

FIPS 140-2 Non-Proprietary Security Policy

AQ42-M

Document Version 1.3.0

Digicine Oristar Technology Development (Beijing) Co., Ltd.

Table of Contents

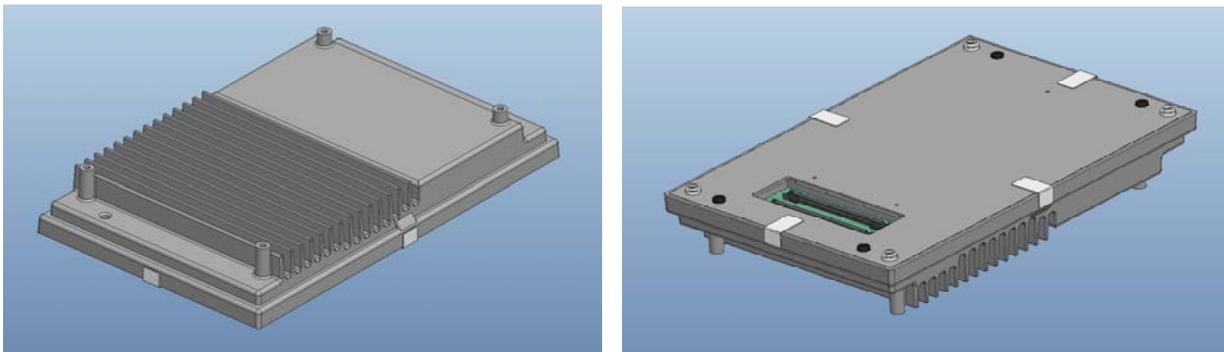
| | |
|---|-----------|
| Table of Contents | 2 |
| 1. Module Overview | 3 |
| 2. Security Level | 5 |
| 3. Modes of Operation..... | 6 |
| 3.1. Approved Mode of Operation | 6 |
| 3.2. Non-Approved Mode of Operation | 7 |
| 4. Ports and Interfaces | 8 |
| 5. Identification and Authentication Policy | 9 |
| 5.1. Assumption of Roles | 9 |
| 5.2. Authentication Mechanism | 9 |
| 6. Access Control Policy..... | 10 |
| 6.1. Roles and Services | 10 |
| 6.2. Definition of Critical Security Parameters (CSPs)..... | 13 |
| 6.3. Definition of Public Keys..... | 13 |
| 6.4. Definition of CSP Access Modes..... | 14 |
| 7. Operational Environment..... | 18 |
| 8. Security Rules..... | 19 |
| 9. Physical Security Policy | 21 |
| 9.1. Physical Security Mechanisms..... | 21 |
| 9.2. Operator Actions..... | 21 |
| 10. Policy on Mitigation of Other Attacks..... | 23 |
| 11. Definitions and Acronyms | 24 |
| 12. Revision History | 26 |

1. Module Overview

The AQ42-M cryptographic module is a multi-chip embedded cryptographic module encased in a hard opaque commercial grade metal case. The cryptographic boundary is defined as the entire metal case perimeter, including all hardware and firmware encapsulated within. The interfaces are all traces that cross the cryptographic boundary.

The primary purpose of the AQ42-M is to provide decryption, decoding/encoding of audio/video data for the digital cinema projector system in which it is used.

The illustration below shows the AQ42-M, along with the cryptographic boundary.



Top Side

Bottom Side

Figure 1 - Image of the AQ42-M Cryptographic Module

This document is written about the following validated hardware / firmware version of AQ42-M:

- Hardware version: 2.0.0
- Firmware version: 1.3.0

AQ42-M firmware configuration table is as follows.

This document may be reproduced and distributed whole and intact including this copyright notice.

Table 1 - AQ42-M Firmware Configuration

| Component | Firmware Component Version |
|----------------------------|-----------------------------------|
| | Firmware 1.3.0 |
| MDC version | 01.30.00 |
| NSA version | 01.21.00 |
| CDM version | 01.30.00 |
| Kernel version | 02.06.33 |
| MBA version | 01.30.00 |
| CTU version | 04.01.01 |
| DSP version | 01.00.09 |
| Boot Loader version | 01.00.00 |

2. Security Level

The AQ42-M meets the overall requirements applicable to Level 2 security of FIPS 140-2.

Table 2 - Module Security Level Specification

| Security Requirements Section | Level |
|---|--------------|
| Cryptographic Module Specification | 3 |
| 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 | 3 |
| Mitigation of Other Attacks | N/A |

3. Modes of Operation

3.1. Approved Mode of Operation

The AQ42-M is designed to continually operate in a FIPS approved mode of operation. The AQ42-M supports the following FIPS approved cryptographic algorithms:

- AES with 128-bit key (as per FIPS 197)
 - CBC and ECB mode of operation - Certificates: #2932, #2934
 - CBC mode of operation (Decrypt only) - Certificate: #2933
- SHA-1 with 160-bit hash value (as per FIPS 180-3) - Certificates: #2469, #2470, #2468
- SHA-256 with 256-bit hash value (as per FIPS 180-3) - Certificates: #2469, #2470, #2471
- HMAC-SHA-1 with 160-bit MAC value (as per FIPS 198) - Certificates: #1858, #1859
- RSA Signature Generation with 2,048-bit key using SHA-256 (as per FIPS 186-4) - Certificates: #1537, #1538
- RSA Signature Verification with 2,048-bit key using SHA-1 (as per FIPS 186-2) - Certificate: #1538
- RSA Signature Verification with 2,048-bit key using SHA-256 (as per FIPS 186-2) - Certificates: #1537, #1538
- ANSI X9.31 RNG using AES (as per ANSI X9.31) - Certificates: #1294, #1295
- FIPS 186-2 RNG using SHA-1 (as per FIPS 186-2) - Certificate: #1293
- SP 800-135rev1 TLS KDF using SHA-1 (as per SP 800-135rev1) - Certificate: #333

In addition to the above algorithms the AQ42-M employs the following Allowed non-FIPS approved cryptographic algorithms for use in the FIPS approved mode of operation.

- RSA Encryption/Decryption only for key encapsulation. (Key establishment methodology provides 112-bit of encryption strength)

This document may be reproduced and distributed whole and intact including this copyright notice.

- NDRNG for the seeding of the ANSI X9.31 RNGs
- HMAC-MD5 for the pseudo random function in TLS
- MD5 for the pseudo random function in TLS
- RSA Signature Generation/Verification with 2,048-bit key using both MD5 and SHA-1 only for TLS 1.0 client authentication

The operator can be assured that the AQ42-M is in the approved mode by verifying that the firmware versions identified using the 'Get Version' service match each of the validated firmware component versions listed in Section 1.

3.2. Non-Approved Mode of Operation

The AQ42-M does not support a non-FIPS Approved mode of operation.

4. Ports and Interfaces

The physical interfaces for AQ42-M are the traces that cross the perimeter of the physical cryptographic boundary. The traces are used to support TLS with the following logical interfaces required by FIPS 140-2:

- Data Input
- Data Output
- Status Output
- Control Input

In addition, the AQ42-M receives power from an outside source and thus supports a power input interface.

- Power Input

5. Identification and Authentication Policy

5.1. Assumption of Roles

The AQ42-M supports two distinct operator roles (User and Crypto-Officer). The AQ42-M enforces the separation of roles using identity-based operator authentication. The Crypto-Officer and User are authenticated using the RSA 2048 signature verification algorithm.

Table 3 - Roles and Required Identification and Authentication

| Role | Type of Authentication | Authentication Data |
|----------------|--|-------------------------|
| User | Identity-based operator authentication | RSA Digital Certificate |
| Crypto-Officer | Identity-based operator authentication | RSA Digital Certificate |

5.2. Authentication Mechanism

The AQ42-M supports an authentication mechanism.

Table 4 - Strengths of Authentication Mechanisms

| Authentication Mechanism | Strength of Mechanism |
|--------------------------------------|---|
| RSA Digital Certificate Verification | <p>The authentication is based on RSA 2,048, which has an equivalent strength of 112-bit. Therefore, the probability with which a random attempt will succeed or a false acceptance will occur is 2^{-112} which is less than 1/1,000,000.</p> <p>There is a 10msec delay after each trial which limits the number of attempts per minute. The probability of a random attempt successfully authenticating to the AQ42-M within one minute is also $6000 * 2^{-112}$ ($< 2^{10} * 2^{-112} = 2^{-102}$) which is less than 1/100,000.</p> |

6. Access Control Policy

6.1. Roles and Services

Table 5 - Crypto-Officer Specific Services

| Service | Description |
|-----------------------|---|
| Clear Log | Deletes all logs required by Digital Cinema Initiative (DCI) specification. |
| Update Start Sequence | Checks a certificate and prepares for firmware update. |
| Update Module | Receives a firmware image from the operator and perform firmware updating. |
| Update End Sequence | Ends a firmware update procedure. |
| Zeroization | Deletes all plaintext CSP. |

* Note: If a non-FIPS validated firmware version is loaded onto the AQ42-M, then the AQ42-M is no longer an FIPS validated module.

Table 6 - Crypto-Officer and User Common Services

| Service | Description |
|---------------------|--|
| Delete KDM | Deletes Key Delivery Message (KDM) specified with Compositions Play list (CPL) ID. |
| Delete KDM ID | Deletes KDM specified with KDM ID. |
| Detail KDM ID | Outputs detailed information of KDM specified with KDM ID. |
| Get Audio Frequency | Outputs the audio frequency. |
| Get Audio Muting | Outputs audio mute information. |
| Get Audio Routing | Outputs the audio routing switch information. |
| Get Certificate | Outputs information of certificates that the module has. |
| Get CPL List ID | Outputs CPL playing information buffer ID of the module. |
| Get Date | Outputs the time and date. |
| Get Delay | Outputs the audio delay value. |
| Get FM ID | Outputs the forensic mark ID. |

| Service | Description |
|----------------------------|--|
| Get Marriage Status | Outputs the current connection status with an external device. |
| Get MS Configuration | Outputs the Master/Slave mode of the module. |
| Get Playback Information | Outputs the current CPL playback status. |
| Get Root Certificate | Outputs information of root certificates. |
| Get Security Status | Outputs the current protection status of the module. |
| Get Status | Outputs information of various statuses. |
| Get Time-zone | Outputs set time-zone information. |
| Get Version | Outputs version information of the module. |
| Get White Point | Outputs the mode of the white point. |
| Heartbeat | Keeps the current session with an operator. |
| Initialize Marriage | Initializes the connection status with an external device. |
| Initialize PCIE Connection | Sends a signal to an external device to reset its own status. |
| List KDM ID | Outputs an ID list of stored KDM and keys. |
| List Root Cert | Outputs a file name list of stored root certificates. |
| List Security Log | Outputs a file name list of stored security logs. |
| Play Pause Execution | Pauses playback of the current content. |
| Play Pause Resume | Resumes playback of the paused content. |
| Play Prepare Completed | Checks the current playback preparation status of an operator. |
| Play Prepare CPL | Prepares playback of CPL. |
| Play Set SPL | Reads the construction of Show Play List (SPL). |
| Play Step | Plays the paused content frame by frame. |
| Play Stop | Stops playback of the current content. |
| Relate KDM ID | Outputs an ID list of KDM specified with CPL ID. |
| Retrieve Certificate | Outputs stored certificates. |
| Retrieve Root Cert | Outputs stored root certificates. |
| Retrieve Security Log | Outputs stored logs required by DCI specification. |

This document may be reproduced and distributed whole and intact including this copyright notice.

| Service | Description |
|-------------------------|---|
| Retrieve Security Log 2 | Output stored logs in the form of XML file. |
| Set AMB IP | Sets the IP address of Audio Media Block. |
| Set Audio Frequency | Sets the audio frequency. |
| Set Audio Muting | Sets the audio muting switch. |
| Set Audio Routing | Sets the audio routing switch. |
| Set Date | Sets a time of the module. |
| Set Date 2 | Sets a time of the module. |
| Set Delay | Sets the audio delay value. |
| Set MS Configuration | Switches the Master/Slave mode of the module. |
| Set Timed Text Key ID | Sets ID of key used for decrypting encrypted Material eXchange Format (MXF) file. |
| Set Time-zone | Sets time-zone. |
| Set White Point | Sets the mode of the white point. |
| Shutdown | Shuts down or reboots the module. |
| Snapshot | Outputs logs in the form of ZIP format. |
| Store KDM | Stores KDM given by an operator. |
| Verify CPL | Checks whether the specified CPL is playable. |
| Version | Checks the version of an operator interface. |

Table 7 - Unauthenticated Services

| Service | Description |
|----------------|-------------------------------|
| Show Status | Outputs the module status. |
| Self-tests | Performs power-up self-tests. |

6.2. Definition of Critical Security Parameters (CSPs)

The following CSPs are included in the AQ42-M.

- Contents Encryption Key (CEK) - AES key used to decrypt contents.
- Content Integrity Key (CIK) - HMAC-SHA-1 key for integrity check of contents.
- Aux Data Key (ADK) - AES key used to protect all stored CSPs.
- Master Key (MK) - AES key used to protect all stored CSPs.
- TLS Session Key (TSK) - The AES key established in TLS.
- TLS MAC Secret (TMACS) - The HMAC key established in TLS.
- RSA Signing Key (RSK) - RSA private key used for generation of a digital signature for the log data and TLS session data.
- Device Private Key (DPK) - RSA private key used for decryption of CEK and decryption of wrapped cryptographic keys which are entered into the AQ42-M in TLS.
- TLS Premaster Secret (TPS) - The parameter used for key establishment in TLS.
- TLS Master Secret (TMS) - The parameter used for key establishment in TLS.
- PRF State (PS) - The internal state used for key establishment in TLS.
- Seed and Seed Key (SSK) - The secret values necessary for the FIPS approved RNGs.

6.3. Definition of Public Keys

The following are the public keys contained in the AQ42-M:

- AQ42-M Manufacturer Public Key - RSASSA 2048 public key used to verify a certificate chain of trust.
- AQ42-M Trusted Public Key - RSASSA 2048 public key used to verify a certificate chain of trust.
- RSA Verifying Key - RSASSA 2048 public key corresponding to the RSA Signing Key.

This document may be reproduced and distributed whole and intact including this copyright notice.

- Device Public Key - RSAES 2048 public key corresponding to the Device Private Key.
- Public Key for F/W Upgrade - RSASSA 2048 public key used to verify the digital signature over the firmware image to be upgraded.
- Operator Public Key - RSASSA 2048 public key used to authenticate operators.
- Projector Public Key - RSAES 2048 public key used to authenticate an external device.
- Aux Data Processor Public Key - RSAES 2048 public key used to authenticate an Aux Data Processor.
- KDM Issuer Public Key - RSASSA 2048 public key used to verify signature of KDM.

6.4. Definition of CSP Access Modes

Table 8 defines the relationship between CSP access modes and module services. The access modes shown in Table 8 are defined as follows:

- **Generate (G):** Generates the Critical Security Parameter (CSP) using an approved Random Number Generator (RNG).
- **Use (U):** Uses the CSP to perform cryptographic operations within its corresponding algorithm.
- **Entry (E):** Enters the CSP into the AQ42-M.
- **Output (O):** Outputs the CSP from the AQ42-M.
- **Zeroize (Z):** Removes the CSP.

Table 8 - CSP Access Rights within Roles & Services

| Role | | Service Name | CSP (<i>Access Mode</i>) |
|------|------|---------------------|----------------------------|
| C.O. | User | | |
| X | | Clear Log | TSK(U), TMACS(U) |
| X | | Update End Sequence | TSK(U), TMACS(U) |
| X | | Update Module | TSK(U), TMACS(U) |

This document may be reproduced and distributed whole and intact including this copyright notice.

| Role | | Service Name | CSP (Access Mode) |
|------|------|--------------------------|--|
| C.O. | User | | |
| X | | Update Start Sequence | TSK(U), TMACS(U) |
| X | | Zeroization | CEK(Z), CIK(Z), ADK(Z), MK(Z), RSK(Z), DPK(Z), TSK(UZ), TMACS(UZ), TPS(Z), TMS(Z), PS(Z), SSK(Z) |
| X | X | Delete KDM | CEK(Z), CIK(Z), ADK(Z), TSK(U), TMACS(U) |
| X | X | Delete KDM ID | CEK(Z), CIK(Z), ADK(Z), TSK(U), TMACS(U) |
| X | X | Detail KDM ID | TSK(U), TMACS(U) |
| X | X | Get Audio Frequency | TSK(U), TMACS(U) |
| X | X | Get Audio Muting | TSK(U), TMACS(U) |
| X | X | Get Audio Routing | TSK(U), TMACS(U) |
| X | X | Get Certificate | TSK(U), TMACS(U) |
| X | X | Get CPL List ID | TSK(U), TMACS(U) |
| X | X | Get Date | TSK(U), TMACS(U) |
| X | X | Get Delay | TSK(U), TMACS(U) |
| X | X | Get FM ID | TSK(U), TMACS(U) |
| X | X | Get Marriage Status | TSK(U), TMACS(U) |
| X | X | Get MS Configuration | TSK(U), TMACS(U) |
| X | X | Get Playback Information | TSK(U), TMACS(U) |
| X | X | Get Root Certificate | TSK(U), TMACS(U) |
| X | X | Get Security Status | TSK(U), TMACS(U) |
| X | X | Get Status | TSK(U), TMACS(U) |
| X | X | Get Time-zone | TSK(U), TMACS(U) |
| X | X | Get Version | TSK(U), TMACS(U) |
| X | X | Get White Point | TSK(U), TMACS(U) |
| X | X | Heartbeat | TSK(U), TMACS(U) |

| Role | | Service Name | CSP (Access Mode) |
|------|------|----------------------------|---|
| C.O. | User | | |
| X | X | Initialize Marriage | RSK(U), TSK(GU), TMACS(GU), TPS(GOU), TMS(GU), PS(GU), SSK(U) |
| X | X | Initialize PCIE Connection | TSK(U), TMACS(U) |
| X | X | List KDM ID | TSK(U), TMACS(U) |
| X | X | List Root Certificate | TSK(U), TMACS(U) |
| X | X | List Security Log | RSK(U), TSK(U), TMACS(U) |
| X | X | Play Pause Execution | TSK(U), TMACS(U) |
| X | X | Play Pause Resume | TSK(U), TMACS(U) |
| X | X | Play Prepare Completed | CEK(U), CIK(U), TSK(U), TMACS(U) |
| X | X | Play Prepare CPL | TSK(U), TMACS(U), ADK(O) |
| X | X | Play Set SPL | TSK(U), TMACS(U) |
| X | X | Play Step | TSK(U), TMACS(U) |
| X | X | Play Stop | TSK(U), TMACS(U) |
| X | X | Relate KDM ID | TSK(U), TMACS(U) |
| X | X | Retrieve Certificate | TSK(U), TMACS(U) |
| X | X | Retrieve Root Certificate | TSK(U), TMACS(U) |
| X | X | Retrieve Security Log | TSK(U), TMACS(U) |
| X | X | Retrieve Security Log 2 | RSK(U), TSK(U), TMACS(U) |
| X | X | Set AMB IP | RSK(U), TSK(GU), TMACS(GU), TPS(GOU), TMS(GU), PS(GU), SSK(U) |
| X | X | Set Audio Frequency | TSK(U), TMACS(U) |
| X | X | Set Audio Muting | TSK(U), TMACS(U) |
| X | X | Set Audio Routing | TSK(U), TMACS(U) |
| X | X | Set Date | TSK(U), TMACS(U) |
| X | X | Set Date 2 | TSK(U), TMACS(U) |

| Role | | Service Name | CSP (<i>Access Mode</i>) |
|------|------|-----------------------|---|
| C.O. | User | | |
| X | X | Set Delay | TSK(U), TMACS(U) |
| X | X | Set MS Configuration | TSK(U), TMACS(U) |
| X | X | Set Timed Text Key ID | TSK(U), TMACS(U) |
| X | X | Set Time-zone | TSK(U), TMACS(U) |
| X | X | Set White Point | TSK(U), TMACS(U) |
| X | X | Shutdown | TSK(U), TMACS(U) |
| X | X | Snapshot | TSK(U), TMACS(U) |
| X | X | Store KDM | CEK(UE), CIK(G), ADK(UE), MK(U), SPK(U), TSK(U), TMACS(U), SSK(U) |
| X | X | Verify CPL | TSK(U), TMACS(U) |
| X | X | Version | TSK(U), TMACS(U) |
| Any | Any | Show Status | - |
| Any | Any | Self-Test | - |

* TPS, TMS, and PS are entered or generated, used and zeroized in TLS establishment.

7. Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements are not applicable because the AQ42-M does not contain a modifiable operational environment.

8. Security Rules

The AQ42-M cryptographic module was designed with the following security rules in mind. These rules are comprised of both those specified by FIPS 140-2 and those derived from Digicine Oristar Technology Development (Beijing) Co., Ltd.'s company policy.

1. The AQ42-M shall provide two distinct operator roles. These are the User role, and the Crypto-Officer role.
2. The AQ42-M shall provide identity-based authentication.
3. When the AQ42-M has not been placed in an authenticated role, the operator shall not have access to any cryptographic services.
4. The AQ42-M shall perform the following tests:
 - i. Power-up Self-Tests:
 - a. Cryptographic algorithm tests (for each implementation):
 - AES 128 CBC Encryption/Decryption Known-Answer Tests
 - AES 128 ECB Encryption/Decryption Known-Answer Test
 - ANSI X9.31 RNG Known-Answer Test
 - FIPS 186-2 RNG Known-Answer Test
 - SHA-1 Known-Answer Test
 - SHA-256 Known-Answer Test
 - HMAC-SHA-1 Known-Answer Test
 - RSA PKCS#1 v1.5 Signature Generation/Verification Known-Answer Test
 - SP 800-135rev1 TLS KDF Known-Answer Test
 - b. Firmware Integrity Test (CRC-16 and CRC-32)
 - c. Critical Functions Test:
 - HMAC-MD5 Known-Answer Test
 - RSA OAEP Pair-wise Consistency Test (Encryption/Decryption)

This document may be reproduced and distributed whole and intact including this copyright notice.

- RSA PKCS#1 v1.5 Pair-wise Consistency Test (Encryption/Decryption)
- ii. Conditional Self-Tests:
 - a. Continuous (RNG) Tests (ANSI X9.31 RNGs, FIPS 186-2 RNG, NDRNG)
 - b. Firmware Load Test (RSA Digital Signature Verification)
- 5. The operator shall be capable of commanding the AQ42-M to perform the power-up self-test using recycling power.
- 6. Data output shall be inhibited during self-tests, zeroization, and error states.
- 7. Data output shall be logically disconnected from key generation processes.
- 8. Status information shall not contain CSPs or sensitive data that if misused could lead to a compromise of the AQ42-M.
- 9. The AQ42-M does not support concurrent operators.
- 10. The AQ42-M shall not support a bypass capability or a maintenance interface.
- 11. If a non-FIPS validated firmware version is loaded onto the AQ42-M, then the AQ42-M ceases to be a FIPS validated module.
- 12. HMAC-MD5 is only used as the pseudo random function in TLS.
- 13. RSA Signature Generation/Verification using both MD5 and SHA-1 is only used for TLS 1.0 client authentication.
- 14. The AQ42-M only supports the electronic entry form of key establishment.
- 15. RSA Signing Key is used for TLS establishment when the AQ42-M behaves as a TLS client in communication with an external device.
- 16. Device Private Key is used for TLS establishment when the AQ42-M behaves as a TLS server in communication with an external device.

9. Physical Security Policy

9.1. Physical Security Mechanisms

The AQ42-M is a multi-chip embedded cryptographic module with the following physical security mechanisms:

- Production-grade components,
- The enclosure of AQ42-M has a removable cover that four tamper evidence seals (See Figure 2 and Figure 3) are sealed by Digicine Oristar Technology Development (Beijing) Co., Ltd. in secure manufacturing facility. When the cover is removed or the power supply from the outside is lost, all plaintext CSPs within the AQ42-M are zeroized,
- The enclosure is opaque and provides tamper evidence.

The enclosure is sufficiently hard, providing tamper detection and response in accordance with FIPS 140-2 level 3 physical security requirements. Hardness testing was performed at ambient temperature.



Figure 2 – Image of Tamper Evidence Seal

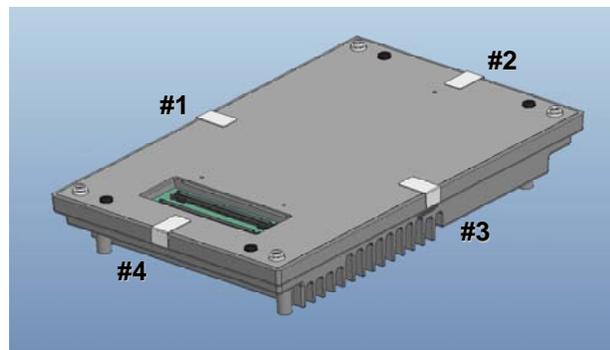


Figure 3 – Seal Location

9.2. Operator Actions

Due to the intended deployment environment for the AQ42-M, Digicine Oristar Technology Development (Beijing) Co., Ltd. defers the physical inspection criteria to the end user of the cryptographic module. Any such inspection shall be based on the customer security policy, in particular with regards to the inspection frequency.

This document may be reproduced and distributed whole and intact including this copyright notice.

Table 9 - Inspection/Testing of Physical Security Mechanisms

| Physical Security Mechanisms | Recommended Frequency of Inspection/Test | Inspection/Test Guidance Details |
|-------------------------------------|---|---|
| Hard Removable Enclosure | Every startup and reboot. | Inspect for scratches or deformation of the metal case. If such evidence is found, user should not use the module. |
| Tamper Evidence Seals | Every startup and reboot. | Inspect for curled corner, peel, rips, or appearance of words “WARRANTY VOID IF REMOVED”. If found such evidences, user should not use the module. |
| Tamper detection | Every startup and reboot. | If the module was zeroized, user should return it to Digicine Oristar Technology Development (Beijing) Co., Ltd.. |

10. Policy on Mitigation of Other Attacks

The AQ42-M was not designed to mitigate other attacks outside of the specific scope of FIPS 140-2. Therefore, this section is not applicable.

Table 10 - Mitigation of Other Attacks

| Other Attack | Mitigation Mechanism | Specific Limitations |
|--------------|----------------------|----------------------|
| N/A | N/A | N/A |

11. Definitions and Acronyms

Table 11 -Definitions and Acronyms

| Term | Definition |
|-------------|--|
| AES | Advanced Encryption Standard |
| CDM | Contents Decryption and Decode Module |
| CPL | Compositions Playlists |
| CRC | Cyclic Redundancy Code |
| CSP | Critical Security Parameter |
| CTU | Counter Tampering & Tamper Detection Unit |
| DCI | Digital Cinema Initiative |
| DCP | Digital Cinema Package |
| DRNG | Deterministic RNG |
| DSP | Digital Signal Processor |
| EMI / EMC | Electromagnetic Interference / Electromagnetic Compatibility |
| HMAC | Hash-based Message Authentication Code |
| KDF | Key Derivation Function |
| KDM | Key Delivery Message |
| MBA | Media Block Application |
| MDC | Media Decrypt & Decode Controller |
| NSA | Nios & Audio Mapping |
| OAEP | Optimal Asymmetric Encryption Padding |
| PAD | FPGA that processes video and audio data |
| PKCS | Public Key Cryptography Standards |
| PRF | Pseudo Random Function |
| RNG | Random Number Generator |
| RSA | Rivest-Shamir-Adleman |

This document may be reproduced and distributed whole and intact including this copyright notice.

| Term | Definition |
|-------------|---|
| RSA ES/SSA | RSA Encryption Standard / Secure Signature Algorithm |
| RTC | Real Time Clock |
| SHA | Secure Hash Algorithm |
| SPL | Show Play List |
| TLS | Transport Layer Security |

