Classification: External

quadient

# Quadient Technologies France

Quadient Postal Security Device

# FIPS 140-3 Non-Proprietary Security Policy

Version No.: V 1.0
Version Date: 07/14/2026

quadient
Because connections matter.

## TABLE OF CONTENTS

## LIST OF TABLES



## LIST OF FIGURES

# 1. General

## 1.1. Overview

This document describes the security policy of the Quadient Technologies France (Quadient) Postal Security Device (PSD) under the terms of FIPS 140-3 validation. This document contains a statement of the security rules under which the Quadient Postal Security Device operates.

## 1.2. Security Levels

The Quadient Postal Security Device is designed to meet the overall requirements applicable for FIPS 140-3 Security Level 3.

| Section | Title | Security Level |
|---|---|---|
| 1 | General | 3 |
| 2 | Cryptographic module specification | 3 |
| 3 | Cryptographic module interfaces | 3 |
| 4 | Roles, services, and authentication | 3 |
| 5 | Software/Firmware security | 3 |
| 6 | Operational environment | N/A |
| 7 | Physical security | 3 |
| 8 | Non-invasive security | N/A |
| 9 | Sensitive security parameter management | 3 |
| 10 | Self-tests | 3 |
| 11 | Life-cycle assurance | 3 |
| 12 | Mitigation of other attacks | 3 |
| | Overall Level | 3 |

**Table 1: Security Levels**

# 2. Cryptographic Module Specification

## 2.1. Description

**Purpose and Use:**
The Quadient Postal Security Device is a hardware cryptographic module embedded within the postal franking machines. The Quadient Postal Security Device performs all the franking machine's cryptographic and postal security functions and protects the Critical Security Parameters (CSPs) and Postal Relevant Data from unauthorized access.

**Module Type**: Hardware

**Module Embodiment**: Multi-Chip Standalone

**Module Characteristics**:
The module is enclosed within a hard, opaque, plastic enclosure encapsulating the epoxy potted module which is wrapped in a tamper detection envelope with a tamper response mechanism. This enclosure constitutes the cryptographic module's physical boundary.

**Cryptographic Boundary:**
The module's Cryptographic Boundary is defined at the module's physical perimeter (Figure 1).


Figure 1: Cryptographic Boundary

## 2.2. Tested and Vendor Affirmed Module Version and Identification

**Tested Module Identification – Hardware:**

| Model and/or Part Number | Hardware Version | Firmware Version | Processors | Features |
|---|---|---|---|---|
| Quadient Postal Security Device | P/N: A0150156B | a40_08, P/N: A0167558A | NXP MIMXRT1051, ARM-Cortex M7 | N/A |

Table 2: Tested Module Identification – Hardware

**Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):**

N/A for this module.

**Tested Module Identification – Hybrid Disjoint Hardware:**

N/A for this module.

**Tested Operational Environments - Software, Firmware, Hybrid:**

N/A for this module.

**Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:**

N/A for this module.

## 2.3. Excluded Components

The module does not exclude any components from the requirements of FIPS 140-3.

## 2.4. Modes of Operation

**Modes List and Description:**

| Mode Name | Description | Type | Status Indicator |
|---|---|---|---|
| Approved Mode | For country configurations where only approved algorithms are used. | Approved | FIPS_APPROVED_MODE = 1 |
| Non-Approved Mode | For country configurations where non-approved algorithms are requested by their respective postal specifications. | Non-Approved | FIPS_APPROVED_MODE = 0 |

Table 3: Modes List and Description

The module supports two modes of operation: Approved and Non-Approved.
When initialized (in manufacturing) for countries that utilize only Approved security functions, the module is said to be in an Approved mode of operation.
The module returns an explicit indicator (FIPS_APPROVED_MODE) showing whether the module is in an Approved mode or non-Approved mode via the Show Status service (Read Status).
To change modes of operation, the module must be initialized for a specific country in manufacturing.
The mode of operation cannot be changed outside of manufacturing. Therefore, it is impossible to share CSPs between modes of operation.

The module does not support a degraded mode of operation.

## 2.5. Algorithms

**Approved Algorithms:**

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| AES-CBC | A5237 | Direction - Decrypt, Encrypt<br>Key Length - 128 | SP 800-38A |
| AES-CMAC | A5238 | Direction - Generation<br>Key Length - 128 | SP 800-38B |
| AES-GCM | A5267 | Direction - Decrypt, Encrypt<br>IV Generation - Internal<br>IV Generation Mode - 8.2.2<br>Key Length - 128 | SP 800-38D |
| Conditioning Component Block Cipher Derivation Function SP800-90B | A3803 | Key Length - 128 | SP 800-90B |
| Counter DRBG | A5239 | Prediction Resistance - No<br>Mode - AES-128<br>Derivation Function Enabled - Yes | SP 800-90A Rev. 1 |
| DSA KeyGen (FIPS186-4) | A5240 | L - 2048<br>N - 224 | FIPS 186-4 |
| ECDSA KeyGen (FIPS186-5) | A5243 | Curve - P-224, P-256<br>Secret Generation Mode - extra bits | FIPS 186-5 |
| ECDSA SigGen (FIPS186-5) | A5243 | Curve - P-224, P-256<br>Hash Algorithm - SHA2-256<br>Component - No | FIPS 186-5 |
| ECDSA SigVer (FIPS186-5) | A5243 | Curve - P-224, P-256<br>Hash Algorithm - SHA2-256 | FIPS 186-5 |
| HMAC-SHA-1 | A5241 | Key Length - Key Length: 160 | FIPS 198-1 |
| HMAC-SHA2-256 | A5241 | Key Length - Key Length: 256 | FIPS 198-1 |
| KAS-FFC-SSC Sp800-56Ar3 | A5268 | Domain Parameter Generation Methods - FB, ffdhe2048<br>Scheme -<br>dhEphem -<br>KAS Role - responder | SP 800-56A Rev. 3 |
| KDA HKDF SP800-56Cr2 | A5270 | Derived Key Length - 1024<br>Shared Secret Length - Shared Secret Length: 2048<br>HMAC Algorithm - SHA2-256 | SP 800-56C Rev. 2 |
| KDF TLS (CVL) | A5269 | TLS Version - v1.2<br>Hash Algorithm - SHA2-256 | SP 800-135 Rev. 1 |
| RSA KeyGen (FIPS186-5) | A5271 | Key Generation Mode - probable<br>Modulo - 2048 | FIPS 186-5 |

| Algorithm | CAVP Cert | Properties | Reference |
|---|---|---|---|
| | | Primality Tests - 2pow100<br>Private Key Format - standard | |
| RSA SigGen (FIPS186-5) | A5271 | Modulo - 2048<br>Signature Type - pkcs1v1.5, pss | FIPS 186-5 |
| RSA SigVer (FIPS186-5) | A5271 | Modulo - 2048<br>Signature Type - pkcs1v1.5, pss | FIPS 186-5 |
| SHA-1 | A5242 | Message Length - Message Length: 0-65536 Increment 8 | FIPS 180-4 |
| SHA2-256 | A5242 | Message Length - Message Length: 0-65536 Increment 8 | FIPS 180-4 |

Table 4: Approved Algorithms

**Vendor-Affirmed Algorithms:**

| Name | Properties | Implementation | Reference |
|---|---|---|---|
| CKG | Key Type:Symmetric and Asymmetric | N/A | NIST SP 800-133r2 Section 4 Example 1, Section 5.1, and Section 5.2. |

Table 5: Vendor-Affirmed Algorithms

**Non-Approved, Allowed Algorithms:**

N/A for this module.

**Non-Approved, Allowed Algorithms with No Security Claimed:**

N/A for this module.

**Non-Approved, Not Allowed Algorithms:**

| Name | Use and Function |
|---|---|
| ECDSA (P-192) | Key Generation/Signature Generation (Canadian Configuration) |
| RSA (1024) | Key Generation/Key Wrapping (German Configuration) |

Table 6: Non-Approved, Not Allowed Algorithms

## 2.6. Security Function Implementations

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| BC-Auth | BC-Auth | Authenticated encryption/decryption | Standard:FIPS 197, NIST SP 800-38A | AES-GCM: (A5267) Direction: Encrypt, |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | Decrypt<br>IV Generation: Internal<br>IV Generation Mode: 8.2.2<br>Key Length: 128 |
| BC-UnAuth | BC-UnAuth | Symmetric encryption/decryption | Standard:FIPS 197, NIST SP 800-38A | AES-CBC: (A5237)<br>Direction: Encrypt, Decrypt<br>Key Length: 128 |
| CKG | CKG | Symmetric key generation | Standard:NIST SP 800-133rev2 | CKG: ()<br>Key Type: Symmetric |
| DRBG | DRBG | Random bit generation | Standard:SP 800-90A | Counter DRBG: (A5239)<br>Prediction Resistance: No<br>Mode: AES-128<br>Derivation Function Enabled: Yes<br>Entropy Input: 384 bits<br>Additional Input: 128 bits<br>Nonce: 64 bits<br>Personalization String: 64 bits<br>Returned Bits: 512 bits |
| ESV | ENT-ESV | Physical Entropy Source | Standard:NIST SP 800-90B | Conditioning Component Block Cipher Derivation Function SP800-90B: (A3803)<br>Key Length: 128<br>Payload Length: 256 |
| KAS1.2 | KAS-Full | Key agreement scheme per IG D.F Scenario 2 path (2) using KDF TLS. Used in TLS 1.2 handshake protocol. | Standard:NIST SP 800-56Ar3<br>IG:IG D.F Scenario 2, path (2), split Key confirmation:No Key derivation:IG 2.4.B SP 800-135rev1 CVL Caveat:Key establishment | KAS-FFC-SSC Sp800-56Ar3: (A5268)<br>Domain Parameter Generation Methods: FB, ffdhe2048<br>KAS Role: responder<br>KDF TLS: (A5269)<br>TLS Version: v1.2 |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | methodology provides 112 bits of security strength | Hash Algorithm: SHA2-256 |
| KAS1.3 | KAS-Full | Key agreement scheme per IG D.F Scenario 2 path (2) using KDA HKDF. Used in TLS 1.3 handshake protocol. | Standard:NIST SP 800-56Ar3<br>IG:IG D.F Scenario 2, path (2), split<br>Key confirmation:No<br>Key derivation:KDA (separately tested)<br>Caveat:Key establishment methodology provides 112 bits of security strength | KDA HKDF SP800-56Cr2: (A5270)<br>Derived Key Length: 1024<br>Shared Secret Length: 2048<br>HMAC Algorithm: SHA2-256<br>KAS-FFC-SSC Sp800-56Ar3: (A5268)<br>Parameter Generation Methods: FB, ffdhe2048<br>KAS Role: responder |
| KTS1.2 | KTS-Unwrap<br>KTS-Wrap | Key wrapping and unwrapping per IG D.G | Standard:NIST SP 800-38F<br>IG:Approved method from IG D.G<br>Caveat:Key establishment methodology provides 112 bits of security strength | AES-CBC: (A5237)<br>Direction: Encrypt, Decrypt<br>Key Length: 128<br>HMAC-SHA2-256: (A5241)<br>Key Length: 256 |
| KTS1.3 | KTS-Unwrap<br>KTS-Wrap | Key wrapping and unwrapping per IG D.G | Standard:NIST SP 800-38F<br>IG:Approved method from IG D.G<br>Caveat:Key establishment methodology provides 112 bits of security strength | AES-GCM: (A5267)<br>Direction: Encrypt, Decrypt<br>IV Generation: Internal<br>IV Generation Mode: 8.2.2<br>Key Length: 128 |
| KeyGen | AsymKeyPair-KeyGen | Asymmetric key generation | Standard:FIPS 186-4, FIPS 186-5 | DSA KeyGen (FIPS186-4): (A5240)<br>L: 2048<br>N: 224<br>ECDSA KeyGen (FIPS186-5): (A5243)<br>Curve: P-224, P-256 |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | Secret Generation Mode: extra bits RSA KeyGen (FIPS186-5): (A5271) Key Generation Mode: probable Modulo: 2048 Primality Tests: 2pow100 Private Key Format: standard CKG: () Key Type: Asymmetric |
| MAC | MAC | Message authentication codes | Standard:FIPS 197, NIST SP 800-38B, FIPS 198-1 | AES-CMAC: (A5238) Direction: Generation Key Length: 128 HMAC-SHA-1: (A5241) Key Length: 160 HMAC-SHA2-256: (A5241) Key Length: 256 |
| SHS | SHA | Message digest | Standard:FIPS 180-4 | SHA-1: (A5242) Message Length: 0-65536 Increment 8 SHA2-256: (A5242) Message Length: 0-65536 Increment 8 |
| SigGen | DigSig-SigGen | Digital signature generation | Standard:FIPS 186-5 | ECDSA SigGen (FIPS186-5): (A5243) Curve: P-224, P-256 Hash Algorithm: SHA2-256 Component: No RSA SigGen (FIPS186-5): (A5271) Modulo: 2048 Signature Type: PKCS1v1.5, PSS |
| SigVer | DigSig-SigVer | Digital signature verification | Standard:FIPS 186-5 | ECDSA SigVer (FIPS186-5): (A5243) Curve: P-224, P-256 Hash Algorithm: |

| Name | Type | Description | Properties | Algorithms |
|---|---|---|---|---|
| | | | | SHA2-256<br>RSA SigVer (FIPS186-5): (A5271)<br>Modulo: 2048<br>Signature Type: PKCS1v1.5, PSS |

Table 7: Security Function Implementations

## 2.7. Algorithm Specific Information

The module's AES-GCM implementation conforms to IG C.H scenario 2. The module uses the approved DRBG (Cert. #A5267) to generate the IV with a length of 96 bits. The entropy source producing the DRBG seed is located inside the module's cryptographic boundary.

The module's use of DSA KeyGen complies with IG C.K. DSA KeyGen (Cert. #A5240) is used exclusively for KAS-FFC-SSC SP 800-56Ar3 (Cert. #A5268). This usage is allowed per IG C.K Resolution 3. The strength of the DSA key pairs thus generated is 112 per NIST SP 800-57 Part 1 Rev. 5, Section 5.6.1.1, Table 2. These DSA keys are ephemeral keys. No DSA static keys are generated.

The module's TLS 1.2 KDF (Cert. #A5269) can only be performed in the context of the TLS protocol.

The module does not truncate HMAC outputs or SHA digests.

For KAS-FFC, the module conforms to IG D.F Scenario 2 path (2). The key derivation functions comply with NIST SP 800-135r1 (i.e., KDF TLS CVL Cert. #A5269) and NIST SP 800-56Cr2 (i.e., KDA HKDF Cert. #A5270). Furthermore, the module obtains the appropriate assurances as required in Section 5.6.2 of NIST SP 800-56Ar3. For KAS-FFC, the module uses C(2e,0s), thus no static key pairs are used as a part of the KAS schemes per NIST SP 800-56Ar3. Full public key validations are implemented (NIST SP 800-56Ar3 Section 5.6.2.3.1). No key confirmation is implemented.

The module does not utilize SHA-1 for digital signature generation. SHA-1 is not offered to an operator, and its usage is fully controlled by the module.

## 2.8. RBG and Entropy

The module includes an internal entropy source for the generation of the DRBG (Cert. #A5239) seed. Please refer to the entropy source validation (ESV) certificate #E58.

| Cert Number | Vendor Name |
|---|---|
| E58 | Quadient Technologies France |

Table 8: Entropy Certificates

| Name | Type | Operational Environment | Sample Size | Entropy per Sample | Conditioning Component |
|---|---|---|---|---|---|
| Quadient Postal Security Device Entropy Source | Physical | Quadient Postal Security Device (PSD) - Alcor | 128 bits | Full entropy | Conditioning Component Block Cipher Derivation Function SP800-90B (Cert. A3803) |

Table 9: Entropy Sources

The entropy source generates 384 bits of entropy input which is combined with a 64-bit nonce, 64-bit personalization string, and 128 bits of additional input. This input is used to instantiate (or reseed) the Counter DRBG. The entropy source produces full entropy output and therefore provides the DRBG with a full 128-bit security strength. The module implements a reseed counter that is incremented each time the DRBG is utilized. When the counter reaches 1,000,000,000 the module will reseed prior to the next usage of the DRBG.

## 2.9. Key Generation

The Quadient Postal Security Device generates symmetric cryptographic keys in conformance with NIST SP 800-133r2 using a NIST SP 800-90A conforming DRBG (Cert. #A5239) for the encryption and protection of data. The module generates asymmetric cryptographic key pairs in conformance with FIPS 186-5 for the facilitation of key agreement in conformance with NIST SP 800-56Ar3. In compliance with FIPS IG C.K Additional Comment 2, the module uses DSA KeyGen (Cert. #A5240) per FIPS 186-4 solely as part of an approved NIST SP 800-56Arev3 FFC scheme.

## 2.10. Key Establishment

The module supports the establishment of cryptographic keys in conformance with ISO/IEC 19790:2012, Annex D and NIST SP 800-140D. The module implements KAS-FFC-SSC per NIST SP 800-56A Rev3 (Cert. #A5268), used in conjunction with KDF TLS per NIST SP 800-135 (Cert. #A5269). KDF TLS is only used within the context of the TLS 1.2 protocol. The module also implements KAS-FFC-SSC per NIST SP 800-56A Rev3 (Cert. #A5268), used in conjunction with KDA HKDF per NIST SP 800-56Cr2 (Cert. #A5270). Key establishment methodology provides at least 112 bits of encryption strength.

The module supports key transport in conformance with ISO/IEC 19790:2012, Annex D and NIST SP 800-140D. The module implements key wrapping using AES-GCM (Cert. #A5267). The module also implements key wrapping using AES-CBC (Cert. #A5237) in conjunction with HMAC-SHA2-256 (Cert. #A5241).

## 2.11. Industry Protocols

The cryptographic module implements the TLS v1.2 protocol and uses only one cipher suite (TLS-DHE-RSA-WITH-AES-128-CBC-SHA256).

The cryptographic module implements the TLS v1.3 protocol and uses only one cipher suite (TLS_AES_128_GCM_SHA256).

The TLS protocol is composed of TLS Handshake protocol (used for mutual authentication and shared keying material establishment) and TLS Record protocol (used for application data confidentiality and integrity). No parts of the TLS protocols, other than the KDF, have been tested by the CAVP or CMVP.

# 3. Cryptographic Module Interfaces

## 3.1. Ports and Interfaces

To communicate with the franking machine's base the cryptographic module provides a physical 10-pin serial connector with five logical interfaces:

| Physical Port | Logical Interface(s) | Data That Passes |
|---|---|---|
| PIN 1: Ground | None | None |
| PIN 2: Ground | None | None |
| PIN 3: RX | Data Input<br>Control Input | Service inputs, SSPs, commands |
| PIN 4: RX | Data Input<br>Control Input | Service inputs, SSPs, commands |
| PIN 5: TX | Data Output<br>Status Output | Service outputs, SSPs, status |
| PIN 6: TX | Data Output<br>Status Output | Service outputs, SSPs, status |
| PIN 7: Power | Power | None |
| PIN 8: Power | Power | None |
| PIN 9: Ground | None | None |
| PIN 10: Ground | None | None |

Table 10: Ports and Interfaces

The data output interface and cryptographic operations are inhibited during zeroization, key generation, self-tests, firmware loading, and error states. No plaintext CSPs are input or output from the module through the serial interface.

# 4. Roles, Services, and Authentication

## 4.1. Authentication Methods

| Method Name | Description | Security Mechanism | Strength Each Attempt | Strength per Minute |
|---|---|---|---|---|
| TLS Handshake, X509 certificates | Mutual authentication based on the TLS Handshake Protocol using the "TLS-DHE-RSA" cryptographic suite, with 2048 RSA key length for authentication. | RSA SigVer (FIPS186-5) (A5271) | The RSA key is 2048 bits and is considered to have 112 bits of strength. For any attempt to use the authentication mechanism, the probability that a random attempt will succeed, or a false acceptance will occur will be 1 in 2^112 (equivalent to less than 2 x 10-34). This is considerably more difficult to break than 1 in 1,000,000 random attempts. | The time necessary to generate an authentication is 60 ms; therefore, 1000 attempts could occur in a one-minute period. For multiple attempts to use the authentication mechanism during a one-minute period the probability that a random attempt will be accepted or that a false acceptance will occur will be 1 in 2^112 multiplied by 1000 (equivalent to less than 2 x 10^-31). This is considerably more difficult to break than 1 in 100,000 within a one-minute period. |

**Table 11: Authentication Methods**

The authentication method of all authenticated roles supported by the module is “Single-Factor Crypto Software” in the form of RSA Signature Verification in conformance with NIST SP 800-140E (refer to Section 6.2) and SP 800-63B (refer to Section 5.1.6). The assumption of roles is implicit. The operator is uniquely identified via a X509 digital certificate that includes RSA signature verification. The authentication mechanism is initialized in manufacturing.

## 4.2. Roles

| Name | Type | Operator Type | Authentication Methods |
|---|---|---|---|
| Field Crypto-Officer | Identity | Crypto Officer | TLS Handshake, X509 certificates |
| Postal Crypto-Officer | Identity | Crypto Officer | TLS Handshake, X509 certificates |
| Base User | Identity | User | TLS Handshake, X509 certificates |
| R&D Signer User | Identity | User | TLS Handshake, X509 certificates |
| Unauthenticated | Role | Other | None |

Table 12: Roles

## 4.3. Approved Services

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| Check Firmware Integrity | Check firmware integrity | SERVICE_INDICATOR | N/A | N/A | BC-UnAuth<br>BC-Auth<br>SigVer<br>SHS | Base User<br>- Utility Public Key: E<br>- TLS 1.2 Secret Keys: E<br>- TLS 1.3 Secret Keys: E |
| Generate PKI Key | Ask the module to generate its TLS communication key pair | SERVICE_INDICATOR | N/A | PSD TLS Communication Certificate | BC-UnAuth<br>KeyGen<br>DRBG<br>ESV | Field Crypto-Officer<br>- PSD TLS Communication Private Key: G<br>- PSD TLS Communication Public Key: G,R<br>- DRBG Parameters-Key & V: E<br>- Master Secret Key: E<br>- DRBG Seed: E,Z<br>- Entropy Input: G,E,Z |
| Generate Stamp Key | Ask the module to generate Indicia Authentication Key(s) (Secret or Private/Public, depending on country configuration) | SERVICE_INDICATOR | N/A | Indicia Authentication Key(s) | BC-UnAuth<br>BC-Auth<br>KeyGen<br>CKG<br>DRBG<br>ESV<br>KTS1.2<br>KTS1.3<br>MAC<br>SHS | Postal Crypto-Officer<br>- Indicia Authentication Secret Key: G,R<br>- Indicia Authentication Private Key: G<br>- Indicia Authentication Public Key: G,R<br>- DRBG Parameters-Key & V: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - Master Secret Key: E<br>- TLS 1.2 Secret Keys: E<br>- TLS 1.3 Secret Keys: E<br>- DRBG Seed: E,Z<br>- Entropy Input: G,E,Z |
| Get PKI Certificate | Ask the module to send its TLS communication certificate | SERVICE_INDICATOR | N/A | PSD TLS Communication Certificate Chain | None | Field Crypto-Officer<br>- Root Public Key: R<br>- Region Public Key : R<br>- PSD TLS Communication Public Key: R |
| Get Self-Test Error Log | Get the most recent self-test error code | SERVICE_INDICATOR | N/A | Last failed self-test date, time and error code | BC-UnAuth<br>BC-Auth | Base User<br>- TLS 1.2 Secret Keys: E<br>- TLS 1.3 Secret Keys: E |
| Postal Indicia | Ask the module to print the indicia | SERVICE_INDICATOR | N/A | Indicia digital signature or MAC | BC-UnAuth<br>BC-Auth<br>DRBG<br>SigGen<br>ESV<br>MAC<br>SHS | Base User<br>- Indicia Authentication Secret Key: E<br>- Indicia Authentication Private Key: E<br>- Master Secret Key: E<br>- DRBG Seed: E,Z<br>- Entropy Input: G,E,Z<br>- TLS 1.2 Secret Keys: E<br>- TLS 1.3 Secret Keys: E |
| Postal Services | Perform postal services (i.e. | N/A | N/A | N/A | BC-UnAuth<br>BC-Auth | Postal Crypto-Officer<br>- TLS 1.2 Secret Keys: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | Set resetting value, ...) | | | | | - TLS 1.3 Secret Keys: E |
| Read Part Number | Show version | SERVICE_INDICATOR | N/A | Module identifier/version | None | Unauthenticated |
| Read Status (Status) | Show status | SERVICE_INDICATOR (Status_rep) | N/A | PSD State, SERVICE_INDICATOR, FIPS_APPROVED_MODE | None | Unauthenticated |
| Self-test | Ask the module to perform the following self-tests: Tamper detection test, Cryptographic Algorithm Self-Test (KAT), Accessibility and validity test of the following CSPs: Master Secret Key , DRBG - Key & V, TLS RSA Communication key, Firmware integrity test | SERVICE_INDICATOR | N/A | N/A | BC-UnAuth BC-Auth | Base User - TLS 1.2 Secret Keys: E - TLS 1.3 Secret Keys: E |
| Set PKI Certificate | Set the TLS communication certificate | SERVICE_INDICATOR | PSD TLS Communication Certificate Chain | N/A | BC-UnAuth BC-Auth SigVer SHS | Field Crypto-Officer - Root Public Key: W,E - Region Public Key : W,E - PSD TLS Communication Public Key: W,E - TLS 1.2 Secret Keys: E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - TLS 1.3 Secret Keys: E |
| Set Stamp Key | Send to module the Indicia Secret key | SERVICE_INDICATOR | Indicia Authentication Secret Key (encrypted) | N/A | BC-UnAuth BC-Auth KTS1.2 KTS1.3 MAC | Postal Crypto-Officer<br>- Indicia Authentication Secret Key: W<br>- Master Secret Key: E<br>- TLS 1.2 Secret Keys: E<br>- TLS 1.3 Secret Keys: E |
| Software Download | Firmware update | SERVICE_INDICATOR | Utility Certificate, Root Certificate | N/A | BC-UnAuth BC-Auth SigVer SHS | Postal Crypto-Officer<br>- Utility Public Key: W,E<br>- Root Public Key: E<br>- TLS 1.2 Secret Keys: E<br>- TLS 1.3 Secret Keys: E |
| TLS Handshake | TLS handshake protocol | SERVICE_INDICATOR, Status_Req before and after TLS Handshake | DKM Server/Postal Server/Base TLS Communication Certificate Chain, DKM Server/Postal Server/Base DH Public Key | PSD TLS Communication Certificate Chain, PSD DH Public Key | DRBG SigGen SigVer ESV KAS1.2 KAS1.3 SHS | Field Crypto-Officer<br>- TLS DH Private Key: G,E<br>- TLS DH Public Key: G,R<br>- TLS 1.2 Secret Keys: G<br>- Root Public Key: R<br>- Region Public Key : R<br>- PSD TLS Communication Public Key: R<br>- PSD TLS Communication Private Key: E<br>- DKM Server Public Key: |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | W,E<br>- Peer DH Public Key: W,E<br>- TLS 1.2 Shared Secret: G,E<br>- TLS 1.3 Shared Secret: G,E<br>- TLS 1.3 Secret Keys: G<br>- DRBG Seed: E,Z<br>- Entropy Input: G,E,Z<br>Postal Crypto-Officer<br>- TLS DH Private Key: G,E<br>- TLS DH Public Key: G,R<br>- TLS 1.2 Secret Keys: G<br>- Root Public Key: R<br>- Region Public Key : R<br>- PSD TLS Communication Public Key: R<br>- PSD TLS Communication Private Key: E<br>- Postal Server Public Key: W,E<br>- Peer DH Public Key: W,E<br>- TLS 1.2 Shared Secret: G,E<br>- TLS 1.3 Shared Secret: G,E |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - TLS 1.3 Secret Keys: G<br>- DRBG Seed: E,Z<br>- Entropy Input: G,E,Z<br>Base User<br>- TLS DH Private Key: G,E<br>- TLS DH Public Key: G,R<br>- TLS 1.2 Secret Keys: G<br>- Root Public Key: R<br>- Region Public Key : R<br>- PSD TLS Communication Public Key: R<br>- PSD TLS Communication Private Key: E<br>- Base Public Key: W,E<br>- Peer DH Public Key: W,E<br>- TLS 1.2 Shared Secret: G,E<br>- TLS 1.3 Shared Secret: G,E<br>- TLS 1.3 Secret Keys: G<br>- DRBG Seed: E,Z<br>- Entropy Input: G,E,Z |
| Verify Files | Verify file's signature | SERVICE_INDICATOR | Utility Certificate, Root Certificate, file's | N/A | BC-UnAuth BC-Auth SigVer SHS | R&D Signer User<br>- Utility Public Key: E<br>- Root Public |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | signature and hash | | | Key: E<br>- TLS 1.2 Secret Keys: E<br>- TLS 1.3 Secret Keys: E |
| Zeroise SPPs | Zeroise all SSPs | SERVICE_INDICATOR | N/A | N/A | None | Unauthenticated<br>- Master Secret Key: Z<br>- DRBG Parameters- Key & V: Z<br>- PSD TLS Communication Private Key: Z<br>- PSD TLS Communication Public Key: Z<br>- TLS DH Private Key: Z<br>- TLS DH Public Key: Z<br>- TLS 1.2 Shared Secret: Z<br>- TLS 1.2 Secret Keys: Z<br>- TLS 1.3 Shared Secret: Z<br>- TLS 1.3 Secret Keys: Z<br>- Indicia Authentication Secret Key: Z<br>- Indicia Authentication Private Key: Z<br>- Indicia Authentication Public Key: Z<br>- Root Public Key: Z<br>- Region Public Key : Z |

| Name | Description | Indicator | Inputs | Outputs | Security Functions | SSP Access |
|---|---|---|---|---|---|---|
| | | | | | | - Utility Public Key: Z<br>- DKM Server Public Key: Z<br>- Postal Server Public Key: Z<br>- Base Public Key: Z<br>- DRBG Seed: Z |

Table 13: Approved Services

## 4.4. Non-Approved Services

| Name | Description | Algorithms | Role |
|---|---|---|---|
| Generate Stamp Key | Ask the module to generate Indicia Authentication Key(s) (Canadian configuration) | ECDSA (P-192) | Postal Crypto-Officer |
| Generate Transport Key | Ask the module to generate Indicia Transport Key(s) (German configuration) | RSA (1024) | Postal Crypto-Officer |
| Set Stamp Key | Send to module the m-secret encrypted with Transport Public Key (German configuration) | RSA (1024) | Postal Crypto-Officer |
| Postal Indicia | Ask the module to print the indicia (Canadian configuration) | ECDSA (P-192) | Base User |

Table 14: Non-Approved Services

## 4.5. External Software/Firmware Loaded

The PSD can upload its firmware from an external source. The new firmware is validated in accordance with the FIPS 140-3 standard by a validation authority before being loaded into the PSD.
The Firmware Load Test (RSA PKCS1 v1.5 2048 signature verification) is performed before the loaded code can be executed. All data output via the data output interface is inhibited until the firmware loading and load test has completed successfully. Once the firmware has been successfully loaded, the PSD restarts and runs pre-operational self-tests. The module versioning information is modified to represent the newly loaded firmware update.

# 5. Software/Firmware Security

## 5.1. Integrity Techniques

At power-up, the Quadient Postal Security Device tests the integrity of its firmware by verifying the RSA 2048 signature. If the signature verification fails, the PSD enters an error state.

## 5.2. Initiate on Demand

At any time, the operator can initiate the firmware integrity test on demand by either power-cycling the module or calling the 'Self-Test' service.

# 6. Operational Environment

## 6.1. Operational Environment Type and Requirements

**Type of Operational Environment**: Limited

**How Requirements are Satisfied**:

The cryptographic module's operational environment is limited. The module can load its firmware from Flash.

# 7. Physical Security

The Quadient Postal Security Device is designed to meet FIPS 140-3 Level 3 Physical Security requirements. It includes a non-removable enclosure comprised of hard epoxy resin with an outer plastic casing. The outer plastic casing is defined as the cryptographic boundary of the cryptographic module. Within the module is a tamper detection envelope designed to detect penetration attempts and a response mechanism that will zeroize all plaintext Sensitive Security Parameters.

## 7.1. Mechanisms and Actions Required

| Mechanism | Inspection Frequency | Inspection Guidance |
|---|---|---|
| Non-removable enclosure | Inspected for tampering each time the module is returned to Quadient manufacturing or for servicing. | Visual inspection |
| Tamper detection and response | Inspected for tampering each time the module is returned to Quadient manufacturing or for servicing. | Verify log files |

Table 15: Mechanisms and Actions Required

## 7.2. EFP/EFT Information

Quadient Postal Security Device was designed to securely operate when the voltage supplied to the module is between 9.6V and 16.9V and the environmental temperature is between -30°C and 84°C.

| Temp/Voltage Type | Temperature or Voltage | EFP or EFT | Result |
|---|---|---|---|
| LowTemperature | -30°C | EFT | Undefined Failure |
| HighTemperature | 84°C | EFP | Zeroisation |

| Temp/Voltage Type | Temperature or Voltage | EFP or EFT | Result |
|---|---|---|---|
| LowVoltage | 9.6V | EFT | Shutdown |
| HighVoltage | 16.9V | EFT | Undefined Failure |

Table 16: EFP/EFT Information

The module mitigates environmental attacks by using a high temperature fuse so that when the temperature of the module exceeds 84°C, the module zeroizes all plaintext SSPs.

## 7.3. Hardness Testing Temperature Ranges

The non-removable enclosure and epoxy resin maintain strength and hardness characteristics over the operating, storage and distribution temperature range of the PSD, i.e. -30°C and 84°C.

| Temperature Type | Temperature |
|---|---|
| LowTemperature | -30°C |
| HighTemperature | +84°C |

Table 17: Hardness Testing Temperatures

# 8. Non-Invasive Security

The module does not provide protections against non-invasive security methods.

# 9. Sensitive Security Parameters Management

## 9.1. Storage Areas

| Storage Area Name | Description | Persistence Type |
|---|---|---|
| Non-volatile memory | CSPs are stored encrypted (with Master Secret) and the PSPs are stored in plaintext | Dynamic |
| Volatile memory protected by tamper response mechanism | CSP stored in plaintext | Dynamic |
| Volatile memory | Temporary SSPs stored in plaintext | Dynamic |

Table 18: Storage Areas

## 9.2. SSP Input-Output Methods

| Name | From | To | Format Type | Distribution Type | Entry Type | SFI or Algorithm |
|---|---|---|---|---|---|---|
| Encrypted Input (TLS 1.2) | Outside the module | Non-volatile memory | Encrypted | Automated | Electronic | KTS1.2 |
| Encrypted Output (TLS 1.2) | Non-volatile memory | Outside the module | Encrypted | Automated | Electronic | KTS1.2 |
| Encrypted Input (TLS 1.3) | Outside the module | Non-volatile memory | Encrypted | Automated | Electronic | KTS1.3 |
| Encrypted Output (TLS 1.3) | Non-volatile memory | Outside the module | Encrypted | Automated | Electronic | KTS1.3 |
| Plaintext Input | Outside the module | Volatile memory | Plaintext | Automated | Electronic | |
| Plaintext Output | Non-volatile memory | Outside the module | Plaintext | Automated | Electronic | |

Table 19: SSP Input-Output Methods

## 9.3. SSP Zeroization Methods

| Zeroization Method | Description | Rationale | Operator Initiation |
|---|---|---|---|
| Invocation of "Zeroize SSPs" service | Zeroize all PSD's SSPs (including "Master Secret Key") by overwriting with zeroes. | Prevent retrieval and reuse of SSPs. Make PSD unusable. | Yes |
| Tamper detection | The module employs a tamper detection envelope designed to detect penetration attempts and a response mechanism that will zeroize all Sensitive Security Parameters. Breach of flex circuit triggers the "Zeroize SSPs" service. | Tamper detection | No |
| PSD temperature over +84°C | PSD temperature over 84°C triggers the "Zeroize SSPs" service (EFP measure). | EFP - High Temperature | No |
| TLS session closure | Zeroization of temporary SSPs upon TLS session closure. | TLS session closure | No |
| Zeroize SSP immediately after use | Zeroization of temporary SSPs immediately after use. | Immediately after use | No |

Table 20: SSP Zeroization Methods

## 9.4. SSPs

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| Base Public Key | Public key residing in a signed X509 Certificate of the Base used to authenticate the Base User. | 2048 bits - 112 | Public key - PSP | Externally | | SigVer |
| DKM Server Public Key | Public key residing in a signed X509 Certificate of the DKM Server used to authenticate the Field CO. | 2048 bits - 112 | Public key - PSP | Externally | | SigVer |
| DRBG Parameters- Key & V | Internal state of DRBG. | 2 x 128 bits - 128 | DRBG - CSP | DRBG | | DRBG |
| DRBG Seed | Seed for the DRBG. Nonce is 64 bits. Personalization string is 64 bits. | 512 bits - 384 | ENT - CSP | ESV | | DRBG |
| Entropy Input | Entropy for the DRBG. | 384 bits - 384 | ENT - CSP | ESV | | DRBG |
| Indicia Authentication Private Key | Key used for indicia authentication (dependent on country configuration). | 224 bits or 256 bits - 112 | Private key - CSP | KeyGen | | SigGen |
| Indicia Authentication Public Key | Key used for indicia authentication (dependent on country configuration). | 2048 bits - 112 | Public key - PSP | KeyGen | | SigGen |
| Indicia Authentication Secret Key | Key used for Indicia authentication (dependent on country configuration). | 160 bits or 256 bits or 128 bits - 112 | Symmetric Key - CSP | CKG | KTS1.2 KTS1.3 | MAC |
| Master Secret Key | Key used to protect the PSD's Critical Security Parameters. | 128 bits - 128 | Symmetric Key - CSP | CKG | | BC-UnAuth |
| PSD TLS Communication Private Key | Authenticates messages and data output from the PSD during TLS Handshake protocol. | 2048 bits - 112 | Private key - CSP | KeyGen | | SigGen |
| PSD TLS Communication Public Key | Public key residing in a signed X509 certificate used for authentication by the cryptographic module to the Base/Postal Server/DKM Server. | 2048 bits - 112 | Public key - PSP | KeyGen | | SigVer |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| Peer DH Public Key | Diffie-Hellman public key of the DKM Server/Postal Server/Base used during the TLS handshake. | 2048 bits - 112 | Public key - PSP | Externally | | |
| Postal Server Public Key | Public key residing in a signed X509 Certificate of the Postal Server used to authenticate the Postal Crypto Officer. | 2048 bits - 112 | Public key - PSP | Externally | | SigVer |
| Region Public Key | Public key residing in a signed X509 Certificate used for the verification of authenticated messages input from the DKM Server/Postal Server/Base. | 2048 bits - 112 | Public key - PSP | Externally | | SigVer |
| Root Public Key | Public key residing in a signed X509 Certificate used for the verification of authenticated messages input from the DKM Server/Postal Server/Base. | 2048 bits - 112 | Public key - PSP | Externally | | SigVer |
| TLS 1.2 Secret Keys | Used for encryption, decryption, and integrity during TLS record communication. | 2 x 128 bits; 2 x 256 bits - 112 | Symmetric Key - CSP | | KAS1.2 | BC-UnAuth KTS1.2 MAC |
| TLS 1.2 Shared Secret | Shared secret used in the TLS 1.2 handshake protocol. | 256 bytes - 112 | Shared secret - CSP | | KAS1.2 | KAS1.2 |
| TLS 1.3 Secret Keys | Used for encryption, decryption, and integrity during TLS record communication. | 2 x 128 bits; 2 x 96 bits - 112 | Symmetric Key - CSP | | KAS1.3 | BC-Auth KTS1.3 |
| TLS 1.3 Shared Secret | Shared secret used in the TLS 1.3 handshake protocol. | 256 bytes - 112 | Shared secret - CSP | | KAS1.3 | KAS1.3 |
| TLS DH Private Key | Diffie-Hellman private key used to agree upon a TLS pre-master/shared secret. | 224 bits - 112 | Private key - CSP | KeyGen | | KAS1.2 KAS1.3 |
| TLS DH Public Key | Diffie-Hellman public key used during TLS handshake to agree upon a TLS pre-master/shared secret. | 2048 bits - 112 | Public key - PSP | KeyGen | | KAS1.2 KAS1.3 |

| Name | Description | Size - Strength | Type - Category | Generated By | Established By | Used By |
|---|---|---|---|---|---|---|
| Utility Public Key | Public key residing in a signed X509 Certificate of the R&D Signer User for authentication of files loaded into module. | 2048 bits - 112 | Public key - PSP | Externally | | SigVer |

Table 21: SSP Table 1

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| Base Public Key | Encrypted Input (TLS 1.3) Plaintext Input | Non-volatile memory:Plaintext | During TLS handshake (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | Root Public Key:Used With Region Public Key :Used With |
| DKM Server Public Key | Encrypted Input (TLS 1.3) Plaintext Input | Non-volatile memory:Plaintext | During TLS handshake (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | Root Public Key:Used With Region Public Key :Used With |
| DRBG Parameters- Key & V | | Volatile memory protected by tamper response mechanism:Plaintext | Generation time (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | Master Secret Key:Generates PSD TLS Communication Private Key:Generates PSD TLS Communication Public Key:Generates Indicia Authentication Secret Key:Generates Indicia Authentication Private Key:Generates Indicia Authentication |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | | | | | Public Key:Generates |
| DRBG Seed | | Non-volatile memory:Encrypted | | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | DRBG Parameters- Key & V:Used With Entropy Input:Used With |
| Entropy Input | | Non-volatile memory:Encrypted | Generation time (few ms) | Zeroize SSP immediately after use | DRBG Parameters- Key & V:Used With |
| Indicia Authentication Private Key | | Volatile memory:Encrypted | During Key Generation, Signature Generation (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | Master Secret Key:Encrypted By DRBG Parameters- Key & V:Generated By |
| Indicia Authentication Public Key | Encrypted Output (TLS 1.2) Encrypted Output (TLS 1.3) | Non-volatile memory:Plaintext | During Key Generation (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | Indicia Authentication Private Key:Paired With TLS 1.2 Secret Keys:Encrypted By |
| Indicia Authentication Secret Key | Encrypted Input (TLS 1.2) Encrypted Output (TLS 1.2) Encrypted Input (TLS 1.3) Encrypted Output (TLS 1.3) | Volatile memory:Encrypted | During Key Generation, Signature Generation (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | Master Secret Key:Encrypted By TLS 1.2 Secret Keys:Encrypted By |
| Master Secret Key | | Volatile memory protected by tamper response mechanism:Plaintext | Encryption/ Decryption time (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD | PSD TLS Communication Private Key:Encrypts Indicia Authentication |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | | | | temperature over +84°C | Secret Key:Encrypts Indicia Authentication Private Key:Encrypts |
| PSD TLS Communication Private Key | | Non-volatile memory:Encrypted | Generation time (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | PSD TLS Communication Public Key:Paired With Master Secret Key:Encrypted By |
| PSD TLS Communication Public Key | Encrypted Output (TLS 1.3) Plaintext Output | Non-volatile memory:Plaintext | Generation time (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | Indicia Authentication Private Key:Paired With Master Secret Key:Encrypted By |
| Peer DH Public Key | Plaintext Input | Volatile memory:Plaintext | During TLS handshake (few ms) | Zeroize SSP immediately after use | TLS DH Private Key:Used With |
| Postal Server Public Key | Encrypted Input (TLS 1.3) Plaintext Input | Non-volatile memory:Plaintext | During TLS handshake (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | Root Public Key:Used With Region Public Key :Used With |
| Region Public Key | Encrypted Input (TLS 1.3) Encrypted Output (TLS 1.3) Plaintext Input Plaintext Output | Non-volatile memory:Plaintext | During TLS handshake (few ms) | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | PSD TLS Communication Public Key:Used With Region Public Key :Used With |
| Root Public Key | Encrypted Input (TLS 1.3) Encrypted | Non-volatile memory:Plaintext | During TLS handshake (few ms) | Invocation of "Zeroize SSPs" service Tamper | PSD TLS Communication Public Key:Used With |

| Name | Input - Output | Storage | Storage Duration | Zeroization | Related SSPs |
|---|---|---|---|---|---|
| | Output (TLS 1.3) Plaintext Input Plaintext Output | | | detection PSD temperature over +84°C | Region Public Key :Used With |
| TLS 1.2 Secret Keys | | Volatile memory:Plaintext | During TLS session | TLS session closure | TLS 1.2 Shared Secret:Derived From |
| TLS 1.2 Shared Secret | | Volatile memory:Plaintext | During TLS handshake (few ms) | Zeroize SSP immediately after use | TLS DH Private Key:Derived From |
| TLS 1.3 Secret Keys | | Volatile memory:Plaintext | During TLS session | TLS session closure | TLS 1.3 Shared Secret:Derived From |
| TLS 1.3 Shared Secret | | Volatile memory:Plaintext | During TLS handshake (few ms) | Zeroize SSP immediately after use | TLS DH Private Key:Derived From |
| TLS DH Private Key | | Volatile memory:Plaintext | During TLS handshake (few ms) | Zeroize SSP immediately after use | DRBG Parameters- Key & V:Generated By TLS DH Public Key:Paired With |
| TLS DH Public Key | Plaintext Output | Volatile memory:Plaintext | During TLS handshake (few ms) | Zeroize SSP immediately after use | TLS DH Private Key:Paired With |
| Utility Public Key | Encrypted Input (TLS 1.2) Encrypted Input (TLS 1.3) | Non-volatile memory:Plaintext | Few ms | Invocation of "Zeroize SSPs" service Tamper detection PSD temperature over +84°C | Root Public Key:Used With |

**Table 22: SSP Table 2**

## 9.5. Transitions

**SHA-1:** The module does not utilize SHA-1 for digital signature generation. Per CMVP Programmatic Transitions and NIST SP 800-131Ar2, usage of SHA-1 for non-digital-signature applications is deprecated through Dec 31, 2030 and is disallowed thereafter.

**Minimum key size transition:** In accordance with NIST SP 800-131Ar2, the module meets the minimum key size requirement of 112. NIST SP 800-57, Part 1 includes a transition to a security strength of 128 bits from 2031 and beyond.

# 10. Self-Tests

The Quadient Postal Security Device performs pre-operational (Table 10.1) and conditional self-tests (Table 10.2) without external control or operator intervention either in approved or non-approved mode.

The Quadient Postal Security Device inhibits the data output and control interfaces during self-tests.

If a self-test fails, the Quadient Postal Security Device enters in error state and outputs an error indicator (error code). The Quadient Postal Security Device does not perform any cryptographic operations or output control and data via the control and data output interface while in an error state. The PSD must be re-powered to exit the error state and if the error persists the module must be returned to Quadient. The Quadient Postal Security Device maintains a self-test error log that is accessible by an authorized operator of the module.

## 10.1. Pre-Operational Self-Tests

The Quadient Postal Security Device performs the following pre-operational self-tests at power-up:

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|---|---|---|---|---|---|
| Firmware Integrity Test | Key length = 2048 | Signature Verification | SW/FW Integrity | SERVICE_INDICATOR | The module verifies the integrity of its firmware using RSA 2048 signature verification. The RSA 2048 signature verification self-test is performed prior to the firmware integrity test. If the signature verification fails, the module enters the error state and outputs an error indicator (error code). |
| Accessibility and Validity Test | 16-Bit EDC | 16-bit EDC Verification | Critical Function | SERVICE_INDICATOR | Accessibility and validity test of the following CSPs: Master Secret Key, DRBG Key and V, TLS Communication Private Key. If any of these CSPs are not accessible (i.e., device failure) or contains erroneous data, the module enters the error state and outputs an error indicator (error code). |
| Tamper Detection Test | N/A | Tamper detection/Fuse burn out | Critical Function | SERVICE_INDICATOR | If tampering is detected, the module enters the faulted state, outputs an error |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details |
|---|---|---|---|---|---|
| | | | | | indicator (error code) and zeroizes all CSPs. |

Table 23: Pre-Operational Self-Tests

## 10.2. Conditional Self-Tests

The Quadient Postal Security Device performs the following conditional self-tests:

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| AES-CBC (A5237) | Key Length: 128 | KAT | CAST | SERVICE_INDICATOR | Encrypt, Decrypt | At startup/on demand |
| AES-CMAC (A5238) | Key Length: 128 | KAT | CAST | SERVICE_INDICATOR | Encrypt | At startup/on demand |
| AES-GCM (A5267) | Key Length: 128 | KAT | CAST | SERVICE_INDICATOR | Encrypt, Decrypt | At startup/on demand |
| Conditional Critical Functions Test | EDC: 16 bits | 16-bit EDC | Critical Function | SERVICE_INDICATOR | SSPs accessibility and validity test | Before their use |
| Counter DRBG (A5239) | Mode: AES-128 | KAT | CAST | SERVICE_INDICATOR | DRBG: instantiate, generate, reseed | At startup/on demand |
| ECDSA KeyGen (FIPS186-5) (A5243) | Curves: P-224, P-256 | Pair-wise consistency | PCT | SERVICE_INDICATOR | Signature generation | When ECDSA key generation occurs |
| ECDSA SigGen (FIPS186-5) (A5243) | Curves: P-224, P-256 | KAT | CAST | SERVICE_INDICATOR | Signature generation | At startup/on demand |
| ECDSA SigVer (FIPS186-5) (A5243) | Curves: P-224, P-256 | KAT | CAST | SERVICE_INDICATOR | Signature verification | At startup/on demand |
| Entropy Source | Adaptive Proportion Test and | APT, RCT | CAST | SERVICE_INDICATOR | Repetition Count Test, Adaptive | At power up and during the noise |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| Continuous Tests | Repetition Count Test | | | | Proportion Test (ref. SP 800-90B) | source operation |
| Firmware Load Test | RSA Modulus: 2048 | RSA (PKCS1 v1.5) 2048 signature verification | Critical Function | SERVICE_INDICATOR | Signature verification | During firmware download operation |
| HMAC-SHA-1 (A5241) | Key Length: 160 | KAT | CAST | SERVICE_INDICATOR | HMAC generation | At startup/on demand |
| HMAC-SHA2-256 (A5241) | Key Length: 256 | KAT | CAST | SERVICE_INDICATOR | HMAC generation | At startup/on demand |
| KAS Assurances | KAS Role: responder | Private Key Validation, Public Key Validation, and DH Pairwise Consistency Tests | PCT | SERVICE_INDICATOR | Assurances per SP 800-56Ar3 5.6.2 | At power up and when DH key generation occurs |
| KAS-FFC-SSC Sp800-56Ar3 (A5268) | KAS Role: responder | KAT | CAST | SERVICE_INDICATOR | Shared secret computation | At startup/on demand |
| KDA HKDF SP800-56Cr2 (A5270) | Derived Key Length: 1024, Shared Secret Length: 2048, HMAC Algorithm: SHA2-256 | KAT | CAST | SERVICE_INDICATOR | Key derivation | At startup/on demand |
| KDF TLS (A5269) | Hash Algorithm: SHA2-256, Key Block Length: 1024 | KAT | CAST | SERVICE_INDICATOR | Key derivation | At startup/on demand |
| RSA KeyGen (FIPS186-5) (A5271) | Hash Algorithm: SHA2-256, Modulo: 2048 | Pair-wise consistency | PCT | SERVICE_INDICATOR | Signature verification | When RSA key generation occurs |

| Algorithm or Test | Test Properties | Test Method | Test Type | Indicator | Details | Conditions |
|---|---|---|---|---|---|---|
| RSA SigGen (FIPS186-5) (A5271) | Hash Algorithm: SHA2-256, Modulo: 2048, Signature Type: pkcs1v1.5, pss | KAT | CAST | SERVICE_INDICATOR | Signature generation using PKCS#1 v1.5 and PSS | At startup/on demand |
| RSA SigVer (FIPS186-5) (A5271) | Hash Algorithm: SHA2-256, Modulo: 2048, Signature Type: pkcs1v1.5, pss | KAT | CAST | SERVICE_INDICATOR | Signature generation using PKCS#1 v1.5 and PSS | At startup/on demand |
| SHA-1 (A5242) | None | KAT | CAST | SERVICE_INDICATOR | Hash generation | At startup/on demand |
| SHA2-256 (A5242) | None | KAT | CAST | SERVICE_INDICATOR | Hash generation | At startup/on demand |

**Table 24: Conditional Self-Tests**

Per FIPS IG D.J, the Conditioning Component Block Cipher Derivation Function is used solely as an entropy conditioning component, so no cryptographic algorithm self-test is required.

## 10.3. Periodic Self-Test Information

The Quadient Postal Security Device automatically performs self-tests repeatedly at a defined time period without external input or control. The Quadient Postal Security Device performs the periodic self-test at midnight. The time period is configurable between 1 and 30 days (default 30 days). The periodic self-test execution date and time is stored in non-volatile memory. The periodic self-test execution failure is recorded in the error log.

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| Firmware Integrity Test | Signature Verification | SW/FW Integrity | Configurable between 1 and 30 days/at startup/on demand | Automatic |
| Accessibility and Validity Test | 16-bit EDC Verification | Critical Function | Configurable between 1 and 30 | Automatic |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| | | | days/at startup/on demand | |
| Tamper Detection Test | Tamper detection/Fuse burn out | Critical Function | Configurable between 1 and 30 days/at startup/on demand | Automatic |

Table 25: Pre-Operational Periodic Information

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| AES-CBC (A5237) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| AES-CMAC (A5238) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| AES-GCM (A5267) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| Conditional Critical Functions Test | 16-bit EDC | Critical Function | N/A | N/A |
| Counter DRBG (A5239) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| ECDSA KeyGen (FIPS186-5) (A5243) | Pair-wise consistency | PCT | N/A | N/A |
| ECDSA SigGen (FIPS186-5) (A5243) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| ECDSA SigVer (FIPS186-5) (A5243) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| Entropy Source Continuous Tests | APT, RCT | CAST | N/A | N/A |
| Firmware Load Test | RSA (PKCS1 v1.5) 2048 signature verification | Critical Function | N/A | N/A |
| HMAC-SHA-1 (A5241) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| HMAC-SHA2-256 (A5241) | KAT | CAST | Configurable between 1 and 30 days | Automatic |

| Algorithm or Test | Test Method | Test Type | Period | Periodic Method |
|---|---|---|---|---|
| KAS Assurances | Private Key Validation, Public Key Validation, and DH Pairwise Consistency Tests | PCT | N/A | N/A |
| KAS-FFC-SSC Sp800-56Ar3 (A5268) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| KDA HKDF SP800-56Cr2 (A5270) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| KDF TLS (A5269) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| RSA KeyGen (FIPS186-5) (A5271) | Pair-wise consistency | PCT | N/A | N/A |
| RSA SigGen (FIPS186-5) (A5271) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| RSA SigVer (FIPS186-5) (A5271) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| SHA-1 (A5242) | KAT | CAST | Configurable between 1 and 30 days | Automatic |
| SHA2-256 (A5242) | KAT | CAST | Configurable between 1 and 30 days | Automatic |

**Table 26: Conditional Periodic Information**

## 10.4. Error States

| Name | Description | Conditions | Recovery Method | Indicator |
|---|---|---|---|---|
| Error state | The module does not perform any cryptographic operations or output control and data via the control and data output interface while in an error state. Only non-secure services (e.g. Get Status...) are available. | Self-tests (pre-operational, conditional, and periodic) failure. Inconsistency of the registers at power up. Failed to read Master key & DRBG parameters. | The module must be re-powered to exit the error state and if the error persists the module must be returned to Quadient. | Error Code |

| Name | Description | Conditions | Recovery Method | Indicator |
|---|---|---|---|---|
| Faulted state | The module zeroizes all plaintext CSPs. | Tamper detection. Temperature exceeds 84°C. Zeroisation service invoked. | No recovery. The module must be returned to Quadient. | Error code and PSD Status = Faulted |

Table 27: Error States

## 10.5. Operator Initiation of Self-Tests

Self-tests may be triggered by the user using the 'Self-Test' service, which runs the module's pre-operational self-tests and cryptographic algorithm known answer tests (KATs).

# 11. Life-Cycle Assurance

Quadient Technologies France uses a system configuration management tool (Windchill) to manage products configurations (including the cryptographic module).

## 11.1. Installation, Initialization, and Startup Procedures

The module is initialized in manufacturing and installed into a compatible postal meter. The postal meter is then authorized and shipped to the end customer.

## 11.2. Administrator Guidance

The PSD TLS Communication key pair is generated internally by the module at the customization center during manufacturing. Once the key pair is available, the public key is immediately output for certification by the Manufacturing CA entity. After the certificate is available and downloaded into the module, all communication between the manufacturing environment and the module are mutually authenticated and encrypted via a TLS-tunnel.
Once installed in the postage meter (at the customer site), the module first connects to the DKM Server via mutual authenticated TLS session and sends its certificate for certification by the Country Region CA entity. A new certificate chain is downloaded into the module to be used for communication with Quadient infrastructure (DKM/Postal Servers) to access available services during the operational phase.
The KMS Server may decide to update stored keys and certificates before they reach the end of cryptographic periods by triggering the re-keying of module:

- issuing certificates for newly generated module public keys and
- replacement of certificate chain stored in the module.

This takes place during the secure mutually authenticated TLS sessions.

## 11.3. Non-Administrator Guidance

The Quadient postage meters include detailed user guidance in its free online manuals: iX Range - KCMS (quadient.com).

## 11.4. Design and Rules

The cryptographic module's firmware has been implemented using a high-level language (C), except for the limited use of assembly language where it was essential for performance. The module's firmware is present in the form of a binary file which is executed by the module's processor. The firmware image does not require further compilation and there is no dynamically modified code.

The following security rules are enforced by the cryptographic module to implement the security requirements of a FIPS 140-3 Security Level 3 module:

1. The module processes only one request at a time (single thread). The PSD will ignore all other inputs to the module while processing the request. The only output performed by the PSD is the response to the request.
2. The module employs identity-based authentication mechanism.
3. All authenticated sessions end when the module is power cycled.
4. All keys generated in the module have at least 112 bits of cryptographic security strength for an Approved mode of operation.
5. The module does not provide any bypass capability.
6. The module does not support a maintenance role.
7. The module does not support manual input or output of CSPs.
8. The module performs pre-operational and conditional self-tests without external control or operator intervention either in approved or non-approved mode. The PSD enters the error state if the test fails.
9. The module automatically performs periodic self-tests without external input or control. The PSD enters the error state if the test fails.
10. The module inhibits all data output interfaces when performing self-tests, firmware loading, zeroization or while in the error state.
11. The module does not output any CSP in plaintext form.
12. The module does not accept any CSP in plaintext form.
13. The module tests the accessibility and validity of all CSP values in nonvolatile memories at power up. If any are not accessible (i.e., device failure) or contain erroneous data (16-bit EDC fails) then the PSD enters the error state.
14. The module enters in the Faulted state and zeroizes all SSPs if physical cryptographic boundary is breached or if the temperature inside the module exceeds 84°C.
15. Once the module has been zeroized, it must be returned to the factory for destruction.

## 11.5. End of Life

Upon end of life, the module is withdrawn from service and returned to manufacturing for decommissioning and scrapping.

# 12. Mitigation of Other Attacks

The module employs a tamper detection envelope designed to detect penetration attempts and a response mechanism that zeroizes all the module's CSPs.