JOVEAI

44081 Old Warm Springs Boulevard, Fremont, CA, 94538
Info@joveai.com
510 573-4939

JoveAI Innovation, Inc.
STAR-2000-3 FIPS 140-2 SECURITY POLICY
Non-Proprietary

Document Revision: 1.5

H.W. P/N and Version: JV00002-03-1B-2
F.W. Version: 1.0.0.1

Date: December 6, 2022

REVISION HISTORY

Author(s)	*Version*	*Updates*
Eddie Rossi Yu Fei Leung	1.0	Initial Release
	1.1	Change HW P/N and Version and FW Version. Updated Exhibit 8 to include new services. Updated listing of Unauthenticated Services to: ▪ Remove *non-compliant* algorithms from the listing of Self Tests. ▪ Add "SMS listener for SPL Timed Notifications" under listing of Status Output services. ▪ *Tentatively* added "PIB Passthrough TCP Services".
	1.2	Updates to match STAR-2000 Security Policy changes made in response to TID-1114 NIST Round#1 Comments.
	1.3	▪ Clean-up Exhibit 10 description of AES-GCM. ▪ Add GetScaling / SetScaling to list of Unauthenticated Services for the Projector Intelligence Block.
	1.4	Clarified access rights in Exhibit 7, with one row per Public Key.
	1.5	Clarified Exhibit 9 to indicate that the module only uses algorithms listed in this table. In the list of self-tests, removed those algorithms which are only available in non-FIPS mode.

Table of Contents

INTRODUCTION 4
ACRONYMS 5
CRYPTOGRAPHIC BOUNDARY 6
BLOCK DIAGRAM 10
FIPS 140-2 MODES OF OPERATION 11
PHYSICAL PORTS AND LOGICAL INTERFACES 12
SECURITY LEVEL SPECIFICATION 13
SECURITY RULES 14
CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS 15
IDENTIFICATION AND AUTHENTICATION POLICY 16
ACCESS CONTROL POLICY 17
ALGORITHMS 24
UNAUTHENTICATED SERVICES 26
PHYSICAL SECURITY POLICY 28
MITIGATION OF OTHER ATTACKS POLICY 29
REFERENCES 29

INTRODUCTION

The JoveAI Innovation, Inc. STAR-2000-3 Cryptographic Module (H.W. P/N and Version: **JV00002-03-1B-2**, with F.W. Version: **1.0.0.1**) is a multi-chip embedded cryptographic module compliant with FIPS 140-2 and the Digital Cinema System Specification (DCSS) version 1.4. Any firmware loaded into the module with a version not shown in the module certificate is out of scope of this validation and requires a separate FIPS 140-2 validation.

The STAR-2000-3 provides protection of Digital Cinema Content (confidentiality of Digital Cinema Content Keys) and facilitates presentations of Digital Cinema Content. The STAR-2000-3 is the IMB (Image Media Block).

Note that the STAR-2000-3 IMB must be installed into a C3 Digital Cinema Projector in order to provide its full suite of services.

ACRONYMS

Below is a list of acronyms related to the cryptographic module that will be referenced in this document:

TERM	DESCRIPTION
BBRAM	Battery-Backed-RAM.
CPL	Composition Playlist.
DCI	Digital Cinema.
DCP	Digital Cinema Package.
DCSS	Digital Cinema System Specification.
DLP	Digital Light Processing
DMD	Digital Micromirror Device
ESV	Encrypted Seed Value
FEK	Firmware Encryption Key
FPC	Flexible Printed Circuit.
IMB	Image Media Block, the heart of the DCI Projector. This is the Cryptographic Module.
KDM	Key Delivery Message. Refer to SMPTE's [ST 430-1].
MPSoC	The Multi-Processor System-on-Chip, the Secure Silicon.
OCM	On-Chip Memory, an SRAM of the MPSoC.
PIB	Projector Intelligence Block.
PPK	Primary Public Key
SEK	Seed Encryption Key
SM	Security Manager.
SMS	Screen Management System (implemented on the PIB Board) used to interface with the IMB via a web browser-based GUI.
SPB	Secure Processing Block. Refer to DCI's [DCSS v1.4], section 9.4.2.2.
SPB1	Secure Processing Block Type 1, synonymous with the FIPS Physical Protection Boundary of the Cryptographic Module.
SPB2	Secure Processing Block Type 2, which defines the outer protection perimeter surrounding the entire DCI Projector.
SPK	Secondary Public Key
SPL	Show Playlist.
SV	Seed Value
TEL	Tamper Evident Label

Exhibit 1 – *Specification of Acronyms and their Descriptions*

CRYPTOGRAPHIC BOUNDARY

The following illustrations indicate the cryptographic boundary and the physical ports defined on the boundary.

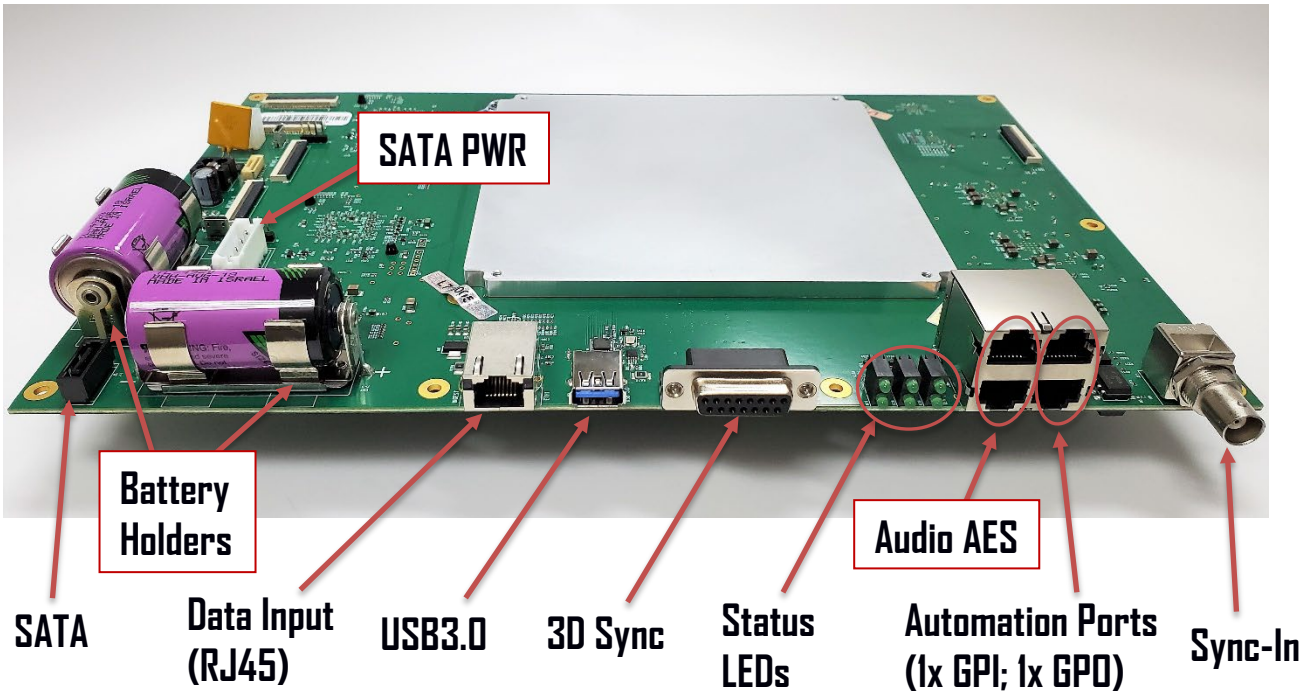

Figure 1: Front View of STAR-2000-3 Module

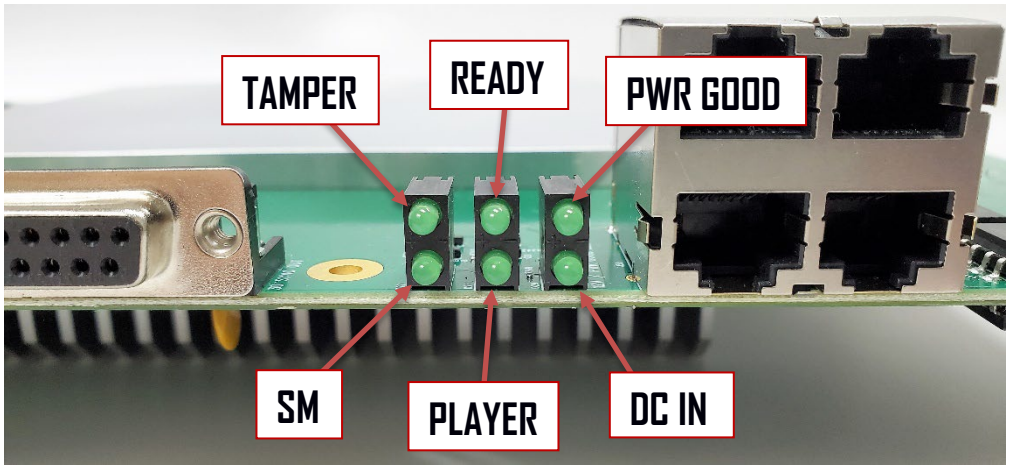

Figure 2: Status LEDs of STAR-2000-3 Module

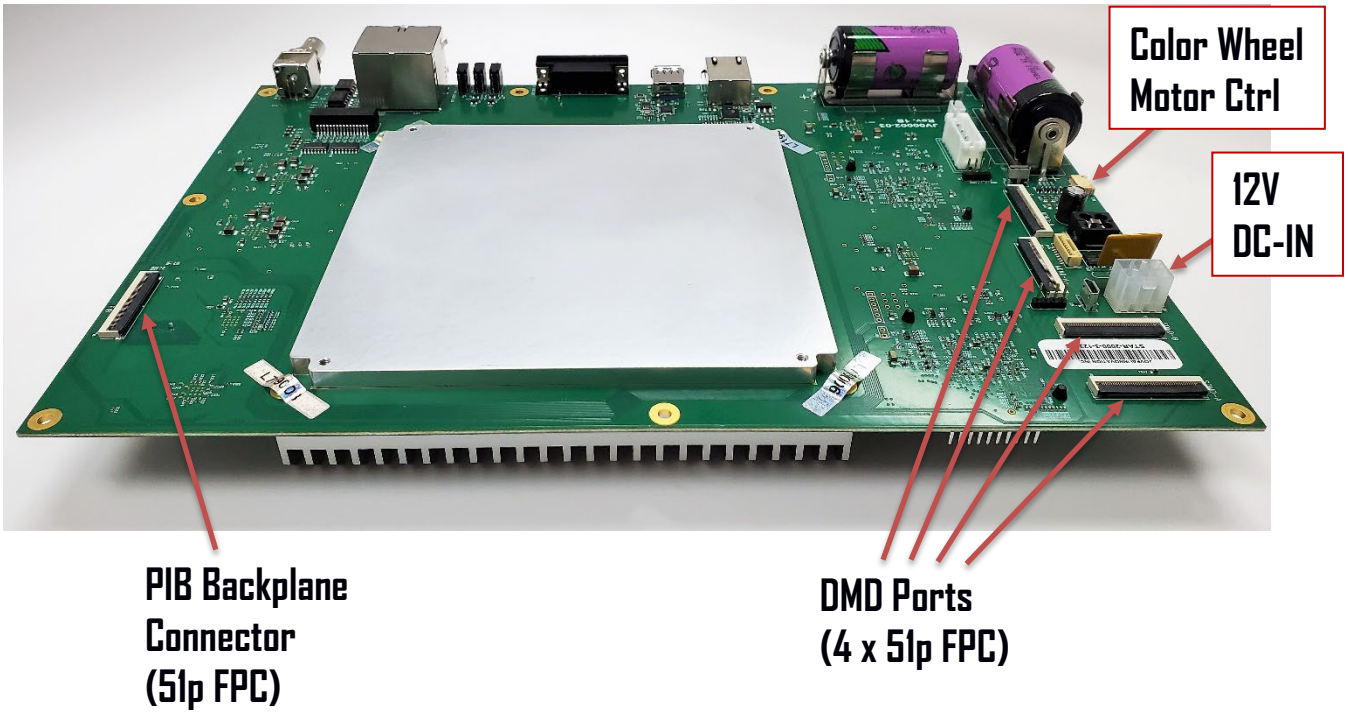

Figure 3: Back View of STAR-2000-3 Module

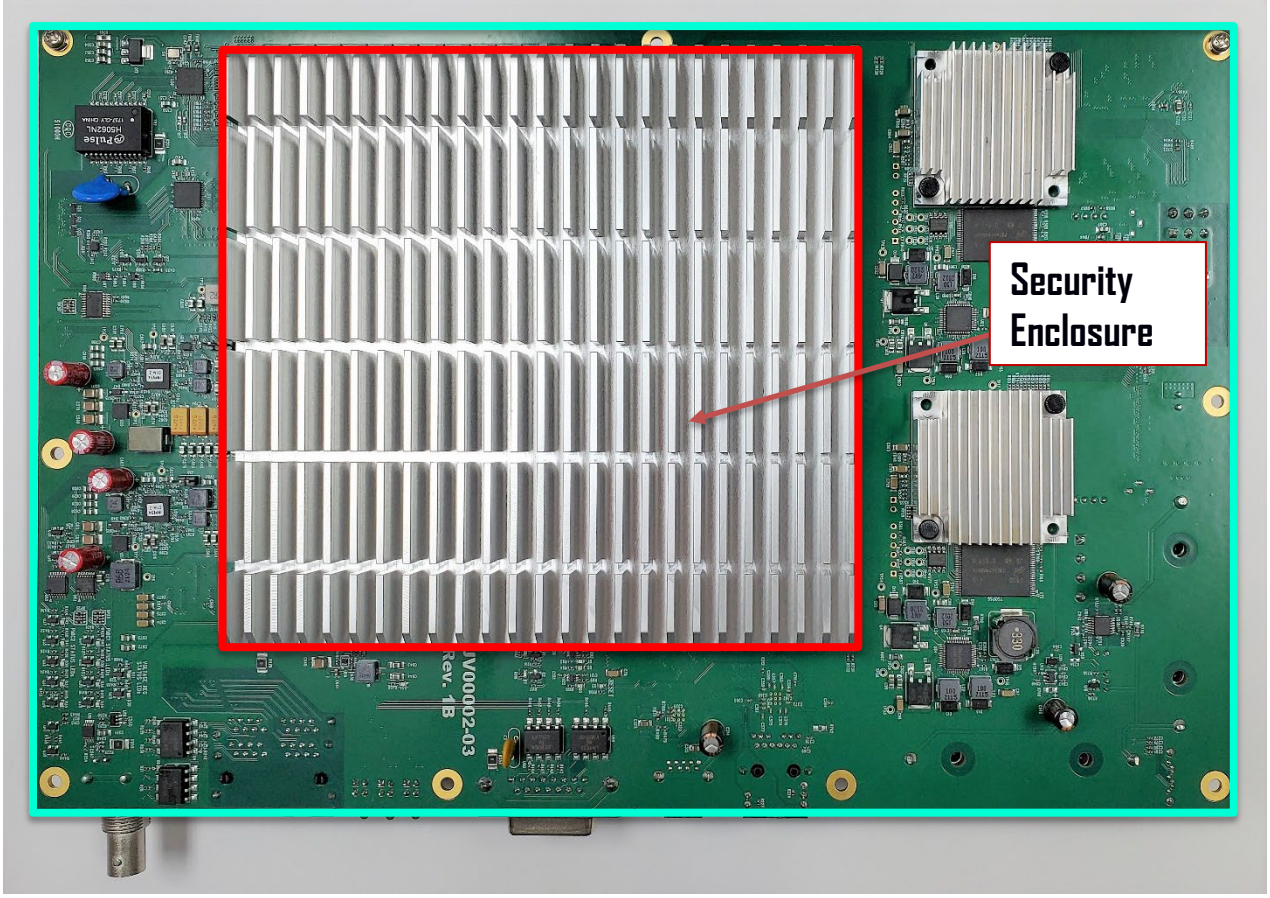

Figure 4: Top View of STAR-2000-3 Module

Note: All components which lie outside the security enclosure are not security relevant.

The cryptographic boundary is defined by the outer perimeter of the module's PCB. It is outlined in green. All security related components are enclosed within an opaque metal cover outlined in red.

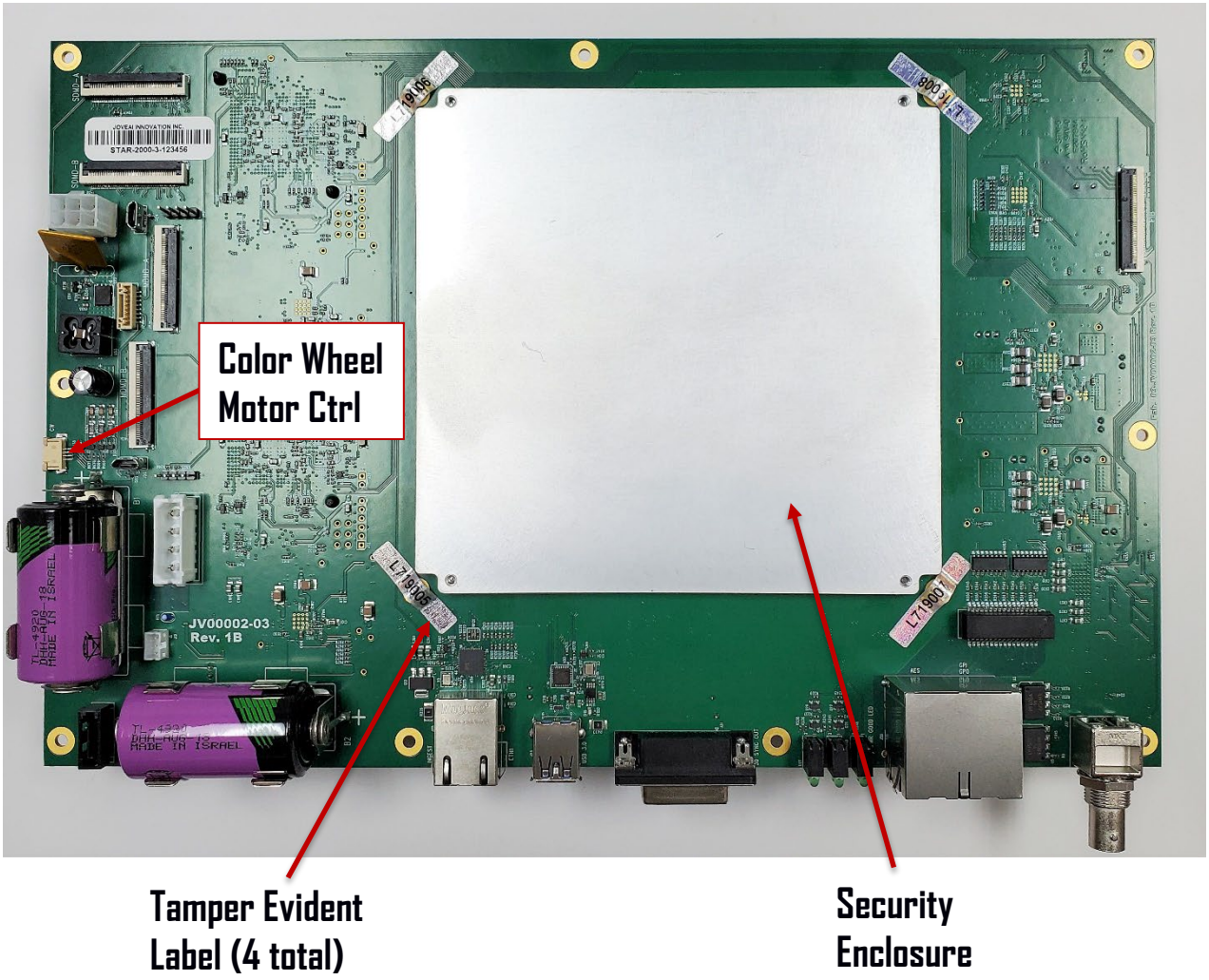

Figure 5: Bottom View of STAR-2000-3 Module

Note: All components which lie outside the security enclosure are not security relevant.

The metal cover, referred to (from the DCI perspective) as a Type I Secure Processing Block (SPBI) enclosure, is protected by tamper detection and response mechanisms. Tamper evident labels are present to allow for tamper evidence examination. The components outside the SPBI enclosure are not

security-relevant and do not affect the security of the STAR-2000-3 module, both from FIPS 140-2 and DCI standpoints. Therefore, they are explicitly excluded from FIPS 140-2 requirements.

The excluded components list consists of non-security relevant data input and data output devices, passive components (capacitors, resistors, inductors), voltage regulators, non-secure clock distribution, DLP formatter ICs (which do not perform security functions), battery management devices, status LEDs, traces and signals routed to these components, the PCB lying outside the metal enclosure, and all the faceplate and backplane connectors.

BLOCK DIAGRAM

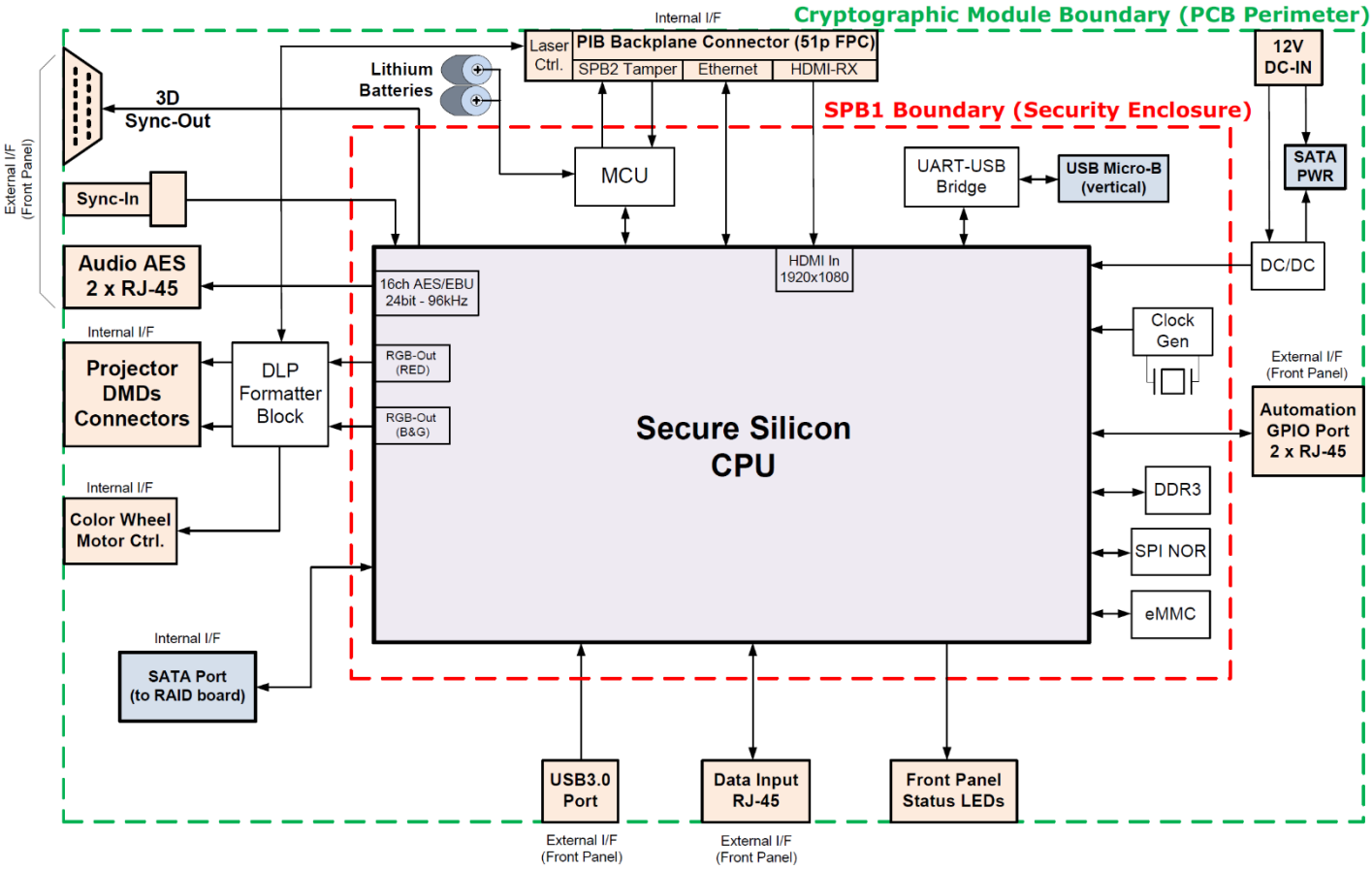

Figure 6: Block Diagram of the STAR-2000-3 Module.

FIPS 140-2 MODES OF OPERATION

The Module operates in both FIPS Approved and non-Approved Modes of Operation.

The Module enters the Approved Mode of Operation after powering-up and completing all power-on self-tests. This is indicated when the Status LEDs on the Front Panel show (PWR GOOD), (DC IN), (READY), and (PLAYER) are solidly on, and the (SM) LED must be off. The (TAMPER) LED may or may not be on, since this LED is not an indicator of the status of the FIPS physical protection enclosure, but is instead an indicator for the DCI Projector's SPB2 boundary.

If the Module enters a Hard Error state (such as if a power-on self-test failed), then the (SM) Status LED will be lit up.

In the FIPS Approved mode of operation only the services listed in Exhibit 6, Exhibit 7, Exhibit 8 and the unauthenticated services are available and the module transitions to the non-Approved Mode of Operation whenever services from Exhibit 11 are invoked.

PHYSICAL PORTS AND LOGICAL INTERFACES

Physical Ports	Logical Interfaces				
	Control Input	Data Input	Data Output	Status Output	Power
Data Input (RJ45)		●	●	●	
USB3.0		●			●
SATA (Int RAID array)		●	●		
SATA PWR					●
Automation GPI (1x RJ45)	●				
Automation GPO (1x RJ45)			●		
Audio AES (2x RJ45)			●		
3D Sync (DB-15)			●		●
Sync-In (BNC)		●			
DMD Ports (4 x 51p FPC)			●		●
Color Wheel Motor Ctrl			●		
PIB Backplane Connector	●	●	●	●	
Status LEDs				●	
12V DC-IN (PCIE-6P)					●
Battery Holders (3.6V)					●

Exhibit 2 – *Physical Ports and Logical Interfaces*

SECURITY LEVEL SPECIFICATION

The STAR-2000-3 module is designed to meet FIPS 140-2 security requirements at the given security levels corresponding to each area below:

SECURITY REQUIREMENTS AREA	LEVEL
Cryptographic Module Specification	2
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

Exhibit 3 – *Security Level Table*

The STAR-2000-3's overall FIPS 140-2 Security Level is 2.

SECURITY RULES

The following specifies the security rules under which the cryptographic module shall operate:

1. The Module supports power input only over the defined power input interface.
2. The Module executes a Limited Operational Environment, which is a self-contained Linux kernel that runs applications contained wholly in its embedded RootFS. When booting, the Module performs firmware integrity tests on the images in the SPI NOR flash prior to launching them.
3. When considering a candidate firmware upgrade image, the Module authenticates its signature using RSA-2048 with SHA256.
4. The Module meets EMI/EMC Class A certification for FCC Part 15 Subpart B.
5. The Module supports 2 tiers of operator roles:
    a. Cryptographic Officer (CO)
    b. User
6. The Module utilizes identity-based authentication.
7. The Module does not support a maintenance interface or role.
8. Switching roles is not permitted.
9. Access to cryptographic services in Approved Mode are not permitted unless the operator is authenticated and has the role which allows them to execute that service. This security policy will indicate which services are performed in Approved Mode, however the Module itself does not provide an explicit indication of when an Approved Mode service is selected.
10. The Module does not support concurrent operators.
11. The Module clears authentication status upon power cycling. This requires an operator to re-authenticate to obtain cryptographic services.
12. An operator may deliberately initiate power-on self tests by power-cycling the Module. These power-on self tests run automatically and do not require or use any input from the operator.
13. The Module does not support manual key entry.
14. The Module does not support both the entry and output of a given CSP or Public Key.
15. The Module's status output shall never output CSPs or other sensitive security information that could compromise the Module. The Module shall not output intermediate key generation values.
16. If an SPBI Tamper Event occurs, the CSPs are zeroized and the Module becomes permanently inoperative.
17. When Module enters Hard Error state, data output is inhibited and all services, both authenticated and unauthenticated, are disabled - the Module will not respond to any requests or commands. The only way to attempt to recover is to power cycle the Module.

CRITICAL SECURITY PARAMETERS, PUBLIC KEYS, AND PRIVATE KEYS

The following is a list of all CSPs, Public Keys, and Private Keys. For each one, it also specifies the process of key generation, storage, and zeroization.

CSPs and Private Keys:

- The Module does not support CSPs or Private Keys in the FIPS Approved Mode.

Public Keys:

1. **Intermediate RSA X.509v3 Certificate**: The intermediate certificate in the JoveAI DCI Certificate chain.
    a. **Generation**: Generated outside of the Module by JoveAI Manufacturing.
    b. **Storage**: Plaintext in SPI NOR as part of the Root FS of the kernel images. Also present in DRAM as plaintext.
    c. **Zeroization**: N/A
2. **Root RSA X.509v3 Certificate**: The root certificate in the JoveAI DCI Certificate chain.
    a. **Generation**: Generated outside of the Module by JoveAI Manufacturing.
    b. **Storage**: Plaintext in SPI NOR as part of the Root FS of the kernel images. Also present in DRAM as plaintext.
    c. **Zeroization**: N/A
3. **Firmware Update Key**: An RSA-2048 Public Key.
    a. **Generation**: Generated outside of the Module by JoveAI Manufacturing.
    b. **Storage**: Held in DRAM in plaintext as part of the Candidate Firmware Update Image's Signing Certificate.
    c. **Zeroization**: N/A

IDENTIFICATION AND AUTHENTICATION POLICY

Listed below are the Module's roles, type of authentication mechanism, and the associated authentication data:

ROLE	AUTHENTICATION TYPE	AUTHENTICATION DATA
Cryptographic Officer	Identity Based	RSA Digital Signature Verification *(Firmware Update Key)*
User	Identity Based	RSA Digital Signature Verification *(Firmware Update Key)*

Exhibit 4 - *Roles and Required Identification and Authentication (FIPS 140-2 Table C1)*

The Cryptographic Officer (CO) is the operator responsible for the installation of the Cryptographic Module and inspection of physical security. The User is the general user of the Module.

The strength of the implemented authentication mechanism is described below, along with probabilities associated with random attempts, and multiple consecutive attempts within a one-minute period to subvert the implemented authentication mechanisms:

AUTHENTICATION MECHANISM	STRENGTH OF MECHANISM
RSA Digital Signature Verification	The Module implements an RSA-2048-bit Public Key for the RSA Digital Signature Verification. As per SP 800-57, this key has a security strength equivalent to 112 bits. As such, the probability of a single attempt is limited to ($1 / 2^{112}$) which is much less than 1 / 1,000,000. The Module takes approximately 10 seconds to complete a power-cycle and its power-on-self-tests. If an unsuccessful firmware update takes place (e.g., Firmware Load self-test fails), the Module enters an Error State and must be power-cycled. As such it is only possible to attempt the Firmware Update service up to 6 times within a 1 minute period. The probability of success in a 1 minute period would thus be ($6 / 2^{112}$), which is much less than 1 / 100,000.

Exhibit 5 - *Strengths of Authentication Mechanisms (FIPS 140-2 Table C2)*

ACCESS CONTROL POLICY

Below is a list of *authenticated* services, and a description of the operations carried out by that service for services used in the Approved mode of operation:

SERVICE	DESCRIPTION
Firmware Update	Update IMB Firmware. Get IMB Firmware Update Progress.

Exhibit 6 – *List of services and their descriptions in the Approved mode of operation*

Below is a list of services, cryptographic keys & CSPs, types of access to the cryptographic keys & CSPs, and for which authorized roles a service is available via the corresponding services in the Approved mode of operation:

Service	Public Keys	Private Keys and CSPs	Types of Access:			Operator Permissions	
			Read	Write	Exec	CO *(Crypto Officer)*	User
Firmware Update	Root RSA X.509v3 Certificate	None	X		X	X	X
	Intermediate RSA X.509v3 Certificate	None	X		X	X	X
	Firmware Update Key	None	X	X	X	X	X

Exhibit 7 – *Services Authorized for Roles, Access Rights within Services in the Approved mode of operation*

Below is a list of non-Approved services that are available only in the Non-Approved mode of operation:

SERVICE	DESCRIPTION	NON-APPROVED ALGORITHMS	Operator Permissions	
			CO *(Crypto Officer)*	User
SPB2 Door Closure Confirmation	Attempt to confirm that the SPB2 Door is closed.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	
Battery Management	Used to manage battery sensor parameters, set thresholds, and to replace batteries.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	
Projector Testing	Projects the specified X'Y'Z' color.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	
User Account Administration	Creation and deletion of new users. Query for a list of existing user accounts.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant), SHA-256 (non-compliant)	X	X

Modify SPB Clock	Modifies the SPB Clock offset, adjusting the clock faster or slower. Restricted to ±6 minutes each year.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
Device Certificate Operations	Retrieval of Leaf Certificates for SM, RES, and LS.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
Audit Log Retrieval	Get DCI Audit Logs, extract syslogs.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant), SHA-256 (non-compliant)	X	X
DCI Ingestion Operations	Ingest DCPs, ingest KDMs, Direct KDM Ingest. Get DCP ingestion status, stop DCP ingestion in progress. Remove DCPs, remove KDMs.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant), SHA-256 (non-compliant)	X	X
DCI Show Administration	Ingest Show Playlist, update Show Playlist, remove Show Playlist, remove interrupted Show Playlist. Ingest Show Schedule, remove Show Schedule.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X

Set Audio / Video Configuration	Set IMB: Output Audio Sample Rate Output Video Mode Audio Delay Audio Mapping Get IMB Output Video Mode	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
RAID HDD Management	Set RAID rebuild priority, RAID create, RAID delete. RAID filesystem check. Format DCP store. Get Format DCP store status, get RAID filesystem check status.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
GPIO Configuration	Set Automation GPO. Set GPI Check Interval.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
DCI Show Management	Query available SPLs, query available DCPs, query available KDMs. Get SPL, get CPL, get KDM. Validate SPL, validate DCP. Execute SPL, stop SPL. Query interrupted SPL. Query available Show Schedules. Get Show Schedule. Enable Schedule Mode, disable Schedule Mode, get Schedule Mode. Set IMB Command (play/pause). Set IMB Seek. Get MB Status. Get AuthId of Playing SPL.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant), RNG (FIPS 186-2)	X	X
Get SPB Clock	Get SPB Clock, get SPB Clockset Initial Time and Current Offset.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X

Storage Management	Query Internal IMB Storage, Query Internal SM Storage. Get RAID Controller Info, Get RAID Smart Info, Get RAID Rebuild Percentage, Get RAID Performance, Get RAID Usage.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
External Storage Utilization	Open Directory, Read Directory, Close Directory. Open File, Read File, Close File.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
Thermal Status	Get Thermal Readings.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
Get Audio / Video Configuration	Get IMB Output Audio Delay. Get Audio Mapping.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
SMS Status and Configuration	SMS Provide Status Info, SMS Provide Network Info, SMS Has Set Network Info. Store New SMS Data Blob. Remove SMS Data Blob. List SMS Data Blobs. Retrieve SMS Data Blob. Overwrite SMS Data Blob.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X

System Boot	Power off, reboot.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
IMB Status and Control	Get IMB Command Set Status, Get SPB2 Door Status, Get Model and Serial, Get SPB Version.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
Battery Status	Used to read the last known battery status, retrieve thresholds, and get the battery parameter description.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
User Account Management	Change user account password. Get Current User ID. Logout Current User.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant), SHA-256 (non-compliant)	X	X
GPIO Operations	Get GPI Check Interval, Get GPI State, Get Automation GPO.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X

TLS-based Notifications	Module Firmware Update Status. SMS Status Request and Network Configuration. DCI Show Management. IMB Status and Control. Thermal Status. Battery Operations. GPIO Operations.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant)	X	X
User Login Operations	Login User Account.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant), SHA-256 (non-compliant)	X	X
Time Licensing System	Ingest License File. Get License File. Get License Status. Manage License Revocation.	NDRNG, SHA-1 (non-compliant), MD5, AES (non-compliant), DRBG (non-compliant), HMAC (non-compliant), RSA (non-compliant), TLS KDF (non-compliant), SHA-256 (non-compliant)	X	X

Exhibit 8 – *Non-Approved Services*

ALGORITHMS

APPROVED MODE OF OPERATION

The module uses the following Approved cryptographic algorithms in the Approved mode of operation:

CAVP CERT	ALGORITHM	STANDARD	MODE / METHOD	KEY LENGTHS, CURVES, OR MODULI	USE
C1913	RSA	FIPS 186-4	PKCS1.5 (SHA256)	2048	Digital Signature Verification
C1913	SHS	FIPS 180-4	SHA256	N/A	Message Digest

Exhibit 9 – *Table of Approved Algorithms used in the Approved mode of operation*

In the Approved mode of operation, the module does not use other algorithms/modes contained in CAVP certificate #C1913. There are algorithms, modes, and keys that have been CAVP tested but not used by the module. Only the algorithms, modes/methods, and key lengths/curves/moduli shown in this table are used by the module.

The module uses the following Non-Approved cryptographic algorithm in the Approved mode of operation:

ALGORITHM	RATIONALE
AES-GCM	Proprietary algorithm used to encrypt firmware at rest ("no security claimed" as per IG 1.23). • The algorithm is not used whatsoever to meet any FIPS 140-2 requirements. • The algorithm does not access or share CSPs in a way that counters the requirements of this IG. • The algorithm is not intended to be used as a security function. The GCM cryptographic operation is applied for "good measure". • The use and purpose of GCM is unambiguous, this operation is not exposed to the operator and it cannot be confused for a security function. The only security function that the Module provides in the FIPS approved mode is Firmware Update.

Exhibit 10 – *Table of Non-Approved Algorithms used in the Approved mode of operation*

NON-APPROVED MODE OF OPERATION

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

ALGORITHM	USE
NDRNG *(non-compliant)*	Seeding the DRBG.
RNG (FIPS 186-2) *(non-compliant)*	Shared secret computation
SHA-1 *(non-compliant)*	Used only for the FIPS 186-2 RNG.
SHA-256 *(non-compliant)*	Secure hashing.
MD5	Message Digest (used only in TLS).
AES *(non-compliant)*	Data Decryption DRBG Encrypt the Seed Value. Decrypt the Encrypted Seed Value.
DRBG *(non-compliant)*	Generating the Seed Encryption Key and Seed Value. Generates the IV for encrypting the Seed Value using the Seed Encryption Key. Generating Salt values for Password hashing.
HMAC *(non-compliant)*	Used to perform integrity checking on encrypted content.
RSA *(non-compliant)*	Key Generation Digital Signature Generation Key Transport
TLS KDF *(non-compliant)*	TLSv1.0 PRF, Key Agreement

Exhibit 11 – *Table of Non-Approved Algorithms used in the Non-Approved mode of operation*

UNAUTHENTICATED SERVICES

Below is a list of services that do not require an authorized role (e.g. services that do not require authentication, for example self-tests and show status). These services will not disclose, modify, or substitute CSPs, use an Approved security function, or otherwise affect the security of the cryptographic module.

Self-Tests:

1. **Power-On Self Tests:**
    a. Firmware Integrity Test (Bootloader): 384-bit EDC computed over the Bootloader image components in SPI NOR Flash.
    b. Firmware Integrity Test (S3BL): 384-bit EDC computed over the S3BL (Stage 3 Bootloader) in SPI NOR Flash.
    c. Firmware Integrity Test (Stage 4 Bitstream): 384-bit EDC computed over Stage 4 Bitstream image in SPI NOR Flash.
    d. Firmware Integrity Test (Stage 4 Kernel): 384-bit EDC computed over Stage 4 Kernel image in SPI NOR Flash.
    e. SHA-256 KAT
    f. RSA-2048 SHA-256: RSA Signature Verification KAT

2. **Conditional Self Tests:**
    a. Firmware Load: RSA-2048 with SHA256 signature verification computed over the candidate firmware update image.

Status Output:

1. **TCP-based Notifications:**
    a. IMB Status and Control:
        i. IMB Shutdown completed.
        ii. IMB Boot Status.
    b. SMS listener for SPL Timed Notifications:
        i. Communications will be done on port 9009 . The IMB will initiate an unauthenticated TCP connection, and send the data in the ShowPlaylist at the time specified in the ShowPlaylist.
        ii. This is used as a status notification for the SMS. The data sent to the SMS is opaque to the SM, as the SM just forwards the data back to the SMS. The maximum length for the data is 64KB.
        iii. No response is expected of the SMS.
2. **Physical Notifications:**
    a. Front-panel LEDs.

Services for the Projector Intelligence Block:

1. Image Media Block Status and Control.
2. Projector Calibration.
3. GetScaling / SetScaling.

PIB Passthrough TCP Services:

1. SMS to PIB Passthrough.

Zeroization Service:

1. Zeroization can be triggered by deliberately inducing a Tamper Event, either by removing the FIPS Physical Security Enclosure, or removal of the batteries.

PHYSICAL SECURITY POLICY

The following physical security mechanisms are employed by the Module:

- Production grade materials.
- A hard, opaque metal enclosure which depresses a set of tamper detection switches, which are battery powered and actively monitor the enclosure 24/7. If the metal enclosure is lifted, or the batteries are removed, it will result in zeroization.
- Tamper evidence is given by 4 tamper-evident labels (TELs) affixed during manufacturing. The location of these 4 TELs is illustrated in Figure 5. Inspection of these TELs is prescribed in Exhibit 12 below:

PHYSICAL SECURITY MECHANISMS	RECOMMENDED FREQUENCY OF INSPECTION/TEST	INSPECTON/TEST GUIDANCE DETAILS
Tamper-response zeroization	If tampering is suspected (Module is unresponsive, and SM LED is always on when the Module is powered up). Batteries must be checked for their state of health and replaced when necessary.	Inspect metal enclosure for signs of damage. Confirm that the batteries are installed and still hold a charge at 3.6V.
Tamper Evident Labels	1 year	Visually inspect the TELs, checking for scratches or tearing.

Exhibit 12 - *Inspection/Testing of Physical Security Mechanisms (FIPS 140-2 Table C5)*

MITIGATION OF OTHER ATTACKS POLICY

The STAR-2000-3 is not designed to mitigate against attacks outside of the scope of the FIPS 140-2 specification.

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

Exhibit 13 - *Mitigation of other attacks*

REFERENCES

[ST 430-1] The Society of Motion Picture and Television Engineers.
D-Cinema Operations — Key Delivery Message. January 12, 2017.
Available at:
https://ieeexplore.ieee.org/document/7864300

[DCSS v1.4] Digital Cinema Initiatives, LLC, Member Representatives Committee.
Digital Cinema System Specification Version 1.4. July 20, 2020.
Available at:
https://www.dcimovies.com/specification/DCI_DCSS_v1-4_20-July-2020.pdf