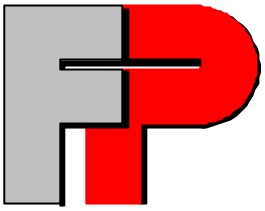

FPSM Security Policy
Version 1.4

Francotyp-Postalia AG & Co.
- Development Department -
D. Rosenau, P. Post, T. Schlaaff
Triftweg 21-26
D-16547 Birkenwerder

List of Contents

List of Figures

List of Tables

History of Documents

#	Version	Date	Authors	Comments/Modifications
1.	1.0	April 99	Rosenau	Initial revision
2.	1.1	April 99	Rosenau	Initial revision of FP
3.	1.2	April 99	Rosenau	minor changes
4.	1.3	June 99	Wagner	Clarification on Roles, Levels
5.	1.4	August 99	Rosenau	NIST Comments

1 Introduction

1.1 Scope

This Security Policy specifies the security rules under which the Francotyp Postalia Security Module, herein identified as the FPSM, must operate. Included in these rules are those derived from the security requirements of FIPS 140-1 and additionally, those imposed by Francotyp Postalia. These rules, in total, define the interrelationship between the:

1. module operators,
2. module services, and
3. security relevant data items (SRDIs) / postal relevant data items (PRDIs).

1.2 Overview of FPSM

The FPSM, shown in Figure 1, consists of microprocessor controlled custom circuitry which is mounted on a printed circuit board (PCB). The FPSM performs all of the Postage Meter cryptographic and postal security functions.

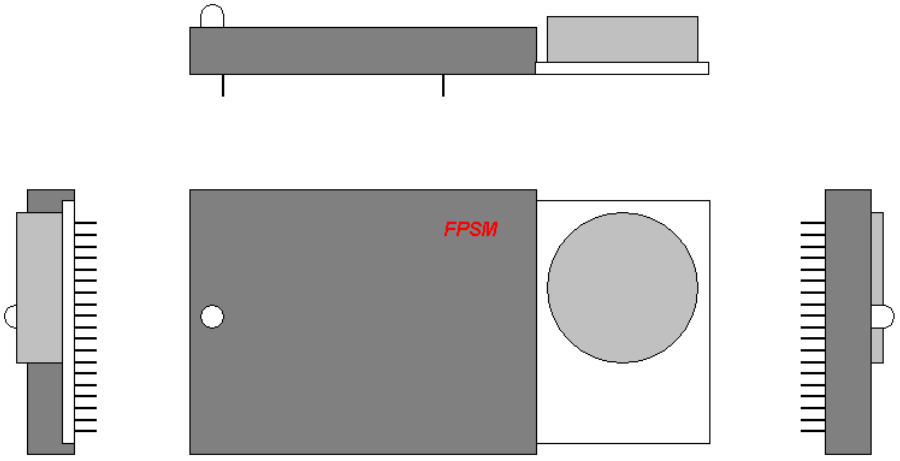

Figure 1: View of FPSM

1.3 Implementation and Cryptographic Boundary of FPSM

The FPSM is implemented as a multi-chip embedded cryptographic module defined by FIPS 140-1. The cryptographic boundary includes all hardware components, with the exception of the battery, located on the FPSM. The circuitry contained within the cryptographic boundary is potted with *hard opaque potting material*. All FPSM software/firmware is included within the cryptographic boundary.

2 FIPS 140-1 Security Level

The FPSM is certified to meet the FIPS 140-1 security levels shown in Table 1.

Table 1: FPSM Security Levels

FIPS 140-1 Security Requirements Section	Level
1. Cryptographic Module	2
2. Module Interfaces	3
3. Roles and Services	2
4. Finite State Machine Model	2
5. Physical Security	3
6. Software Security	3
7. Operating System Security	N/A
8. Key Management	3
9. Cryptographic Algorithms	2
10. EMI / EMC	3
11. Self Tests	3

3 Security Rules

The Product Module shall enforce the following security rules. These rules are separated into two categories,

1. those imposed by FIPS 140-1 and,
2. those imposed by the United States Postal Service (also referred to as the USPS or the Post).

3.1 FIPS 140-1 Related Security Rules

1. The FPSM shall support the following interfaces:
   - Data input interface.
   - Data output interface.
   - Control input interface.
   - Status output interface.
2. The FPSM shall inhibit all data output via the data output interface whenever an error state exists and during self-tests.
3. The FPSM shall logically disconnect the output data path from the circuitry and processes performing key zeroization.
4. Authentication data, secret cryptographic keys, and other critical security parameters shall be entered in encrypted form.
5. The FPSM shall inhibit all output of secret cryptographic keys.
6. The FPSM shall support an User role and a Cryptographic Officer.
7. The FPSM shall re-authenticate a role when it is powered-up after being powered-off.
8. The Product Module shall provide the following services:
   - Show Status
   - Self Test
   - Computerized Remote Meter Setting (CMRS)
   - Deinstallation

- Accounting
- Adjusting
- Check of MAC
- Data Load
- Scrap
- Go Non-Valid

9. The FPSM shall not support a bypass mode.
10. The FPSM shall enforce Role-based authentication.
11. The FPSM shall be protected using a hard, opaque removal-resistant coating.
12. The FPSM shall implement all software using a high-level language, except the limited use of low-level languages to enhance performance.
13. The FPSM shall protect secret keys from unauthorized disclosure, modification and substitution.
14. The FPSM shall provide a means to ensure that a key entered into or stored within from the FPSM is associated with the correct entities to which the key is assigned.
15. The FPSM shall deny access to plaintext secret keys contained within the FPSM.
16. The FPSM shall provide the capability to zeroize all plaintext cryptographic keys and other unprotected critical security parameters within the FPSM (Note: Items listed as Postal Relevant Data Items (PRDIs) are not considered to be critical security parameters.).
17. The FPSM shall support the following FIPS algorithms:
    - DES: for symmetric encryption / decryption.
    - DES: for message MACing.
    - 3DES: for symmetric encryption / decryption.
    - 3DES: for internal and indicia MACing.
18. The FPSM shall conform to the EMI/EMC requirements specified in FCC Part 15, Subpart J, Class B.
19. The FPSM shall perform the following self tests:
    - Power-up and on-demand tests
        - Cryptographic algorithm test.
        - Software/firmware test.
            1. All parts of code.
        - Critical functions test.
            1. Custom specific hardware test (power-up and on-demand).
            2. Postal registers test (power-up and on-demand).
            3. Real Time Clock test (power-up).
    - Conditional tests
        - Postal data load test.
20. The FPSM shall output an error indicator via the status interface whenever an error state is entered due to a failed self-test.
21. The FPSM shall not perform any cryptographic functions while in an error state.
22. The FPSM shall not support multiple concurrent operators.
23. The FPSM shall not support a maintenance role/interface.
24. The FPSM shall not implement key generation and/or a random number generator.

3.2 Postal Imposed Security Rules

1. The FPSM shall protect the postal registers against substitution and/or modification.
2. The FPSM shall provide both local and remote value/history audit mechanisms.
3. The FPSM shall provide mechanisms to disable lost meters.
4. The FPSM shall provide mechanisms to facilitate periodic electronic and physical inspection.

4 Roles and Services

The FPSM shall support two distinct operator roles. These operator roles are:

1. Cryptographic Officer Role
2. User Role

The interaction between the FPSM and the Cryptographic Officer /User is done by a set of command service messages.

The Cryptographic Officer Role is authenticated using a unique cryptographic DES key to verify the authenticity of each command service message. The Cryptographic Officer Role shall provide those services necessary to install, reinstall, and scrap a FPSM by loading all necessary data into it. This includes the following services:

- *Request Status.* This service presents all status data of the FPSM (e.g. postal register sets and its MAC, date and time, control and data limits, lifetime state and watchdog information)
- *Data Load.* This service loads all working keys into the FPSM, set and initializes the necessary counter values and time of the module.
- *Scrap.* This service forces the module to zeroize all keys and set the FPSM out of service such that no further operation is possible.
- *Go Non-Valid.* This service changes the state of the FPSM to Non-Valid.

The User Role is also authenticated using a unique cryptographic DES key to verify the authenticity of each command service message. The User Role shall provide those services necessary to use the stored keys in order to perform a secure computerized remote meter setting procedure. This includes the following service:

- *Computerized Remote Meter Setting.* This includes encrypt and decrypt of data, transferred via the data interface.

No role is required to perform the following services:

- *Request Status.* This service presents all status data of the FPSM (e.g. postal register sets and its MAC, date and time, control and data limits, lifetime state and watchdog information)
- *Deinstall.* This service deinstalls a FPSM by zeroizing the working keys.
- *Accounting.* This service performs all necessary actions to perform an accounting for a purchased amount of money.
- *Adjusting.* This service enables storage of data concerned with the time zone and lifetime.
- *Self Test.* This service starts the self test.
- *Check of MAC.* This service checks for a valid MAC to ensure the authenticity of the incoming cliché data from the Service Center.

5 Access Control

The following abbreviations are introduced:

Table 2: Abbreviation of Roles

Role	Abbreviation
Cryptographic Officer	CO
User	U

Table 3: Abbreviation of Security Relevant Data Items / Postal Relevant Data Items

Security relevant data item (SRDI) / Postal relevant data item (PRDI)	Abbreviation	Description
postal register sets (PRDI)	PR	The FPSM stores redundant register sets. These register sets store the amount of money to be franked by the franking machine.
RTC date & time (PRDI)	TI	This is the time and date information.
Control and limit data (PRDI)	LI	These data is used to set the limits of the FPSM (e.g. maximum postage, maximum ascending register,...).
Lifetime state information (PRDI)	ST	This is the variable which holds the information of the current lifetime state of the FPSM.
Watchdog information (PRDI)	WD	This information is used to disable lost meters or ensure the periodical inspection of the FPSM.
MAC of the postal registers (PRDI)	PM	This MAC is used to ensure data integrity.
Security Code (PRDI)	SC	This item is used to sign for an accounting which was done by the FPSM.
Keys (SRDI)	KE	This item stands for all of the cryptographic keys stored inside of the FPSM.
Key Counters (PRDI)	KC	These items are used during data load.
CMRS values (PRDI)	CM	These items are used by the CMRS to prevent replay attacks and enable error handling.

Table 4: Abbreviation of Access Rights on SRDIs / PRDIs

Access Right on SRDI/PRDI	Access Right on SRDI/PRDI	Abbreviation
Read	The SRDI/PRDI is read only	R
Write	The SRDI/PRDI is written by a well defined procedure and/or value.	W
Delete	The SRDI/PRDI is deleted by a well defined procedure and/or value	D
Modify	The SRDI/PRDI is readable and writeable (modified by a well defined procedure)	M

Table 5: Assignment of Management Services and Roles

Management Services		effected SRDI/PRDI										Roles		
#	Service	PR	TI	LI	ST	WD	PM	SC	KE	KC	CM	CO	U	No Role
1	Go Non-Valid				W							×		

Table 6: Assignment of Services and Roles in the Valid State

Services In Valid State		effected SRDI										Roles		
#	Service	PR	TI	LI	ST	WD	PM	SC	KE	KC	CM	CO	U	No Role
1	Request Status	R	R	R	R	R	R					×		×
2	Computerized Meter Remote Setting	M		R	W	M	M				M		×	
3	Deinstall				W				D					×
4	Accounting	M	R	R	M	M	M	S						×
5	Adjusting													×
6	Selftest	R			W		R		D					×
7	Check of MAC				W				R					×
8	Data Load	W	W		W	M			W	M	W	×		
9	Scrap				W				D			×		