories, 2002
SMPTE 429-6	MXF Track File Essence Encryption, 2006
SMPTE 429-7	D-Cinema Operations - Composition Playlist, 2006
SMPTE 430-1	D-Cinema Operations - Key Delivery Message
SMPTE 430-2	D-Cinema Operations - Digital Certificate, 2006
SP800-90A	Recommendation for Random Number Generation using Deterministic Random Bit Generators

Table 10 - References

11.3 Document History

Editor	Date	Changes	Revision
MikroM	2012-12-26	Release	1.00
MikroM	2014-03-04	Updates per CMVP comments	1.01
MikroM	2014-06-18	Added FW Version 1.20.98.19460	1.02
MikroM	2014-07-15	Added AES Cert. #2898 & HMAC Cert. #1833	1.03
MikroM	2015-04-09	Added FW Version 1.20.118.19949	1.04
MikroM	2016-10-11	Added FW Version 1.23.148.20724, Updated algorithm certs.	1.1

Table 11 - Document History