POSTAL SECURITY DEVICE

NON-PROPRIETARY SECURITY POLICY

Version 12.0

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			**A0014227-B and A0014227-C**			
Firmware Version			**a22.17.01, a22.17.02**	**a23.08.01, a23.08.03**	**a28.02.01, a28.02.04**	**a28.05, a28.08**
NIST Approved Security Functions	**AES** (Cert. #2565)	Version A0018322A	YES	YES	YES	YES
	CMAC (Cert. #2566)	Version A0018326A	YES	YES	YES	YES
	ECDSA[1] (Cert. #441)	Version A0018325A	YES	YES	YES	YES
	HMAC (Cert. #1583)	Version A0018327A	NO	NO	NO	YES
	HMAC (Cert. # 1603)	Version A0019557	YES	YES	YES	NO
	CVL (Cert. #92)	Version A0018320A	YES	YES	YES	YES
	RNG (Cert. #1217)	Version A0018328A	YES	YES	YES	YES
	RSA[2] (Cert. #1314)	Version A0018321A	YES	YES	YES	YES
	SHS[3] (Cert. #2162)	Version A0018324A	YES	YES	YES	YES

Figure 2 – PSD Configuration

Country (Postal Authority)/Specification	Firmware Version
USPS/ IBI_Lite	**a23.08.01, a23.08.03**
USPS/ IMI_2013	**a28.02.01, a28.02.04**
UK Royal Mail	**a22.17.01, a22.17.02**
UK Royal Mail/EIB	**a28.05**
TNT	**a23.08.03**
CPC	**a22.17.02, a23.08.03**
DPAG	**a22.17.02, a23.08.03 a28.08**

Figure 3 – PSD Firmware Version

[1] non-compliant for ECDSA SigGen P192

[2] non-compliant for RSA key lengths less than 2048-bit (less than 112 bits of encryption strength)

[3] SHA-1 is non-compliant when used for hashing (e.g. used with RSA or ECDSA SigGen function)

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 4 – FIPS 140-2 Security Level

2.4 Security Industry Protocols

The cryptographic module implements the TLS v1.0[4] protocol and uses only one cipher suite (TLS-DHE-RSA-WITH-AES-128-CBC-SHA). The TLS v1.0 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).

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

2.5 Modes of Operation

Approved Mode of Operation

The PSD cryptographic module has only one mode of operation that uses both FIPS and non-FIPS approved algorithms. The details and use of FIPS Approved algorithms are presented below:

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);	**2565**
SHS (SHA-1)	Hashing algorithm used for: • Digital signature process: ○ RSA SigVer, • HMAC Generation	SHA-1 (BYTE-only)	**2162**
SHS (SHA-256)	Hashing algorithm used for: • Digital signature process: ○ ECDSA P224 • HMAC Generation	SHA-256 (BYTE-only)	**2162**
HMAC (SHA-1)	TLS messages authentication	(Key Sizes Ranges Tested: KS<BS KS=BS)	**1583 and 1603**
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	ALG [RSASSA-PKCS1_V1_5]: SIG(gen): 2048 SIG(ver): 1024 ,1536, 2048	**1314**
CVL (TLS-KDF SP800-135)	TLS KDF function	TLS (TLS1.0/1.1)	**92**
RNG (ANSI X9.31)	Key generation; with 16 bytes seed/seed key (externally generated by FIPS validated module and imported into the PSD in secure factory environment) ; based on AES 128 as transition function	[AES-128 Key]	**1217**
Algorithm/key size(s) required per Postal Authority/Postal Standard: Unites States Postal Service IMI_2013			
ECDSA (P224; SHA-256)	Indicia Authentication	PKG: CURVE P-224 ExtraRandomBits SigGen: CURVE P-224: (SHA-256) SigVer: CURVE P-224: (SHA-256)	**441**
Algorithm/key size(s) required per Postal Authority/Postal Standard: Unites States Postal Service IBI_Lite			
CMAC (AES)	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)	**2566**
Algorithm/key size(s) required per Postal Authority/Postal Standard: United Kingdom Royal Mail EIB			
HMAC (SHA-256)	Indicia Authentication	HMAC-SHA256	**1583**

Algorithm	Usage	Characteristics	Cert. #
		(Key Size Ranges Tested: KS<BS)	
Algorithm required per Postal Authority/Postal Standard: Canada Post CPC			
ECDSA (P192; SHA-1)	Indicia Authentication	SigVer: CURVE P-192: (SHA-1)	**441**
HMAC (SHA-1)	Indicia Authentication	HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS)	**1603**
Algorithm required per Postal Authority/Postal Standard: TNT Post			
HMAC (SHA-1)	Indicia Authentication	HMAC-SHA1 (Key Sizes Ranges Tested: KS<BS KS=BS)	**1603**

Figure 5 – FIPS Approved Algorithms Details and Use

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

Algorithms	Usage	Caveat
Algorithm/key size(s) required per Postal Authority/Postal Standard: United Kingdom Royal Mail EIB		
RSA PKCS #1 v1.5	Key Transport RSA 2048-bit key (Key Encapsulation)	RSA (Cert. #1314, key wrapping; key establishment methodology provides 112 bits of encryption strength)

Figure 6 – FIPS Allowed Security Functions

The PSD supports the following Non-Approved security functions:

Algorithms	Usage	Caveat
Diffie-Hellman	As used in TLS v1.0 key exchange for key agreement of TLS pre-master secret during TLS Handshake protocol	Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength; non-compliant)
SHS (SHA-1)	Hashing algorithm used for digital signature process: • RSA SigGen, ECDSA P192 SigGen	SHA-1 (BYTE-only)
RSA (PKCS #1 v1.5)	Signature generation	ALG [RSASSA-PKCS1_V1_5]: SigGen: 1024, 1536
Algorithm required per Postal Authority/Postal Standard: USPS/ Canada Post CPC /TNT		
RSA PKCS #1 v1.5	Key Transport using RSA 1536-bit key (Key Encapsulation)	RSA (key wrapping; key establishment methodology provides 90 bits of encryption strength, non-compliant due to having less than 112-bits of encryption strength);
ECDSA (P192; SHA-1)	Indicia Authentication	PKG: CURVE P-192 ExtraRandomBits SigGen: CURVE P-192: (SHA-1)
Algorithm required per Postal Authority/Postal Standard: Deutsche Post's FRANKIT program		
RSA PKCS #1 v1.5	Key Transport RSA 1024-bit key (Key Encapsulation)	RSA (key wrapping; key establishment methodology provides 80 bits of encryption strength, non-compliant due to having less than 112-bits of encryption strength);

Figure 7 – Non-Approved Security Functions

3 SENSITIVE SECURITY PARAMETERS MANAGEMENT

3.1 Critical Security Parameters

The PSD Critical Security Parameters are listed below:

Name	Algorithm / Key Size	Description/Usage	Generation	Storage	Distribution	Zeroization
Common CSPs (independent of country configuration)						
Master Secret Key	AES CBC 128 bits	Internally encrypt & decrypt PSD's critical security parameters	Internally ANSI X9.31 RNG	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
RNG Seed	ANSI X9.31 128 bits	Current status of the seed used by the Approved RNG.	N/A	In plaintext in tamper protected memory	Entered in factory	
RNG Key	ANSI X9.31 AES 128 bits	Key used by the Approved RNG underlying encryption algorithm	N/A	In plaintext in tamper protected memory	Entered in factory	
TLS Communication Private Key	RSA PKCS #1 v1.5 2048 bits	Authenticates messages and data output from the PSD during TLS Handshake Protocol.	Internally ANSI X9.31 RNG	encrypted	N/A	Rendered unusable by zeroization of "Master Secret"
CSPs Specific to United States Postal Service IMI_2013 Standard						
Indicia Authentication Private Key	ECDSA P224 224 bits	Indicia authentication	Internally ANSI X9.31 RNG	encrypted	N/A	Rendered unusable by zeroization of "Master Secret"
CSPs Specific to United States Postal Service IBI_Lite Standard						
Indicia Authentication Secret Key	CMAC AES 128 bits	Indicia authentication	Internally ANSI X9.31 RNG	encrypted	RSA Encapsulation	Rendered unusable by zeroization of "Master Secret"
CSPs Specific to United Kingdom Royal Mail EIB Standard						
Indicia Authentication Secret Key	HMAC-SHA-256	Indicia authentication	Internally ANSI X9.31 RNG	encrypted	RSA Encapsulation	Rendered unusable by zeroization of "Master Secret"

Name	Algorithm / Key Size	Description/Usage	Generation	Storage	Distribution	Zeroization
CSPs Specific to Canada Post CPC						
Indicia Authentication Private Key	ECDSA P192 192 bits	Indicia authentication	Internally ANSI X9.31 RNG	encrypted	N/A	Rendered unusable by zeroization of "Master Secret"
Indicia Authentication Secret Key	HMAC-SHA-1 160 bits	Indicia authentication	Internally ANSI X9.31 RNG	encrypted	RSA Encapsulation	
CSPs Specific to DPAG						
m-secret	N/A	DPAG secret information	DPAG	encrypted	RSA Encapsulation	Rendered unusable by zeroization of "Master Secret"
m-secret Encapsulation Key [5]	RSA PKCS #1 v1.5 1024 bits	transport m-secret from Post to PSD	Internally ANSI X9.31 RNG	encrypted	N/A	

Figure 8 – Critical Security Parameters

Name	Algorithm / Key Size	Description/Usage	Generation	Storage	Distribution	Zeroization
DH private key (TLS Handshake)	Diffie-Hellman 1024 bits	Diffie-Hellman private key used to agree TLS pre-master	Internally via ANSI X9.31 RNG	N/A	N/A	Immediately after use (i.e. TLS-pre-master key establishment)
TLS pre-master key [6]	128 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 9 – TLS v1.0 Handshake Protocol Critical Security Parameters (independent of country configuration)

Name	Algorithm / Key Size	Description/Usage	Generation	Storage	Distribution	Zeroization
TLS Communication Secret Keyset (TLS Record Protocol Keys)	AES, HMAC 4 x 128 bits	Encrypt & Decrypt & Integrity TLS Communication	Approved TLS KDF	plaintext	N/A	TLS session closure

Figure 10 – TLS v1.0 Record Protocol Critical Security Parameters (independent of country configuration)

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.

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

[6] This key is negotiated using a non-compliant algorithm (the algorithm offers less than minimum of 112-bit of security strength), therefore it shall not be used in the approved mode of operation

3.2 Public Security Parameters

Name	Algorithm	Description	Storage	Generation
Common public keys (independent of country configuration)				
Root Public Key (Neopost Root Certificate)	RSA 2048	Signed X509 Certificate of the current Root Public key used for the verification of authenticated messages input from the Neopost server	plaintext	N/A
Previous Root Public Key (Neopost Previous Root Certificate)	RSA 2048	Signed X509 Certificate of the previous Root Public key used for the verification of authenticated messages input from the Neopost server.	plaintext	N/A
Region Public Key (Neopost Region Certificate)	RSA 2048	Signed X509 Certificate of the current Region Public key used for the verification of authenticated messages input from the Neopost server.	plaintext	N/A
TLS Communication Public Key (Neopost PSD Certificate)	RSA 2048	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.	plaintext	Internally via ANSI X9.31 RNG
TLS Diffie-Hellman Public Parameters	Diffie-Hellman	Diffie-Hellman parameters (G, P, Ys) used during TLS handshake to agree upon a TLS premaster secret.	plaintext	N/A
Public Keys Specific to United States Postal Service IMI_2013 Standard				
Indicia Authentication Public Key	ECDSA P224	Indicia authentication	plaintext	Internally via ANSI X9.31 RNG
Public Keys Specific to United States Postal Service IBI_Lite				
Indicia Key Encapsulation Public Key [7]	RSA (1536 bits)	Encrypts the Indicia Secret Key before sending it to the Neopost server.	plaintext	N/A
Public Keys Specific to UK Royal Mail EIB Standard				
Indicia Key Encapsulation Public Key [8]	RSA (1536 bits)	Encrypts the Indicia Secret Key before sending it to the Neopost server.	plaintext	N/A
Public Keys Specific to Canada Post CPC				
Indicia Authentication Public Key	ECDSA P192 (192 bits)	Indicia authentication	plaintext	Internally via ANSI X9.31 RNG
Indicia Key Encapsulation Public Key [9]	RSA (1536 bits)	Encrypts the Indicia Secret Key before sending it to the Neopost server.	plaintext	N/A
Public Keys Specific to DPAG				
m-secret Encapsulation Public Key [10]	RSA (1024 bits)	Encrypts the “m-secret” before sending it to the PSD.	plaintext	N/A

Figure 11 – Public Security Parameters

All public keys are protected from unauthorized modification and substitution.

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

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

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

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

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
- RNG error
- High temperature detected error
- Conditional test error
    - DH Pairwise Consistency
    - ECDSA P224 Pairwise Consistency
    - ECDSA P192 Pairwise Consistency
    - RSA Pairwise Consistency

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

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 12 – 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) : is the Crypto-Officer and it 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 v1.0 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 v1.0 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	NA
		Read Status Data	NA
	Field Crypto-Officer	Generate PKI Key	(Write/Read) Master Secret Key, RNG parameters, TLS Comm. private key & secret key
		Get/Set PKI Certificate	(Write) TLS comm. private key
		Read Status Data	NA
	Postal Crypto-Officer	Generate Stamp Key	(Write) Indicia Authentication Key(s)
		Set Stamp Info (CPC)	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 comm. private key (Write) TLS comm. secret keys
		Initiate/End Rekey Connection	(Write) TLS comm. private key (Write) TLS comm. secret keys
		Postal Indicia	(Read) Indicia authentication key
		Other Base Services	NA
		Read Status Data	NA
File Signer Tool	R&D Signer	Verify Files	NA
Expertise Tool	Unauthenticated User role	Read Status Data	NA
		Zeroise CSP	(Zeroize) Master Secret Key and RNG parameters (RNG Seed, RNG Key)

Figure 13 – Roles, Services, Operators

5.1 Operator Authentication

The mutual authentication between the Customer / Neopost Administrator and the PSD is based on the TLS v1.0 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^{28}). This is considerably more difficult to break than the 1 in 1,000,000 requirement.
- 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^{26}). 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.

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 1024 encrypt KAT
- RSA 1024 decrypt KAT
- RSA 2048 sign KAT
- RSA 2048 signature verify KAT
- ECDSA P224 sign KAT
- ECDSA signature verification P224 KAT
- ECDSA P192 sign KAT
- ECDSA signature verification P192 KAT
- AES Encrypt KAT
- AES Decrypt KAT
- AES CMAC KAT
- HMAC (SHA-1) KAT
- HMAC (SHA-256) KAT
- Diffie-Hellman KAT
- RNG 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
- RNG continuous test
- ECDSA Pair wise Consistency Tests
- DH Pair wise Consistency Tests

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 APPENDIX A - Glossary

Abbreviation	Description
AES	Advanced Encryption Standard
CMAC	Message Authentication Code
CPC	Canada Post Corporation (courier company, postal operator)
CSP	Critical Security Parameter
DH	Diffie-Hellman key exchange (DHE Diffie Hellman Ephemeral)
DPAG	Deutsche Post AG (courier company, postal operator)
DRBG	Deterministic Random Bit Generator
ECDSA	Elliptical Curve Digital Signature Algorithm
EFP/EFT	Environmental Failure Protection /Testing
FIPS	Federal Information Processing Standard
HMAC	Hashed Message Authentication Code
IBI	Information-Based Indicia
IMI_2013	Intelligent Mail Indicia
NIST	National Institute of Standards and Technology
NRBG	Non-deterministic Random Bit Generator
PSD	Postal Security Device
PKI	Public Key Infrastructure
Royal Mail	Postal service in the United Kingdom of Great Britain and Northern Ireland (courier company, postal operator)
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
TNT	Dutch international transport and logistics corporation (courier company, postal operator)
USPS	United States Postal Service (courier company, postal operator)

12 APPENDIX B – List of Changes

Version	Date	Modification	Writer
0.1	21/06/2013	Creation	Adriana Rosca
1.0	25/07/2013	Update after review with Penumbra Security	Adriana Rosca
2.0	19/09/2013	Update after review with Penumbra Security	Adriana Rosca
3.0	07/10/2013	Update after review with Penumbra Security	Adriana Rosca
4.0	15/10/2013	Update software versions	Adriana Rosca
5.0	25/10/2013	Update after review with Penumbra Security	Adriana Rosca
6.0	20/02/2014	Updated to address CMVP comments regarding algorithm transitions as of 2014	Adriana Rosca
7.0	20/03/2014	Updated to address CMVP comments regarding algorithm transitions as of 2014	Penumbra Security

8.0	15/04/2014	Updated to address CMVP comments regarding algorithm transitions as of 2014	Penumbra Security
9.0	28/05/2014	Updated to address CMVP comments regarding OE and algorithm	Penumbra Security
10.0	30/07/2014	Updated to address additional firmware versions	Penumbra Security
11.0	09/10/2015	Updated to address additional firmware versions	Penumbra Security
12.0	12/16/2015	Updated to address additional hardware versions	Penumbra Security