REV	EN NO.	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
C	DPP000455			D. Collings	11/12/2001
D	DPP000600			D. Collings	10/29/2001
E	DPP000671			D. Collings	2/27/2002
F	DPP001125			D. Collings	8/15/2002
G	DPP001162			D. Collings	9/3/2002
H	DPP001201			D. Collings	9/19/2002
J	DPP0001420		FIPS 140-2 Revision	D. Collings	1/30/2003
P	DPP001509		See Change History Table	D. Collings	3/20/2003
R	CO02438		See Change History Table	D. Crowe	3/18/2004
R.3	CO02438		See Change History Table	D. Crowe	5/11/2005
S	CO06165		Changes requested by NIST	D. Crowe	11/18/2004
T	CO006645	4.4.1, 6.4	Changes requested by NIST	D. Crowe	12/17/2004
U	CO10930	1	Revert to revision R.3, add 1ACT PCN to scope	D. Crowe	2/13/2006

PRODUCT CODE NO.	1A00ABA, 1AECABA, 1A51AAA, 1A0TAAA	**Pitney Bowes**	
APPROVALS			
BY	DATE	TITLE	**CVA Engineering PSD Security Policy**
Robert Tolmie			
Maria Parkos		PREPARED David Collings	DATE 8-May-2001
Tom Athens		CHECKED Catherine Morrisey	DATE 8-May-2001
SHEET 1 OF 25 SHEETS		EN NO. CO10930	DWG NO. VA97004

Table of Contents

1 Module Overview

This document describes the security policy for the Pitney Bowes Compliant Meter (Comet) Postal Security Device (PSD). It is intended to describe the requirements for the PSD and not the entire postage metering system.

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 PSD provides security services to support the creation of digital postage marks that are securely linked to accounting. A PSD provides two types of data protection: secrecy of critical security parameters (CSPs), such as cryptographic keys, and data integrity protection for funds relevant data items (FRDIs) such as accounting data. CSPs and FRDIs reside in the PSD. The Comet PSD cryptographic module consists of a multi-chip standalone module residing within a tamper resistant enclosure. The module provides a logical USB interface.

The module configurations under FIPS 140-2 validation are:

- United States PSD Configurations: 1A00ABA Rev. A, 1A0TAAA Rev. A
- Canadian PSD Configuration: 1AECABA Rev. A, 1ACTAAA Rev A
- German PSD Configuration: 1A51AAA Rev. B

1.1 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 product control numbers (PCN) will be accommodated by downloading different software into the UIC. Similarly, the Comet PSD will be customized in manufacturing to match the specific PCN.

The Comet PSD software is organized into discrete layers as shown in Figure 1 – Logical View of Software Architecture.

The Control Layer (CL) communicates with the Middle Layer (ML) software which provides low-level functions such as cryptographic functions, file management, communications, etc. It communicates with the Comet 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. Both layers co-exist on the same 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 firmware calls the Control Layer firmware to process the message.

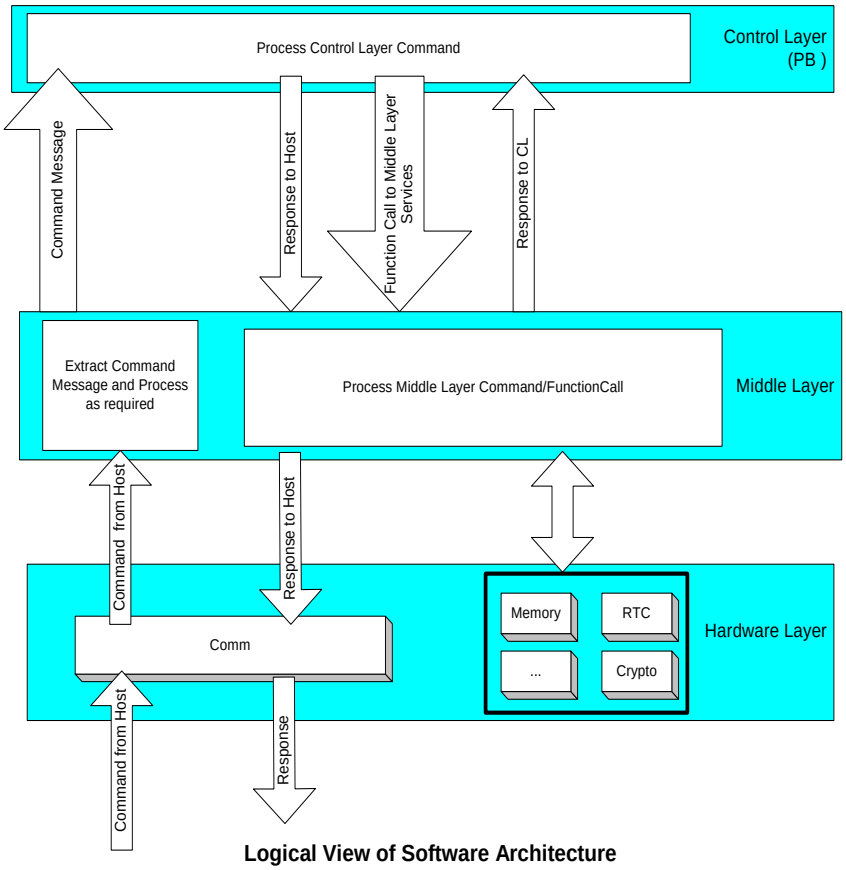

Figure 1 – Logical View of Software Architecture

Figure 2 - Photograph of Physical Configuration

2 Security Level

The Comet PSD cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3 + EFP
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	N/A

Figure 3 - Module Security Level Specification

3 Modes of Operation

The module shall not be designed with a non-FIPS Approved mode of operation. Hence, the module will always be in a FIPS Approved mode of operation.

The module supports the following FIPS Approved algorithms:

- DSA - FIPS 186-2: This algorithm is used to digitally sign and verify signatures.
- ECDSA – FIPS 186-2: This algorithm is used to digitally sign and verify signatures.
- HMAC SHA-1 – FIPS 198
- SHA-1 - FIPS 180-2: This hashing algorithm is used as part of the digital signature process for DSA and ECDSA. This same algorithm is used in the HMAC-SHA-1 algorithm.
- Skipjack – FIPS 46-3: This encryption algorithm is used to protect CSPs that are stored within the cryptographic boundary.

- Triple-DES - FIPS 46-3, FIPS 81: This encryption algorithm is used to encrypt and decrypt other cryptographic keys for secure storage. The module supports TDES ECB and CBC.
- Triple–DES MAC: This algorithm is used to create and verify MACs.
- PRNG per FIPS 186-2, Appendix 3 with SHA-1 based G function

The module supports the following non-FIPS Approved algorithm:

- Diffie-Hellman: This algorithm is used as a key agreement method when establishing session keys between the module and the Infrastructure.
- RSA Decryption: This algorithm is used as a key transport method when establishing secret CSPs between the module and the Infrastructure.

4 Ports and Interfaces

The Comet PSD was designed with a single 12-pin physical edge connector where all power input, data input, data output, control input, and status output interfaces are logically assigned. The edge connector was designed as a logical USB interface.

Pin	Description	Interface Type
1	Not Used	N/A
2	Ground	Power
3	LED	Status Output
4	Ground	Power
5	Not Used	N/A
6	USB Voltage Supply	Power
7	Not Used	N/A
8	I/O	Data Input, Data Output, Control Input, & Status Output
9	LED	Status Output
10	I/O	Data Input, Data Output, Control Input, & Status Output
11	Not Used	N/A
12	Ground	Power

Figure 4 – Interface Table

5 Identification and Authentication Policy

There is no login process for an operator for any role in the Comet PSD design. No role or identity is active other than during the processing of a valid authorized transaction.

Each request sent to the Comet PSD is signed with a particular key. The Comet PSD authenticates the entity by verifying the digital signature with the associated public certificate. Every transaction requires authentication; no transaction is made "available" to a user without authentication per transaction.

Role	Authentication Method	Authentication Type
Crypto-Officer	Digital Signature Verification	Identity-based
PSD Administrator	Digital Signature Verification	Identity-based
Printhead Administrator	Digital Signature Verification	Identity-based
Financial Officer	Digital Signature Verification	Identity-based
Customer	On behalf of the PSD Administrator, Printhead Administrator, or Financial Officer	None

Figure 5 – Roles and Authentication Type

Authentication Mechanism	Strength Mechanism
Digital Signature	Based on number of protected bits in key or signature, the probability is 1 in 2^xB tries where x is the number of protected bits. The digital signature algorithm, with the associated cryptographic key, provides 80 bits of key strength or a probability of random success of 1 in 1,208,925,819,614,630,000,000,000. The module can execute 9.6 transactions per second therefore the probability of a success in a one minute period is 1 in 2,098,829,547,942,060,000,000.

Figure 6 –Authentication Strength

6 Access Control Policy

Each identity and corresponding services are described in the following section.

Crypto-Officer (CO):

The CO is responsible for the high level key management within the box. The primary functions are to load, authorize the generation and use of cryptographic keys into the Comet PSD. The service allocated to this role is as follows:

- Authorize PSD Key: The Authorize PSD Key message shall cause the Comet PSD to complete the Generate PSD Key transaction. This shall place the Comet PSD in Full Postal State. The Authorize PSD Key command shall instruct the Comet 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 Comet PSD shall validate the message header and data content and then shall make the new key active.

The Comet PSD shall also prepare the Authorize PSD record and shall sign it with the unique PSD Authentication Information Based Indicia (IBI) private key.

- Delete All Keys and Control Layer: In response to the Host, the Comet PSD shall zeroize all private and secret keys in the system and shall remove the control layer from the system and place the Comet PSD in Transport Mode.
- Generate Key Exchange Key: This service is configurable to behave in one of the following manners:

  United States Configuration:

  The host shall instruct the Comet 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. This will only be used if secret keys are to be loaded.

  Note: The current US implementation does not load any secret keys.

  Canadian and German Configuration:

  The host shall instruct the Comet PSD to establish a Triple-DES secret key in coordination with the Host via a Diffie-Hellman process. This secret key will be used as a one time Key Exchange Key to load a secret key into the Comet PSD. This key has a deterministic life of 30 minutes from generation before it becomes inactive. It is destroyed immediately upon completion of a Load Secret Key transaction.

  The Diffie-Hellman process and the Triple-DES key being established are both 80 bits in strength.

  This process is based on transmission of a parameter set and a 'public key' from the host followed by the generation of a 'private' key and associated public key and computation (establishment) of the shared secret key by the Comet PSD. The Comet PSD then transmits its 'public' key back to the host so the host can compute the shared secret key.

- Generate PSD Key: The public and private key pair that is the PSD Authentication Key shall be generated by the Comet PSD, when the Host sends this command message. It shall generate either a DSA public/private key set or an ECDSA public/private key set based upon PCN configuration. The message shall include the Signed Key Record (SKR), with parameters to be used. The cryptographic algorithm used by the Comet PSD for IBI is either DSA or ECDSA per configuration data. The Record Type and the Key Name in the SKR shall determine the algorithm to be used. In this state, the Comet 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 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.

- Get Certificate Key: This service shall cause the Comet PSD to output the signed crypto key record that contains the public data included in the specified Certificate key.
- Get Key Exchange Key: In response to this command, the Comet PSD shall output the signed crypto key record that contains the public data included in the PSD Key Exchange Key. If a key exchange key has not been generated, this service will return an error.
- Get PSD Certificate: The Host instructs the Comet 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 Get Public service.
- Get Public Key Data: After the Load Public Key command has been executed, in order to load the public crypto key data into the Comet PSD, the Host shall use this command to retrieve the public key data from the Comet PSD.
- Load Certificate Key: The Load Certificate Key message shall cause the Comet 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.
- Load Public Key: The Comet PSD shall be instructed by the Host to load a public key, which is to be stored in the NVM. In this state, the Comet 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 validity dates
  - Key identifier, which is composed of the Revision and Key Name
- Load Secret Key: This command from the Host shall cause the Comet PSD to load the signed key record that contains an encrypted secret key. In this state, the Comet 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 then re-encrypting it with the Key Encryption Key for storage, the key attributes shall be retained.

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

  The following market-specific applications use the Load Secret Key service:

  - Canadian Configuration: Key Exchange Key
  - German Configuration: Frankit Smeter Key

- US Configuration: None

- Revoke Key: The revoke key message is a signed message that instructs the Comet PSD to remove a key from the key table.

PSD Administrator (PSDA):

The PSD Administrator manages non-key data used to set internal parameters and settings in the Comet PSD. The Postage by Phone system and the Manufacturing Systems are the only individuals who act as the PSD Administrator.

- Disable PSD: This command shall place the Comet PSD in the Disabled state. No indicia shall be generated and no postage value downloads shall be performed.

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

- Reinitialize PSD: Immediately before this command is issued, the Get Challenge command function must have been executed. When the Host instructs the Comet 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 Comet PSD shall be placed in the Transport Mode by the command. The command will not be accepted if there are any funds in the Comet PSD.

Printhead Administrator (PHA):

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.

- Verify and Sign Hash: The Comet 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.

Financial Officer (FO):

Funds transfer into and out of the Comet PSD is the responsibility of the Financial Officer. This corresponds to the “User” role as identified by FIPS 140-2. Postage by Phone is the Financial Officer.

- Create Postage Value Refund Request: Requests a return of funds from the Comet PSD to the PbP account.

- Generate Postage Value Download Request: This command shall initiate a Postage Value Download (PVD) request.

- Load Postal Configuration Data: For the Comet 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.

- Perform Postage Value Download: To perform a download of postage value (PVD), the Host sends the message to the Comet 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.

- 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 Comet PSD shall verify the signature of the included SDR.
- Process Audit Results: The PCN parameter settings shall cause the Comet 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 Comet PSD to process the signed data record that is returned from the PB Infrastructure Data Center.
- Prepare Audit Record: At the time that Comet PSD is manufactured, the Message Definition File shall be created and written with information that is appropriate for a specific country. The Comet PSD shall use the data in this file to prepare a signed Audit Record, in response to this command from the Host.
- Generate Finalizing Franking Record: The Host sends this message to request that the PSD prepare a signed Finalizing Franking Record. This message is valid only for Germany FrankIT and includes a SHA-1 hash with the input data elements according to the FrankIT specification. The Finalizing Franking Record in the Generic Data File must be populated and the Indicia Security Type must be set to Germany FrankIT.

Customer (CU):

This role performs services on behalf of the PSD Administrator, Financial Officer and Printhead Administrator; services allocated to this role require other authorized transactions to occur in conjunction with the service being invoked.

- Indicium / Debit Services: The following messages make up the Indicium/Debit Services:
  - 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 shall be accepted by the PSD for PHC authentication:
    - 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). A DSA1024 signature is used by the PSD to authenticate the record. This record is signed by the infrastructure and the signed data record is installed into the PHC during manufacturing. Verification of the record is done by the PSD.
    - 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.
  - Complete Debit: Completes the update of all information based on the last Perform Debit request. This is done on behalf of the Financial Officer.
  - Initialize Printer Session: Completes the update of all information based on the last perform debit request.

- Print Head Data Input: This service is used by the Authenticate to PHC services as part of one of the optional authentication procedures. The Host sends this message to instruct the PSD to retain the input Print Head ID, nonce, and Base PCN for use in authenticating itself to the PHC and for Printer Session. The input is a nonce, the print head ID and the Base PCN. Authentication is accomplished by including the input nonce in the signed response message. This is done on behalf of the Printhead Administrator.
- 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 Comet 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 in the United States and Germany or the UNIQUE_PSD_AUTH_IBI_ECDSA_FP160_PRIVATE key in Canada shall be output. This is done on behalf of the Financial Officer.
- 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 Comet PSD is manufactured, these data items are defined in the Message Definition File. This command shall only function in Full Postal state. This is done on behalf of the Financial Officer.

- Miscellaneous Services: The following messages make up the Miscellaneous Services:
  - Get Challenge: The Host shall instruct the Comet 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.
  - Toggle Out of Service Lockout: This command shall toggle the Comet 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.

Unauthenticated Services:

Miscellaneous functions that do not require the Comet PSD authentication of the entity; these services are permitted to all roles.

- Class Support Request: Used to determine whether the Comet PSD supports a particular class of messages.
- General Class Support Request: Used to get information from the Comet PSD on all supported message classes via a single message.

- Get Real Time Clock with Offsets: This command shall cause the Comet PSD to return the value of the real time clock with all of the offsets calculated, including the GMT offset and drift correction.
- Get Real Time Clock Value with no Offsets: Returns the real time clock, with no offsets.
- Get Real Time Clock Offsets: Returns the Comet PSD clock offset values.
- Set Clock Drift Correction: The Host shall use this command to set the clock drift correction factor into the Comet PSD.
- Set GMT Offset: The user may apply time zone and daylight savings time offsets to produce the Greenwich Mean Time (GMT) offset in the Comet PSD, by using this command from the Host.
- Perform Diagnostic Test: This command shall cause the Comet PSD to perform the diagnostic test specified in the message.
- Perform Full Diagnostics: The Comet PSD shall perform its full diagnostics routines when the Host issues this command.
- Get File Attributes: Causes the Comet PSD to get and output the attributes from a specified file.
- Read Cyclic File: Causes the Comet PSD to read an output a specified record from a cyclic file.
- Read Linear File: Causes the Comet PSD to read and output the next record from a linear file.
- Setup Cyclic File for Read: Sets up the parameters for a cyclic file so a specified record can be read.
- Write Cyclic File: Causes the Comet PSD to write the specified record into a cyclic file.
- Write Linear File: Causes the Comet PSD to write a record into the end of a linear file.
- Get Key List: Instructs the Comet PSD to return a list of all active keys stored in the Comet PSD.
- Modify ACK Timeout Request: Provides a means of modifying the timeout period, prior to the retransmission of an unacknowledged message.
- Product Code Number (PCN) Request: Commands the postal security device to return its PCN.
- Set Unsolicited Message Capability Request: Tells the Comet PSD whether or not it can send unsolicited message.
- Get PSD Status: The status information shall include:
    - PSD Application Level
    - Hardware Status
    - Current PSD Mode
    - Current PSD internal state

- Debit cycle counter

- Get PSD Attributes: The Host requires that the Comet PSD identify itself by its attributes. This includes:
  - PSN Serial number (Indicia #)
  - PSD PCN
  - PSD software version
  - Middle Layer firmware version
  - Hardware version
  - Comet device serial number (Manufacturing Number)
- Get Middle Layer Attributes: The command shall call the Comet PSD to report the attributes of the Middle Layer, which include:
  - Middle Layer firmware version
  - Hardware version
  - Comet device serial number
- Get ML Error Log: The host device sends this message to the PSD to get the Middle Layer Error Log.
- Get Low Level PSD Status: The Host shall get low level Comet PSD status information with this command, which includes:
  - Hardware status registers
  - 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
- Reboot PSD: This service will cause the current session to be closed, the PSD rebooted, and a new session initialized.

7 Definition of Critical Security Parameters (CSPs)

The following table describes the CSPs contained in the module:

Key	Description
KSPsdP-KECB	TDES 2key CBC session key exchange key Canadian and German Configuration

Key	Description
KUPsdA-IDHM	HMAC SHA-1 key used in Canadian Indicia Canadian Configuration
KUPsdP-KYSJ	Skipjack Key Encryption Key US, Canadian, and German Configuration
P'UpsdP-KER	RSA 1024 Key Exchange Key US Configuration
P'UPsdA-IBD	DSA IBI authorization key that is also used to authenticate the Comet PSD US and German Configuration
P'UPsdA-IBE1	ECDSA IBI authorization key that is also used to authenticate the Comet PSD Canadian Configuration
P'UPsdP-KEDH	DH1024 private component Canadian and German Configuration
P'UpsdP-IDRO	RSA 1024 S_{meter} private key German Configuration
M_{secret}	TDES key used according to the FrankIT specification German Configuration

CSP Table

The following table describes the public keys contained in the module:

Key	Description / Usage
PDInfA-CD	DSA Certificate Authentication
PDInfA-GCD	DSA Postal Critical Graphics Authentication
PDInfA-KUD	DSA Key Update Authentication
PDInfA-PVD	DSA Postage Value Download authentication
PDInfA-RootD	DSA root authentication
PDInfA-VD	DSA vendor authentication
PDInfC-NPcGD	DSA verifying signature on non-postal critical graphics
PUPsdA-IBD	DSA public IBI authorization key
PUPsdA-IBE1	ECDSA public IBI authorization key
PUPsdP-KER	RSA Key Exchange Key
PUPsdP-KEDH	DH1024 public key

Public Key Table

The following table describes the modes of access for each key to each role supported by the module. The modes of access are defined as:

- Zeroize: The Comet PSD zeros the key memory location.
- Generates: The Comet PSD generates the key using the FIPS Approved PRNG.
- Establishes: A key agreement process is used to establish the specified key.
- Load: Inputs the key.
- Decrypt: Decrypts something with the specified key.
- Sign: Signs something with the specified key.
- MAC: Performs a MAC with the specified key.

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
X					Authorize PSD Key	N/A
X					Delete All Keys and Control Layer	Zeroizes all CSPs in Figure 7
X					Generate Key Exchange Key	Generates P'UpsdP-KER Generates P'UpsdP-KEDH Establishes KSPsdP-KECB
X					Generate PSD Key	Generates P'UPsdA-IBD Generates P'UPsdA-IBE1
X					Get Certificate Key	N/A
X					Get Key Exchange Key	N/A
X					Get PSD Certificate	N/A
X					Get Public Key Data	N/A
X					Load Certificate Key	N/A
X					Load Public Key	N/A
X					Load Secret Key	Load KUPsdsA-IDHM Decrypt with KSPsdP-KECB Decrypt with P'UpsdP-KER
X					Revoke Key	N/A
			X		Create Postage Value Refund Request	N/A
			X		Generate Postage Value Download	N/A
			X		Load Postal Configuration Data	N/A
			X		Perform Postage Value Download	Decrypt with P'UpsdP-IDR
			X		Perform Postage Value Refund	N/A
			X		Process Audit Results	N/A

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
			X		Prepare Audit Record	Sign with P'UPsdA-IBD Sign with P'UPsdA-IBE1
			X		Generate Finalizing Franking Record	Hash of M_{secret} Sign with P'UPsdA-IBD
		X			Verify and Sign Hash	Sign with P'UPsdA-IBD
	X				Disable PSD	N/A
	X				Enable PSD	N/A
	X				Reinitialize PSD	N/A
				X	Authenticate to PHC	Sign with P'UpsdA-IBD Sign with P'UpsdA-IBE1
				X	Complete Debit	Sign with P'UPsdA-IBD Sign with P'UPsdA-IBE1
				X	Get Challenge	N/A
				X	Initialize Printer Session	Sign with P'UPsdA-IBD Sign with P'UPsdA-IBE1
				X	Perform Debit	Sign with P'UPsdA-IBD Sign with P'UPsdA-IBE1 MAC with KUPsdA-IDHM
				X	Pre Debit	Sign with P'UPsdA-IBD
				X	Printhead Data Input	N/A
				X	Toggle Service Lockout	N/A
X	X	X	X	X	Class Support Request	N/A
X	X	X	X	X	General Class Support	N/A
X	X	X	X	X	Get File Attributes	N/A
X	X	X	X	X	Get Key List	N/A
X	X	X	X	X	Get Low Level PSD Status	N/A
X	X	X	X	X	Get Middle Layer Attributes	N/A
X	X	X	X	X	Get Middle Layer Error Log	N/A
X	X	X	X	X	Get PSD Attributes	N/A
X	X	X	X	X	Get PSD Status	N/A
X	X	X	X	X	Get Real Time Clock Offsets	N/A
X	X	X	X	X	Get Real Time Clock Value with No Offsets	N/A
X	X	X	X	X	Get Real Time Clock with Offsets	N/A

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
X	X	X	X	X	Modify ACK Timeout Requests	N/A
X	X	X	X	X	PCN Request	N/A
X	X	X	X	X	Perform Diagnostic Test	N/A
X	X	X	X	X	Perform Fully Diagnostics	N/A
X	X	X	X	X	Read Cyclic File	N/A
X	X	X	X	X	Read Linear File	N/A
X	X	X	X	X	Reboot PSD	N/A
X	X	X	X	X	Set Clock Drift Correction	N/A
X	X	X	X	X	Set GMT Offset	N/A
X	X	X	X	X	Set Unsolicited Msg Capability Request	N/A
X	X	X	X	X	Setup Cyclic File for Read	N/A
X	X	X	X	X	Write Cyclic File	N/A
X	X	X	X	X	Write Linear File	N/A

CSP Modes of Access

8 Funds Relevant Data Items

FRDIs are data items whose authenticity and integrity are critical to the protection of postage funds, but which are not CSPs and should not be zeroized. In Comet PSD, all FRDIs are stored in nonvolatile memory in the Comet PSD. FRDIs include:

- Indicia Serial Number is the identification number registered with the USPS for the meter license.
- Ascending Register. This register contains the total amount of funds spent over the lifetime of the module.
- Descending Register: This register contains the amount of funds currently available in the module.
- 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.
- PSD Piece Count: The number of indicia plus the number of correction indicia dispensed by the Comet PSD.

9 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements for the Comet PSD are not applicable because it does not contain a modifiable operational environment.

10 Security Rules

This section documents the security rules enforced by the Comet PSD to implement the security requirements of this FIPS 140-2 Level 3 module.

- The Comet PSD shall not process more than one request at a time (i.e., single threaded). While processing a transaction, prior to returning a response, the Comet PSD will ignore all other inputs to the Comet PSD. No output is performed until the transaction is completed, and the only output is the transaction response.
- The Comet PSD shall validate identities using digital signature.
- All keys generated in the module shall have 80-bits of strength.
- All methods of key generation shall be at least as strong as the key being generated.
- All methods of key establishment shall be at least as strong as the key being established.
- Signed digital indicium data shall not be output unless the proper funds accounting has been performed.
- The Comet PSD shall sign digital indicium data using an approved USPS signature method as defined in the IBIP specification.
- The Comet PSD shall not provide a bypass state where plaintext information is just passed through the module.
- The Comet PSD shall not support a maintenance mode.
- The Comet PSD shall not support a safety state.
- The Comet PSD shall not provide a bypass state where plaintext information is just passed through the module.
- The Comet PSD shall not output any secret or private key in plaintext form.
- The Comet PSD shall not accept any secret or private key in plaintext form.
- There shall be no seed keys entered into the system.
- There shall be no manual entry of keys into the system.
- There shall be no entry or output of split keys from the system.
- There shall be no key archiving.
- Keys shall be either generated or entered into the system through valid processes (i.e., Load Secret Key, etc.).
- Only those keys necessary for the domain specified by the PCN shall be loaded during manufacturing or generated during operation

- The Comet PSD shall support the following conditional tests:
  - Pairwise consistency test for RSA, DSA, and ECDSA key pair generation
  - Continuous RNG test for both the FIPS approved RNG and the non-FIPS approved RNG
- The Comet PSD shall support power up self-tests, which include:
  - MYK82A Internal Self-Tests
    - SRAM
    - Multiplier
    - BRAM
    - ROM
    - BRAM
    - Middle Layer Verification
    - Control Layer Verification
  - DES Known Answer Test
  - TDES Known Answer Test
  - TDESMAC Known Answer Test
  - Skipjack Known Answer Test
  - DSA Sign/Verify Pairwise Consistency Test
  - ECDSA Sign/Verify Pairwise Consistency Test
  - HMAC SHA-1 Known Answer Test
  - RSA Encrypt/Decrypt Known Answer Test
  - RSA Signature Known Answer Test

11 Physical Security Policy

The Comet PSD includes the following physical security mechanisms:

- Upon detecting a tamper event, the Comet PSD shall execute a zeroize activity that completely eliminates its ability to perform any operation requiring authentication.
- Upon detecting a tamper event, the Comet PSD shall abort any transaction in process.
- The module shall protect two types of data items: Funds relevant data items (FRDIs) and critical security parameters (CSPs).

Physical Security Mechanisms	Recommended Frequency of Inspection/Test	Inspection/Test Guidance Details
Tamper Barrier	N/A	Periodic remote data communications
Battery Power	Continuous	Internal SW
Temperature Sensing	N/A	Proof of Design Test, Manufacturing Sampling
Voltage Sensing	N/A	Proof of Design Test, Manufacturing Sampling

Inspection/Testing of Physical Security Mechanisms

12 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks.

13 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, 1996
- Digital Signature Standard (DSA) – FIPS PUB 186-2, January 27, 2000, including change notice of October 5, 2001
- Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems, PCIBI-C, Draft January 12, 1999
- PKCS #1: RSA Encryption Standard version 1.5, November 1, 1993 – More current version available
- Secure Hash Standard – FIPS PUB 180-2, August 26, 2002
- Security Requirements for Cryptographic Modules – FIPS PUB 140-2, Change Notices December 3, 2002

14 Definitions and Acronyms

- Diffie-Hellman: A process where two secure facilities may establish a shared secret key using unsecured communications.
- Key Establishment: There are three methods for the establishment of a key within the Comet PSD. These are 1) internal generation 2) load from external source and 3) Diffie-Hellman process.

- 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 Comet PSD.

15 Acronyms

ANSI	American National Standards Institute
CL	Control Layer
CM	Cryptographic Module
CSP	Critical Security Parameter
DEA	Data Encryption Algorithm
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
DSS	Digital Signature Standards
ECDSA	Elliptic Curve Digital Signature Algorithm
EFP	Environmental Failure Protection
EFT	Environmental Failure Testing
EMC	Electromagnetic Compatibility
EMI	Electromagnetic interference
FIPS	Federal Information Processing Standards
FRDI	Funds Relevant Data Items
HMAC	A hashing algorithm used for message authentication
IBI	Information Based Indicia
ISO	International Standards Organization
MAC	Message Authentication Code
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 (Indicia Serial Number)
PVD	Postage Value Download
RSA	Rivest, Shamir, and Adelman
SDR	Signed Data Record
SHA	Secure Hash Algorithm
SKR	Signed Key Record
TDEA	Triple Data Encryption Algorithm
UIC	User Interface Controller

16 Change History

Change History Table

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	7/15/2001
		12	Clarified Printer Session Derived Key Added Key Name Reference Section	D. Collings	10/29/2001
C	DPP000455	4, 6.3	removed references to manufacturing officer	D. Collings	11/12/2001
D	DPP000600		Update per comments	D. Collings	12/10/2001
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 sentence	D. Collings	9/19/2002
J	DPP001420		Revised to meet FIPS 140-2 Requirements	D Collings	1/30/2003
K	NR		Clarified usage of HMAC	D Collings	2/24/2003
			Clarified usage of Key Exchange Key service	D Collings	2/24/2003
		12.6	Corrected name of VENDOR_SOFTWARE key	D. Collings	3/7/2003
L	NR	Multiple	Corrected based on review by Infogard	D. Collings	3/14/2003

Rev	EN	Section	Description	By	Date
M	NR	6.5	Replaced root key with certificate key Added footnote ref on Certificate Key in 6.5 Added HMAC key to Debit function in table 9 Added index to document	D. Collings	3/17/2003
N	NR	9.1.1	Added RSA KEK to Table	D Collings	3/18/2003
		4.1.4.4	Added RSA Private Key to USA		
		Several	Changed ECDSA160 to ECDSA_FP160		
P	DPP001509		Per Email from Infogard 3/19.2003	D Collings	3/20/2003
R draft1		Several	Per NIST comments Added German Keys and Services	D Collings	12/19/2003
R draft2			Added Germany to Keys/Svcs usage 4.1.3.3, 4.1.3.11, 4.1.4.1, 4.1.4.4, 4.1.4.6, 4.5.2.1.5, Add Get ML Error Log Service not previously listed 4.6.3.4, 9.1.2, 12.2 Change reference to NEW_KEY, now has definition for Germany 4.1.4.6, 9.1 Correct mnemonic for Germany secret key , 9.1, 12.2	D. Crowe	3/4/2004
R	CO02438		Complete restructure to comply with NIST document formatting requirements	D. Crowe	3/8/2004
R.3	CO02438		Update to incorporate NIST comments.	D. Crowe	5/11/2005
S	CO06165	Several	Updates per request of NIST	D. Crowe	11/18/2004
T	CO06645	4.4.1, 6.4	Updates per request of NIST	D. Crowe	12/17/2004
U	CO1930	1	Revert to Rev R, Add TurboJet Configuration 1A0TAAA to list of covered PCNs.	D. Crowe	2/13/2006