FIPS 140-2 Non-Proprietary Security Policy

Postal mRevenector GB 2013

Version 1.6

Hardware P/N: 580036020300/01 & 580036020300/02

Firmware Version:

Bootloader: *90.0036.0201.00/2011485001*

Softwareloader: *90.0036.0206.00/2011485001*

GB Application: 90.0036.0215.00/2013463001

Francotyp-Postalia GmbH
Triftweg 21-26
16547 Birkenwerder
Germany

fp-francotyp.com

Contents

Figures

Tables

1 Introduction

1.1 Overview

Francotyp-Postalia (FP) is one of the leading global suppliers of mail center solutions. A major component of the business of FP is the development, manufacture and support of postal franking machines (postage meters). These postal franking machines incorporate 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 mRevenector GB 2013 is FP's latest generation of PSD.

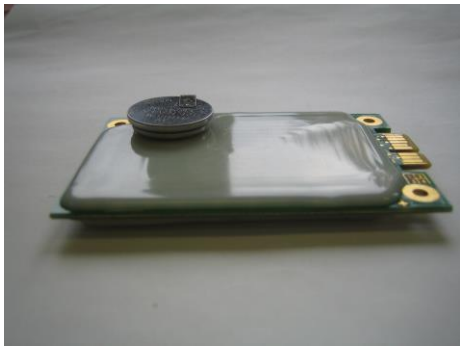

Figure: 1 *Postal mRevenector GB 2013*

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.

1.2 Implementation

The Postal mRevenector GB 2013 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 module has a proprietary electrical connector forming the interface to the module.

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/EFT
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, Interfaces & Excluded Components

3.1 Physical Interface

The cryptographic module uses a 36 pin card edge connector. The usage of these physical ports for FIPS 140-2 logical interfaces is detailed in the table below:

Type	**Pin**
Data Input	A4, A5, A10, A11, A12, A13, A14, A15
Data Output	A4, A5, A10, A11, A12, A13, A14, A15
Control Input	A4, A5, A8, A9, A10, A11, A12, A13, A14, A15
Status Output	A2, A3, A4, A5, A10, A11, A12, A13, A14, A15
Power	A1, A6, A7, A16, A17, A18, B1, B7, B8, B9, B10, B11, B16, B17, B18
Not Used	B2, B3, B4, B5, B6, B12, B13, B14, B15

Table 2: Cryptographic Ports & Types

3.2 Cryptographic boundary

The cryptographic boundary is defined to be the outer edge of both the epoxy covered printed circuit board and the exposed battery. The battery is excluded from the requirements of FIPS 140-2. It is connected to the circuitry of the module in such a way that it cannot be used to compromise the security of the module.

4 Rules of Operation

4.1 FIPS 140-2 Related Security Rules

The Postal mRevenector GB 2013 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. Perform the self-test as described in section 10 of this document.
11. Support the following logically distinct interfaces:
    - Data input interface
    - Data output interface
    - Control input interface
    - Status output interface
    - Power interface.
12. Implement all software using a high-level language, except the limited use of low-level languages to enhance performance.
13. Protect critical security parameters from unauthorized disclosure, modification and substitution.
14. 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.
15. Support a FIPS approved deterministic random bit generator (DRBG) as specified in NIST 800-90a section 10.2.1
16. Perform the self tests listed in section 10 during power-on and on-demand when the corresponding service is used.
17. 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.
18. Not perform any cryptographic functions while in an error state.
19. Not support multiple concurrent operators.

4.2 Royal Mail Related Security Rules

Based on the specifications of the Royal Mail (RM) the Postal mRevenector GB 2013 shall:

20. Protect the postal registers against unauthorized substitution or modification.

21. Never zeroize the postal registers.

22. Comply with the specifications of the Royal Mail (RM) for Mailmark™.

23. Provide mechanisms to disable the Accounting-Service when it has no connection with its partnering infrastructure on a regular basis.

24. Provide mechanisms to re-key the indicia key on a regular basis

25. 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 mRevenector GB 2013 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 three way handshake protocol using secret passphrases and user identifications (UIDs) known to both parties. The Host System typically acts on behalf of the User and can request authenticated services.

5.4 Cryptographic Officer Role

The *Cryptographic Officer* is authenticated using an identity based authentication method based on an RSA signature verification process, which utilizes a 2048-bit RSA public key over the CO's identifier. This method uses two pairs of asymmetric keys and two distinguished names. The public parts and distinguished names are each known to the other party. In this way, the PSD and the infrastructure are able to identify and authenticate themselves to the other by verifying the exchanged distinguished name and signature. In addition the Diffie-Hellman key agreement protocol is used to establish secret keys that may be used for further key encryption and authentication of data exchange.

The Cryptographic Officer role shall provide those services necessary to initialize, authorize and validate the Postal mRevenector GB 2013. This role provides those services which enter, modify or generate critical security parameters.

A Francotyp-Postalia Infrastructure server typically acts on behalf of a Cryptographic Officer.

5.5 Services and Roles

The following abbreviations are used in the service and roles matrix:

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

The following services are offered by the cryptographic module:

Service	Approved Security Functions Used	Associated CSPs	Access Rights	Roles	Note
Get Device Status	None	None	-	DU	
Echo	None	None	-	DU	Echoes back data payload.
Postal Module Registration	AES-CBC, HMAC-SHA256, DRBG	Passphrase Local Session Authentication Key Local Session Encryption Key	W R R	U	Enters postal configuration data and registers the module in the country and initializes the module for postal usage.
Reboot Device	None	None	-	DU	Service to cause the device to reboot.
Scrap	None	Data Encryption Master Key Data Authentication Master Key Working Encryption Key Working Authentication Key	Z Z Z Z	DU	Zeroizes all plaintext CSPs.
Setup Parameter	None	None	-	DU	Enters postal configuration data.
Self-test	All listed in chapter 6	None	-	DU	
Logoff	None	None	-	CO, U	Leaves the CO or User role.
Local Login	AES-CBC, HMAC-SHA256, DRBG	Passphrase, Local Session Encryption Key Local Session Authentication Key DRBG State	R W W R,W	DU	The passphrase is used for authentication as part of a 3-way challenge response protocol.
Remote Login	KAS, DSA Key Generation RSA 2048 Sign & Verify with SHA-256, DRBG	PSD Transport Key Pair PSD Keys Pair Remote Session Encryption Key Remote Session Authentication Key DRBG State	R R W W R,W	DU	Required to enter the CO role.
Verify Mac	None	FP Mac Secret	R	U	Authenticates a data payload.
Postal Initialization	RSA 2048 Sign/Verify using SHA-256, 3-Key Triple DES CBC, HMAC-SHA1, DRBG	PSD Key Pair Remote Session Encryption Key Remote Session Authentication Key DRBG State	G R R R,W	CO	Initialize the device according to the UK Mailmark and IPMAR requirements.
Postal Authorization	HMAC-SHA1, DRBG	Remote Session Authentication Key	R	CO	Authorize the device according to the UK Mailmark and IPMAR requirements.

Service	Approved Security Functions Used	Associated CSPs	Access Rights	Roles	Note
Generate Indicia Key	3-Key Triple DES CBC, HMAC-SHA1, DRBG	Indicia Key Remote Session Encryption Key Remote Session Authentication Key DRBG State	G R R R,W	CO	Generating and re-keying indicia key
Postage Value Download	3-Key Triple DES CBC, HMAC-SHA1	Remote Session Encryption Key Remote Session Authentication Key	R R	CO	Finance service, managing postal funds
Accounting	HMAC-SHA256	Indicia Key	R	U	Debits the postal funds and returns indicia content.
Postage Value Refund	3-Key Triple DES CBC, HMAC-SHA1	Remote Session Encryption Key Remote Session Authentication Key	R R	CO	Finance service, managing postal funds.
Re-Authorization	HMAC-SHA1	Remote Session Authentication Key	R	CO	Updates customer configuration data
Re-Initialization	HMAC-SHA1	Remote Session Authentication Key	R	CO	Updates postal configuration data
Reenter FP Mac Secret	3-Key Triple DES CBC, HMAC-SHA1	Remote Session Encryption Key Remote Session Authentication Key FP Mac Secret	R R W	CO	Enters FP Mac Secret used to authenticate proprietary data
Rekey PSD key	3-Key Triple DES CBC, RSA 2048 Sign/Verify using SHA-256, HMAC-SHA1, DRBG	PSD Key Pair, Remote Session Encryption Key Remote Session Authentication Key	R,W R R	CO	
Renew PKM key	RSA 2048 Verify using SHA-256	None		CO	Loads signed PKM certificate
Secure Echo	3-Key Triple DES CBC, HMAC-SHA1	Remote Session Encryption Key Remote Session Authentication Key	R R	CO	Echoes back data payload within a secure session.
Secure Update Parameters	3-Key Triple DES CBC, HMAC-SHA1	Remote Session Encryption Key Remote Session Authentication Key	R R	CO	Updates security relevant postal configuration data.
Secure Get Status	HMAC-SHA1	Remote Session Authentication Key	R	CO	Provides status within a secure session.
Secure Set Time	HMAC-SHA1	Remote Session Authentication Key	R	CO	Synchronizes the RTC within a secure session.
Sign PMD Data	AES-CBC, HMAC-SHA256 RSA 2048 Sign using SHA-256	Private PMD Key Local Session Authentication Key Local Session Encryption Key	R R R	U	Sign postal related items and communication data.
Program FLASH with Firmware	RSA- PKCS#1 V1.5 verification using 2048 and SHA-256	Working Encryption Working Authentication keys	R R	U	Receives firmware from an external source and programs it into the cryptographic module's FLASH memory.
Select Programmed Firmware	None	None	-	DU	Configures the bootloader.

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 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 (alphanumeric input). 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, except the battery and the card edge connector, 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; no assurance is provided for Level 3 hardness conformance at any other temperature.

7 Operational Environment

The cryptographic module's operational environment is a limited operational environment.

8 Cryptographic Functions

The module has one mode of operation, the FIPS mode of operation. It implements the following FIPS approved algorithms:

Security Function	Usage	Certificate
SHA-1, SHA-256	Hashing	NIST Certificate #1346
DRBG	On key generation	NIST Certificate #61
AES 128 (ECB & CBC)	On data encryption and authentication	NIST Certificate #1493
HMAC-SHA-1, HMAC-SHA-256	On message authentication, on indicia authentication	NIST Certificate #878
Key Agreement Scheme SP800-56A	On key establishment (provides 112 bits of security strength)	NIST Certificate #16
RSA PKCS#1 V1.5 Signature Verification using RSA 2048 and SHA-256	On signature verification	NIST Certificate #732
RSA PKCS#1 V1.5 Signature Generation or Verification using RSA 2048 and SHA-256	On signature verification or generation	NIST Certificate #785
3-Key Triple DES (ECB & CBC)	On data encryption and decryption	NIST Certificate #1122
DSA	On key generation for KAS	NIST Certificate #522

Table 4: Cryptographic Functions

The module has the following non-approved security functions (allowed in FIPS mode of operation):

- Non-Deterministic Random Number Generator (NDRNG), used for seeding the DRBG.
- Automated key output via a secure session based on 3-Key Triple DES CBC (Cert. #1122) and HMAC-SHA-1 (Cert. #878) (key wrapping; key establishment methodology provides 112 bits of encryption strength)

9 Cryptographic Keys and Critical Security Parameters

The following section lists the critical and public security parameters that are retained by the device. The device generates cryptographic keys whose strengths are modified by available entropy of the DRBG to a maximum of 128-bits.

Critical Security Parameters

The table below lists the critical security parameters:

Name	Algorithm	Storage	Generation	Establishment	Destruction	Purpose
DRBG State	CTR_DRBG using AES 128	Encrypted	Seeded by internal NDRNG	N/A	N/A	Internal state of the Deterministic Random Bit Generator.
Data Encryption Master Key (MKEK) (128 bit key)	AES CBC	Plaintext	Internal DRBG	N/A	Scrap service or tamper event	Serve to encrypt and decrypt critical security parameters.
Data Authentication Master Key (MKAK) (128 bit key)	HMAC-SHA256	Plaintext	Internal DRBG	N/A	Scrap service or tamper event	Serve to authenticate critical security parameters.
Working Encryption Key (VDEK) (128 bit key)	AES CBC	Plaintext	Internal DRBG	N/A	Scrap service, tamper event or power cycle	Serve to encrypt and decrypt other internally used data.
Working Authentication Key (VDAK)	HMAC-SHA256	Plaintext	Internal DRBG	N/A	Scrap service, tamper event or power cycle	Serve to authenticate other internally used data.
Data Encryption Key (NVDEK) (128 bit key)	AES CBC	Encrypted	Internal DRBG	N/A	N/A	Serve to encrypt and decrypt other internally stored critical security parameters.
Data Authentication-Key (NVDAK) (128 bit key)	HMAC-SHA256	Encrypted	Internal DRBG	N/A	N/A	Serve to authenticate other internally stored critical security parameters.
Transport Signing (private) Key (2048 bit key)	RSA PKCS#1 V1.5	Encrypted	Internal DRBG	N/A	N/A	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	N/A	N/A	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	Serves to setup regular secure sessions.
Indicia Key (256 bit key)	HMAC-SHA256	Encrypted	Internal DRBG	Encrypted Output	N/A	Serves to authenticate indicia (barcode part).
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 key, 112 bits of strength)	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 key, 112 bits of strength)	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).
Local Session Authentication Key (LSAK) (256 bit key)	HMAC – SHA256	Not persistently stored	N/A	PBKDF	Zeroized after use	Serves to authenticate data during a local secure session (User role)
Local Session Encryption Key (LSEK) (128 bit key)	AES CBC	Not persistently stored	N/A	PBKDF	Zeroized after use	Serves to encrypt and decrypt data during a local secure session (User role).
FP Mac Secret	N/A	Encrypted	N/A	Encrypted Entry	N/A	Used to authenticate proprietary data
Passphrase	N/A	Encrypted	N/A	N/A	N/A	Used for User Identity based authentication

Table 5: Critical Security Parameters

Public Security Parameters.

The following public keys are stored in the device:

Name of certificate or public key	Algorithm	Storage	Generation	Purpose
FPRootCACert & public key	2048 bit RSA key	Plaintext	N/A	Serves to authenticate FDC and PKM keys
FDCCert & public key	2048 bit RSA key	Plaintext	N/A	Serves to authenticate TransportKey
PKMCert & public key	2048 bit RSA key	Plaintext	N/A	Serves to authenticate Cryptographic Officer
TransportCert & public key	2048 bit RSA key	Plaintext	Internal DRBG	Serves to initially authenticate Postal mRevenector GB 2013
PSDKey (certificate & public key)	2048 bit RSA key	Plaintext	Internal DRBG	Serves to authenticate Postal mRevenector GB 2013
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	Used to support hosting device during its authentication services.
Firmware Verification Key	2048 bit RSA key	Plaintext	N/A	Used to verify firmware from Francotyp-Postalia.
Ephemeral Diffie-Hellman Client (public) Key (2048 bit key)	KAS SP800-56A	Not persistently stored	Internal	Serves to derive session keys for the Cryptographic Officer.
Ephemeral Diffie-Hellman Server (public) Key (2048 bit key)	KAS SP800-56A	Not persistently stored	N/A	Serves to derive session keys for the Cryptographic Officer.

10 Self-Tests

10.1 Power on self tests

The following self tests are performed when the Postal mRevenector GB 2013 starts:

Firmware Integrity Test

The mRevenector checks the SHA 256 hash of the Postal mRevenector GB 2013 firmware of the cryptographic module and verifies this against a known hash value generated as part of the PKCS#1 V1.5 (Signature Scheme).

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. For corresponding NIST certificates see Table 4.

Security Function	Type of self-test
DBRG	Known answer test (KAT)
AES 128 Encrypt/Decrypt (ECB & CBC)	KAT
HMAC-SHA-1 & HMAC-SHA-256 (includes SHA tests)	KAT
Key Agreement Scheme	KAT
RSA 2048 bit Sign/Verify using SHA-256	KAT
RSA 2048 bit Verify using SHA-256	KAT
Triple DES Encrypt/Decrypt (ECB & CBC)	KAT

Table 6: FIPS 140-2 Cryptographic Algorithm Tests

Register Consistency Test

This test checks the consistency of the redundantly stored postal registers.

10.2 Conditional Tests

The following conditional tests are performed:

Security Function	Performed
CTR-DBRG and NDRNG	On usage: see FIPS 140-2 section 4.9.2 "Continuous RNG test 1".
Diffie-Hellmann Key Agreement	On key establishment: see FIPS 140-2 section 4.9.2 "Pair-wise consistency test 2".
RSA 2048 bit using SHA-256	On key generation: see FIPS 140-2 section 4.9.2 "Pair-wise consistency test 2".

Security Function	Performed
Firmware Loading Test	On loading of programmed firmware: Performs RSA 2048 SHA 256 signature verification

Continuous DRBG Test

The cryptographic module uses a Deterministic Random Bit Generator (DRBG) based on a block cipher algorithm as specified in the recommendation NIST SP 800-90. The implemented CTR DRBG uses AES-128 as its cryptographic function. The entropy input is at least 128 Bits. The DRBG uses a hardware-based random number generator as the entropy source. Consecutive outputs of the DRBG are compared to ensure that they differ. The module has a single, non-approved algorithm, its hardware implemented NDRNG. Consecutive outputs of the NDRNG are compared to ensure that they differ.

10.3 Error States

In the event of an error being detected, the Postal mRevenector GB 2013 enters an error state and stores the reason (error identifier) persistently. The error state information can be retrieved via the Get Device Status service.

11 Mitigating Other Attacks

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

The device is designed in such a way that temperature changes outside the normal operating ranges will not compromise the security of the device.

The device includes failure protection means for the frequency of the internal Real Time Clock (RTC). If an attack is detected then the contents of the cryptographic IC's battery powered key storage are automatically zeroized, leaving the module inoperable.

The device includes failure protection means for the main input voltage, the internal core voltage, and the main clock frequency. If one of these conditions is outside a defined range the device is held in the reset condition.

The cryptographic module's processor 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 the RTC frequency 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.