FRAMA
SMART MAILING

Postal Security Device

Security Policy

FRAMA AG

PSD - I

Version:	**R01.06**
Date:	**25.05.2007**
Doc.-ID:	**DE_FNKPSD_510_SPE**
File name:	**DE_FNKPSD_510_SPE_R0106_EN.Security Policy PSD**
Author:	**Bernd Zinke, Timo Bohl, IT & E** **FRAMA AG** **Unterdorf** **CH – 3438 Lauperswil / Switzerland**
Acceptance:	**Stefan Pfeiffer, IT & E**

» Non-Confidential «

CONTENT

1 Introduction

1.1 Document overview

The following table gives a short overview of the goal of this document; it lists all relevant information sources under references. The restrictions give information about what is not described here. The primary intended audience is described as the target readers.

Document overview	
Document goal:	Show fulfillment of requirements concerning the Security Policy according to FIPS 140-2 Security Level 3, IPMAR and FRANKIT
Target readers:	Potential buyers of the module
Restrictions:	
References:	[FIPS 140-2] [FIPS 140-2 DTR] [IPMAR] [FRANKIT] [FRANKIT-DTR]

1.2 Document history

The following table records all changes that were made in this document. In case of little changes (e.g. format, spelling, minor corrections or omissions) the version number after the [.] has to be incremented. For important changes (e.g. content) the version number before the [.] has to be increased.

Date	**Version**	**Action**	**Author(s)**
13.07.2004	D01.00	Document created	Timo Bohl (TB)
09.11.2004	D01.01	Spell check	Frank Roski (FR)
18.11.2004	R01.01	Review	Stefan Pfeiffer (SP)
01.03.2005 01.03.2005 03.03.2005 04.03.2005 23.03.2005	D01.02	2.3 modified, Operational environment as not applicable 2.4.1 modified, non FIPS approved algorithms, new table included 2.4.2 new title , power analysis deleted 2.4.4.2 clarification of PRNG Table formatting, smaller corrections	Bernd Zinke (BZ) Bernd Zinke (BZ) Bernd Zinke (BZ) Bernd Zinke (BZ) Timo Bohl
01.04.2005	D01.03	Added Service ServiceRequest	Timo Bohl
14.04.2005 22.04.2005	D01.04	Extended Chapter “Access rights” Chapter “Roles” inserted table login delays , Tab 2-2 modified	Timo Bohl
12.05.2005	R01.04	Review	Stefan Pfeiffer (SP)
27.09.2005	D01.05	Changed PSD firmware version	Timo Bohl (TB)
27.09.2005	R01.05	Review	Stefan Pfeiffer (SP)
25.05.2007	R01.06	Changes according to FIPS 140-2 level 3 validation comments of last review cycle	Stefan Pfeiffer (SP)

1.3 Document structure

This document especially deals with the requirements of Appendix C: “Cryptographic Module Security Policy“ of [FIPS 140-2] and [FIPS 140-2 DTR] Security Level 3.

The specification will be sufficiently detailed to answer the following questions:

- What access does operator X, performing service Y while in role Z, have to security-relevant data item W for every role, service, and security-relevant data item contained in the cryptographic module?
  -> This requirement will be addressed in chapter 2.4.1“Security policy – security rules”.
- What physical mechanisms are implemented to protect the cryptographic module and what actions are required to ensure that the physical security of the module is maintained?
  -> This requirement will be addressed in chapter 2.4.2 ”Physical Security Policy“.
- What security mechanisms are implemented in the cryptographic module to mitigate against attacks for which testable requirements are not defined in the standard?
  -> This requirement will be addressed in chapter 2.4.3 ”Policy for mitigation of other attacks“.

2 Cryptographic module security policy

2.1 Cryptographic module definition

The cryptographic module specified in this document is the FRAMA Postal Security Device called PSD – I.

Identification of the cryptographic module hardware:

PSD – I

Identification of the cryptographic module software:

FRAMA PSD V1.0.6

2.2 Introduction

The PSD supports booking processes within postal meters as well as value loading processes in order to increase the postage credits. In detail the use of cryptographic services, like the production of cryptographic keys, the encoding, decoding or signature and signature inspection is part of PSD internal purposes to this.

The PSD is a multi-chip embedded module covered by a sealed opaque metal case with penetration tamper protection. A microprocessor mounted on a printed circuit board, executes the firmware and controls tamper detection hardware. The cryptographic boundary includes all hardware components with exception of the pin connector.

Figure 2-1 FRAMA PSD - I shows the PSD (FRAMA PSD - I). It is validated against FIPS 140-2, and is capable to reliable handle its own critical security parameters (CSP) and cryptographic keys. FRAMA use it as part of his franking meters. The franking meter is the host, connected to the PSD by a direct connected serial port, and is used also as power supply for the PSD power port.

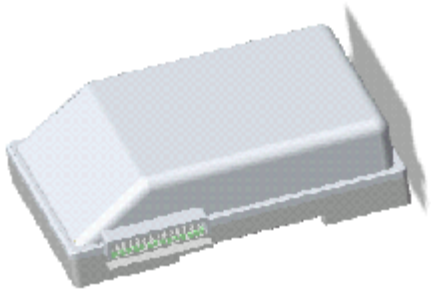

Figure 2-1 FRAMA PSD - I

2.3 Security level

The item under test was constructed to fulfil FIPS 140-2, Security Level 3:

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[1]
6	**Operational environment**	Not applicable
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

Tab. 2-1 Security level

[1] The PSD exceeds FIPS 140-2 Level 3 by an active enclosure penetration detection, and active CSP zeroization, without actually claiming that additional Level 4 requirements (e.g. EFT or EFP) are met.

2.4 Specification of the cryptographic module security policy

2.4.1 Security policy – security rules

This section specifies the security rules the FRAMA PSD enforces.

- The PSD implements the following logically interfaces sharing one physical port
  - Data input interface
  - Data output interface
  - Control input interface
  - Status output interface
  - Power interface
- The PSD performs autonomous executed power up and conditional self tests.
- The PSD inhibits all output through the data output interface during self test, key generation and any error state.
- The PSD not outputs any secret or private key.
- The PSD supports the following FIPS 140-2 specified approved algorithms
  - Triple-DES conform to NIST SP800-20
  - SHA1 conform to NIST PUB180-1
  - RSA conform to PKCS#1 V1.5
  - PRNG conform to FIPS 186-2
- The PSD supports the following none FIPS Approved Algorithms. These are used in connection with FIPS Approved Algorithms. Therefore the PSD is always used in an Approved Mode of Operation.
  - CRC32
  - Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength), conform to PKCS#3 “Diffie-Hellman Key-Agreement Standard”
  - Key generation
- The PSD supports only identity-based authentication.
- The PSD supports FIPS 140-2 specified roles, Crypto Officer and User.
- The PSD does not support multiple concurrent operators.
- The PSD not retains operator authentication data after power on. Authentication data gets lost at power down.
- The PSD does not support a bypass mode.
- The PSD software is implemented using a high-level language, except time critical functions to enhance performance.
- The PSD does not support software or firmware update.
- The PSD does not support manual entry of keys or other CSP.
- The PSD zeroizes it’s private or secret keys and CSPs if a tamper is detected.
- The PSD is protected using a metal case with penetration tamper protection.
- The PSD detects temperature and voltage failure, and cover removal or penetration.

No.	Attack	Countermeasure

No.	Attack	Countermeasure
1	Analysis of communication between PSD and external devices	All security relevant communication is realized via a trusted path and uses identity-based authentication.
2	Unauthorized decryption out of secret keys.	Secure key generation by a PSD internal hardware True Random Number Generator. Secure key management ensures a protected access to the keys.
3	Unauthorized manipulation or read out of secret keys by opening the enclosure.	Protection against opening the enclosure.
4	Unauthorized read out of secret keys by using EMI probes.	Shielded enclosure protects against spying by radiated emission. EMI line filters protect against conducted emission.
5	Unauthorized determination of secret keys by probing and penetration.	Secure enclosure protects against probing and penetration.
6	Manipulation of secret keys memory or postal application registers by chemicals and radiation.	Secure enclosure protects against chemicals and radiation.
7	Unauthorized determination of secret keys by Simple Power Analysis.	Combined hardware and software countermeasures.
8	Unauthorized determination of secret keys by Differential Power Analysis.	Combined hardware and software countermeasures.
9	Unauthorized determination of secret keys by timing analysis.	Combined hardware and software countermeasures.
10	Manipulation of secret keys memory or postal application registers.	Secure enclosure protects against several physical attacks.
11	Generation of malfunction by reverse supply polarity.	PSD internal reverse voltage protection.
12	Generation of malfunction by short cut of the power supply.	PSD internal overcurrent protection. An internal battery supplies the tamper mechanisms. The battery voltage is monitored.
13	Generation of malfunction by impermissible high supply voltage.	PSD internal overvoltage protection.
14	Generation of malfunction by impermissible low supply voltage.	PSD internal undervoltage protection. An internal battery supplies the tamper mechanisms. The battery voltage is monitored.
15	Generation of malfunction by impermissible high or low ambient temperature.	PSD internal high and low ambient temperature protection.
16	Generation of malfunction by undefined clock oscillation.	PSD internal clock generation.

Tab. 2-2 Countermeasures against attacks

2.4.2 Physical Security Policy

There are several physical mechanisms implemented to protect the cryptographic module against attacks. There are no actions required to ensure that the physical security of the module is maintained.

The cryptographic module offers the following physical security mechanisms:

Physical Security Mechanism	Recommended Frequency of Inspection	Inspection Guidance
Reverse voltage protection	not required	not required
Overcurrent protection	not required	not required
Overvoltage protection	not required	not required
Undervoltage protection	not required	not required
High and low ambient temperature protection	not required	not required
Battery-Low protection	not required	not required
Preventing undefined clock oscillation	not required	not required
Protection against chemicals and radiation	not required	not required
Protection against opening the enclosure	not required	not required
Protection against probing and penetration	not required	not required
Tamper detection	not required	not required
Tamper response and zeroization	not required	not required

Tab. 2-3 Physical Security Mechanisms

End of Life

Under normal conditions the PSD will have its end of life when the customer will buy a new franking machine and/or will return the old franking machine in exchange for a new one. In this case FRAMA will perform a termination process[2], during which FRAMA will trigger zeroization by physical tampering of the PSD.

[2] The termination process includes franking out the credit remaining on the franking machine, claiming the remaining credit at a local post office, and de-registration of the machine by giving notice to the local postal organization. The machine and the PSD will then be properly disposed of according to national laws, and as the first corresponding step FRAMA will zeroize the PSD contents by physical tampering.

2.4.3 Policy for mitigation of other attacks

The item under test implements security mechanisms to mitigate the following “Other attacks”:

- Simple- and Differential Power Analysis (SPA/DPA)
- Differential Fault Attack (DFA)
- Timing Attacks

Protection is based on an appropriate Hardware Design of the internal power management, using DC/DC converter, optocouplers and voltage regulator. Exponent and message blinding are implemented to mask timing and power consumption behavior.

Other attacks	Mitigation mechanism	Specific limitations
SPA	Appropriate Hardware Design of the internal power management, and an appropriate Algorithm implementation.	Mechanisms may be broken by newer attacks.
DPA	Appropriate Hardware Design of the internal power management, and an appropriate Algorithm implementation.	Mechanisms may be broken by newer attacks.
DFA	The PSD does not return false calculation results, or intermediate values. Key establishment is restricted.	Unknown
Timing Attacks	Appropriate Algorithm implementation.	Mechanisms may be broken by newer attacks.

Tab. 2-4 Mitigation Of Other Attacks

2.4.4 Identification and authentication policy – Roles & Services

Identification and authentication are specified in the I&A policy as follows.

2.4.4.1 Roles

The following table specifies all roles an operator of the cryptographic module can take with the corresponding authentication data.

Role	Type of authentication	Authentication data
Crypto Officer	Identity based	Password, name
User	Identity based	Password, name

Tab. 2-5 Roles and required identification and authentication

Authentication Mechanism	Strength of Mechanism
Login with Name and Password	worst case 256^6 up to 256^{30} multiplied by $256^{(1..20)}$ statistically 128

Tab. 2-6 Strengths of the Authentication Mechanisms

The strengths of authentication mechanism is 256 to the power of 6 in worst case scenario and statistically $\frac{128^6}{2}$. The probability to randomly find the password is smaller than 1 to 1.000.000.
Additionally the name can be 1 up to 20 alphanumeric characters.
Each false try will increase the reply time exponentially, starting at 0.5 seconds.

The following table demonstrates the delay between false logins and shows the time offsets at where a newly login retry can be executed if the previous failed.

Attempt Number	Executable after Seconds	Delay in Seconds
1	0	0.5
2	0.5	1
3	1.5	2
4	3.5	4
5	7.5	8
6	15.5	16
7	31.5	32
8	63.5	64

Tab. 2-7 Delay between false logins

Therefore only 7 retries are possible within 1 minute.
The probability to find the Password within one minute may than be calculated as:

$7 : \left(\frac{128^6}{2}\right)$ = ~3,18323e-12

2.4.4.2 Services

The PSD offers several services for which in most cases an authentication of an operator within a specific role is necessary.
The following table lists all crypto module services, and describes which role authentication is necessary to execute it.

If none of the roles is necessary, an authentication is also not necessary. This is only applicable for services which do not modify, disclose or substitute cryptographic keys and CSPs. These Services do not even read the memory of such values.

Role			Approved mode of operation	
Non Authorized	User	Crypto Officer	Authorized Services	Signature needed
		X	Do self test	
	X	X	Get status (is adequate to the Sow Status Service of FIPS)	
	X		Value franking, (modify counter and registers)	
		X	Zero franking, NOT decrementing a counter	
		X	Generate private key (RSA)	YES
		X	Set public key	YES
		X	Recredit, (monetary load)	YES
		X	Get recredit log	
		X	Reset recredit log	YES
	X	X	Service Request	
	X	X	Get usage statistic	

Tab. 2-8 Authorized Services

Role			Non approved mode of operation	
Non Authorized	User	Crypto Officer	Unauthorized Services	Signature needed
X	X	X	Login	
X	X	X	Get the FRM ID	
X	X	X	Get time	
X	X	X	Get current register	

Tab. 2-9 Unauthorized Services

To guarantee the reliable functioning of the security module, several self tests are implemented.
Power up tests will be executed at every start up. The power up test checks the hardware, the software and memory integrity, the cryptographic algorithms and the true random number generator.
The hardware test verifies the serial number stored in memory, is equal to the serial number of the hardware serial number chip. The battery voltage will be tested to signal the operator if the battery becomes weak.
The firmware test verifies the firmware consistency by a checksum. The calculated checksum will be compared with the checksum stored in memory.
The other self tests verify integrity of all memory blocks, which contains logically grouped data. Also the integrity of PSD keys and the public manufacturer and country keys will be tested.
Statistical random number generator tests verify the output of the PRNG to be really random. The FIPS recommended statistic tests are implemented for this purpose (these tests are no longer required by FIPS 140-2 in its current version, nevertheless they are implemented in the module). The implemented random number generator is conformant to FIPS 186-2.

Finally each implemented and FIPS approved cryptographic algorithm will be tested by known answer tests. Tested algorithms are Triple-DES, SHA1, RSA where RSA will be tested for signature creation and encryption.

Test	Type	Description
Hardware test		
Hardware ID check	Power up, on demand	Tests if the stored Id matches the serial number chip
Battery check	Power up, on demand	Checks the battery voltage
Software/Firmware test		
Firmware test	Power up, on demand	Checksum verification
Other self tests		
Memory consistency	Power up, on demand	Checksum verification
Key consistency	Power up, on demand	Checksum verification
Statistical random number generator tests (no longer required by FIPS 140-2, nevertheless implemented)		
Mono bit test	Power up, on demand	Checks proportionality of ones and zeros
Poker test	Power up, on demand	Checks proportionality byte value occurrences
Runs test	Power up, on demand	Checks occurrence of runs (same bits in a row)
Long run test	Power up, on demand	Checks occurrence of long runs
Cryptographic algorithm test		
Triple-DES test	Power up, on demand	Known answer test
SHA1 test	Power up, on demand	Known answer test
RSA encryption test	Power up, on demand	Known answer test
RSA signature test	Power up, on demand	Known answer test
Conditional tests		
Pair wise consistency test	Conditional	Checks generated RSA key after creation
Continuous random number generator test	Conditional	Checks function of the PRNG continuously

Tab. 2-10 Self tests

2.4.4.3 Cryptographic keys and CSPs

The cryptographic security module uses cryptographic keys and CSPs as follows:

Key name	Description
VRCAK	Verification RootCA Key (Certifying authority)
VMCAK	Verification ManufacturerCA Key
VCOK	Verification Crypto Officer Key (not the FIPS role!)
VECK	Verification ECPS Key
VMSK	Verification Manufacturer Software Key
VCCAK	Verification CountryCA Key
VFOK	Verification Finance Officer Key
VPOK	Verification Postal Officer Key
EPOK	Postal Officer Key
VRSCK	Verification Remote Setting Center Key (RRC)
VPMK	public Verification PSD Master Key
SPMK	private Signature PSD Master Key
EPMK	public Encryption PSD Master Key
DPMK	private Decryption PSD Master Key
EAFK	public Encryption AFM Key
DAFK	private Decryption AFM Key

Tab. 2-11 Cryptographic keys

Authentication data	Description
M_{Secret}	Secret Postage Point security attribute
FrmId	FRM ID, Board number and Hardware serial number
PostageID	Postage Point provided credit information
Crypto String	Postage Point provided secret value

Tab. 2-12 Authentication data

The table lists postal account data, reflecting the usage within the AFM.
The counters are integral values which counts created imprints, or zero imprints.
The registers handle monetary credit and consumption values.
The recredit log data element is a complex structured list of previous recredit results.
Listed if successfully or failed including the fail reason.

Other critical data	Description
UC	Usage Counter since last recredit
PC	Piece Counter
ZC	Zero franking Counter
UR	Usage monetary Register
DR	Descending monetary Register
AR	Ascending monetary Register
RECREDIT_LOG	Log list of recredit attempts

Tab. 2-13 Other critical data

2.4.5 Access control policy – authentication

The table Tab. 2-8 Authorized Services specifies for each role, the services an operator is authorized to perform within that role.

None of the FIPS roles has direct access to CSP or key data. Every modification to them must be authorized by a digital signature of an appropriate authority and it's key.
The following table lists Read (R) or Write (W) accesses to keys and other security data by the specified services, and which role has indirect access to them (X) (only via serial interface).

Cryptographic keys and CSPs	Do self test	Get status	Value franking	Zero franking	Generate private key	Set public key	Recredit	Get recredit log	Reset recredit log	Get usage statistic		User role	Crypto Officer role
VRCAK	R					RW							X
VMCAK	R					RW							X
VCOK	R				R	W							X
VECK	R					W							X
VMSK	R					W							X
VCCAK	R					RW							X
VFOK	R					W	R		R				X
VPOK	R					W							X
EPOK	R					W							X
VRSCK	R					W							X
VPMK	R				W								X
SPMK	R				W			R					X
EPMK	R				W								X
DPMK	R				W								X
EAFK	R				W								X
DAFK	R				W								X
M_{Secret}	R		R	R			W					X	X
FrmId	R		R	R				R	R			X	X
PostageID	R		R	R			W					X	X
Crypto String	R		R	R			W					X	X
UC	R		W				W			R		X	X
PC	R		W							R		X	X
ZC	R			W						R		X	X
UR	R		W				W			R		X	X
DR	R		W				W			R		X	X
AR	R		W				R			R		X	X
RECREDIT_LOG	R						W	R	W				X

Tab. 2-14 Access Rights within Services

How this table shall be read will be demonstrated in the following examples.

M_{Secret}:
M_{Secret} will be read during the self test to be verified. Also when “Value Franking” or “Zero franking” will be executed M_{Secret} is necessary to read, to create the matrix code.
During “Recredit” it will be replaced (overwritten) if a newer M_{Secret} has been send with.
Indirect read access has an operator within User role if he executes “Value Franking”.
Indirect read access has an operator within Crypto Officer role if he executes “Do self test” or “Zero franking”, and write access if he executes “Recredit”.

Indirect access does not mean that he will get access to the memory where the value is stored. Access is always wrapped by communication messages.
Read is meant for the value to be accessed by a service and not modified. Write says the value will be modified by an executed service but the operator has not directly access to it.

DPMK:
The key DPMK will be read during self test to verify its integrity. It may be overwritten with a newer generation of key if the RRC activates this key. Both services can only be executed with an operator in role Crypto Officer.

AR:
The ascending register (AR) will be read during self test as part of verification of the statistic integrity. Value franking will write (increment) the value if an appropriate operator (User role) is logged in. During Recredit and Get usage statistic, the value will be read to be send within the data output of the service.

3 Appendix

3.1 Literature

3.1.1 Standards

[FRANKIT]	FRANKIT Digitale Freistempelung der neuen Generation, Deutsche, Post AG, Version 1,3a, 15.Mai.2003.
[FRANKIT DTR]	Prüfvorgaben für die Zulassung von Systemen zu digitalen Freistempelung der neuen Generation, Deutsche, Post AG, Version 1,1, 31.07.2003.
[FIPS 140-2]	Security requirements for cryptographic modules, National Institute of Standards and Technology, FIPS Pub 140- 2, 25.05.2001
[FIPS 140-2 DTR]	Derived Test Requirements for FIPS 140-2, National Institute of Standards and Technology, FIPS Pub 140- 2DTR, 12.02.2003

3.2 Abbreviations

AFM	Absenderfreistempelmaschine / Digital Postal Meter
AR	Ascending monetary Register
CRC32	Cyclic Redundancy Check 32 bit
DR	Descending monetary Register
ECPS	Electronic Cliché Programming System
FIPS	Federal Information Processing Standard
FRM	FRAMA Revenue Module
PSD	Postal Security Device, represents the cryptographic module in this document
PC	Piece Counter
PRNG	Pseudo Random Number Generator
RSA	Rivest Shamir Adleman
SHA1	Secure Hash Algorithm 1
TRNG	True Random Number Generator
UC	Usage Counter since last recredit
UR	Usage monetary Register
ZC	Zero franking Counter
Triple-DES	Triple Data Encryption Standard

3.3 List of illustrations

3.4 List of tables