CCV Cryptographic Module
For
Pitney Bowes ClickStamp Online
Security Policy

(Non-Confidential)

TABLE OF CONTENTS

TABLE OF TABLES

1. INTRODUCTION

Digital postal payment systems, such as the United States Postal Service's Information-based Indicia Program (IBIP) rely on secure accounting of postage funds and printing of secure postage information on a mail piece. A Postal Security Device (PSD) provides security services to support the creation of mail pieces. A Cryptographic Coprocessor for Virtual Meter (CCV), using a secured database of virtual PSD (VPSD) records, provides PSD security functions for many mailers over a wide area network. A CCV, when securely loaded with a VPSD record, acts as the PSD corresponding to that record.

1.1 SCOPE

This document describes the security policy for the secure coprocessor of the Pitney Bowes ClickStamp Online service. It is intended to describe the requirements for the secure coprocessor only and not the entire system.

1.2 REFERENCES

The following documents are referenced by this document, are related to it, or provide background material related to it:

Data Encryption Standard – FIPS PUB 46-2, March 28, 1994
Digital Signature Standard (DSA) – FIPS PUB 186, 1992
Financial Institution Retail Message Authentication – ANSI X9.19, August 13, 1986
PCIBISAIBIPMS, August 19, 1998
PKCS #1: RSA Encryption Standard version 1.5, November 1, 1993
Secure Hash Standard – FIPS PUB 180-1, April 17, 1995
Security Requirements for Cryptographic Modules – FIPS PUB 140-1, January 11, 1994

2. SECURITY LEVEL

The CCV cryptographic module is a multi-chip embedded device based on the IBM4758 hardware. The module provides a PCI bus interface. The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-1.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module	3
Module Interfaces	3
Roles and Services	3
Finite State Machine	3
Physical Security	4
EFP/EFT	4
Operating System Security	NA
Key Management	3
Cryptographic Algorithms	3
EMI/EMC	3
Self Test	3

3. ROLES AND SERVICES

The CCV supports two distinct roles, the PB security administrator role and the VPSD User role. The PB security administrator role provides the services necessary to modify IBIP data, perform key management functions and zeroize keys. The VPSD User role provides the services necessary to dispense indicia and request crediting funds to the descending register. After responding to any command by the PB security administrator or VPSD User, the module will automatically return to its default (unauthenticated) state. The ability to provide a correct Triple-DES MAC proves the knowledge of a key. This key is associated with an individual (or entity) and provides identity-based authentication. Authentication is valid for only one command at a time.

The PB security administrator Role shall provide all the services necessary to credit funds register values, modify IBIP data in PSD records (Date of next required remote inspection, meter license information and public key certificate) and perform key management including key update and zeroize keys. For each command executed, a PB security administrator must authenticate himself to the CCV module via a Triple-DES MAC generated by a ClickStamp Online cryptographic coprocessor for key management (CCK). The CCK is a secure coprocessor used by the PB infrastructure to sign messages

to the CCV on behalf of the PB security administrator. The CCV shall authenticate the PB security administrator based upon a correct Triple-DES MAC presented with each service request. Authentication is valid for only one command at a time.

The PB security administrator services are:

Update Secret Key: Updates the CCV system TDES keys.

Zeroize Keys: Zeroizes CCV system TDES keys.

Manage CCV: Configure CCV with a unique name and set the CCV clock.

Manage Freshness: Synchronize freshness records between CCVs.

IBIP Initialize: Create a new VPSD record, including VPSD specific keys.

Rekey VPSD: Creates a new set of VPSD specific keys.

Authorize VPSD: Authorizes a VPSD to accept refill requests and generate IBIP indicia.

Generate User Key: Generates a TDES key shared between a VPSD user and a VPSD record.

Update VPSD Certificate: Authorize generation of indicia with a new VPSD IBIP public key.

System IBIP Request: Change the IBIP operational status of a VPSD record through enable, disable, cancel and withdraw.

For each command executed to access VPSD services using a VPSD record, a VPSD User must authenticate herself to a CCV via a Triple-DES MAC generated by the ClickStamp Online client application. The CCV verifies the authenticity of the request using information provided in the VPSD record associated with the individual VPSD User. The ability to provide a correct Triple-DES MAC proves the knowledge of a key. This key is associated with an individual (or entity) and provides identity-based authentication. Authentication is valid for only one command at a time.

A VPSD User may request the following VPSD User IBIP request services using a VPSD record associated with the VPSD User.

VPSD User IBIP request services

- Prepare Refill: Generate a Postage Value Download Request message to request crediting funds to the descending register of the VPSD User's VPSD record.
- Dispense Indicium: Generate an indicium and account for the transaction in the ascending and descending register of the VPSD User's VPSD record.
- Dispense Correction Indicium: Generate a correction indicium and account for the transaction in the ascending and descending register of the VPSD User's VPSD record.

A no-role user may perform functions, which do not modify the security or cryptographic state of the module.

The no-role user services are:

Status Inquiry: Generate a message containing status of the CCV.

Initialize Freshness: Process in initializing the CCV for acceptance of new VPSDs.

Prepare Device Audit: Generates a message containing device audit information for a particular VPSD.

The cryptographic module provides services as specified in the IBM4758 security policy. IBM layer 1 code for the 4758 establishes crypto officer roles for layers 2 and 3. Once the CCV is operational, the only services available to these crypto officers is to reload firmware for layers 2 and 3.

4. ALGORITHMS

The cryptographic module implements the following FIPS approved algorithms: DEA, DSA, pseudo-random number generation and SHA-1.

The module also includes these algorithms: RSA, 3DES, OAEP padding for public-key encryption, ISO9796 padding for public key signatures, and hardware random number generation. As required in the USPS IBIP performance criteria, RSA is implemented using PKCS #1 message encoding instead of the FIPS approved ANSI X9.31 message encoding method.

DEA is used in the generation of a triple DEA (TDEA) encryption and in the generation of message authentication.

SHA-1 is used to hash data for generation of message authentication.

5. SELF-TEST

The IBM 4758 provides a series of power-on self-tests to the module prior to execution of the first service request.

After successful completion of the IBM 4758 power-on self-test and prior to execution of the first service request the module shall perform a series of self-tests of all cryptographic functions and the system clock.

6. SECURITY RULES

This section documents the security rules enforced by the cryptographic module to implement the security requirements of this module.

1. The cryptographic module shall provide the PB security administrator Role.
2. The cryptographic module shall provide the VPSD User Role.
3. The cryptographic module shall provide identity-based authentication.
4. Immediately, following the execution of any service request the cryptographic module shall return to the default state.

5. After the cryptographic module has been initialized, the cryptographic module shall not accept any secret or private key in plaintext form.
6. The cryptographic module shall not output any secret or private key in plaintext form.
7. The cryptographic module shall sign digital indicium data using an algorithm selected from the DSA algorithm or the RSA algorithm as defined by the USPS IBIP specification.
8. Digital indicium data shall not be signed unless the proper accounting has been performed.
9. After application of power and prior to execution of the first service request the cryptographic module shall perform the following self-tests: RSA digital signature known answer test (includes a SHA-1 test), DES known answer test, DSA signature test, firmware checksum.
10. The cryptographic module shall allow the PB security administrator to zeroize the keys of the module.
11. The cryptographic module shall verify freshness of the VPSD record before output of a response to any command that updates the VPSD record.
12. The cryptographic module shall verify freshness of the VPSD freshness record before output of a response to any command that updates the VPSD freshness record.

7. ITEMS PROTECTED BY THE MODULE

The module shall protect two types of data items: Security Relevant Data Items (SRDIs) and Funds Relevant Data Items (FRDIs).

7.1 SRDIS STORED IN THE CCV

7.1.1 Definition of SRDIs

The module's stored SRDIs consist of six TDES keys. These keys are stored in plaintext within the cryptographic module boundary. . The keys are:

1. Communication Key: This is a two-key TDES key used to authenticate the PB security administrator.
2. Key Encryption Key: This is a two-key TDES key used to encrypt and decrypt key material.
3. VPSD Record Encryption Key: This is a two-key TDES key used as a VPSD record encryption key.

4. Prior VPSD Record Encryption Key: This is a two-key TDES key used as a prior VPSD record encryption key.
5. VPSD Record Signature Key: This is a two-key TDES key used as a VPSD record signature key.
6. Prior VPSD Record Signature Key: This is a two-key TDES key used as VPSD record signature key.

7.1.2 Definition of SRDI Modes of Access

1. Verify Communication Key Signature: This operation uses the Communication Key to verify the identity of the PB security administrator requesting a service.
2. Encrypt Key with Key Encryption Key: This operation uses the key encryption key to encrypt a key.
3. Decrypt with VPSD Record Encryption Key: This operation uses the VPSD record encryption key or prior VPSD record encryption key to decrypt a VPSD record.
4. Encrypt with VPSD Record Encryption Key: This operation uses the VPSD record encryption key to encrypt a VPSD record.
5. Create VPSD Record Signature Key Signature: This operation uses the VPSD Record Signature Key to generate a signature on a record.
6. Verify VPSD Record Signature Key Signature: This operation uses the VPSD Record Signature Key or Prior VPSD Record Signature Key to authenticate a signed record.
7. Create Communication Key Signature: This operation uses the communication key to sign a message.
8. Decrypt Key with Key Encryption Key: This operation uses the key encryption key to decrypt a key.

7.2 SRDIs STORED IN THE VPSD RECORD

7.2.1 Definition of SRDIs

The VPSD record stored SRDIs consist of a VPSD authentication key, a VPSD user key and a VPSD IBIP private key. These keys are stored encrypted in a signed VPSD record. These keys are generated within the CCV and can be updated by a PB security administrator. The keys are:

1. VPSD IBIP Private Key: This is a DSA private key used to sign IBIP messages produced by the CCV loaded with the VPSD record.

2. VPSD Authentication Key: This is a two-key TDES key used to authenticate messages from the PB security administrator to the VPSD.
3. VPSD User Key: This is a two-key TDES key used to authenticate messages from the VPSD User to the VPSD.

7.2.2 Definition of SRDI Modes of Access

1. Verify VPSD Authentication Key Signature: This operation uses the VPSD authentication key to verify the identity of the PB security administrator.
2. Verify VPSD User Key Signature: This operation uses the VPSD user Authentication key to verify the identity of the VPSD User.
3. Generate VPSD User Key: This operation generates a new VPSD user key for a VPSD.
4. Generate VPSD IBIP Key Pair: This operation generates and stores a new IBIP key pair for a VPSD.
5. Generate VPSD Authentication Key: This operation generates and stores a new VPSD authentication key for a VPSD.
6. Create VPSD Authentication Key Signature: This operation uses the VPSD authentication key to sign a message.
7. Create IBIP Private Key Signature: This operation uses the VPSD IBIP private key to sign an IBIP message from the VPSD.

7.3 FUNDS RELEVANT DATA ITEMS (FRDIS)

7.3.1 DEFINITION OF FRDIs

FRDIs are data items whose authenticity and integrity are critical to the protection of postage funds, but which are not SRDIs and should not be zeroized.

Total Postage Credited: is the sum of all refills to VPSD records by the CCV.
Total Postage Dispensed: is the sum of the values of all indicia and correction indicia evidenced by the CCV.
Total Piece Count: is the number of indicia plus the number of correction indicia dispensed by the CCV.
VPSD Descending Register: is the total funds available to be dispensed by the VPSD.
VPSD Ascending Register: is the sum of the values of all indicia and correction indicia evidenced by the VPSD.
VPSD Piece Count: is the number of indicia plus the number of correction indicia dispensed by the VPSD.
VPSD Record Freshness Data: are data for proving freshness of a VPSD record.

Table 2: Security Relevant Data Item Modes of Access

SRDI Modes of Access **User Services**	Verify Communication Key Signature	Verify VPSD Authentication Key Signature	Verify VPSD User Key Signature	Encrypt Key with Key Encryption Key	Generate VPSD User Key	Generate VPSD IBIP Key Pair	Generate VPSD Authentication Key	Decrypt with VPSD Record Encryption Key	Encrypt with VPSD Record Encryption Key	Create VPSD Record Signature Key Signature	Verify VPSD Record Signature Key Signature	Create Communication Key Signature	Create VPSD Authentication Key Signature	Create IBIP Private Key Signature	Decrypt Key with Key Encryption Key	**Role Requesting Mode of Access**	PB Security Administrator	VPSD User	No-role User
Status Inquiry												x							x
Initialize Freshness										x	x	x							x
Prepare Device Audit	x									x	x	x		x					x
Update Secret Key	x											x			x		x		
Zeroize Keys	x																x		
Manage CCV	x											x					x		
Manage Freshness	x									x	x	x					x		
IBIP Initialize	x			x		x	x		x	x		x		x			x		
Rekey VPSD	x			x		x	x		x	x	x	x	x				x		
Authorize VPSD	x									x	x	x					x		
Generate User Key	x			x	x				x	x	x	x					x		
Update VPSD Certificate	x									x	x	x					x		
System IBIP Request	x	x						x		x	x	x					x		
VPSD User IBIP Request	x		x					x		x	x	x		x				x	

Table 2 shows, for each user role, the SRDI modes of access required by each user service request. An x in a user role column indicates that role is authorized to perform the corresponding user service. Each user service row has an x for each SRDI mode of access required by that service.