REV	EN NO.	SECTION	DESCRIPTION	BY	DATE
A	CO13651	All	Initial Release	J. Steinmetz	Jan 16 2007
B	C014623	1	Add BAE configurations	J. Steinmetz	Feb 9, 2007
C	C015292	1	Add BAF configuration. Corrects ECDSA signature verification.	J. Steinmetz	**Apr 25, 2007**

PRODUCT CODE NO. 1MEC

Pitney Bowes

APPROVALS

BY	DATE

TITLE: Pitney Bowes Cygnus X-2 PSD Security Policy - Canada

PREPARED	J. Steinmetz	DATE	**Jan 16 2007**
CHECKED	D. Clark	DATE	**Jan 16 2007**

SHEET 1 OF 23 SHEETS

EN NO CO15292

DWG NO. 1M00019

Pitney Bowes Inc.

TABLE OF CONTENTS

1 Module Overview

This document describes the security policy for the Pitney Bowes Cygnus X-2 Postal Security Device (PSD). It is intended to describe the requirements for the secure processor only and not the entire system.

Digital postal payment systems, such as the Digital Meter 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 Cygnus X-2 PSD cryptographic module consists of a multi-chip standalone module residing within a tamper resistant enclosure. The module's cryptographic boundary is defined as the metal enclosure surrounding the entire module. The module provides a logical USB interface.

The module configurations under FIPS 140-2 validation are:

- Canada PSD Configurations:

  1MEC BAC, 1MEC BAE, 1MEC BAF

  1MES BAC, 1MES BAE, 1MES BAF (Specimen)

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 Cygnus X-2 PSD will be customized in manufacturing to match the specific PCN.

The Cygnus X-2 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 Cygnus X-2 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.

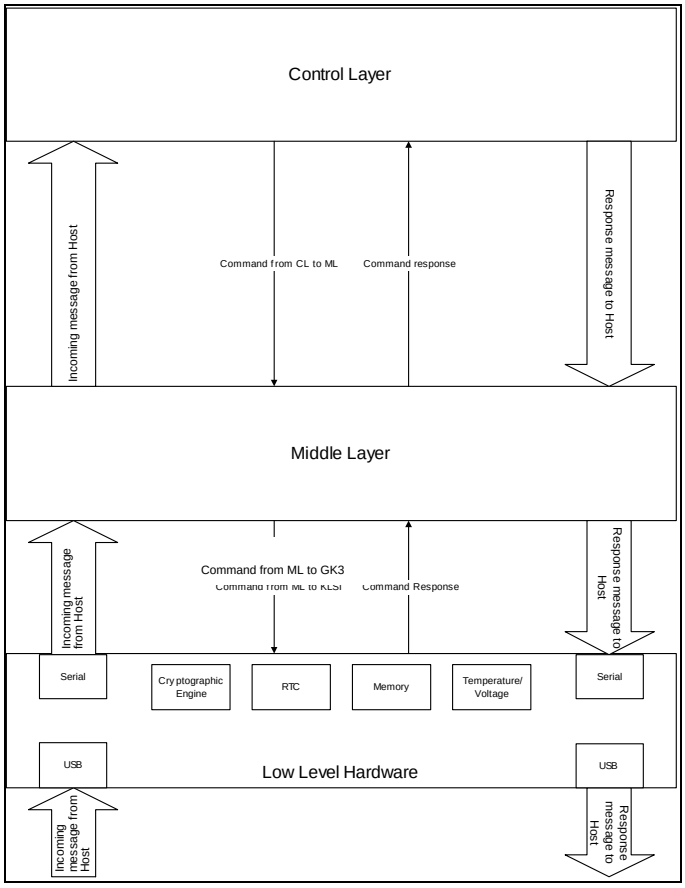

Figure 1 – Logical View of Software Architecture

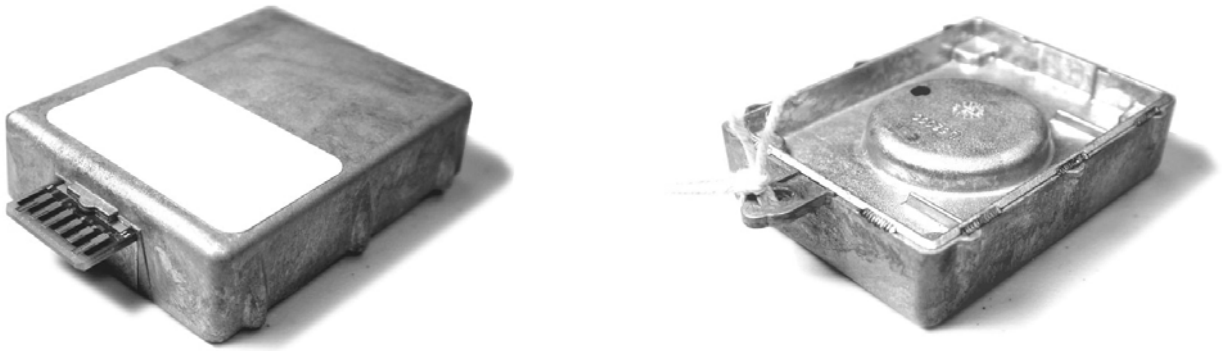

Figure 2 - Photographs of Physical Configuration. The metal enclosure forms the cryptographic boundary.

2 Security Level

The Cygnus X-2 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 contain no 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.

- 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.
- DRNG per FIPS 186-2, Appendix 3 with SHA-1 based G function

The module supports the following non-FIPS Approved algorithm:

- Diffie-Hellman (key agreement; key establishment methodology provides 80 bits of encryption strength): This algorithm is used as a key agreement method when establishing session keys between the module and the Infrastructure. While Diffie-Hellman is not FIPS Approved, it can be used in a FIPS Approved mode of operation.
- Non-Approved RNG: used as a seeding mechanism for the FIPS 186-2 DRNG.

4 Ports and Interfaces

The Cygnus X-2 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 Cygnus X-2 PSD design. No role or identity is active other than during the processing of a valid authorized transaction.

Each request sent to the Cygnus X-2 PSD is signed with a particular key. The Cygnus X-2 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 operator 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 2^80. 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 keys into the Cygnus X-2 PSD and to authorize the generation and use of an IBI key. The services allocated to this role are as follows:

- Authorize PSD Key: The Authorize PSD Key message shall cause the Cygnus X-2 PSD to complete the Generate PSD Key transaction. This shall place the Cygnus X-2 PSD in Full Postal State. The Authorize PSD Key command shall instruct the Cygnus X-2 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 Cygnus X-2 PSD shall validate the message header and data content and then shall make the new key active. The Cygnus X-2 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 Cygnus X-2 PSD shall zeroize all private and secret keys in the system and shall remove the control layer from the system and place the Cygnus X-2 PSD in Transport Mode.
- Generate Key Exchange Key: The host shall instruct the Cygnus X-2 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 Cygnus X-2 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 Cygnus X-2 PSD. The Cygnus X-2 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 Pair shall be generated by the Cygnus X-2 PSD, when the Host sends this command message. It shall generate an ECDSA public/private key set. The message shall include the Signed Key Record (SKR), with parameters to be used. The cryptographic algorithm used by the Cygnus X-2 PSD is ECDSA. In this state, the Cygnus X-2 PSD shall verify the signature on the incoming message. It shall use the middle layer key pair generation algorithm, GenerateKeyPair.

  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 Cygnus X-2 PSD to output the signed crypto key record that contains the public data included in the specified Certificate key.
- Get PSD Certificate: The Host instructs the Cygnus X-2 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 Cygnus X-2 PSD, the Host shall use this command to retrieve the public key data from the Cygnus X-2 PSD.
- Load Certificate Key: The Load Certificate Key message shall cause the Cygnus X-2 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 Cygnus X-2 PSD shall be instructed by the Host to load a public key, which is to be stored in the NVM. In this state, the Cygnus X-2 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.
- Load Secret Key: This command from the Host shall cause the Cygnus X-2 PSD to load the signed key record that contains an encrypted secret key. In this state, the Cygnus X-2 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.

  The HMAC SHA-1 Key is loaded using this transaction.
- Load Secret Key Response: The Load Secret Key Response message is output from the PSD in response to a Load Secret Key message.

  The response from the PSD shall contain signed data generated from the key loaded during the Load Secret Key message. The Host shall verify the signature in the response message to ensure that the key has been properly loaded into the PSD.

- Revoke Key: The revoke key message is a signed message that instructs the Cygnus X-2 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 Cygnus X-2 PSD. The Postage by Phone system and the Manufacturing Systems are the only entities who act as the PSD Administrator.

- Disable PSD: This command shall place the Cygnus X-2 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 Cygnus X-2 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 Cygnus X-2 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 Cygnus X-2 PSD shall be placed in the Transport Mode by the command. The command will not be accepted if there are any funds in the Cygnus X-2 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 Cygnus X-2 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 Cygnus X-2 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 Cygnus X-2 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 Cygnus X-2 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).
- Perform Postage Value Download: To perform a download of postage value (PVD), the Host sends the message to the Cygnus X-2 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 Cygnus X-2 PSD shall verify the signature of the included SDR.
- Process Audit Results: The PCN parameter settings shall cause the Cygnus X-2 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 Cygnus X-2 PSD to process the signed data record that is returned from the PB Infrastructure Data Center.

- Prepare Audit Record: At the time that Cygnus X-2 PSD is manufactured, the Message Definition File shall be created and written with information that is appropriate for a specific country. The Cygnus X-2 PSD shall use the data in this file to prepare a signed Audit Record, in response to this command from the Host.

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.

- Complete Debit: Completes the update of all information based on the last Perform Debit request. This is done on behalf of the Financial Officer.
- Complete Debit With Parameters: Completes the update of all information based on the last Perform Debit request. Then, 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 Cygnus X-2 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.
- Non-Secure Print Head ID Data: This service is used by the Authenticate to PHC services as part of one of the optional authentication procedures. 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 Cygnus X-2 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 is signed with the UNIQUE_PSD_AUTH_IBI_ECDSA_FP160_PRIVATE key. 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 Cygnus X-2 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.
- Get Challenge: The Host shall instruct the Cygnus X-2 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 Cygnus X-2 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 Cygnus X-2 PSD authentication of the entity; Unauthenticated Services are available to all roles, both authenticated and unauthenticated.

- Class Support Request: Used to determine whether the Cygnus X-2 PSD supports a particular class of messages.
- General Class Support Request: Used to get information from the Cygnus X-2 PSD on all supported message classes via a single message.
- Get Real Time Clock with Offsets: This command shall cause the Cygnus X-2 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 Cygnus X-2 PSD clock offset values.
- Set Clock Drift Correction: The Host shall use this command to set the clock drift correction factor into the Cygnus X-2 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 Cygnus X-2 PSD, by using this command from the Host.
- Perform Diagnostic Test: This command shall cause the Cygnus X-2 PSD to perform the diagnostic test specified in the message.
- Perform Full Diagnostics: The Cygnus X-2 PSD shall perform its full diagnostics routines when the Host issues this command.
- Get File Attributes: Causes the Cygnus X-2 PSD to get and output the attributes from a specified file.
- Read Cyclic File: Causes the Cygnus X-2 PSD to read an output a specified record from a cyclic file.
- Read Linear File: Causes the Cygnus X-2 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 Cygnus X-2 PSD to write the specified record into a cyclic file.
- Write Linear File: Causes the Cygnus X-2 PSD to write a record into the end of a linear file.
- Get Key List: Instructs the Cygnus X-2 PSD to return a list of all active keys stored in the Cygnus X-2 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 Cygnus X-2 PSD whether or not it can send unsolicited message.
- Get PSD Status: If the Cygnus X-2 PSD is in a state where a specified command is expected, this command is used by the Cygnus X-2 PSD to its Idle state.
- Get PSD Attributes: The Host requires that the Cygnus X-2 PSD identify itself by its attributes.
- Get Middle Layer Attributes: The command shall call the Cygnus X-2 PSD to report the attributes of the Middle Layer.
- Get Low Level PSD Status: The Host shall get low level Cygnus X-2 PSD status information with this command.
- Get Middle Layer Error Log: Returns the Middle Layer Error/Event log.

7 Definition of Critical Security Parameters (CSPs)

The following table describes the CSPs contained in the module:

Key	Description / Usage	Generation / Agreement	Storage	Entry / Output	Destruction
KUPsdP-KY3DESCBC	TDES 2key Key Encryption Key	Internally by FIPS approved PRNG	Clear text	Entry: N/A Output: N/A	On tamper event and Delete All Keys and Control Layer service
KSPsdP-KECB	TDES 2key CBC session key exchange key	Diffie Hellman process with Infrastructure	Ciphertext	Entry: N/A Output: N/A	Delete All Keys and Control Layer service

Key	Description / Usage	Generation / Agreement	Storage	Entry / Output	Destruction
KUPsdA-IDHM	HMAC SHA-1 key used in Indicia	Externally	Ciphertext	Entry: Encrypted via KSPsdP-KECB Output: N/A	Delete All Keys and Control Layer service
P'UPsdA-IBE1	ECDSA IBI authorization key that is also used to authenticate the Cygnus X-2 PSD	Internally by a FIPS Approved PRNG	Ciphertext	Entry: N/A Output: N/A	Delete All Keys and Control Layer service
P'UPsdP-KEDH	DH1024 private key	Internally by a FIPS Approved PRNG	N/A	Entry: N/A Output: N/A	End of transaction

Figure 7 – CSP Table

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

Key	Description / Usage	Generation / Agreement	Storage	Entry / Output
PDInfA-CD	DSA Certificate Authentication	Externally	Plaintext	Entry: Certificate form Output: Certificate form
PDInfA-GCD	DSA Postal Critical Graphics Authentication	Externally	Plaintext	Entry: Certificate form Output: Certificate form
PDInfA-KUD	DSA Key Update Authentication	Externally	Plaintext	Entry: Certificate form Output: Certificate form
PDInfA-PVD	DSA Postage Value Download authentication	Externally	Plaintext	Entry: Certificate form Output: Certificate form
PDInfA-RootD	DSA root authentication	Externally	Plaintext	Entry: Certificate form Output: Certificate form

Key	Description / Usage	Generation / Agreement	Storage	Entry / Output
PDInfA-VD	DSA vendor authentication	Externally	Plaintext	Entry: Certificate form Output: Certificate form
PDInfC-NPcGD	DSA verifying signature on non-postal critical graphics	Externally	Plaintext	Entry: Certificate form Output: Certificate form
PUPsdA-IBE1	ECDSA public IBI authorization key	Internally	Plaintext	Entry: N/A Output: Certificate form
PUPsdP-KEDH	DH1024 public key	Internally	N/A	Entry: N/A Output: Certificate form

Figure 8 – 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 Cygnus X-2 PSD zeros the key memory location.
- Generates: The Cygnus X-2 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 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-KEDH

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
						Establishes KSPsdP-KECB
X					Generate PSD Key	Generates P'UPsdA-IBE1
X					Get Certificate 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
X					Load Secret Key Response	Sign with P'UPsdA-IBE
X					Revoke Key	N/A
			X		Create Postage Value Refund Request	Sign with P'UPsdA-IBE1
			X		Generate Postage Value Download Request	Sign with P'UPsdA-IBE1
			X		Load Postal Configuration Data	N/A
			X		Perform Postage Value Download	Verify with PDInfA-PVD
			X		Perform Postage Value Refund	N/A
			X		Process Audit Results	N/A
			X		Prepare Audit Record	Sign with P'UPsdA-IBE1
		X			Verify and Sign Hash	Sign with P'UPsdA-IBE1
	X				Disable PSD	N/A
	X				Enable PSD	N/A
	X				Reinitialize PSD	N/A

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
				X	Complete Debit	Sign with P'UPsdA-IBE1
				X	Complete Debit with Parameters	Sign with P'UPsdA-IBE1
				X	Get Challenge	N/A
				X	Perform Debit	Sign with P'UPsdA-IBE1 MAC with KUPsdA-IDHM
				X	Pre Debit	Sign with P'UPsdA-IBE1
				X	Non Secure Printhead ID Data	N/A
				X	Toggle Out of Service Lockout	N/A
X	X	X	X	X	Class Support Request	N/A
X	X	X	X	X	General Class Support Request	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
X	X	X	X	X	Modify ACK Timeout Requests	N/A
X	X	X	X	X	PCN Request	N/A

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
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	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

Figure 9 – 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 Cygnus X-2 PSD, all FRDIs are stored in nonvolatile memory in the Cygnus X-2 PSD. FRDIs include:

- Indicia Serial Number is the identification number associated with 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 Cygnus X-2 PSD.

9 Operational Environment

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

10 Security Rules

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

- The Cygnus X-2 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 Cygnus X-2 PSD will ignore all other inputs to the Cygnus X-2 PSD. No output is performed until the transaction is completed, and the only output is the transaction response.
- The Cygnus X-2 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 Cygnus X-2 PSD shall sign digital indicium data using an approved IPMAR signature method.
- The Cygnus X-2 PSD shall not provide a bypass state where plaintext information is just passed through the module.
- The Cygnus X-2 PSD shall not support a maintenance mode.
- The Cygnus X-2 PSD shall not support a safety state.
- The Cygnus X-2 PSD shall not output any secret or private key in plaintext form.
- The Cygnus X-2 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 via an Approved method 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 Cygnus X-2 PSD shall support the following conditional tests:
  - Pairwise consistency test for ECDSA key pair generation
  - Continuous RNG test for both the FIPS approved RNG and the non-FIPS approved RNG
- The Cygnus X-2 PSD shall support power up self-tests, which include:
  - Software/Firmware Integrity Tests:
    - Middle Layer Verification (SHA-1 and DSA)
    - Control Layer Verification (SHA-1)
  - GK3 Power On Self-Tests (POST) (Critical functions test)
  - Application Code Self-Tests: After successful completion of the GK2S POST and prior to execution of the first service request, the Cygnus X-2 PSD shall perform the following additional tests via the middle layer code in FLASH memory. The tests are listed in order of execution. The tests performed are:
  - Critical functions tests:
    - SRAM Databus Test
    - SRAM Address Bus Test
    - SRAM Pattern Test
    - BRAM pattern test
    - Timer Test
    - RTC Test
  - Cryptographic Algorithm Known Answer Tests:
    - SHA-1 Known Answer Test
    - HMAC SHA-1 Known Answer Test
    - Triple-DES Known Answer Test
    - Triple-DES MAC Known Answer Test
    - DSA Known Answer Test
    - ECDSA Known Answer Test
    - Diffie-Hellman Known Answer Test
    - DRNG Known Answer Test (FIPS 186-2)

11 Physical Security Policy

The Cygnus X-2 PSD includes the following physical security mechanisms:

- Upon detecting a tamper event, the Cygnus X-2 PSD shall execute a zeroize activity that completely eliminates its ability to perform any operation requiring authentication.
- Upon detecting a tamper event, the Cygnus X-2 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

Figure 10 – Inspection/Testing of Physical Security Mechanisms

12 Mitigation of Other Attacks Policy

The module has not been designed to mitigate any specific attacks outside the scope of FIPS 140-2.

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
- International Postage Meter Approval Requirements (IPMAR) - S30 UPU Standard
- Secure Hash Standard – FIPS PUB 180-2, August 26, 2002
- Security Requirements for Cryptographic Modules – FIPS PUB 140-2, Change Notices December 3, 2002

- 1M97002 Cygnus X-2 Multi-Chip PSD Hardware Requirements, Rev A, August 30, 2004. 1L97006 Cygnus PSD Middle Layer / Control Layer Interface Specification, Rev A, October 3, 2003.

14 Definitions

- 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 Cygnus X-2 PSD. These are internal generation, load from external source, and the 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 Cygnus X-2 PSD.

15 Acronyms

3DES	Triple Data Encryption Standard
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
GK3	Gate Keeper 3 SRAM ASIC
HMAC	A hashing algorithm used for message authentication
IPMAR	International Postal Meter Approval Requirements
ISO	International Standards Organization
MAC	Message Authentication Code
ML	Middle Layer
NVM	Nonvolatile Memory
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
SDR	Signed Data Record
SHA	Secure Hash Algorithm
SKR	Signed Key Record
TDEA	Triple Data Encryption Algorithm
UIC	User Interface Controller