SECURITY POLICY

PITNEY BOWES
PC METER

APRIL 1999

TABLE OF CONTENTS

LIST OF TABLES

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 Pitney Bowes PC Meter. It is intended to describe the requirements for the Postal Security Device (cryptographic module) 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
Financial Institution Retail Message Authentication – ANSI X9.19, August 13, 1986
Information Based Indicia Program Indicium 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 multiple chip standalone device. The interface the PC is a serial RS232 interface. The module contains a previously validated smart card (FIPS 140-1 certificate 30). 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
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 supports 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 associated with an individual (or group of individuals acting as a single entity) and provides identity-based authentication. 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.

No key data or algorithm parameters of the cryptographic module may be modified after the module has been manufactured. Therefore, the Crypto Officer and User Roles have been combined. The Crypto Officer/User Role may is able to credit funds register values, modify IBIP data and zeroize keys.. The Crypto Officer/User is authenticated based upon a correct digital signature presented with each service request.

An operator of the module may act on behalf of the Crypto/Officer/User to perform functions that do not modify the security or cryptographic state of the module. The

operator may request digital certificates from the module, which indicate the state of the module or provide evidence that funds have been debited from the module. In addition, an operator may read the status of the module and read data, which is not security critical.

4. ALGORITHMS & SELF-TEST

The cryptographic module implements the following FIPS approved algorithms: DEA and SHA-1. The DEA is used in the generation of ANSI X9.19 digital signatures to provide user authentication services. The SHA-1 is used to hash data as part of the RSA (PKCS#1) digital signature algorithm. RSA digital signatures form part of the digital certificates which provide evidence of funds debit operations and module state.. After application of power and prior to execution of the first service request the module performs a full self-test of all cryptographic functions.

5. SECURITY MECHANISMS

The module meets FIPS 140-1 level 3 requirements for physical security. The crypto module is fully protected with a hard, opaque coating to resist observation and/or probing of the module. Additional proprietary security features to detect and respond to tampering are also implemented.