Neopost, Inc.
30955 Huntwood Avenue
Hayward, CA 94544

FIPS 140-2

Cryptographic Security Policy

for the

Neopost, Inc.

Production Postal Security Device

Neopostage PSD Module

Date: November 20, 2003
Version: V1.R2
File: NPPSDModuleSecurityPolicy.pdf

Table of Contents

Revisions

Version	Primary Author(s)	Description of Version	Date Completed
V1.R0	David Grimes Michael Thompson Green Springs Technologies, LLC www.greenspringstech.com	First Public Version	October 30, 2003
V1.R1	Ken Daniels Mailroom Technology Inc.	Accepted Red Line Changes from Infoguard	November 20, 2003
V1.R2	Sidhartha Sridharan Mailroom Technology Inc.	Accepted all changes.	November 20, 2003

Referenced Documents

Title	Description
1. FIPS 186-2	DSS Digital Signature Standard
2. FIPS PUB 140-2	Security Requirements For Cryptographic Modules
3. FIPS 46-3	Data Encryption Standard
4. FIPS 180-1	Secure Hash Standard
5. IBM 4758 Model 002 with CP/Q++ Non-Proprietary Security Policy	IBM 4758 Model 002 with CP/Q++ Non-Proprietary Security Policy

1. Introduction

This document describes the security policy for the Neopostage PSD Module (HW P/N 04K9131 Version IBM 4758 Model 2 40H9952, FW Version CP/Q++ 2.41, SW Version 1.0.0.0) in order to achieve the requirements set forth in Federal Information Processing Standard 140-2 (FIPS 140-2). The security policy specifies the relationship between the roles and services provided by the module and different types of security relevant data items (keys, key components). Only applicable requirements of FIPS 140-2 as they relate to the PSD Module's capabilities and protections will be discussed.

The Neopostage Postal Security Device (PSD) Module functions as a software-based PSD that utilizes IBM 4758 Model 002 with CP/Q++ (Cert. #345) hardware-based cryptographic modules for securely managing accounting functions and indicia via encryption and digital signature techniques. The digitally signed PSD firmware is loaded onto the IBM 4758 Model 002 with CP/Q++ hardware via an Approved technique described in the IBM 4758 Model 002 with CPQ++ security policy. The PSD firmware resident on the IBM 4758-002 with CPQ ++ constitutes a single cryptographic module (Neopostage Postal Security Device (PSD)). The PSD has a multi-chip embedded embodiment. The module is ideally suited to Internet and proof of postage based applications requiring high-speed cryptographic functions. The module is designed to meet the applicable United States Postal Service Information-Based Indicium Program (USPS IBIP) specifications for postage meters.

The IBM 4758 Model 002 with CPQ++ has a set of non-Approved functionality that is not used or accessible when the PSD firmware is present. As such the PSD module does not support a non-FIPS mode of operation, and always runs in FIPS mode.

2. Security Level

The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 2.1 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Cryptographic Module Ports and Interfaces	3
Roles, Services, and Authentication	3
Finite State Model	3
Physical Security	4
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

3. Roles, Services, & Authentication

The PSD Module enforces access control using identity-based authentication, via verification of DSA signatures (see Ref. 1) using the Certificate Server Public Key.

The PSD Module supports the Crypto Officer/User role; the means of authentication and access to services is the same.

The associated false acceptance or random access rate is less than one in 1,000,000. DSA signatures have at least 80 bits of strength. The odds of randomly guessing the correct key used to generate a DSA signature is 1 in 2^80 which is less than 1/1,000,000. Since the PSD Module uses 1024 bit DSA signatures, it is well below the false acceptance limit.

During a one-minute period, the probability is less than one in 100,000 that a random attempt will succeed or a false acceptance will occur. The PSD supports a maximum of 10 authentication attempts per minute. For multiple attempts to use the Authenticate service during a one-minute period, the probability is 1 in 2^80/10 which is less than one in 100,000.

Note: The IBM 4758 Model 002 with CP/Q++ provides other roles and services; see IBM 4758 Model 002 with CP/Q++ non-proprietary security policy for details. Briefly, the IBM 4758 Model 002 with CP/Q++ "External User role" has been redefined to the Crypto Officer/User role described above. The IBM 4758 Model 002 with CP/Q++ supports four Crypto-Officer roles (0-3). The IBM 4758 Model 002 with CP/Q++ "Internal User role" no longer exists when PSD firmware is present.

The following services are described below:

- Disable: This service disables the PSD Module, thus preventing its use. The next time the module is restarted, it will go to the error state. Only way to clear the condition is to clear Battery Backed RAM (BBRAM). This service will zero out all PSD keys and PSD data. The IBM 4758 Model 002 with CP/Q++ also provides a zeroization service which zeroizes all CSPs; see IBM 4758 Model 002 with CP/Q++ non-proprietary security policy for details.

- Status: This unauthenticated service returns the PSD Module's current status including state, status, error condition (if applicable), PSD Serial Number, board time and User ID.

- Open Connection: This unauthenticated service opens a connection between the caller and the firmware. This service provides a unique identifier, Session ID, which must be provided by the caller, as required. The Crypto Officer/User must then properly authenticate to the module via the Authenticate service before any services that require authentication are provided.

- Imprint: This unauthenticated service validates the postal related data items.

- Create DSA Keys: This service creates and temporarily stores the Indicia Signing Key Pair necessary to key the PSD Module prior to operation.

- Store DSA Keys: This service permanently stores the PSD Certificate; Indicia Signature Private Key and Random Number Key (generated at same time that call is made).

- Authenticate: This service is used to identify the PSD Operator and authenticate its use of the postal-related services.

- Create PSD: This service handles the creation of PSDs.

- Delete PSD: This service handles the deletion of PSDs.

- Start: This service notifies the module to enter the Running state in order to process postal-related services.

- Stop: This service notifies the module to exit the Running state in order to stop processing postal-related services.

- Purchase: This service results in the creation of indicia with two options:

  A) Low-speed: signed with DSA (Cert #68) during the call.

- B) High-speed: for optimization purposes the indicia is NOT signed with DSA during this service; instead a random number (K value) encrypted with the Random Number Key along with SHA-1 hash is returned; this value will be used as the K value during the "Sign Data service" (a separate service described below).

- Sign Data: This service results in the signing of indicia where an encrypted random number (K value) was generated during the high-speed option of the Purchase service (a separate service described above). First the SHA-1 hash of the encrypted K value is checked and the random number is decrypted. Finally, DSA signing (Cert #84) takes place using the K value that was just decrypted.

- Verify Data: This service verifies indicia signatures generated by the PSD Module.

- Fund: Allows the Crypto Officer/User to fund the PSD and recalculate the ascending, descending and control registers.

- Close Connection: This unauthenticated service closes the connection to the PSD Module.

- Self-Test: The module performs a DSA known answer test upon power recycle; the IBM 4758 Model 002 with CP/Q++ performs the remaining required self-tests; see IBM 4758 Model 002 with CP/Q++ non-proprietary security policy for details.

Note: Status, Open, Close, Imprint, and Self-Test services do not require authentication.

4. Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 3 module.

1. The cryptographic boundary shall consist of the hardware secure module (IBM 4758 Model 002 with CP/Q++) including all software located inside the hardware.
2. Access control shall be identity based.
3. The module will only allow a single PSD Module Crypto Officer/User at any given time; the module does not support concurrent operators.
4. The module will use the following FIPS 140-2 approved cryptographic algorithms: Triple-DES (Cert #124), SHA-1 (Cert. #107) and DSA (Certs. #68 for digital signature generation/verification, #84 for digital signature generation).
5. Before the Crypto Officer/User has authenticated to the module, all access to cryptographic services relating to funding, PSD administration, generating signatures and performing signature verifications are disabled and denied.
6. The module shall enter the error state following up to (10) consecutive unsuccessful authentication attempts.
7. The module shall provide a "Status" service, which includes the status, PSD Serial Number, User ID, state, and last error.
8. The module shall meet level 4 physical security, and provide tamper detection and response mechanisms. Note: The physical security for this module is provided by the IBM 4758 Model 002 with CP/Q++ (validated to FIPS 140-1 requirements).
9. The module shall maintain logical separation of the data input, control input, data output, and status output interfaces.
10. The data output interface shall be inhibited during error states, key generation, and zeroization.
11. Cryptographic operations are not provided when the module is in an error state.
12. Unauthorized modification, substitution, or disclosure of CSPs shall not be allowed.
13. Unauthorized modification or substitution of public keys shall not be allowed.
14. The PSD module shall rely on the Approved key generation techniques implemented in the IBM 4758 Model 002 with CP/Q++ for generation of all keys; see IBM 4758 Model 002 with CP/Q++ non-proprietary security policy for details.
15. The loading of any non-validated code invalidates the FIPS 140-2 validations.

5. Definition of Critical Security Parameters (CSPs)

The following are the CSPs contained in the PSD Module:

- Indicia Signature Private Key (IS_X): This is a private DSA key used to sign the indicia. It is stored in Battery Backed RAM (BBRAM).

- Random Number Key (RNK): This is a triple-DES key used to encrypt the random numbers used in the indicia DSA signature process. It is stored in Battery Backed RAM (BBRAM).

- K value: This is a secret value used during the DSA signature generation process. It is stored in DRAM.

Note: The IBM 4758 Model 002 with CP/Q++ manages additional keys; see IBM 4758 Model 002 with CP/Q++ non-proprietary security policy for details

6. Definition of Public Keys and X.509 Certificates

The following are Public Keys and corresponding X.509 Certificates contained in the PSD Module:

- Indicia Signature Public Key (IS_Y): This is a public DSA key used to verify indicia signatures. This key is contained within the X.509 PSD Certificate. It is stored in Battery Backed RAM (BBRAM).

- Certificate Server Public Key (CS_Y): This is a public DSA key used to verify the CA Root Certificate, Authentication Certificate and PSD Certificate. This key is contained within the X.509 CA Root Certificate. It is stored in Battery Backed RAM (BBRAM).

- Authentication Certificate Public Key (AC_Y): This is a public DSA key used during the Authenticate service. This key is contained within the X.509 Authentication Certificate. It is stored in DRAM.

Note: The IBM 4758 Model 002 with CP/Q++ manages additional keys; see IBM 4758 Model 002 with CP/Q++ non-proprietary security policy for details

7. Definition of CSP Modes of Access

Table 7.1 defines the relationship between access to CSPs and the different PSD Module services. The modes of access shown in the table are defined as follows:

C_1 If not available in storage, a one-time creation will be allowed
C_2 If not available in storage a one-time storage will be allowed.
C The item will be created and immediately encrypted with RNK.
D The item will be deleted from storage and memory
S_H The item will be used to sign a given piece of data in high speed mode
S_L The item will be used to sign a given piece of data in low speed mode
S_K The item will be used during signing of a given piece of data in high speed mode
X The item will be used to decrypt a given K value
X_1 The item will be used to encrypt a given K value
K The item will be decrypted with RNK.

Table 7.1 PSD Module Services Versus CSP Access

Crypto Officer/User Role	**PSD Module Services**																	
CSP Access	Disable	Status	Self-Test	Open Connection	Imprint	Authenticate	Create DSA Keys	Store DSA Keys	Create PSD	Delete PSD	Start	Stop	Purchase(high-speed)	Purchse(low-speed)	Sign Data	Fund	Verify Data	Close Connection
$\underline{IS_x}$	D	-	-	-	-	-	C_1	C_2	-	-	-	-	-	S_L	S_H	-	-	-
RNK	D	-	-	-	-	-	-	C_1, C_2	-	-	-	-	X_1	-	X	-	-	-
K Value	D	-	-	-	-	-	-	-	-	-	-	-	C	-	K, $S_{K,}$	-	-	-

8. Mitigation Of Other Attacks

The PSD Module has not been designed to mitigate specific attacks that are outside of the scope of FIPS 140-2.