Revision History

Revision	Date	Description of change
A	10/20/2018	Initial release
B	1/11/2019	Update to roles and services
C	6/20/2019	Update to approved algorithms and CSP's
D	6/20/2019	Update to mfg certificate name
E	7/15/2019	Update to firmware version
F	7/31/2019	Update to security rules
G	8/2/2019	Update for FIPS 140-2 IG D.11 Statements
H	5/15/2020	Update based on NIST comments and questions from 4/24/2020
J	10/8/2020	Update to Table 3, RSA Caveat

Reference Documents

Reference #	Document Name
FIPS PUB 140-2	Security Requirements For Cryptographic Modules
DCI DCSS CTP v1.2	Digital Cinema System Specification Compliance Test Plan, v1.2

Contents

1. Scope

This document is the Security Policy for the Secure Processing Block (SPB) of the QSC CMS-5000 Cinema Media Server. This policy is a specification of the security rules under which the CMS-5000 is operated, meeting the FIPS 140-2 Level 3 requirements.

2. Module Overview

The CMS-5000 (Hardware Version: AP-000128-01 Rev J, Firmware Version: 1.0.01391), includes a cryptographic module designed in accordance with FIPS 140-2 and the Digital Cinema Initiatives (DCI) Digital Cinema System Specification requirements for a Secure Processing Block (SPB). For FIPS 140-2 purposes, the CMS-5000 SPB is categorized as a multi-chip embedded cryptographic module encased in a metallic enclosure. The module does not have non-FIPS mode of operation.

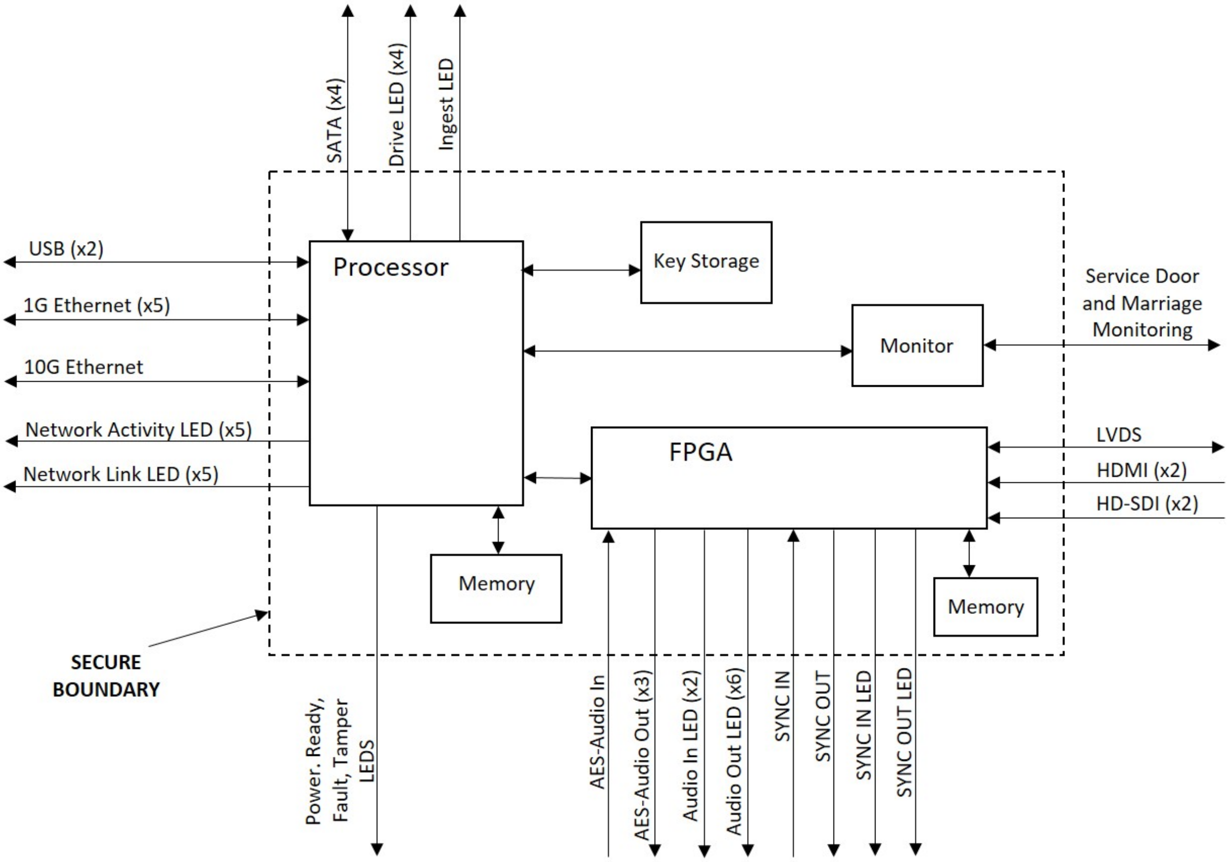
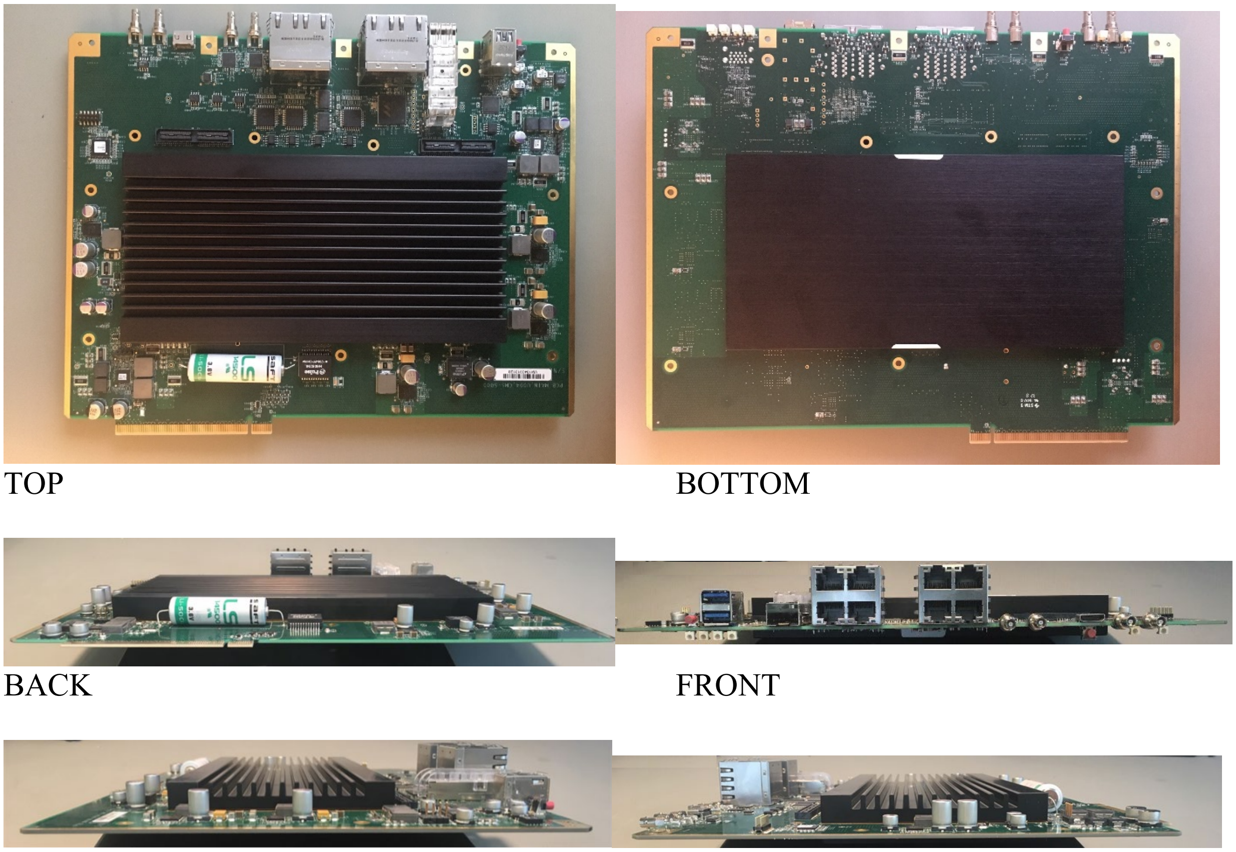


Figure 1 – CMS-5000 Cryptographic Module Block Diagram

The images below depict the cryptographic module; all components not contained within the metallic enclosure are explicitly excluded from the requirements of FIPS 140-2 as they are non-security relevant and have no impact on the overall security of the modules. The cryptographic boundary of the module is defined as being the outer physical perimeter of the module's PCB board; the effective security boundary is the physical perimeter of the module's metal Security Enclosure. The logical boundary of the cryptography module encompasses the Processor, FPGA, Key Storage, Monitor and Memory blocks as shown in Figure 1.



TOP

BOTTOM

BACK

FRONT

LEFT SIDE

RIGHT SIDE

Figure 2 – CMS-5000 Cryptographic Module

3. Security Level

The cryptographic module meets the overall requirements applicable to FIPS 140-2 Level 3.

Table 1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

4. Modes of Operation

Approved mode of operation

The module only supports an Approved mode of operation, which is specified during power-on with a message to the log, “Operating in FIPS compliant mode”.

The module will indicate the power up self-tests executed successfully by setting the Tamper, Fault and Ready LEDs as follows:

Tamper: OFF, Fault: OFF, Ready: FLASH (green)

The module supports the following Approved algorithms:

Table 2 - FIPS Approved Algorithms

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
C419	AES	FIPS 197 SP 800-38A	AES-CBC AES-ECB	128, 192, 256[1]	Data Encryption/Decryption
C419	CVL	SP 800-135rev1	TLS V1.0 KDF[2]		Key Derivation
C419	CVL	SP 800-56B	RSA Decryption Primitive	2048	Decryption Primitive for RSA Key Unwrap
C419	DRBG	SP 800-90Arev1	CTR_DRBG (with DF)	AES-256	Deterministic Random Bit Generation
C419	HMAC	FIPS 198-1	HMAC-SHA-1	160	Message Authentication
C419	RSA[3]	FIPS 186-4	KeyGen	2048	RSA Key Generation
C419	RSA	FIPS 186-4	SigGen PKCS 1.5 (SHA-256)	2048	Digital Signature Generation

[1] Only 128-bit key size is used in the FIPS Approved Mode.

[2] As per FIPS 140-2 IG, D.11, TLS protocol has not been reviewed or tested by the CAVP and CMVP.

[3] RSA FIPS 186-4 KeyGen is not supported in the FIPS Approved Mode. RSA Key pairs are generated at manufacturing.

CAVP Cert	Algorithm	Standard	Mode/Method	Key Lengths, Curves or Moduli	Use
C419	RSA	FIPS 186-4	SigVer PKCS 1.5 (SHA-1 and SHA-256)	2048	Digital Signature Verification
C419	RSA[4]	FIPS 186-2	SigVer PKCS 1.5 (SHA-1)	1024	Digital Signature Verification
C419	SHS	FIPS 180-4	SHA-1, SHA-256		Message Digest

The module supports the following non-Approved but allowed algorithms (Table 3, Part 1) and the following no security claimed algorithms (Table 3, Part 2):

Table 3, Part 1 - Allowed Algorithms

Algorithm	Caveat	Use
MD5	Exclusively used within TLS V1.0 KDF as per SP 800-135	Key Derivation
NDRNG	The module generates cryptographic keys whose strengths are modified by available entropy; module meets 112-bit minimum requirement. The NDRNG of the module supports 128 bit security strength.	Seeding SP 800-90A AES-256 CTR_DRBG
RSA	RSA (CVL Cert. #C419, key wrapping)	RSA Key Wrapping and Unwrapping

[4] RSA 1024 modulus size is not supported in the FIPS Approved Mode.

Table 4, Part 2 – No Security Claimed Algorithms

Algorithm	Caveat	Use
FIPS 186-2 RNG (no security claimed)	Non-Approved Random Number Generator used to perform Key Transforms; not security relevant. (No security claimed as per FIPS 140-2 IG 1.23)	Key transform
TI S-BOX (no security claimed)	Proprietary algorithm used to facilitate the marriage between a Projector and the module; not security relevant. (No security claimed as per FIPS 140-2 IG 1.23)	Proprietary Algorithm

5. Ports and Interfaces

The cryptographic module provides the following physical ports and logical interfaces:

Table 5 - Module Logical Interfaces and Physical Ports

Logical Interface	Module Physical Ports
Data Input Interface	1G Ethernet (x5), 10G Ethernet, Sync In, USB (x2), SATA (x4), AES-Audio In (x3), HDMI (x2), HD-SDI (x2)
Data Output Interface	1G Ethernet (x5), 10G Ethernet, Sync Out, USB (x2), SATA (x4), AES-Audio Out (x3), LVDS
Control Input Interface	1G Ethernet (x5), 10G Ethernet, Reset Switch, Restore Switch, Service Door and Marriage Monitoring
Status Output Interface	1G Ethernet (x5), 10G Ethernet, Service Door and Marriage Monitoring, Power LED, Ready LED, Fault LED, Tamper LED, Sync Out LED, Sync In LED, Network Link LED (x5), Network Activity LED (x5), Audio In LED (x2), Audio Out LED (x6)
Power Interface	Power traces

Additional LED Information

Table 5 – Module LED Descriptions

LED	Description
Power	Off or Green. Used to indicate power status.
Ready	Off or Green. Used to indicate module status.

Fault	Off or Yellow. Used to indicate module status.
Tamper	Off or Red. Used to indicate module status.
Drive	Off or Blue. Used to indicate drive activity.
Ingest	Off or Blue. Used to indicate ingest operation.
Network Link	Off or Green. Used to indicate Ethernet link.
Network Activity	Off or Yellow. Used to indicate Ethernet traffic.
Audio In	Off, Green or Yellow. Used for audio interface.
Audio Out	Off, Green or Yellow. Used for audio interface.
Sync In	Off or Green. Used to indicate sync in status.
Sync Out	Off or Green. Used to indicate sync out status.

6. Identification and Authentication Policy

Assumption of roles

The cryptographic module supports the roles listed in the table below. The Cryptographic-Officer role is distinct from the four User roles of ADMIN, INSTALLER, MANAGER and PROJECTIONIST.

Table 6 - Roles and Required Identification and Authentication

Role	Type of Authentication	Authentication Method
Cryptographic-Officer	Identity-based operator authentication	2048-bit Digital Signature Verification
ADMIN	Identity-based operator authentication	Password based authentication or SHA-256 Token Signature Verification
INSTALLER	Identity-based operator authentication	Password based authentication or SHA-256 Token Signature Verification
MANAGER	Identity-based operator authentication	Password based authentication or SHA-256 Token Signature Verification
PROJECTIONIST	Identity-based operator authentication	Password based authentication or SHA-256 Token Signature Verification

Username and Password Rules:

- Allowed characters are from UTF-8 character set, except for values in the ranges of 0x0000–0x001F and 0x007F–0x009F
- Must be a minimum of 4 and maximum of 64 characters in length
- The module is shipped with default passwords for each the user roles, and the user is responsible for changing those passwords

Table 7 – Strengths of Authentication Mechanisms

Authentication Mechanism	Strength of Mechanism
Digital Signature	This applies to both the 2048-bit Digital Signature Verification and the SHA-256 Token Signature Verification. Both methods utilize the RSA 2048 SHA-256 Digital Signature Verification. The strength of a 2048-bit RSA key is known to be 112-bits. Therefore, the strength of a 2048-bit digital signature is 1/(2^112), which is less than 1/1,000,000. In a worst case scenario, the module can perform 10000 signature verifications per second, which does not include network limitations or timing constraints. Therefore, the probability that multiple attacks within a given minute will be successful is 10000/(2^112), which is less than 1/100,000.
Password based authentication	The allowed UTF-8 character set provides well over 100,000 assigned possible characters. However, for these purposes, we'll assume a much smaller set of 100 possible characters. With a minimum 4-character authentication password, the probability that a random attempt will succeed is (1/100)^4, which is 1 x 10^(-8); which is less than 1/1,000,000. The module allows a maximum of 600 attempts per minute (100ms delay after failed attempt), so the probability of successfully authenticating to the module within one minute is 600 x 10^(-8); which is less than 1/100,000.

7. Access Control Policy

7.1. Roles and Services

Table 8 – Services Authorized for Roles

Role	Authorized Services
Cryptographic-Officer	• Perform Projector Marriage • Start operation
ADMIN	After Successful Projector Marriage: • saveuser *All accounts • deleteuser *All accounts • All INSTALLER services
INSTALLER	After Successful Projector Marriage: • addautomationcue • addbundlecue • deleteautomationcue • deletebundlecue • removedevice • savedevice • getlease • installfirmware • reloadethconfig • removeconfig • saveconfig • setlease • uploadfirmware • setsecuretime • setraidaction • getusers • installlicense • uninstalllicense • saveuser *Cannot change ADMIN accounts • deleteuser *Cannot change ADMIN accounts • All MANAGER services
MANAGER	After Successful Projector Marriage: • rebootserver • deleteasset • getasseturi • saveplaylist • saveschedule • adhoctransfer

	• canceltransfer • cleartransferhistory • exportasset • listtransferrableassets • resumetransfers • setsubmitkdm • suspendtransfers • transferasset • transfersrunning • cancelgetsecuritylogs • getinstalledlicenses • getsecuritylogs • getsecuritylogsnext • getdriveinfo • All PROJECTIONIST services
PROJECTIONIST	After Successful Projector Marriage: • getissuerid • getaudiostatus • getautomationcues • getbundlecues • getdevices • getprojectorstatus • refreshprojectormacros • triggercommand • getchangecounts • getconfig • getsecureclock • getassetmetadata • getassets • getassetxml • gettransferdetails • listtransferlocations • scanftpmount • getperfdiag • getsysdiag • getdrivediag • getinputtelemetry • getplaybackmode • getplaybackstatus • getplaystatedetail • loadclip

	• loadplaylist • setplaybackmode • setplaystate • setposition • skipback • skipforward • getcertificate • getlockcode • getalerts • clearalerts • getdiskspaceusage • getimbstatus • getnetworkstatus • getraidstatus • getsecuritystatus • getserialnumber • getssidnumber • getsystemlogs • getversions

7.2. Unauthenticated Services:

The cryptographic module supports the following unauthenticated services:

1. *Power On/Off and resulting module self-tests*
2. *LED Visual Inspection*
3. *Reset Button*
4. *Restore Button - Boot to Restore Partition*
5. *Restore Button – Zeroization*

Ethernet Connections:

6. *UDP - Ethernet Discover Response*
7. *UDP - QLAN Response*
8. *DHCP Client (CMS-5000 is the Client)*
9. *Establish HTTPS connection*
10. *Ping Response*
11. *Retrieve System Log Package response*
12. *ARP request response*
13. *Web page request for Web Application (HTML pages)*
14. *API login request*

7.3. Definition of Critical Security Parameters (CSPs)

The module contains the following CSPs:

Table 9 – Critical Security Parameters

CSP Name	Description	Generation	Storage	Zeroization
Device Private Key (Transport)	RSA 2048	N/A – Generated in Factory	Plaintext DDR Plaintext SecureFlash	Actively overwritten via Restore Button – Zeroization
Device Private Key (Log Signing)	RSA 2048	N/A – Generated in Factory	Plaintext DDR Plaintext SecureFlash	Actively overwritten via Restore Button – Zeroization
SMS Private Key	RSA 2048	N/A – Generated in Factory	Plaintext DDR Plaintext SecureFlash	Actively overwritten via Restore Button – Zeroization
Web Server Private Key	RSA 2048	N/A – Generated in Factory	Plaintext DDR AES-128-ECB Encrypted on Filesystem	DDR: Actively overwritten via Restore Button – Zeroization Filesystem: N/A – AES-128-ECB encrypted
Web Server Key Encryption Key	AES-128-ECB	N/A – Generated in Factory	Plaintext DDR Plaintext SecureFlash	Actively overwritten via Restore Button – Zeroization
Firmware Protection Key	AES-128-CBC	N/A – Generated in Factory	Plaintext DDR Plaintext SecureFlash	Actively overwritten via Restore Button – Zeroization
Content Encryption Key	AES-128-CBC	N/A	Plaintext DDR	Actively overwritten via Restore Button – Zeroization

CSP Name	Description	Generation	Storage	Zeroization
TLS Encryption Keys	AES-128-CBC	N/A	Plaintext DDR	Actively overwritten via Restore Button – Zeroization
TLS Integrity Keys	HMAC-SHA-1	N/A	Plaintext DDR	Actively overwritten via Restore Button – Zeroization
TLS KDF Internal State	TLS KDF V1.0 (SP 800-135)	N/A	Plaintext DDR	Actively overwritten via Restore Button – Zeroization
TLS Pre-Master Secret	Secret 48-bytes for TLS KDF V1.0 (SP 800-135)	CTR_DRBG (AES-256)	Plaintext DDR	Actively overwritten via Restore Button – Zeroization
TLS Master Secret	Secret 48-bytes for TLS KDF V1.0 (SP 800-135)	TLS KDF V1.0 (SP 800-135)	Plaintext DDR	Actively overwritten via Restore Button – Zeroization
Entropy Seed	NDRNG Seed 384-bits	NDRNG	Plaintext DDR	Actively overwritten via Restore Button – Zeroization
SP 800-90A DRBG Internal State	CTR_DRBG (AES-256)	CTR_DRBG (AES-256)	Plaintext DDR	Actively overwritten via Restore Button – Zeroization

CSP Name	Description	Generation	Storage	Zeroization
Authentication Passwords	Minimum of 4 and maximum of 64 characters in length Or SHA-256 Tokens	N/A	Plaintext DDR SHA-256 Hashed in Filesystem	DDR: Actively overwritten via Restore Button – Zeroization Filesystem: N/A – Passwords are SHA-256 Hashed

Definition of Public Keys:
The following are the public keys contained in the module:

Table 10 – Public Keys

Public Key Name	Description	Generation	Storage
Device Public Key (Transport)	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A – Generated in Factory	Plaintext Filesystem
Device Public Key (Log Signing)	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A – Generated in Factory	Plaintext Filesystem
SMS Public Key	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A – Generated in Factory	Plaintext Filesystem
Web Server Public Key	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A – Generated in Factory	Plaintext DDR AES-128-ECB Encrypted on Filesystem
Projector Public Key	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A	Plaintext DDR Plaintext Filesystem
QSC Manufacturing Public Key	RSA 2048	N/A	Plaintext DDR Plaintext Filesystem
Root CA Certificate (root.ca.qsc-cms5000.com)	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A	Plaintext DDR Plaintext Filesystem

Public Key Name	Description	Generation	Storage
Intermediate Certificate (.slo02.ca.qsc-cms5000.com)	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A	Plaintext DDR Plaintext Filesystem
HTTPS CA (root.ca.qsc-cms5000-https.com)	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A	Plaintext DDR Plaintext Filesystem
HTTPS Intermediate Certificate (.slo02.ca.qsc-cms5000-https.com)	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A	Plaintext DDR Plaintext Filesystem
Manufacturing Certificate (cs.slo02.ca.qsc-cms5000-mfg1.com)	RSA 2048 X.509 Public Certificate (PEM Encoded)	N/A	Plaintext DDR Plaintext Filesystem

7.4. Definition of CSPs Modes of Access

Table 9 defines the relationship between access to CSPs and the different module services. The modes of access shown in the table are defined as follows:

- Read
- Write
- Zeroize

Please note that all services are sent through an encrypted TLS tunnel and as such, TLS related CSPs are utilized during each service.

In the following table, "Secure Channel CSPs" means the following CSPs are utilized:

Read/Write:

TLS Encryption Keys
TLS Integrity Keys
TLS KDF Internal State
TLS Pre-Master Secret
TLS Master Secret

Read:

SMS Private Key
SMS Public Key
Web Server Private Key
Web Server Public Key
Web Server Encryption Key
SP 800-90A DRBG Internal State
Root CA Certificate (root.ca.qsc-cms5000.com)
Intermediate Certificate (.slo02.ca.qsc-cms5000.com)
HTTPS CA (root.ca.qsc-cms5000-https.com)
HTTPS Intermediate Certificate (.slo02.ca.qsc-cms5000-https.com)

Table 11 – CSP Access Rights within Roles & Services

Service	**Cryptographic Keys and CSPs Access Operation**
Perform Projector Marriage	Read: Device Private Key (Transport) Device Public Key (Transport) Read/Write: Projector Public Key TLS Encryption Keys TLS Integrity Keys TLS KDF Internal State TLS Pre-Master Secret TLS Master Secret
Start operation	Read/Write: Projector Public Key (X.509) TLS Encryption Keys (AES-128-CBC) TLS Integrity Keys (HMAC-SHA-1) TLS KDF Internal State (TLS KDF v1.0) TLS Pre-Master Secret (TLS v1.0) TLS Master Secret (TLS v1.0)
saveuser *All accounts for admin role	Secure Channel CSPs Write: Authentication Passwords
deleteuser *All accounts for admin role	Secure Channel CSPs
addautomationcue	Secure Channel CSPs
addbundlecue	Secure Channel CSPs
deleteautomationcue	Secure Channel CSPs
deletebundlecue	Secure Channel CSPs
removedevice	Secure Channel CSPs
savedevice	Secure Channel CSPs
getlease	Secure Channel CSPs
installfirmware	Secure Channel CSPs Read: Firmware Protection Key QSC Manufacturing Public Key Manufacturing Certificate (cs.slo02.ca.qsc-cms5000-mfg1.com)
reloadethconfig	Secure Channel CSPs
removeconfig	Secure Channel CSPs
saveconfig	Secure Channel CSPs
setlease	Secure Channel CSPs

Service	Cryptographic Keys and CSPs Access Operation
uploadfirmware	Secure Channel CSPs Read: QSC Manufacturing Public Key Manufacturing Certificate (cs.slo02.ca.qsc-cms5000-mfg1.com)
getlockcode	Secure Channel CSPs Read: Device Public Key
setsecuretime	Secure Channel CSPs
setraidaction	Secure Channel CSPs
getusers	Secure Channel CSPs
saveuser *Cannot change ADMIN accounts unless admin role	Secure Channel CSPs Write: Authentication Passwords
deleteuser *Cannot change ADMIN accounts unless admin role	Secure Channel CSPs
rebootserver	Secure Channel CSPs
deleteasset	Secure Channel CSPs
getasseturi	Secure Channel CSPs
saveplaylist	Secure Channel CSPs
saveschedule	Secure Channel CSPs
adhoctransfer	Secure Channel CSPs
canceltransfer	Secure Channel CSPs
cleartransferhistory	Secure Channel CSPs
exportasset	Secure Channel CSPs
listtransferrableassets	Secure Channel CSPs
resumetransfers	Secure Channel CSPs
setsubmitkdm	Secure Channel CSPs Read: Device Private Key (Transport)
suspendtransfers	Secure Channel CSPs
transferasset	Secure Channel CSPs
transfersrunning	Secure Channel CSPs
cancelgetsecuritylogs	Secure Channel CSPs
getinstalledlicenses	Secure Channel CSPs
getsecuritylogs	Secure Channel CSPs Read: Device Private Key (Log Signing)
getsecuritylogsnext	Secure Channel CSPs
installlicense	Secure Channel CSPs Read: Device Public Key (Transport)
uninstalllicense	Secure Channel CSPs
getdriveinfo	Secure Channel CSPs

Service	Cryptographic Keys and CSPs Access Operation
getissuerid	Secure Channel CSPs Read: Device Public Key (Log Signing)
getaudiostatus	Secure Channel CSPs
getautomationcues	Secure Channel CSPs
getbundlecues	Secure Channel CSPs
getdevices	Secure Channel CSPs
getprojectorstatus	Secure Channel CSPs
refreshprojectormacros	Secure Channel CSPs
triggercommand	Secure Channel CSPs
getchangecounts	Secure Channel CSPs
getconfig	Secure Channel CSPs
getsecureclock	Secure Channel CSPs
getassetmetadata	Secure Channel CSPs
getassets	Secure Channel CSPs
getassetxml	Secure Channel CSPs
listtransferlocations	Secure Channel CSPs
scanftpmount	Secure Channel CSPs
getperfdiag	Secure Channel CSPs
getsysdiag	Secure Channel CSPs
getdrivediag	Secure Channel CSPs
getinputtelemetry	Secure Channel CSPs
getplaybackmode	Secure Channel CSPs
getplaybackstatus	Secure Channel CSPs
getplaystatedetail	Secure Channel CSPs
loadclip	Secure Channel CSPs Read: Device Private Key (Transport) Write: Content Encryption Key
loadplaylist	Secure Channel CSPs Read: Device Private Key (Transport) Write: Content Encryption Key
setplaybackmode	Secure Channel CSPs Read: Device Private Key (Transport) Write: Content Encryption Key
setplaystate	Secure Channel CSPs Read: Device Private Key (Transport) Write: Content Encryption Key
setposition	Secure Channel CSPs Read: Device Private Key (Transport) Write: Content Encryption Key
skipback	Secure Channel CSPs

Service	Cryptographic Keys and CSPs Access Operation
	Read: Device Private Key (Transport) Write: Content Encryption Key
skipforward	Secure Channel CSPs Read: Device Private Key (Transport) Write: Content Encryption Key
getcertificate	Secure Channel CSPs Read: Device Public Key (Transport) Device Public Key (Log Signing) SMS Public Key Web Server Public Key Projector Public Key QSC Manufacturing Public Key Manufacturing Certificate (cs.slo02.ca.qsc-cms5000-mfg1.com) Root CA Certificate (root.ca.qsc-cms5000.com) Intermediate Certificate (.slo02.ca.qsc-cms5000.com)
getalerts	Secure Channel CSPs
clearalerts	Secure Channel CSPs
getdiskspaceusage	Secure Channel CSPs
getimbstatus	Secure Channel CSPs Read: Device Public Key (Transport)
getnetworkstatus	Secure Channel CSPs
getraidstatus	Secure Channel CSPs
getsecuritystatus	Secure Channel CSPs
getserialnumber	Secure Channel CSPs
getsystemlogs	Secure Channel CSPs
getversions	Secure Channel CSPs

Table 12 – CSP Access Rights within Unauthenticated Services

Service	Cryptographic Keys and CSPs Access Operation
Power On/Off and resulting module self-tests	N/A (NOTE: Upon module initialization, the module will Read/Write the SP 800-90A DRBG Internal State and Entropy Seed. CSPs are not exposed outside of the module)
LED Visual Inspection	N/A
Reset Button	N/A
Restore Button - Boot to Restore Partition	N/A
Restore Button – Zeroization	Zeroize: Device Private Key (Transport) Device Private Key (Log Signing) SMS Private Key Web Server Private Key Web Server Key Encryption Key Firmware Protection Key Content Encryption Key TLS CSPs: TLS Encryption Keys TLS Integrity Keys TLS KDF Internal State TLS Pre-Master Secret TLS Master Secret Entropy Seed SP 800-90A DRBG Internal State
UDP - Ethernet Discover Response	N/A
UDP - QLAN Response	N/A
DHCP Client (CMS-5000 is the Client)	N/A
Establish HTTPS connection	N/A
Ping Response	N/A
Retrieve System Log Package response	N/A
ARP request response	N/A
Web page request for Web Application (HTML pages)	N/A
API login request	N/A

8. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable; the cryptographic module supports a limited operational environment that restricts the loading of firmware by ensuring all firmware installed is appropriately signed (i.e. the module will only load new firmware delivered in RSA 2048 SHA-256 signed packages). Any firmware loaded into the module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

9. Security Rules

The cryptographic module's design corresponds to the cryptographic 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 module provides identity-based authentication.
2. The module will only provide access to cryptographic services if a valid role has been assumed.
3. The cryptographic module shall perform the following tests:

   A. Power up Self-Tests:

   1. Cryptographic algorithm tests:
      DRBG-AES-256-CTR with DF Known Answer Test
      DRBG-AES-256-CTR with DF SP 800-90A Section 11.3 Health Tests
      SHA-1 Known Answer Test
      HMAC-SHA-1 Known Answer Test
      AES-ECB (128,192,256) Encrypt Known Answer Test
      AES-ECB (128,192,256) Decrypt Known Answer Test
      RSA 2048 SHA-256 Digital Signature Generation Known Answer Test
      RSA 2048 SHA-256 Digital Signature Verification Known Answer Test
      FIPS 186-2 RNG Known Answer Test
      SHA-256 Known Answer Test
      SP 800-135 TLS V1.0 KDF Known Answer Test
      SP 800-56B RSADP Known Answer Test
      SP 800-56B RSAEP Known Answer Test

   2. Firmware Integrity Tests (32-bit EDC):

      Boot Image CRC-32c

      Boot Environment CRC-32

      Root File System CRC-32c

   3. Critical Functions Tests: N/A.

B. Conditional Self-Tests:

1. Continuous Random Number Generator (RNG) test – performed on NDRNG
2. Continuous RNG test – performed on DRBG.
3. Firmware Load Test (RSA 2048 SHA-256 Digital Signature Verification)

4. The module will indicate the power up self-tests executed successfully by setting the Tamper, Fault and Ready LEDs as follows:

   Tamper: OFF, Fault: OFF, Ready: FLASH (green)

5. Data output shall be inhibited during self-tests and error states. The module will indicate an error state by setting the Tamper, Fault and Ready LEDs as follows:

   Tamper: OFF, Fault: ON (yellow), Ready: OFF

6. If the module has been tampered, CSPs will have been zeroized, and the tampered state will be indicated with the Tamper, Fault and Ready LEDs set as follows:

   Tamper: ON (red), Fault: OFF, Ready: OFF

7. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the module.
8. Upon power off, the module will clear any previous authentications and require the operator to authenticate to the module again.
9. The module will obscure authentication data during data entry.
10. The physical and logical paths used by all major categories of output data exiting the cryptographic module are disconnected from the processes performing zeroization of cryptographic keys and CSPs.

10. Physical Security Policy

10.1. Physical Security Mechanisms

The Secure Media Block is a multi-chip embedded cryptographic module, which includes the following physical security mechanisms:

- Production-grade components.
- Tamper responsive hard, metallic enclosure.
- There are two tamper evident labels applied at manufacturing.
- The tamper labels cover screws on the bottom cover of the metallic enclosure.
- The metallic enclosure cannot be removed or displaced without removing both screws covered by the tamper labels.
- If either tamper label shows evidence of tampering, the user is instructed to return the module to the factory.

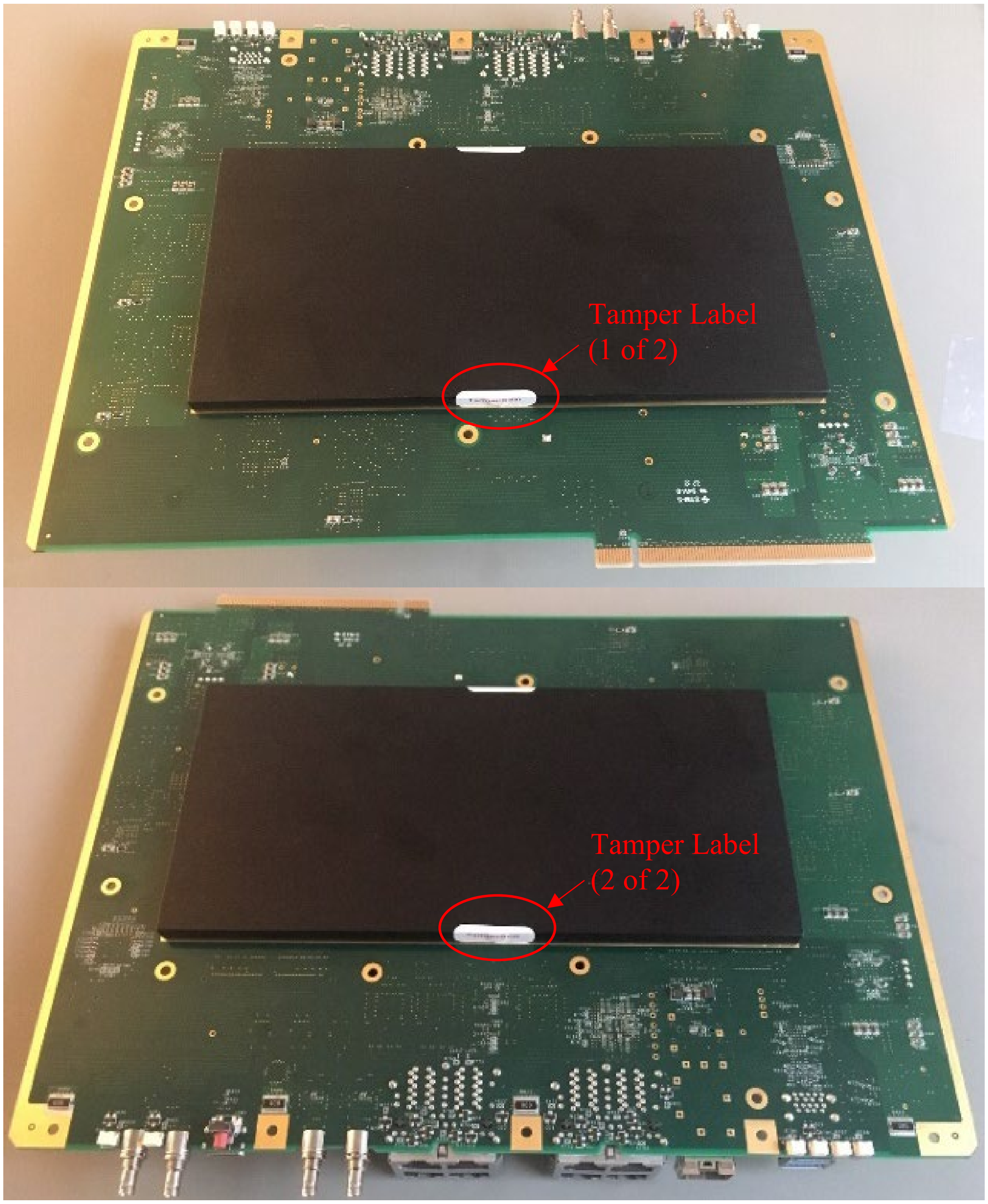


Figure 3 – Placement of the Two Tamper Labels

10.2. Operator Required Actions

The operator is required to periodically inspect the module for evidence of tampering.

Table 13 – Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper evidence	Monthly	Ensure the module does not display any characteristics of an attempted breach. If there is any evidence of an attempted breach, module is to be returned to factory.

11. Mitigation of Other Attacks Policy

The module has not been designed to mitigate attacks beyond the scope of FIPS 140-2 requirements.

Table 14 – Mitigation of Other Attacks

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

12. Definitions and Acronyms

AES	Advanced Encryption Standard
AES-Audio	Audio Engineering Society Audio
ANSI	American National Standards Institute
CO	Cryptographic Officer
CSP	Critical Security Parameter
DCI	Digital Cinema Initiative
DRNG	Deterministic Random Number Generator
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standard
FPGA	Field Programmable Gate Array
HMAC	Hash Message Authentication Code
KAT	Known Answer Test
N/A	Not Applicable
NDRNG	Non-Deterministic Random Number Generator
PCI-E	Peripheral Component Interconnect Express
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SM	Security Manager
SMS	Screen Management System
SPB	Secure Processing Block