Barco ICMP

FIPS 140-2

Non-Proprietary

Security Policy

Table of Content

1 Introduction

The Barco Integrated Cinema Media Processor (ICMP) 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 versions apply for FIPS 140-2 certification:

Table A – Hardware Revision and Firmware Version

Hardware Revision	Firmware Version
R7681133-08	1.1 build 9202
R7681133-12	1.2 build 10163B

1.1 Security Level

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

Table 1 – Security levels

Security Requirements Section	Level
Cryptographic Module Specifications	3
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	2
Mitigation of Other Attacks	N/A

1.2 Cryptographic Boundary

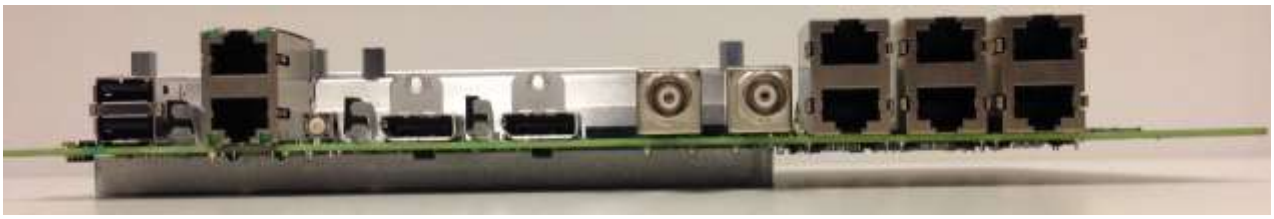
The cryptographic boundary is defined by the outer perimeter of the main board's PCB. It is outlined in red in the below picture.

Picture 1 – Barco ICMP main board bottom view

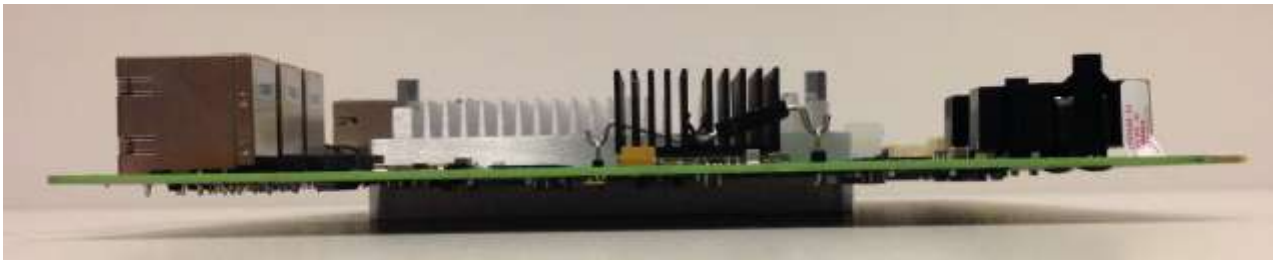
All security related components are enclosed within a opaque metal cover and protected by tamper detection and response mechanisms. It is outlined in yellow in the above picture.

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

Picture 2 – Barco ICMP main board top view



Picture 3 – Barco ICMP main board front view



Picture 4 – Barco ICMP main board right view

Picture 5 – Barco ICMP main board left view

Picture 6 – Barco ICMP main board rear 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 FIPS 140-2 Approved Mode of Operation

The module only performs in a FIPS Approved mode of operation. This mode is invoked when the operator powers up the projector host.

Indication that the module has successfully performed all the power-up tests and has entered Approved mode of operation is given by a green status of both the Power/Error and the Ready LEDs.

Picture 7 – Barco ICMP full assembly front panel with highlighted Power/Error LED

System logs can also be extracted from from the module using the ExportSystemLog service. Such logs include hardware, firmware and software components versions and they shall match the versions listed in the introduction section.

Note that when the cryptographic module is in an error state, e.g. due the power-up tests failure, the Power/Error LED is the only available indicator and shows a static red status .

1.3.1 Approved cryptographic algorithms

In FIPS Approved mode of operation, the module uses the following Approved cryptographic algorithms:

- AES 128 bits in CBC mode: encryption and decryption – certificate #2725
- AES 128 bits in ECB mode: encryption only – certificate #2725
- HMAC-SHA1 (128 bits) – certificate #1704
- ANSI X9.31 Appendix A.2.4 DRNG with AES 128 bits – certificate #1262
- FIPS 186-2 Appendix 3.1 and 3.3 DRNG (with Change Notice 1 General Purpose accommodations) – certificate #1262
- SHA1 – certificate #2295
- SHA256 – certificate #2295

- RSA with 2048 bits modulus Key Generation – certificate #1418
- RSA with 2048 bits modulus Digital Signature Generation – certificate #1418
- RSA with 2048 bits modulus Digital Signature Verification – certificate #1418
- TLS 1.0/1.1 Key Derivation (CVL) – certificate #178
- [FPGA implementation] AES 128 bits in CBC mode: decryption only – certificate #2726
- [FPGA implementation] HMAC-SHA1 (128 bits) – certificate #1705
- [FPGA implementation] SHA1 – certificate #2296

Users should reference the transition tables that will be available at the CMVP Web site (http://csrc.nist.gov/groups/STM/cmvp/). The data in the tables will inform users of the risks associated with using a particular algorithm and a given key length.

1.3.2 Non Approved cryptographic algorithms

In FIPS Approved mode of operation, the module also uses the following non-Approved cryptographic algorithms:

- MD5 and HMAC-MD5 used in TLS 1.0
- Hardware NDRNGs used to seed the ANSI X9.31 DRNG
- RSA with 2048 bits modulus Key: encryption and decryption: used for key unwrapping and TLS 1.0 key establishment. NOTICE: only used by the cryptographic module as a non-Approved but allowed method of commercially available key establishment and "is not" used by the cryptographic module for any other purposes whatsoever.
- EC Diffie-Hellman used for non-security relevant legacy communication protocols and considered plaintext from a FIPS standpoint

2 Ports and Interfaces

The module provides the following physical ports and logical interfaces:

Table 1 – 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
AES3 audio interfaces (Qty. 2)	Data Output
Display Port interfaces (Qty. 2)	Control Input Data Input Data Output
GPIO input interfaces (Qty. 2)	Data Input
GPIO output interfaces (Qty. 2)	Data Output
USB 2.0 (Qty. 2)	Data Input
USB 3.0 (Qty. 2)	Data Input
LEDs (Qty. 20)	Status output
Reset (Qty. 1)	Control Input
LTC sync input connector (Qty. 1)	Control Input
LTC sync output connector (Qty. 1)	Data Output
Backplane interface (Qty. 1)	Control Input Data Input Data Output Status Output Power
Laser port (Qty. 1)	Data Input Data Output
PCIe storage controller (Qty. 1)	Data Input Data Output Power
HDD removal tamper interface	Data Input
HDD power output (Qty. 2)	Power
MicroSD card holder port (Qty. 1)	Data Input
Security Mezzanine interface (Qty. 1)	Data Input
Video Mezzanine interface (Qty. 1)	Data Input Data Output
Audio Mezzanine interface (Qty. 1)	Data Input Data Output
Battery holders +3V (Qty. 2)	Power

3 Identification and Authentication policy

3.1 Roles

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

Table 2 – Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication data
User-Monitoring	Identity-Based	Authentication password
User-Projectionist	Identity-Based	Authentication password
User-ShowManager	Identity-Based	Authentication password
User-Administrator	Identity-Based	Authentication password
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 3 – Strength of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Authentication Password	The password is required to use visible ASCII characters: 95 characters are possible. The module checks for a minimum length of 8 characters which brings the probability of success or false acceptance to less than 1/1000000: 1/95^8 = 1,507339769528871500598329601124 8e-16 The module ensures that no more than 1000 attempts are possible per second. The probability of success or false acceptance within one minute is less than 1/100000: 1000*60/95^8 = 9,044083837366314869734995556637e-11
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 = 1,925929944387235853055977942584 9e-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 = 5,777789833161707559167933827754 8e-32

4 Critical Security Parameters

4.1 Private keys, secret keys and other CSPs

All CSPs hosted on the module are listed below. These parameters are protected from unauthorized modification, substitution and disclosure, and therefore submitted to active zeroization.

- **IMB-Projector Identity private key**: RSA 2048 bits private key used for key unwrapping, data decryption and TLS server operations
- **IMB Log Signer private key**: RSA 2048 bits private key used for document signing
- **SMS Identity private key**: RSA 2048 bits private key used for TLS client operations
- **HTTPS Server private key**: RSA 2048 bits private key used for HTTPS server operations
- **TLS pre-master secret**: transient data used in TLS 1.0 key establishment
- **TLS master secret**: transient data used in TLS 1.0 key establishment
- **TLS AES keys**: transient AES 128 bits keys used in TLS 1.0 bulk encryption
- **TLS HMAC keys**: transient HMAC key used in TLS 1.0 integrity mechanism
- **ANSI X9.31 DRNG seed values**: transient data used to seed the Approved ANSI X9.31 DRNG
- **ANSI X9.31 DRNG states**: ANSI X9.31 DRNG internal states
- **Essence keys**: transient AES 128 bits keys used to protect digital cinema content
- **Essence HMAC keys**: transient HMAC keys used to check digital cinema content integrity
- **CSP wrapping key**: AES 128 bits key used to encrypt CSPs on the module
- **User authentication secret**: authentication data used for identity-based authentication
- **User authentication data**: authentication data used for identity-based authentication
- **Update Package decryption key**: AES 128 bits key used to decrypt module update packages
- **FIPS 186-2 DRNG XKEY**: seed key for Approved FIPS 186-2 DRNG
- **FIPS 186-2 DRNG states:** FIPS 186-2 DRNG internal states

4.2 Public keys and other public data

All public keys hosted on the module are listed below. These keys are protected from unauthorized modification and substitution but are not submitted to active zeroization.

- **IMB-Projector Identity public key**: RSA 2048 bits public key used for TLS server operations and carried within an X509 certificate
- **IMB Log Signer public key**: RSA 2048 bits public key carried within an X509 certificate
- **SMS Identity public key**: RSA 2048 bits public key used for TLS client operations and carried within an X509 certificate
- **HTTPS Server public key**: RSA 2048 bits public key used for HTTPS server operations and carried within an X509 certificate
- **ICMP CA public keys**: IMB, SMS and HTTPS RSA public keys carried within CA and root X509 certificates
- **Barco Crypto Officer public keys**: transient RSA public keys used to identify a Barco Crypto Officer and carried within leaf and CA X509 certificates
- **Barco Crypto Officer root public key**: Barco Security Officer RSA public key used to authenticate Barco security officers and carried within a root X509 certificate
- **Content signer public keys**: transient RSA public keys used to authenticate digital cinema package files (DCPs) and carried within X509 certificates
- **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 provide a list of services requiring operator authentication and map authorized roles and CSP access for each service.

Available roles are:

- **M**: User-Monitoring
- **P**: User-Projectionist
- **S**: User-ShowManager
- **A**: User-Administrator
- **CO**: Barco Crypto Officer

Table 4 – HTTPS Services

M	P	S	A	CO	Services	Cryptographic Keys and CSPs	Type(s) of Access
x	x	x	x		**Get User List:** read module user list for operator login	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP wrapping key User authentication secret User authentication data ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
x	x	x	x		**Information:** read various module information (make, model, version info, certificate list, license status…)	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP wrapping key ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
x	x	x	x		**Status:** read various status information from the module	HTTPS Server private key HTTPS Server public key SMS Identity private key	Read

					(player, projector, ingest, content, scheduler, storage, recovery…)	SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP wrapping key ICMP CA public keys	
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
			x		**Export System Logs:** export operational logs	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP wrapping key IMB Log Signer private key IMB Log Signer public key ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
			x		**License Manager:** add/remove licenses to enable/disable product features	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP wrapping key ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
						Barco Crypto Officer public keys Barco Crypto Officer root public key	Read
		x	**x**		**Content Manager:** content and key management: add/remove, ingest jobs, external storage…	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP wrapping key ICMP CA public keys	Read

						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
						Content signer public keys	Read
		x	**x**		**Show Editor:** add/remove, select, edit…	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP wrapping key ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
		x	**x**		**Schedule Editor:** add/remove, select, edit…	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP wrapping key ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
	x	**x**	**x**		**Player Control:** clear, select, play/resume, pause/stop, positioning…	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP wrapping key ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
						Essence keys	Read
						Essence HMAC keys	Read

						FIPS 186-2 DRNG XKEY FIPS 186-2 DRNG states	Write
						Content signer public keys	Read
	x	**x**	**x**		**Projector Control:** lamp, dowser, macro execution, test patterns…	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP Wrapping key ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
			x		**Settings:** read or write module and user settings	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP Wrapping key ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
						User authentication data	Read Write
			x		**Security Logs Export:** export DCI security log report from the module	HTTPS Server private key HTTPS Server public key SMS Identity private key SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP Wrapping key IMB Log Signer private key IMB Log Signer public key ICMP CA public keys	Read
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write
			x		**Adjust RTC:** module real time clock adjustment	HTTPS Server private key HTTPS Server public key SMS Identity private key	Read

					within valid DCI range	SMS Identity public key IMB-Projector Identity private key IMB-Projector Identity public key CSP Wrapping key ICMP CA public keys	
						TLS pre-master secret TLS master secret TLS AES keys TLS HMAC keys ANSI X9.31 DRNG seed values ANSI X9.31 DRNG states	Read Write

Table 5 – Barco Crypto Officer Services

Roles	Services	Cryptographic Keys and CSPs and other public data	Type(s) of Access
Barco Crypto Officer	**Update package validation:** authenticate the update package and perform actual update	Barco Crypto Officer public keys Barco Crypto Officer root public key	Read
		Update Package Signer (public data) Update Package decryption key	Read

5.2 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 6 – HTTPS Unauthenticated Services

Services	Cryptographic Keys and CSPs	Type(s) of Access
Operator Login: operator login/logout	None	N/A

Table 7 –Other ICMP Unauthenticated Services

Services	Cryptographic Keys and CSPs	Type(s) of Access
FTP Server: FTP server for Barco update package upload, security and system logs download and local storage access	None	N/A
Display Port 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

Additionally the following services require legacy user authentication through EC Diffie-Hellman. From a FIPS 140-2 perspective they are considered plaintext as they make no use of any Approved security function.

Table 8 – Unauthenticated Update Services

Services	Cryptographic Keys and CSPs	Type(s) of Access
Version: read versions of currently installed components	None	N/A
Login/Logout: legacy protocol authentication mechanism	None	N/A
Install Update Package: trigger update package installation and read progress status	None	N/A
Remove Web Update Package: fall back to the original web package	None	N/A
Identifier: read the module's identification string	None	N/A

Table 9 – Legacy IMB Unauthenticated Services

Services	Cryptographic Keys and CSPs	Type(s) of Access

System Status: get various status information from the module (general, system or security)	None	N/A
Version: get version information	None	N/A
Login/Logout: legacy protocol authentication mechanism	None	N/A
Serial Number: get the module serial number	None	N/A
Get Certificate: read out available device certificates	IMB-Projector Identity certificate IMB Log Signer certificate	Read
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	None	N/A
Identifier: read the module's identification string	None	N/A

Table 10 – Legacy Projector Unauthenticated Services

Services	Cryptographic Keys and CSPs	Type(s) of Access
Projector Control commands: processing path selection, macro execution, input port selection…	None	N/A
File Management commands: read/write/copy/delete projector files	None	N/A
Image Control commands: brightness, hue, saturation…	None	N/A
Port Configuration: RS-232 and Etherner port configuration	None	N/A
Composite/Overlay commands: subtitle control	None	N/A
General System commands: read status, version, legacy protocol login/logout…	None	N/A
3D commands: control	None	N/A
System Administration commands	None	N/A

5.3 Zeroization service

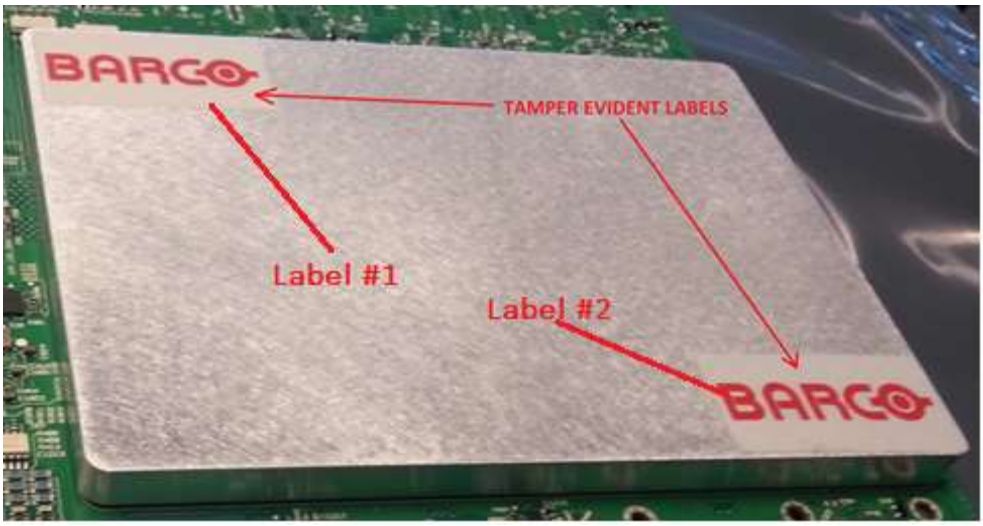
Since zeroization can be triggered by any operation by removing the module's battery or issuing the zeroization command, no other zeroization service exists within the module.

6 Physical Security policy

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 11 – 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 and the Power/Error LED status is static red) - 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 below.
Tamper-evident void labels on the metal cover fasteners	- At module installation - On suspicion of tampering (module is unresponsive and the Power/Error LED status is static red) - Regular inspection is recommended	Visual inspection for visible scratches or scrapes, signs of tearing or damage. See picture below.
Tamper-responsive zeroization mechanisms	- On suspicion of tampering (module is unresponsive and the Power/Error LED status is static red) - Regular inspection of the battery level is necessary	Perform the above inspections to confirm the hard metal cover was not tampered with. Check the Power/Error LED status. Confirm the module's battery is in place. Consult the manufacturer manuals for battery level monitoring.



Picture 8 – 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 the above inspections.

7 Self-tests

7.1 Power-up tests

The module implements the following power-up tests:

- AES 128 bits CBC encryption KAT
- AES 128 bits CBC decryption KAT
- HMAC-SHA1 (128 bit key) KAT
- ANSI X9.31 Appendix A.2.4 DRNG with AES 128 bits KAT
- FIPS 186-2 Appendix 3.1 and 3.3 DRNG (with Change Notice 1 General Purpose accommodations) KAT
- RSA 2048 bits with SHA256 Signature generation KAT
- RSA 2048 bits with SHA256 Signature verification KAT
- TLS 1.0/1.1 Key Derivation KAT
- FPGA AES 128 bits in CBC decryption KAT
- FPGA HMAC-SHA1 (128 bit key) KAT
- Software and firmware components integrity tests using a 32 bits EDC

Successful completion of power-up tests is a primary condition for the module to reach the FIPS Approved mode of operation. A green status of the Power/Error LED is an indicator that the power-up tests completed successfully. A red LED means the module is in error state and if further information is required as to which power-up test failed, operational logs must be extracted for examination.

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:

- Key pair-wise consistency test on all RSA key pairs (sign/verify or encrypt/decrypt depending on key usage)
- Firmware load test (RSA 2048 bits with SHA-256 Signature Verification)
- Manual key entry test is not applicable
- Continuous RNG test on all Approved DRNGs
- Continuous RNG test on non-Approved hardware NDRNG
- Bypass test is not applicable

8 Mitigation of Other Attacks policy

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

Table 12 – 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 SHA-256 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 only performs in a FIPS Approved mode of operation.
- 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 and manipulation of CSPs.
- 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.
- The FIPS 186-2 DRNG is seeded via an XKEY that is generated outside of the cryptographic boundary and entered into the cryptographic module wrapped (encapsulated) via RSA 2048. The 2048 bit RSA wrap (encapsulation) has an equivalent comuptational resistance to attack of 112 bits as per SP800-57. Therefore the module generates keys (Essence HMAC Keys) whose strengths are modified by available entropy (i.e. 112 bits of equivalent computational resistance to attack).

Appendix A – 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

[ANSI X9.31] NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms
http://csrc.nist.gov/groups/STM/cavp/index.html#04

[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

[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 B – 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 which specifically means the module must meet the physical security requirements for FIPS 140-2 level 3.