Dolphin DCI 1.2

FIPS 140-2 Level 3 Validation

Non-Proprietary Security Policy

Version 1.0

Table of Contents

1 Introduction

1.1 Purpose

This document is a non-proprietary Cryptographic Module Security Policy for the Doremi Cinema LLC Dolphin DCI 1.2. 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.

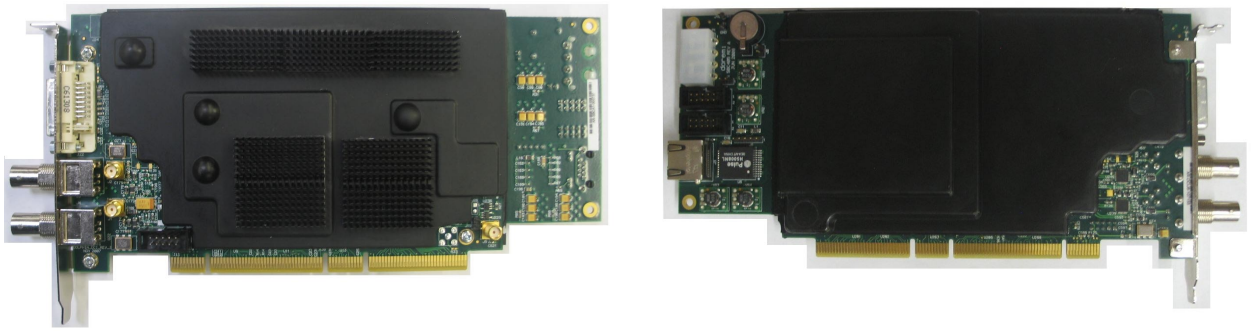
- For more information on the FIPS 140-2 standard and validation program, please refer to the NIST website at http://csrc.nist.gov/cryptval/.
- For more information about Doremi Cinema LLC solutions, please visit the following website: http://www.doremicinema.com/

2 Dolphin DCI 1.2 Overview

The Dolphin DCI 1.2 is a PCI-card that provides a standard-definition/high-definition serial digital interface. This is a Doremi decoder card that contains the JPEG-2000 decoder hardware and BNC serial digital interface connectors used in Doremi Digital Cinema servers like the DCP-2000.

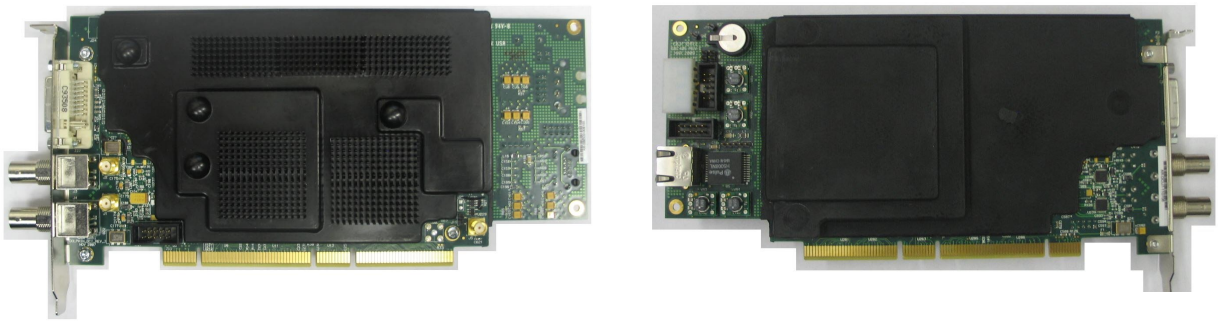
The Dolphin DCI 1.2 utilizes a dual-link encoded serial digital interface for output of DCI-compliant resolutions up to 2048x1080p24 (2K-film). It can also operate single-link for lower resolution material (i.e. trailers, advertisements, etc.).

The pictures below present the four Dolphin DCI 1.2 hardware models:



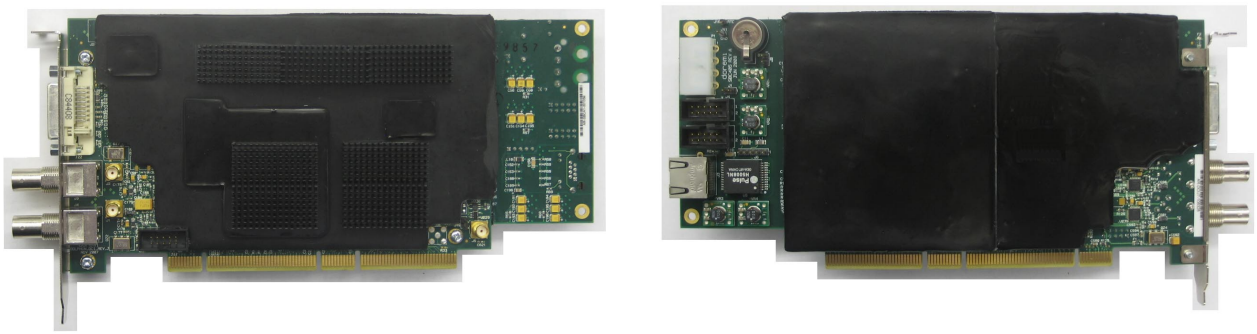
Front View Rear View

Figure 1: Hardware Model DOLPHIN-DCI-1.2-A0



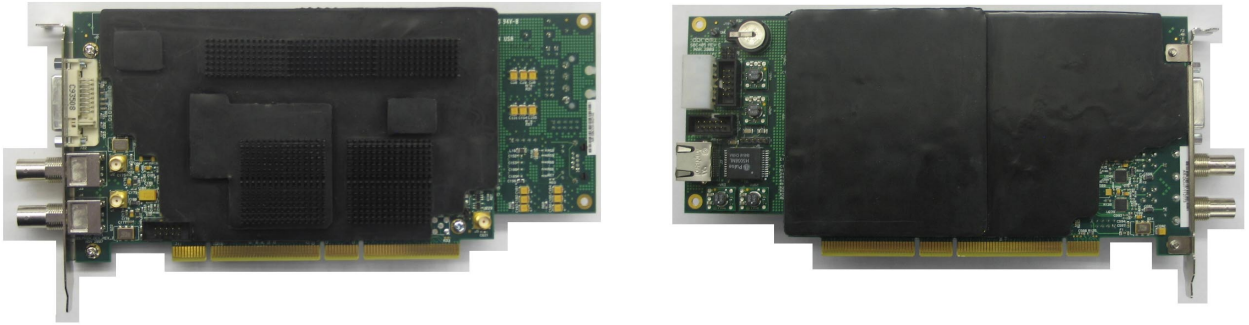
Front View Rear View

Figure 2: Hardware Model DOLPHIN-DCI-1.2-C0



Front View Rear View

Figure 3: Hardware Model DOLPHIN-DCI-1.2-A1



Front View Rear View

Figure 4: Hardware Model DOLPHIN-DCI-1.2-C1

The Dolphin DCI 1.2 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 firmware and hardware 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 DCI 1.2 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
- AES with 128 bit keys for encryption and decryption in CBC mode – see Certificate #1252
- HMAC-SHA1 – see Certificate #271
- HMAC-SHA1 – see Certificate #731
- SHA-1, used by other algorithms (like HMAC-SHA1) – see Certificate #593
- SHA-1 and SHA-256, used by other algorithms (like HMAC-SHA1, FIPS 186-2 RNG or RSA Digital Signature) – see Certificate #1148
- NIST-Recommended RNG based on ANSI X9.31, Appendix A.2.4 with AES 128 bits key – see Certificate #326
- ANSI X9.31 RNG, using TDES-2Keys – see Certificate #696
- FIPS 186-2 RNG – see Certificate #700
- FIPS 186-2 RNG – see Certificate #693
- RSA Key generation and Digital Signature Generation/Verification – see Certificates #600 and #601

3.2 Non-Approved Algorithms

The Dolphin DCI 1.2 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
- First TRNG (RNG Hardware based) – used to seed the approved NIST-Recommended RNG based on ANSI X9.31 presented in paragraph 3.1.
- Second TRNG (RNG Hardware based) – used to seed the approved ANSI X9.31 RNG presented in paragraph 3.1
- MD5 used for TLS key establishment
- HMAC-MD5 used for TLS key establishment

4 Security Levels

The Dolphin DCI 1.2 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 DCI 1.2, Hardware Models DOLPHIN-DCI-1.2-A0, DOLPHIN-DCI-1.2-C0, DOLPHIN-DCI-1.2-A1 and DOLPHIN-DCI-1.2-C1 firmware versions 2.0.4, 22.03-0, 22.03-1 and 99.03, is tested to meet the FIPS security requirements for the levels shown in the following Table 1.

These configurations are identified on the FIPS 140-2 validation certificate as follows:

> (*Hardware Versions: DOLPHIN-DCI-1.2-A0, DOLPHIN-DCI-1.2-A1, DOLPHIN-DCI-1.2-C0 and DOLPHIN-DCI-1.2-C1; Firmware Versions: (2.0.4, 99.03 and 22.03-0) or (2.0.4, 99.03 and 22.03-1)*; Hardware)

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. Cryptographic 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 ports:

Table 2 – FIPS 140-2 Logical Interfaces

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

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 wrapping, signatures and TLS
2. External Private Key – Private RSA Key used for key wrapping
3. Reset Private Key – Private RSA Key used for key wrapping, signatures and TLS
4. Reset Secret Key – AES key used to protect the Reset Private key
5. CSP Secret Key – AES key used to protect the Reset Secret Key, the Doremi HMAC Key, the AES Shared knowledge Key, the AES Wrapping Key and the PCI User Authentication Secrets
6. AES Wrapping Key – AES key used for AES Key Wrapping
7. AES Content Encryption Keys – AES keys that protect content.
8. Link Encryption Keys – AES keys used during the Link Encryption processing.
9. AES Binary Update Key – Used to decrypt binaries being imported into the module
10. Seed Values – Used to seed the FIPS approved RNGs.
11. AES Shared Knowledge Key – AES key used to secure import/export of CSPs.
12. Doremi HMAC Key - HMAC key used for Firmware Load Test.
13. Content Integrity Keys – HMAC keys used to verify the integrity of encrypted content.
14. TLS AES Session Keys – AES keys used for TLS communication
15. TLS HMAC Sessions Keys – HMAC keys used for TLS communication
16. TLS PRF Data – Used for TLS session key establishment
17. TLS Master Secret – Used for TLS session key establishment
18. TLS Pre-Master Secret – Used for TLS session key establishment
19. PCI User Authentication Secrets – PCI User Authentication Secrets used by the module (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:

1. Device Public Key – Public RSA key used for TLS and within Digital Certificate.
2. External Public Key – Public RSA key used within Digital Certificate.
3. Reset Public Key – Public RSA key used for TLS and within Digital Certificate.
4. SMS User Public Key – Public RSA key used for TLS and within Digital Certificate.
5. SAS User Public Key – Public RSA key used for TLS and within Digital Certificate.
6. SOS (Crypto-Officer) User Public Key – Public RSA key used for TLS and within Digital Certificate.
7. Cinema Equipment Public Key(s) – Public RSA key(s) used for TLS and within Digital Certificate.
8. Signers Public Key(s) – Public RSA key(s) used to verify XML files signature and within Digital Certificate.

7 Roles and Services

The cryptographic module supports four distinct operator roles: PCI User, SMS User, SAS User and SOS (Crypto-officer) User. No maintenance role is supported.

The services belonging to each user are presented in the following paragraphs.

7.1 PCI User Services

Table 3 below summarizes specific services available to the PCI Users only.

Table 3: PCI User Services

Services	Description	CSP(s) and Public Key(s) Possibly Involved	Type of access to CSP(s) and Public Key(s)
Basic Configuration	This service allows setting and getting basic configuration parameters.	AES Shared Knowledge Key, AES Content Encryption Keys	Read
		Content Integrity Keys	Read/Write
Advanced Configuration	This service allows setting and getting advanced configuration parameters.	Doremi HMAC Key, AES Binary Update Key, External Private Key, CSP Secret Key, AES Shared Knowledge Key, External Public Key	Read
		AES Content Encryption Keys	Read/Write
Get Status Information	This service allows getting status information.	-	-
GPIO	This service allows loading and getting GPIO data.	-	-
Get Advanced Information	This service allows getting advanced information.	Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, Reset Public Key, External Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		Cinema Equipment Public Key(s)	Write

Services	Description	CSP(s) and Public Key(s) Possibly Involved	Type of access to CSP(s) and Public Key(s)
Basic Operations	This service allows performing basic operations.	Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, AES Wrapping Key, Device Public Key, Reset Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		AES Binary Update Key, AES Content Encryption Keys, Content Integrity Keys, Link Encryption Keys, Seed Values, Signers Public Key(s), Cinema Equipment Public Key(s)	Write
		External Private Key, External Public Key	Read/Write

7.2 SMS User Services

Table 4 below presents all the services available to the SMS User – *Screen Manager*.

Table 4: SMS User Services

Services	Description	CSP(s) and Public Key(s) Possibly Involved	Type of access to CSP(s) and Public Key(s)
Get Advanced Information	This service allows getting advanced information.	Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, Reset Public Key, External Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		Cinema Equipment Public Key(s)	Write
Basic Operations	This service allows performing basic operations.	Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, AES Wrapping Key, Device Public Key, Reset Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		AES Binary Update Key, AES Content Encryption Keys, Link Encryption Keys, Seed Values, Signers Public Key(s), Cinema Equipment Public Key(s)	Write
		External Private Key, External Public Key	Read/Write

Services	Description	CSP(s) and Public Key(s) Possibly Involved	Type of access to CSP(s) and Public Key(s)
Basic Settings	This service allows performing some of the module's settings.	Device Private Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		AES Binary Update Key, Doremi HMAC Key, Signers Public Key(s)	Read/Write
Suite Management	This service provides suite management operations.	Device Private Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, SMS User Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key, Link Encryption Keys, External Private Key	Read
		AES Binary Update Key, AES Content Encryption Keys, Content Integrity Keys, Signers Public Key(s)	Read/Write

7.3 SAS User Services

Table 5 below presents all the services available to the SAS User – *Security Agent*.

Table 5: SAS User Services

Services	Description	CSP(s) and Public Key(s) Possibly Involved	Type of access to CSP(s) and Public Key(s)
All the services listed in **Table 4** for the SMS User are also available for the SAS User.			
Reset Board	This service resets the module.	Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, Reset Public Key, SAS User Public Key, SOS (Crypto-Officer) User Public Key	Read
		Device Private Key, Device Public Key, External Private Key, External Public Key, Link Encryption Keys, Content Integrity Keys, Seed Values, AES Content Encryption Keys, AES Binary Update Key, Signers Public Key(s)	Write

7.4 SOS (Crypto-Officer) User Services

Table 6 below presents all the services available to the SOS (Crypto-Officer) User – *Security Officer*.

Table 6: SOS (Crypto-Officer) User Services

Services	Description	CSP(s) and Public Key(s) Possibly Involved	Type of access to CSP(s) and Public Key(s)
All the services listed in **Table 5** for the SAS User are also available for the SOS (Crypto-Officer) User.			
SOS Configuration	This service allows performing specific SOS (Crypto-Officer) User configuration operations.	Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, AES Wrapping Key, Device Public Key, Reset Public Key, SOS (Crypto-Officer) User Public Key	Read
		Device Private Key, Device Public Key, External Private Key, External Public Key, SMS User Public Key	Read/Write
Zeroization	This service zeroizes sensitive data (including all plaintext CSPs)	Device Private Key, Reset Private Key, Reset Secret Key, CSP Secret Key, TLS AES Session Keys, TLS HMAC Session Keys, TLS PRF Data, TLS Master Secret, TLS Pre-Master Secret, Device Public Key, Reset Public Key, SOS (Crypto-Officer) User Public Key	Read
		All plaintext CSPs, Device Public Key, External Public Key, SMS User Public Key, Signers Public Key(s)	Write

7.5 Un-authenticated Services

The cryptographic module supports the following unauthenticated services:

Table 7: Un-authenticated Services

Services	Description	CSP(s) and Public Key(s) Possibly Involved	Type of access to CSP(s) and Public Key(s)
Get Session Id	Exports the current Session Id of the module	-	-
Show Status	This "service" corresponds to the status information exported automatically through the Serial Port	-	-
Host Reset	Resets the host	-	-
Reset	Resets the module from the host	-	-

The power recycling of the Dolphin DCI 1.2 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 DCI 1.2 to be powered-off and powered-on again.

7.6 Authentication Strength

The cryptographic module enforces the separation of roles using identity-based operator authentication. The PCI User role is authenticated through the use of "PCI User Authentication Secrets" – known by Doremi Cinema LLC only – associated with the current Session Id. Note that data to be compared to authentication secrets are imported encrypted in the module.

SMS, SAS and SOS (Crypto-Officer) User roles are authenticated through the use of 2048 bits RSA Signatures. Note that these authentications rely on the usage of TLS.

Table 8: Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Mechanism
PCI User	Identity-based operator authentication	Authentication Secret Verification
SMS User	Identity-based operator authentication	2048 bits RSA Signature Verification
SAS User	Identity-based operator authentication	2048 bits RSA Signature Verification
SOS (Crypto-Officer) User	Identity-based operator authentication	2048 bits RSA Signature Verification

Table 9: 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 x 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 x 10^{-}(17) that is less than 1/100,000.
2048 bits RSA Signature Verification	It relies on 2048 bits RSA keys known to provide an equivalent of 112 bits of encryption strength. Therefore, a random attempt has an associated probability of fault acceptance of (1/2)^112, which is less than 1/1,000,000. Given the processing capabilities and the clock speed, the number of consecutive attempt that could be launched in a one minute period is extremely limited. An extremely conservative estimate is that the probability of successfully authenticating in a one minute period would be (1/2)^69, which is much less than 1/100,000.

8 Physical Security

The Dolphin DCI 1.2 is classified as a multiple-chip embedded module for FIPS purposes. It is comprised of production grade components.

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.

The cryptographic boundary is the outer perimeter of the board's edge and it includes the hard, opaque and tamper-evident epoxy covering all security relevant components.

Components excluded from the FIPS 140-2 requirements are not security relevant. The excluded components are the non-security relevant data input and data output, filtering components (capacitors, resistors, inductance), voltage oscillators, voltage regulators, fuses, linear time code signal output, magnetic, traces and signals routed to said components, PCB outside potting, and connectors.

9 Operational Environment

The Dolphin DCI 1.2 supports a limited operational environment that only allows the loading of trusted, validated, and HMACed binary images through authenticated service. Doremi Cinema LLC maintains sole possession of the corresponding HMAC key needed to validate the uploaded binary into the Dolphin DCI 1.2.

10 Self-Tests

The module performs the following self-tests:

- Power Up Self-tests
  - Firmware Integrity Test (32 bits CRC and HMAC-SHA1)
  - AES Encryption/Decryption known answer tests
  - HMAC-SHA1 and HMAC-SHA256 known answer test
  - SHA1 known answer test
  - RSA Digital Signature Generation/Validation known answer test
  - RNGs known answer test (NIST-Recommended RNG Based on ANSI X9.31 Annex A.2.4 with AES 128 bits key, ANSI X9.31 RNG and FIPS 186-2 RNGs)
  - Critical Functions Tests:
    - CRC 32-bit known answer test
    - RSA Encryption/Decryption Pair-wise Consistency Test
- Conditional Tests
  - Continuous ANSI X9.31 related RNGs Test (NIST-Recommended RNG Based on ANSI X9.31 Annex A.2.4 with AES 128 bits key and ANSI X9.31 RNG)
  - Continuous FIPS 186-2 RNGs Test
  - Continuous TRNGs Test (Hardware RNGs Test)
  - Firmware Load Test (HMAC-SHA1)
  - Pair-wise consistency test (RSA Keys Generation: Digital Signature Generation/Verification; Encryption/Decryption)

The bypass test and the manual key entry test are N/A.

11 Mitigation of Other Attacks

The Dolphin DCI 1.2 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 four distinct operator roles. These are the PCI User role, the SMS User role, the SAS User role and the SOS (Crypto-Officer) User 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 self-tests and error states.
5. Data output shall be logically disconnected from the internal process performing key generation and zeroization.
6. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
7. The module shall not support a bypass capability or a maintenance interface.
8. The cryptographic module performs the tests as presented in section 10 above.
9. At any time the operator is capable of commanding the module to perform the power-up self-test by a power-cycle.
10. Prior to each use, the ANSI X9.31 DRNGs and the hardware based TRNGs are tested using the conditional test specified in FIPS 140-2 §4.9.2.
11. The module supports concurrent operators.
12. The module only supports a FIPS mode of operation (i.e. non-FIPS mode is not supported). To determine that the module is running in FIPS mode, invoke the "Get Advanced Information" service and check that the firmware versions are the same as those written in this Security Policy document. Also, check that the hardware version written on the module's sticker matches the one specified in this Security Policy document.

13 Acronyms

Term	Definition
AES	Advanced Encryption Standard
AES-EBU	Audio Engineering Society - European Broadcasting Union
ANSI	American National Standards Institute
CSP	Critical Security Parameter
DCI	Digital Cinema Initiatives
DRNG	Deterministic Random Number Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
FPGA	Field-Programmable Gate Array
GPI	General Purpose Input
GPIO	General Purpose Input/Output
GPO	General Purpose Output
HD	High Definition
HMAC	Keyed Hash Message Authentication Code
KAT	Known Answer Test
LTC	Linear Time-Code
N/A	Not Applicable
NIST	National Institute of Standards and Technology
OSD	On Screen Display
PCI	Peripheral Component Interconnect
PRF	Pseudo Random Function
RNG	Random Number Generator
RSA	Rivest, Shamir and Adelman
RTC	Real Time Clock
SAS	Security Agent System
SDI	Serial Digital Interface
SHA	Secure Hash Algorithm
SMS	Screen Management System

Term	Definition
SOS	Security Officer System
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TRNG	True Random Number Generator

14 Document Revision History

Date	Version	Description
07/30/2010	1.0	First version