

REVISIONS				
REV	DESCRIPTION	ECO	DATE	APPROVED
F	Initial Release	2108109	06/02/10	Lee Armstrong
G	Update for hardware revision change	2109405	07/27/10	Lee Armstrong
H	Update for hardware revision change. Added details on tamper potting identification.	2119966	11/16/11	G. STRUNK
I	Update for software release 1.7(23).	2128242	10/16/12	G. STRUNK

*Copyright © 2010-2012 by Texas Instruments.
May only be reproduced in its entirety without modification.*

Security Policy, DLP Cinema[®], Series 2 Enigma Link Decryptor

The data in this specification is preliminary and subject to correction or change as required.

TEXAS INSTRUMENTS INCORPORATED (c) COPYRIGHT 2010-2012 TEXAS INSTRUMENTS ALL RIGHTS RESERVED				
		DWN/CHK	DATE	TITLE Security Policy, DLP Cinema [®] , Series 2 Enigma Link Decryptor
		ENGR	DATE	
	<i>314PH</i>	MANU	DATE	
<i>NHA</i>	<i>Used On</i>	QA	DATE	SIZE A DRAWING NO 2510293 REV I
APPLICATION		APVD	DATE	SCALE NONE SHEET 1 OF 23

Table Of Contents

1 REFERENCE DOCUMENTS.....4

2 INTRODUCTION4

2.1 CRYPTOGRAPHIC BOUNDARY.....4

2.2 APPROVED ALGORITHMS.....6

2.3 NON-APPROVED ALGORITHMS.....7

2.4 PHYSICAL PORTS AND LOGICAL INTERFACES.....7

3 SECURITY RULES8

4 IDENTIFICATION AND AUTHENTICATION POLICY11

5 ACCESS CONTROL POLICY12

6 ROLES, SERVICES, CSPTS13

7 UNAUTHENTICATED SERVICES18

8 PHYSICAL SECURITY POLICY.....19

9 MITIGATION OF OTHER ATTACKS POLICY22

10 APPENDIX.....23

10.1 GLOSSARY/ACRONYMS23

Index of Figures

FIGURE 1. ENIGMA CRYPTOGRAPHIC BOUNDARY (TOP VIEW).....5

FIGURE 2. ENIGMA CRYPTOGRAPHIC BOUNDARY (BOTTOM VIEW)6

FIGURE 3. LOCATION OF TOP-SIDE POTTED FASTENERS AND MATERIAL INDICATOR LABEL20

FIGURE 4. LOCATION OF BOTTOM-SIDE POTTED FASTENERS20

Index of Tables

κTABLE 1. REFERENCE DOCUMENTS 4

TABLE 2. MAP OF PHYSICAL PORTS TO LOGICAL INTERFACES 7

TABLE 3. ROLES AND REQUIRED IDENTIFICATION AND AUTHENTICATION 11

TABLE 4. STRENGTHS OF AUTHENTICATION MECHANISMS 11

TABLE 5. MARRIAGE INITIATION SERVICE 13

TABLE 6. MARRIAGE VERIFICATION SERVICE 13

TABLE 7. UPDATE TI LOGIN LIST SERVICE 14

TABLE 8. UPDATE SECURITY OFFICER LOGIN LIST SERVICE 14

TABLE 9. TLS SESSIONS FOR CRYPTOGRAPHIC OFFICER SERVICE 15

TABLE 10. ZEROIZE VIA TWO-LAYER COMMAND SERVICE 15

TABLE 11. TLS SESSIONS FOR CINEMA SERVER SERVICE 16

TABLE 12. SHOW MOVIE SERVICE 16

TABLE 13. LOG RETRIEVAL SERVICE 17

TABLE 14. LOAD NEW CODE SERVICE 17

TABLE 15. INSPECTION/TESTING OF PHYSICAL SECURITY MECHANISMS 19

TABLE 16. TAMPER EVIDENT FASTENER IDENTIFICATION (POTTING MATERIAL COVERING SCREWS.) 21

TABLE 17. MITIGATION OF OTHER ATTACKS 22

1 Reference Documents

Document Number	Description
FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS 197	Advance Encryption Standard (AES)
FIPS 198-1	The Keyed-Hash Message Authentication Code (HMAC)
ANSI X9.31-1998	Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry (rDSA)
	Digital Cinema System Specification (Digital Cinema Initiatives, LLC) 1.2
IETF RFC 2246	The TLS Protocol, Version 1.0
FIPS 180-2	Secure Hash Standard

Table 1. Reference Documents

2 Introduction

The Texas Instruments Enigma Cryptographic Module [Hardware version 2509488 Rev G or Rev H or Rev I; Software version 1.4(19) or 1.5(21) or 1.6(22) or 1.7(23); Firmware version 2.12(12)], hereafter referred to as “Enigma” or “cryptographic module”, is a multi-chip embedded cryptographic module designed to protect digital movie content in accordance with Digital Cinema Initiatives V1.2. The Enigma is a Link Decryptor module designed to reside within a host cinema projector.

2.1 Cryptographic Boundary

The cryptographic boundary is defined as the outer perimeter of the metal enclosure that encompasses all hardware, software, and firmware that support cryptography and security functions with three multi-pin connector ports exposed as interfaces.

The following images define the cryptographic boundary:

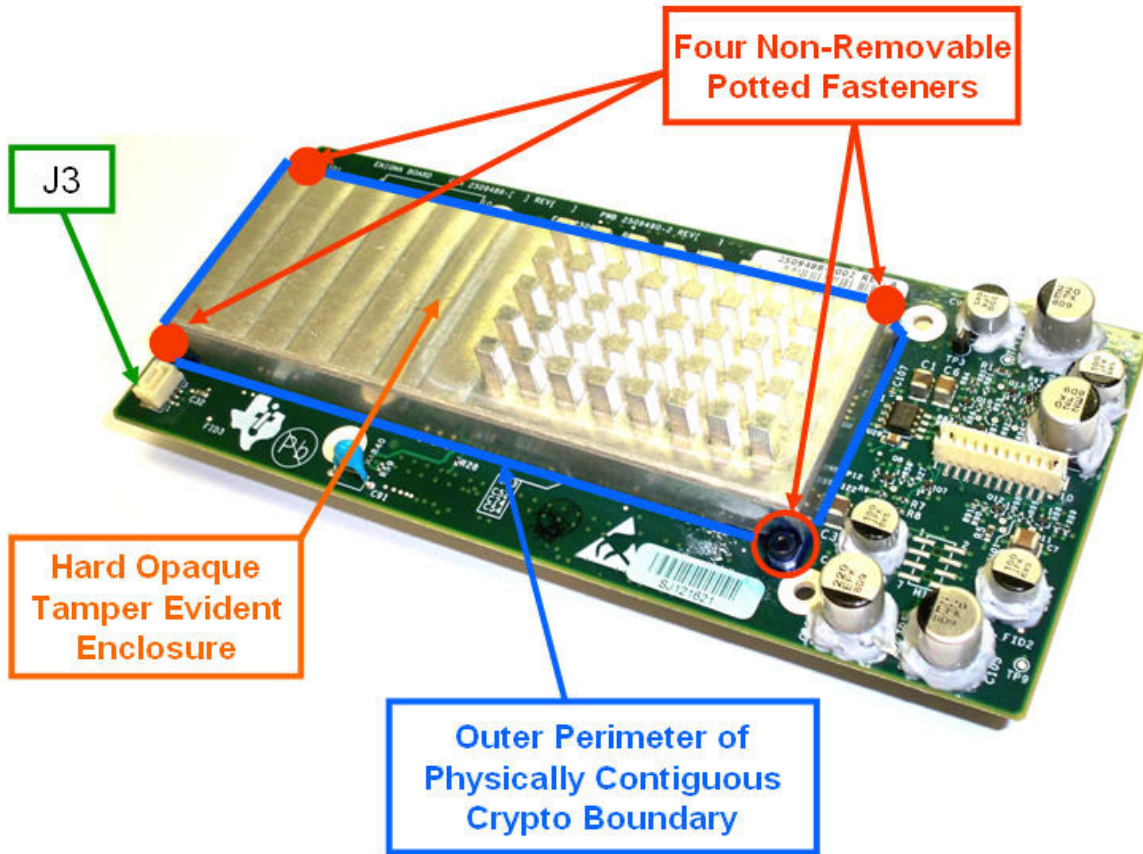


Figure 1. Enigma Cryptographic Boundary (top view)

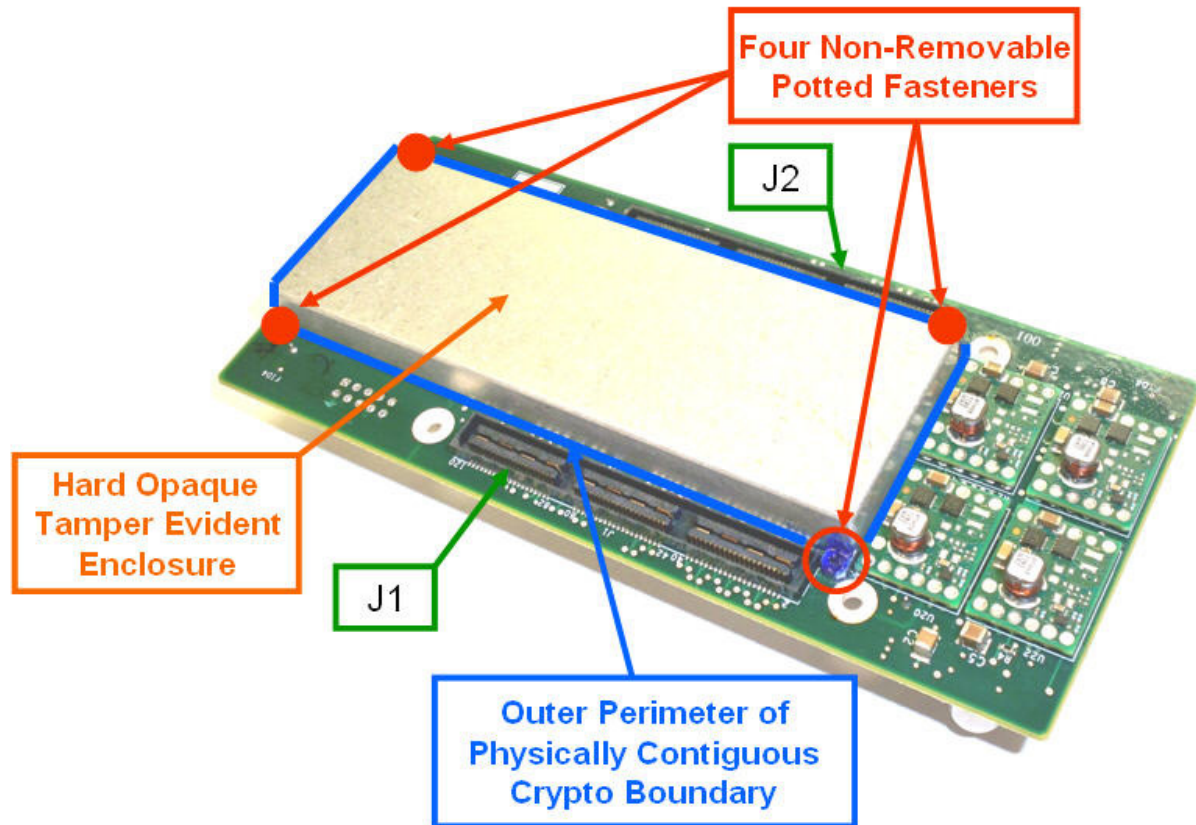


Figure 2. Enigma Cryptographic Boundary (bottom view)

2.2 Approved Algorithms

The cryptographic module supports the following Approved algorithms:

- AES CBC Encrypt/Decrypt (Cert# 1014)
- AES ECB Encrypt – Core 1 (Cert# 999)
- AES ECB Encrypt – Core 2 (Cert# 1000)
- AES ECB Encrypt – Core 3 (Cert# 1001)
- AES ECB Encrypt – Core 4 (Cert# 1002)
- SHA-1 (Cert# 971)
- ANSI X9.31 DRNG with AES 128 core (Cert# 581)
- HMAC-SHA-1 (Cert# 568)
- RSA (Cert# 487)

Security Policy, DLP Cinema®, Series 2 Enigma Link Decryptor**May only be reproduced in its entirety without modification****2.3 Non-Approved Algorithms**

The cryptographic module supports the following non-Approved algorithms:

- ECDH – considered as non-security relevant and only used to interoperate with legacy equipment
- TI S-box - considered as non-security relevant data obfuscation (plaintext); only used for status and control.
- NDRNG – only used to seed the Approved DRNG.
- MD5 (within TLS PRF)
- RSA key wrap (within TLS): (key wrapping; key establishment methodology provides 112 bits of encryption strength)

2.4 Physical Ports and Logical Interfaces

The cryptographic module supports the following physical ports:

- J1: 120-Pin 0.8mm QSE Series Hi-Speed Socket
- J2: 120-Pin 0.8mm QSE Series Hi-Speed Socket
- J3: 3-pin, polarized, 2.5mm pitch, header
- 12VDC, FPGA, FIPS, ST, SDMT, VS, DCRPT: a series of traces that extend to seven external light emitting diodes (LEDs)
- DC power supply circuit/filter: a series of traces that extend to peripheral power related components that are outside of the cryptographic boundary

The following table maps of each physical port to the logical interfaces:

Physical Port	Logical Interface
J1, J2	Data Input
J1, J2	Control Input
J1, J2	Data Output
J1, J2, 12VDC, FPGA, FIPS, ST, SDMT, VS, DCRPT	Status Output
J1, J2, J3, DC power supply circuit/filter	Power

Table 2. Map of Physical Ports to Logical Interfaces

3 Security Rules

The following specifies security rules under which the cryptographic module shall operate in accordance with FIPS 140-2:

- The cryptographic module does not support a non-FIPS mode of operation and only operates in an Approved mode of operation. The method used to indicate the Approved mode of operation is the combination of LEDs displayed in the following pattern with main power applied:
 - 12VDC LED is illuminated green
 - FPGA LED is illuminated green
 - FIPS LED is not illuminated
 - ST LED is illuminated green
 - SDMT LED is illuminated green
 - VS LED is not illuminated
 - DCRPT LED is not illuminated
- The cryptographic module provides logical separation between all of the data input, control input, data output, status output interfaces. The module receives external power inputs through the defined power interface.
- The cryptographic module supports identity based authentication for all services that utilize CSPs and Approved security functions.
- The data output interface is inhibited during self tests, zeroization, and when error states exist.
- When the cryptographic module is in an error state it ceases to provide cryptographic services, inhibits all data outputs, and provides status of the error.
- The cryptographic module maintains internal separation of concurrent operators.
- When the cryptographic module is powered off and subsequently powered on, the results of previous authentications are not be retained and the cryptographic module requires the operator to be re-authenticated in an identity based fashion.
- The cryptographic module protects CSPs from unauthorized disclosure, unauthorized modification, and unauthorized substitution.
- The cryptographic module protects public keys from unauthorized modification, and unauthorized substitution.
- The cryptographic module satisfies the FCC EMI/EMC requirements specified by 47 Code of Federal Regulations, Part 15, Subpart B, Unintentional Radiators, Digital Devices, Class B (i.e., for home use).
- The cryptographic module implements the following self-tests:
 - Power-up self-tests
 - AES CBC Encrypt/Decrypt KAT
 - AES ECB Encrypt KAT on each of the 4 FPGA cores
 - SHA-1 KAT
 - HMAC-SHA-1 KAT
 - RSA-SHA-1 KAT (signature generation/verification)
 - DRNG KAT
 - Firmware integrity test (32-bit checksum verification)

Security Policy, DLP Cinema®, Series 2 Enigma Link Decryptor**May only be reproduced in its entirety without modification**Critical functions tests

- MD5 KAT
- TLS PRF KAT
- RSA decryption KAT

Conditional self-test

- Continuous DRNG test
 - Continuous NDRNG test
 - Firmware load test (RSA 2048 bit signature verification).
-
- Manual key entry is not supported and the cryptographic module does not implement manual key entry tests.
 - The cryptographic module does not support bypass capability and does not implement bypass tests.
 - The module does not support RSA key generation, and does not implement conditional pair-wise consistency tests.
 - Key generation and split-knowledge processes are not supported.
 - All maintenance related services (i.e. maintenance role, physical maintenance interface, logical maintenance interface) are not applicable.
 - There are no components within the cryptographic boundary that are excluded from the requirements of FIPS 140-2.
 - Plaintext CSP input/output is not supported.
 - The cryptographic module does not contain dedicated physical ports for CSP input/output
 - The continuous comparison self-tests related to twin implementations are not applicable.
 - Upon authenticating into a particular role, it is not possible to switch into another role without re-authenticating.
 - The cryptographic module does not provide the means to feedback authentication data.
 - The finite state machine does not support the following states: maintenance, key generation, CSP output.
 - The requirements of FIPS 140-2 Section 4.6 are not applicable; there exists no support for the execution of untrusted code. All coded loaded from outside the cryptographic boundary is cryptographically authenticated via RSA 2048 bit digital signatures.
 - The cryptographic module is not a radio, does not support any wireless interfaces or OTAR.
 - The EFP and EFT requirements are not applicable.
 - The requirements of FIPS 140-2 Section 4.11 are not applicable; the cryptographic module was not designed to mitigate specific attacks beyond the scope of FIPS 140-2.

Following are the additional security rules imposed by the Texas Instruments.

- The cryptographic module shall conform to the DCI version 1.2.
- The cryptographic module shall support electrical and logical marriage to its host cinema projector. The cryptographic module continuously monitors its electrical connection to the host cinema projector via J1 and J2 connector. The cryptographic module maintains its logical marriage via verification of RSA 2048 bit digital signatures. In the event that the marriage is broken (for example through removal of the cryptographic module from the host cinema

DRAWING NO	REV	
2510293	I	SHEET 9

Security Policy, DLP Cinema®, Series 2 Enigma Link Decryptor

May only be reproduced in its entirety without modification

projector or failed User role authentication attempts during Marriage Verification service) the Show Movies AES keys are zeroized. Additionally, the cryptographic module rejects all attempts to enter Show Movie AES Keys until such a time as the Cryptographic Officer performs another Marriage Initiation service.

- The cryptographic module shall continuously monitor the service doors of the projector via the J1 and J2 connectors and respond to the opening of multiple external doors within the host cinema projector. The external doors are not included within the cryptographic module boundary and opening of said doors does not constitute a breach of the cryptographic boundary. When the external doors are opened, the Show Movie AES Keys are zeroized. Additionally, the cryptographic module rejects all attempts to enter Show Movie AES Keys until such a time as the external doors are closed and the cryptographic module receives the Service Door Tamper Termination command.

DRAWING NO	REV	
2510293	I	SHEET 10

4 Identification and Authentication Policy

The following constitutes the cryptographic modules identification and authentication policy including an itemization of the roles, type of authentication, and corresponding authentication data. Additionally the strength of each authentication mechanism is specified for random attempts and multiple consecutive attempts within a one-minute period.

Role	Type of Authentication	Authentication Data
Cryptographic Officer (Security Officer)	Identity-Based	Username & Password
User (ICP)	Identity-Based	RSA signature verification
TI Login List Updater	Identity-Based	RSA signature verification
Security Officer Login List Updater	Identity-Based	RSA signature verification
TI Code Signer	Identity-Based	RSA signature verification

Table 3. Roles and Required Identification and Authentication

Authentication Mechanism	Strength of Mechanism
Username & Password	Random attempt: 1 in 92^{10} Multiple attempts during one minute period: 3 in 92^{10} . The Enigma will refuse login attempts for one minute after 3 unsuccessful login attempts.
RSA signature verification	Random attempt: 1 in 2^{112} Multiple attempts during one minute period: 6000 in 2^{112}

Table 4. Strengths of Authentication Mechanisms

5 Access Control Policy

Following is a listing of the authorized roles with a description of responsibilities.

- Cryptographic Officer (Security Officer) role: this role is responsible for the initialization and administration of the cryptographic module. This role is also responsible for inspection of the implemented physical security mechanisms during marriage initiation.
- User role (ICP): this role is responsible for playing movies and periodically checking status.
- TI Login List Updater role: this role is responsible for updating the TI Login List.
- Security Officer Login List Updater role: this role is responsible for updating the Security Officer Login List.
- TI Code Signer role: this role is responsible for updating the executable code that is encrypted with AES and cryptographically authenticated via 2048 bit RSA digital signatures.

Security Policy, DLP Cinema®, Series 2 Enigma Link Decryptor**May only be reproduced in its entirety without modification****6 Roles, Services, CSPs**

Following is listing of roles, services, cryptographic keys & CSPs, and types of access to the cryptographic keys & CSPs that are available to each of the authorized roles via the corresponding services.

Role	Service	Cryptographic Keys & CSPs	Type(s) of Access
Cryptographic Officer (Security Officer)	Marriage Initiation: binding the identity of the cryptographic module (Link Decryptor) to the external Integrated Cinema Processor both electronically and logically via RSA signatures.	Enigma Public Key (RSA 2048)	Output
		Enigma Private Key (RSA 2048)	Use for signature generation
		Security Officer TLS Public Key (RSA 2048)	Input, Use for TLS session establishment
		Security Officer Login List (Usernames and Passwords)	Input, Use for authentication via TLS
		<ul style="list-style-type: none"> TLS HMAC Key (160-bit) TLS AES Key (128-bit) TLS PRF State (takes the TLS Pre-master Secret, 64-byte random number, 13-byte label – converts to TLS Master Secret) TLS Pre-master Secret (48-byte) TLS Master Secret (48-byte) 	Established via commercially available key establishment protocol TLS 1.0 (protocol version = 3.1); Used with Cipher-Suite “RSA_WITH_AES_128_CBC_SHA” = {0x00, 0x2F} (RFC 3268).
		DRNG State (16-byte)	Use for random number generation for use in TLS
Integrated Cinema Processor Public Key (RSA 2048)	Input; Use for signature verification of future marriage verification services		

Table 5. Marriage Initiation Service

Role	Service	Cryptographic Keys & CSPs	Type(s) of Access
User	Marriage Verification: verify a digital signature from the User to confirm that the logical marriage is still intact.	Integrated Cinema Processor Public Key (RSA 2048)	Input, Use for signature verification to authenticate the User role

Table 6. Marriage Verification Service

Security Policy, DLP Cinema®, Series 2 Enigma Link Decryptor

May only be reproduced in its entirety without modification

Roles	Service	Cryptographic Keys & CSPs	Type(s) of Access
TI Login List Updater	Update TI Login List: Verify RSA signature, decrypt the login list received, update the list.	TI Login List Update AES Key (128-bit)	Use for decryption of TI Login List
		TI Login List Update Public Key (RSA 2048)	Use for signature verification
		TI Login List (Usernames and Passwords)	Input and update
		CSP AES Key	Use for storage

Table 7. Update TI Login List Service

Roles	Service	Cryptographic Keys & CSPs	Type(s) of Access
Security Officer Login List Updater	Update Security Officer Login List: Verify RSA signature, decrypt the login list received, update the list.	Security Officer Login List Update AES Key (128-bit)	Use for decryption of Security Officer login list
		Security Officer Login List Update Public Key (RSA 2048)	Use for signature verification
		Security Officer Login List (Usernames and Passwords)	Input and update
		CSP AES Key	Use for storage

Table 8. Update Security Officer Login List Service

Security Policy, DLP Cinema®, Series 2 Enigma Link Decryptor

May only be reproduced in its entirety without modification

Roles	Service	Cryptographic Keys & CSPs	Type(s) of Access
Cryptographic Officer (Security Officer)	TLS Sessions for Cryptographic Officer: Establish a TLS session with RSA client certificates, Login (open) by authenticating to the cryptographic module via username, and password. Logout (close) by terminating the session upon completion.	Security Officer TLS Public Key (RSA 2048)	Input, Use for signature verification
		Security Officer Login List (Usernames and Passwords)	Input, Use for login via TLS
		<ul style="list-style-type: none"> • TLS HMAC Key (160-bit) • TLS AES Key (128-bit) • TLS PRF State (takes the TLS Pre-master Secret, 64-byte random number, 13-byte label – converts to TLS Master Secret) • TLS Pre-master Secret (48-byte) • TLS Master Secret (48-byte) 	Established via commercially available key establishment protocol TLS 1.0 (protocol version = 3.1); Used with Cipher-Suite “RSA_WITH_AES_128_CBC_SHA” = {0x00, 0x2F} (RFC 3268).
		DRNG State (16-byte)	Use for random number generation for use in TLS
		Enigma Public Key (RSA 2048).	Output
		Enigma Private Key (RSA 2048)	Use for TLS establishment.
	Self-Test Via Command Over TLS: Allow the Cryptographic Officer to execute self-tests	N/A	N/A

Table 9. TLS Sessions for Cryptographic Officer Service

Role	Service	Cryptographic Keys & CSPs	Type(s) of Access
Cryptographic Officer (Security Officer)	Zeroize via Two-Layer Command	All plaintext CSPs.	Zeroization (i.e. active overwrite of all memory locations where the CSPs reside)

Table 10. Zeroize via Two-Layer Command Service

Security Policy, DLP Cinema®, Series 2 Enigma Link Decryptor

May only be reproduced in its entirety without modification

Role	Service	Cryptographic Keys & CSPs	Type(s) of Access
User	TLS Sessions for Cinema Server (port #0x0495): cryptographically process I/O via the TLS protocol and process SMPTE ASM commands via the TLS protocol: - GetTime - QuerySPB - LEKeyLoad - LEKeyQueryID - LEKeyQueryAll - LEKeyPurgeID - LEKeyPurgeAll - PurgeLEKeyID - PurgeAllLEKey - GetEventID - GetEventList - BadRequest	<ul style="list-style-type: none"> • TLS HMAC Key (160-bit) • TLS AES Key (128-bit) • TLS PRF State (takes the TLS Pre-master Secret, 64-byte random number, 13 byte label – converts to TLS Master Secret) • TLS Pre-master Secret (48-byte) • TLS Master Secret (48-byte) 	Established via commercially available key establishment protocol TLS 1.0 (protocol version = 3.1); Used with Cipher-Suite “RSA_WITH_AES_128_CBC_SHA” = {0x00, 0x2F} (RFC 3268).
		DRNG State (16-byte)	Use for random number generation for use in TLS
		Show Movie AES key (128-bit)	Input, use for AES ECB, Zeroize.
		Cinema Server Public Key (RSA 2048)	Input, Use for signature verification
		Enigma Public Key (RSA 2048)	Output
		Enigma Private Key (RSA 2048)	Use for TLS establishment.

Table 11. TLS Sessions for Cinema Server Service

Role	Service	Cryptographic Keys & CSPs	Type(s) of Access
User	Show Movie: Cryptographically process data with AES ECB using the Show Movie AES key.	Show Movie AES Key (128-bit)	Use for AES ECB.

Table 12. Show Movie Service

Security Policy, DLP Cinema®, Series 2 Enigma Link Decryptor

May only be reproduced in its entirety without modification

Role	Service	Cryptographic Keys & CSPs	Type(s) of Access
User	Log Retrieval: obtain forensic log of public identifiers per DCI Spec v1.2.	<ul style="list-style-type: none"> • TLS HMAC Key (160-bit) • TLS AES Key (128-bit) • TLS PRF State (takes the TLS Pre-master Secret, 64-byte random number, 13-byte label – converts to TLS Master Secret) • TLS Pre-master Secret (48-byte) • TLS Master Secret (48-byte) 	Use existing session parameters.
		DRNG State (16-byte)	Use for random number generation for use in TLS

Table 13. Log Retrieval Service

Role	Service	Cryptographic Keys & CSPs	Type(s) of Access
TI Code Signer	Load New Code: update the executable code via RSA signature verification.	TI Code Update Public Key (RSA 2048)	Input, Use for signature verification of code
		TI Code Update AES Key (128-bit)	Input; Use for decryption of code
		TI Login List Update AES Key (128-bit)	Input and store
		TI Login List Update Public Key (RSA 2048)	Input and store
		Security Officer Login List Update AES Key (128-bit)	Input and store
		Security Officer Login List Update Public Key (RSA 2048)	Input and store
		CSP AES Key	Use for storage

Table 14. Load New Code Service

7 Unauthenticated Services

The cryptographic module supports unauthenticated services that do not use Approved security functions, disclose, modify, substitute CSPs or otherwise affect the security of the module as follows:

- Show Status: obtain non-security relevant status items.
- Self-tests: perform the full suite of power-on self tests by power cycling the cryptographic module.

Note that the following unauthenticated services are accessible by connecting to the cryptographic module through ECDH and TI S-box, the use of which is considered non-security relevant data obfuscation from FIPS 140-2 perspective as related to this cryptographic module; this does not provide any security relevant functions and is not used to protect sensitive unclassified data. The I/O therein is obfuscated to support interoperability with existing legacy equipment and is only used to set and retrieve non-security relevant items. **Note that all such services are considered to be plaintext with respect to FIPS 140-2, and do not use the Approved security functions, disclose, modify, or substitute CSPs or otherwise affect the security of the module as follows:**

- RGB Status output: the cryptographic module outputs status of red-green-blue signal.
- Black Status output: the cryptographic module outputs a constant signal of black status.
- Read Status: output non-security relevant status information.
- Run self-tests via command: perform the full suite of power-on self tests on demand.
- Ethernet Port Configuration: used to define the MAC address associated with the Ethernet port
- Version: used to read the software, firmware, and login list version information.
- Set RTC Time: used to read and write the date and time information.
- Serial Number: used to read the serial number of the module.
- System Reset: used to reset the module.
- Input Data Packing Format: used to configure the module's video input.
- Power Mode Select: used to place the module into a low-power mode (or exit a low-power mode).
- Security Log: used to retrieve plaintext security log information.
- Service Door Tamper Terminate: used to resume monitoring of the service door tamper inputs.

Security Policy, DLP Cinema®, Series 2 Enigma Link Decryptor**May only be reproduced in its entirety without modification****8 Physical Security Policy**

The following table describes:

- Physical security mechanisms that are implemented in the cryptographic module
- Actions required by the operators to ensure that physical security is maintained

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Hard, opaque, tamper evident, production grade, non-removable metal enclosure	Each time the Marriage Initiation service is performed	Inspect all sides of the cryptographic boundary under a bright light for scratches, gouges, scrapes, and other signs of malice.
Tamper evident fasteners (opaque potting material covering screws)	Each time the Marriage Initiation service is performed	Inspect each of the fasteners at the four corners of the cryptographic boundary, top and bottom, under a bright light for scratches, gouges, scrapes, and other signs of malice. See Figure 3, Figure 4, and Table 16 for details on identifying the tamper evident potting material.
Tamper detection and response zeroization circuitry	N/A	Obtain status from the cryptographic module during each use. If a tamper event has occurred send the cryptographic module to the manufacturer.
Marriage connection	Each time the Marriage Initiation service is performed	Inspect the physical connection between the cryptographic module and the external host cinema projector. Ensure that no intervening systems are present at the physical connection (e.g. protruding wires, unauthorized components).
External Service door connection	Prior to each closure of the external service door.	Inspect the physical connection between the cryptographic module and the external host cinema projector. Ensure that no intervening systems are present at the physical connection (e.g. protruding wires, unauthorized components).

Table 15. Inspection/Testing of Physical Security Mechanisms

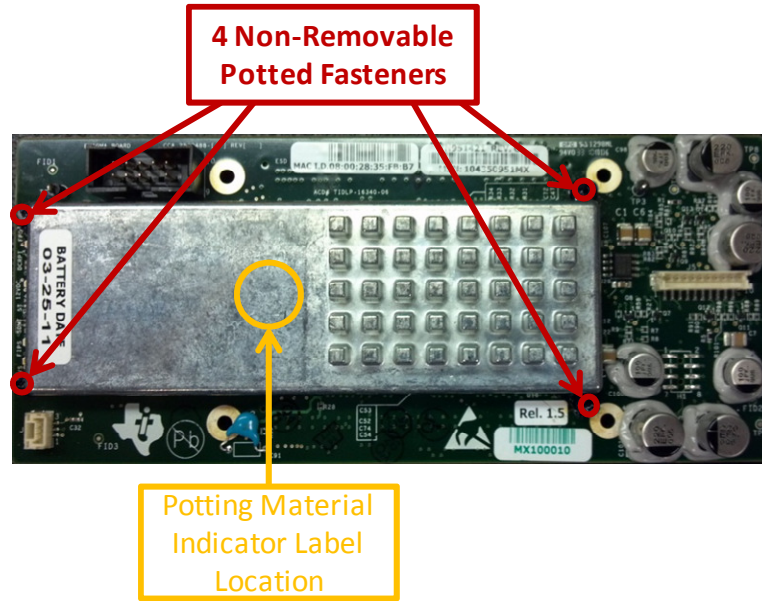


Figure 3. Location of Top-side Potted Fasteners and Material Indicator Label

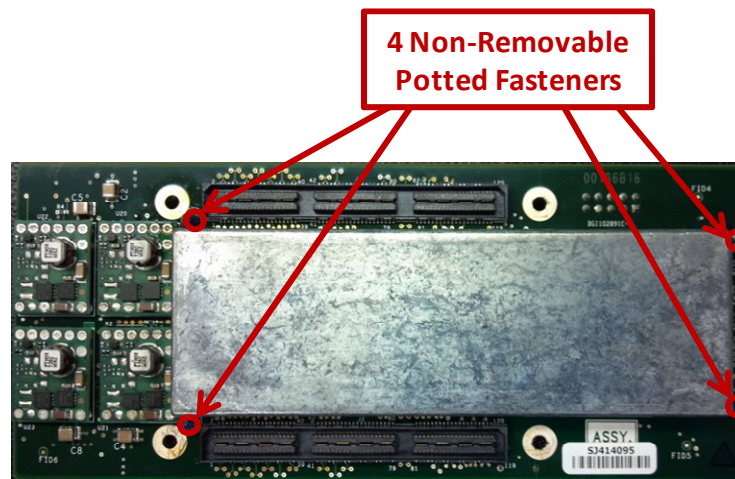


Figure 4. Location of Bottom-side Potted Fasteners



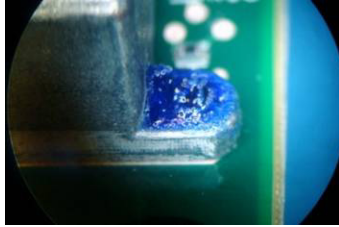

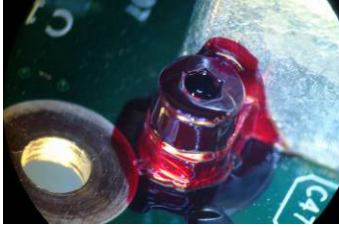
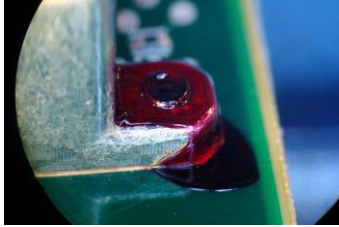

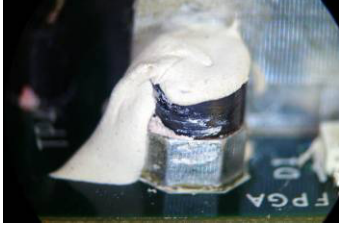

Indicator Label	Material Color	Example Top Side Screw Potting	Example Bottom Side Screw Potting
 No Label	Blue		
 Red Label	Red		
 White Label	White		

Table 16. Tamper Evident Fastener Identification (Potting Material Covering Screws.)

9 Mitigation of Other Attacks Policy

The cryptographic module was not designed to mitigate any specific attacks beyond the scope of FIPS 140-2.

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

Table 17. Mitigation of Other Attacks

10 Appendix

10.1 Glossary/Acronyms

AES	Advanced Encryption Standard
ASM	Auditorium Security Messages
CO	Cryptographic Officer
CSP	Critical Security Parameter
DCI	Digital Cinema Initiatives, LLC
DRNG	Deterministic Random Number Generator
ECDH	Elliptic Curve Diffie-Hellman
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
ICP	Integrated Cinema Processor
I/O	Input/Output
KAT	Known Answer Test
MAC	Media Access Control
NDRNG	Non-deterministic Random Number Generator
RGB	Red-green-blue
RSA	Rivest-Shamir-Adleman (public key cryptography algorithm)
RTC	Real time clock
SHA	Secure Hash Algorithm
SMPTE	The Society of Motion Picture and Television Engineers
TLS	Transport Layer Security