REV	EN NO.	SECTION	DESCRIPTION	BY	DATE
A	CO16061	All	Initial Review	D. Clark	20-JUL-07
B	CO16450	All	Initial Release	D. Clark	10-AUG-07
C	CO16786	All	Final Release	D. Clark	01-NOV-07
D	CO17991	All	Updated per CMVP comments	D. Clark	04-APR-08
E	CO18324	Section 6	Clarified wording for Load Certificate Key.	D. Clark	21-MAY-08
F	CO19707	3	Added reference to DH algorithm	D. Clark	19-NOV-08
		7	Added DH1024 public and private key info		
G	CO20652	1	Added reference to PSD Application software version and corrected firmware version number.		
		All	Changed content of page footers		
		Figure 6	Added XKEY and XSEED info	D. Clark	23-MAR-09
		Figure 6	Added reference for Derived Session Key using DH	D. Clark	11-SEP-09

CONFIGURATION CONTROL DOCUMENT CCUXXXXXX REQUIRES CHANGING WHENEVER THIS DOCUMENT IS UPDATED.

PRODUCT CODE NO. 1R00

APPROVALS

BY	DATE

Pitney Bowes

TITLE **Pitney Bowes Cygnus X3 PSD Security Policy – USA**

PREPARED D. Clark DATE 20-JUL-07

CHECKED T. Athens DATE 20-JUL-07

SHEET 1 OF 20 SHEETS

EN NO. CO20652

DWG NO. 1R00022

55019

TABLE OF CONTENTS

1 MODULE OVERVIEW 3
2 SECURITY LEVEL 4
3 MODES OF OPERATION 4
4 PORTS AND INTERFACES 5
5 IDENTIFICATION AND AUTHENTICATION POLICY 6
6 ACCESS CONTROL POLICY 7
7 DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) 11
8 FUNDS RELEVANT DATA ITEMS 16
9 OPERATIONAL ENVIRONMENT 16
10 SECURITY RULES 16
11 PHYSICAL SECURITY POLICY 19
12 MITIGATION OF OTHER ATTACKS POLICY 19
13 REFERENCES 19
14 ACRONYMS 20

1 Module Overview

This document describes the security policy for the Pitney Bowes Cygnus X3 Postal Security Device (PSD) Cryptographic Module (HW:1R84000 Version A, FW:01.00.06, SW:01.05.05).

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 X3 PSD cryptographic module is a single chip module. The module's cryptographic boundary is defined as the package of the secure processor, the Sigma ASIC, designed by Pitney Bowes.

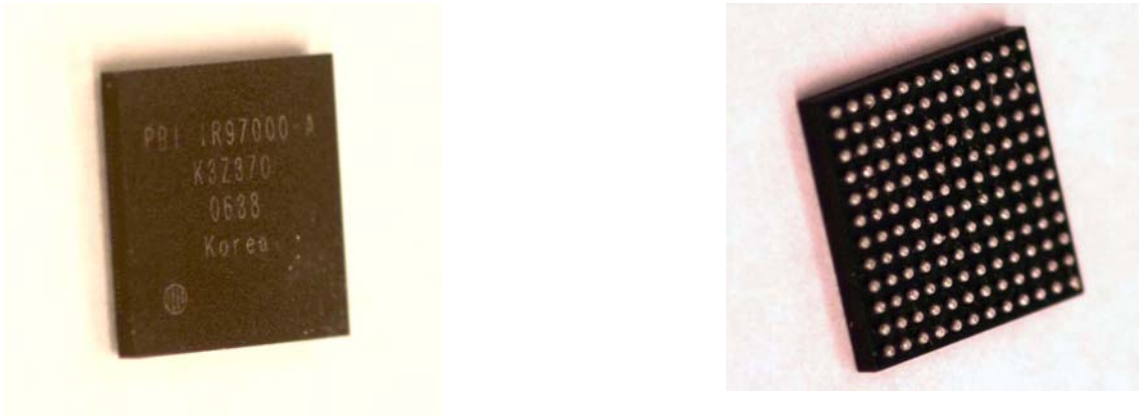

Figure 1 - Cryptographic Module

2 Security Level

The Cygnus X3 PSD ASIC 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 2 - Module Security Level Specification

3 Modes of Operation

The module shall not contain a non-FIPS Approved mode of operation. Hence, the module will only operate 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.
- SHA-1 & SHA-256 - FIPS 180-2: SHA-1 provides the hashing algorithm used as part of the digital signature process for DSA. SHA-256 is used by the module as an EDC for the firmware integrity test.
- AES – FIPS 197: This encryption algorithm is used to encrypt and decrypt other cryptographic keys for secure storage.
- PRNG per FIPS 186-2, Appendix 3 with SHA-1 based G function
- HMAC – HMAC-SHA-1

The module supports the following non-FIPS Approved algorithms:

- Non-Approved RNG: used as a seeding mechanism for the FIPS 186-2 PRNG.

The following algorithms are supported by the cryptographic module, but are not available for use as the module is configured for the current validation:

- ECDSA (Cert. #65)
- Triple-DES – CBC mode; 2-key (Cert. #572)
- RNG – ANSI X9.62 (P-192 and P256) and ANSI X9.31 (TDES 2-key, AES 128-key, AES 192-key, and AES 256-key) (Cert. #342)
- SHA-224 (non-Approved and non-compliant)
- Diffie-Hellman (key agreement) – Used only in a secure factory environment

4 Ports and Interfaces

The Cygnus X3 PSD ASIC is implemented as a 144-pin BGA where all power input, data input, data output, control input, and status output interfaces are supported.

Type	Pin
Data Input	A1, B1, C12, A12
Data Output	A1, B1, D12, A12
Status Output	A1, B1, D1, E1, F2, E12, F11
Control Input	A1, B1, B11, C9, C7, D2, E3, F1, F2, F3, F4, M1, K6, M8, M12, L12, L11, H10, H9, G12, G11, F11, C11
Power	B10, A10, C10, B9, A9, D9, D8, A8, E8, A7, D7, E7, F7, E6, C5, D5, A4, C2, C3, D3, D4, E2, E4, E5, F5, F6, G6, G4, G5, H4, J4, J5, H5, L6, J6, H6, H7, J7, L8, J8, L10, M11, K11, J12, J10, J11, J9, H8, H12, H11, G10, F12, G9, G8, G7, F9, F8, B12
Disabled	A11, B8, C8, B7, C6, A6, B6, D6, A5, B5, B4, C4, B3, A3, B2, A2, G1, G2, G3, H1, H2, H3, J1, J2, J3, K1, K2, L1, M2, L2, M3, L3, K3, M4, L4, K4, M5, L5, K5, M6, M7, L7, K7, K8, L9, M9, K9, K10, M10, K12, F10, E11, E10, D11, E9, D10

Figure 3 – Interface Table

5 Identification and Authentication Policy

There is no login process for an operator for any role in the Cygnus X3 PSD design. No role or identity is active other than during the processing of a valid authorized transaction.
Each request sent to the Cygnus X3 PSD is signed with a particular key. The Cygnus X3 PSD authenticates the entity by verifying the digital signature with the associated public certificate.

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 4 – 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^X 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 2.1 X 10^{21}

Figure 5 –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 X3 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 X3 PSD to complete the Generate PSD Key transaction. This shall place the Cygnus X3 PSD in Full Postal State. The Authorize PSD Key command shall instruct the Cygnus X3 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 X3 PSD shall validate the message header and data content and then shall make the new key active. The Cygnus X3 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 Application: In response to the Host, the Cygnus X3 PSD shall zeroize all private and secret keys in the system and shall remove the PSD Application from the system and place the Cygnus X3 PSD in ROM Firmware Startup State.
- Generate PSD Key: The public and private key pair that is the PSD Authentication Key Pair shall be generated by the Cygnus X3 PSD, when the Host sends this command message. It shall generate a DSA 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 X3 PSD is DSA. In this state, the Cygnus X3 PSD shall verify the signature on the incoming message.
  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 X3 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 X3 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 PSD Application 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 X3 PSD, the Host shall use this command to retrieve the public key data from the Cygnus X3 PSD.
- Load Certificate Key: The Load Certificate Key message shall cause the Cygnus X3 PSD to store the PDInfA-CD public key. The incoming signed message shall be verified prior to taking action on the request.
- Load Public Key: The Cygnus X3 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 X3 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. Upon successful completion of this service, the key attributes shall be retained.
- Revoke Key: The revoke key message is a signed message that instructs the Cygnus X3 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 X3 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 X3 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 X3 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 X3 PSD to reinitialize, the file system shall be cleared. Except for the Key Encryption Key, all keys shall be cleared. The Cygnus X3 PSD shall be placed in the ROM Firmware Startup State by the command. The command will not be accepted if there are any funds in the Cygnus X3 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 X3 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 X3 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 X3 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 X3 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 X3 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 X3 PSD shall verify the signature of the included SDR.
- Process Audit Results: The PCN parameter settings shall cause the Cygnus X3 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 X3 PSD to process the signed data record that is returned from the PB Infrastructure Data Center.
- Prepare Audit Record: At the time that Cygnus X3 PSD is manufactured, the Message Definition File shall be created and written with information that is appropriate for a specific country. The Cygnus X3 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 X3 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 to submit Printer Identification data to the PSD for use in printer session with the Cygnus X3 PSD. 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 X3 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_DSA_1024_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 X3 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 X3 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 X3 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 X3 PSD authentication of the entity; Unauthenticated Services are available to all roles, both authenticated and unauthenticated.

- Get Real Time Clock with Offsets: This command shall cause the Cygnus X3 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 X3 PSD clock offset values.
- Set Clock Drift Correction: The Host shall use this command to set the clock drift correction factor into the Cygnus X3 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 X3 PSD, by using this command from the Host.
- Perform Diagnostic Test: This command shall cause the Cygnus X3 PSD to perform the diagnostic test specified in the message.

- Perform Full Diagnostics: The Cygnus X3 PSD shall perform its full diagnostics routines when the Host issues this command.
- Get File Attributes: Causes the Cygnus X3 PSD to get and output the attributes from a specified file.
- Read Cyclic File: Causes the Cygnus X3 PSD to read an output a specified record from a cyclic file.
- Read Linear File: Causes the Cygnus X3 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 X3 PSD to write the specified record into a cyclic file.
- Write Linear File: Causes the Cygnus X3 PSD to write a record into the end of a linear file.
- Get Key List: Instructs the Cygnus X3 PSD to return a list of all active keys stored in the Cygnus X3 PSD.
- Get PSD Status: If the Cygnus X3 PSD is in a state where a specified command is expected, this command is used to return the Cygnus X3 PSD to its Idle state and provide status.
- Get PSD Attributes: The Host requires that the Cygnus X3 PSD identify itself by its attributes.
- Get Middle Layer Attributes: The command shall call the Cygnus X3 PSD to report the attributes of the ROM firmware
- Get Low Level PSD Status: The Host shall get low level Cygnus X3 PSD status information with this command.
- Get Event Log: Returns the 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-KYA2	AES Key Encryption Key	Internally by FIPS approved PRNG	Clear text	Entry: N/A Output: N/A	On tamper event and Delete All Keys and Application service

Key	Description / Usage	Generation / Agreement	Storage	Entry / Output	Destruction
P'UPsdA-I	DSA IBI authorization key that is also used to authenticate the Cygnus X3 PSD	Internally by a FIPS Approved PRNG	Ciphertext	Entry: N/A Output: N/A	Delete All Keys and Application service
P'UPsdP-KEDH	DH1024 private key	Given e input parameter, generate pseudo-random integer **b** e bits in length. This is the private key. Internally by a FIPS Approved PRNG	N/A	Entry: N/A Output: N/A	End of transaction
KUPsdA-IDHM	HMAC SHA-1 key used in Indicia	Externally	Ciphertext	Entry: N/A Output: N/A	Delete All Keys and Application service
XKEY	Secret Value for the seed-Key in key generation	Xkey is generated internally using method specified in FIPS186-2 Appendix 3.1	N/A	N/A	Wipe to 0 after key generated and wrapped
XSEED	NOT USED	N/A	N/A	N/A	N/A

Figure 6 – 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

Key	Description / Usage	Generation / Agreement	Storage	Entry / Output
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
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-I	DSA public IBI authorization key	Internally	Plaintext	Entry: N/A Output: Certificate form
PUPsdP-KEDH	DH1024 public key	Internally Using previously generated **b** (DH1024 private key), and public parameters g and p that were passed in with generation request, compute $(g^b \bmod p)$ This is the PSDs DH1024 public key.	N/A	Entry: N/A Output: Certificate form

Figure 7 – 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 module zeros the key memory location.
- Generates: The module 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.

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
X					Authorize PSD Key	N/A
X					Delete All Keys and Application	Zeroizes all CSPs in Figure 6
X					Generate PSD Key	Generates P'UPsdA-I, Encrypt with KUPsdP-KYA2
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					Revoke Key	N/A
			X		Create Postage Value Refund Request	Sign with P'UPsdA-I
			X		Generate Postage Value Download Request	Sign with P'UPsdA-I
			X		Load Postal Configuration Data	N/A
			X		Perform Postage Value Download	N/A
			X		Perform Postage Value Refund	N/A
			X		Process Audit Results	N/A
			X		Prepare Audit Record	Sign with P'UPsdA-I
		X			Verify and Sign Hash	Sign with P'UPsdA-I
	X				Disable PSD	N/A
	X				Enable PSD	N/A

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
	X				Reinitialize PSD	N/A
				X	Complete Debit	Sign with P'UPsdA-I; MAC with KUPsdA-IDHM
				X	Complete Debit with Parameters	Sign with P'UPsdA-I MAC with KUPsdA-IDHM
				X	Get Challenge	N/A
				X	Perform Debit	Sign with P'UPsdA-I MAC with KUPsdA-IDHM
				X	Pre Debit	Sign with P'UPsdA-I MAC with KUPsdA-IDHM
				X	Non Secure Printhead ID Data	N/A
				X	Toggle Out of Service Lockout	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 Event 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	Perform Diagnostic Test	N/A
X	X	X	X	X	Perform Full 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	N/A

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
					Correction	
X	X	X	X	X	Set GMT Offset	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 8 – 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. All FRDIs are stored in nonvolatile memory in the module. 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 X3 PSD.

9 Operational Environment

The FIPS 140-2 Area 6 Operational Environment requirements for the module 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 module to implement the security requirements of this FIPS 140-2 Level 3 module.

- The module shall not process more than one request at a time (i.e., single threaded). While processing a transaction, prior to returning a response, the module will ignore all

other inputs to the module. No output is performed until the transaction is completed, and the only output is the transaction response.

- The module shall validate identities using digital signature.
- All keys generated in the module shall have at least 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 module shall not provide a bypass state where plaintext information is just passed through the module.
- The module shall not support a maintenance mode.
- The module shall not support a safety state.
- The module shall not output any secret or private key in plaintext form.
- The module 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.
- Only those keys necessary for the domain specified by the PCN shall be loaded during manufacturing or generated during operation
- The module shall support the following conditional tests:
    - Pairwise consistency test for DSA key pair generation
    - Pairwise consistency test for ECDSA key pair generation
    - Continuous RNG test for both the FIPS approved RNG and the non-FIPS approved RNG

- The module shall support power up self-tests, which include:
    - Software/Firmware Integrity Tests:
        - EDC for PSD Application Verification (SHA-256)
    - Sigma ASIC Power On Self-Tests (POST) (Critical functions test)
    - Application Code Self-Tests: After successful completion of the Sigma ASIC POST and prior to execution of the first service request, the module shall perform the following additional tests via the PSD Application in FLASH memory. The tests performed are:
    - Critical functions tests:
        - RTC Test
    - Cryptographic Algorithm Known Answer Tests:
        - SHA 256 Known Answer Test
        - SHA 224 Known Answer Test
        - SHA-1 Known Answer Test
        - AES Known Answer Test
        - TDES Known Answer Test
        - DSA verification Known Answer Test
        - ECDSA verification Known Answer Test
        - DSA Pairwise consistency
        - ECDSA Pairwise consistency
        - PRNG Known Answer Test (FIPS 186-2)
        - HMAC-SHA-1 Known Answer Test

- Self-tests may be initiated by the following means:
    - Perform Diagnostic Test service
    - Perform Full Diagnostics service

- Physically recycling the module's power

- The status of self-tests shall be available via the Get Low Level Status service.

11 Physical Security Policy

The Cygnus X3 PSD ASIC is a single chip cryptographic module. The module is covered by a hard opaque encapsulant material. Attempts to penetrate the ASIC device packaging has a high probability of causing serious damage to the module.
The module shall protect two types of data items:

- Funds Relevant Data Items (FRDIs)
- Critical Security Parameters (CSPs).

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:

- 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
- 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
- 1R00023 Cygnus X3 PSD Hardware Requirements, Rev B, May 22, 2007.

14 Acronyms

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
CM	Cryptographic Module
CSP	Critical Security Parameter
DSA	Digital Signature Algorithm
DSS	Digital Signature Standards
EFP	Environmental Failure Protection
EMC	Electromagnetic Compatibility
EMI	Electromagnetic interference
FIPS	Federal Information Processing Standards
FRDI	Funds Relevant Data Items
IPMAR	International Postal Meter Approval Requirements
ISO	International Standards Organization
NVM	Nonvolatile Memory
PB	Pitney Bowes
PCN	Product Code Number
PHC	Print Head Controller
PSD	Postal Security Device
PVD	Postage Value Download
SDR	Signed Data Record
SHA	Secure Hash Algorithm
SKR	Signed Key Record
TDEA	Triple Data Encryption Algorithm
TDES	Triple Data Encryption Standard
UIC	User Interface Controller

*** End of Document ***