REV	EN NO.	SECTION	DESCRIPTION	BY	DATE
1	PCP000034	ALL	INITIAL RELEASE	RC	18JAN00
2			Updated crypto services to match the current module	BMR	3FEB00
3		ALL	Update to limit references to systems outside the CCM	RC	4FEB00
4		3-7	Removed naming inconsistencies. Made document public.	RC	4FEB00
5		All	Added permission to copy to footer	RC	18FEB00
6		ALL	Updated references, TDES Self-test, FIPS table	AS	6APR00
7		6	Modified security rule 7 to indicate use of “uninstall”	RC	13APR00
8		1.2	Corrected 186-1 to 186-2	RC	14APR00

CONFIGURATION CONTROL DOCUMENT P48200 _ _ _ REQUIRES CHANGING WHENEVER THIS DOCUMENT IS UPDATED

PRODUCT CODE NO. P400		Pitney Bowes	
APPROVALS			
BY	DATE	TITLE	Client Cryptographic Module For Pitney Bowes ClickStamp™ Online Security Policy
		PREPARED R. Cordery	DATE 6APR00
		CHECKED	DATE
SHEET 1 OF 7 SHEETS		EN NO. PCP000034	DWG NO. P492058

Oct . 28, 1999

TABLE OF CONTENTS

1 INTRODUCTION......3

1.1 SCOPE......3

1.2 REFERENCES......3

2 SECURITY LEVEL......4

3 ROLES AND SERVICES......4

3.1 CCM USER SERVICES......4

3.2 CCM CRYPTO-OFFICER SERVICES......5

4 ALGORITHMS......5

5 SELF-TEST......5

6 SECURITY RULES......5

7 ITEMS PROTECTED BY THE MODULE......6

7.1 DEFINITION OF SRDI MODES OF ACCESS......6

TABLE OF TABLES

TABLE 1: MODULE SECURITY LEVEL SPECIFICATION 4

TABLE 2: SECURITY RELEVANT DATA ITEM MODES OF ACCESS 7

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. The ClickStamp™ Online (CSO) software Client Cryptographic Module (CCM) provides authentication of client IBIP requests to the remote CSO system. The CCM software module is a separate DLL in the CSO client application. The CCM runs on a general purpose personal computer. The remote CSO system consists of a set of servers, databases and secure coprocessors in a secure facility. The CSO system securely performs the accounting and generation of postage indicium information in secure coprocessor at the secure facility.

1.1 Scope

This document describes the security policy for the client cryptographic module (CCM) of the Pitney Bowes ClickStamp Online client application. It describes requirements for the CCM only and not the entire client application, nor any part of the remote CSO system. This policy includes descriptions of the CSO client application and the remote CSO system where necessary for clarity.

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 46-3, January 15, 1999

Digital Signature Standard (DSA) – FIPS PUB 186-2, December 15, 1998

Financial Institution Retail Message Authentication – ANSI X9.19-1996, May 7, 1996

Triple Data Encryption Modes of Operation – ANSI X9.52-1998, July 29, 1998

PCIBI-O, February 23, 2000

PKCS #1 v2.0: RSA Cryptography Standard, October 1, 1998

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 CCM cryptographic module is a multi-chip standalone device based on general purpose personal computer hardware. The cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-1.

Table 1: Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module	1
Module Interfaces	1
Roles and Services	1
Finite State Machine	1
Physical Security	1
Software Security	1
Operating System Security	1
Key Management	1
Cryptographic Algorithms	1
EMI/EMC	1
Self Test	1

3 Roles and Services

The CCM supports a CCM user role and a CCM crypto-officer role. A CSO customer assumes a CCM user role by requesting a CCM user service. The CSO server acts as the CCM crypto-officer by providing keys to the CCM. The first request for any CCM service causes the CCM to initialize and perform a self-test.

The CCM operates in no authentication mode: neither CCM users nor CCM crypto-officers need to perform any authentication function in order to use the cryptographic module.

3.1 CCM user services

TDES Sign Buffer: The CCM signs a buffer on behalf of the CCM user by generating a SHA-1 message digest and TDES encrypting eight bytes of the digest. All key material is actively zeroized before the TDES Sign Buffer service completes.

Get State: The CCM maintains an internal record of its current state. The Get State function returns the state. Because the CCM is single-threaded, it should not return a value indicating it is performing a calculation, as the current command completes before the get state command. The only returned values should indicate that the CCM is not initialized, the security feature self test failed, or the module is ready to respond to a command.

SHA-1 Buffer: Computes a SHA-1 hash of the contents of a memory buffer. This service is called by the TDES Sign Buffer service.

SHA-1 File: Computes a SHA-1 hash of a file on disk or other storage media.

3.2 CCM crypto-officer services

TDES Encrypt: Encrypts a TDES key with a TDES key encrypting key. Triple DES in CFB mode is used for encryption. The CCM crypto-officer provides the TDES key encrypting key. All key material is actively zeroized before the TDES Encrypt service completes.

TDES Decrypt: Decrypts a TDES key with the TDES key encrypting key. The CCM crypto-officer provides the TDES key encrypting key. Triple DES in CFB mode is used for decryption. All key material is actively zeroized before the TDES Decrypt service completes.

4 Algorithms

The cryptographic module implements the following FIPS approved algorithms: DES, TDES, and SHA-1.

DES is used in the generation of a triple DES (TDES) CFB (Cipher Feedback) operation. DES is also used to compute a CBC (Cipher Block Chaining) based MAC (Message Authentication Code) during the CCM code integrity test.

TDES is used in CFB mode for encrypt and decrypt.

SHA-1 is used to hash data for generation of message authentication. It is also used by the client system configuration manager to demonstrate file integrity.

5 Self-Test

The CCM performs a series of self-tests of all cryptographic functions and a cryptographic check sum of the CCM binary code. Specifically, the CCM performs three self tests:

1. A SHA-1 known answer test

2. A TDES known answer test that is performed with key1 = key2 = key3.

3. A code integrity test performed by verifying that an externally supplied eight byte value equals a DES MAC of the CCM binary file.

The CCM performs the self-test before performing any cryptographic operation.

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 CCM crypto-officer role.
2. The cryptographic module shall provide the CCM user role.
3. The cryptographic module shall operate in no authentication mode.
4. Immediately following the execution of any service request the cryptographic module shall return to the default state.
5. After initialization and prior to execution of the first service request, the cryptographic module shall perform the self-tests defined in section 5.
6. The cryptographic module shall actively zeroize memory allocated for the keys dynamically stored in the module upon the completion of each cryptographic service request.
7. The user deletes the code validation key by uninstalling the cryptographic module using the Microsoft Windows® operating system uninstall facility to remove the ClickStamp Online application.

7 Items Protected by the module

The module does not store any Security Relevant Data Item (SRDI) internal to the module. The TDES signing key is stored encrypted on the hard drive of the personal computer. The code validation key is hard-coded in the CCM binary code. This key is loaded into the module during the code integrity self test.

1. TDES Signing Key: This is a two-key TDES key used to authenticate messages.
2. Key Encryption Key: This is a two-key TDES key used to encrypt and decrypt key material.
3. Code Validation Key: This is a single DES key used to calculate a MAC on the crypto module binary executable code.

7.1 Definition of SRDI Modes of Access

1. Encrypt Key with Key Encryption Key: This operation uses the key encryption key to encrypt a TDES signing key on behalf of the CCM crypto-officer. This mode is implemented in the TDES Encrypt service.
2. Decrypt Key with Key Encryption Key: This operation uses the key encryption key to decrypt a TDES signing key on behalf of the CCM crypto-officer. This mode is implemented in the TDES Decrypt service.
3. Sign Message: This operation uses the TDES signing key to sign a message on behalf of the CCM user. The key encryption key is provided by the CCM user. This mode is implemented in the TDES Sign service.
4. Code Integrity Test: This operation uses the code validation key to compute a DES CBC based MAC of the binary executable file that implements the crypto module. The code validation key hard coded in the CCM binary code.

Table 2: Security Relevant Data Item Modes of Access

User Services	SRDI Modes of Access				Role Requesting Mode of Access	
	Encrypt Key with Key Encryption Key	Decrypt Key with Key Encryption Key	Code Integrity Test with Code Validation Key	Sign Message with Key encryption Key	CCM Crypto-Officer	CCM user
TDES Encrypt	x				x	
TDES Decrypt		x			x	
TDES Sign Buffer				x		x
SHA-1 Buffer						x
SHA-1 File						x
Get State						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.