Dolphin Board

FIPS 140-2 Level 3 Validation

Security Policy

Version 1.5

Table of Contents

1 Introduction

1.1 Purpose

This document is a non-proprietary Cryptographic Module Security Policy for the Doremi Labs Dolphin board. It describes how this module meets all the requirements specified in the FIPS 140-2 for security Level 3. This Policy forms a part of the submission package provided to the testing lab.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2) specifies the security requirements for a cryptographic module protecting sensitive information. Based on four security levels for cryptographic modules this standard identifies requirements in eleven sections. For more information about the standard, visit:

http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

1.2 References

This Security Policy describes how this module complies with the eleven sections of the standard.

- For more information on the FIPS 140-2 standard and validation program, please refer to the NIST website at http://csrc.nist.gov/cryptval/.
- For more information about Doremi Labs solutions, please visit the following website: http://www.doremilabs.com/

2 Dolphin Board Overview

The Dolphin board is a PCI-card that provides a standard-definition/high-definition serial digital interface. This is the Doremi decoder card that contains the JPEG-2000 decoder hardware and BNC serial digital interface connectors used in the Doremi DCP-2000 Digital Cinema Server.

The Dolphin board utilizes a dual-link encoded serial digital interface for output of DCI-compliant resolutions up to 2048x1080p24 (2K-film). It can also operate single-link for lower resolution material (i.e. trailers, advertisements, etc.).

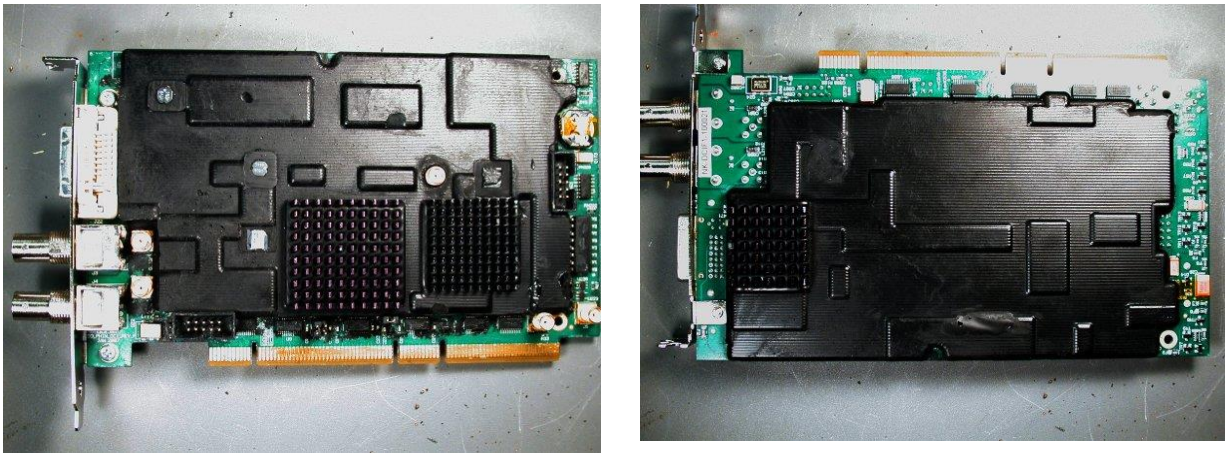

Figure 1: Dolphin Board

The Dolphin board has been designed for compliance with FIPS 140-2, Level 3 requirements.

3 FIPS 140-2 Mode of Operation

The module only provides a FIPS approved mode of operation. This mode of operation makes use of approved algorithms and also supports non-approved algorithms that are allowed in a FIPS approved mode of operation.

In order to verify that the module is in a FIPS approved mode of operation the operator shall ensure that the FW and HW are the FIPS approved versions. The versions should match those listed on the validation certificate or found on the cryptographic module validation list webpage (http://csrc.nist.gov/cryptval/140-1/140val-all.htm). The operator shall also ensure that all self tests pass and that the module transitions into operational mode.

3.1 Approved Algorithms

The Dolphin board supports the following algorithms approved for use in a FIPS mode of operation:

- AES (FPGA implementation) with 128 bit keys for encryption in ECB mode and decryption in CBC mode – see Certificate #532
- AES with 128 bit keys for encryption and decryption in ECB mode – see Certificate #521
- HMAC-SHA1 – see Certificate #271
- SHA-1, used by other algorithms (like HMAC-SHA1 or FIPS 186-2 RNG) – see Certificate #593
- NIST-Recommended RNG based on ANSI X9.31, Appendix A.2.4 – see Certificate #326
- FIPS 186-2 RNG with change notice – see Certificate #297

3.2 Non-Approved Algorithms

The Dolphin board also supports the following non-approved algorithms that are allowed for use in a FIPS mode of operation:

- RSA Decryption (modulus 2048) – used for key unwrapping only, key establishment methodology provides 112 bits of strength
- TRNG (RNG Hardware based) – used to seed the approved RNG based on ANSI X9.31 presented in paragraph 3.1.

4 Security Levels

The Dolphin board design, development, tests and production has satisfied the requirements to ensure a secure product. It is especially adapted to Digital Cinema security requirements.

The Dolphin board, Hardware Model ***DOLPHIN-DCI-F***, firmware versions ***22.00-0*** and ***22.00-1***, is tested to meet the FIPS security requirements for the levels shown in the following table. The overall module is tested FIPS 140-2 Security Level 3.

Table 1 – FIPS 140-2 Security Level

FIPS 140-2 Security Requirements	Section Level
1. Cryptographic Module Specification	3
2. Module Ports and Interfaces	3
3. Roles, Services and Authentication	3
4. Finite State Model	3
5. Physical Security	3
6. Operational Environment	N/A
7. Cryptographic Key Management	3
8. EMI/EMC	3
9. Self Tests	3
10. Design Assurance	3
11. Mitigation of Other Attacks	N/A
FIPS Overall Level	3

5 Module Interfaces

The following table lists the logical interfaces of the module and how they map to physical interfaces:

Table 2 – FIPS 140-2 Logical Interfaces

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	PCI interface, GPIO connector, SDI dual HD input
Data Output Interface	PCI interface, SDI dual HD output, GPIO connector, Audio connector, LTC (time code) output connector, Host Reset connector
Control Input Interface	PCI interface, Reset connector, Video sync. Input
Status Output Interface	PCI interface, Serial Port, Video sync. Output
Power Interface	PCI interface, Battery

No maintenance access interface is present.

6 Critical Security Parameters

6.1 Secret and Private Keys and Other CSPs

The secret and private keys that exists within the cryptographic module are identified below:

1. Device Private Key – Private RSA Key used for key transport.
2. External Private Key – Private RSA Key unused by the module, stored in the module for convenience only.
3. Content Encryption Keys – AES Keys that protect content.
4. Cinelink Keys – AES Keys used by the AES FPGA algorithm (see Certificate #532) during the Cinelink processing.
5. Seed Values – Used to seed the FIPS approved RNGs.
6. AES Shared Knowledge Key – AES Key used to secure import/export of Critical Security Parameters.
7. Doremi HMAC Key – HMAC Key used for Firmware Load Test.
8. Content Integrity Keys – HMAC keys used to verify the integrity of encrypted content.
9. Authentication Secrets – The Authentication Secrets used by the module are identified below:
    - Crypto-Officer authentication secret – 8 characters.
    - User authentication secret – 8 characters.

6.2 Public Keys

Public keys are not considered as Critical Security Parameters because of their public status. The public keys contained in the module are listed below for consistency:

2. Device Public Key – Public RSA key unused by the module, stored in the module for key storage purposes only.
3. External Public Key – Public RSA key unused by the module, stored in the module for key storage purposes only.

7 Roles and Services

The cryptographic module supports two distinct operator roles: Cryptographic Officer (Crypto-Officer) and User. No maintenance role is supported. The Crypto-Officer has access to all services while the User has only access to a subset of these services as identified in the paragraph **7.2**.

7.1 Crypto-Officer Specific Services

Table 3 below summarizes specific services available to the Crypto-Officer only. The Crypto-Officer also has access to all the services available to the User – see section **7.2**.

Table 3: Crypto-Officer Specific Services

Service	Description	Input	Output	CSP	Types of Access to CSP
Set Device Public Key	Imports the Device Public Key into module – service allowed only if no Device Public Key already exits in the module	Device Public key	-	-	N/A.
Set Device Private Key	Imports the Device Private Key into module – service only allowed if no Device Private Key already exits in the module	Encrypted Device Private Key	-	Device Private Key	Write
				AES Shared Knowledge Key	Read
Set Serial Number	Imports the Serial Number -Service only allowed if no Serial Number is present	Serial Number	-	-	N/A.
Set External Public Key	Imports the External Public Key into the module – service only allowed if no External Public Key already exits in the module	External Public Key	-	-	N/A.
Set External Private Key	Imports the External Private Key into the module – service only allowed if no External Private Key already exits in the module	Encrypted External Private Key	-	External Private Key	Write
				AES Shared Knowledge Key	Read
Reset Identity	Destroys the following parameters: - Private/Public keys - Content Encryption Keys - Content Integrity Keys - Cinelink Keys - Seeds - Serial Number - Time value	-	-	All Private Keys, Content Encryption Keys, Content Integrity Keys, Cinelink Keys and Seeds	Write

Service	Description	Input	Output	CSP	Types of Access to CSP
Zeroization	Zeroizes CSPs and Public Keys.	-	-	All CSPs	Write

7.2 Crypto-Officer and User Common Services

Table 4 below presents all the services available to both the Crypto-Officer and the User.

Table 4: Crypto-Officer and User Common Services

Service	Description	Input	Output	CSP	Types of Access to CSP
Get GPI Data	Exports GPI data through PCI interface	-	GPI data	-	N/A.
Load GPO Data	Imports GPO data through PCI interface in order it can be exported through the GPIO connector	GPO data	-	-	N/A.
Get GPO Data	Exports GPO data through PCI interface	-	GPO data	-	N/A.
Get Update Status	Provides status information concerning update process	-	Update Status	-	N/A.
RSA KDM Block Decryption	Imports and decrypts an RSA KDM cipher block. Then, exports decrypted data without the Content Encryption Key itself	KDM Cipher Block	Decrypted data without the Content Encryption Key itself	Device Private Key	Read
				Content Encryption Key	Write
Generate Cinelink Data	Generates and exports Cinelink data	Number of Cinelink Keys to generate	Encrypted Cinelink data	Cinelink Keys	Write
				AES Shared Knowledge Key	Read
Watermark Data Import	Imports Watermarking data into the module and decrypts them	Encrypted Watermarking Data	-	AES Shared Knowledge Key	Read
Get Mcore Status	Provides status related to Micro-controller command	-	MCore Status	-	N/A.
Configure Audio	Sets the audio configuration parameters of the module	Audio configuration parameters	-	-	N/A.
Get Audio Configuration	Exports the current audio configuration parameters	-	Audio configuration parameters	-	N/A.

Service	Description	Input	Output	CSP	Types of Access to CSP
Set DMA Configuration	Sets the transfer DMA configuration parameters and/or executes a transfer DMA	Transfer DMA data	-	Doremi HMAC Key in case of firmware upload	N/A.
Get DMA Configuration	Exports the transfer DMA configuration parameters	-	DMA configuration parameters	-	N/A.
Get DMA Interrupt Status	Exports DMA interrupt status	-	DMA Interrupt Status	-	N/A.
Configure Video	Sets video configuration parameters	Video configuration parameters	-	-	N/A.
Get Video Configuration	Provides video configuration parameters	-	Video configuration parameters	-	N/A.
Set Video Interrupt	Enable or disable video interrupt	Video interrupt configuration	-	-	N/A.
Get Video Interrupt status	Exports status of video interrupt	-	Video interrupt status	-	N/A.
Configure ADV	Sets ADVs configuration parameters	ADVs configuration parameters	-	-	N/A.
Get ADV Configuration	Exports ADVs configuration parameters	-	ADVs configuration parameters	-	N/A.
Configure OSD	Sets OSD configuration parameters	OSD configuration parameters	-	-	N/A.
Get OSD Configuration	Exports OSD configuration parameters	-	OSD configuration parameters	-	N/A.
Configure AES	Sets AES algorithm configuration parameters	AES configuration parameters	-	-	N/A.
Get AES Configuration	Exports AES algorithm configuration parameters	-	AES configuration parameters	-	N/A.

Service	Description	Input	Output	CSP	Types of Access to CSP
Get Firmware Version	Provides the version of the current firmware	-	Firmware version	-	N/A.
Get Firmware Capabilities	Provides capabilities of the firmware	-	Firmware capabilities	-	N/A.
Get Device Public Key	Exports the Device Public Key present in the module	-	Device Public Key	-	N/A.
Get Serial Number	Exports the Serial Number of the module	-	Serial Number	-	N/A.
Get External Public Key	Exports the External Public Key	-	External Public key	-	N/A.
Get External Private Key	Exports the External Private Key encrypted in AES	-	Encrypted External Private key	External Private key	Read
				AES Shared Knowledge Key	Read
Find Content Encryption Key	Provides the Content Encryption Key offset in the module's memory	Key Id	Offset	-	N/A.
Add Content Encryption Key	Writes into memory the Content Encryption Key and associated Key Id resulting from a KDM cipher block decryption	Key Id	Offset	Content Encryption key	Write
Copy Content Encryption Key	Provides the required Content Encryption Key to the FPGA	Content Encryption Key Offset	-	Content Encryption Key	Read Write
Copy Cinelink Key	Provides the required Cinelink Key to the FPGA	Cinelink Key Offset	-	Cinelink Key	Read Write
Purge Key	Delete a specific Content Encryption Key	Offset	-	Content Encryption Key	Write
Get Content Encryption Keys Status	Exports Content Encryption Keys status: number of Content Encryption Keys used and maximum allowed number of such Keys.	-	Content Encryption Keys status	-	N/A.
Check Content Encryption Key	Check if the Content Encryption Key is already present	Key Id	-	-	N/A.

Service	Description	Input	Output	CSP	Types of Access to CSP
Get Content Integrity Key	Generates, encrypts and exports a Content Integrity Key corresponding to a specific Content Encryption Key	Content Encryption Key offset	Encrypted Content Integrity Key	Content Encryption Key	Read
				Content Integrity Key	Write
				AES Shared Knowledge Key	Read
Set Time	Sets time if not present or Adjusts Time if the amount of already adjusted time per year is less than the DCI maximum allowed	Time value	-	-	N/A.
Get Time	Exports the time value	-	Time value	-	N/A.
Configure Watchdog	Configures the Watchdog	Watchdog configuration parameters	-	-	N/A.
Get Watchdog status	Exports the current Watchdog configuration	-	Watchdog configuration	-	N/A.

7.3 Unauthenticated Services

The cryptographic module supports the following unauthenticated services:

Table 5: Unauthenticated Services

Service	Description	Input	Output	CSP	Types of Access to CSP
Get Session Id	Exports the current Session Id of the module	-	Session Id	-	N/A.
Authentication	Imports authentication data to perform user authentication – or a user switch if already logged as an authorized user	AES encrypted authentication data (authentication secret and current Session Id)	-	Authentication Secrets	Read
				AES Shared Knowledge Key	Read
Show Status	This “service” corresponds to the status information exported automatically through the Serial Port	-	Status	-	N/A.
GPI Data Import	Gets GPI data from the GPIO connector	GPI data	-	-	N/A.
GPO Data Export	Exports GPO data through the GPIO connector	-	GPO data	-	N/A.

Service	Description	Input	Output	CSP	Types of Access to CSP
Video Import	Imports video from the HD-SDI input and exports it through the HD-SDI output “as-is” and only if allowed by the video configuration parameters – otherwise, no video import is possible. Note that no processing is applied to the video before being exported in this service.	Video	Video	-	N/A.
Host Reset	Resets the host	-	-	-	N/A.
Reset	Resets the module from the host	-	-	-	N/A.

The power recycling of the Dolphin board allows executing the suite of power-up tests required by FIPS 140-2. No other defined service allows executing these power-up tests. It has to be considered as an unauthenticated service as it only requires the Dolphin board to be powered-off and powered-on again.

Note: GPIO data are just data routed through the Dolphin board for external usages, but no processing is applied on them and they are not in relation with other Dolphin board information.

7.4 Authentication Strength

The cryptographic module enforces the separation of roles using identity-based operator authentication. The Crypto-Officer role is authenticated through the use of “Crypto-Officer authentication secret” – known by Doremi Labs only – associated with the current Session Id while the User role is authenticated through the use of the “User authentication secret” associated with the current Session Id.

Note that data to be compared to authentication secrets are imported encrypted in the module.

Table 6: Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Data
User	Identity-based operator authentication	Authentication Secret
Crypto-Officer	Identity-based operator authentication	Authentication Secret

Table 7: Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Authentication Secret Verification	With 256 possible characters and 8-character Authentication Secret, the probability that a random attempt will succeed or a false acceptance will occur is $5.42 \times 10^{-}(20)$ that is less than 1/1,000,000. The probability of successfully authenticating to the module within one minute with a replay delays of 200 ms is $1.63 \times 10^{-}(17)$ that is less than 1/100,000.

8 Physical Security

The Dolphin board is classified as a multiple-chip embedded module for FIPS purposes.

The physical security mechanism employed by the module is a hard, opaque and tamper-evident epoxy material. The tamper evident epoxy coverage shall be periodically inspected to ensure that physical security is maintained. Components excluded from the cryptographic boundary are not security relevant.

9 Operational Environment

This Dolphin board supports a limited operational environment that only allows the loading of trusted, validated, and hashed firmware images through authenticated service. Doremi Labs maintains sole possession of the corresponding HMAC key needed to validate the uploaded firmware into the Dolphin board (the firmware load test is based on HMAC-SHA1).

10 Self-Tests

The module performs the following self-tests:

- Power Up Self-tests
    - Firmware Integrity Test
    - AES encryption/decryption known answer tests
    - HMAC-SHA1 known answer test
    - RSA Decryption known answer test
    - ANSI X9.31 RNG known answer test (NIST-Recommended RNG Based on ANSI X9.31 Annex A.2.4)
    - FIPS 186-2 RNG known answer test
- Conditional Tests
    - Continuous ANSI X9.31 RNG Test (NIST-Recommended RNG Based on ANSI X9.31 Annex A.2.4)
    - Continuous FIPS 186-2 RNG Test
    - Continuous TRNG Test (Hardware RNG Test)
    - Firmware Load Test

11 Mitigation of Other Attacks

The Dolphin board does not mitigate any specific attacks beyond the scope of FIPS 140-2 requirements.

12 Security Rules

The cryptographic module's design corresponds to the module's security rules. This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

1. The cryptographic module shall provide two distinct operator roles. These are the User role and the Cryptographic-Officer role.
2. The cryptographic module shall provide identity-based authentication.
3. When the module has not been placed in a valid role, the operator shall not have access to any cryptographic services.
4. Data output shall be inhibited during key generation, self-tests, zeroization, and error states.
5. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
6. The module shall not support a bypass capability or a maintenance interface.
7. The cryptographic module performs the following tests:

- Power Up Self-tests
    - Firmware Integrity Test
    - AES encryption/decryption known answer tests
    - HMAC-SHA1 known answer test
    - RSA Decryption known answer test
    - ANSI X9.31 RNG known answer test (NIST-Recommended RNG Based on ANSI X9.31 Annex A.2.4)
    - FIPS 186-2 RNG known answer test
- Conditional Tests
    - Continuous ANSI X9.31 RNG Test (NIST-Recommended RNG Based on ANSI X9.31 Annex A.2.4)
    - Continuous FIPS 186-2 RNG Test
    - Continuous TRNG Test (Hardware RNG Test)
    - Firmware Load Test (HMAC verification)

8. At any time the operator is capable of commanding the module to perform the power-up self-test.
9. Prior to each use, the ANSI X9.31 DRNG, FIPS 186-2 and the hardware based NDRNG is tested using the conditional test specified in FIPS 140-2 §4.9.2.

10. Data output is inhibited during key generation, self-tests, zeroization, and error states.
11. The module does not support concurrent operators.

13 Acronyms

Term	Definition
AES	Advanced Encryption Standard
CSP	Critical Security Parameter
DCI	Digital Cinema Initiative
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
GPI	General Purpose Input
GPIO	General Purpose Input/Output
GPO	General Purpose Output
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OSD	On Screen Display
PCI	Peripheral Component Interconnect
RNG	Random Number Generator
RSA	Rivest, Shamir and Adleman
SHA	Secure Hash Algorithm
TRNG	True Random Number Generator

14 Document Revision History

Date	Version	Description
05/10/2007	1.0	First version
05/11/2007	1.1	Minor editorial changes
06/15/2007	1.2	All sections revised
09/18/2007	1.3	Updated to reflect comments from NIST
10/22/2008	1.4	Editorial change
03/29/2013	1.5	Company name changed to Doremi Labs