FRANCOTYP-POSTALIA

Security Policy
Revenector
Version 1.1

NON-CONFIDENTIAL

Francotyp-Postalia AG & Co. KG
- Development Department -
D. Rosenau
Triftweg 21-26
D-16547 Birkenwerder

Table of Contents

Figures

Tables

1 Introduction

1.1 Scope

This is a Cryptographic Module Security Policy for the Francotyp Postalia Revenector. It was written for the purpose of a FIPS 140-2 validation of the Revenector. This Security Policy specifies the security rules under which the Revenector must operate. Included in these rules are those derived from the security requirements of FIPS 140-2 and additionally, those imposed by Francotyp Postalia. These rules, in total, define the interrelationship between

- The module operators,
- Module services

1.2 Overview

Revenector, shown in Figure 1-1, consists of a microprocessor controlled custom circuitry which is mounted on a printed circuit board (PCB). The hardware of Revenector is designed to protect critical security parameters as well as application specific revenues. Revenector is validated against FIPS 140-2 with a Boot Loader. The Boot Loader is a firmware which enables hosting systems to load or update signed application specific firmware. This application specific firmware is then capable of accessing its own critical security parameters (CSPs) or revenues. The application specific firmware is outside the scope of the FIPS 140-2 validation of the Revenector.
The Revenector is used by peripheral equipment also referred to as host systems. Francotyp Postalia uses the Revenector as the hardware security modules for their meter systems like the Postage Meters MyMail and UltiMail.

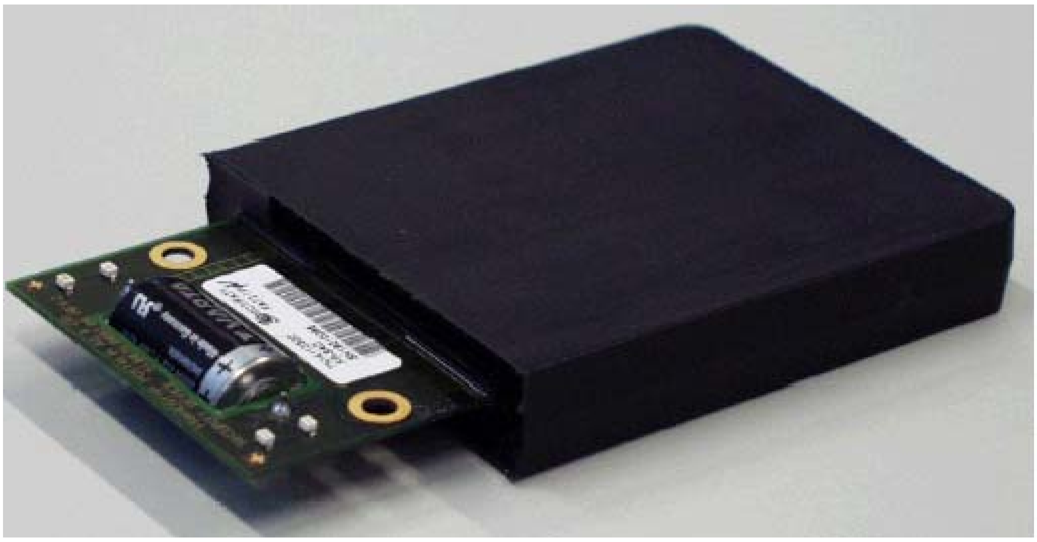

Figure 1-1: View of Revenector

1.3 Implementation and Cryptographic Boundary

The Revenector is implemented as a multi-chip embedded cryptographic module defined by FIPS 140-2. The cryptographic boundary includes all hardware components, with the exception of the battery, the connector and the LEDs, located on the Revenector. The circuitry contained within the cryptographic boundary is potted with hard opaque potting material. Revenector has been validated with two different hardware configurations. One configuration is identified under *58.0036.0001.00/05,* the other is identified under *58.0036.0006.00/02.* The following table briefly describes the differences.

58.0036.0001.00/05	This hardware configuration additionally wraps the cryptographic boundary with a tamper detecting hull and provides a separate memory area for application specific critical security parameters (CSPs) that is zeroized as response upon tamper detection.
58.0036.0006.00/02	This hardware configuration does not contain the above mentioned tamper detecting hull and separate memory area for CSPs.

Both configurations protect the electronic circuitry from unauthorized access or modification and provide tamper evidence. All parts of the Boot Loader firmware are included within the cryptographic boundary.

The version of the Boot Loader firmware is: *3.22*.

2 Security Level

Revenector is designed to meet the FIPS 140-2 security level 3 overall as shown in Table 2-1.

Table 2-1: FIPS 140-2 Security Levels

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/IMC)	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	N/A

The module meets FIPS 140-2 Level 4, Environmental Failure Protection (EFP).

3 Security Rules

The Revenector shall enforce the following FIPS 140-2 related security rules.

1. Revenector shall support the following logically distinct interfaces sharing one physical port:

   - Data input interface
   - Data output interface
   - Control input interface
   - Status output interface
   - Power interface

2. Revenector shall inhibit all output via the data output interface during self-tests and whenever an error state is entered.
3. Revenector does not support zeroization of critical security parameters because the module does not store, use, generate, or input/output critical security parameters.
4. Revenector shall not support any entry of keys or other critical security parameters.
5. Revenector shall enforce identity-based authentication.
6. Revenector shall support the following authorized roles: User role and Cryptographic Officer role.
7. Revenector shall not retain authentication of an operator when it is powered-up after being powered off.
8. Revenector shall not support a bypass mode.
9. Revenector shall be protected using a hard opaque potting material as coating.
10. Revenector shall implement environmental failure protection for temperature and voltage.
11. Revenector shall implement all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
12. Revenector shall support the following FIPS approved security functions:

    - RSA Verify as specified in PKCS#1
    - SHA-1 as specified in FIPS 180-2

13. Revenector shall conform to the EMI/EMC requirements specified in FCC Part 15, Subpart B, Class B.
14. Revenector shall perform the self tests during power on and on demand listed in section 4
15. Revenector shall output an error indicator via the status interface whenever an error state is entered due to a failed self-test.
16. Revenector shall not perform any cryptographic functions while in an error state.
17. Revenector shall not support multiple concurrent operators.

4 Self Tests

The following section lists the self tests which are performed on power up, on demand and continuously. All FIPS approved security functions that are used in the Revenector are listed, too.

Table 4-1: Self-Tests

Name	**Type**	**Description**
Software firmware integrity test		
Firmware integrity test	Power Up & On Demand	Check CRC16 of internal system firmware
Critical function test		
		none
Cryptographic algorithm test		
Security Function tests	Power Up & and on Demand	For details see Table 4-2.

Table 4-2: Security Functions

Security Function (SF)	**Approved SF**	**Type of self-test**	**Conditional test**
SHA-1	Yes, NIST Certificate #158	KAT on power up and on demand.	None
RSA	Yes, no Certificate required. Implementation according to PKCS#1	Known answer test (KAT) of supported mode (verfication) on power up and on demand.	None

5 Roles and Services

Revenector shall support two distinct roles. These roles are:

- Cryptographic Officer
- User

All services which do not read, update, modify or generate critical security parameters (CSPs) do not require authentication. These are the following Services:

Echo This service requests the Boot Loader firmware to receive arbitrary bytes and return a copy of them back to the sender.

Reboot Device This service requests the Boot Loader firmware to reboot the module.

Get Status This service requests the Boot Loader firmware for status output (e.g. : self test result, firmware version information).

Invalidate Firmware This service requests the Boot Loader firmware to erase a pre-defined location that indicates to the Boot Loader whether an application firmware is present.

> Note: The application specific firmware is not part of the module cryptographic boundary configuration and therefore this service will not affect the functionality or configuration of the module.

5.1 Cryptographic Officer

The *Cryptographic Officer* is authenticated through an RSA signature verification process, which utilizes a RSA public key. This is done implicitly by adding the signature to the requested service.

The Cryptographic Officer Role shall provide those services necessary to initially load or update application specific firmware.

The following service is provided to the *Cryptographic Officer* and requires authentication:

Firmware Download This service requests the Boot Loader firmware to load application specific firmware into the module and on success enable it to be executed. In addition a pre-defined location is written and used to indicate to the Boot Loader that application firmware is present.

5.2 User

The *User* is authenticated through an RSA signature verification process, which utilizes a RSA public key. This is done implicitly by adding the signature to the requested service.

The User Role shall provide those services necessary to initially load or update application specific firmware.

The following service is provided to the *User* and requires authentication:

Firmware Download See description above.

6 Strength of Authentication

To meet the requirements for strength of authentication, the probability shall be less than one in 1,000,000 that a random attempt will succeed or a false acceptance will occur.

This requirement is met by the above-specified authentication methods as follows:

The key size for the Cryptographic Officer is 2048 bit

For multiple attempts to use the authentication mechanism 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 requirements equals with 1667 attempts per second or a minimum time delay of 6 ms between two attempts. This time is granted by the implementation by a time delay between two authentication attempts of more than 6 ms.

7 Service to Roles Relationship

Revenector's Boot Loader firmware does not contain any critical security parameters. It does only use a public key to authenticate the Cryptographic Officer.

Table 7-1: Service to Roles Relationship

Role Service	CO-Role	User-Role
Echo	X	X
Reboot Device	X	X
Get Status	X	X
Invalidate Firmware	X	X
Firmware Download	X	X