Quadient Postal Security Device Security Policy

Valid from:	27/11/2024
Version No.:	V 1.2

Because connections matter.

This document is non-proprietary.
It may be reproduced or transmitted only in its entirety without revision.

Content

Figure list

Table list

1. General

This document describes the security policy of the Quadient Technologies France (Quadient) Postal Security Device 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.

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

ISO/IEC 24759 Section 6	FIPS 140-3 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. Overview

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

Model	Hardware Part Number	Firmware Part Number	Firmware Version
Quadient Postal Security Device	A0014227-B and A0014227-C	A0156569A	a31.05

Table 2: Cryptographic Module Tested Configuration

The Quadient Postal Security Device (***Figure 1***) is a multi-chip standalone cryptographic module 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.

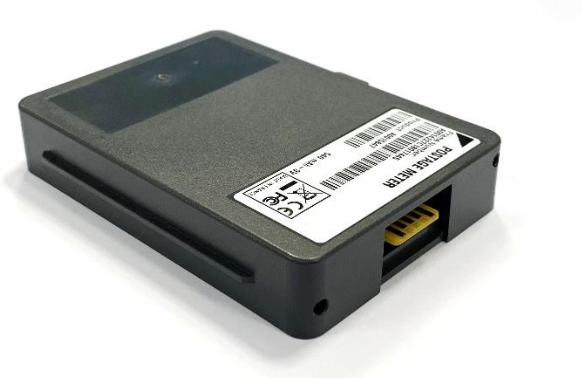

Figure 1 – Quadient Postal Security Device

2.2. Excluded Components

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

2.3. Modes of operation

The module only supports an Approved mode of operation that is entered upon powering-on the module. The module does not support a degraded mode of operation.

2.4. Security 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 TLS protocol is composed of TLS Handshake protocol (used for mutual authentication and TLS pre-master secret establishment) and TLS Record protocol (used for application data confidentiality and integrity).

2.5. Security functions

2.5.1. Approved Algorithms

The Quadient Postal Security Device supports the following approved security functions:

CAVP Cert.	Algorithm and Standard	Modes/ Methods	Description/ Key Size(s)/ Key Strength(s)	Use/Function
Cert. #A728	**AES CBC** FIPS 197 SP 800-38A	CBC	128	Encryption/Decryption of: • CSPs for storage within the module • Data exchanged using TLS v1.2
Cert. #A760	**AES CMAC** FIPS 197 SP 800-38B	AES	128	Indicia Authentication
Cert. #A3803	**Conditioning Component Block Cipher** SP 800-90B	N/A	N/A	Conditioning component of module's entropy source.
Cert. #A2930	**CTR-DRBG** SP 800-90A	AES	128	Key generation
Cert. #A761	**CVL (KDF TLS)** SP 800-135	SHA-256		TLS 1.2 KDF
Cert. #A767	**DSA** FIPS 186-4	KeyGen	(2048, 224)	Used for KAS-SSC
Cert. #A2931	**ECDSA** FIPS 186-4	SHA-256	P-224, P-256	Key Generation, Digital Signature Generation (Indicia Authentication)[1]
Cert. #A729	**HMAC-SHA-1, HMAC-SHA-256** FIPS 198-1	(Key Sizes Ranges Tested: KS<BS)	160 256	TLS messages authentication, Indicia Authentication

[1] ECDSA P-244 Signature Verification is included on the algorithm certificate but not used by the module.

CAVP Cert.	Algorithm and Standard	Modes/ Methods	Description/ Key Size(s)/ Key Strength(s)	Use/Function
Cert. #A2929	**KAS-SSC** SP 800-56A r3	FFC DH	112	Key agreement used to establish TLS session keys C(2e, 0s, FFC DH), with DSA KeyGen (Cert. #A767) as a prerequisite, using loaded ffdhe2048 safe prime domain parameters. Provides 112 bits of encryption strength.
AES (Cert. #A728) HMAC (Cert. #A729)	**KTS** SP 800-38F	AES CBC HMAC-SHA-256	128 bits 256 bits	TLS key transport scheme, using keys established with KAS-SSC and TLS KDF. Provides 112 bits of encryption strength.
Cert. #A765	**RSA** FIPS 186-4	SHA-256 PKCS1 v1.5	2048	Key Generation Signature generation/Signature verification of X509 certificates used by TLS Handshake protocol, Signature verification of signed files imported into the module[2]
Cert. #A730	**SHS** FIPS 180-4	SHA-1, SHA-256	N/A	Hashing algorithm used for: ● HMAC Generation ● Digital signatures

Table 3: Approved Algorithms

2.5.2. Vendor Affirmed Algorithms

The module supports the following vendor affirmed algorithms.

Algorithm and Standard	Modes/ Methods	Description/ Key Size(s)/ Key Strength(s)	Use/Function
CKG SP 800-133r2	Per Sections 4 and 5.2	The unmodified output from SP 800-90A DRBG (128 bits)	The unmodified output of the DRBG is used for symmetric and asymmetric key generation

Table 4: Vendor Affirmed Algorithms

2.5.3. Allowed Algorithms

The module supports only approved algorithms.

Algorithm and Standard	Modes/ Methods	Description/ Key Size(s)/ Key Strength(s)	Use/Function
N/A	N/A	N/A	N/A

Table 5: Allowed Algorithms

[2] RSA Signature Verification to FIPS 186-2 with modulo 1536 is listed on the algorithm certificate but not utilized by the module.

2.5.4. Non-Approved Algorithms

The module supports only approved algorithms.

Algorithm and Standard	Modes/ Methods	Description/ Key Size(s)/ Key Strength(s)	Use/Function
N/A	N/A	N/A	N/A

Table 6: Non-Approved Algorithms

2.5.5. Security Function Implementations (SFI)

Name	Type	Description	SF Properties	Algorithms / CAVP Cert.
KAS	KAS	NIST SP 800-56Arev3 KAS-SSC Per IG D.F Scenario 2 path (2).	FFC (2048, 224) Providing 112 bits of encryption strength	KAS-SSC (Cert. #A2929) CVL (Cert. #A761)
KTS	KTS	NIST SP 800-38F. KTS (key wrapping and unwrapping) per IG D.G.	128-bit key providing 128 bits of encryption strength	AES-CBC (Cert. #A728) HMAC-SHA-256 (Cert. #A729)

Table 7: Security Function Implementations

2.5.6. Entropy Sources

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

Vendor Name	Certificate Number
Quadient Technologies France	E58

Table 8: Entropy Source Implementations

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 CTR-DRBG. The entropy source has a rate of 88% and therefore provides the DRBG with a full 128-bit security strength.

2.5.7. Key Establishment

The module supports the establishment of cryptographic keys using finite field cryptography (FFC) in conformance with NIST SP 800-56A Rev3. The module implements KAS-FFC-SSC per NIST SP 800-56A Rev3 (Cert. #A2929), used in conjunction with TLS KDF per NIST SP 800-135 (Cert. #A761). Key establishment methodology provides at least 112 bits of encryption strength. This is used to establish TLS v1.2

communication sessions in conformance with NIST SP 800-38F using AES (Cert. #A728) and HMAC (Cert. #A729).

2.6. Security Rules

This section documents the security rules applied by the cryptographic module to implement the security requirements of a FIPS 140-3 level 3 module:

1. The PSD **shall** process 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. Quadient Postal Security Device **shall** employ identity-based authentication mechanism.
3. All authenticated sessions **shall** end when the module is power cycled.
4. All keys generated in the module **shall** have at least 112 bits of cryptographic security strength for an Approved mode of operation.
5. The module **shall not** provide any bypass capability.
6. The PSD **shall not** support a maintenance role.
7. The PSD **shall not** support manual input or output of CSPs.
8. The PSD **shall** perform pre-operational and conditional self-tests without external control or operator intervention either in approved or non-approved mode. The PSD **shall** pass into the error state if the test fails.
9. The PSD **shall** automatically perform periodic self-tests without external input or control. The PSD **shall** enter the error state if the test fails.
10. The PSD **shall** inhibit all data output interfaces when performing self-tests, firmware loading, zeroization or while in the error state.
11. The module **shall not** output any CSP in plaintext form.
12. The module **shall not** accept any CSP in plaintext form.
13. The PSD **shall** test 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 shall enter in error state.
14. The PSD **shall** enter in the Faulted state and zeroize all SSPs if physical cryptographic boundary is breached or if the temperature inside the module exceeds 84°C.
15. Once the PSD has been zeroized, it must be returned to the factory for destruction.

3. Cryptographic module 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	Data that passes over port/interface
PIN 1: Ground	N/A	N/A
PIN 2: Ground	N/A	N/A
PIN 3: RX	data input/control input	PSD TLS Communication Certificate chain Indicia Authentication Secret Key
PIN 4: RX	data input/control input	PSD TLS Communication Certificate chain

		Indicia Authentication Secret Key
PIN 5: TX	data output/status output	PSD TLS Communication Certificate chain PSD DH Public Key Indicia Authentication Public Keys
PIN 6: TX	data output/status output	PSD TLS Communication Certificate chain PSD DH Public Key Indicia Authentication Public Keys
PIN 7: Power	power	N/A
PIN 8: Power	power	N/A
PIN 9: Ground	N/A	N/A
PIN 10: Ground	N/A	N/A

Table 9: Ports and Interfaces

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

4. Roles, services, and authentication

4.1. Roles

The Quadient Postal Security Device supports authorized roles for operators and corresponding services within each role.
The Quadient Postal Security Device supports the following **Crypto-Officer** roles: Field Crypto-Officer and Postal Crypto-Officer.

The Quadient Postal Security Device supports the following **User** roles: Base User, R&D Signer and Unauthenticated User.
For each role, the Quadient Postal Security Device provides the following services and the corresponding input and outputs:

Role	Service	Input	Output
Field Crypto-Officer	TLS Handshake	Field Server TLS Communication Certificate chain, Field Server DH Public parameters (p, g, Y)	PSD TLS Communication Certificate chain, TLS DH Public Key (Y)
	Generate PKI Key	N/A	PSD TLS Communication Certificate (self-signed)
	Get PKI Certificate	N/A	PSD TLS Communication Certificate chain
	Set PKI Certificate	PSD TLS Communication Certificate chain	N/A
Postal Crypto-Officer	TLS Handshake	Postal Server TLS Communication Certificate chain, Postal Server DH Public parameters (p, g, Y)	PSD TLS Communication Certificate chain, TLS DH Public Key (Y)
	Generate Stamp Key	Expiry date	Indicia Authentication Secret or Private and Public Keys
	Set Stamp Key	Indicia Authentication Key (encrypted), expiry date	N/A
	Software download	Utility certificate, Root Certificate	Ok or error code
	Postal services (set resetting value, get statistic)	Postal data	Postal data, status
	Read Status (Get Device Info service)	N/A	PSD State
	Read Part Number (Get Device Info service)	N/A	PART_NUMBER (package/firmware)
Base User	TLS Handshake	Base TLS Communication Certificate chain, Base DH Public Key (Y)	PSD TLS Communication Certificate chain, TLS DH Public parameters (p, g, Y)
	Postal Indicia	Indicia input data	Indicia digital signature or MAC
	Read Status (Status request)	N/A	PSD State
	Read Part Number (Get Device Info service)	N/A	PART_NUMBER (package/firmware)
	Self-test	N/A	Ok or error message
	Get Error Log	N/A	Error log information, includes most recent error codes, date & time stamps

Role	Service	Input	Output
R&D Signer User	Verify Files (Check File)	Utility Certificate, Root Certificate, file's signature & hash	Ok or error code
	TLS Handshake	R&D Signer Communication Certificate chain R&D Signer User DH Public Key (Y)	PSD TLS Communication Certificate chain, TLS DH Public parameters (p, g, Y)
Unauthenticated User	Read Status (Status request)	N/A	PSD State
	Read Part Number (Get Device Info service)	N/A	PART_NUMBER (package/firmware)
	Zeroize SSP	N/A	Ok or error code

Table 10: Roles, Service Commands, Input and Output

4.2. Authentication

To control access to the module the Quadient Postal Security Device employs identity-based authentication mechanism.
For each role, the Quadient Postal Security Device provides the following authentication method:

Role	Authentication Method	Authentication Strength (bits)
Field Crypto-Officer	TLS 1.2 handshake, X509 certificates	112
Postal Crypto-Officer	TLS 1.2 handshake, X509 certificates	112
Base User	TLS 1.2 handshake, X509 certificates	112
R&D Signer User	TLS 1.2 handshake, X509 certificates	112
Unauthenticated User	N/A	N/A

Table 11: Roles and Authentication

Mutual authentication is based on the TLS v1.2 Handshake Protocol using the "TLS-DHE-RSA" cryptographic suite, with 2048 RSA key length for authentication.

- 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 at least 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 100ms; therefore, 600 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 600 - maximum number of attempts in one minute (equivalent to 1 x 10^{-31}). This is considerably more difficult to break than 1 in 100,000 within a one-minute period.

4.3. Services

4.3.1. Approved services

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to keys and/or SSPs	Indicator
Generate PKI Key	Ask the module to generate its TLS communication key pair	RSA 2048, DRBG, AES 128	PSD TLS Communication Private and Public Keys, DRBG entropy input (if needed), DRBG parameters – Key & V, Master Secret Key	Field Crypto-Officer	(G) PSD TLS Communication Private Key, (G) PSD TLS Communication Public Key (X509 certificate), (G, E) DRBG entropy input (if needed), (G, E) DRBG parameters – Key & V, (E) Master Secret Key	APPR_MODE
Get PKI Certificate	Ask the module to send its TLS communication certificate	N/A	PSD TLS Communication Public Key (TLS Communication Certificate chain)	Field Crypto-Officer	(R) PSD TLS Communication Public Key (TLS Communication Certificate chain)	APPR_MODE
Set PKI Certificate	Set the TLS communication certificate	RSA 2048, SHA-256	PSD TLS Communication Public Key (TLS Communication Certificate chain), Root Public Key, Previous Root Public Key	Field Crypto-Officer	(W) PSD TLS Communication Public Key (TLS Communication Certificate chain), (E) Root Public Key, (E) Previous Root Public Key	APPR_MODE

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to keys and/or SSPs	Indicator
Generate Stamp Key	Ask the module to generate Indicia Authentication Key(s) (Secret or Private/Public, depending on country configuration)	HMAC-SHA-1 or HMAC-SHA-256 or CMAC AES 128 or ECDSA P-224 or ECDSA P-256, SHA-256, DRBG, CBC AES 128	Indicia Authentication Secret or Private & Public Key, DRBG entropy input (if needed), DRBG parameters – Key & V, Master Secret Key	Postal Crypto-Officer	(G) Indicia Authentication Secret Key or (G) Indicia Authentication Private and Public Keys, (G, E) DRBG entropy input (if needed), (G, E) DRBG parameters – Key & V, (E) Master Secret Key	APPR_MODE
Postal Indicia	Ask the module to print the indicia	HMAC-SHA-1 or HMAC-SHA-256 or CMAC AES 128 or ECDSA P-224 or ECDSA P-256, SHA-256, DRBG, AES 128	Indicia Authentication Secret Key, Indicia Authentication Private Key, Master Secret Key	Base User	(E) Indicia Authentication Secret Key or (E) Indicia Authentication Private Key, (E) Master Secret Key	APPR_MODE
Set Stamp Key	Import encrypted Indicia Secret key	AES 128 CMAC AES 128	Indicia Authentication Secret Key, Master Secret Key	Postal Crypto-Officer	(W) Indicia Authentication Secret Key, (E) Master Secret Key	APPR_MODE
Read Status (Status)	Show status	N/A	N/A	Postal Crypto-Officer, Base User, Unauthenticated User	N/A	APPR_MODE (Get device info, Status_rep)
Read Part Number	Show version	N/A	N/A	Postal Crypto-Officer, Base User, Unauthenticated User	N/A	APPR_MODE (Get device info/ Part_Nb_Rep, Part_Nb_Soft_Rep)

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to keys and/or SSPs	Indicator
TLS Handshake	TLS handshake protocol	RSA 2048, SHA-256, KAS-SSC (DH), KDF (CVL)	PSD TLS Communication Public Key, TLS DH Private Key (x), TLS DH Public parameters (p, g Y) or TLS DH Public Key (Y), TLS Communication Secret Keysets, TLS pre-master key, TLS master key, Field Server or Postal Server or Base or R&D Signer User Public Key, DRBG entropy input (if needed), DRBG parameters – Key & V, Master Secret Key	Field Crypto-Officer, Postal Crypto-Officer, Base User, R&D Signer User	(E) PSD TLS Communication Public Key (TLS Communication Certificate chain), (G) TLS DH Private Key (x), (G) TLS DH Public Key (Y) or (G) TLS DH Public parameters (p, g, Y), (G) TLS pre-master key, (G) TLS master key, (G) TLS communication secret keyset, (E) Field Server or Postal Server or Base or R&D Signer User Public Key, (G, E) DRBG entropy input (if needed), (G, E) DRBG parameters – Key & V, (E) Master Secret Key	APPR_MODE Status_REQ before and after TLS Handshake
Verify Files	Verify file's signature	RSA 2048, SHA-256	Utility Public Key (Utility Certificate), Root Public Key (Root Certificate)	R&D Signer User	(E) Utility Public Key (Utility Certificate), (E) Root Public Key (Root Certificate)	APPR_MODE
Zeroize SSP	Zeroise all SSPs	N/A	All SSPs listed in Table 15	Unauthenticated User	(Z) SSPs listed in Table 15	APPR_MODE and Zeroization indicator

Service	Description	Approved Security Functions	Keys and/or SSPs	Roles	Access rights to keys and/or SSPs	Indicator
Self-test		AES (CBC 128), AES (CMAC 128), DRBG, ECDSA (P-224), ECDSA (P-256), HMAC (SHA-1), HMAC (SHA-256), KAS-SSC, TLS-KDF, RSA, SHA-1, SHA-256	N/A	Base User	N/A	APPR_MODE
Postal Services	Set resetting value Audit	N/A	N/A	Postal Crypto-Officer	N/A	N/A
Get Error Log	Get the module's most recent error code	N/A	N/A	Base User	N/A	APPR_MODE
Software Download	Firmware update	RSA 2048, SHA-256	Utility Public Key (Utility Certificate), Root Public Key (Root Certificate)	Postal Crypto-Officer	(E/W) Utility Public Key (Utility Certificate), (E) Root Public Key (Root Certificate)	APPR_MODE

Table 12: Approved Services

G = Generate: The module generates or derives the SSP.

R = Read: The SSP is read from the module (e.g., the SSP is output).

W = Write: The SSP is updated, imported, or written to the module.

E = Execute: The module uses the SSP in performing a cryptographic operation.

Z = Zeroise: The module zeroises the SSP.

4.3.2. Non-approved services

The module does not support any non-approved services.

5. Software/Firmware security

At power-up, the Quadient Postal Security Device tests the integrity of its firmware (binary file) by verifying the RSA 2048 PKCS1 v1.5 signature with SHA-256 hash function. If the signature verification fails, the PSD enters an error state.

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

The cryptographic module's operational environment is limited.

7. Physical security

The Quadient Postal Security Device is designed to meet FIPS 140-3 Level 3 Physical Security requirements.

The Quadient Postal Security Device includes a non-removable enclosure that comprises a hard epoxy resin with an outer plastic casing. The outer plastic casing is defined as the cryptographic boundary of the cryptographic module.

The Quadient Postal Security Device employs a tamper detection envelope designed to detect penetration attempts and a response mechanism that will zeroize all plaintext Sensitive Security Parameters.

Physical Security Mechanism	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
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 13: Physical Security Inspection Guidelines

Quadient Postal Security Device was designed to securely operate when voltage supplied to the module is between 9.6V and 15.6V and the environmental temperature is between -30°C and 84°C.
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.

	Temperature or voltage measurement	EFP / EFT	Specify if this condition results in a shutdown or zeroisation
Low temperature	-30°C	EFT	The PSD ceases operation
High temperature	+84°C	EFP	Zeroization
Low voltage	9.6V	EFT	Undervoltage protection (infinite while loop)
High voltage	15.6V	EFT	Overvoltage protection

Table 14: EFP/EFT

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.

8. Non-invasive security

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

9. Sensitive security parameters management

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use & related keys
Master Secret Key	128	AES CBC 128 bits (Cert. #A728)	Internally: DRBG	N/A	N/A	Plaintext in volatile memory protected by tamper response mechanism	- Invocation of "Zeroize SSPs" service; - Breach of flex circuit triggers "Zeroize SSPs" service; - PSD temperature over 84°C triggers "Zeroize SSPs" service (EFP measure);	Internally encrypt & decrypt PSDs critical security parameters.
DRBG entropy input	128	ESV (Cert. #E58)	Internally: Entropy Source	N/A	N/A	Plaintext in volatile memory protected by tamper response mechanism	Invocation of "Zeroize SSPs" service; - Breach of flex circuit triggers "Zeroize SSPs" service; - PSD temperature over 84°C triggers "Zeroize SSPs" service (EFP measure);	Input to DRBG.
DRBG parameters – Key & V	128	CTR DRBG using AES 128 (Cert. #A2930)	Internally: Entropy Source	N/A	N/A	Plaintext in volatile memory protected by tamper response mechanism	Invocation of "Zeroize SSPs" service; - Breach of flex circuit triggers "Zeroize SSPs" service; - PSD temperature over 84°C triggers "Zeroize SSPs" service (EFP measure);	Internal state of DRBG.
PSD TLS Communication Private Key	112	RSA PKCS #1 v1.5 2048 bits (Cert. #A765)	Internally: FIPS186-4 KEYGEN	N/A	N/A	Encrypted (w/Master Secret)	Rendered unusable by zeroization of "Master Secret"	Authenticates messages and data output from the PSD during TLS Handshake protocol.

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use & related keys
PSD TLS Communication Public Key	112	RSA PKCS #1 v1.5 2048 bits (Cert. #A765)	Internally: FIPS186-4 KEYGEN	Export	N/A	Plaintext	Invocation of "Zeroize SSPs" service;	The key resides in a signed X509 certificate used for authentication by the cryptographic module to the Base/Field server/Postal Server.
TLS DH Private Key	112	Diffie-Hellman 224 bits	Internally: DRBG	N/A	N/A	N/A	Immediately after use (i.e., TLS-pre-master key establishment)	Diffie-Hellman private key used to agree TLS pre-master.
TLS DH Public Key and Public parameters	112	Diffie-Hellman 2048 bits	Internally: SP 800-56Ar3	Export	SP 800-56Ar3	N/A	Immediately after use (i.e., TLS-pre-master key establishment)	Diffie-Hellman Public Key (Y) and Public parameters (p, g, Y) used during TLS handshake to agree upon a TLS pre-master secret. DH Public Key is relevant when the module acts as an initiator whereas DH Public parameters are relevant when the module acts as a responder.
TLS pre-master key	256 bytes	KAS-SSC (Cert. #A2929)	Internally	N/A	KAS-SSC	N/A	Immediately after use	TLS Private and Public Keys
TLS master key	48 bytes	TLS KDF (Cert. #A761)	Internally	N/A	TLS KDF	N/A	TLS session closure	Used to derive the keys used by TLS Record Protocol (TLS Communication Secret Keyset).
TLS Communication Secret Keyset	128	AES CBC: 2 x 128 bits (Cert. #A728); HMAC-SHA-256: 2 x 256 bits (Cert. #A730).	Internally	N/A	TLS KDF	N/A	TLS session closure	Encrypt & Decrypt & Integrity TLS Communication.
Indicia Authentication Secret Key	160 or 256 or 128	HMAC-SHA-1 (160 bits key)[3] (Cert. #A729)	Internally	Export	KTS and	Encrypted (w/Master Secret)	Rendered unusable by zeroization of "Master Secret"	Indicia authentication (dependent on country configuration).

[3] Netherlands

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use & related keys
		or HMAC-SHA-256 (256 bits key[4]) (Cert. #A729) or CMAC AES 128[5] (Cert. #A760)			TLS Communication Secret Keyset			
Indicia Authentication Private Key	112	ECDSA P224[6] or ECDSA P256[7] (Cert. #A2931)	Internally: DRBG	N/A		Encrypted (w/Master Secret)	Rendered unusable by zeroization of “Master Secret”	Indicia authentication (dependent on country configuration).
Indicia Authentication Public Key	112	ECDSA P224 or ECDSA P256 (Cert. #A2931)	FIPS 186-4 ECDSA KEYGEN	Export		Plaintext	Invocation of “Zeroize SSPs” service;	Indicia authentication (dependent on country configuration).
Root Public Key (Root Certificate)	112	RSA PKCS #1 v1.5 2048 *bits* (Cert. #A765)	Externally	Import	N/A	Plaintext	Invocation of “Zeroize SSPs” service;	Signed X509 Certificate of the Current Root Public key used for the verification of authenticated messages input from the Field server/Postal server/Base.
Previous Root Public Key (Previous Root Certificate)	112	RSA PKCS #1 v1.5 2048 bits (Cert. #A765)	Externally	Import	N/A	Plaintext	Invocation of “Zeroize SSPs” service;	Signed X509 Certificate of the Previous Root Public key used for the verification of authenticated messages input from the Field server/Postal server/Base.
Region Public Key (Region Certificate)	112	RSA PKCS #1 v1.5 2048 bits (Cert. #A765)	Externally	Import	N/A	Plaintext	Invocation of “Zeroize SSPs” service;	Signed X509 Certificate of the current Region Public key used for the verification of authenticated messages input

[4] UK
[5] Belgium
[6] USPS
[7] Canada

Key/SSP Name/Type	Strength	Security Function and Cert. Number	Generation	Import/ Export	Establishment	Storage	Zeroisation	Use & related keys
								from the Field server/Postal server/Base.
Utility Public Key (Utility certificate)	112	RSA PKCS #1 v1.5 2048 bits (Cert. #A765)	Externally	Import	N/A	Plaintext	Invocation of "Zeroize SSPs" service;	Signed X509 Certificate of the R&D Signer User for authentication of files loaded into module.
Field Server Public Key (Field Server Certificate)	112	RSA PKCS #1 v1.5 2048 bits (Cert. #A765)	Externally	Import	N/A	Plaintext	Invocation of "Zeroize SSPs" service;	Signed X509 Certificate of the Field Server used to authenticate the Field CO.
Postal Server Public Key (Postal Server Certificate)	112	RSA PKCS #1 v1.5 2048 bits (Cert. #A765)	Externally	Import	N/A	Plaintext	Invocation of "Zeroize SSPs" service;	Signed X509 Certificate of the Postal Server used to authenticate the Postal CO
Base Public Key (Base Certificate)	112	RSA PKCS #1 v1.5 2048 bits (Cert. #A765)	Externally	Import	N/A	Plaintext	Invocation of "Zeroize SSPs" service;	Signed X509 Certificate of the Base used to authenticate the Base User.
R&D Signer User Public Key (R&D Signer Certificate)	112	RSA PKCS #1 v1.5 2048 bits (Cert. #A765)	Externally	Import	N/A	Plaintext	Invocation of "Zeroize SSPs" service;	Signed X509 Certificate of the R&D Signer used to authenticate the R&D Signer User.

Table 15: SSPs

10. Self-tests

The Quadient Postal Security Device performs pre-operational (§10.1) and conditional self-tests (§10.20) without external control or operator intervention.

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:

- Firmware integrity test
- Critical security functions test

10.1.1. Firmware integrity test

The Quadient Postal Security Device verifies the integrity of its firmware using RSA 2048 with SHA-256. To ensure the validity of the underlying algorithm, the RSA 2048 signature verification known answer self-test is performed prior to performing the firmware integrity test.

At any time, the operator is able to initiate the firmware integrity test on demand.

10.1.2. Critical security functions test

The Quadient Postal Security Device performs the following pre-operational critical functions tests:

- Accessibility and validity test (16-bit EDC) of the following CSPs:
  - Master Secret Key
  - DRBG - Key & V
  - PSD TLS Communication Public Key
- Tamper detection test

If any of these CSP is not accessible (i.e., device failure) or contains erroneous data, the Quadient Postal Security Device enters an error state.

If the tamper detection test fails, the Quadient Postal Security Device enters an error state and zeroizes all plaintext CSPs.

10.2. Conditional self-tests

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

- Cryptographic Algorithm Self-Test (see 10.2.1), at power up
- RSA (2048) Pairwise Consistency Tests, at power up and when RSA key generation occurs
- ECDSA (P-224) Pairwise Consistency Tests, at power up and when ECDSA key generation occurs
- ECDSA (P-256) Pairwise Consistency Tests, at power up and when ECDSA key generation occurs
- KAS-SSC Assurances per SP 800-56Ar3 5.6.2 (Private Key Validation, Public Key Validation, and DH Pairwise Consistency Tests) at power up and when DH key generation occurs
- Firmware load test
- Conditional Critical Functions Test: SSPs accessibility and validity test (16-bit EDC), before their use

10.2.1. Cryptographic Algorithm Self-Tests

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

- AES (CBC 128) Encrypt KAT
- AES (CBC 128) Decrypt KAT
- AES (CMAC 128) KAT
- DRBG KATs (CTR-DRBG) (Instantiate KAT, Generate KAT, Reseed KAT)
- ECDSA (P-224) signature generation KAT
- ECDSA (P-224) signature verification KAT
- ECDSA (P-256) signature generation KAT
- ECDSA (P-256) signature verification KAT
- HMAC (SHA-1) KAT
- HMAC (SHA-256) KAT
- KAS-SSC KAT
- TLS-KDF (SHA-256) KAT
- RSA (2048) signature generation KAT
- RSA (2048) signature verification KAT
- SHA-1 KAT
- SHA-256 KAT

Entropy Source Continuous Tests, at power up and during the noise source operation:

- Repetition Count Test (ref. NIST SP 800-90B)
- Adaptive Proportion Test (ref. NIST SP 800-90B)

10.3. Periodic self-tests

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.

11. Life-cycle assurance

Quadient Technologies France is using 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 and configured for a specific country in manufacturing. The postal meter is then authorized and shipped to the end customer.

11.2. Administrator Guidance

The PSD TLS Communication RSA key pair is generated at the customization center during manufacturing.

The PSD TLS Communication key pair is generated internally, by the module itself.

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 Postal Server via a mutually authenticated TLS session and sends its certificate for certification. A new certificate chain is downloaded into the module to be used for communication with Quadient infrastructure (Postal Server) to access available services, during the operational phase.

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.

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 immediately zeroizes all plaintext CSPs.

13. Glossary

Abbreviation	Description
AES	Advanced Encryption Standard
CMAC	Cipher-based Message Authentication Code
CSP	Critical Security Parameter
DH	Diffie-Hellman key exchange (DHE Diffie Hellman Ephemeral)
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptic Curve Digital Signature Algorithm
EDC	Error Detection Code
EFP/EFT	Environmental Failure Protection /Testing
ESV	Entropy Source Validation
FIPS	Federal Information Processing Standards
HMAC	Hashed Message Authentication Code
KAS	Key Agreement Scheme
KAT	Known Answer Test
KDF	Key Derivation Function
KTS	Key Transport Scheme
NIST	National Institute of Standards and Technology
PSD	Postal Security Device
PKI	Public Key Infrastructure
RSA	Rivest Shamir Adleman
SFI	Security Function Implementation
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication
SSP	Sensitive Security Parameter
TLS	Transport Layer Security