


REV	SECTION NO.	EN	DESCRIPTION	BY	DATE
0.1	All		Original Document	F. Ryan, Jr.	July 18, 1997
0.2	2 3,5 4 5		Clarified description of crypto module as a single chip Combined Crypto Officer and User Role and added operations "On-behalf of" Modified security rules for power up self test Added key storage and access description	F. Ryan, Jr.	Jan. 12, 1998
0.3	2 3.1 3.2 4 5.1 5.1.3		Changed self test from level 2 to level 3 – since no statistical random number generator test is required for RSA digital signatures  Added the zeroize keys service  Changed SIGN ECC command name to Debit & Sign  Changed ECDSA signatures to RSA signatures Changed startup self test to include known answer for RSA (including SHA-1) and DES Added key zeroization  Changed crypto algorithm references from ECDSA to RSA  Added zeroize keys to table	F. Ryan, Jr.	Jun. 02, 1998
0.4	3.2 4 5.1.3 5.2.3		Added Postage Value Update  Removed RNG self test policy  Added Postage Value Update to table  Added Postage Value Update & Zeroize Keys to table	F. Ryan, Jr.	Jun. 12, 1998
0.5	4 4		Removed requirement that the devie not operate outside of its intended operating range, since it is not required by FIPS level 3  Added hard opaque epoxy requirement	F. Ryan, Jr.	Jun. 19, 1998

		TITLE	
		<b>PC Meter Cryptographic Module Security Policy</b>	
PREPARED BY	DATE	ER NO.	DOC NO.
Frederick W. Ryan, Jr.	June 19, 1998		<b>P297012</b>
CHECKED BY	DATE	PRODUCT CODE NO.	
		P200	<b>SHEET 1 OF 12</b>

This document/data record is the property of Pitney Bowes Inc. and contains PROPRIETARY and CONFIDENTIAL information, and is not to be copied.

# SIGNATURES

---

APPROVED BY:	SIGNATURE:	DATE:

# TABLE OF CONTENTS

<b>1. INTRODUCTION.....</b>	<b>5</b>
1.1 SCOPE.....	5
1.2 REFERENCES.....	5
<b>2. SECURITY LEVEL .....</b>	<b>6</b>
<b>3. ROLES AND SERVICES.....</b>	<b>6</b>
3.1 CRYPTO OFFICER/USER ROLE .....	6
3.2 ON BEHALF OF CRYPTO OFFICER/USER.....	7
3.3 OTHER SERVICES .....	7
<b>4. SECURITY RULES.....</b>	<b>7</b>
<b>5. ITEMS PROTECTED BY THE MODULE .....</b>	<b>8</b>
5.1 SECURITY RELEVANT DATA ITEMS (SRDI'S).....	8
5.1.1 Definition of SRDI's .....	8
5.1.2 Definition of SRDI Modes of Access.....	8
5.1.3 Service to SRDI Access Operation Relationship.....	9
5.2 FUNDS RELEVANT DATA ITEMS (FRDI'S) .....	10
5.2.1 DEFINITION OF FRDI'S .....	10
5.2.2 Definition of FRDI Modes of Access.....	10
5.2.3 Service to FRDI Access Operation Relationship.....	11
<b>6. OTHER SERVICES DISABLED IN MANUFACTURING.....</b>	<b>12</b>

# TABLE OF TABLES

MODULE SECURITY LEVEL SPECIFICATION .....	6
SERVICE TO SRDI RELATIONSHIP .....	9
SERVICE TO FRDI RELATIONSHIP .....	11

# 1. INTRODUCTION

---

A new Postal Payment System has been proposed. This system relies 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 as defined by the Information Based Indicia Program (IBIP).

## 1.1 SCOPE

This document describes the security policy for the smart card vault of the Pitney Bowes PC Meter. It is intended to describe the requirements for the vault 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

The Elliptic Curve Digital Signature Algorithm - ANSI X9.62 (draft standard), August 31, 1996

Financial Institution Retail Message Authentication – ANSI X9.19, August 13, 1986

IEEE P1363 Standard (Working Draft) Elliptic Curve Systems, February 6, 1997

Information Based Indicia Program Indiciium Specification, June 13, 1996

Information Based Indicia Program Key Management Plan, April 25, 1997

Information Based Indicia Program Postal Security Device Specification, June 13, 1996

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 PC Meter Cryptographic Module consists of a single integrated circuit. The interface to the integrated circuit is a serial interface which conforms to the ISO/IEC 7816-3 smart card standard. The cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-1..

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

Module Security Level Specification

## 3. ROLES AND SERVICES

The cryptographic module shall support one distinct role, the Crypto Officer/User Role. A Crypto Officer/User must authenticate himself to the module via a digital signature for each command executed. The ability to provide a correct signature proves the knowledge of a key. This key is stored in a secure coprocessor which must be initialized by at least three Pitney Bowes corporate officers. As a result, all successful Crypto Officer/User authentications can be traced back to these three individuals. Other module services may be accessed by anyone in possession of the device. Authentication is valid for only one command at a time. After execution of any command by the Crypto Officer/User the module will automatically return to its default (unauthenticated) state.

### 3.1 CRYPTO OFFICER/USER ROLE

Since no key data or algorithm parameters of the cryptographic module may be modified after the module has been manufactured, there is no explicit cryptographic officer role. Therefore, the Crypto Officer and User Roles have been combined. The Crypto Officer/User Role shall provide all the services necessary to credit funds register values and modify IBIP data (Date of next required remote inspection, meter license information and public key certificate). The Crypto Officer/User shall be authenticated based upon a correct digital signature presented with each service request. This includes the following services:

- Credit. This service allows the Crypto Officer/User to add funds to the descending register (and control sum) of the module.
- Put IBIP Data. This service allows the Crypto Officer/User to write data related to IBIP functions to the module, such as: Date of next required remote inspection, meter license information and public key certificate.
- Zeroize Keys. This service allows the Crypto Officer/User to instruct the module to zeroize the Vault Private Key and Certificate Keys.

### 3.2 ON BEHALF OF CRYPTO OFFICER/USER

Two services are available to the operator of the module. These functions do not permit the operator to modify the security or cryptographic state of the module. However, these services do allow the operator to act on behalf of the Crypto Officer/User to perform the following functions:

- Get Inspection Certificate. This service instructs the module to generate a signature of the data contained in the module's internal registers.
- Debit & Sign. This service debits funds from the module and generates a certificate verifying that the funds have been debited.
- Postage Value Update. This service debits funds from the module and generates a certificate verifying that the funds have been debited.

### 3.3 OTHER SERVICES

The module shall provide all the services necessary to produce IBIP open systems compliant digital signatures to anyone in possession of the module. This includes the following services:

- Card Info. This service queries the module to obtain: the card serial number, GEMPlus and PBI references, Card reference date, funds register values (ascending and descending registers), piece counter, recharge counter and optionally the Chip Serial Number.
- Real Time. This service informs the module of the current time.
- Get Info. This service reads data from the card related data areas.
- Get IBIP Data. This service reads data related to IBIP functions from the module, such as: Date of next required remote inspection, meter license information and public key certificate.
- Verify Code. This service enables the reading of various log files (via the Get Data command) by entering a specific code.
- Get Data. This service returns the data contained in various log files.

## 4. 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 one distinct operator role. The Crypto/Officer User Role.

2. The cryptographic module shall provide identity based authentication.
3. Immediately, following the execution of any service request the cryptographic module shall return to the default state.
4. The cryptographic module shall authenticate the Crypto Officer/User for each service requested based upon the presence of a correct digital signature.
5. The cryptographic module shall validate the User signature using a digital signature (message authentication code) as defined by ANSI X9.19.
6. The cryptographic module shall sign digital indicium data using the RSA algorithm as defined by PKCS#1 (ANSI X9.62).
7. Digital indicium data shall not be signed unless the proper accounting has been performed.
8. 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, firmware checksum.
9. The cryptographic module shall be covered with a hard opaque epoxy.
10. The cryptographic module shall allow the Crypto Officer/User to zeroize the keys of the module.

## 5. ITEMS PROTECTED BY THE MODULE

---

The module shall protect two types of data items: Security Relevant Data Items (SRDI's) and Funds ).

### 5.1 SECURITY RELEVANT DATA ITEMS (SRDI's)

#### 5.1.1 Definition of SRDI's

The module's SRDI's consist of two signature keys. These keys are stored in plaintext within the cryptographic module boundary. Programming of these keys is performed at the time of manufacture of the module. Once the module has been manufactured these keys are unable to be output by the module in any form. The keys are:

1. Vault Private Key: This is an RSA private key used to sign postal indicium and inspection certificates produced by the module. All data signed by this key has the USPS as its intended recipient.
2. Certificate Key: This is two DES keys used to authenticate the signatures of the Crypto Officer/User. All data correctly signed by this key originated from the Pitney Bowes Data Center.

#### 5.1.2 Definition of SRDI Modes of Access

1. Create RSA Signature: This operation creates an RSA signature of the supplied data using the Vault Private Key.



2. Verify Crypto Officer/User Signature: This operation uses the Communication Key to verify the identity of the Crypto Officer/User (the Pitney Bowes Data Center) requesting a service.

### 5.1.3 Service to SRDI Access Operation Relationship

The following table has been devised to show these relationships:

<i>Services Versus SRDI Access</i>	SRDI Access Operation		Applicable Role		
	Create RSA Signature	Verify Crypto Officer/User Signature	Crypto Officer/User Role	On-Behalf of Crypto Officer/User	Other Services
User Service					
Credit		X	X		
Put IBIP Data		X	X		
Card Info					X
Real Time					X
Get Info					X
Get Inspection Certificate	X			X	
Debit & Sign	X			X	
Postage Value Update	X			X	
Get IBIP Data					X
Verify Code					X
Get Data					X
Zeroize Keys		X	X		

Service to SRDI Relationship

## 5.2 FUNDS RELEVANT DATA ITEMS (FRDI's)

### 5.2.1 DEFINITION OF FRDI's

The funds registers are used to account for funds credit to and debit from the module. The module may be debited by anyone in possession of it. The module may only be credited by a Crypto Officer/User. These registers are:

1. Ascending Register. This register contains the total amount of funds spent over the lifetime of the module.
2. Descending Register. This register contains the amount of funds currently available in the module.
3. Control Sum. This register contains the total amount of funds credited to the module over the lifetime of the module.

### 5.2.2 Definition of FRDI Modes of Access

1. Debit Funds: This operation subtracts funds from the vault.
2. Credit Funds: This operation adds funds to the vault.

### 5.2.3 Service to FRDI Access Operation Relationship

The following table has been devised to show these relationships:

<i>Services Versus FRDI Access</i>	FRDI Access Operation		Applicable Role		
	Debit Funds	Credit Funds	Crypto Officer/User	On-Behalf of Crypto Officer/User	Other Services
User Service					
Credit		X	X		
Put IBIP Data			X		
Card Info					X
Real Time					X
Get Info					X
Get Inspection Certificate				X	
Debit & Sign	X			X	
Postage Value Update	X			X	
Get IBIP Data					X
Verify Code					X
Get Data					X
Zeroize Keys			X		

Service to FRDI Relationship

## 6. OTHER SERVICES DISABLED IN MANUFACTURING

The PC Meter Cryptographic Module includes additional services common to other Pitney Bowes products which may be used in the future. However, these services require another type of authentication process. This authentication will be disabled in Pitney Bowes manufacturing facility by setting the Failed Authentication Counter (FAC) stored in Card Data Area 2 to its maximum value (255). In addition, two commands exist for initialization purposes. These commands will also be disabled (by locking the card, Bissuer=1) immediately following card personalization in manufacturing. The commands are listed in the following table:

<b>Command</b>	<b>Function</b>	<b>Disable Mechanism</b>
Select Key	Set up a Session Key	FAC = 255
Debit	Deduct funds	FAC = 255
Sign	Generate Digital Tokens	FAC = 255
Update Keys	Compute new Token Keys	FAC = 255
External Authenticate	Verify knowledge of a key, enable commands	FAC = 255
Put Info	Modify Card Related Data Areas 1 and 2	FAC = 255
Update Memory	Card Initialization	Bissuer = 1
Read Memory	Card Initialization	Bissuer = 1