FIPS 140-2 Non-Proprietary Security Policy

Postal NRevenector GB 2019

Document Version 1.0

Hardware P/N: 58.0036.0301.00 or 58.0036.0302.00

Firmware Version:

Bootloader: *90.0036.0401.00/**2019141001***

*GB Application: 90.0036.0415.00/**2019366001***

FP InovoLabs GmbH
Prenzlauer Promenade 28
13089 Berlin
Germany

fp-francotyp.com

THIS DOCUMENT MAY BE FREELY REPRODUCED AND DISTRIBUTED

Contents

Figures

Tables

1 Introduction

1.1 Overview

Figure: 1 *Postal NRevenector GB 2019*

FP InovoLabs GmbH is a wholly-owned subsidiary of Francotyp-Postalia Holding AG (FP), one of the leading global suppliers of mail center solutions. A major component of FP's business is the production and support of postal franking machines (postage meters). FP InovoLabs GmbH is responsible for developing these postal franking machines for FP.

Each postal franking machine incorporates a postal security device (PSD) that performs all postage meter cryptographic and postal security functions and which protects both Critical Security Parameters (CSPs) and Postal Relevant Data Items (PRDIs) from unauthorized access. The *Postal NRevenector GB 2019* is FP's latest generation of PSD.

This document forms a Cryptographic Module Security Policy for the cryptographic module of the device under the terms of the NIST FIPS 140-2 validation. This Security Policy specifies the security rules under which this device operates, and covers both the operation of the bootloader and the postal application.

1.2 Implementation

The *Postal NRevenector GB 2019* is a multiple-chip embedded cryptographic module, based around a cryptographic integrated circuit, together with a small number of support components. The components, mounted on a PCB, are covered by hard opaque potting material. The extent of the potting forms the cryptographic boundary of the module. The module has a proprietary electrical connector forming the interface to it. The module does not contain a modifiable operational environment.

2 Cryptographic Module Specification

2.1 FIPS Security Level Compliance

The cryptographic module is designed to meet FIPS 140-2 as shown in the table below:

Section	Security Requirement	Level
1	Cryptographic Module Specification	3
2	Cryptographic Module Ports and Interfaces	3
3	Roles, Services and Authentication	3
4	Finite State Model	3
5	Physical Security	3 + EFP
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC)	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	3

Table 1: FIPS 140-2 Security Levels

3 Cryptographic Ports and Interfaces

The cryptographic module ports and interfaces are as indicated in Table 2.

External Port	Interface Type	Description
36-pin Serial IO card edge connector	Data input Data output Control input Status output Power input	Interface for communicating with module
USB Port (disabled for version 58.0036.0302.00)	Data input Data output Control input Status output Power input	Alternate interface for communicating with module
Status LEDs (ERR, BL, PWR, APP)	Status output	• ERR: error • BL: Bootloader running • PWR: internal power supply on • APP: Application running
Battery	Power input	Additional power supply for module.

Table 2: Cryptographic Ports & Interfaces

3.1 Cryptographic boundary

The cryptographic boundary is defined to be the outer edge of the epoxy that covers most of the printed circuit board, as shown below.

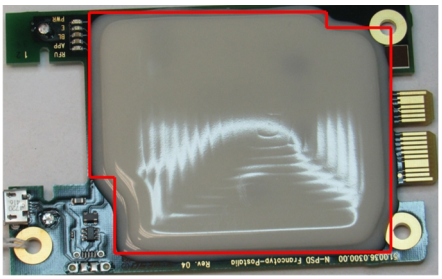

Figure: 2 Module Boundary (Outer Edge of Epoxy)

There are a small number of components on the printed circuit board that lie outside the cryptographic boundary, which may or may not be present depending on the build version of the device. These components have no impact on security-related aspects of the module.

4 Rules of Operation

4.1 FIPS 140-2 Related Security Rules

The *Postal NRevenector GB 2019* shall:

1. Support only an Approved mode of operation. The Approved mode indicator is returned via the Get Device Status service.
2. Not allow unauthenticated operators to have any access to the module's cryptographic services.
3. Inhibit data output during self-tests and error states.
4. Logically disconnect data output from the processes performing zeroization and key generation.
5. Enforce identity-based authentication for roles that access Approved algorithms and CSPs.
6. Not retain the authentication of an operator following power-off or reboot.
7. Support the following roles: Default User, User, and Cryptographic Officer.
8. Not permit the output of plaintext cryptographic keys or other CSPs.
9. Not support a bypass mode or maintenance mode.
10. Support the following logically distinct interfaces:
    - Data input interface
    - Data output interface
    - Control input interface
    - Status output interface
    - Power interface.
11. Implement all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
12. Protect critical security parameters from unauthorized disclosure, modification and substitution.
13. Provide means to ensure that a key entered into or stored within the device is associated with the correct entities to which the key is assigned.
14. Support a FIPS approved deterministic random bit generator (DRBG) as specified in NIST SP 800-90a section 10.2.1
15. Perform self-tests as listed in section 9 during power-on and on-demand when the corresponding service is used.
16. Store an error indication whenever an error state is entered. As a result, the error indication can be read by the Get Device Status Service.
17. Not perform any cryptographic functions while in an error state.
18. Not support multiple concurrent operators.
19. Ensure that no more than 2^{16} data block encryptions are performed using the same key during Triple-DES encryptions, in accordance with NIST Implementation Guideline for FIPS 140-2 §A13.

4.2 Postal Related Security Rules

Based on the specifications of the Royal Mail (RM), the *Postal NRevenector GB 2019* shall:

1. Comply with the specifications of the Royal Mail for the Mailmark™ franking system.
2. Protect the postal registers against unauthorized substitution or modification.
3. Never zeroize the postal registers.
4. Provide mechanisms to disable the Accounting-Service when it has no connection with its partnering infrastructure on a regular basis.
5. Provide mechanisms to re-key the indicia key on a regular basis
6. Provide services for protecting postal related data inside its hosting system against unauthorized substitution or modification.

5 Roles, Services, Authentication & Identification

5.1 Roles

The *Postal NRevenector GB 2019* supports three distinct roles:

- Default User
- User
- Cryptographic Officer

Any services which do not read, update, modify or generate critical security parameters (CSPs) do not require authentication.

5.2 Default User Role

By default, the device enters the *Default user* role, which is an unauthenticated role, for services that do not require authentication. The Host System typically acts on behalf of the Default operator and can request unauthenticated services.

5.3 User Role

The *User* is authenticated using an identity-based authentication method. This method is based on a challenge-response protocol using a User ID (UID) and secret passphrase known to both parties (pre-loaded into the module). The Host System typically acts on behalf of the User and can request authenticated services (which may access critical security parameters).

5.4 Cryptographic Officer Role

The *Cryptographic Officer* is authenticated using an identity-based authentication method in the form of an RSA 2048 digital signature. The *Cryptographic Officer* presents a 2048-bit RSA digital signature, which is verified by the module's corresponding public key (PKM public key). After authentication, key agreement is used to generate ephemeral session keys (RSEK and RSAK). The ephemeral session keys (3-Key Triple DES and HMAC-SHA-1) are then used additionally to authenticate several further messages that require CO authentication during that session and to secure the Indicia Key.

The Cryptographic Officer role shall provide those services necessary to initialize, authorize and validate the *Postal NRevenector GB 2019*. This role provides those services which enter, modify or generate critical security parameters.

An infrastructure server belonging to FP typically acts on behalf of a Cryptographic Officer.

5.5 Services and Roles

The following services are offered by the cryptographic module; the abbreviations used in the table are:

- Roles: U = User, DU = Default User, CO= Cryptographic Officer
- Access Rights: R = read, W = write, Z = zeroize, G = generate

Service	Approved Security Functions Used	Associated CSPs	Access Rights	Roles	Note
(All services that access CSPs)	AES 128 CTR AES 128 CBC HMAC-SHA-256	MKEK NVDEK NVDAK	R R R	CO, DU, U	The module automatically encrypts, decrypts, and authenticates stored critical security parameters. Operators do not have read access to these CSPs.
Accounting	HMAC-SHA256	Indicia Key	R	U	Debits the postal funds and returns indicia content.
Echo	None	None	-	DU	Echoes back data payload.
Generate Indicia Key	HMAC-SHA256, 3TDES CBC, HMAC-SHA1, DRBG	Indicia Key RSEK RSAK DRBG State[1]	G,W R R R,W,G	CO	Generating and re-keying indicia key
Get Device Status	None	None	-	DU	
Local Login	DRBG	Passphrase DRBG State	R R,W,G	DU	The passphrase is used for authentication as part of a 3-way challenge response protocol.
Logoff	None	None	-	CO, U	Leaves the CO or User role.
Postage Value Download	3TDES CBC, HMAC-SHA1	RSEK RSAK	R R	CO	Finance service, managing postal funds
Postage Value Refund	3TDES CBC, HMAC-SHA1	RSEK RSAK	R R	CO	Finance service, managing postal funds.
Postal Authorization	HMAC-SHA1	RSAK	R	CO	Authorize the device according to the Royal Mail requirements.
Postal Initialization	RSA 2048 Sign/Verify using SHA-256, 3TDES CBC, HMAC-SHA1, DRBG	PSD Key (private) RSEK RSAK DRBG State	G,W R R R,W,G	CO	Initialize the device according to the Royal Mail Mailmark and IPMAR requirements.
Program Flash with firmware	RSA 2048 Verify using SHA-256	None	-	U	Receives firmware from an external source and programs it into the cryptographic module's FLASH memory.
Re-Authorization	HMAC-SHA1	RSAK	R	CO	Updates customer configuration data
Re-Initialization	HMAC-SHA1	RSAK	R	CO	Updates postal configuration data
Reboot Device	None	None	-	DU	Service to cause the device to reboot.
Reenter FP Mac Secret	3TDES CBC, HMAC-SHA1	RSEK RSAK	R R	CO	Enters FP Mac Secret used to authenticate proprietary data

[1] DRBG State may include the following CSPs: Entropy string, DRBG seed, DRBG state: Key, and DRBG State: V

Service	Approved Security Functions Used	Associated CSPs	Access Rights	Roles	Note
Rekey PSD key	RSA 2048 Sign/Verify using SHA-256, 3TDES CBC, HMAC-SHA1, DRBG	PSD Key (private) RSEK RSAK DRBG State	G,W R R R,W,G	CO	Generation of a new PSD Key Pair and exchange with the PKM
Remote Login	KAS/KDF, DSA Key Generation, RSA 2048 Sign/Verify using SHA-256, 3TDES CBC, HMAC-SHA1, DRBG	Ephemeral DH private key Transport Key[2] (private) PSD Key (private) RSEK RSAK DRBG State	G,W,R R R G,W,R G,W,R R,W,G	DU	Required to enter the CO role.
Renew PKM key	RSA 2048 Verify using SHA-256	None	-	CO	Loads signed PKM certificate
Scrap	None	MKEK NVDEK NVDAK DRBG State	Z Z Z Z	DU	Zeroizes all plaintext CSPs.
Secure Echo	3TDES CBC, HMAC-SHA-1	RSEK RSAK	R R	CO	Echoes back data payload within a secure session.
Secure Get Status	HMAC-SHA-1	RSAK	R	CO	Provides status within a secure session.
Secure Set Time	HMAC-SHA-1	RSAK	R	CO	Synchronizes the RTC within a secure session.
Select Programmed Firmware	None	None	-	DU	Configures the bootloader.
Self-Test	All listed in section 9	None	-	DU	
Setup Parameter	None	None	-	DU	Enters postal configuration data.
Sign PMD Data	RSA 2048 Sign using SHA-256	PMD Key (private)	R	U	Sign postal related items and communication data.
Verify Mac	None	None	-	U	Authenticates a data payload (using FP Mac Secret).

Table 3: Services and Roles

5.6 Authentication Strength

5.6.1 Cryptographic Officer Role

The probability that a random attempt will succeed or a false acceptance will occur shall be less than one in 1,000,000. This is achieved through use of a 2048-bit RSA key to authenticate the role, which has been determined to have an effective strength of 112 bits. The probability that a random attempt will succeed is therefore $1/(2^{112})$, which is less than 1/1,000,000.

Should multiple attempts be made to authenticate during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur. This is

[2] The Transport Key Pair is used once during initialization, then replaced by the PSD Key Pair on subsequent Remote Logins

achieved by inserting a delay of 1 second after any failed attempt resulting in a maximum of 60 attempts per minute. The probability is therefore $60/(2^{112})$, which is less than 1/100,000.

5.6.2 User Role

The passphrase contains at least 6 randomly chosen characters for the *User* resulting in a total of more than 62^6 combinations (here, 62 represents the complete set of 26 upper- and 26 lower-case ASCII letters, together with 10 digits). The probability that a random attempt will succeed is therefore $1/(62^6)$, which is less than 1/1,000,000.

Should multiple attempts be made to authenticate during a one-minute period, the probability shall be less than one in 100,000 that a random attempt will succeed or a false acceptance will occur. This is achieved by inserting a delay of 1 second after any failed attempt resulting in a maximum of 60 attempts per minute. The probability is therefore $60/(62^6)$, which is less than 1/100,000.

6 Physical Security

All the components of the device are covered with a hard, tamper-evident potting material, which is tamper evident and opaque within the visible spectrum. The module is inspected for tamper evidence each time it is retrieved from the field. Because of the potting material it is not possible to physically access any internal components without seriously damaging the module or causing zeroization. Hardness testing was performed at ambient temperature and at the extremes of the module's documented operating temperature range (-12 ˚C to 72 ˚C).

7 Cryptographic Functions

7.1 Modes of Operation

The module has one mode of operation, the FIPS mode of operation. Once the module has completed its self-test and entered its FIPS mode of operation, the LED marked "APP" will light on the printed circuit board. This LED will extinguish when the module is re-booted, for example to restart the FP Bootloader. Additionally, the Approved mode indicator is returned via the Get Device Status service.

7.2 Approved Algorithms

The module implements the following FIPS approved algorithms:

Algorithm	Standard	Mode/ Method	Key Lengths, Curves or Moduli	CAVP Cert.	Use
AES	FIPS 197, SP 800-38A	ECB, CBC, CTR	128	#5662	Data encryption / decryption
CKG	SP 800-133			Vendor affirmed	The unmodified output of the DRBG is used for symmetric key generation and seeds for asymmetric generation
DRBG	SP 800-90A & SP 800-90B	CTR-DRBG: Block Cipher DF	128	#2497	Deterministic random bit generation
DSA	FIPS 186-4		(2048, 224)	#1455	Key generation only for KAS
HMAC	FIPS 198-1	HMAC-SHA-1 HMAC-SHA-256	160 128, 256	#3769	Message authentication MAC Calculation for the indicia
KAS-SSC	SP 800-56Ar3	dhEphem, C(2e, 0s, FFC DH)	(2048, 224)[3]	Vendor affirmed	Key Agreement: Shared Secret Computation (key establishment methodology provides 112 bits of encryption strength)
KDA	SP 800-56Cr1	Single-Step KDF	SHA-256	Vendor Affirmed	Key Agreement: Key Derivation Function
KTS	SP 800-38F	3TDES CBC HMAC-SHA-1	192 bits 160 bits	Triple-DES Cert. #2839 and HMAC Cert. #3769	Key Transport Scheme (key establishment methodology provides 112 bits of encryption strength)
RSA	FIPS 186-4	KeyGen PKCS 1.5 SigGen PKCS 1.5 SigVer PKCSPSS SigVer	(2048) (2048, SHA-256) (2048, SHA-256) (2048, SHA-256)	#3046	Key Generation, Digital signature generation and verification
SHS	FIPS 180-4	SHA-1 SHA-256		#4538	Message digest
TDES	SP 800-67r2	ECB, CBC	192	#2839	Data encryption / decryption

Table 4: FIPS 140-2 Approved Security Functions

7.3 Allowed Algorithms

The module uses a single hardware implemented NDRNG for seeding the DRBG. The NDRNG is allowed, but not FIPS approved. The NDRNG is used as the entropy source for the module's DRBG, which is seeded with full entropy (security strength of 128 bits).

[3] 186-type FFC primes

7.4 Allowed Algorithms (Not Security Functions)

The following algorithms may be used in the Approved mode of operation because they are considered non-approved cryptographic algorithms that are not security functions per IG 1.23. Data secured with these algorithms is considered plaintext.

Algorithm	Caveat	Use
AES	(no security claimed)	Proprietary implementation used for obfuscation of data that remains within the module.
FP MAC	(no security claimed)	Proprietary implementation used for non-compliant legacy verification of non-security relevant data.
KDF	(no security claimed)	Proprietary implementation used to derive non-compliant keys used for obfuscation in the Local Login challenge-response protocol. This algorithm is compliant with FIPS 140-2 requirements for authentication strength.
PBKDF	(no security claimed)	Used to derive non-compliant keys used for obfuscation of data in transit during the Local (User) session. This algorithm is compliant with FIPS 140-2 requirements for authentication strength.

Table 5: FIPS 140-2 Non-Approved Algorithms (Not Security Functions)

8 Cryptographic Keys and Critical Security Parameters

The following section lists the critical and public security parameters that are retained by the device. All encrypted critical security parameters in the module are protected by 128-bit AES using the MKEK (which encrypts the NVDEK and NVDAK, which encrypt and authenticate all encrypted CSPs), which is zeroized by the scrap service. The Indicia Key is output protected by an Approved Key Transport Scheme (KTS) that is conformant to SP 800-38F. All other critical security parameters, including private and secret keys, are not output by or input to the module.

8.1 Critical Security Parameters

The table below lists the critical security parameters:

Name	Algorithm	Storage	Generation	Establishment	Destruction	Purpose
Data Encryption Master Key (MKEK) (128-bit key)	AES-128 bits, Counter mode	Plaintext	Internal DRBG (during manufacturing)	N/A	Scrap service or tamper event	Serves to encrypt and decrypt critical security parameters.
Data Encryption Key (NVDEK) (128-bit key)	AES CBC	Encrypted	Internal DRBG (during manufacturing)	N/A	Scrap service, tamper event.	Serves to encrypt and decrypt other internally stored critical security parameters.
Data Authentication Key (NVDAK) (128-bit key)	HMAC-SHA256	Encrypted	Internal DRBG (during manufacturing)	N/A	Scrap service, tamper event.	Serves to authenticate other internally stored critical security parameters.
Entropy string	NDRNG	Not persistently stored	Internal NDRNG	N/A	Power cycle (volatile)	Required for generation of DRBG state
DRBG seed	CTR_DRBG using AES 128	Not persistently stored	Internal NDRNG	N/A	Power cycle (volatile)	Internal state of the Deterministic Random Bit Generator.
DRBG State: Key	CTR_DRBG using AES 128	Encrypted	Updated during random number generation	N/A	Scrap service, tamper event.	Internal state of the Deterministic Random Bit Generator.
DRBG State: V	CTR_DRBG using AES 128	Encrypted	Updated during random number generation	N/A	Scrap service, tamper event.	Internal state of the Deterministic Random Bit Generator.
Passphrase	N/A	Encrypted	N/A	Pre-loaded (during manufacturing)	N/A (encrypting key zeroized by scrap/tamper)	Used for User Identity based authentication
Indicia Key (256-bit key)	HMAC-SHA256	Encrypted	Internal DRBG	Encrypted Output by KTS	N/A (encrypting key zeroized by scrap/tamper)	Serves to authenticate indicia (barcode part).
Transport Signing (private) Key (2048 bit key)	RSA PKCS#1 V1.5	Encrypted	Internal DRBG (during manufacturing)	N/A	N/A (encrypting key zeroized by scrap/tamper)	Serves to properly identify device after shipping and to establish initial secure session.
PMD Signing (private) Key (2048 bit key)	RSA PKCS#1 V1.5	Encrypted	Internal DRBG (during manufacturing)	N/A	N/A (encrypting key zeroized by scrap/tamper)	Used to support hosting device during its authentication services.

Name	Algorithm	Storage	Generation	Establishment	Destruction	Purpose
PSD Signing (private) Key (2048 bit key)	RSA PKCS#1 V1.5	Encrypted	Internal DRBG	N/A	N/A (encrypting key zeroized by scrap/tamper)	Serves to setup regular secure sessions.
Ephemeral Diffie-Hellman Client (private) Key (224 bit key)	KAS SP800-56A	Not persistently stored	Internal DRBG	N/A	Zeroized after use	Serves to derive session keys for the Cryptographic Officer.
Remote Session Authentication Key (RSAK) (160-bit HMAC key)	HMAC -SHA1	Not persistently stored	N/A	Key Agreement/ Derivation	Zeroized after use	Serves to authenticate data during a remote secure session (CO role)
Remote Session Encryption Key (RSEK) (192-bit 3TDES key)	3-Key Triple-DES CBC	Not persistently stored	N/A	Key Agreement/ Derivation	Zeroized after use	Serves to encrypt and decrypt data during a remote secure session (CO role).

Table 6: Critical Security Parameters

8.2 Public Security Parameters

The following public keys are stored in the device:

Name of certificate or public key	Algorithm	Storage	Establishment	Purpose
FPRootCACert & public key	2048-bit RSA key	Plaintext	N/A	Serves to authenticate FDC and PKM keys
FPCustomerRootKey	2048-bit RSA key	Plaintext	N/A	Used to verify integrity of Bootloader firmware
Firmware Verification Key	2048-bit RSA key	Plaintext	N/A	Used to verify firmware from Francotyp-Postalia.
FDCCert & public key	2048-bit RSA key	Plaintext	N/A	Serves to authenticate TransportKey
PKMCert & public key	2048-bit RSA key	Plaintext	Loaded upon expiration	Serves to authenticate Cryptographic Officer
TransportCert & public key	2048-bit RSA key	Plaintext	Internal DRBG (Manufacturing)	Serves to initially authenticate *Postal NRevenector GB 2019*
PSDKey (certificate & public key)	2048-bit RSA key	Plaintext	Internal DRBG	Serves to authenticate *Postal NRevenector GB 2019*
RootCABCCert & public key	2048-bit RSA key	Plaintext	N/A	Serves to authenticate FDCBC and PMD keys
FDCBCCert & public key	2048-bit RSA key	Plaintext	N/A	Serves to authenticate PMDKey
PMDKeyCert & public key	2048-bit RSA key	Plaintext	Internal DRBG (Manufacturing)	Used to support hosting device during its authentication services.
Ephemeral Diffie-Hellman Client (public) Key (2048 bit key)	KAS SP 800-56A	Not persistently stored	Internal (KAS SP 800-56A)	Serves to derive session keys for the Cryptographic Officer.
Ephemeral Diffie-Hellman Server (public) Key (2048 bit key)	KAS SP 800-56A	Not persistently stored	KAS SP 800-56A	Serves to derive session keys for the Cryptographic Officer.

Table 7: Public Security Parameters

8.3 Zeroization

Zeroization may occur under the following conditions:

Event	Effect	Resulting State	Speed	Recovery Action
Tamper	All CSPs rendered unreadable.	Chip unbootable until tamper cause has been removed and device is power cycled. If bootable, device permanently enters DEFECT state. No cryptographic functions may be used.	Immediate	Return to FP.
Battery removed	All CSPs rendered unreadable.	Restoring battery will result in device permanently entering DEFECT state. No cryptographic functions may be used.	Immediate	Return to FP.
Scrap service run	All CSPs rendered unreadable.	Device permanently enters SCRAPPED state. No cryptographic functions may be run.	Fast (<40µs)	Return to FP.

Table 8: Zeroization

9 Self-Tests

9.1 Power on self-tests

The following self-tests are performed when the module starts:

9.1.1 Firmware Integrity Test

The integrity of the *NRevenector 2019* (Bootloader) is verified at initial power-on of the module by comparing the generated hash against a known SHA 256 hash from PKCSPSS (RSA #3046). The *NRevenector 2019* (Bootloader) checks the SHA 256 hash of the *Postal NRevenector GB 2019* (Royal Mail Application) firmware in the cryptographic module and verifies this against a known hash value generated as part of the PKCS#1 V1.5 (Signature Scheme) (RSA #3046).

9.1.2 Cryptographic Algorithm Tests

The following table lists the cryptographic algorithm tests for approved security functions that are performed as part of the power-on self-tests. See Table 4 for corresponding NIST certificates.

Security Function	Type of self-test
AES 128 Encrypt/Decrypt (ECB, CBC)	Encrypt KATs (Known Answer Tests) Decrypt KATs
DRBG[4]	Instantiate KAT Generate KAT Reseed KAT
DSA Key Pair Generation (2048, 224)	DSA does not include Sign/Verify functionality; only testing for key generation is applicable (included in Diffie-Hellman Key Agreement conditional test)
HMAC-SHA-1 & HMAC-SHA-256 (includes SHA tests)	HMAC-SHA-1 KAT HMAC-SHA-256 KAT
Key Agreement Scheme	Diffie-Hellman Primitive Z computation KAT SHA-256 KDF KAT (covered by HMAC-SHA-256 KAT)
RSA 2048-bit Sign/Verify using SHA-256	Sign KAT Verify KAT
Triple-DES Encrypt/Decrypt (ECB, CBC)	Encrypt KATs Decrypt KATs

Table 9: FIPS 140-2 Cryptographic Algorithm Tests

[4] In accordance with FIPS 140-2 Implementation Guidelines December 2019 sect 9.8, the SP 800-90A compliant DRBG does not perform the continuous random number generator test as described in FIPS 140-2 section 4.9.2

9.2 Conditional Tests

The following conditional tests are performed:

Security Function	Self-Test Performed
NDRNG[5]	Repetition count test and adaptive proportion test in accordance with FIPS 140-2 Implementation Guidelines December 2019 sect 9.8.
Diffie-Hellman Key Agreement	DH FFC Pairwise Consistency Test (covers Key Generation for DSA Cert. #1455) Assurance of Public Key Validation Assurance of Domain Parameter Validity On key establishment: See SP 800-56A, see FIPS 140-2 section 4.9.2 "Pair-wise consistency test 2" See SP 800-56A section 5.6.2 and 5.5.2
RSA 2048 bit using SHA-256	On key generation: see FIPS 140-2 section 4.9.2 "Pair-wise consistency test 2".
Triple-DES (ECB & CBC)	Triple-DES encryption limit of 2^16. This is enforced by the use of a counter that is incremented every time that the module performs a Triple-DES encryption. If the counter reaches the encryption limit, then the module will enter an error state, the user session will be broken, and the module will be re-booted.
Firmware Loading Test	On loading of programmed firmware (Royal Mail Application): Performs RSA 2048 SHA 256 signature verification.

Table 10: Conditional Tests

9.2.1 Critical Function Tests

The module continuously checks the consistency of the redundantly stored postal registers and tests the Microcontroller Operational Mode.

9.3 Error States

The module implements several self-tests during power up and as conditional self-tests linked to cryptographic operations.

In the event of an error being detected, the *Postal NRevenector GB 2019* enters an error state and stores the reason (error identifier) persistently. The error state information can be retrieved via the Get Device Status service.

Error states may be cleared only by power-cycling the module.

[5] In accordance with FIPS 140-2 Implementation Guidelines December 2019 sect 9.8, the NDRNG performs the repetition count test instead of the continuous random number generator test as described in FIPS 140-2 section 4.9.2

10 Mitigating Other Attacks

The device includes environmental failure protection means for the battery voltage and the module temperature. If an attack is detected then the contents of the cryptographic integrated circuit's battery-powered key storage are automatically zeroized, leaving the module inoperable.

The device includes environmental failure protection means for the main input voltage, and the internal core voltage. If one of these conditions is outside a defined range the device is held in the reset condition. The device also includes environmental failure protection such that temperature changes outside the normal operating ranges will not compromise the security of the device.

The device includes a protection means to test for drift in the main clock frequency of the processor. The cryptographic module's processor also incorporates a layer of metal shielding as one of its layers, used to detect attempts at intrusion at a die level. In the event of an intrusion attempt being detected, the contents of its battery-powered key storage are automatically zeroized leaving the module inoperable.

The failure protection for the battery voltage and temperature, and the tamper detection for the physical breach of the module's physical boundary are present using power from the battery even when the device is switched off. The module's processor responds by destroying the stored plaintext CSPs.

11 Glossary and Abbreviations

Term	Definition
AES	Advanced Encryption Standard
CKG	Cryptographic Key Generation
CSPs	Critical Security Parameters
CO	Cryptographic Officer
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECDSA	Elliptic Curve Digital Signature Algorithm
EMI/EMC	Electromagnetic Interference/ Electromagnetic Compatibility
FP	Francotyp-Postalia Holding AG
HMAC	Hash-based Message Authentication Code
KAS	Key Agreement Scheme
KDF	Key Derivation Function
MAC	Message Authentication Code
MKEK	Data Encryption Master Key
NVDAK	Non-Volatile Data Authentication Key
NVDEK	Non-Volatile Data Encryption Key
PBKDF	Password-Based Key Derivation Function
PRDIs	Postal Relevant Data Items
PSD	Postal Security Device
RSA	Rivest–Shamir–Adleman (asymmetric algorithm)
RSAK	Remote Session Authentication Key
RSEK	Remote Session Encryption Key
SHS	Secure Hash Algorithm
TDES or Triple DES	Triple Data Encryption Standard
UID	User ID

Table 11: Glossary and Abbreviations

12 References

Reference	Publication
FIPS 140-2 Derived Test Requirements (DTR)	January 2011
FIPS 140-2 Implementation Guidance (IG)	December 2019
FIPS 140-2 Publication (PUB)	May 2001
FIPS 180-4	August 2015
FIPS 186-4	July 2013
FIPS 197	November 2001
FIPS 198-1	July 2008
NIST SP 800-38A	December 2001
NIST SP 800-56A	Revision 1, March 2007; Revision 3, April 2018
NIST SP 800-56C	Revision 1, April 2018
NIST SP 800-67	Revision 2, November 2017
NIST SP 800-90A	June 2015
NIST SP 800-90B	January 2018
NIST SP 800-133	December 2012

Table 12: References