Security Policy

mRevenector 2011

Version 1.3

Hardware P/N: 580036020300/01

Firmware Version:

Bootloader: *90.0036.0201.00/2011485001*

Software-Loader: *90.0036.0206.00/2011485001*

Francotyp-Postalia GmbH
Development Department
Dirk Rosenau / Hasbi Kabacaoglu
Triftweg 21-26
D-16547 Birkenwerder
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 *mRevenector 2011* is FP's latest generation of PSD.

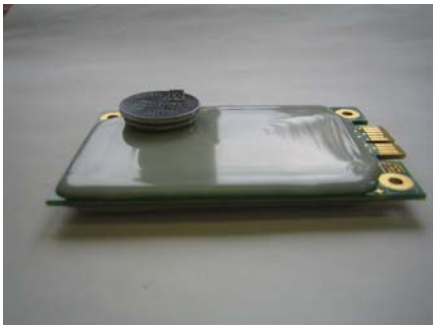

Figure: 1 *mRevenector 2011*

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 Purpose of Module

The main purpose of the Cryptographic Module is the running of the Start Firmware service. The selected firmware is authenticated and prepared for secure execution. To do this, the device must be in an authenticated role. Once the firmware has been loaded, control is passed to it.

1.3 Implementation

The *mRevenector 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.

1.4 Modes of Operation and Security Functions

The module only has one mode of operation, its FIPS Approved mode of operation. It implements the following FIPS-Approved security functions:

Security Function	Approval
AES-128 (encrypt and decrypt), ECB and CBC, as specified in FIPS 197.	NIST Certificate #1493
SHA-256 as specified in FIPS 180-2.*	NIST Certificate #1346
HMAC SHA-256 as specified in FIPS 198*	NIST Certificate #878
RSA PKCS#1 (signature verification) using SHA-256	NIST Certificate #732
DRBG as specified in NIST SP800-90 DRBG.	NIST Certificate #61

* SHA-1 and HMAC-SHA-1 were tested and included on the respective validation certificates; however, these options are not available for use in the module as configured for this validation.

Table 1: FIPS 140-2 Approved Security Functions

The module has a single, non-Approved algorithm, its hardware implemented NDRNG.

1.5 Approved Deterministic Random Bit Generator

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.

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 2: 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 3: 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

The *mRevenector 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.
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-tests as described in section 8 of this document.
11. Support the following logically distinct interfaces:
    - Data input interface
    - Data output interface
    - Control input interface
    - Status output interface
    - Power interface.

5 Roles, Services, Authentication & Identification

5.1 Roles

In the *mRevenector2011* the User and the Cryptographic Officer are the same roles and share the same services. These roles require identity based authentication.

The Default User role performs all services which do not read, update, modify or generate critical security parameters (CSPs) and does not require authentication.

5.2 Identity Based Authentication

The operator 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. After successful authentication the operator implicitly assumes the *Cryptographic Officer (CO)* or *User role.*

5.3 Services

The following services are offered by the cryptographic module. The only one that requires authentication is the Program FLASH service.

Service	Approved Security Functions Used	Associated CSPs	Roles	Notes
Reboot Device	None	None	Default User	Service to cause the device to reboot.
Get Device Status	None	None	Default User	
Scrap	None	None	Default User	Zeroizes all plaintext CSPs.
Self-Test	All listed in section 1.4	None	Default User	Performed by power-cycling the device.
Local Login	AES-CBC HMAC-SHA256 DRBG	Passphrase	CO or User	Required to enter the CO or User role.
Logoff	None	None	CO or User	Leaves the CO or User role.
Program FLASH with Firmware	RSA- PKCS#1 V1.5 verification using 2k and SHA-256	Working Encryption & Working Authentication keys	CO or User	Receives firmware from an external source and programs it into the cryptographic module's FLASH memory.
Select Programmed Firmware	None	None	Default User	Configures the bootloader.

Table 4: Services and Roles

5.4 Authentication Strength

The passphrase contains at least 6 randomly chosen characters for the *Cryptographic Officer* or *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 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	Establishment	Generation	Destruction	Purpose
Data Encryption Master Key	AES- CBC 128 bits	Plaintext	N/A	Internal DRBG	Scrap service or tamper event	Serve to encrypt and decrypt other critical security parameters.
Data Authentication Master Key (128 bit key)	HMAC-SHA256	Plaintext	N/A	Internal DRBG	Scrap service or tamper event	Serve to authenticate other critical security parameters.
Working Encryption Key	AES- CBC 128 bits	Not persistently stored	N/A	Internal DRBG	Scrap service, tamper event or power cycle	Serve to encrypt and decrypt other internally used data.
Working Authentication Key (128 bit key)	HMAC-SHA256	Not persistently stored	N/A	Internal DRBG	Scrap service, tamper event or power cycle	Serve to authenticate other critical internally used data.
DRBG State	CTR_DRBG using AES 128 bits	Encrypted	N/A	Seeded by internal NDRNG	N/A	Internal state of the Deterministic Random Bit Generator.
Passphrase	N/A	Encrypted	N/A	N/A	N/A	Identity based authentication

Table 5: Critical Security Parameters

Public Security Parameters

The following public keys are stored in the device:

- Firmware Verification Key: RSA 2048 bit certificate used to verify firmware from Francotyp-Postalia.

8 Self-Tests

8.1 Power up self tests

The following self tests are performed when the module starts (either following a power on, or following the call to a reboot service):

Firmware Integrity Test

The mRevenector checks the SHA 256 hash of the mRevenector 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 security functions that are performed as part of the power-up self tests.

Security Function	Type of self-test
AES 128 - CBC & EBC Encrypt and Decrypt	Known answer tests (KAT)
SHA-256	KAT, tested as part of RSA verification
HMAC-SHA256	KAT.
RSA 2048 verify with SHA256	KAT, includes SHA-256 verification
DBRG	KAT

Table 6: FIPS 140-2 Cryptographic Algorithm Tests

8.2 Conditional Tests

The following conditional tests are performed:

Continuous RNG Test

On each access, compares consecutive outputs of the DRBG to ensure that they differ. A Non-Deterministic Random Number Generator (NDRNG) is used for seeding the DRBG. Consecutive outputs of the NDRNG are compared to ensure that they differ.

Firmware Load Test

The module performs RSA 2048 SHA 256 signature verification for loaded application firmware.

8.3 Error States

In the event of an error being detected, the mRevenector 2011 enters an error state. The device remains in the error state until it is rebooted. The error state information can be retrieved via the Get Device Status service.

9 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.