



PSD MODEL 145, 146, 147, 148

SECURITY POLICY

Version 27

Distribution List

Reference of the document (identification and localization):			
PSD – OTH – SecurityPolicy.doc			
(eRoom) R&D Cross-Projects eRoom > Cross-Project R&D Interface Documents			
Writer			
ROLE	NAME	DATE	VISA
Technical Architect	Nathalie Tortellier/Setonnougbo Hodonou/Jean-Marc Maurizio/RaksmeY Taing		
Validation List			
ROLE	NAME	DATE	VISA
PSD Software Manager	Christophe Cubilier		
Project Manager	François Bousquet		
Diffusion List			
Validation list, plus :			
ROLE	NAME(S)		

List of Changes

REVISION	DATE	REVISION CAUSE, MODIFICATION
1.0	16/02/2007	Creation
2.0	12/03/2007	Modification after IGL remarks
3.0	19/03/2007	Add Triple-DES Keys for France
4.0	22/03/2007	Cut Security Policy in 2 documents : 1 for Canada, 1 for US
5.0	18/10/2007	Final release
6.0	30/10/2007	Update model names
7.0	14/12/2007	Update PSD versions
8.0	1/17/2008	Update PSD versions and indicate CSPs zeroization process
9.0	2/13/08	Add zeroization service
10.0	10/03/2008 05/08/2008	Add the locking conditions (transition to “LOCKED” state) Update PSD versions
11.0	08/09/2009	Suppress locked conditions
12.0	20/10/2008	Update PSD versions
13.0	05/01/2009	Update PSD version (22.4)
14.0	11/06/2009	Update PSD version (22.4.3)
15.0	16/03/2010	Correction of Hasler PSD model. Add Alpha 1 PSD model.
16.0	17/03/2010	Update PSD version (22.17)
17.0	24/06/2010	Update PSD version (22.17.1). Add SYMPHONY PSD model.
18.0	09/02/2011	Update PSD version (23.06) scanner version.
19.0	07/06/2011	Append a new PSD PCB part number
20.0	07/02/2012	Correct Symphony PSD Model
21.0	27/03/2012	Update PSD version (23.08)
22.0	22/02/2013	Add References to IMI + Add ECDSA algorithm
22.1	27/03/2013	Remove references to previous models
22.2	14/05/2013	Change Hasler PSD Models + Remove mention to PSD Models in algorithms definition
23	30/05/2013	Penumbra Additions following new NIST requirements + Minor corrections
24	22/07/2013	Fix Diffie-Hellman Parameters Size + Add details on Diffie-Hellman parameters
25	08/10/2013	Modifications following Penumbra suggestions
26	08/10/2013	Added HMAC-SHA-1 KAT to match implemented self-tests
27	12/18/2013	Set Area 6 to N/A per CMVP guidance

The writer of the document is responsible for sending the last validated revision to the whole distribution list.

Contents

DISTRIBUTION LIST 2

LIST OF CHANGES 3

CONTENTS 4

FIGURES 6

1 INTRODUCTION 7

1.1 System Overview 7

1.2 Purpose of the Document 7

 1.2.1 Scope 7

1.3 Reference Documents 7

1.4 Terminology 8

 1.4.1 Acronyms and Abbreviations 8

2 SECURITY LEVEL 10

3 PSD MODULE OVERVIEW 11

3.1 I/O Port 11

3.2 Life Cycle States 12

4 MODES OF OPERATION 14

4.1 Approved mode of operation 14

4.2 Non-FIPS mode of operation 14

5 ROLES, SERVICES AND AUTHENTICATION 15

5.1 Neopost Administrator (Crypto-Officer roles: Postal User, Region, Root, Postal Crypto-Officer and Field Crypto-Officer) 16

 5.1.1 Resetting 17

 5.1.2 Update Registration 17

 5.1.3 Withdraw 17

 5.1.4 Rekey 17

5.2 File Signer Tool (Other role: R&D Signer role) 18

5.3 Expertise Tool (Other role: Unauthenticated User role)..... 18

5.3.1 Read status data..... 18

5.3.2 Zeroize CSPs..... 18

5.4 Customer (User role: Printing Base role)..... 18

5.4.1 Initiate/End Postal Core Connection..... 19

5.4.2 Initiate/End Rekey Connection 19

5.4.3 Postal Indicium 19

5.4.4 Other Base Services..... 19

5.4.5 Read Status Data 19

6 SECURITY RULES 19

6.1 Authentication Rules..... 19

6.2 CSP/Key Overview..... 20

6.3 TLS Configuration 20

6.4 PSD Key Generation..... 20

6.4.1 RSA Key Generation 20

6.4.2 AES Key Generation..... 21

6.4.3 ECDSA Key Generation 21

6.5 Conditional Self Test Rules 21

6.6 Power Up Self-Test Rules 21

6.7 CSP Storage..... 22

6.8 Tamper Response 22

6.9 Operational Environment..... 23

6.10 Status Indication..... 23

6.11 Operators/Customers..... 23

7 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSP)..... 23

8 DEFINITION OF PUBLIC PARAMETERS 26

9 DEFINITION OF CSP MODES OF ACCESS 26

10 DEFINITION OF PUBLIC PARAMETERS MODES OF ACCESS 28

11 APPENDIX A: RELATIONS TRANSACTIONS/STATES 30

12 APPENDIX B:RELATION SERVICES/ROLES 31

Figures

Figure 1 – PSD Life Cycle 12

1 Introduction

1.1 System Overview

The Neopost Postal Secure Device (PSD) is a module embedded within the Alpha, Delta and Omega postal franking machines. Integrated within the PSD are a cryptographic sub function and postal services sub function.

The postal services relate to the ultimate objective of the PSD which is to store postage credit belonging to a customer until it is needed by the indicium dispensing system of the franking machine. The indicia are dispensed in the form of a digitally signed image. This image is a unique bit pattern that can be determined to have originated from a particular PSD at a particular point in time.

The cryptographic functions are used to restrict access to postal services and to authenticate, where necessary, postal service output.

The module configuration under FIPS 140-2 validation is:

United States PSD Configuration:

- Hardware P/N 4150859LB
- Firmware P/N A0015972B, Version 28.02

The official name of the Delta PSD is "PSD Model xxx", where xxx is a 3-digit number that corresponds with the module used in Alpha1, Alpha2, Delta and Omega franking machines marketed as Hasler/Neopost in Standard/Governmental configurations.

- PSD Model 145: Hasler ALPHA1 USPS IMI Government
- PSD Model 146: Hasler ALPHA1 USPS IMI Commercial
- PSD Model 147: Neopost ALPHA1 USPS IMI Government
- PSD Model 148: Neopost ALPHA1 USPS IMI Commercial

1.2 Purpose of the Document

1.2.1 Scope

This document contains a statement of the security rules under which the PSD module must operate. A number of these rules are wholly or partially a consequence of the general franking machine environment in which the PSD is intended to be placed and for this reason a brief description of this environment is included.

1.3 Reference Documents

General Documents (procedures, guides, templates, manuals, etc.):

Id	Title	Reference	Accountable
1	Spécification Technique de Besoin – Machines à Affranchir Connectées	SP 6414 Vers 2.d	DTC
2	Information Based Indicia Program (IBIP) Performance Criteria for information – based indicia and security architecture for closed IBI postage metering systems	PCIBI – C	USPS
3	FRANKIT - New Generation - Digital Franking	V2.06	DPAG

Id	Title	Reference	Accountable
4	FRANKIT Admission Requirements for next generation digital metering systems	V2.06	DPAG
5	Postal franking machine approval process	V3.0	ROYAL MAIL
6	Security Requirements for Cryptographic modules, Federal Information Processing Standards Publication	FIPS140-2	NIST
7	The TLS Protocol Version 1.0	RFC 2246	Internet Society
8	Information Technology - Open Systems Interconnection - The Directory: Authentication Framework	ITU-T Recommandation X509	Telecommunication Standardization Sector of ITU
9	Secure Hash Standard, Federal Information Processing Standards Publication	FIPS 180-2	NIST
10	PKCS #1 v1.5 RSA Cryptography Standard		RSA labs
11	ANSI X9.17 standard, Financial Institution Key Management (Wholesale)		ANSI
12	Specification for the Advanced Encryption Standard (AES), Federal Information Processing Standards Publication	FIPS 197	NIST
13	Intelligent Mail Indicia (IMI) Performance Criteria	IMI-PC	USPS
14	ANSI X9.62 Public Key Cryptography for the Financial Services Industry, The Elliptic Curve Digital Signature Algorithm (ECDSA)	ANSI X9.62	ANSI

1.4 Terminology

1.4.1 Acronyms and Abbreviations

Abbreviation	Description
AES	Advanced Encryption Standard (Reference [12])
Triple-DES	Triple-DES : symmetric encryption algorithm build using 3 executions of DES (actually 2 Encrypt and 1 Decrypt for Encryption). Key length 112 bits or 168 bits
CSP	Critical Security Parameter
DPAG	Deutsche Post A.G. : German Post Office
DTC	Direction Technique du Courrier : French Post Technical Service

Abbreviation	Description
EFPP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMI	Electromagnetic Interference
EMC	Electromagnetic Compatibility
ECDSA	Elliptic Curve Digital Signature Algorithm
FIPS	Federal Information Processing Standards Publication : US standards to be complied with to get access to US administrative and governmental markets
FKT	Reference to the German with FRANKIT features (Reference [3])
IBIP	Information-Based Indicia Program : USPS Program for "Intelligent Indicia" spec
IMI	Intelligent Mail Indicia: New USPS Indicia spec
I/O	Input / Output
MTBF	Mean time between failures
NIST	National Institute of Standards and Technology : Part of US Department of Commerce in charge of publishing and managing FIPS standards
NVEM	Non Volatile Electronic Memory
PSD	Postal Secure Device
PKI	Public Key Infrastructure
RNG	Random number generator
RSA	An algorithm for encryption/decryption and signature/verification (Rivest Shamir Adleman) (Reference [10])
SHA-1 or -2	Secure Hash Algorithm (Reference [9])
USPS	United State Postal Service : US Post-Office

2 Security Level

The PSD is a multi-chip embedded cryptographic module as defined in FIPS140-2 (reference [1], [2], [3], [4]). The PSD module shall meet the overall requirements for Level 3 security as defined in reference [6]. The following table shows the security level requirement, as defined in reference [6], for each area of the PSD: -

Security Requirements Section	Level
Cryptographic Module	3
Cryptographic Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Machine	3
Physical Security	3 + EFP/EFT
Operating System Security	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

3 PSD Module Overview

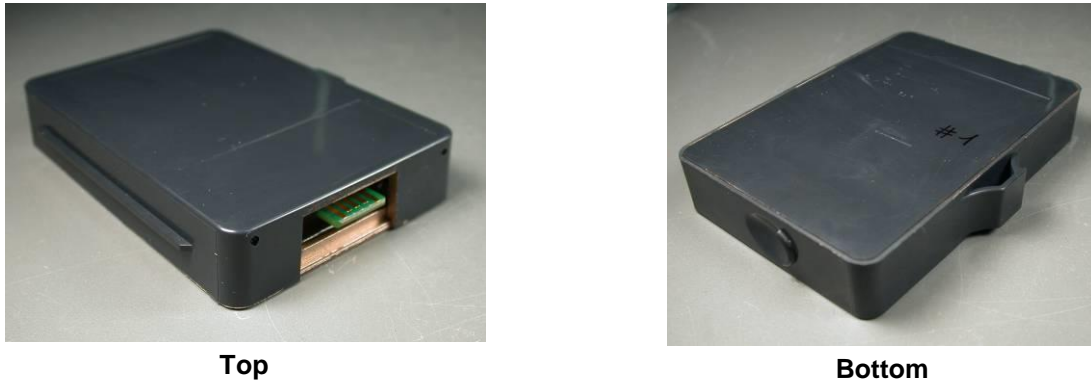


Figure 1 – Postal Security Device module (PSD)

The PSD (Figure 1) consists of a cryptographic sub function and postal services sub function sharing common hardware that is contained on a printed circuit board and enclosed within a hard opaque plastic enclosure encapsulating the epoxy potted module which is wrapped in a special tamper detection envelope with a tamper response mechanism that zeroizes all plaintext CSPs. This enclosure constitutes the cryptographic physical boundary.

Note: The module’s epoxy hardness is proven within the module’s normal operating temperature range (between -30°C and 84°C); no assurance is provided for Level 3 hardness conformance at any temperature outside this range.

The PSD contains dual redundant non-volatile electronic memories, which enables both critical security parameters and postal related data items to be stored in duplicate if required. Duplicate storage is typically used to increase MTBF.

The PSD will input and output authenticated data which requires the services of the cryptographic sub function. The PSD will also input and output certain other data that has no security implications and that is permitted to pass freely across the cryptographic physical boundary. This latter data relates to the general control and use of the franking machine in which the PSD is embedded.

3.1 I/O Port

To enable communication with a base, the module provides a 10-pin serial communication physical edge connector (RS232 communicating at 921,600 bits per second). Power input, data input, data output, control input, and status output interfaces are logically assigned. The base is the main function that controls a transport motor, an indicium dispensing system, a display and a keypad. Keys and CSPs are always input and output from the module encrypted through the serial interface. No plaintext CSPs are input or output from the module through this serial interface.

PIN	Description	Interface Type
1	Ground	
2	Ground	
3	RX	Data In/Control
4	RX	Data In/Control
5	TX	Data Out/Status
6	TX	Data Out/Status
7	Power (5V – 17V)	Power
8	Power (5V – 17V)	Power
9	Ground	
10	Ground	

Table 1 – Interface

3.2 Life Cycle States

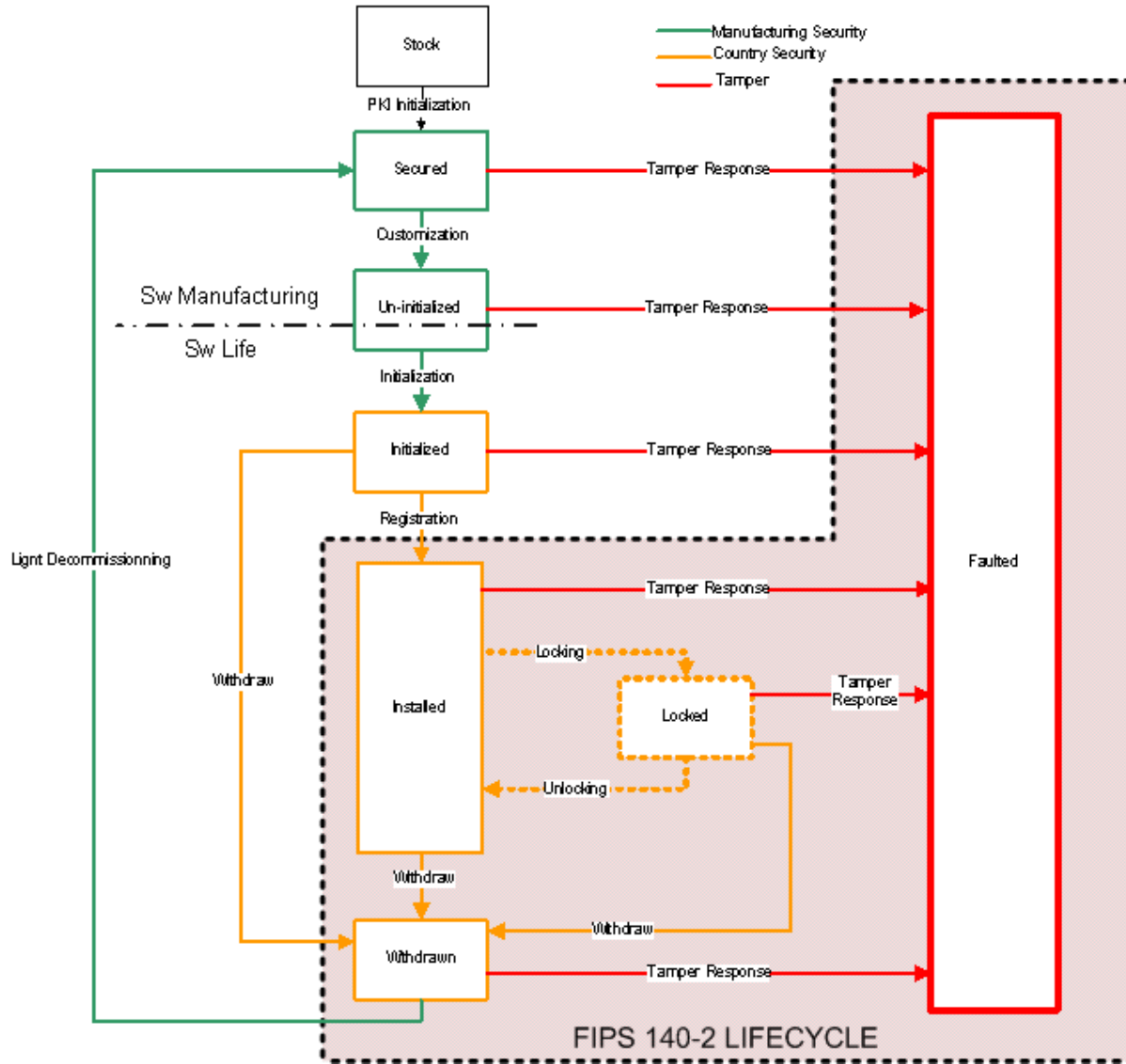


Figure 1 – PSD Life Cycle

The PSD assumes one of seven main overall states during its life cycle. These states are relevant to the accessibility of cryptographic services. The states are:

- Stock**
 This is the default at manufacture. The PSD does not contain the cryptographic parameters necessary to support interaction with the Neopost Infrastructure. A PKI-initialisation is required.
- Secured**
 The PSD contains the cryptographic parameters necessary to support interaction with the Neopost Infrastructure but has not yet been configured for a country.
- Uninitialized**
 The PSD has been configured for a country but does not contain the postal cryptographic parameters necessary to this country. An initialisation with the corresponding Neopost Postal Infrastructure is required.

- **Initialized**

The PSD contains the cryptographic parameters necessary to this country but has not yet been registered with the corresponding Neopost Postal Infrastructure.

Module's FIPS 140-2 Lifecycle States

- **Installed**

The PSD is registered with the corresponding Neopost Postal Infrastructure and may perform postal functions.

- **Locked**

The PSD is temporarily locked and can't perform printing.

- **Withdrawn**

The PSD is withdrawn from the corresponding Neopost Postal Infrastructure and may not perform postal functions. It cannot go back to the 'Initialised' state until it has undergone a factory process, which will reconfigure the contents of the PSD system memory.

- **Faulted**

The PSD is faulted due to self-test failure, Zeroization service or tamper attempt and may not perform cryptographic functions. The only available function is Get Status in an un-authenticated way.

In this document, only the FIPS life cycle states of the PSD are described.

4 Modes of Operation

4.1 *Approved mode of operation*

The cryptographic module supports the following FIPS Approved algorithms:

- RSA with variable key sizes (1536 and 2048 bits key sizes) for
 - As used within TLS v1.0 protocol: Sign(1536 bits key size) / Verify(2048 bits key sizes) Signature/Verification of signed X509 certificates used by TLS v1.0 Handshake protocol for authentication
 - Verify – verification of signed files imported into the module (1536 bits key size)
(See RSA Validation Certificate # 260)
- AES CBC with 128 bits key size for
 - Encryption/Decryption of:
 - CSPs for storage within the module
 - Data exchanged with the base or servers using the TLS protocol
 (See AES Validation Certificate # 563)
- HMAC-SHA-1
 - Authentication of TLS messages
(See HMAC Validation Certificate # 300)
- SHA-1, SHA-256 for hashing
(See Secure Hash Standard Validation Certificate # 629)
- ECDSA p224 for
 - Indicia authentication
(See ECDSA Validation Certificate # 385)
- TLS¹ KDF for
 - TLS keys derivation
(See CVL Validation Certificate #96)

Furthermore, the Delta PSD module offers key generation services:

- RSA key pair generation
- AES key generation
- ECDSA key pair generation using extra random bits
- Diffie-Hellman used for key agreement of TLS master secret during TLS Handshake protocol (DH $Y_{Client/Server} = 1024$ bits) (key establishment methodology provides 80 bits of security)

For random value generation and generation of all cryptographic keys listed above, the PSD module relies on an implemented deterministic random number generator (DRNG) that is compliant with ANSI X9.31 with 16 bytes seed (externally generated by FIPS validated module and imported into the module in secure factory environment) which has 90-bits of entropy and based on AES as transition function. This DRNG is FIPS Approved; see Random Number Generator Validation Certificate # 328.

4.2 *Non-FIPS mode of operation*

The module always operates in Approved mode of operation.

¹ The TLS protocol has not been reviewed or tested by the CAVP and CMVP

5 Roles, Services and Authentication

The PSD assures an identity-based authentication. The PSD shall support different identities. Each identity has one or several roles. The PSD authorizes transactions according to the state of the module and services according to the role. Transactions are defined for the rest of this document as an ordered sequence of services.

These allowable identified entities are:

- Expertise Tool
- Customer (Printing Base)
- Neopost Administrator (Field Server)
- File Signer Tool

Except for “Expertise Tool” which is unsecured, the identity-based authentication is a certificate-based authentication with TLS secure protocol.

The following table gives the link between the type of authentication and the identified entity for the PSD:

IDENTIFIED ENTITY ▸	EXPERTISE TOOL	NEOPOST ADMINISTRATOR	CUSTOMER (PRINTING BASE)	FILE SIGNER TOOL
AUTHENTICATION ▾				
No Authentication (Unsecured)	✓			
Mutually authenticated TLS (Secured)		✓	✓	
Authentication by signature and certificate chain (Secured)				✓

The allowable roles of the system are:

- Printing Base
- Postal User
- Postal Crypto-Officer
- Field Crypto-Officer
- R&D Signer

- Region
- Root
- Unauthenticated User

The following table gives the link between the identity and role for the PSD:

ROLE ▾	PRINTING BASE	POSTAL USER	POSTAL CRYPTO OFFICER	FIELD CRYPTO OFFICER	R&D SIGNER	REGION	ROOT	UNAUTHENTICATED USER
IDENTIFIED ENTITY ▾								
Expertise Tool								▾
Customer (Printing Base)	▾							
Neopost Administrator		▾	▾	▾		▾	▾	
File Signer Tool					▾			

Where transactions have a state dependency, the PSD must be first placed into an appropriate FIPS life cycle state. The relationship between PSD transactions and states is summarised in Section 11 - Appendix A: Relations transactions/states.

The relationship between PSD services and roles is summarised in Section 12 – Appendix B: Relation services/roles.

5.1 Neopost Administrator (Crypto-Officer roles: Postal User, Region, Root, Postal Crypto-Officer and Field Crypto-Officer)

The Neopost Administrator has available some transactions necessary to control, sustain, and monitor the postal operation of a PSD – Postal Core Services (i.e. postage funding, usage auditing, withdrawal, etc.). The transactions require the PSD to be in an appropriate state (see Section 11 - Appendix A: Relations transactions/states).

The Neopost Administrator can have the following Crypto-Officer roles and associated services:

Postal User role: The services available to the Postal User role are:

- Postal Core Services
 - Resetting Transaction
 - Update Registration Transaction
 - Withdraw Transaction

- Rekey Transaction

- Read Status Data

Postal Crypto-Office role: The service available to the Postal Crypto-Officer is:

- Generate Stamp Key

Field Crypto-Officer role: The services available to the Field Crypto-Officer role are:

- Generate PKI Key
- Get PKI Certificate
- Set PKI Certificate

Root role: The services available to the Root role are:

- Verify Region Certificate
- Verify Root Certificate

Region role: The service available to the Region role is:

- Verify Device Certificate

The Neopost Administrator has available some services (included in previous transactions) to initialize and maintain the parameters within the PSD that are necessary for interaction with the Neopost infrastructure.

For each transaction, the Neopost Administrator and the PSD are authenticating each other (with the TLS secure protocol).

5.1.1 Resetting

This transaction will carry out the following actions:

- The PSD sends its postal data
- The PSD sends its postal statistics
- The PSD generates the stamp authentication key pair if necessary (using the services “Generate Stamp Key”)
- Adjust the date and time of the PSD
- Set the funds to the PSD

5.1.2 Update Registration

This transaction will carry out the following actions:

- The PSD sends its postal data
- Update the information linked to the country or to the customer to the PSD

5.1.3 Withdraw

This transaction will carry out the following actions:

- Set the PSD state to WITHDRAWN
- The PSD sends its postal data to the server

5.1.4 Rekey

This transaction will carry out the following actions:

- If necessary, generate a new communication key (using the service “Generate PKI Key”) (see Section 7 - Definition of Critical Security Parameters (CSP))
- Update the chain of certificates (using the service “Get PKI Certificates”)
- If necessary, attach to a new region on PKI infrastructure (using the service “Set PKI Certificates”)

5.2 File Signer Tool (Other role: R&D Signer role)

The file Signer Tool can have the following role and associated service:

R&D Signer role: The service available to the R&D Signer role is:

- Verify Files: The file signer tool shall provide the service required to sign the files used by the franking machine. The PSD verifies the signature of the signed files.

5.3 Expertise Tool (Other role: Unauthenticated User role)

The expertise tool shall provide the services required to read postal data of the machine, in a unauthenticated way.

The Expertise Tool can have the following role and associated service:

Unauthenticated User role: The service available to the Unauthenticated User role is:

- Read Status Data
- Zeroize CSPs

5.3.1 Read status data

This service will carry out the following actions:

- The PSD sends its statistical data (these data are linked to the imprints or the errors)
- The PSD sends its registers
- The PSD sends its life cycle state

5.3.2 Zeroize CSPs

This service will carry out the following actions:

- Overwrites with 0s the memory location of plaintext CSPs
 - Master Secret Key,
 - Random Number Seed and
 - Random Number Key
 - All TLS keys if an active connection is available when the service is issued
- Irreversibly moves the PSD into “Faulted” state

5.4 Customer (User role: Printing Base role)

The base shall provide the services required to use the franking machine which hosts the PSD.

The Customer can have the following role and associated services:

Printing Base role: The services available to the Printing Base role are:

- Initiate/End Postal Core Connection
- Initiate/End Rekey Connection
- Postal Indicium
- Other Base Services
- Read Status Data

For each of the services, the Printing Base and the PSD authenticate each other (with the TLS secure protocol).

5.4.1 Initiate/End Postal Core Connection

This service will carry out the following actions:

- Initiate Postal Core Connection: the customer initiates a transaction (Resetting, Update Registration, Withdraw); the PSD will connect to the server via the base (see §5.1)
- End Postal Core Connection: the base gets a connection result on the previous transaction to inform the customer.

5.4.2 Initiate/End Rekey Connection

This service will carry out the following actions:

- Initiate Rekey Connection: when the PSD needs to update its certificate chains, the base initiates a rekey transaction; the PSD will connect to the server via the base (see §5.1)
- End Rekey Connection: the base gets a connection result on the previous rekey transaction to inform the customer.

5.4.3 Postal Indicum

This service will carry out the following actions:

- Send bitmap to print
- Send print authorization
- Send data to print

5.4.4 Other Base Services

This service will carry out the following actions:

- Time adjustment
- Download bitmaps
- Verify files signature
- Read date and time

5.4.5 Read Status Data

This service is the same as §5.3.1 Read status data but is accessible in an authenticated way.

6 Security Rules

6.1 Authentication Rules

- The PSD shall provide identity-based authentication.
- The authentication of the user entity (Customer and Neopost Administrator) by the PSD is based on the TLS Secure Protocol using the "TLS-DHE-RSA-WITH-AES-128-CBC-SHA" cryptographic suite, with variable RSA key length (1536 to 2048 bits).
- The authentication of the PSD by the user entities (Customer and Neopost Administrator) is based on TLS Secure Protocol using of the "TLS-DHE-RSA-WITH-AES-128-CBC-SHA" cryptographic suite, with variable RSA key length (1536 to 2560 bits).
- The random number implementation employed shall be according to ANSI X9.31 using AES algorithm (Reference [12]).
- For any attempt to use the authentication mechanism, the probability that a random attempt will be accepted or that a false acceptance will occur will be at least 1 in 296 (equivalent to at least 12 x 1028).

- The RSA key is 1536 bits and is considered to have 96 bits of strength. This is considerably more difficult to break than the 1 in 1,000,000 requirement.
- The maximum time to generate an authentication shall be 100ms.
- For multiple attempts to use the authentication mechanism then the probability that a random attempt will be accepted or that a false acceptance will occur will be 1 in 296 divided by 600 (equivalent to 1 x 1026). This is considerably more difficult to break than the 1 in 100,000 requirement.

6.2 CSP/Key Overview

There are three groups of keys and CSPs in the PSD.

Communication keys: These keys are used by the TLS protocol to authenticate the messages exchanged with the franking machine base or with the Neopost infrastructure (servers), and to establish a session secret keyset used for encrypting and authenticating the communication to and from the PSD as dictated by the TLS protocol.

RNG keys: These are keys used to initialize the approved pseudo-random number generator.

Postal keys: These are keys used by the PSD to provide and perform postal functionality.

6.3 TLS Configuration

The PSD is always the client in the TLS negotiation. The server in the TLS negotiation is either the base, the Neopost Region server or the Neopost Root server. The TLS protocol is configured to use the following parameters during the handshake negotiation:

Client: ClientHello message

- SessionID length = 0 (indicates that session-reuse is not allowed)
- ClientRandomValue (32 bytes) is generated by concatenation of the PSD time (4 bytes) and a random number generated by FIPS Approved PRNG.
- There is only one CipherSuite advertised to the server: **TLS-DHE-RSA-WITH-AES-128-CBC-SHA** to indicate that the server will use RSA to sign/verify Diffie-Hellman parameters used between the client and server to agree on a premaster secret that will be used in turn to form the 128 bits AES encryption key (TLS Communication Secret Keyset) followed by a HMAC-SHA-1 for each message.

Server: ServerHello message

- ServerRandomValue (32 bytes) is generated by concatenation of server time (4 bytes) and random number generated by FIPS Approved PRNG.
- The CipherSuite field is selected from the set of ciphers advertised by the client: **TLS-DHE-RSA-WITH-AES-128-CBC-SHA**

Server: Certificate message

- The server will present to the client a chain of signed X509 certificates that will be used for authentication and selection of roles.

6.4 PSD Key Generation

6.4.1 RSA Key Generation

RSA keys are used for authentication of the communication (communication keys of TLS protocol) with a length of 1536 bits.

- For the generation of the seed used to generate the two secret primes “p” and “q” the module follows the FIPS IG 7.8

- The PSD RSA public key corresponding to the private key shall be calculated according to the relationship for derivation of a RSA public key defined in reference [10]
- During private/public key pair generation data output from the PSD shall be inhibited

6.4.2 AES Key Generation

An AES key is used for encryption of the CSPs (master key) with a length of 128 bits.

- The PSD AES Master Secret Key shall be a random number according to ANSI X9.31 – Reference [11] using the AES algorithm (Reference [12]).

6.4.3 ECDSA Key Generation

ECDSA keys are used for indicia authentication using the p224 curve.

- This PSD ECDSA Private Stamp key shall be generated according the ECDSA algorithm reference [14]
- The PSD ECDSA public key corresponding to the private key shall be calculated according to the relationship for derivation of a ECDSA public key defined in reference [14]
- During private/public key pair generation data output from the PSD shall be inhibited

6.5 Conditional Self Test Rules

- If the RSA key pair is invalid then all CSPs shall be zeroized and the PSD shall pass in the Faulted state. The validity of a key pair shall be determined by a pairwise consistency check, i.e. the encryption of a plaintext value and decryption of the cipher text value. This check shall be performed at the generation of each new key pair and at power up.
- If the ECDSA key pair is invalid then all CSPs shall be zeroized and the PSD shall pass in the Faulted state. The validity of a key pair shall be determined by a pairwise consistency check, i.e. the encryption of a plaintext value and decryption of the cipher text value. This check shall be performed at the generation of each new key pair and at power up.
- Before generating the private/public keys and secret keys using the Approved random number generator, the PSD shall perform the continuous random number generator test, as defined in reference for conditional self-tests, for every number generated and shall pass in the Faulted state if it fails.
- During TLS Handshake the module generates DH parameters. A pairwise test is performed using these parameters before the module outputs the DH public key.

6.6 Power Up Self-Test Rules

- The PSD shall test the operation of RAM areas used for secure operations at power up. The PSD shall pass into the Faulted state if the test fails.
- The PSD shall test the firmware integrity by examining the contents of its program memory area at power up by calculating the hash (SHA-256) of the contents and comparing the result with a known answer. The PSD shall pass into the Faulted state if the test fails.
- The PSD shall test the accessibility and validity of all keys and CSP values in NVRAM at power up. If any are not accessible (i.e. device failure) or contain erroneous data (16 bits EDC fails) then the PSD shall pass into the Faulted state.
- The PSD shall test the RSA algorithm at power up by performing individual known answer tests for encryption, decryption, signature, and verification using predetermined data embedded into the PSD firmware.
- The PSD shall test the ECDSA P224 algorithm at power up by performing a known answer test for signature/verification using predetermined data embedded into the PSD firmware.

- The PSD shall test the DHE algorithm at power up by performing a known answer test for calculation of keys using predetermined data embedded into the PSD firmware. The PSD shall pass into the Faulted state if the test fails.
- The PSD shall test the SHA-1 algorithm at power up by performing a known answer test for hashing predetermined data embedded into the PSD firmware. The PSD shall pass into the Faulted state if the test fails.
- The PSD shall test the HMAC-SHA-1 algorithm at power up by performing a known answer test for predetermined data embedded into the PSD firmware. The PSD shall pass into the Faulted state if the test fails.
- The PSD shall test the SHA-256 algorithm at power up by performing a known answer test for hashing predetermined data embedded into the PSD firmware. The PSD shall pass in the Faulted state if the test fails.
- The PSD shall test the AES algorithm at power up by performing a known answer test for CMAC and both encryption of a plaintext value and decryption of the cipher text value using predetermined data embedded into the PSD firmware. The PSD shall pass into the faulted state if the test fails.
- The PSD shall test the PRNG algorithm at power up by performing a known answer test for activating algorithm using predetermined data embedded into the PSD firmware. The PSD shall pass into the Faulted state if the test fails.
- The PSD shall test the accessibility and validity of all public keys values (communication keys, stamp authentication key, certificates) in NVRAM at power up. If any are not accessible (i.e. device failure) or contain erroneous data then the PSD shall pass into the Faulted state.

6.7 CSP Storage

The definition and the storage of CSP are described in Section 7 - Definition of Critical Security Parameters (CSP).

All CSPs (except Master Secret Key, Random Number Seed and Random Number Key stored in the RTC RAM) are stored encrypted by the Master Secret Key.

- The PSD shall detect data corruption of the value held for any particular CSP by the incorporation of 16 bits error detection data.
- Plain text CSPs (Master Secret Key, Random Number Seed and Random Number Key) shall be zeroized
 - by issuing “Zeroize CSPs” service or
 - by breaching the special flex circuit envelope that surrounds the module or
 - by bringing the module temperature above 84°C.
 - Any CSP access failure shall cause the PSD to pass in faulted state.

6.8 Tamper Response

- In addition to the required FIPS 140-2 physical security protection mechanisms, the module incorporates a tamper detection and response mechanism in the form of a tamper detection envelope that protects the module from direct penetration attacks such as drilling or cutting the module.
- The RTC-RAM shall be erased to zero (the RTC-RAM contains all plaintext CSPs, Master Secret Key, Random Number Seed and Random Number Key) if the PSD physical cryptographic boundary is breached. At the same time the PSD shall pass in faulted state.
- The RTC-RAM shall be erased to zero (the RTC-RAM contains all plaintext CSPs: Master Secret Key, Random Number Seed, and Random Number Key) if the temperature inside the PSD covers exceeds 84 degrees Centigrade. At the same time the PSD shall pass in faulted state.

- The CSPs shall not be output from of the module in plain text under any circumstances.
- The module employs a high temperature fuse for the EFP circuitry such that when the module temperature exceeds 84°C, the module will zeroize all plaintext CSPs.

6.9 Operational Environment

- The cryptographic module's operational environment is non-modifiable.

6.10 Status Indication

- *The following 'module not ready' module states shall be indicated:*
 - CSPs zeroed
 - Private/Public key pairs invalid (module not initialised)
 - Tamper mechanism tampered
 - Power Up tests error
 - RNG error
 - High temperature detected error

Indication will be via a unique text message output by the module suitable for viewing on an alphanumeric display device. The absence of one of these messages indicates that the module is in a 'ready' state.

6.11 Operators/Customers

- Operators/customers shall be instructed to check for any errors, indicated by the status output, or for tamper evidence. Detection of any such errors or tamper evidence shall be required to be reported to Neopost such that the return of the PSD to the factory environment for withdrawal can be arranged.

7 Definition of Critical Security Parameters (CSP)

This section describes each CSP maintained by the PSD module.

CSP NAME	DESCRIPTION	STORAGE	ZEROIZATION	KEY LENGTH
Master Secret Key	Master key of the PSD; used with AES algorithm to encrypt CSPs before their storage and decrypt the stored CSPs before usage.	RTC-RAM	Zeroize CSPs service, breach of flex circuit or module temperature over 84°C.	128 bits
Random Number Seed	Current status of the seed value is used by the random number generator.	RTC-RAM	Zeroize CSPs service, breach of flex circuit or module temperature over 84°C.	128 bits
Random Number Key	Key value is used by the random number generator.	RTC-RAM	Zeroize CSPs service, breach of flex circuit or module temperature over 84°C.	128 bits
Communication Private Key	The PSD private RSA key is used to authenticate (sign) messages and data output from the PSD during TLS handshake protocol. The current value and the future value of the key is always available	Flash(stored encrypted by the AES Master Key)	Zeroization of the AES Master Key	1536 bits
Neopost Diffie-Hellman Exponent	Diffie-Hellman parameter used and generated during TLS handshake to agree upon a TLS premaster secret.	RAM only	At power off or end of TLS session.	1024 bits

<p>TLS Communication Secret Keyset</p>	<p>The 4 session keys generated by TLS Handshake protocol to ensure confidentiality and authenticity of messages exchanged between the client and the server or base.</p>	<p>RAM only</p>	<p>At power off or end of TLS session.</p>	<p>4 x 128 bits</p>
<p>Stamp Authentication Private Key</p>	<p>The PSD stamp private key (ECDSA P224) is used to authenticate the stamp. The current value and the future value of the key is always available</p>	<p>Flash (stored encrypted by the Master Secret Key)</p>	<p>Zeroization of the AES Master Key</p>	<p>224 bits</p>

8 Definition of Public Parameters

This section describes public parameters maintained by the PSD.

PUBLIC KEYS AND PARAMETERS	DESCRIPTION	STORAGE	KEY LENGTH
Root Public Key Neopost Root Certificate	Signed X509 Certificate of the current Root Public key used for the verification of authenticated messages input from the Neopost server.	EEPROM	2048 bits
Previous Root Public Key Neopost Previous Root Certificate	Signed X509 Certificate of the previous Root Public key used for the verification of authenticated messages input from the Neopost server.	EEPROM	2048 bits
Region Public Key Neopost Region Certificate	Signed X509 Certificate of the Region Public Key used for the verification of authenticated messages input from the Neopost server.	EEPROM	2048 bits
Communication Public Key Communication Certificate	The PSD public RSA key used to authenticate messages and data output from the PSD (TLS protocol) The current value and the future value of the key is always available	Flash (stored encrypted by the master key)	1536 bits
Device Public Key Neopost Device Certificate	Signed X509 Certificate of the Device Public key used for the verification of authenticated messages input from the Neopost server.	EEPROM	1536 bits
Neopost Diffie-Hellman Modulus	Diffie-Hellman parameter used during TLS handshake to agree upon a TLS premaster secret.	EEPROM	1024 bits
Neopost Diffie-Hellman Generator	Diffie-Hellman parameter used during TLS handshake to agree upon a TLS premaster secret.	EEPROM	8 bits
Stamp Authentication Public Key	The ECDSA – P224 public key is used to authenticate the stamp.	Flash	448 bits

9 Definition of CSP Modes of Access

The section describes how CSPs are accessed by the services that can be activated by an operator. The modes of access are defined as follows:

- u The data item will be read for internal use.
- e The data item will be read and exported.

- w The data item will be updated directly from an imported value.
- m The data item will be modified to a value created by an internal process.
- z The data item will be zeroized.
- s The data item will be initialised to a starting value created by an internal process.
- i The data item will be initialised to a benign value (typically zeroized).

Note:

The notation -/u means that in the first case, for an unauthenticated user, the parameter is not used and in the second case, for an authenticated user, the parameter will be read for internal use.

The notation m+e means that the key or CSP will be firstly modified to a value created by an internal process and then exported out of the module.

The notation m+z means that the parameter will be firstly modified to a value created by an internal process and then will be zeroized.

The first table summarises the relationship between generic CSPs maintained by the PSD and the services that access them.

The second table summarises the relationship between country specific CSPs maintained by the PSD and the services that access them.

GENERIC CSP ▾	MASTER SECRET KEY	RANDOM NUMBER SEED	RANDOM NUMBER KEY	COMMUNICATION PRIVATE KEY	DIFFIE-HELLMAN PRIVATE PARAMETER	TLS COMMUNICATION SECRET KEYSET	STAMP AUTHENTICATION PRIVATE KEY
SERVICE ▾							
Read Status Data	-/u	-/m	-/u	-/u	-/u	-/u	-
Initiate Postal Core Connection	u	m	u	u	u	m	-
End Postal Core Connection	u	m	u	u	u	m+z	-
Initiate Rekey Connection	u	m	u	u	u	u	-
End Rekey Connection	u	m	u	u	u	u	-
Postal Indicum	u	m	u	u	u	u	u
Other Base Services	u	m	u	u	u	u	-
Postal Core Services	u	m	u	u	u	u	-

Generate Stamp Key	u	m	u	u	u	u	m
Generate PKI Key	u	m	u	m	-	u	-
Get PKI Certificates	u	m	u	m	u	u	-
Set PKI Certificates	u	m	u	m	u	u	-
Zeroize CSPs / Tamper detection triggered / EFP High temp	z	z	z	-	-	-	-

10 Definition of Public Parameters Modes of Access

The section describes how CSPs are accessed by the services that can be activated by an operator. The modes of access are defined as follows: -

- u The key or CSP item will be read for internal use.
- e The key or CSP item will be read and exported.
- w The key or CSP item will be updated directly from an imported value.
- m The key or CSP item will be modified to a value created by an internal process.
- z The key or CSP item will be zeroed.
- s The key or CSP item will be initialised to a starting value created by an internal process.
- i The key or CSP item will be initialised to a benign value (typically zeroed).

Note:

The notation -/u means that in the first case, for an unauthenticated user, the parameter is not used and in the second case, for an authenticated user, the parameter will be read for internal use.

The notation m+e means that the key or CSP will be firstly modified to a value created by an internal process and then exported out of the module.

The following table summarises the service relationships for generic public key parameters maintained by the PSD.

Generic Public Parameter Name ▾	Root Public Key	Previous Root Public Key	Region Public Key	Communication Public Key	Device Public Key	Diffie-Hellman Parameters	Stamp Authentication Public Key
SERVICE ▾							
Zeroize CSPs	-	-	-	-	-	-	-

Read Status Data	-/u	-/u	-/u	u	-/u	-/u	-
Initiate/End Postal Core Connection	u	u	u	u	u	u	-
Initiate/End Rekey Connection	u	u	u	u	u	u	-
Postal Indicum	u	u	u	u	u	u	-
Other Base Services	u	u	u	u	u	u	-
Postal Core Services	u	-	u	u	u	u	-
Generate Stamp Key	u	-	u	u	u	u	m+e
Generate PKI Key	-	-	-	m	-	-	-
Get PKI Certificates	u	u	u	u	u	u	-
Set PKI Certificates	w	w	w	u	w	u	-

11 Appendix A: Relations transactions/states

The following table summarises the legality of transactions according to the prevailing life cycle state of a PSD:

PSD STATE ▸			
TRANSACTION ▾	INSTALLED	LOCKED	WITHDRAWN
Resetting	✓	✓	
Update Registration	✓	✓	
Withdrawal	✓	✓	✓
Rekey	✓	✓	✓

A transaction is not permitted for a particular state unless indicated:

✓ = permitted

12 Appendix B:Relation services/roles

ROLE ▾								
SERVICE ▾	PRINTING BASE	POSTAL USER	POSTAL CRYPTO OFFICER	FIELD CRYPTO OFFICER	R&D SIGNER	UNAUTHENTICATED USER	REGION	ROOT
Zeroize CSPs						✓		
Read Status Data	✓	✓		✓		✓		
Initiate/End Postal Core Connection	✓							
Initiate/End Rekey Connection	✓							
Postal Indicium	✓							
Other Base Services	✓							
Verify Files					✓			
Verify Device Certificates							✓	
Verify Region Certificates								✓
Verify Root Certificates								✓
Postal Core Services		✓						
Generate Stamp Key			✓					
Generate PKI Key				✓				
Get/Set PKI Certificates				✓				

Service is not accessible to a particular entity unless specifically indicated:

✓ = can be accessed