Barco ICMP

FIPS 140-2

Non-Proprietary

Security Policy

Prepared by,
Barco n.v.

Revision	Date	Comments
1.0	4/27/2020	Initial Release
1.1	3/22/2021	Revision for new hardware revision: - New hardware revision and pictures in Section 1

Table of Content

1 Introduction

The Barco n.v. Integrated Cinema Media Processor, or **Barco ICMP** as branded by the company and used throughout this document, is a cryptographic module designed in accordance with FIPS 140-2 and the Digital Cinema Initiative Digital Cinema System Specification (DCI DCSS v1.2). It is aimed at protecting digital cinema content when hosted within a Barco DCI compliant digital cinema projector.

From the DCI perspective it is referred to as a Type 1 Secure Processing Block (SPB1) defining Image Media Block, Projector and Screen Management System secure entities.

From FIPS 140-2 perspective the module is implemented as a multi-chip embedded module designed to meet FIPS 140-2 requirements.

The following hardware versions apply for FIPS 140-2 certification:

- Hardware part number: R7681360-06 (where -06 is the revision of the module)
- Hardware part number: R7681360-09 (where -09 is the revision of the module)

The following firmware version applies for FIPS 140-2 certification:

- Firmware package version is 1.4.0.0.20979.

Any firmware loaded into the module with a version not showing in the module certificate is out of scope of this validation and requires a separate FIPS 140-2 validation.

1.1 Security Level

The Barco ICMP module is designed to meets FIPS 140-2 security requirements as defined in the table below:

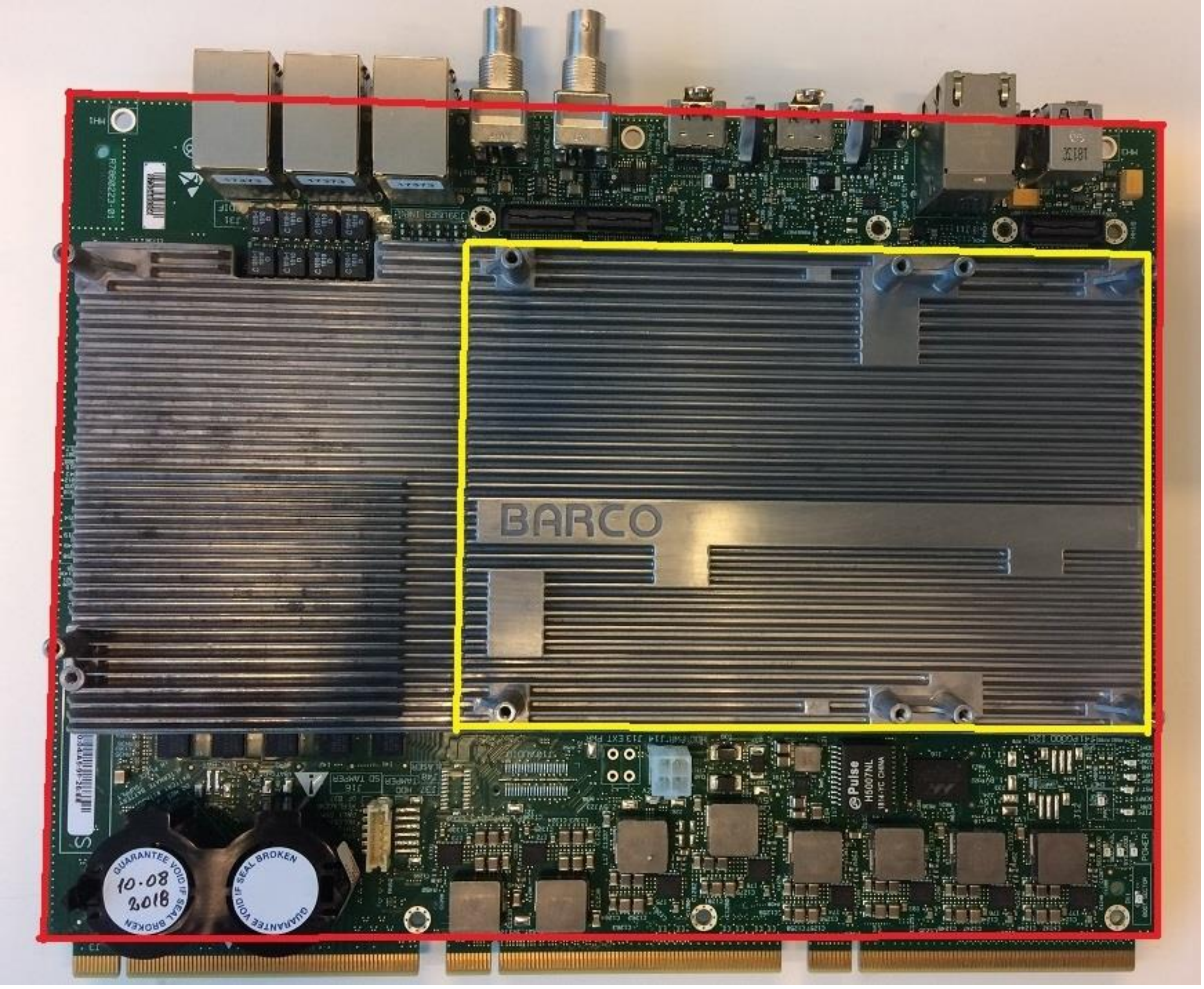
Table 1 – Security levels

Security Requirements Section	Level
1 - Cryptographic Module Specifications	2
2 - Cryptographic Module Ports and Interfaces	2
3 - Roles, Services and Authentication	3
4 - Finite State Model	2
5 - Physical Security	3
6 - Operational Environment	N/A
7 - Cryptographic Key Management	2
8 - EMI/EMC	2
9 - Self-Tests	2
10 - Design Assurance	2
11 - Mitigation of Other Attacks	N/A
Overall	**2**

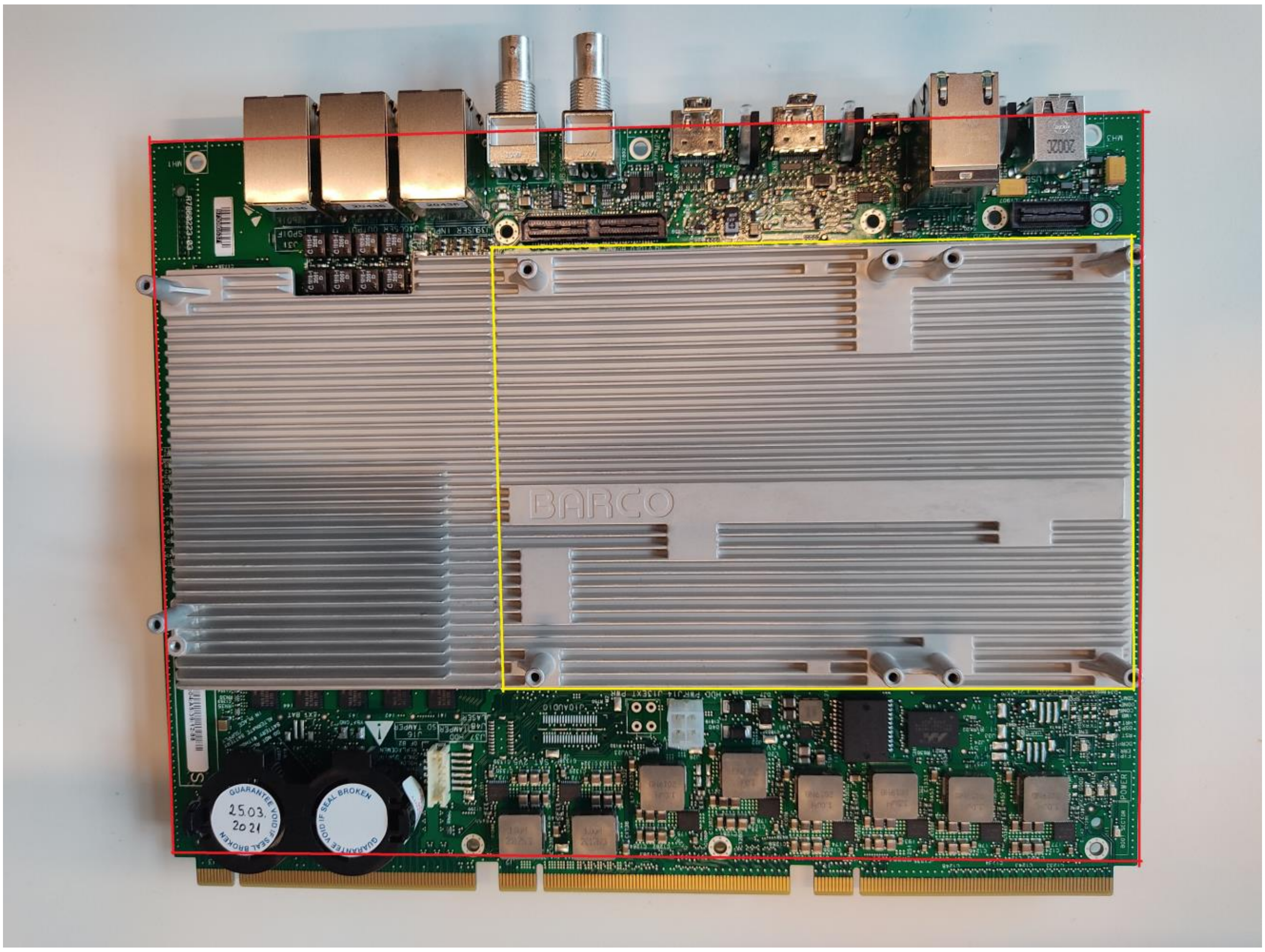
The module overall meets FIPS 140-2 compliance at level 2.

1.2 Cryptographic Boundary

The cryptographic boundary is defined by the outer perimeter of the main board's PCB. It is outlined in red in the below picture.



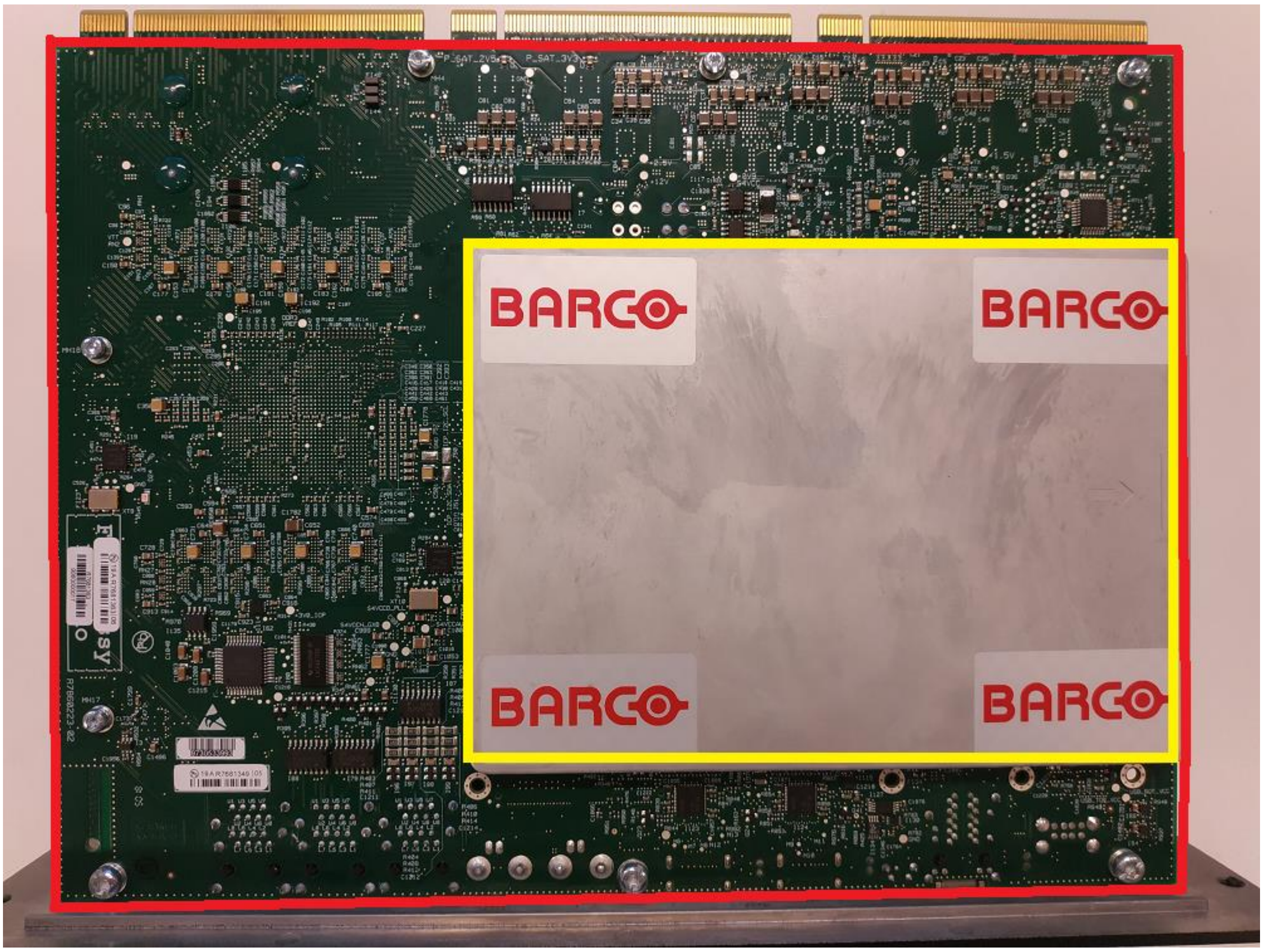
Picture 1 – Barco ICMP R7681360-06 main board top view



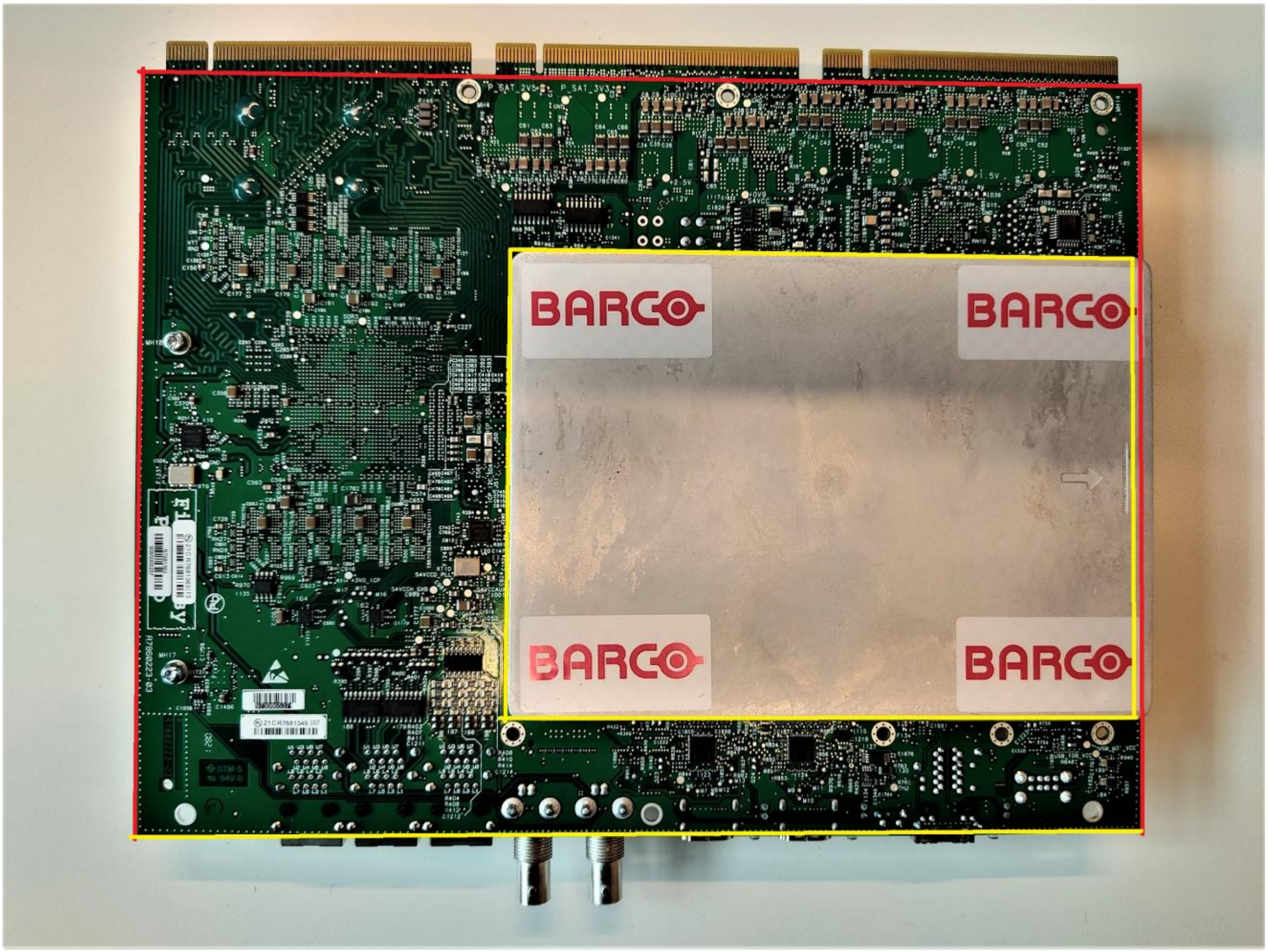
Picture 1a – Barco ICMP R7681360-09 main board top view

All security related components are enclosed within an opaque metal cover and protected by tamper detection and response mechanisms. It is outlined in yellow in the above picture.

Tamper evident labels are present to allow for tamper evidence examination.



Picture 2 – Barco ICMP R7681360-06 main board bottom view

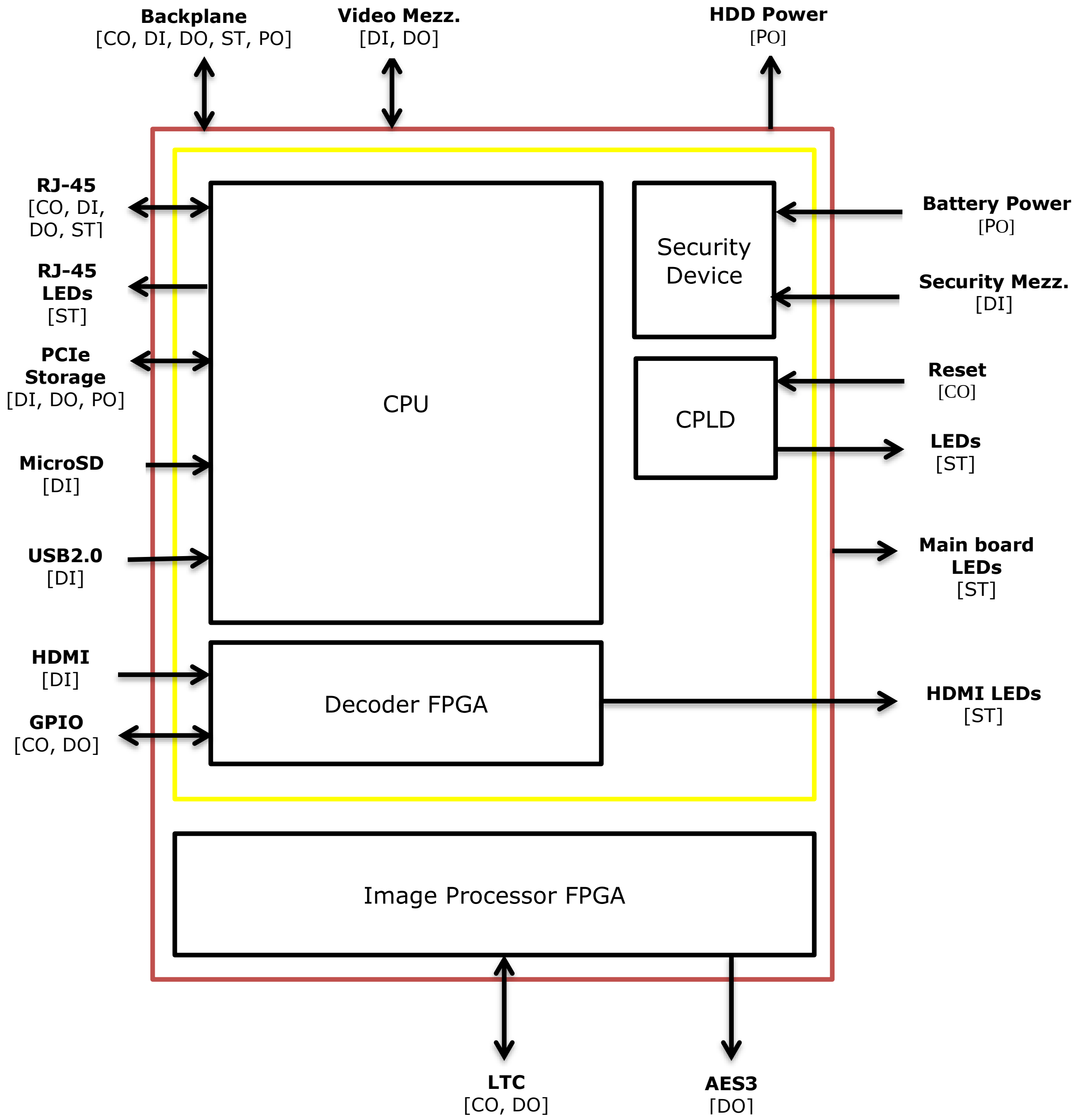


Picture 2 – Barco ICMP R7681360-09 main board bottom view

All the components outside the above enclosure are not security-relevant and do not harm the security functions of the module, both from FIPS 140-2 and DCI standpoints. Therefore they are explicitly excluded from FIPS 140-2 requirements.

The excluded components list consists in power devices, non-security relevant interfaces and related buses and traces, temperature sensors, clock distribution, filtering components and the video processing FPGA (which does not perform any security function).

1.3 Block Diagram



Captions:

- CO: Control Input
- DI: Data Input
- DO: Data Output
- ST: Status
- PO: Power

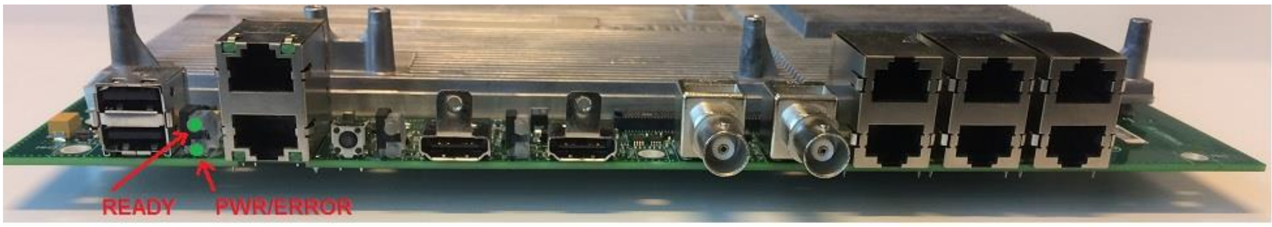
Red solid line: cryptographic module boundary

Yellow solid line: metal cover enclosure

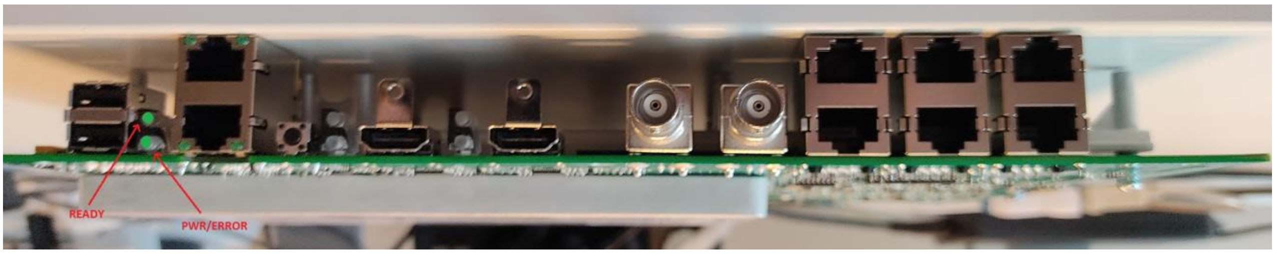
1.4 FIPS 140-2 Modes of Operation

The module performs in both FIPS Approved and non-Approved Modes of Operation.

The module reaches Approved Mode of Operation upon each power-up and indication that the module has successfully performed all the power-up tests and health checks is given by static green status of both the PWR/ERROR and READY LEDs.



Picture 3 – Barco ICMP R7681360-06 front view



Picture 3 – Barco ICMP R7681360-09 front view

Note that when the cryptographic module is in an error state, e.g. due the power-up tests failure, the front panel LEDs are the only available indicators: the PWR/ERROR LED shows a static red status and the READY LED is off.

In FIPS Approved Mode of Operation only the services listed in table 8 are available and the module transitions to non-Approved Mode of Operation whenever services from tables 9 to 14 are invoked.

1.4.1 Approved Mode of Operation

The module uses the following Approved cryptographic algorithms in Approved Mode of Operation:

Table 2 - Embedded Software Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	Use
#C 397	RSA	FIPS 186-2	RSASSA-PKCS1_V1_5	2048	Digital Signature Verification
#C 397	RSA	FIPS 186-4	RSASSA-PKCS1_V1_5	2048	Digital Signature Verification
#C 397	SHS	FIPS 180-4	SHA-1 SHA-256		Message Digest Note: SHA-1 is only used to calculate certificate thumbprints, it is never used for digital signature operations.

In FIPS Approved Mode of Operation, the module does not use other algorithms/modes contained in CAVP certificate #C 397, and it also does not use any non-Approved but allowed cryptographic algorithms.

1.4.2 Non-Approved Mode of Operation

In FIPS non-Approved Mode of Operation, the module uses the following non-Approved cryptographic algorithms:

Table 3 - Embedded Software non-Approved Algorithms

Algorithm	Use
AES (non-compliant)	AES 128 bits Data Encryption (CBC) Data Decryption (CBC) Key Wrapping
DRBG (non-compliant)	Hash_DRBG SHA-256 Deterministic Random Bit Generator
EC Diffie-Hellman (non-compliant)	Key Agreement
HMAC-MD5	Message Authentication
HMAC-SHA-1 (non-compliant)	Message Authentication
MD5	Message Digest
NDRNG	DRBG seeding
RNG (FIPS 186-2)	Shared secret computation
RSA (non-compliant)	RSA 2048 bits Digital Signature Generation Key Transport
SHA-1 (non-compliant)	Message Digest
TLS KDF (non-compliant)	TLS 1.0 PRF Key Agreement

Table 4 - FPGA non-Approved Algorithms

Algorithm	Use
AES (non-compliant)	AES 128 bits Data Decryption (CBC)
HMAC-SHA-1 (non-compliant)	Message Authentication
SHA-1 (non-compliant)	Message Digest

2 Ports and Interfaces

The module provides the following physical ports and logical interfaces:

Table 5 – Specification of Cryptographic Module Physical Port and Logical Interfaces

Physical Port	Logical Interfaces
RJ-45 Ethernet ports (Qty. 2)	Control Input Data Input Data Output Status Output
RJ-45 LEDs (Qty. 4)	Status Output
AES3 audio interfaces (Qty. 2)	Data Output
HDMI interfaces (Qty. 2)	Data Input
HDMI LEDs (Qty. 2)	Status Output
GPIO input interfaces (Qty. 2)	Control Input
GPIO output interfaces (Qty. 2)	Data Output
USB 2.0 (Qty. 2)	Data Input
LEDs (Qty. 2)	Status Output
LTC sync input connector (Qty. 1)	Control Input
LTC sync output connector (Qty. 1)	Data Output
Reset (Qty. 1)	Control Input
Main board LEDs (Qty. 11)	Status Output Caveat: this interface is latent, it is reserved for future use. Not visible under normal operation of the module.
MicroSD card holder port (Qty. 1)	Data Input
HDD power output (Qty. 2)	Power
Security Mezzanine interface (Qty. 1)	Data Input
Battery holders +3V (Qty. 2)	Power
PCIe storage controller (Qty. 1)	Data Input Data Output Power
Video Mezzanine interface (Qty. 1)	Data Input Data Output Caveat: this interface is latent, it is reserved for future use.
Backplane interface (Qty. 1)	Control Input Data Input Data Output Status Output Power

3 Identification and Authentication policy

3.1 Roles

The roles defined within the module are listed in the following table.

Table 6 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication data
Barco User	Identity-Based	RSA Signature Verification
Barco Crypto Officer	Identity-Based	RSA Signature Verification

3.2 Authentication

Supported authentication mechanisms are designed to meet the required strength for FIPS 140-2 level 3.

Table 7 – Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
RSA Signature Verification	The module uses RSA 2048 bits keys which are equivalent in strength to 112 bits symmetric keys. The probability of success or false acceptance is less than 1/1000000: 1/2^112 = 1,9259299443872358530559779425849e-34 A rough measurement of the processor’s capabilities gives us less than five RSA 2048 Signature Verification operations per second. The probability of success or false acceptance within one minute is less than 1/100000: 5*60/2^112 = 5,7777898331617075591679338277548e-32

4 Critical Security Parameters

4.1 Private keys, secret keys and other CSPs

The module does not contain any private key, secret key or CSP in the FIPS Approved Mode of Operation.

4.2 Public keys and other public data

Relevant public keys for FIPS Approved Mode of Operation are listed below. These keys are protected from unauthorized modification and substitution but are not submitted to active zeroization.

- **Barco Authority public keys**: Barco Authority identity keys for Barco Users and Crypto Officers RSA 2048 bits; transient RSA public keys used to identify a Barco Authority and carried within leaf and CA X509 certificates

- **Barco Authority root public key**: Barco Authority root signing key for Barco Users and Crypto Officers RSA 2048 bits; RSA public key used to authenticate Barco Users and Crypto Officers and carried within a root X509 certificate

- **Update Package signer (public data)**: SHA1 certificate thumbprint of the authorized signer for module update packages

5 Access Control policy

5.1 Services requiring authentication

The following tables list the services requiring operator authentication and map authorized roles and CSP access for each service.

Available roles are:

- **BU**: Barco User
- **CO**: Barco Crypto Officer

Table 8 – Authenticated Services

BU	CO	Services	Public Keys and other public data	Type(s) of Access
x	x	**Update package validation:** authenticate the update package	Barco Authority public keys	Read
			Barco Authority Root public key	Read
			Update Package Signer	Read

5.2 Non-Approved services

The following table define non-Approved services available on the module. These services make use of non-Approved cryptographic algorithms and are only supported in non-Approved Mode of Operation.

Table 9 – HTTPS Services

Roles	Services	Non-Approved algorithms
Barco User / Barco Crypto Officer	**Get User List:** read module user list for operator login	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG
Barco User / Barco Crypto Officer	**Information:** read various module information (make, model, version info, certificate list, license status…)	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG
Barco User / Barco Crypto Officer	**Status:** read various status information from the module (player, projector, ingest, content, scheduler, storage, recovery…)	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant)

		NDRNG
Barco User / Barco Crypto Officer	**Export System Logs:** export operational logs	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG
Barco User / Barco Crypto Officer	**License Manager:** add/remove licenses to enable/disable product features	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG
Barco User / Barco Crypto Officer	**Content Manager:** content and key management: add/remove, ingest jobs…	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDNRG
Barco User / Barco Crypto Officer	**Storage Manager:** external storage management, RAID rebuild…	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG
Barco User / Barco Crypto Officer	**Show Editor:** add/remove, select, edit…	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG
Barco User / Barco Crypto Officer	**Schedule Editor:** add/remove, select, edit…	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG

Barco User / Barco Crypto Officer	**Player Control:** clear, select, play/resume, pause/stop, positioning…	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG RNG (FIPS 186-2)
Barco User / Barco Crypto Officer	**Cue Control:** manual cue trigger, GPO control…	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG
Barco User / Barco Crypto Officer	**Projector Control:** lamp, dowser, macro execution, test patterns…	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG
Barco User / Barco Crypto Officer	**Settings:** read or write module and user settings	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG
Barco User / Barco Crypto Officer	**Security Logs Export:** export DCI security log report from the module	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDNRG
Barco User / Barco Crypto Officer	**Adjust RTC:** module real time clock adjustment within valid DCI range	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant) TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDNRG
Barco User / Barco	**Multi-Projector Control:** clock sync, ingest and playback control	AES (non-compliant) HMAC-MD5, HMAC-SHA1 (non-compliant)

Crypto Officer		TLS KDF (non-compliant) MD5, SHA-1 (non-compliant) RSA (non-compliant) DRBG (non-compliant) NDRNG

Table 10 –Update Services

Roles	Services	Non-Approved algorithms
Barco User / Barco Crypto Officer	**System Status:** get various status information from the module (general, system or security)	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Version:** read versions of currently installed components	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Login/Logout:** legacy protocol authentication mechanism	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Install Update Package:** trigger update package installation and read progress status	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Remove Web Update Package:** fall back to the original web package	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Identifier:** read the module's identification string	EC Diffie-Hellman (non-compliant)

Table 11 – Legacy IMB Services

Roles	Services	Non-Approved algorithms
Barco User / Barco Crypto Officer	**System Status:** get various status information from the module (general, system or security)	EC Diffie-Hellman (non-compliant)
Barco User / Barco	**Version:** get version information	EC Diffie-Hellman (non-compliant)

Crypto Officer		
Barco User / Barco Crypto Officer	**Login/Logout:** legacy protocol authentication mechanism	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Serial Number:** get the module serial number	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Upload File Select/Upload Data:** get error description files from the IMB	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Get Certificate:** read out available device certificates	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Power Mode Select:** switch between normal and low power consumption	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Service Door Tamper Termination:** clear the event indicative that either the host projector service door was opened or that module was installed in the projector	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Identifier:** read the module’s identification string	EC Diffie-Hellman (non-compliant)

Table 12 – Legacy Projector Services

Roles	Services	Non-Approved algorithms
Barco User / Barco Crypto Officer	**Projector Control commands:** processing path selection, macro execution, input port selection…	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**File Management commands:** read/write/copy/delete projector files	EC Diffie-Hellman (non-compliant)

Barco User / Barco Crypto Officer	**Image Control commands:** brightness, hue, saturation…	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Port Configuration**: RS-232 and Ethernet port configuration	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Composite/Overlay commands:** subtitle control	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**General System commands:** read status, version	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Login/Logout:** legacy protocol authentication mechanism	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**Upload File Select/Upload Data:** get error description files from the image processing part	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**3D commands:** control	EC Diffie-Hellman (non-compliant)
Barco User / Barco Crypto Officer	**System Administration commands**	EC Diffie-Hellman (non-compliant)

Table 13 –SNMP Services

Roles	Services	Non-Approved algorithms
Barco User / Barco Crypto Officer	**SNMP**	None

Note: the SNMP service has not been reviewed or tested by the CAVP and CMVP.

5.3 Unauthenticated services

The following tables define unauthenticated services available on the module. These services do not modify or disclose CSPs and do not use any Approved security function.

Table 14 –Other ICMP Unauthenticated Services

Services	Cryptographic Keys and CSPs	Type(s) of Access
Show Status: main status of the module given by the front panel PWR/ERR and READY LEDs.	None	N/A
Self-Tests: power-up self-tests invocation is performed through a module power-cycle. The self-tests listed in section 7.1 are invoked.	None	N/A
HTTP server: HTTP server for closed captions and auxiliary data frames access	None	N/A
FTP Server: FTP server for Barco update package upload, security and system logs download and local storage access	None	N/A
HDMI auxiliary channel control	None	N/A
Automation input signals	None	N/A
LTC sync input signal	None	N/A
Manual reset	None	N/A
Tamper signals: external tamper signals (projector host service door…)	None	N/A
Power	None	N/A
Automation over IP	None	N/A

5.4 Zeroization service

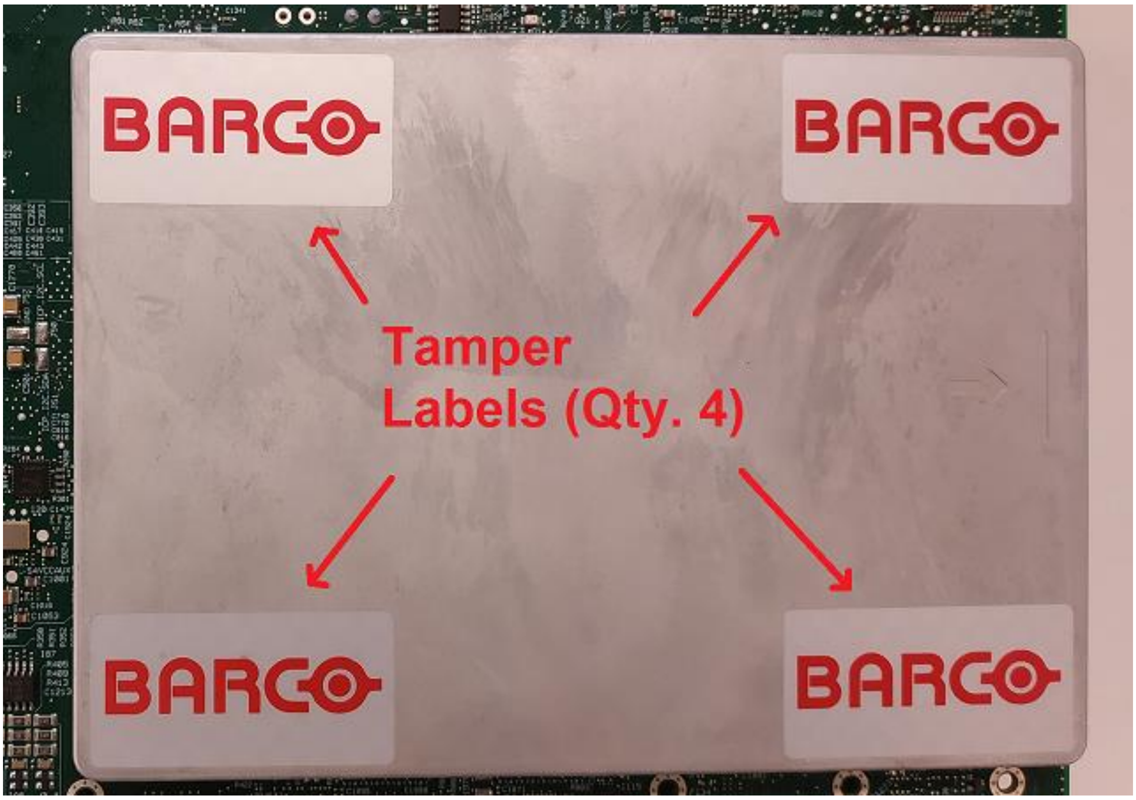
Zeroization can be triggered by a tamper event such as removal of the module’s battery or opening of the security enclosure; therefore no other zeroization service exists within the module.

6 Physical Security policy

The opaque tamper-evident production grade metal cover is monitored 24/7 by battery-backed tamper detection and response mechanisms. Any attempt to remove the metal cover, or attempt to remove the battery power, will result in active zeroization.

The hardness testing of the metal cover was performed at a single temperature and no assurance is provided for Level 3 hardness conformance at any other temperature.

Tamper Labels are applied during the manufacturing process by Barco and shall not be removed (i.e. maintenance role is not supported, there is not maintenance interface).



Picture 3 – Barco ICMP security enclosure tamper evident labels

All physical mechanisms are inspected by a Crypto Officer before the module leaves the production facilities and the User guidance manual recommends regular inspection of the module, as summarized in table 15.

The table below describes the existing physical protection mechanisms and the examination procedures required to ensure the integrity of the module is not compromised.

Table 15 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Opaque tamper-evident production grade metal cover	- At module installation - On suspicion of tampering (module is unresponsive, *PWR/ERROR* LED status is static red, READY LED is off) - Regular inspection is recommended	Visual inspection for visible scratches, dents or any evidence there was an attempt to shift or dislodge the cover. See picture 3 above.
Tamper-evident void labels (Qty. 4) on the metal cover fasteners	- At module installation - On suspicion of tampering (module is unresponsive, *PWR/ERROR* LED status is static red, READY LED is off) - Regular inspection is recommended	Visual inspection for visible scratches or scrapes, signs of tearing or damage. See picture 3 above
Tamper-responsive zeroization mechanisms	- On suspicion of tampering (module is unresponsive, *PWR/ERROR* LED status is static red, READY LED is off) - Regular inspection of the battery level is necessary	Perform the above inspections to confirm the metal cover was not tampered with. Check the *PWR/ERROR* LED status. Confirm the module's battery is in place. Consult the manufacturer manuals for battery level monitoring.

In the event tampering of the module is confirmed or suspected: Barco Support shall be contacted immediately. Barco Support engineers will provide guidance to further proceed. Barco Support desk is available 24/7 worldwide to all Barco customers through the Barco web portal: https://www.barco.com/en/support.

7 Self-tests

7.1 Power-up tests

The module implements the following power-up tests:

- RSA 2048 bits with SHA256 Signature Verification KAT
- SHA1 KAT
- Software and firmware components integrity tests using a 32 bits EDC
- Critical functions tests listed in section 7.3

Indication that the module has successfully performed all power-up tests is given by a static green PWR/ERROR LED and blinking green READY LED.

Failure to successfully complete these tests will put the module in error state. Indication is given by a static red PWR/ERROR LED and off READY LED.

Power-up tests may be triggered on-demand at any time by power-cycling the module.

7.2 Conditional tests

The module implements the following conditional tests:

- Firmware load test (RSA 2048 bits with SHA256 Signature Verification)
- Manual key entry test is not applicable
- Bypass test is not applicable

Failure to successfully complete these tests will put the module in error state.

7.3 Critical functions tests

As a requirement for [DCI DCSS 1.2] the module also performs power-up and conditional tests on non-Approved cryptographic algorithms and CSPs used in non-Approved Mode of Operation:

- AES 128 bits CBC encryption KAT
- HMAC-SHA1 KAT
- FIPS 186-2 RNG KAT
- SP800-90A DRBG KAT
- RSA 2048 bits with SHA256 Signature verification KAT
- RSA 2048 bits with SHA256 Signature generation KAT
- TLS 1.0/1.1 Key Derivation KAT
- SP800-56B RSA Encryption Primitive KAT
- SP800-56B RSA Decryption Primitive KAT
- FPGA AES 128 bits in CBC decryption KAT
- FPGA HMAC-SHA1 KAT
- Key pair-wise consistency test on all RSA key pairs (sign/verify and encrypt/decrypt)
- Continuous RNG test on NDRNG
- Continuous RNG test on SP800-90A DRBG
- Continuous RNG test on FIPS 186-2 RNG
- Security logs health check

Failure to successfully complete these tests will put the module in error state. Critical functions tests may be triggered on-demand at any time by power-cycling the module.

8 Mitigation of Other Attacks policy

The module is not designed to mitigate attacks outside the scope of FIPS 140-2 requirements.

Table 16 – Mitigation of other attacks

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

9 Security Rules

The requirements for FIPS 140-2 level 2 are enforced in the module's implementation by following the security rules below:

- The module provides a physically contiguous cryptographic boundary without any gaps or other openings; all sensitive circuitry resides within the defined cryptographic boundary.
- The module enforces logical separation between all logical interfaces: data input, data output, control input, status output.
- The module only supports power input over the defined power interface.
- The module enforces a limited operational environment; the module only supports the loading and execution of trusted code that is cryptographically authenticated by Barco via RSA 2048 digital signature.
- The module satisfies the EMI/EMC requirements for FCC Part 15, Subpart B, Class A.
- No Approved security function exists outside the security enclosure.
- Non-Approved security functions used within the cryptographic boundary do not undermine the security of the module.
- The module performs the power-up and conditional tests described in the "self-tests" section of this document.
- The module does not provide any bypass capability.
- The module does not support manual key entry.
- Roles are implicit; therefore users cannot select nor switch roles.
- No maintenance role exists and the module does not implement any maintenance interface or service.
- Identity-based authentication is required for all services involving usage of Approved security functions.
- Authentication states are transient; the authentication states are erased when the module is powered off, requiring operators to log in at each power-cycling of the module.
- The module supports concurrent operators, and maintains separation amongst all concurrent operators.
- The status output interface never carries any key, CSP, secret or any other information whose disclosure could compromise the security of the module.

- The data output interface is disabled during power-up tests and when the module is in error state.
- The data output interface uses data paths that are either physically or logically separated from the process performing key generation or zeroization.
- The module does not input or output plaintext CSPs and no dedicated physical port exists for that purpose.
- The module zeroization can be triggered on-demand at any time by removing the battery.
- Authentication data is obscured while being input.
- Feedback from unsuccessful authentication attempts does not reveal any information that could be used to guess the authentication data.

Appendix A – Critical Security Parameters

The module does not contain any private key, secret key or CSP in the FIPS Approved Mode of Operation.

Appendix B – Public Keys and other public data

Table 17 – Barco Authority public keys

Description	Barco Authority identity keys for Barco Users and Crypto Officers RSA 2048 bits
Generation	N/A
Establishment	N/A
Key Entry	Automated plaintext – Carried by Barco ICMP update packages
Key Output	N/A
Storage	Transient in RAM
Key-To-Entity	Process

Table 18 – Barco Authority Root public key

Description	Barco Authority root signing key for Barco Users and Crypto Officers RSA 2048 bits
Generation	N/A
Establishment	N/A
Key Entry	N/A – Installed at Barco Secure Factory
Key Output	N/A
Storage	Transient in RAM and persistent storage
Key-To-Entity	Process

Table 19 – Update Package signer (public data)

Description	SHA1 certificate thumbprint of the authorized signer for module update packages (NOTE: this "is not" a key.)
Generation	N/A
Establishment	N/A
Key Entry	N/A – this "is not" a key.
Key Output	N/A – this "is not" a key.
Storage	Transient in RAM
Key-To-Entity	N/A – this "is not" a key.

Appendix C – References

[FIPS 140-2] FIPS PUB 140-2 - Security Requirements for Cryptographic Modules
http://csrc.nist.gov/publications/PubsFIPS.html

[FIPS 197] Advanced Encryption Standard - 2001
http://csrc.nist.gov/publications/PubsFIPS.html

[FIPS 198-1] The Keyed-Hash Message Authentication Code (HMAC)
http://csrc.nist.gov/publications/PubsFIPS.html

[FIPS 180-4] Secure Hash Standard (SHS)
http://csrc.nist.gov/publications/PubsFIPS.html

[FIPS 186-2] Digital Signature Standard (DSS)
http://csrc.nist.gov/publications/PubsFIPSArch.html

[FIPS 186-4] Digital Signature Standard (DSS)
http://csrc.nist.gov/publications/PubsFIPS.html

[IETF RFC 2246] The TLS Protocol Version 1.0
http://www.ietf.org/rfc/rfc2246.txt

[NIST SP800-135] Recommendation for Existing Application-Specific Key Derivation Functions
http://csrc.nist.gov/publications/PubsSPs.html

[NIST SP800-90A] Recommendation for Random Number Generation Using Deterministic Random Bit Generators
http://csrc.nist.gov/publications/PubsSPs.html

[DCI DCSS 1.2] Digital Cinema System Specification Version 1.2 with Errata as of 30 August 2012 Incorporated
http://dcimovies.com/specification/index.html

Appendix D – Glossary of terms and acronyms

- **AES**: Advanced Encryption Standard.
- **ANSI**: American National Standards Institute.
- **CSP**: Critical Security Parameter.
- **CA certificate**: Certificate Authority: signing X509 certificate, including self-signed root certificates
- **DCI**: Digital Cinema Initiative. See [DCI DCSS 1.2].
- **DRNG**: Deterministic Random Number Generator.
- **FPGA**: Field Programmable Gate Array.
- **HMAC**: Hashed Message Authentication Code.
- **ICMP**: Integrated Cinema Media Processor. Barco DCI compliant Image Media Block which is the subject of the current certification process.
- **Image Media Block**: see IMB.
- **IMB:** Image Media Block. Type 1 SPB defined by the DCI that hosts the critical security and cryptographic portions of the digital cinema content workflow in an auditorium.
- **KAT**: Known-Answer Test.
- **NDRNG**: Non-Deterministic Random Number Generator. See [FIPS 140-2].
- **RSA**: Rivest-Shamir-Adleman.
- **SE:** Security Entity. Hardware or software block defined by the DCI. Several SEs are defined in [DCI DCSS 1.2] to fulfill specific functions.
- **SHA**: Secure Hash Algorithm.
- **Screen Management System**: see SMS.
- **Secure Processing Block**: see SPB.
- **SMS**: Screen Management System. This is a Security Entity defined by the DCI for the operational management of an auditorium for digital cinema content playback.
- **SPB:** Secure Processing Block. This is a Security Entity defined by the DCI as a hardware component with a physical security perimeter. The ICMP meets the DCI requirements for a type 1 SPB.