Security Policy

Postal mRevenector DE 2011

Version 1.6

Hardware P/N: 580036020300/01

Firmware Version:

Bootloader: 90.0036.0201.00/2011485001

Software-Loader: 90.0036.0206.00/2011485001

FRANKIT-Application: 90.0036.0204.00/2012095001

Francotyp-Postalia GmbH
Development Department
Hasbi Kabacaoglu / Dirk Rosenau
Prenzlauer Promenade 28
D-13089 Berlin
Germany

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 DE 2011 is FP's latest generation of PSD.

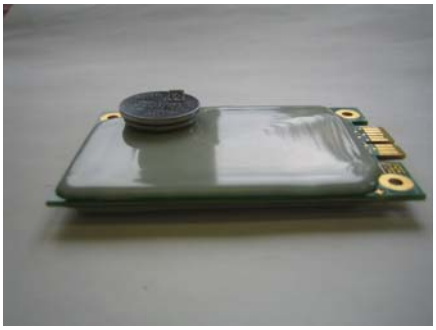

Figure: 1 *Postal mRevenector DE 2011*

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 DE 2011 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/IMC)	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 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 DE 2011 shall:

1. Support only an Approved mode of operation.
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, 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 9 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 800-90 section 10.2.1
16. Perform the self tests listed in section 9 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 Postal Related Security Rules

The Postal mRevenector DE 2011 shall:

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

21. Never zeroize the postal registers.

22. Comply with the specifications given in the "*FRANKIT-New Generation Digital Franking*" specification from the Deutsche Post AG (DPAG).

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

24. 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 DE 2011 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 pass phrases and user identifications (UIDs) known to both parties.

The Host System typically acts on behalf of the User to 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 DE 2011. This role provides any 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 services are offered by the cryptographic module:

Service	Approved Security Functions Used	Associated CSPs	Roles	Note
Echo	None	None	Default User	Echoes back data payload.

Service	Approved Security Functions Used	Associated CSPs	Roles	Note
Get Device Status	None	None	Default User	
Reboot Device	None	None	Default User	Service to cause the device to reboot.
Scrap	None	None	Default User	Zeroizes all plaintext CSPs.
Select Programmed Firmware	None	None	Default User	Configures the bootloader.
Selftest	All listed in chapter 6	None	Default User	
Setup Parameter	None	None	Default User	Enters postal configuration data.
Logoff	None	None	CO, User	Leaves the CO or User role.
Local Login	AES-CBC, HMAC-SHA256, DRBG	Passphrase	Required to enter the User role	Required to enter the User role.
Remote Login	KAS, DSA Key Generation RSA 2048 Sign & Verify with SHA-256, DRBG	PSD Transport Key Pair, PSD Keys Pair, PKM Public Key Remote Session Encryption Key Remote Session Authentication Key	Required to enter the CO role	Required to enter the CO role.
Postal Initialization	RSA 2048 Sign/Verify using SHA-256, 3TDES CBC, HMAC-SHA1, DRBG	PSD Key Pair Remote Session Encryption Key Remote Session Authentication Key	CO	Initialize the device according to the DPAG FRANKIT requirements.
Postal Authorization	HMAC-SHA1,	Remote Session Authentication Key	CO	Authorize the device according to the DPAG FRANKIT requirements.
Postage Value Download	RSA 1024 Decryption, 3TDES CBC, HMAC-SHA1	DPAG Private Key Remote Session Encryption Key Remote Session Authentication Key Indicia Key (m_{Secret})	CO	Finance service, managing postal funds.
Postage Value Refund	RSA 1024 Decryption, 3TDES CBC, HMAC-SHA1	DPAG Private Key Remote Session Encryption Key Remote Session Authentication Key	CO	Finance service, managing postal funds.
Re-Initialization	HMAC-SHA1	Remote Session Authentication Key	CO	Updates postal configuration data
Reenter FP Mac Secret	3TDES CBC, HMAC-SHA1	Remote Session Encryption Key Remote Session Authentication Key FP Mac Secret	CO	Enters FP Mac Secret used to authenticate proprietary data
Rekey DPAG Keys	RSA 1024 Encryption/ Decryption, 3TDES CBC, HMAC-SHA1 DRBG	DPAG Key Pair Remote Session Encryption Key Remote Session Authentication Key	CO	

Service	Approved Security Functions Used	Associated CSPs	Roles	Note
Rekey PSD keys	TDES CBC, RSA 2048 Sign/Verify using SHA-256, HMAC-SHA1, DRBG	PSD Key Pair, Remote Session Encryption Key Remote Session Authentication Key	CO	
Renew PKM key	RSA 2048 Verify using SHA-256,	PKM public key	CO	Loads signed PKM certificate
Secure Echo	HMAC-SHA1	Remote Session Authentication Key	CO	Echoes back data payload within a secure session.
Secure Get Status	HMAC-SHA1	Remote Session Authentication Key	CO	Provides status within a secure session.
Secure Set Time	HMAC-SHA1	Remote Session Authentication Key	CO	Synchronizes the RTC within a secure session.
Accounting	SHA1 with secret suffix method	mSecret	User	Debits the postal funds and returns indicia content.
Postal Module Registration	AES-CBC, HMAC-SHA256	None	User	Enters postal configuration data and registers the module in the country and initializes the module for postal usage.
Program FLASH with Firmware	RSA- PKCS#1 V1.5 verification using 2048 and SHA-256	Working Encryption keys Working Authentication keys	User	Receives firmware from an external source and programs it into the cryptographic module's FLASH memory.
Sign PMD Data	AES-CBC, HMAC-SHA256, RSA 2048 Sign using SHA-256	Local Session Encryption Key, Local Session Authentication Key, Private PMD Key	User	Sign postal related items and communication data.
Verify Mac	None	FP Mac Secret	User	Authenticates a data payload.

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 opaque within the visible spectrum. Because of the potting material it is not possible to physically access any internal components without seriously damaging the module or causing zeroization.

7 Cryptographic Functions

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

Security Function	Usage	Certificate
SHA-1, SHA-256	Hashing	NIST Certificate #1346
DRBG	On key generation	NIST Certificate #61
AES 128 (EBC & CBC)	On data encryption and authentication	NIST Certificate #1493
HMAC-SHA1, HMAC-SHA-256	On message authentication	NIST Certificate #878
Key Agreement Scheme(KAS) SP800-56A	On key establishment, key establishment method provides 112 bits of security strength.	NIST Certificate #16
RSA PKCS#1 V1.5 Verification using 2048 and SHA-256	On signature verification	NIST Certificate #732
RSA PKCS#1 V1.5 Signing using 2048 and SHA-256	On signature generation	NIST Certificate #785
RSA PKCS#1 V1.5 Encryption/Decryption* using 1024 and SHA-1	On key decryption, key establishment method provides 80 bits of security strength.	N/A
3TDES (ECB & CBC)	On data encryption and decryption	NIST Certificate #1122
DSA	On key generation for KAS	NIST Certificate #522
Non-Approved RNG	Non-Deterministic Random Number Generator (NDRNG), used for seeding the DRBG.	N/A

* The Approved Signature Generation and Verification functions of this RSA implementation were issued NIST Certificate #731.

Table 4: Cryptographic Functions

8 Cryptographic Keys and Critical Security Parameters

The following section lists the critical and public security parameters that are retained by the device.

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 Keys	AES CBC 128 bits	Plaintext	Internal DRBG	N/A	Scrap service or tamper event	Serve to encrypt and decrypt critical security parameters.
Data Authentication Master Keys (128 bit key)	HMAC-SHA256	Plaintext	Internal DRBG	N/A	Scrap service or tamper event	Serve to authenticate critical security parameters.
Working Encryption Keys	AES CBC 128 bits	Plaintext	Internal DRBG	N/A	Scrap service, tamper event or power cycle	Serve to encrypt and decrypt other internally used data.
Working Authentication Keys (128 bit key)	HMAC-SHA256	Plaintext	Internal DRBG	N/A	Scrap service, tamper event or power cycle	Serve to authenticate other internally used data.
Data Encryption Keys	AES CBC 128 bits	Encrypted	Internal DRBG	N/A	N/A	Serve to encrypt and decrypt other internally stored critical security parameters.
Data Authentication-Keys (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	RSA PKCS#1 V1.5 -2048	Encrypted	Internal DRBG	N/A	N/A	Serves to properly identify device after shipping and to establish initial secure session.
PMD Signing (private) Key	RSA PKCS#1 V1.5 -2048	Encrypted	Internal DRBG	N/A	N/A	Used to support hosting device during its authentication services.
PSD Signing (private) Key	RSA PKCS#1 V1.5 -2048	Encrypted	Internal DRBG	N/A	N/A	Serves to setup regular secure sessions.
DPAG Decryption Key	RSA PKCS#1 V1.5 -1024	Encrypted	Internal DRBG	N/A	N/A	Serves to decrypt the mSecret.
mSecret (128 bit)	SHA1	Encrypted	N/A	Encrypted Entry	N/A	Serves to authenticate indicia.

Name	Algorithm	Storage	Generation	Establishment	Destruction	Purpose
Ephemeral Diffie-Hellman	KAS SP800-56A -2048	Not persistently stored	Internal DRBG	N/A	Zeroized after use	Serves to derive session keys for the Cryptographic Officer.
Remote Session Authentication Key (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 (192 bit key, 112 bits of strength)	3TDES-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).
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
FPRootCA (certificate & public key)	2048 bit RSA key	Plaintext	N/A	Serves to authenticate FDC and PKM keys
FDC (certificate & public key)	2048 bit RSA key	Plaintext	N/A	Serves to authenticate TransportKey
PKM (certificate & public key)	2048 bit RSA key	Plaintext	N/A	Serves to authenticate Cryptographic Officer
TransportKey (certificate & public key)	2048 bit RSA key	Plaintext	Internal DRBG	Serves to initially authenticate Postal mRevenector DE 2011
PSDKey (certificate & public key)	2048 bit RSA key	Plaintext	Internal DRBG	Serves to authenticate Postal mRevenector DE 2011
DPAGKey (certificate & public key)	1024 bit RSA key	Plaintext	Internal DRBG	Serves to encrypt the m_{Secret} on the Postage Point
RootCABC (certificate & public key)	2048 bit RSA key	Plaintext	N/A	Serves to authenticate FDCBC and PMD keys
FDCBC (certificate & public key)	2048 bit RSA key	Plaintext	N/A	Serves to authenticate PMDKey
PMDKey (certificate & 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.

9 Self-Tests

9.1 Power on self tests

The following self tests are performed when the Postal mRevenector DE 2011 starts:

Firmware Integrity Test

The mRevenector checks the SHA 256 hash of the Postal mRevenector DE 2011 firmware of the cryptographic module and verifies this against a known signature generated with PKCS#1 V1.5 (Signature Scheme).

Cryptographic Algorithm Tests

The following table lists the cryptographic algorithm tests for approved and allowed security functions that are performed as part of the power-on self tests. For corresponding NIST certificates see * The Approved Signature Generation and Verification functions of this RSA implementation were issued NIST Certificate #731.

Table 4.

Security Function	Type of self-test
RSA 1024 bit Decryption	Decrypt KAT
DRBG	Known answer test (KAT)
AES 128 – ECB & CBC	Encrypt and Decrypt KAT
HMAC-SHA1 & HMAC-SHA256	KAT (includes SHA KAT)
Key Agreement Scheme	KAT
RSA 2048 bit Sign/Verify using SHA-256	KAT
RSA 2048 bit Verify using SHA-256	KAT
TDES (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.

9.2 Conditional Tests

The following conditional tests are performed:

Security Function	Performed
CTR-DRBG and NDRNG	On usage: see FIPS 140-2 section 4.9.2 “Continuous RNG test 1”.
Diffie-Hellman 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”.
RSA 1024 bit	On key generation: see FIPS 140-2 section 4.9.2 “Pair-wise consistency test 2”. Runs an Encrypt-Decrypt Test.

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 non-approved hardware implemented NDRNG. Consecutive outputs of the NDRNG are compared to ensure that they differ.

9.3 Error States

In the event of an error being detected, the Postal mRevenector DE 2011 enters an error state and stores the reason (error identifier) persistently. The error state information can be retrieved via the Get Device Status service.

10 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 module's processor are present using power from the battery even when the device is switched off.