Classification: External

Quadient Postal Security Device (PSD) Security Policy

Valid from:	15-10-2020
Version No.:	V 9.0

Contents

Figures

1 Introduction

This document forms a Cryptographic Module Security Policy for the Quadient Technologies France (former Neopost Technologies S.A.) Postal Security Device (PSD) under the terms of the FIPS 140-2 validation. This document contains a statement of the security rules under which the Quadient Technologies France (Quadient) PSD operates.

2 Cryptographic Module Specification

2.1 Quadient PSD Overview

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

The Quadient PSD (Figure 1) is a multi-chip embedded 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. The Quadient PSD was designed to securely operate when voltage supplied to the module is between +5V and +17V and the environmental temperature is between -30°C and 84°C.

Figure 1 – Quadient Postal Security Device

2.2 Quadient PSD Configuration

Quadient PSD (Cryptographic Module)			Description
Hardware P/N			A0014227-B and A0014227-C
Firmware P/N			A0134483A
Firmware Versions			a30.08
NIST Approved Security Functions	**ECDSA**	(Cert. #517)	A0038110A
	AES-CMAC	(Cert. #A760)	A0038111B
	SHS	(Cert. #A730)	A0038112B
	AES-CBC	(Cert. #A728)	A0038113B
	KDF (CVL)	(Cert. #A761)	A0038114B
	RSA	(Cert. #A765)	A0038115B
	DRBG	(Cert. #1835)	A0038116B
	HMAC	(Cert. #A729)	A0038118B
	DSA	(Cert. #A767)	A0136247A

Figure 2 – Quadient PSD Configuration

2.3 FIPS Security Level Compliance

The Quadient PSD is designed to meet the overall requirements applicable for Level 3 of FIPS 140-2.

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

Figure 3 – FIPS 140-2 Security Level

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). No parts of this protocol, other than the KDF, have been tested by the CAVP and CMVP.

2.5 Modes of Operation

The module supports both Approved and non-Approved modes of operation. 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 showing whether the module is in an Approved mode or non-Approved mode via the Get Status command (Read Status Data). This command returns either a 1 or 0 for Approved mode or non-Approved mode respectively.
In order to change modes of operation the module must be initialized for a specific country (this occurs in manufacturing). Therefore, it is impossible to share CSPs between modes of operation.

2.5.1 Approved Security Functions

The Quadient PSD supports the following FIPS Approved security functions in Approved Mode of Operation:

CAVP Cert.	Algorithm	Standard	Modes/Methods	Key Length, Curves or Moduli	Usage
A728	AES CBC	FIPS 197	CBC	128	Encryption/Decryption of: • CSPs for storage within the module • Data encryption/decryption using TLS v1.2
A760	AES CMAC	FIPS 197 SP 800-38B	AES	128	Indicia Authentication
Vendor affirmed	CKG	SP 800-133r2			The unmodified output of the DRBG is used for symmetric key and asymmetric seed generation
A761	KDF (CVL)	SP 800-135	SHA-256		TLS 1.2 KDF function
1835	CTR-DRBG	SP 800-90A	AES	128	Key generation

CAVP Cert.	Algorithm	Standard	Modes/Methods	Key Length, Curves or Moduli	Usage
A767	DSA	FIPS 186-4	KeyGen	(2048, 224)	Used for KAS-SSC
517	ECDSA	FIPS 186-4	SHA-256	P-224	Key Generation, Digital Signature Generation, and Digital Signature Verification (all for Indicia Authentication)
A729	HMAC-SHA-1, HMAC-SHA-256	FIPS 198-1	(Key Sizes Ranges Tested: KS<BS)	160, 256	TLS messages authentication, Indicia Authentication
Vendor affirmed	KAS-SSC	SP 800-56A r3	FFC DH	224	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 128 bits of encryption strength.
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
A730	SHS	FIPS 180-4	SHA-1, SHA-256	N/A	Hashing algorithm used for: • HMAC Generation • Digital signatures

Figure 4 – FIPS Approved Algorithms

2.5.2 Allowed Security Functions

The Quadient PSD supports the following FIPS Allowed security functions in Approved Mode of Operation:

Algorithms	Caveat	Use
NDRNG	Entropy source conformant to IG 7.15	Seeding for the DRBG (full 128-bit security strength)

Algorithms	Caveat	Use
RSA Key Wrapping (no security claimed)	No security claimed, per IG 1.23	CSP obfuscation

Figure 5 – FIPS Allowed Security Functions

2.5.3 Non-Approved Security Functions (non-Approved modes)

Some Postal Authorities/Standards may require implementation of non-FIPS Approved security functions (i.e. operation in a non-Approved mode of operation). For these specific firmware configurations, the Quadient PSD supports the following non-FIPS Approved security functions:

Algorithms	Use
SHS (SHA-1)	Hashing algorithm used for digital signature generation process: ECDSA P192 SigGen – non-compliant, cryptographic strength less than 112-bits (Postal Indicia Service – Canada Only)
ECDSA (P-192)	Digital Signature Generation – non-compliant, cryptographic strength less than 112-bits (Postal Indicia Service – Canada Only)
RSA (1536, SHA-1) PKCS1 v1.5	Digital Signature Verification per FIPS 186-2, validated under RSA Cert. #A765. FIPS compliant for Legacy verification, but is used only in a non-Approved mode of operation.
RSA (1024) PKCS1 v1.5	Key Wrapping – non-compliant, cryptographic strength less than 112-bits (Postal Core Services – Germany Only)

Figure 6 – Non-Approved Security Functions

3 Sensitive Security Parameters Management

3.1 Critical Security Parameters and Keys

Name	Algorithm/Size	Description	Generation	Storage	Distribution	Zeroization
Master Secret Key	AES CBC 128 bits	Internally encrypt & decrypt PSDs critical security parameters	Internally: DRBG	Plaintext in volatile memory protected by tamper response mechanism	N/A	- Invocation of “Zeroize CSPs” service; - Breach of flex circuit triggers “Zeroize CSPs” service; - PSD temperature over 84°C triggers “Zeroize CSPs” service (EFP measure); - Failure of a self-test triggers “Zeroize CSPs” service;
DRBG - Key	CTR DRBG using AES 128	Internal state of DRBG.	Internally: NDRNG	Plaintext in volatile memory protected by tamper response mechanism	N/A	
DRBG - V	CTR DRBG using AES 128	Internal state of DRBG.	Internally: NDRNG	Plaintext in volatile memory protected by tamper response mechanism	N/A	
TLS Communication Private Key	RSA PKCS #1 v1.5 2048 bits	Authenticates messages and data output from the PSD during TLS Handshake protocol.	Internally: FIPS186-4 KEYGEN	Encrypted (w/Master Secret)	N/A	Rendered unusable by zeroization of “Master Secret”
Indicia Authentication Secret Key	HMAC-SHA-1 (160 bits key) or HMAC-SHA-256 (256 bits key) or CMAC AES 128	Indicia authentication (dependent on country configuration)	Internally: DRBG	Encrypted (w/Master Secret)	TLS Communication Secret Keyset	Rendered unusable by zeroization of “Master Secret”
Indicia Authentication Private Key	ECDSA P224	Indicia authentication (dependent on country configuration)	Internally: DRBG	Encrypted (w/Master Secret)	N/A	Rendered unusable by zeroization of “Master Secret”

Figure 7 – Critical Security Parameters

Name	Algorithm/Size	Description	Generation	Storage	Distribution	Zeroization
DH private key (TLS Handshake)	Diffie-Hellman 224 bits	Diffie-Hellman private key used to agree TLS pre-master	Internally: DRBG	N/A	N/A	Immediately after use (i.e. TLS-pre-master key establishment)
TLS pre-master key	256 bytes	Pre-master secret	KAS-SSC	N/A	N/A	Immediately after use
TLS master key	48 bytes	Used to derive the keys used by TLS Record Protocol (TLS Communication Secret Keyset)	Approved TLS KDF	N/A	N/A	TLS session closure

Figure 8 – TLS v1.2 Handshake Protocol Critical Security Parameters

Name	Algorithm/Size	Description	Generation	Storage	Distribution	Zeroization
TLS Communication Secret Keyset (TLS Record Protocol Keys)	AES CBC: 2 x 128 bits; HMAC-SHA-256: 2 x 256 bits	Encrypt & Decrypt & Integrity TLS Communication	Approved TLS KDF	N/A	N/A	TLS session closure

Figure 9 – TLS v1.2 Record Protocol Critical Security Parameters

The CSPs are protected from unauthorized disclosure, modification and substitution.
The plaintext CSPs are stored in the tamper protected memory. All other CSPs are stored encrypted by the Master Secret Key.
The Quadient PSD detects data corruption of the value held for any particular CSP by the incorporation of 16-bit error detection code. Any CSPs access failure causes the zeroization of tamper protected memory.
The Quadient PSD never output the CSPs in plaintext.

3.2 Public Security Parameters and Keys

Name	Algorithm/Size	Description	Generation	Storage
Root Public Key (Quadient Root Certificate)	RSA PKCS #1 v1.5 2048 bits	Signed X509 Certificate of the current Root Public key used for the verification of authenticated messages input from the Quadient server	N/A	Plaintext
Previous Root Public Key (Quadient	RSA PKCS #1 v1.5 2048 bits	Signed X509 Certificate of the next Root Public key used for the verification of authenticated messages input from the Quadient server.	N/A	Plaintext

Name	Algorithm/Size	Description	Generation	Storage
Previous Root Certificate)				
Region Public Key (Quadient Region Certificate)	RSA PKCS #1 v1.5 2048 bits	Signed X509 Certificate of the current Region Public key used for the verification of authenticated messages input from the Quadient server.	N/A	Plaintext
Postal Core Server public key	RSA PKCS #1 v1.5 2048 bits	Signed X509 Certificate of the Postal Core Server	N/A	Plaintext
Base (Postage Meter) public key	RSA PKCS #1 v1.5 2048 bits	Signed X509 Certificate of the Postage Meter	N/A	Plaintext
Utility public key	RSA PKCS #1 v1.5 2048 bits	Signed X509 Certificate of the File Signer Tool	N/A	Plaintext
TLS Communication Public Key (Quadient PSD Certificate)	RSA PKCS #1 v1.5 2048 bits	Used to authenticate messages and data output from the Quadient PSD (TLS Handshake protocol). The key resides in a signed X509 certificate used for authentication by the cryptographic module to the Quadient server.	FIPS 186-4 RSA KEYGEN	Plaintext
TLS Diffie-Hellman Public Parameters	KAS-SSC: Diffie-Hellman 2048 bits	Diffie-Hellman parameters (p, g, Y) used during TLS handshake to agree upon a TLS premaster secret.	SP 800-56Ar3 or N/A	Plaintext
Indicia Authentication Public Key	ECDSA P224	Indicia authentication	FIPS 186-4 ECDSA KEYGEN	Plaintext

Figure 10 – Public Security Parameters

All public keys are protected from unauthorized modification and substitution.

3.3 Status Indicator

A status indicator will be output by the Quadient PSD via the status output interface. It consists of a unique text message which will be displayed on the franking machine User Interface.
The following module states are indicated:

- CSPs zeroed
- Private/Public key pairs invalid (module not initialized)
- Tamper mechanism tampered
- Power Up tests error
- DRBG error
- High temperature detected error

- Conditional test error
    - ECDSA Pairwise Consistency
    - RSA Pairwise Consistency
    - KAS-SSC Pairwise Consistency Tests
- FIPS Approved Mode

The absence of one of these messages indicates that the module is in a ‘ready’ state

4 Ports and Interfaces

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

- power interface
- data input interface
- data output interface
- control input interface
- status output interface

PIN	Description	Interface Type
1	Ground	
2	Ground	
3	RX	Data Input/Control Input
4	RX	Data Input/Control Input
5	TX	Data Output/Status Output
6	TX	Data Output/Status Output
7	Power (5V – 17V)	Power
8	Power (5V – 17V)	Power
9	Ground	
10	Ground	

Figure 11 – 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.

5 Roles, Services and Authentication

The Quadient PSD supports authorized roles for operators and corresponding services within each role. In order to control access to the module the Quadient PSD employs identity-based authentication mechanism.

The Quadient PSD supports the following operators:

- **Quadient Administrator (Field Server)**: The Crypto-Officer can assume the following Crypto-Officer roles:
    - Postal User
    - Field Crypto-Officer
    - Postal Crypto-Officer
    - Root
    - Region

  The Quadient Administrator authenticates to the module via digitally signed X509 certificates using the TLS v1.2 Handshake protocol.
- **Customer (Base)**: is the end user of the cryptographic module and can assume one User Role: the Printing Base role. The Quadient Administrator authenticates to the module via digitally signed X509 certificates using the TLS v1.2 Handshake protocol.
- **R&D File Signer Tool**: assumes the R&D Signer role and is authenticated via signed X509 certificates. This role allows the Quadient PSD to authenticate and use additional external files.
- **Expertise Tool**: assumes an unauthenticated User Role.

5.1 Approved Services

OPERATOR	ROLES	SERVICES	CSP ACCESS MODE
Quadient Administrator	Postal User	Postal User Services	N/A
		Read Status Data	N/A
		Read Part Number	N/A
		TLS Handshake	(Write/Read) DRBG parameters (V, Key), DH Private Key, TLS pre-master key, TLS master key, TLS communication secret keyset
	Field Crypto-Officer	Generate PKI Key	(Write/Read) Master Secret Key, DRBG parameters (V, Key), TLS Communication private key & secret keyset
		Get/Set PKI Certificate	N/A
		Read Status Data	N/A
		Read Part Number	N/A
		TLS Handshake	(Write/Read) DRBG parameters (V, Key), DH Private Key, TLS pre-master key, TLS master key, TLS communication secret keyset
	Postal Crypto-Officer	Generate Stamp Key	(Write) Indicia Authentication Key(s) (Secret or Private) (Write/Read) DRBG parameters (V, Key)
		Set Stamp Key	(Write) Indicia Authentication Key(s) (Secret)
		Generate Transport Key	(Write/Read) DRBG parameters (V, Key)
		TLS Handshake	(Write/Read) DRBG parameters (V, Key), DH Private Key, TLS pre-master key, TLS master key, TLS communication secret keyset
	Root	Verify Region Certificate	N/A
		Verify Root Certificate	N/A
	Region	Verify Device Certificate	N/A
Customer	Printing Base (User)	Initiate/End Postal Core Connection	(Write) TLS Communication private key (Write) TLS Communication secret keyset
		Initiate/End Rekey Connection	(Write) TLS Communication private key (Write) TLS Communication secret keyset

OPERATOR	ROLES	SERVICES	CSP ACCESS MODE
		Postal Indicia	(Read) Indicia Authentication Key(s) (Secret or Private)
		Other Base Services	N/A
		Read Status Data	N/A
		Read Part Number	N/A
		TLS Handshake	(Write/Read) DRBG parameters (V, Key), DH Private Key, TLS pre-master key, TLS master key, TLS communication secret keyset
File Signer Tool	R&D Signer	Verify Files	N/A
Expertise Tool	Unauthenticated User role	Read Status Data	N/A
		Read Part Number	N/A
		Zeroize CSP	(Zeroize) Master Secret Key and DRBG parameters (V, Key)
All	All	Invoke Tests	N/A

Figure 12 – Approved Roles, Services, Operators

5.2 Non-Approved Services

The module provides the same roles and services in non-approved and approved modes.

The non-approved mode specificities are highlighted in the table below:

OPERATOR	ROLES	SERVICES	DIFFERENCE IN SERVICE
Quadient Administrator	Postal Crypto-Officer	Generate Stamp Key	Canadian configuration: ECDSA P-192 with SHA-1 is used for Indicia Authentication Private Key/Public Key German configuration: Service is not available
		Set Stamp Key	Canadian configuration: Service is not available German configuration: RSA 1024 key wrapping with SHA-1 is used (m-secret)
		Generate Transport Key	German configuration: RSA 1024 key wrapping with SHA-1 is used (for m-secret)

OPERATOR	ROLES	SERVICES	DIFFERENCE IN SERVICE
Quadient Administrator or Customer	Postal User, Field Crypto-Officer, Postal Crypto-Officer, or Printing Base (User)	TLS Handshake	French configuration; RSA 1536 SigVer may be used to verify the signature of the TLS partner
Customer	Printing Base (User)	Postal Indicia	Canadian configuration: ECDSA P-192 with SHA-1 is used for Indicia Authentication Private Key/Public Key German configuration: RSA 1024 key wrapping with SHA-1 is used (for m-secret)

Figure 13 – Non-Approved Roles, Services, Operators

5.3 Operator Authentication

The mutual authentication between the Customer / Quadient Administrator and the Quadient PSD 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 the 1 in 1,000,000 requirement.
- 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 the 1 in 100,000 requirement.

6 Operational Environment

The cryptographic module's operational environment is non-modifiable.

7 Physical Security

The Quadient PSD is designed to meet FIPS 140-2 Level 3 + EFP/EFT Physical Security requirements.

The Quadient PSD defined as a multi-chip embedded cryptographic module includes a non-removable enclosure that comprises a hard epoxy resin with an outer plastic casing. The non-removable enclosure and epoxy resin was tested and verified to be effective within the environmental operational range of the module (environmental temperature between -30°C and 84°C). No assurance is provided for Level 3 hardness conformance at any temperature outside this range.

The Quadient PSD employs a tamper detection envelope designed to detect penetration attempts, and a response mechanism that will zeroize all plaintext Critical Security Parameters.
The outer plastic casing is defined as the cryptographic boundary of the cryptographic module. It is inspected for tampering each time the module is returned to Quadient manufacturing or for servicing.

The module mitigates environmental attacks by employing a high temperature fuse for the EFP circuitry such that when the module temperature exceeds 84°C, the module will zeroize all plaintext CSPs.

8 Self-Tests

The Quadient PSD performs power up and conditional self-tests. The Quadient PSD inhibits the data output interface during the self-tests. The module can exercise the power-up self-tests, from within any role, at any time by power-cycling the module.

8.1 Power Up Self-Tests

8.1.1 Cryptographic Algorithm Tests

Upon power-up the Quadient PSD performs the following cryptographic algorithm self-tests without operator intervention:

- 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) sign generation KAT
- ECDSA (P-224) signature verification KAT
- HMAC (SHA-1) KAT
- HMAC (SHA-256) KAT
- KAS-SSC KAT per IG D.8
- TLS-KDF (SHA-256) KAT
- RSA (2048) signature generation KAT
- RSA (2048) signature verification KAT
- SHA-1 KAT
- SHA-256 KAT

If a cryptographic algorithms self-test fails, the Quadient PSD enters in error state and zeroizes all plaintext CSPs.

8.1.2 Firmware Integrity Tests

The Quadient PSD tests the contents of its program memory area at power up by calculating the hash (SHA-256) of the contents and comparing the result with a known answer. If the test fails, the Quadient PSD enters an error state and zeroizes all plaintext CSPs.

8.1.3 CSP Integrity Tests (Critical Function Test)

For the RAM CSPs integrity test, the Quadient PSD tests the accessibility and validity of all keys and CSP values in non-volatile memory at power up. If any are not accessible (i.e. device failure) or contain erroneous data (16-bit EDC fails) then the Quadient PSD enters an error state and zeroizes all plaintext CSPs.

The Quadient PSD also performs the following tests:

- RAM Integrity test (16-bit EDC)
- Tamper Detection test

8.2 Conditional Self-Tests

The PSD performs the following conditional self-tests:

- RSA (2048) Pairwise Consistency Tests
- ECDSA (P-224) Pairwise Consistency Tests
- KAS-SSC Assurances per SP 800-56Ar3 5.6.2 (Private Key Validation, Public Key Validation, and DH Pairwise Consistency Tests)
- NDRNG Continuous Tests:
  - Repetition Count Test (ref. SP 800-90B)
  - Adaptive Proportion Test (ref. SP 800-90B)
- DRBG Continuous test per AS.09.42

9 Design Assurance

Quadient Technologies is using the Windchill configuration management system to manage product configurations (including the cryptographic module).

All firmware implemented within the cryptographic module has been implemented using a high-level language (C), except for the limited use of assembly language where it was essential for performance.

10 Mitigation of Other Attacks

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

11 Glossary

Abbreviation	Description
AES	Advanced Encryption Standard
CMAC	Message Authentication Code
CSP	Critical Security Parameter
DH	Diffie-Hellman key exchange (DHE Diffie Hellman Ephemeral)
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptical Curve Digital Signature Algorithm
EFP/EFT	Environmental Failure Protection /Testing
EMI/EMC	Electromagnetic Interference/Compatibility
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
NIST	National Institute of Standards and Technology
NDRNG	Non-deterministic Random Number Generator
PSD	Postal Security Device
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
TLS	Transport Layer Security

12 Revision History

Version	Date	Revision Description
0.1	11/04/2014	Original document
1.0	22/08/2014	Update after review with Penumbra Security
2.0	28/08/2014	[Penumbra]Added additional tests performed (Ram integrity, Tamper test)
3.0	16/03/2015	[Penumbra]Added clarifications per CMVP comments
4.0	07/09/2017	[Neopost]Updated document template (new brand)
5.0	10/10/2017	[Neopost] Added new hardware and firmware version; increased RSA Key size to 2048 (Key Wrapping) for Belgium; added approved FIPS mode
6.0	14/12/2017	[Penumbra] Updated DRBG certificate; added clarifications
7.0	22/03/2018	[Penumbra] Specified CKG; added minor clarifications
8.0	23/05/2018	[Penumbra] Specified additional firmware version
9.0	15/10/2020	[Quadient] Updated document template (Quadient brand) ; Updated firmware versions (updated matrix SSL library and implemented KAS-SSC per NIST SP 800-56A)