neopost

POSTAL SECURITY DEVICE

SECURITY POLICY

Version 3.0

Contents

Figures

1 INTRODUCTION

This document forms a Cryptographic Module Security Policy for Neopost Postal Security Device under the terms of the FIPS 140-2 validation. This document contains a statement of the security rules under which the PSD operates.

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 PSD Overview

The Neopost Postal Security Device (PSD) is a cryptographic module embedded within the postal franking machines. The PSD performs all franking machine's cryptographic and postal security functions and protect the Critical Security Parameters (CSPs) and Postal Relevant Data from unauthorized access.

The PSD (Figure 1) is a multi-chip embedded cryptographic module enclosed within a hard, opaque, plastic enclosure encapsulating the epoxy potted module which is wrapped in a tamper detection envelope with a tamper response mechanism. This enclosure constitutes the cryptographic module's physical boundary. The PSD was designed to securely operate when voltage supplied to the module is between +5V and +17V and the environmental temperature is between -30°C and 84°C.

Figure 1 – Neopost Postal Security Device

2.2 PSD Configuration

PSD (Cryptographic Module)			Description
Hardware P/N			A0014227B
Firmware P/N			A0038091A
Firmware Version			a30.00
NIST Approved Security Functions	**ECDSA**	(Cert. #517)	A0038110A
	AES	(Cert. #2875)	A0038111A
	SHS	(Cert. #2416)	A0038112A
	AES	(Cert. #2874)	A0038113A
	CVL	(Cert. #310)	A0038114A
	RSA	(Cert. #1513)	A0038115A
	DRBG	(Cert. #518)	A0038116A
	HMAC	(Cert. #1813)	A0038118A

Figure 2 — PSD Configuration

2.3 FIPS Security Level Compliance

The PSD is designed to meet the overall requirements applicable for Level 3 of FIPS 140-2.

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

Figure 3 – FIPS 140-2 Security Level

2.4 Security Industry Protocols

The cryptographic module implements the TLS v1.2[1] protocol and uses only one cipher suite (TLS-DHE-RSA-WITH-AES-128-CBC-SHA256). The TLS protocol is composed of TLS Handshake protocol (used for mutual authentication and TLS pre-master secret establishment) and TLS Record protocol (used for application data confidentiality and integrity).

[1] This protocol has not been reviewed or tested by the CAVP and CMVP

2.5 Modes of Operation

The module supports a single mode of operation in which the module alternates service by service between Approved and non-Approved modes of operation. When the module executes the services not relying on cryptographic functions or relying on Approved algorithms, it is said to operate in an Approved mode of operation. Corollary, when the services relying on non-Approved algorithms are executed, the module is said to operate in a non-Approved mode of operation.

The module includes a Stamp Configuration and a Variant file which indicates that the module is in either FIPS mode or non-FIPS mode of operation. This is accessed as part of the Read Part Number service.

The PSD supports the following FIPS Approved security functions in Approved Mode of Operation:

Algorithm	Usage	Characteristics	Cert. #
AES (CBC)	Encryption/Decryption of: • CSPs for storage within the module, • Data exchanged using the TLS Record protocol	CBC (e/d; 128);	2874
SHS (SHA-1)	Hashing algorithm used for: • HMAC Generation, • Indicia Authentication	SHA-1 (BYTE-only)	2416
SHS (SHA-256)	Hashing algorithm used for: • HMAC Generation, • Digital signature process	SHA-256 (BYTE-only)	2416
HMAC (SHA-1)	Indicia Authentication	(Key Sizes Ranges Tested: KS<BS)	1813
HMAC (SHA-256)	TLS messages authentication, Indicia Authentication	(Key Sizes Ranges Tested: KS<BS)	1813
AES CMAC	Indicia Authentication	CMAC (Generation) (KS: 128; Block Size(s): Full / Partial ; Msg Len(s) Min: 0 Max: 2^16 ; Tag Len(s) Min: 1 Max: 16)	2875
RSA (PKCS #1 v1.5)	Signature generation/ Signature verification of X509 certificates used by TLS Handshake protocol, Signature verification of signed files imported into the module	FIPS186-2: ALG[RSASSA-PKCS1_V1_5]: SIG(ver): 1536 FIPS186-4: 186-4KEY(gen): FIPS186-4_Fixed_e ALG[RSASSA-PKCS1_V1_5] SIG(gen) (2048 SHA(256)) SIG(Ver) (2048 SHA(256))	1513
ECDSA (P224)	Indicia Authentication	PKG: CURVE P-224 ExtraRandomBits SigGen : CURVE P-224 : (SHA-256) SigVer : CURVE P-224 : (SHA-256)	517
CVL (TLS-KDF SP800-135)	TLS KDF function	TLS (TLS1.2 (SHA256))	310
CTR DRBG using AES (SP800-90A)	Key generation	[AES-128 Key]	518

Figure 4 — FIPS Approved Algorithms

The PSD supports the following FIPS Allowed security functions in Approved Mode of Operation:

Algorithms	Usage	Characteristics
Diffie-Hellman	As used in TLS key exchange for key agreement of pre-master secret during Handshake protocol	Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
RSA PKCS #1 v1.5	Key Wrapping RSA 2048-bit key (Key Wrapping)	RSA (Cert. #1513, key wrapping; key establishment methodology provides 112 bits of encryption strength)
HW RNG	For seeding Approved SP800-90A DRBG	Internal entropy source

Figure 5 — FIPS Allowed Security Functions

Some Postal Authorities/Standards may require implementation of non-FIPS Approved security functions. For these specific firmware configurations the PSD supports the following non-FIPS Approved security functions:

Algorithms	Usage	Caveat
SHS (SHA-1)	Hashing algorithm used for digital signature generation process: ECDSA P192 SigGen (Postal Indicia Service – Canada Only)	SHA-1 (BYTE-only)
ECDSA (P192)	Indicia Authentication (Postal Indicia Service – Canada Only)	PKG: CURVE P-192 ExtraRandomBits SigGen: CURVE P-192: (SHA-1)
RSA PKCS #1 v1.5	Key Wrapping RSA 1024/1536-bit key (Key Wrapping) (Postal Core Services – Germany and Belgium Only)	RSA (key wrapping; key establishment methodology provides 112 bits of encryption strength, non-compliant less than 112 bits of encryption strength)

Figure 6 – Non-Approved Security Functions

3 SENSITIVE SECURITY PARAMETERS MANAGEMENT

3.1 Critical Security Parameters

Name	Algorithm/Size	Description	Generation	Storage	Distribution	Zeroization
Master Secret Key	AES CBC 128 bits	Internally encrypt & decrypt PSD's critical security parameters	Internal DRBG	In plaintext in tamper protected memory	N/A	- Invocation of "Zeroize CSPs" service; - Breach of flex circuit triggers "Zeroize CSPs" service; - PSD temperature over 84°C triggers "Zeroize CSPs" service (EFP measure); - Failure of a self-test triggers "Zeroize CSPs" service;
DRBG - Key	CTR DRBG using AES 128	Internal state of DRBG.	Internal HW RNG	In plaintext in tamper protected memory	N/A	
DRBG -V	CTR DRBG using AES 128	Internal state of DRBG.	Internal HW RNG	In plaintext in tamper protected memory	N/A	
TLS Communication Private Key	RSA PKCS #1 v1.5 2048 bits	Authenticates messages and data output from the PSD during TLS Handshake protocol.	FIPS186-4 KEYGEN	encrypted	N/A	Rendered unusable by zeroization of "Master Secret"
Indicia Authentication Secret Key	HMAC-SHA-1 (160 bits key) or HMAC-SHA-256 (256 bits key) or CMAC AES 128	Indicia authentication	Internal DRBG	encrypted	RSA Wrapping	Rendered unusable by zeroization of "Master Secret"
Indicia Authentication Private Key	ECDSA P224 or ECDSA P192[2]	Indicia authentication	Internal DRBG	encrypted	N/A	Rendered unusable by zeroization of "Master Secret"
m-secret	N/A	DPAG secret information	External	encrypted	RSA Wrapping	Rendered unusable by zeroization of "Master Secret"
m-secret Encapsulation Key	RSA PKCS #1 v1.5 1024 bits[3]	Encapsulation of m-secret from DPAG to PSD	Internal DRBG	encrypted	N/A	Rendered unusable by zeroization of "Master Secret"

Figure 7 – Critical Security Parameters

[2] This key offers less than 112-bit of security strength and is not used in the approved mode of operation

[3] This key offers less than 112-bit of security strength and is not used in the approved mode of operation

Name	Algorithm/Size	Description	Generation	Storage	Distribution	Zeroization
DH private key (TLS Handshake)	Diffie-Hellman 224 bits	Diffie-Hellman private key used to agree TLS pre-master	Internal DRBG	N/A	N/A	Immediately after use (i.e. TLS-pre-master key establishment)
TLS pre-master key	256 bytes	Pre-master secret	DH Key Agreement	N/A	N/A	Immediately after use
TLS master key	48 bytes	Used to derive the keys used by TLS Record Protocol (TLS Communication Secret Keyset)	Approved TLS KDF	N/A	N/A	TLS session closure

Figure 8 – TLS v1.2 Handshake Protocol Critical Security Parameters

Name	Algorithm/Size	Description	Generation	Storage	Distribution	Zeroization
TLS Communication Secret Keyset (TLS Record Protocol Keys)	AES CBC: 2 x 128 bits; HMAC-SHA-256: 2 x 256 bits	Encrypt & Decrypt & Integrity TLS Communication	Approved TLS KDF	Plaintext	N/A	TLS session closure

Figure 9 – TLS v1.2 Record Protocol Critical Security Parameters

The CSPs are protected from unauthorized disclosure, modification and substitution.

The plaintext CSPs are stored in the tamper protected memory. All other CSPs are stored encrypted by the Master Secret Key.

The PSD detects data corruption of the value held for any particular CSP by the incorporation of 16 bit error detection code. Any CSPs access failure causes the zeroisation of tamper protected memory.

The PSD never output the CSPs in plaintext.

3.2 Public Security Parameters

Name	Algorithm/Size	Description	Generation	Storage
Root Public Key (Neopost Root Certificate)	RSA PKCS #1 v1.5 2048 bits	Signed X509 Certificate of the current Root Public key used for the verification of authenticated messages input from the Neopost server	N/A	plaintext
Previous Root Public Key (Neopost Previous Root Certificate)	RSA PKCS #1 v1.5 2048 bits	Signed X509 Certificate of the next Root Public key used for the verification of authenticated messages input from the Neopost server.	N/A	plaintext
Region Public Key (Neopost Region Certificate)	RSA PKCS #1 v1.5 2048 bits	Signed X509 Certificate of the current Region Public key used for the verification of authenticated messages input from the Neopost server.	N/A	plaintext
TLS Communication Public Key (Neopost PSD Certificate)	RSA PKCS #1 v1.5 2048 bits	Used to authenticate messages and data output from the PSD (TLS Handshake protocol). The key resides in a signed X509 certificate used for authentication the cryptographic module to the Neopost server.	FIPS186-4 RSA KEYGEN	plaintext
TLS Diffie-Hellman Public Parameters	Diffie-Hellman 2048 bits	Diffie-Hellman parameters (p, g, Y) used during TLS handshake to agree upon a TLS premaster secret.	N/A	plaintext
Indicia Authentication Public Key	ECDSA P224 or ECDSA P192[4]	Indicia authentication	Internal DRBG	plaintext
Key Encapsulation Public Key	RSA PKCS #1 v1.5 2048 bits	Encrypts the PSD Indicia Secret Keys before sending to the Neopost server	N/A	plaintext
m-secret Encapsulation Public Key [5]	RSA PKCS #1 v1.5 1024 bits	Encrypts the “m-secret” before sending it to the PSD	N/A	plaintext

Figure 10 – Public Security Parameters

All public keys are protected from unauthorized modification and substitution.

3.3 Status Indicator

A status indicator will be output by the PSD via the status output interface. It consists of a unique text message which will be displayed on the franking machine User Interface.

The following module states are indicated:

- CSPs zeroed
- Private/Public key pairs invalid (module not initialized)
- Tamper mechanism tampered
- Power Up tests error
- DRBG error
- High temperature detected error
- Conditional test error
    - DH Pairwise Consistency
    - ECDSA Pairwise Consistency
    - RSA Pairwise Consistency

The absence of one of these messages indicates that the module is in a ‘ready’ state.

[4] This key offers less than 112-bit of security strength and is not used in the approved mode of operation

[5] This key offers less than 112-bit of security strength and is not used in the approved mode of operation

4 PORTS AND INTERFACES

To communicate with the franking machine's base the module provides a physical 10-pin serial connector with five logical interfaces:

- power interface
- data input interface
- data output interface
- control input interface
- status output interface

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

Figure 11 – Interface

The data output interface is inhibited during zeroization, key generation, self-tests and error states.

No plaintext CSPs are input or output from the module through this serial interface.

5 ROLES, SERVICES AND AUTHENTICATION

The PSD supports authorized roles for operators and corresponding services within each role. In order to control access to the module the PSD employs identity-based authentication mechanism.
The PSD supports the following operators:

- **Neopost Administrator** (Field Server): The Crypto-Officer can assume the following Crypto-Officer roles:
  - Postal User
  - Field Crypto-Officer
  - Postal Crypto-Officer
  - Root
  - Region

  The Neopost Administrator authenticates to the module via digitally signed X509 certificates using the TLS v1.2 Handshake protocol.
- **Customer** (Base): is the end user of the cryptographic module and can assume one User Role: the Printing Base role. The Neopost Administrator authenticates to the module via digitally signed X509 certificates using the TLS v1.2 Handshake protocol.
- **R&D File Signer Tool**: assumes the R&D Signer role and is authenticated via signed X509 certificates. This role allows the PSD to authenticate and use additional external files.
- **Expertise Tool:** assumes an unauthenticated User Role.

OPERATOR	ROLES	SERVICES	CSP ACCESS MODE
Neopost Administrator	Postal User	Postal Core Services[6]	(Read) m-secret Encapsulation Key (Germany only) NA (All other configurations)
		Read Status Data	NA
		Read Part Number	NA
	Field Crypto-Officer	Generate PKI Key	(Write/Read) Master Secret Key, DRBG parameters, TLS Communication private key & secret key
		Get/Set PKI Certificate	(Write) TLS Communication private key
		Read Status Data	NA
		Read Part Number	NA
	Postal Crypto-Officer	Generate Stamp Key[7]	(Write) Indicia Authentication Key(s)
		Set Stamp Info	NA
	Root	Verify Region Certificate	NA
		Verify Root Certificate	NA
	Region	Verify Device Certificate	NA
Customer	Printing Base (User)	Initiate/End Postal Core Connection	(Write) TLS Communication private key (Write) TLS Communication secret keys
		Initiate/End Rekey Connection	(Write) TLS Communication private key (Write) TLS Communication secret keys
		Postal Indicia[8]	(Read) Indicia Authentication Key
		Other Base Services	NA

[6] Non-Approved when configured for Germany.

[7] This service is considered non-Approved if Indicia Authentication Key is of type ECDSA P192 this service is not available when configured for Germany.

[8] This service is considered non-Approved if Indicia Authentication Key is of type ECDSA P192.

		Read Status Data	NA
		Read Part Number	NA
File Signer Tool	R&D Signer	Verify Files	NA
Expertise Tool	Unauthenticated User role	Read Status Data	NA
		Read Part Number	NA
		Zeroise CSP	(Zeroize) Master Secret Key and DRBG internal status (V, Key)
All	All	Invoke Tests	NA

Figure 12 – Roles, Services, Operators

5.1 Operator Authentication

The mutual authentication between the Customer / Neopost Administrator and the PSD is based on the TLS v1.2 Handshake Protocol using the "TLS-DHE-RSA" cryptographic suite, with 2048 RSA key length for authentication.

- The RSA key is 2048 bits is considered to have 112-bits of strength. For any attempt to use the authentication mechanism, the probability that a random attempt will succeed or a false acceptance will occur will be at least 1 in 2^{112} (equivalent to at least 1 x 10^{33}). This is considerably more difficult to break than the 1 in 1,000,000 requirement.
- The time necessary to generate an authentication is 100ms; therefore 600 attempts could occur in a one minute period. For multiple attempts to use the authentication mechanism during the a one minute period the probability that a random attempt will be accepted or that a false acceptance will occur will be 1 in 2^{112} divided by 600 - maximum number of attempts in one minute (equivalent to 1 x 10^{31}). This is considerably more difficult to break than the 1 in 100,000 requirement.

6 OPERATIONAL ENVIRONMENT

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

7 PHYSICAL SECURITY

The Neopost PSD is designed to meet FIPS 140-2 Level 3 + EFP/EFT Physical Security requirements.

The PSD defined as a multi-chip embedded cryptographic module includes a non-removable enclosure that comprises a hard epoxy resin with an outer plastic casing. The non-removable enclosure and epoxy resin was tested and verified to be effective within the environmental operational range of the module (environmental temperature between -30°C and 84°C). No assurance is provided for Level 3 hardness conformance at any temperature outside this range.

The PSD employs a tamper detection envelope designed to detect penetration attempts, and a response mechanism that will zeroize all plaintext Critical Security Parameters.

The outer plastic casing is defined as the cryptographic boundary of the cryptographic module.

The module mitigates environmental attacks by employing a high temperature fuse for the EFP circuitry such that when the module temperature exceeds 84°C, the module will zeroize all plaintext CSPs.

8 SELF-TESTS

The PSD performs power up and conditional self-tests. The PSD inhibits the data output interface during the self tests. If a self-test fail, the PSD enters an error state and zeroize all plaintext CSPs. The module can exercise the power-up self-tests, from within any role, at any time by power-cycling the module.

8.1 Power Up Self-Tests

8.1.1 Cryptographic Algorithm Tests

Upon power up the PSD performs the following cryptographic algorithms self-tests without operator intervention:

- SHA-1 KAT
- SHA-256 KAT
- RSA encrypt KAT
- RSA decrypt KAT
- RSA sign KAT
- RSA signature verify KAT
- ECDSA sign KAT
- ECDSA signature verification KAT
- AES Encrypt KAT
- AES Decrypt KAT
- AES CMAC KAT
- HMAC (SHA-1) KAT
- HMAC (SHA-256) KAT
- Diffie-Hellman KAT
- DRBG KAT
- TLS-KDF KAT

8.1.2 Firmware Integrity Tests

The PSD tests 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.

8.1.3 CSP Integrity Tests (Critical Function Test)

The PSD tests the accessibility and validity of all keys and CSP values in non volatile memory at power up. If any are not accessible (i.e. device failure) or contain erroneous data (16 bit EDC fails) then the PSD enters an error state and zeroize all plaintext CSPs.

8.2 Conditional Self-Tests

The PSD performs the following conditional self tests:

- RSA Pair wise Consistency Tests
- ECDSA Pair wise Consistency Tests
- DH Pair wise Consistency Tests
- HW RNG Continuous Test
- DRBG Continuous test

8.3 Other-Tests

The PSD also performs the following tests:

- RAM Integrity test
- Tamper Detection test

9 DESIGN ASSURANCE

Neopost Technologies is using the Windchill configuration management system to manage product configurations (including the cryptographic module).

All firmware implemented within the cryptographic module has been implemented using a high-level language (C), except for the limited use of assembly language where it was essential for performance.

10 MITIGATION OF OTHER ATTACKS

The module employs a tamper detection envelope designed to detect penetration attempts and a response mechanism that zeroize all plaintext CSPs.

11 GLOSSARY

Abbreviation	Description
AES	Advanced Encryption Standard
CMAC	Message Authentication Code
CSP	Critical Security Parameter
DH	Diffie-Hellman key exchange (DHE Diffie Hellman Ephemeral)
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptical Curve Digital Signature Algorithm
EFP/EFT	Environmental Failure Protection /Testing
EMI/EMC	Electromagnetic Interference/Compatibility
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
NIST	National Institute of Standards and Technology
NRBG	Non-deterministic Random Bit Generator
PSD	Postal Security Device
PKI	Public Key Infrastructure
RNG	Random Number Generator
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
TDEA	Triple Data Encryption Algorithm
TDES	Triple Data Encryption Standard

Revision History

Version	Date	Revision Description
0.1	11/04/2014	Original document
1.0	22/08/2014	Update after review with Penumbra Security
2.0	28/08/2014	[Penumbra]Added additional tests performed (Ram integrity, Tamper test)
3.0	16/03/2015	[Penumbra]Added clarifications per CMVP comments