Pitney Bowes

Compliant Meter PSD Security Policy

Dwg No:VA97004

Rev: H

EN: DPP001201

Created on: February 1, 2002

Last Revised on: September 19, 2002

Name	Signature	Date
Robert Tolmie		
Maria Parkos		
Tom Athens		

Table of Contents

Table of Figures

Table of Tables

1. Introduction

Digital postal payment systems, such as the United States Postal Service's Information-based Indicia Program, rely on secure accounting of postage funds and printing a cryptographic digital postage mark on a mail piece. A Postal Security Device (PSD) provides security services to support the creation of digital postage marks that are securely linked to accounting. A PSD provides protection for two types of data: data integrity, authentication, and secrecy of Security Relevant Data Items (SRDIs), such as keys or passwords , and data integrity protection for Funds Relevant Data Items (FRDIs) such as accounting data and freshness data. SRDIs and FRDIs reside in the PSD.

1.1.Scope

This document describes the security policy for the Pitney Bowes Common Meter (CoMet) PSD . 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 46-3, October 25, 1999
- Financial Institution Retail Message Authentication – ANSI X9 .19, August 13, 1986
- Digital Signature Standard (DSA) – FIPS PUB 186-2, 2000
- 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. Implementation Architecture

The User Interface Controller (UIC) is a common component for multiple product lines within Pitney Bowes. The hardware is structured to fit the general requirements for a mailing system controller. Different Part Control Numbers (PCN) will be accommodated by downloading different software into the UIC. Similarly, the PSD will be customized in manufacturing to match the specific PCN.

Figure 1 shows a high level schematic of the UIC system with its associated PSD . This is only a partial schematic of the UIC to clarify the interface to the PSD.

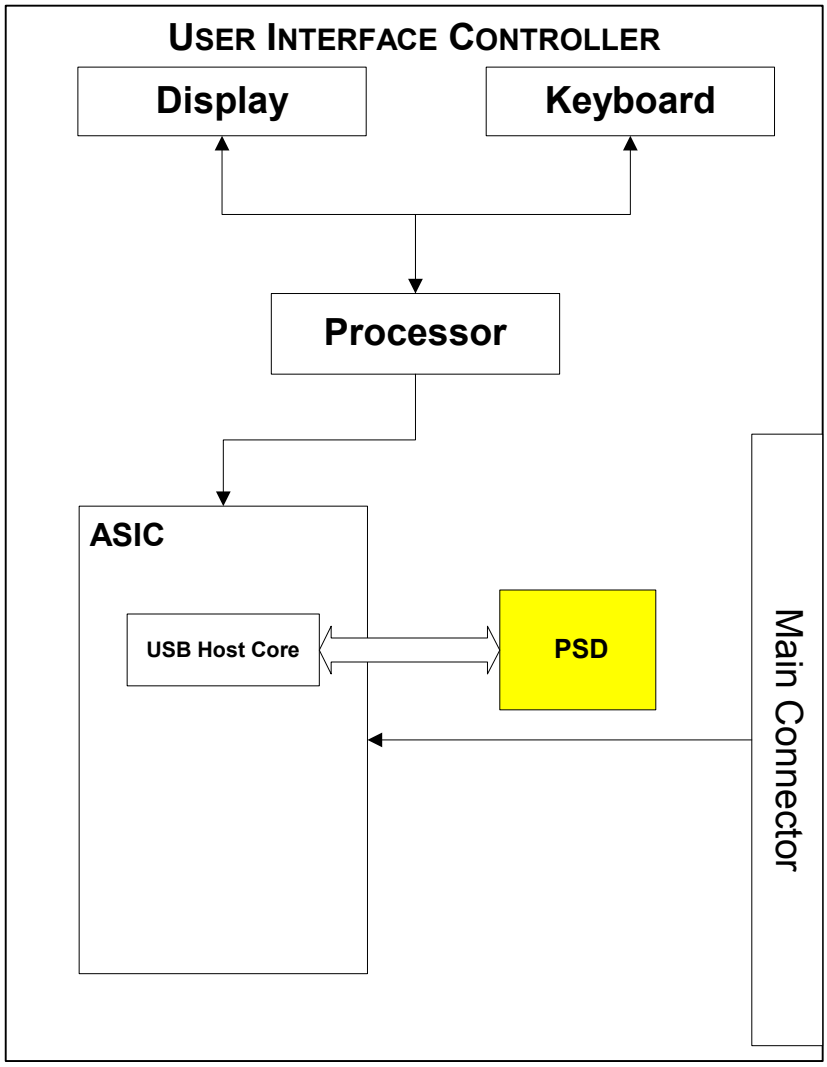


Figure 1 - UIC High Level Schematic

The PSD software is organized into discrete layers as shown in Figure 2 (Logical View of Software Architecture).

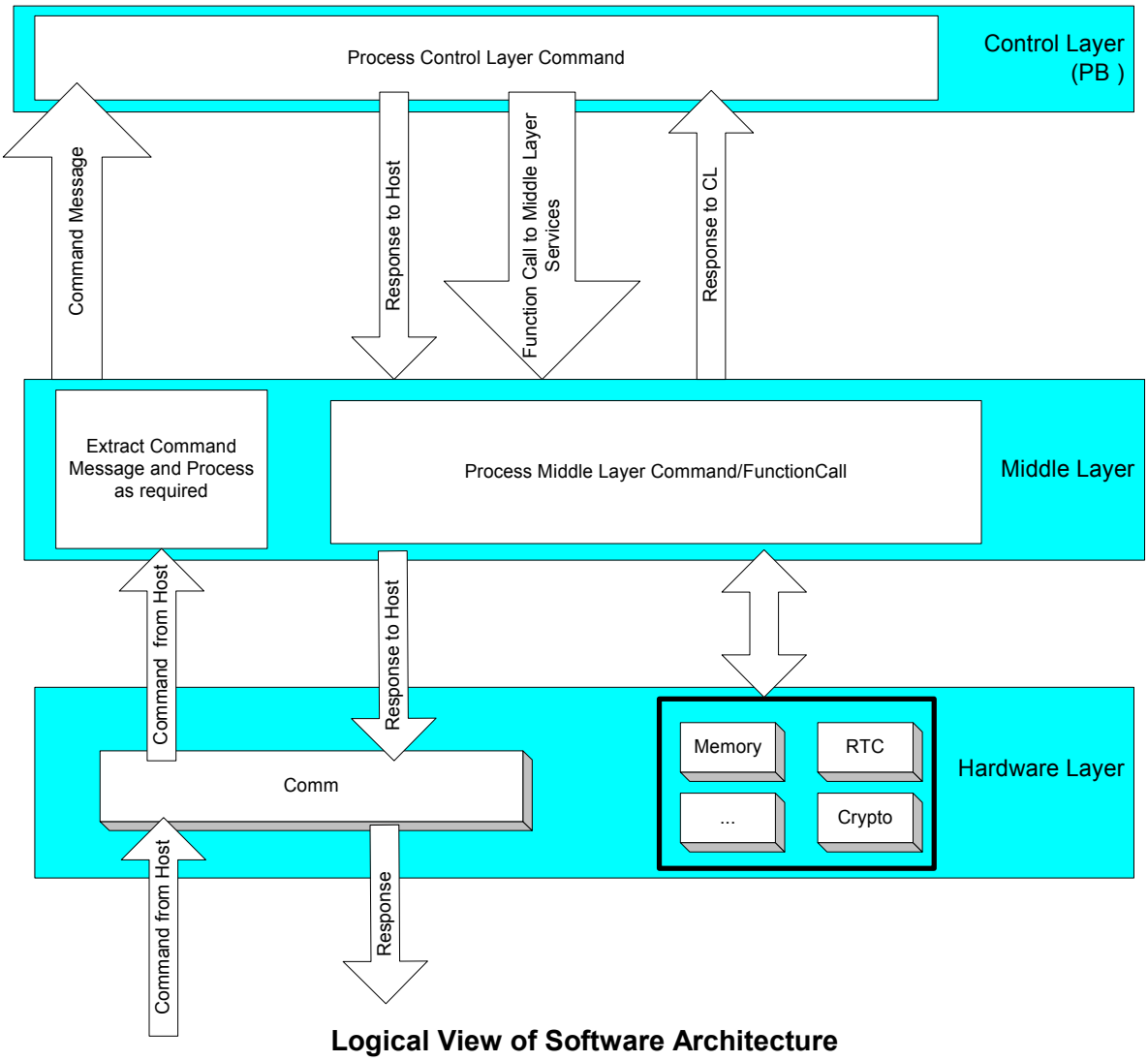
The Control Layer communicates with the Middle Layer software which provides low-level functions such as cryptographic, file management, communications, etc. It communicates with the PSD host and interfaces with other hardware and firmware elements. Generally, the host is the electronic package of a PB meter installed in a mailing machine, which may be in communication with the computer services of the PB Infrastructure Data Center. The Control Layer accesses the nonvolatile memory (NVM) and the real-time clock via the Middle Layer functions. The current interface between the two layers is

specified in the PB-Postal Security Device / MYK-82A Interface Control Document, which is part of the contractual relationship between PB and the current subcontractor.

Both layers co-exist on the same ARM processor with a single thread of control.

When the power is applied, the Middle Layer software has control of the processor until it has successfully completed power up checks, after which the Middle Layer passes control to the CL to perform its power up routines. After the CL has successfully initialized, it returns control to the ML, which waits for host messages. Once a message is received, the Middle Layer software/firmware calls the Control Layer firmware to process the message.

Figure 2- Logical View of Software Architecture



Logical View of Software Architecture

3. Security Level

The Comet Meter Cryptographic Module consists of a multi-chip stand alone module residing within a tamper resistant enclosure . The module provides a logical USB interface. 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 Model	3
Physical Security	3
Software Security	3
Operating System Security	NA
Key Management	3
Cryptographic Algorithms	3
EMI/ EMC	3
Self Test	3

Table 1 - Module Security Level Specification

4. Roles

Each request sent to the PSD that is signed with a particular key authenticates the entity that owns the key to the PSD. The simplest way to look at it: every time the PSD verifies a signature it is authenticating an entity. Each private key has an associated certificate which is used by the PSD to verify message signatures.

The cryptographic module shall support the following roles:

- Crypto Officer
- PSD Administrator
- Printhead Administrator
- Financial Officer
- Customer (on behalf of other role)

Each role is described in detail below.

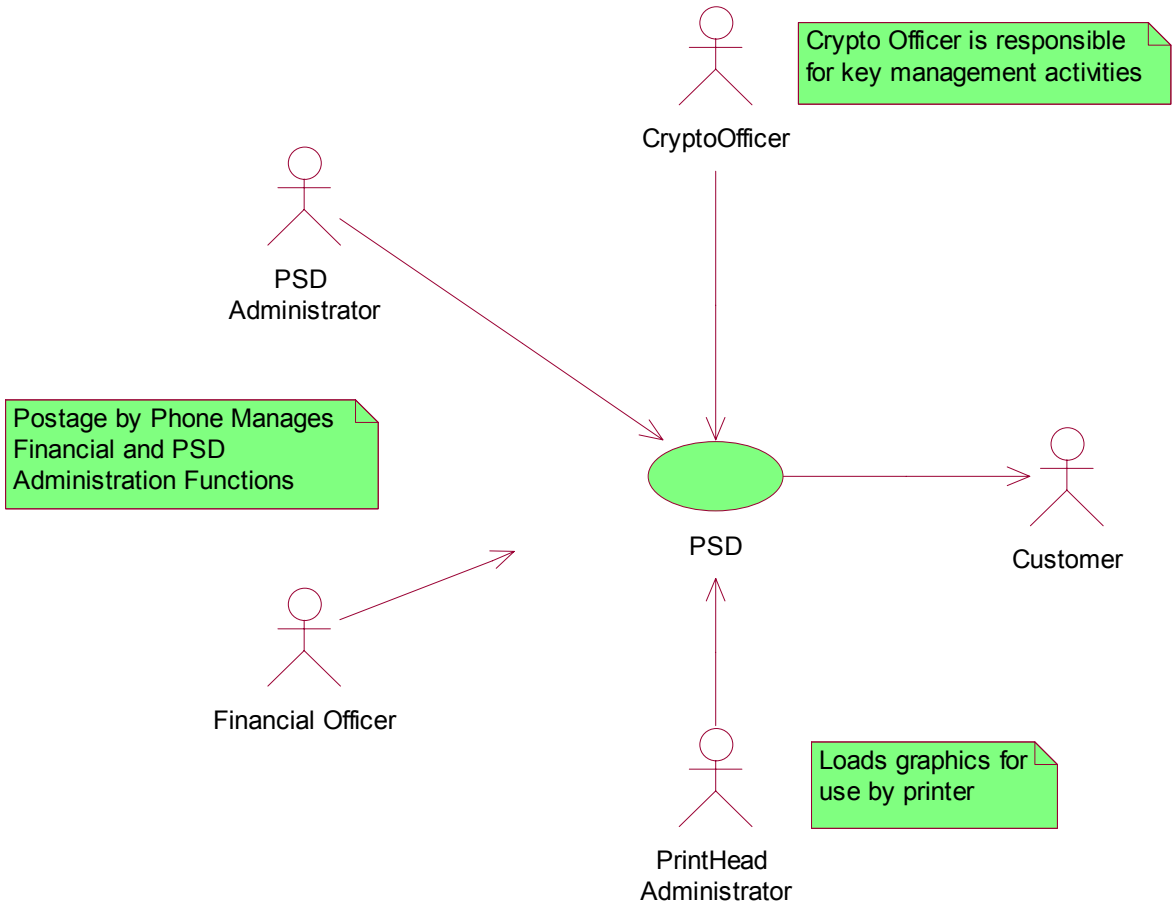


Figure 3 - Roles

4.1.Crypto Officer Role

4.1.1. General Information

The crypto officer is responsible for the high level key management within the box. The primary functions are to load keys into the PSD , and to authorize the generation and use of an IBI key.

Note: The Middle Layer actually stores and manages the key once the message containing the key has been verified by the Control Layer. From that point on, only the Middle Layer has access to the actual key material.

4.1.2. Acting Individual or Organization

The Key Transaction Processor within Pitney Bowes can load signed key records into any secure box.

The vault manufacturing security coprocessor or the PB Data Center can issue the Generate Key and Authorize PSD Key requests.

4.1.3. Services

4.1.3.1. Authorize PSD Key

The Authorize PSD Key message shall cause the PSD to complete the Generate PSD Key transaction. This shall place the PSD in Full Postal state. The Authorize PSD Key command shall instruct the PSD to begin using the new key that was created by the previous Generate PSD Key command. The PB Infrastructure Data Center message with a PSD Key Record shall be included in the transaction. This record shall include the PSD public key and the Certificate ID that was received from the certificate authority. The record shall be signed with the PB Infrastructure Data Center authentication certificate private key. The PSD shall validate the message header and data content and then shall make the new key active. The PSD shall also prepare the Authorize PSD record and shall sign it with the unique PSD Authentication Information Based Indicia (IBI) private key.

4.1.3.2. Delete all Keys & Control Layer

In response to the Host, the PSD shall zeroize all private and secret keys in the system and shall remove the control layer from the system and place the PSD in Transport Mode.

4.1.3.3. Generate Key Exchange Key

The Host shall instruct the PSD to generate an RSA public and private key pair, which is the Key Exchange Key. The response message shall contain the public portion of the Key Exchange Key.

4.1.3.4. Generate PSD Key

The public and private key pair that is the PSD Authentication Key shall be generated by the PSD, when the Host sends this command message. It shall generate the DSA public/private keys. The message shall include the Signed Key Record SKR), with parameters to be used. The cryptographic algorithm used by the PSD for IBI is DSA. The Record Type and the Key Name in the SKR shall determine the algorithm to be used. In this state, the PSD shall verify the signature on the incoming message. It shall use the middle layer key pair generation algorithm, GenerateKeyPair. Upon successful completion of the key generation, the key attributes shall be retained, such as:

- Start and end key validity dates
- Key identifier, which is composed of the Revision and key name

The key that is generated cannot be used for debit functions, until authorized by the post office, but it may be used for other operations, for example: Audit processing and self-signing of the response message (e.g., public key); retrieve a public key and sign a response back to the host.

4.1.3.5. Get Certificate Key

The Get Certificate Key shall cause the PSD to output the signed crypto key record that contains the public date included in the specified Certificate key.

4.1.3.6. Get Key Exchange Key

In response to this command, the PSD shall output the signed crypto key record that contains the public data included in the PSD Key Exchange Key.

4.1.3.7. Get PSD Certificate

The Host instructs the PSD to send the signed key record that shall contain the public data associated with the PSD Authentication key. This command provides the PSD public key data. The command is used by the print head controller. The middle layer service that is called by the Control Layer software is the GetPublicKey service.

4.1.3.8. Get Public Key Data

After the Load Public Key command has been executed, in order to load the public crypto key data into the PSD, the Host shall use this command to retrieve the public key data from the PSD.

4.1.3.9. Load Certificate Key

The Load Certificate Key message shall cause the PSD to pass the certificate key to the middle layer for storage. The incoming signed message shall be verified prior to taking action on the request.

4.1.3.10. Load Public Key

The PSD shall be instructed by the Host to load a public key, which is to be stored in the NVM. In this state, the PSD shall verify the incoming message signature and shall verify that the key that is loaded is signed with the appropriate key. The incoming message shall include the new public key data for storage, key identifier, and the signature. The middle layer service that is called by the software is the StorePublicKey service.

Upon successful completion of this service, the key attributes shall be retained. These include:

- Start and end key validity dates
- Key identifier, which is composed of the Revision and key name

4.1.3.11. Load Secret Key[1]

This command from the Host shall cause the PSD to load the signed key record that contains an encrypted secret key. In this state, the PSD shall verify the signature on the incoming message and shall verify that the key that is being loaded is signed with the appropriate key. The incoming message shall include the encrypted secret key for storage, key identifiers, and the signature. The middle layer service that is called by the embedded program is the StoreSecretKey service.

Upon successful completion of data processing by this service, which included decrypting the secret key with the Key Exchange Key and re-encrypting it with the Key Encryption Key for storage, the key attributes shall be retained. These include:

- Start and end dates during which the key is valid.
- Key identifier, which is composed of the Revision and the key name

[1] The Load Secret Key is required for various International Configurations and is not used in the US Postal Implementation.

4.1.3.12. Revoke Key

The revoke key message is a signed message that instructs the PSD to remove a key from the key table.

4.1.4. Keys

4.1.4.1. PSD Key

This public-private key pair is generated by the PSD upon request.

UNIQUE_PSD_AUTH_IBI_DSA1024_PRIVATE

UNIQUE_PSD_AUTH_IBI_DSA1024_PUBLIC

4.1.4.2. Root key

The root key signs the key update key record . The PSD verifies the identity of the crypto officer using the root certificate. This key is used to sign all key records input into the PSD.

DOMAIN_INF_AUTH_ROOT_DSA1024_PUBLIC

4.1.4.3. Key Update Key

The key update key is used to sign all other certificates. The identity of the crypto officer is verified using the key update key certificate .

DOMAIN_INF_AUTH_KEY_UPDATE_DSA1024_PUBLIC

4.1.4.4. Key Exchange Key

The key exchange key is used by external sources to exchange a key with the PSD

UNIQUE_PSD_PRIVACY_KEY_EXCHANGE_RSA1024_PUBLIC

4.1.4.5. Certificate Key

The certificate key is used when key data downloaded to the PSD must be deleted. The identity of the Crypto officer is verified using the certificate Key.

DOMAIN_INF_AUTH_CERTIFICATE_DSA1024_PUBLIC

4.1.4.6. New Key (generic)

The new key is a generic key that is loaded into the PSD and is country or market specific.

4.2.PSD Administrator Role

4.2.1. General Information

The PSD Administrator manages non-key data used to set internal parameters and settings in the PSD.

4.2.2. Acting Individual or Organization

The Postage by Phone system and the Manufacturing Systems are the only individuals who act as the PSD Administrator .

4.2.3. Services

4.2.3.1. Disable PSD

The command shall place the PSD in the Disabled state. No indicia shall be generated and no postage value downloads shall be performed.

4.2.3.2. Enable PSD

This command may transition the PSD from the Disabled state to the Serial Number Locked state. It shall be valid only if no other lockout states are set.

4.2.3.3. Reinitialize PSD

Immediately before this command is issued, the Get Challenge command function must have been executed. When the Host instructs the PSD to reinitialize, the file system shall be cleared. Except for the Key encryption key, software and transport crypto keys, all keys shall be cleared. The PSD shall be placed in the Transport Mode by the command. The command will not be accepted if there are any funds in the PSD.

4.2.4. Keys

4.2.4.1. Certificate Key

The certificate key is used when any non-key data downloaded to the PSD must be signed for verification. The identity of the PSD administrator is verified using the certificate Key certificate .

DOMAIN_INF_AUTH_CERTIFICATE_DSA1024_PUBLIC

4.3.Printhead Administrator Role

4.3.1. General Information

The Printhead Administrator is in charge of downloading information used in conjunction with the Printhead such as postage critical and non-critical graphics bit-maps.

Keys are used to verify downloaded data and to sign messages to the printhead . The PSD verifies the signature on the downloaded data using the appropriate key in order to authenticate that the data came from the printhead administrator.

4.3.2. Acting Individual or Organization

The product line server security coprocessor is the only entity authorized to sign graphics data that will be printed.

4.3.3. Services

4.3.3.1. Verify and Sign Hash

The PSD shall be instructed to verify the signature on the cryptographic hash that is in a signed data record and then to re-sign the hash with the PSD key and output a new SDR. The embedded program call is for the VerifySignature service.

After the verification, the crypto hash shall be re-signed with the PSD private key and then sent back to the Host. The middle layer command program call is the SignData service.

4.3.4. Keys

4.3.4.1. PSD Key

This public-private key pair is used to sign verified graphic hash records for transmission to the printhead..

UNIQUE_PSD_AUTH_IBI_DSA1024_PRIVATE

4.3.4.2. Non Postage Critical Graphic Key

This key is used to verify an incoming non postage critical graphic hash.

DOMAIN_INF_AUTH_CONF_NPCG_DSA1024_PUBLIC

4.3.4.3. Postage Critical Graphics Key

This key is used to verify an incoming postage critical graphic hash.

DOMAIN_INF_AUTH_PCG_DSA1024_PUBLIC

4.4.Financial Officer Role

4.4.1. General Information

Funds transfer into and out of the PSD are the responsibility of the Financial Officer. This corresponds to the “User” role as identified by FIPS 140-1

4.4.2. Acting Individual or Organization

Postage by Phone is the Financial Officer

4.4.3. Services

4.4.3.1. Create Postage Value Refund Request

This command requests a return of funds from the PSD to the PbP account

4.4.3.2. Generate Postage Value Download Request

This command shall initiate a Postage Value Download (PVD) request.

4.4.3.3. Load Postal Configuration Data

For the PSD to load configuration information that is specific for the postal application, it must receive this command. The specific Postal Configuration Data shall be contained in a signed data record (SDR). The data will vary among PCNs. In some configurations, the PSD cannot dispense postage, unless these data items are loaded. Typically, the command will be used immediately prior to the Authorize PSD command.

4.4.3.4. Perform Postage Value Download

To perform a download of postage value (PVD), the Host sends the message to the PSD, which shall verify the signature on the incoming signed data record. The SDR can be an IBI PVD record or it can be an IBI PVD Error record.

4.4.3.5. Perform Postage Value Refund

This command shall be required to complete the postage refunding operation that was started with the Create Postage Value Refund Request command. The PSD shall verify the signature of the included SDR. If the signature and the content of the SDR are valid, then the PSD shall reset the descending register to zero and remain in the lockout state. If the Infrastructure Data Center status orders that the refund be aborted, the PSD shall not reset the descending register to zero and shall exit the lockout state.

4.4.3.6. Prepare Audit Record

At the time that a PSD is manufactured, the Message Definition File shall be created and written with information that is appropriate for a specific country. The PSD shall use the data in this file to prepare a signed Audit Record, in response to this command from the Host. Typical data included will be the PSD Serial Number, ascending register, descending register, control sum, piece count, software version, configuration revision SMR, error data, PSD date and time (local), PSD PCN and the last inspection date.

4.4.3.7. Process Audit Results

The PCN parameter settings shall cause the PSD to clear inspection lockout or to reset the next inspection due date in response to this command. The Prepare Audit Record command must immediately precede this command in order for the PSD to process the signed data record that is returned from the Pitney Bowes Infrastructure Data Center.

4.4.4. Keys

4.4.4.1. PSD Private Key

This key is used to verify PVD and Refund responses

UNIQUE_PSD_AUTH_IBI_DSA1024_PRIVATE

4.4.4.2. PVD Key

The PVD key is used by the infrastructure to sign postage value downloads and audit requests. The identity of the financial officer is verified using the PVD Key certificate .

DOMAIN_INF_AUTH_PVD_DSA1024_PUBLIC

4.5.Customer Role

4.5.1. Acting Individual or Organization

This role performed services that are done on behalf of another role, and require other authorized transactions to occur in conjunction with the service being invoked.

4.5.2. Services

4.5.2.1. Indicium / Debit Services

These services are all done as part of setting up and printing indicas and are done on behalf of the Financial Officer.

4.5.2.1.1. Authenticate to PHC

The PSD shall be instructed by the Host to conduct a joint authentication between itself and the Print Head Controller (PHC).

Either of the two following methods will be accepted by the PSD for PHC authentication

1. The input shall be a nonce word and a signed data record (SDR), which shall include the print head ID, type and mailing machine base Product Code Number (PCN). The DOMAIN_INF_AUTH_VENDOR_DSA1024_PUBLIC key is used by the PSD to authenticate the record.

Or

2. The input shall be the Print Head serial number used as an initial vector in session piece signatures, and a data record, which shall include the print head ID, type and mailing machine base PCN.

4.5.2.1.2. Complete Debit

Completes the update of all information based on the last perform debit request.

4.5.2.1.3. Initialize Printer Session

This instructs the PSD to use the input session seed and generate session keys for the accounting debits that will follow. The PSD shall respond with the SDR for the Session Parameter.

4.5.2.1.4. Non Secure Print Head Id Data

This service is used by the Authenticate to PHC service as part of one of the optional authentication procedures.

4.5.2.1.5. Perform Debit

Based upon the Pre-Debit command, cryptographic functions that were required and that were not computed shall be completed in accordance with the PCN parameter settings. The PSD shall deduct the postage value in the Pre-Debit message from the Descending register and shall update the Ascending Register, Control Sum and Piece Count registers appropriately. These functions shall only be performed in Full Postal state. The indicia record signed with the UNIQUE_PSD_AUTH_IBI_DSA1024_PRIVATE key shall be output.

4.5.2.1.6. Pre Debit

Based upon the PCN parameter setting, the invocation of this command shall cause the required cryptographic calculations to be made in preparation for use in the upcoming accounting debit. Typical data included in the command are Postage Value, Mail Date and Rate Category. However, these are variables that are PCN specific. At the time that the PSD is manufactured, these data items are defined in the Message Definition File. This command shall only function in Full Postal state.

4.5.2.2. Miscellaneous Services

4.5.2.2.1. Get Challenge

The Host shall instruct the PSD to output an eight byte nonce (random number), which shall be used in a subsequent command that requires that nonce word for authentication. This is always done in conjunction with another authorized transaction, and is then considered as being done on behalf of any role that requires a nonce value.

4.5.2.2.2. Toggle Out of Service Lockout

This command shall toggle the PSD to enter or exit its Out of Service Lockout state. This is done on behalf of the PSD Administrator to manage the PSD State.

4.5.3. Keys

4.5.3.1. Key Exchange Key

The key exchange key is used to establish a session - it is assigned to the PSD.

UNIQUE_PSD_PRIVACY_KEY_EXCHANGE_RSA1024_PRIVATE

UNIQUE_PSD_PRIVACY_KEY_EXCHANGE_RSA1024_PUBLIC

4.5.3.2. Vendor Key

DOMAIN_INF_AUTH_VENDOR_DSA1024_PUBLIC

4.5.3.3. Derived Printer Key

This key is used to sign debit records to the PHC.

DOMAIN_PSD_AUTH_DERIVED_PRINTER_3DES2_SECRET

4.5.3.4. PSD Key

a. PSD IBI Private Key: This is a DSA private key used to sign postal indicium and inspection certificates produced by the module.

b. PSD IBI Public Key: This is a DSA public key used to authenticate IBIP messages produced by the PSD.

Key Name	Owning Role
UNIQUE_PSD_AUTH_IBI_DSA1024_PRIVATE	User
UNIQUE_PSD_AUTH_IBI_DSA1024_PUBLIC	User

4.6.No Role User

4.6.1. General Information

Miscellaneous functions that do not require specific authorization because they are permitted to any role are placed in the no role user category.

4.6.2. Acting Individual or Organization

Any individual or organization can invoke these services and get a the expected response.

4.6.3. Services

4.6.3.1. Class Services

4.6.3.1.1. Class Support Request

This message is used to determine whether the postal security device supports a particular class of messages. The General Class Support Request Message provides a more time-efficient means of determining the classes of messages that are supported by the PSD, however this message is more space-efficient.

4.6.3.1.2. General Class Support Request

This message is used to get information from the PSD on all supported Message Classes via a single message.

4.6.3.2. Clock Services

4.6.3.2.1. Get Real Time Clock with Offsets

This command shall cause the PSD to return the value of the real time clock with all of the offsets calculated, including the GMT offset and drift correction.

4.6.3.2.2. Get Real Time Clock Value with No Offsets

This command shall return the PSD real time clock value, with no offsets.

4.6.3.2.3. Get Real Time Clock Offsets

This command shall return the PSD clock offset values.

4.6.3.2.4. Set Clock Drift Correction

The Host shall use this command to set the clock drift correction factor into the PSD. The clock drift may be positive or negative. The factor shall be calculated to the real time clock of the PSD, when the local time is used.

4.6.3.2.5. Set GMT Offset

The user may apply time zone and daylight savings time offsets to produce the Greenwich Mean Time (GMT) offset in the PSD, by using this command from the Host.

4.6.3.3. Diagnostic Services

4.6.3.3.1. Perform Diagnostic Test

The command shall cause the PSD to perform the diagnostic test specified in the message. For example, a command is issued that causes the PSD to perform a cryptographic algorithm test.

4.6.3.3.2. Perform Full Diagnostics

The PSD shall perform its full diagnostic routines when the Host issues this command.

4.6.3.4. File System Services

4.6.3.4.1. Get File Attributes

This message causes the PSD to get and output the attributes from a specified file.

4.6.3.4.2. Read Cyclic File

The message causes the PSD to read and output a specified record from a cyclic file.

4.6.3.4.3. Read Linear File

The message causes the PSD to read and output the next record from a linear file.

4.6.3.4.4. Setup cyclic file for read

This message sets up the parameters for a cyclic file so a specified record can be read.

4.6.3.4.5. Write Cyclic File

This message causes the PSD to write the specified record into a cyclic file.

4.6.3.4.6. Write Linear File

This message causes the PSD to write a record into the end of a linear file.

4.6.3.5. Get Key List

The Get Key List message instructs the PSD to return a list of all active keys stored in the PSD.

4.6.3.6. Modify ACK Timeout Request

This command provides a means of modifying the timeout period, prior to the retransmission of an unacknowledged message.

4.6.3.7. Product Code Number (PCN) Request

This message commands the postal security device to return its PCN.

4.6.3.8. Reboot PSD

This service will cause the psd to be rebooted. The current session is closed by default.

4.6.3.9. Set Unsolicited Message Capability Request

This command can tell the PSD whether or not it can send unsolicited messages.

4.6.3.10. Status Services

4.6.3.10.1. Get PSD Status

Most PSD commands are processed by the PSD when it is in its normal idle state. If the PSD is in a state where a specific command is expected (Process Audit Response, for example), this command is used the PSD to its idle state. The status information shall include:

- PSD Application level
- Hardware status
- Current PSD Mode
- Current PSD internal state

The Control Layer software must have been loaded before this command can be used.

4.6.3.10.2. Get PSD Attributes

The Host requires that the PSD identify itself by its attributes. These may include:

- PSN serial number (Indicia #)
- PSD PCN
- PSD software version

- PSD file system version
- Middle Layer firmware version
- Hardware version
- Comet device serial number (Manufacturing Number)

4.6.3.10.3. Get Middle Layer Attributes

The command shall call the PSD to report the attributes of the Middle Layer. The attributes may include:

- Middle Layer Firmware Version
- Hardware Version
- Comet Device Serial Number

4.6.3.10.4. Get Low Level PSD Status

The Host shall get low level PSD status information with this command. The Control Layer does not have to be loaded for this to be a valid command. The status reported may include:

- Hardware status register
- First time hardware status set
- Last time hardware status set
- Total transport authentication failures
- Successive transport authentication failures
- Control Layer loaded indicator
- Debit cycle counter

4.6.4. Keys

none applicable

5. Algorithms

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

5.1. General

A FIPS compliant pseudo-random number generator is implemented in hardware .

5.2. Hashing Algorithms

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

5.3. Encryption /Decryption

RSA is implemented in software rather than hardware and is used for encryption and decryption during cryptographic key distribution. It is implemented using the PKCS#1 Ver2.1 message encoding method.

DEA is implemented in hardware as is used in the generation of a triple DEA (TDEA) encryption.

OAEP padding is implemented in software for public-key encryption purposes.

Skipjack is used for encrypting and decrypting keys for secure storage.

5.4. Signatures & Signature Verification

DSA is implemented in hardware and is used for signing messages and for signature verification purposes.

TDEA is used for message authentication codes (MAC).

ISO9796 padding is implemented in software for public key signatures

6. Self-Test

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

6.1. MYK82A Internal Self tests

The MYK82A Cryptograph Processor performs internal self tests. These may be invoked by a power on or reset condition, or by the ARM7TDMI processor executing an SWI #0xF00024 instruction (SELFTEST command) under program control.

These tests are performed in ARM7 Supervisor Mode.

6.1.1. SRAM Self test

This test is intended to thoroughly verify correct operation of the MYK82A's internal SRAM.

6.1.2. Multiplier Self test

This test commands the multiplier logic component to perform an A*A (128 x 128 bit) multiply operation, and compares the numerical result with a Known Answer. Results of the SRAM self test are used as the multiplicands, with the Known Answer residing in the SRAM, a copy of the ROM value. In addition to testing the multiplier's #MULT operation, the #SQRFASTMULT logic is run to a known answer. The inclusion of both tests assures the multiplier is fully operational in all modes.

6.1.3. BRAM Self Test

This test is intended to thoroughly verify correct operation of the MYK82A's battery-backed RAM (BRAM). Note that this self test is identical to the SRAM self test except that the contents of BRAM are preserved where SRAM contents are not.

6.1.4. ROM Self-Test

This self test is intended to generate and check a checksum against the contents of the MYK82A's internal Read-Only Memory (ROM).

6.1.5. BRAM Hash Test

This self test performs a hash on the contents of BRAM to verify their authenticity (or that BRAM hasn't yet been programmed, or is corrupt). All except for the final 5 words in the BRAM are hashed using SHA-1. If the 160-bit hash value produced is identical to the final 5 words of BRAM, the test passes. If not, the test fails.

6.2.Middle Layer Verification

A stored signature is used to verify the middle layer code.

6.3.Control Layer Verification

A hash is generated and compared to a stored value to verify that the Control Layer is valid.

6.4. Cryptographic Function Self Tests

After successful completion of the PSD internal self-tests and prior to execution of the first service request the module shall perform the following additional-tests:

- DSS digital signature known answer test (includes a SHA-1 test)
- DES known answer test
- TDES known answer test
- RSA known answer test
- Skipjack known answer test

7. Security Rules

7.1.General

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

- The cryptographic module (CM) shall not output any secret or private key in plaintext form.
- The CM shall not accept any secret or private key in plaintext form.
- The CM shall not process more than one request at a time (i.e. single threaded).
- The cryptographic module shall validate roles as per the following:

Table 2 - Entity Verification Rules

Role	Signature	Algorithm	Hash
Crypto Officer	DSS 1024	DSA	SHA-1
PSD Administrator	DSS 1024	DSA	SHA-1
Printhead Administrator	DSS 1024	DSA	SHA-1
Manufacturing Officer	DSS 1024	DSA	SHA-1
Financial Officer	DSS 1024	DSA	SHA-1
Customer	DSS 1024	DSA	SHA-1

- Signed Digital indicium data shall not be output unless the proper accounting has been performed.
- The cryptographic module shall sign digital indicium data using an USPS approved signature method as defined in the IBIP specifications.

8. Items Protected by the module

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

8.1. Security Relevant Data Items

8.1.1. Definition of SRDIs

The module's stored SRDIs consist of keys and other information necessary to the management of the security protocols. Secret and private keys are stored as ciphertext , public keys are stored in plaintext within the cryptographic module boundary . The keys are:

Table 3 - SRDI List

Key Name	Owning Role	Short Name
DOMAIN_COMET_AUTH_VENDOR_SOFTWARE_DSA1024	Crypto Officer	PDCmtA-VSD
DOMAIN_INF_AUTH_CERTIFICATE_DSA1024_PUBLIC	PSD Administrator	PDInfA-CD
DOMAIN_INF_AUTH_KEY_UPDATE_DSA1024_PUBLIC	Crypto Officer	PDInfA-KUD
DOMAIN_INF_AUTH_PCG_DSA1024_PUBLIC	Printhead Administrator	PDInfA-GCD
DOMAIN_INF_AUTH_PRINTER_TEST_DSA1024_PUBLIC	Printhead Administrator	PDInfA-PrtTD
DOMAIN_INF_AUTH_PSD_SOFTWARE_DSA1024_PUBLIC	PSD Administrator	PDInfA-DSD
DOMAIN_INF_AUTH_PSD_TRANSPORT_DSA1024_PUBLIC	PSD Administrator	PDInfA-PsdTD
DOMAIN_INF_AUTH_PVD_DSA1024_PUBLIC	Financial Officer	PDInfA-PVD
DOMAIN_INF_AUTH_ROOT_DSA1024_PUBLIC	Crypto Officer	PDInfA-RootD
DOMAIN_INF_AUTH_TRUSTED_SOFTWARE_DSA1024_PUBLIC	Crypto Officer	PDInfA-TSD
DOMAIN_INF_AUTH_VENDOR_DSA1024_PUBLIC	Crypto Officer	PDInfA-VD
DOMAIN_INF_CONF_NPCG_DSA1024_PUBLIC	Printhead Administrator	PDInfC-NPcGD
DOMAIN_PSD_AUTH_DERIVED_PRINTER_3DES2_SECRET	Customer	KDPsdA-DPD1
UNIQUE_PSD_AUTH_IBI_DSA1024_PRIVATE	User	P'UPsdA-IBD
UNIQUE_PSD_AUTH_IBI_DSA1024_PUBLIC	User	PUPsdA-IBD
UNIQUE_PSD_PRIVACY_KEY_EXCHANGE_RSA1024_PRIVATE	User	P'UPsdP-KER
UNIQUE_PSD_PRIVACY_KEY_EXCHANGE_RSA1024_PUBLIC	User	PUPsdP-KER
UNIQUE_PSD_PRIVACY_KEY_ENCRYPTION_SKIPJACK_SECRET	Crypto Officer	KUPsdP-KESJ[2]

A 'Real Time Clock' is required and must be capable of being set securely. It is being used to manage time-outs and function suspension and should be considered an SRDI.

GMT Offset is a parameter to determine the relationship between local time and GMT.

Clock Drift Correction is a parameter used to adjust the clock for drift within specified limits.

The PCN is used by manufacturing to determine security protocols for the system, as well as by other systems to determine the correct domain in order to select the correct keys for authorizing specific services..

A special initial vector ‘key’ is provided by the PHC during Authentication to PHC and is used to derive the secret key chain used to encrypt the indicum records.

[2] The Key Encryption Key is stored as plaintext in a BRAM and is zeroized in the event of a detected tamper, or by loss of power to the BRAM. Loss of this key invalidates all private and secret keys in the system because they cannot be decrypted from their stored encrypted condition.

8.1.2. Definition of SRDI Modes of Access

c. Generate PSD Key: This operation generates and stores a new IBIP key pair for a PSD.

d. Authorize PSD Key approves of use of a newly generated IBIP key pair for a PSD.

e. Verify UNIQUE_PSD_AUTH_IBI_DSA1024_PUBLIC Signature : This operation uses UNIQUE_PSD_AUTH_IBI_DSA1024_PUBLIC Key to verify the identity of the PB security administrator (Secure Configuration or Financial Trusted Coprocessor) requesting a service .

f. Verify DOMAIN_INF_AUTH_PCG_DSA1024_PUBLIC Signature : This operation uses DOMAIN_INF_AUTH_PCG_DSA1024_PUBLIC Key to verify the identity of the PB security administrator (Secure Configuration Trusted Coprocessor) requesting a service .

g. Verify DOMAIN_INF_CONF_NPCG_DSA1024_PUBLIC Signature : This operation uses DOMAIN_INF_CONF_NPCG_DSA1024_PUBLIC Key to verify the identity of the PB security administrator (SSPS Graphics System) requesting a service .

h. Decrypt Unique Comet Confidential Key Exchange Key Encrypted Data: This operation uses the Unique Comet Confidential Key Exchange Private Key to decrypt session initialization parameters from the Comet PHC .

i. Generate Key Exchange Key

j. Generate PSD Key

In addition, a certificate can be produced by the module to provide evidence that a debit has occurred or to certify the state of the registers contained in the module. The certificate is produced by a digitally output message using the UNIQUE_PSD_AUTH_IBI_DSA1024_PRIVATE Key.

k. Get Key Exchange Key

l. Get PSD Certificate

m. Get Public Key Data

n. Load Public Key

o. Load Root Key

p. Load Secret Key

q. Verify Key

r. Set Clock Drift Correction

s. Set GMT Offset

t. Set Real Time Clock

u. Get Real Time Clock Offsets

v. Get Real Time Clock Value with No Offsets

w. Get Real Time Clock with Offsets

x. Delete all keys and control layer

8.2. Funds Relevant Data Items

8.2.1. 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. In Comet, all FRDIs are stored in nonvolatile memory in the PSD .

8.2.2. FRDIs Stored in the PSD

a. Indicia Serial Number is the identification number registered with the USPS for the meter license.

b. Ascending Register. This register contains the total amount of funds spent over the lifetime of the module.

c. Descending Register: This register contains the amount of funds currently available in the module.

d. Control Sum. This register contains the total amount of funds credited to the module over the lifetime of the module. The Control Sum must equal the sum of the Ascending Register and the Descending Register values.

e. PSD Piece Count: is the number of indicia plus the number of correction indicia dispensed by the PSD.

8.2.3. Definition of FRDI Modes of Access

1. Get PSD Attributes will return a defined set of attributes based on PCN
2. Get PSD Status will return a defined set of attributes based on PCN
3. Load Postal Config Data is required prior to accessing any of the FRDI's.
4. Perform Debit: This operation uses the PSD IBIP private key to sign an IBIP message from the PSD. This will adjust the descending register, ascending register and piece count.
5. Perform Postage Value download. This will adjust the descending register and the control sum.
6. Perform Postage Value Refund. This will adjust the descending register and the control sum.
7. Prepare Audit Record will prepare the IBI audit information as a message.
8. Process Audit Results
9. Reinitialize PSD will zero out all FRDI's

9. Nomenclature

9.1. Abbreviations

List and expand all abbreviations used in text here.

3DES Triple Data Encryption Standard

ANSI American National Standards Institute

CL Control Layer

CM Cryptographic Module

DEA Data Encryption algorithm

DES Data Encryption Standard

DSA Digital Signature Algorithm

DSS Digital Signature Standards

EFP Environmental Failure Protection

EFT Environmental Failure Testing

EMC Electromagnetic Compatibility

EMI Electromagnetic interference

FIPS Federal Information Processing Standards

FRDI Funds relevant data items

IBI Information Based Indicia

ISO International Standards Organization

MAC Message Authentication Codes

ML Middle Layer

NVM Nonvolatile Memory

OAEP Optimal Asymmetric Encryption Padding

PB Pitney Bowes

PbP Postage by Phone

PCN Product Code Number

PHC Print Head Controller

PKCS Public Key Cryptography Systems

PSD Postal Security Device

PSN Postal Serial Number (Indica Serial Number)

PVD Postage Value Download

RSA Rivest, Shamir , And Aldeman

SDR Signed Data Record

SHA Secure Hash Algorithm

SKR Signed Key Record

SRDI security relevant data items

TDEA Triple Data Encryption Algorithm

UIC User Interface Controller

9.2. Glossary

Key Transaction Processor The Key Transaction Processor or KTP is a master database system that contains and manages key material in encrypted data records. It is the repository for all Meter related Keys at Pitney Bowes and is the start or end point of a large number of secure transactions involving the distribution of keys.

Secure Configuration Trusted Coprocessor The secure box used in conjunction with Postage by Phone for configuration management

Secure Financial Trusted Coprocessor The secure box used in conjunction with Postage by Phone for funds management

Secure Manufacturing Trusted Coprocessor The secure box used in manufacturing a PSD

10.Change History

Table 4 - Change History

Rev	EN	Section	Description	By	Date
A	VAP000001	All	Initial Release	D. Collings	5/8/2001
B	DPP000237	9,13	Removed Proprietary info and Mfg info	D. Collings	7/12/2001
		5	Added Print Controller Role	D. Collings	7/15/01
		12	Clarified Printer Session Derived Key Added Key Name Reference Section	D. Collings	10/29/01
C	DPP000455	4, 6.3	removed references to manufacturing officer	D. Collings	11/12/01
D	DPP000600		Update per comments	D. Collings	12/10/01
E	DPP000671	5.3	Change X9.31 to PKCS#1	D Clark	2/27/2002
F	DPP001125	7	Added	D Collings	8/15/2002
		4.1.4.6	New Key definition	D Collings	8/15/2002
G	DPP001162		No change	D Collings	9/3/2002
H	DPP001201	9.1	Changed ‘Digital’ to ‘Data’ in 3DES,DES,DEA,	D. Collings	9/19/2002
		4.1.3.3	Changed ‘public key for RSA encryption’ to ‘public portion of Key Exchange Key’	D. Collings	9/19/2002
		4.1.3.6	Removed ‘crypto’ from sentance	D. Collings	9/19/2002

11.Index