REV	EN NO.	SECTION	DESCRIPTION	BY	DATE
1		All	Initial Review	R. Sisson	07-Apr--09
2		All	After initial comments from IG	R.Sisson	14-Apr-09
3		All	Changes to make consistent with other submission docs	R. Sisson	22-Apr-09
4		All	Changes to clarify BOM and Self Tests	R. Sisson	11-May-09
A			BOM changes, self tests (again), official doc number Changes from IG	R. Sisson	17-Jun-09
B		Algorithms, self test	Updated to reflect algorithm cert changes and self test updates	R. Sisson	28-Jul-09
C	CO22125	Section 1, sheet 3	Updated SWDL and PSD App. version numbers. Corrected pre-release REV numbers to reflect CM protocol and added CO number, this page.	R. Sisson	01-Oct-09
D	CO23067	Section 8 Section 1	Updated CSP zeroization information per CMVP. Updated PSD Application version to 03.00.0059.	R. Sisson	09-Mar-10
E	CO23068	Section 1	Updated PSD Application version to 03.00.0064.	R. Sisson	09-Mar-10

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

PRODUCT CODE NO. 1Wxx		**Pitney Bowes**	
APPROVALS			
BY	DATE	TITLE	**Pitney Bowes Cygnus X3 Rev 3 Public Security Policy – USA**
		PREPARED R. Sisson	DATE 12-May-09
		CHECKED T. Athens	DATE 12-May-09
SHEET 1 OF 25 SHEETS		EN NO. CO22125	DWG NO. MW97140

TABLE OF CONTENTS

1 Module Overview

This document describes the security policy for the Pitney Bowes Cygnus X3 Postal Security Device (PSD) Cryptographic Module

Item	Version
Hardware	1R84000 Version A
Firmware	01.00.06
Software Download Utility	01.00.0053
PSD Application	03.00.0064

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.

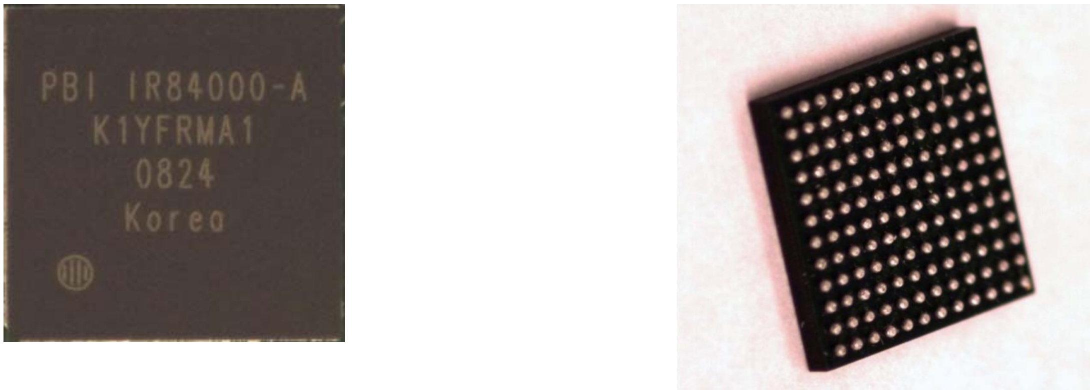

Figure 1 - Cryptographic Module

2 Security Level

The Cygnus X3 PSD 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:

Algorithm	Cert ID	Usage
DSA - FIPS 186-3	374	This algorithm is used to digitally sign and verify signatures
ECDSA – FIPS 186-3	Vendor Affirmed	This algorithm is used to digitally sign and verify signatures
SHA-1 & SHA-256 FIPS 180-3	650	SHA-1 provides the hashing algorithm used as part of the digital signature process for DSA and ECDSA and in the generation of SHA-1 HMAC. SHA-256 provides the hashing algorithm used as part of the digital signature process for ECDSA and in the generation of SHA-1 HMAC is used by the module as an EDC for the firmware integrity test.
AES – FIPS 197	1069	This encryption algorithm is used to encrypt and decrypt other cryptographic keys for secure storage.

Algorithm	Cert ID	Usage
Triple-DES CBC	572	
Triple-DES MAC	572, vendor affirmed	
Hash DRBG – SP 800-90	20	Random Bit Generator
Elliptic Curve Diffie-Hellman – SP 800 56A	3	Key Agreement Protocol - Ephemeral Unified Model C(2, 0, ECC CDH)Elliptic Curve Diffie-Hellman
HMAC-SHA-1 and HMAC-SHA-256 – FIPS 198	601	Used to generated Message Authentication Codes

The module supports the following non-FIPS Approved algorithms:

- AES Key Wrap per the AES Key Wrap Specification (AES Cert. #1069, key wrapping; key establishment methodology provides 128 bits of encryption strength): Used to encrypt symmetric and private keys loaded into the PSD.

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

- RSA PKCS 1.5 for key wrap – provides 80 bits of security
- AES MAC (AES Cert. #600, non-compliant)
- SHA-224 (non-Approved and non-compliant)

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,

Type	Pin
	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
Printing Administrator	Digital Signature Verification	Identity-based
Financial Officer (User)	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. External entities are authenticated using digital signatures based on the ECDSA P256 curve. This provides 128 bits of key strength or a probability of random success in 1 in 2^128.The module can execute 17.85 ECDSA P256 Signature Verifications per second therefore the probability of a success in a one minute period is 1 in 3.2 X 10^{35}

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 a Debit and Operation Keys. The services allocated to this role are as follows:
.

- Generate PSD Key: The Crypto Officer sends this block to instruct the PSD to generate a Public/Private key pair that is the PSD Authentication Operation Key OR the PSD Authentication Debit Key. The message contains a Signed Parameter Record with the parameters for use in the generation of the private and public key values. The cryptographic algorithm supported for use as the PSD Authentication Operation Key is ECDSA. The cryptographic algorithms supported for use as the PSD Authentication Debit Key is DSA or ECDSA. The algorithm used is determined by the Key Descriptor in the Signed Parameter Record and is based on postal requirements.
- Load Certificate Key: The Crypto Officer sends this certificate to instruct the PSD to load the Domain CMT Auth Certificate Key from the host or PB Infrastructure systems in a certificate signed by the Domain CMT Auth Vendor ECDSA P256 Key. The key is to be stored in the NVM for later use in verification of signed records.The PSD shall receive the Load Certificate Key message and then validate the message header and data content. If accepted as valid, the PSD shall verify the Domain Auth CMT Certificate Key Certificate with the Domain CMT Auth Vendor Key. If valid, PSD shall store the Domain CMT Auth Certificate Key. The Domain CMT Auth Certificate Key is an ECDSA P256 Key. Otherwise an error message shall be generated

- Load Vendor Key: The Crypto Officer sends this certificate to instruct the PSD to load the Domain CMT Vendor Key from the host or PB Infrastructure systems in a certificate signed by the Domain Comet Auth Sigma Mfg ECDSA P256 Key. The key is to be stored in the NVM for later use in verification of signed records.The PSD shall receive the Load Vendor Key message and then validate the message header and data content. If accepted as valid, the PSD shall verify the Domain Auth CMT Vendor Key Certificate with the Domain Comet Auth Sigma Mfg Key. If valid, PSD shall store the Domain CMT Auth Vendor Key. Otherwise an error message shall be generated The Domain CMT Auth Vendor Key is an ECDSA P256 Key.

- Load CRL: The Crypto Officer sends this message to request the PSD to store the Certificate Revocation List and the CRL version if needed and store the list in internal memory. The CRL is a signed structure, signed by the Domain CMT Auth Vendor Key. The version of the CRL must be greater than or equal to any previously loaded otherwise an error will be reported and the PSD will be disabled. The version number of the currently loaded PSD is recorded in Flash memory for future comparison. Once the PSD is out of Manufacturing state, it will require that a CRL be loaded. Prior to loading a CRL, all functions requiring cryptographic operations other than Load CRL will be blocked. Any public key identified by the CRL will be blocked from use in the PSD.

- Load Encrypted Key: The Crypto Officer sends this certificate to instruct the PSD to load a signed key record containing an encrypted symmetric or private key. The following keys can be loaded with the Load Encrypted Key command:
  - P'UPsdA-Dbt
  - $P'_{UPsdP\text{-}Dbt}$
  - $K_{UPsdA\text{-}DBT}$

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.

- Load Parameters: The PSD Administrator sends this block to load either functional parameters or data parameters to the PSD. The parameter blocks are signed by the Domain CMT Auth Certificate Key If the PSD is in the operational state, the first parameter in the parameter block must be the challenge value from the most recent "Get Challenge" command to the PSD.

  Supported functional parameters are:

  - Transition to Operational State: The Transition to Operational State_parameter shall cause the Cygnus X3 PSD to transition to operational state. This shall place the Cygnus X3 PSD in Operational State. This is available only in the Manufacturing state.
  - .Transition to Base State: Triggers event to transition the device from Manufacturing state to Base state. Should only be sent to PSD after all parameters required for sign on with the Data Center have been successfully loaded. This is available only in the Manufacturing state.
  - 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: Causes PSD to erase all NVM data except for HW Mfg Data and 'persistent' data (total device cycles, reinit count) and then invalidates the PSD App. Used in the remanufacturing process, or to 'clean' the PSD to retry configuration from scratch. This command zeroizes the Unique PSD Key Encryption Key which results in the loss of all other Private and Secret Keys.

  - Transaction Start: Triggers event to have the PSD prepare for a multi-message transaction that must be completed successfully as a unit (atomic transaction). This means that if any one of the messages within the transaction fails, all messages must be rolled back.

    Not all messages sent after start of a transaction are processed to allow commit/rollback. The messages that are handled in the transaction are PVD (one occurrence), Load Parameters (only data parameters), Load Encrypted Key, and Generate PSD Key.
  - Transaction Commit: Triggers event to 'commit' the updates made by PVD, Load Parameters, Load Encrypted Key, and / or Generate PSD Key made after the Transaction Start event was processed.

  - Transaction Rollback: Triggers event to rollback (cancel) the updates made by PVD, Load Parameters, Load Encrypted Key, and / or Generate PSD Key made after the Transaction Start event was processed.

- Process Flex Debit Block: The PSD Administrator sends this block to load flex debit templates into the PSD. The flex debit template defines the indicia content for subsequent debit operations. The flex debit template is signed by the Domain CMT Auth Certificate Key.

- Generate Session Key: The PSD Administrator sends this block to instruct the PSD to generate a key via Elliptic Curve Diffie-Hellman Key Agreement procedure that will be used for either:

    Infrastructure session, where the generated key will be used once for wrapping a secret/private key to be loaded into the PSD via Load Key Request

    Printer session where the generated key will be used for applying a MAC to all PSD responses for authentication by the 'printer'

    The message contains a Key Block with the initiator public key including EC-DH key parameters signed by the Domain CMT Auth Certificate Key for generating the responder private key and deriving the shared secret key . The response contains the data required for the device doing the key Agreement to compute the shared key.

    If a printer session is required (Communication Authentication Type parameter value is 1) then the PSD will restrict the same functions that are blocked prior to loading the CRL, with the exception of Generate Session Key to allow session to be initiated, and Load Parameters to allow session requirement to be toggled.

- Start Software Update: Triggers event to invalidate the current loaded PSD App and jump to the Software Update Utility entry point to allow start of SW download with new PSD

Application. The Allow SW Updates – this parameter must be set to TRUE before this command can be executed.

Software Update is described in section 7.1Software Update

Printing Administrator (PHA):

The Printing Administrator is in charge of downloading information used in conjunction with the Printing such as images and page layouts.

- Verify Hash Block: The Printing Administrator sends these blocks to instruct the PSD to verify a CMT binary SHA 256 Hash Block.

  The PSD shall receive the CMT Download Certificate and CMT Binary Hash Block and then validate the message header and data content. If accepted as valid, the PSD shall verify the CMT Download Certificate with the Domain CMT Auth Vendor Key. If valid, the PSD will extract the Domain CMT Auth Download key from the download certificate. This key will be used in verifying the input CMT Binary Hash Block. Otherwise, an error message is returned.

  The PSD shall validate the message header and data content of the I_BLK_CMT_BIN_HASH_BLK binary hash block. If accepted as valid, the PSD shall verify the CMT Binary Hash Block with the Domain CMT Auth Download Key that was previously loaded. Otherwise, an error message is returned

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.

- Process Postage Value Download Block: The Funds Officer sends this block to perform a postage value download operation. The PSD will validate the message header and data content and verify the signature of the CMT PVD Response Block with the Domain CMT Authentication Certificate Key.

- Withdraw Request: The Funds Officer sends this message to request the PSD prepare to perform a Withdrawal operation. The PSD will enter a locked state (Withdrawal Pending) that will not permit any debit or credit operations. The PSD creates a Withdraw Request block containging the PSD’s register values. The PSD signs the Withdraw Request block with the Unique PSD Operational Key. The only way to exit the locked state is by the Data Center aborting the withdraw operation in the Withdraw Request

- Process Withdraw Response: The Funds Officer sends this message to complete the withdraw process. The postage is removed from the PSD upon receiving the CMT Withdraw Response Block. This block is signed to verify the integrity and authenticity of the content using the Domain CMT Auth Certificate Key

  The PSD shall receive the message, and then validate the message header and data content. If accepted as valid, the PSD shall verify the CMT Withdraw Response Block. If valid, the PSD will remove the funds from the funds registers and set the state to the Withdrawn State. If the Data Center status indicates that the refund is to be aborted, the PSD will not reset the descending register and will exit the withdraw pending state and return to Operational State if no other lockout conditions exist. If any other Data Center error is indicated, the PSD will remain in the Withdraw Pending state.

- Prepare Audit Record: The Funds Officer sends this command to request that the PSD prepare a signed Audit Request Block. The Audit Request Block contains the PSD register values and real time clock value. The record is signed by the Unique PSD Operational Key and sent to the Financial Officer

- Process Audit Response: .The Funds Officer sends this commandto the PSD so that it may process the CMT Audit Response Block returned from the Pitney Bowes infrastructure in response to the immediate previous Audit Request command. The CMT PSD shall verify the signature of the CMT Audit Response Block with the Domain CMT Auth Certificate Key.

  Depending on PCN parameter settings, this command may cause clearing of the inspection lockout or the resetting of the next inspection due date.

  The PSD shall use clock offset correction to update its clock drift correction parameter

- Generate Finalizing Franking Record: The Funds Officer sends this command to request that the PSD prepare a signed Finalizing Franking Record. This message is valid only for Germany FrankIt and includes a hash implemented according the FrankIt specification. The IndiciaSecurityType parameter must be set to Germany FrankIt. Data items include Indicia Serial Number, ascending register, descending register, piece count, and other defined data items.

Customer (CU):

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

- Precompute r for Debit: The Host sends this message to the PSD to have it pre-compute the ‘r’ signature component for the PSD Auth Key signature (DSA or ECDSA). This message is used for countries whose debit certificate is signed by a DSA or ECDSA key.
- Create Debit Certificate: The Host sends this message to the PSD to have it create a debit certificate in the format defined by the Flex Debit Certificate Template. Input to this command is defined by the Flex Debit Templates.

  The data included in this command is dependent on the country requirements. Typical data includes Debit Value, Mail Date and Data Capture Recovery Data. The definitions of the data input and output by the Debit command is provided in the Flex Debit Templates that are loaded by the host device on each power up or when debit certificate format is updated.

Based on PCN parameter settings, invocation of this command will cause required cryptographic calculations to create the debit certificate. This command will return an error if input data is out of allowable ranges and if Origin Postal Code is NULL, indicating that the postal code data was never set.This is done on behalf of the Financial Officer.

- Finalize Debit: The Host sends this message to have the PSD perform post-debit housekeeping and prepare for the next Debit operation by precomputing the ‘r’ signature parameter if necessary

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 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.
- Get Key List: Instructs the PSD to return a list of all active keys stored in the PSD.
- Set Clock: The Host sends this command to setup the real time clock in the PSD. The real time clock can only be programmed when the PSD is in manufacturing state. It cannot be changed once the PSD is ‘locked’. It is assumed that the clock is set to GMT.
- Get Clock Offsets: Returns the Cygnus PSD clock offset values
- Get Local Time: This command shall cause the Cygnus PSD to return the value of the real time clock with all of the offsets calculated, including the GMT offset and drift correction.
- Get GMT Time: Returns the clock value with the drift correction added (GMT Time if clock is set correctly).
- Set GMT Offset: The Host sends this command to set the GMT offset in the PSD. The GMT offset is a combination of offsets (daylight savings time offset, time zone offset, etc.) that need to be set by the customer.
- Get Parameters: The Host sends this message to the PSD to retrieve parameter values from the PSD. The Host can request individual parameter IDs or all of the Parameters in the PSD.
- Perform Full Diagnostics: The Host device sends this command to the PSD to request the PSD perform its diagnostic processing. The PSD will run its power up tests as well perform other maintenance activities.
- Perform Diagnostic Test: The Host sends this message to request that the Cygnus PSD perform a diagnostic test.
- Read Log File: The Host device sends this message to the PSD to get Log Data. The number of available entries, the size of each entry, and the data contained in each entry will depend on the log that is being requested.

- Get PSD Status: If The Host device sends this message to the PSD to request PSD status information. Included in the status information is the PSD Application status word (32 bits), the HW Status word (32 bits), current PSD State (16 bits) and the current PSD internal state (16 bits).

  The Get PSD Status command is also used to invoke transition of the PSD state from a state where a specific message is expected (i.e. Process Audit Response) to the normal idle state where most PSD commands are processed.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 PSD to request its attribute data.
- Reboot: The Host sends this command to reboot the PSD application.

7 Software Update Access Control Policy

The PSD supports a secure software update process. In order to achieve this, a new layer in the PSD application was created. The purpose of this layer is to update the PSD application in a safe manner. This layer is referred to as the Software Update Utility.

7.1 PSD Software Update

1. The Start Software Update event triggers the software update process. This event instructs the PSD to start the Software Download Utility. PSD Software applications are loaded in chunks. Each chunk is signed by the Domain CMT Software Key (ECDSA 256). In addition a record containing a signed SHA 256 Hash of the entire application is verified by the PSD prior to accepting the new application. This record is also signed by the Domain CMT Software Key. Only FIPS 140-2 validated software shall be loaded. Loading of non-validated software will invalidate the validation.

The Software Download Utility supports the following messages:

PSD Administrator (PSDA):

- Setup Download Data: The Host sends this signed record to make the Software Download Utility aware of the parameters of the software (application) to be downloaded. This message is signed by the the Domain CMT Auth PSD Software Key. Receipt of this message triggers a transition to the state required to load chunk information. The Setup Download Data message is only valid if the SDU is idle and waiting to begin a download.
- Setup Download Chunk: The Host sends this signed record to make the Software Download Utility aware of the parameters of the software (application) chunk to be sent in the following message. Receipt of this message triggers a transition to the state required to load the chunk. The Setup Download Chunk message is only valid if the SDU has received a valid Setup Download Data message.
- Download Chunk: This message contains the data referenced in the Setup Download Chunk message.

Utility Functions
The following utility functions are unauthenticated and intended to aid the host application in managing the software update process.

- Get PSD Attributes: This function is invoked using the same command ID as the PSD Application. It returns a 'PSD Attributes' response message with all fields set to '0' except for the SDU Version, which is set appropriately, and the HW Version Number (PB SMR) and Device Serial Number which are retrieved from the Manufacturing Data written by the HW manufacturer. The structure and memory location of the Manufacturing Data is defined in 1R00024 Manufacturing Specification: Cygnus X-3 Memory Contents (refer to mfgdata.h in PSD Application project for structure used to parse the Manufacturing Data).

- Reboot: This function is invoked using the same command ID as the PSD Application. It returns a 'Reboot' response message, waits for xx milliseconds, then resets the ASIC. This functionality should be ported from the PSD Application.

- Remove SDU: This function is invoked by sending the command ID for 'Remove SDU' to the device. The SDU writes 0's to the Validity Flag, sends a response message, waits milliseconds and resets the ASIC. The PSD transitions to the ROM Firmware State after completion of this message.

- Get PSD Status: The Host device sends this message to the PSD to request PSD status information. Included in the status information is the PSD Application status word (32 bits), the HW Status word (32 bits), current PSD State (16 bits) and the current PSD internal state (16 bits).

8 Definition of Critical Security Parameters (CSPs)

The following table describes the CSPs contained in the module:

Key	Key Name	Description / Usage	Generation / Agreement	Storage	Entry / Output	Destruction
KUPsdP-KYA2	Unique PSD Key Encryption Key	AES Key Encryption Key	Internally by FIPS approved DRBG	Clear text	Entry: N/A Output: N/A	Zeroized on Tamper or Reinitialize or removal of all power
$P'_{UPsdA\text{-}Dbt}$	Unique PSD Auth Debit Private Key	ECDSA or DSA key used sign debit records	Internally by a FIPS Approved DRBG	Ciphertext	Entry: N/A Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power

Key	Key Name	Description / Usage	Generation / Agreement	Storage	Entry / Output	Destruction
$K_{UPsdA\text{-}DBT}$	Unique PSD Auth Debit Secret Key	AES, TDES, HMAC key used to generate Message Authentication codes on debit Records	External	Ciphertext	Entry: Encrypted using AES Key Wrap Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power
$P'_{UPSDA\text{-}Op}$	Unique PSD Auth Operational Private Key	ECDSA keys used to communicate with the infrastructure	Internally by a FIPS Approved DRBG	Ciphertext	Entry: N/A Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power
$P'_{UPSDP\text{-}Dbt}$	Unique PSD Privacy Debit Key	RSA keys used to wrap postal generated debit keys	External	Ciphertext	Entry: Encrypted using AES Key Wrap Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power
$K_{UPSDP\text{-}Dbt}$	Unique PSD Privacy Debit Key	TDES key used to encrypt postal security related parameters to the PSD	External	Ciphertext	Entry: Encrypted using AES Key Wrap Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power
$K_{SPSDA\text{-}Prt}$	Session PSD Auth Printer Key	HMAC Key used to authenticate messages sent to the system controller	Key Agreement per SP 800-56A	Plaintext	Entry: N/A Output: N/A	End of session
$K_{USPDP\text{-}Op}$	Session PSD Privacy Operation Key	AES Key used to encrypt secret or private key data sent from the infrastructure	Key Agreement per SP 800-56A	Plaintext	Entry: N/A Output: N/A	End of session
$P'_{UCMTKA\text{-}Op}$	Unique CMT Key Agreement Operation Key	ECDH key used in SP 800-56A key agreement dialog with the Infrastructure	Internally by a FIPS Approved DRBG	Plaintext	Entry: N/A Output: N/A	End of session
V	DRBG Seed	DRBG seed	Entered in factory environment	Ciphertext	Entry: N/A Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power

Figure 6 – CSP Table

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

Key	Key Name	Description / Usage	Generation / Agreement	Storage	Entry / Output
$P_{DCmtA\text{-}SigMfg}$	Domain Comet Authentication Sigma Manufacturing Key	ECDSA used to validate Software Download Utility and Vendor Certificate	Externally	Plaintext	Entry: Hard Coded in ASIC ROM Output: N/A
$P_{DCMTA\text{-}C}$	Domain CMT Authentication Certificate Key	ECDSA used to validate Authority Data	Externally	Plaintext	Entry: Certificate form Output: N/A
$P_{DCMTA\text{-}Dl}$	Domain CMT Authentication Download Key	ECDSA used to validate data blocks for the Trusted Printer from the infrastructure	Externally	Plaintext	Entry: Certificate form Output: N/A
$P_{DCMTA\text{-}PsdS}$	Domain CMT Authentication PSD Software Key	ECDSA key used to validate PSD application Software	Externally	Plaintext	Entry: Embedded with CMT PSD Software Update Utility form Output: N/A
$P_{DCMTA\text{-}V}$	Domain CMT Authentication Vendor Key	ECDSA vendor authentication	Externally	Plaintext	Entry: Certificate form Output: N/A
$P_{UCMTKA\text{-}B}$	Unique CMT Key Agreement Base Key	ECDH Key used in key agreement between the Base an PSD	Externally	Plaintext	Entry: Certificate form Output: N/A
$P_{UCMTKA\text{-}Op}$	Unique CMT Key Agreement Operation Key	ECDH Key used in Key Agreement between Infrastructure and PSD	Externally	Plaintext	Entry: Certificate Form Output: N/A
$P_{UPsdA\text{-}Dbt}$	Unique PSD Auth Debit Key	ECDSA or DSA key used sign debit records	Internally by a FIPS Approved DRBG	Ciphertext	Entry: N/A Output: Certificate Form
$P_{UPSDA\text{-}Op}$	Unique PSD Auth Operational Key	ECDSA keys used to communicate with the infrastructure	Internally by a FIPS Approved DRBG	Ciphertext	Entry: N/A Output: Certificate Form
$P_{UCMTKA\text{-}Op}$	Unique CMT Key Agreement Operation Key	ECDH key used in SP 800-56A key agreement dialog with the Infrastructure	Internally by a FIPS Approved DRBG	Plaintext	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 DRBG.
- 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.
- Revokes: Revokes a key based on identifiers in the CRL.

Roles					**Services**	**CSP Modes of Access**
CO	**PSDA**	**PHA**	**FO**	**CU**		
X					Generate PSD Key	Generates $P'_{UPsdA-Op}$ and $P'_{UPsdA-Dbt}$ corresponding public key is output signed by current version of $P'_{UPsdA-Op}$ P'UPsdA-I, Encrypt with KUPsdP-KYA2
X					Load CRL	Revokes the key(s) identified in the CRL
X					Load Vendor Key	N/A
X					Load Certificate Key	N/A
X					Load Encrypted Key	Loads the encrypted secret or private key
			X		Withdraw Request	Sign with $P'_{UPSDA-Op}$
			X		Process Postage Value Download Block	N/A
			X		Process Withdraw Response:	N/A
			X		Process Audit Response	N/A
			X		Prepare Audit Record	Sign with $P'_{UPSDA-Op}$
			X		Generate Finalizing Franking Record	N/A
		X			Verify Hash Block	N/A
	X				Load Parameters	N/A
	X				Process Flex	N/A

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
					Debit Block	
	X				Disable PSD	N/A
	X				Enable PSD	N/A
	X				Reinitialize PSD	Zeroizes Secret and Private key data
	X				Transition to Base State	This is available only in the Manufacturing state.
	X				Transition to Operational State	This is available only in the Manufacturing state.
	X				Transaction Start	
	X				Transaction Commit	
	X				Transaction Rollback	
	X				Generate Session Key	
	X				Start Software Update	N/A
	X				Setup Download Data	N/A
	X				Setup Download Chunk	N/A
	X				Download Chunk	
X	X	X	X	X	Remove SDU	N/A
				X	Precompute r for Debit	N/A
				X	Create Debit Certificate	Sign with $P'_{UPsdA\text{-}Dbt}$
				X	Finalize Debit	N/A
X	X	X	X	X	Get Challenge	N/A
X	X	X	X	X	Get Key List	N/A
X	X	X	X	X	Get Parameters	N/A
X	X	X	X	X	Reboot	N/A
X	X	X	X	X	Get PSD Attributes	N/A

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
X	X	X	X	X	Get PSD Status	N/A
X	X	X	X	X	Set Clock	N/A
X	X	X	X	X	Get Clock Offsets	N/A
X	X	X	X	X	Get GMT Time	N/A
X	X	X	X	X	Get Local Time	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 Log File	N/A
X	X	X	X	X	Set GMT Offset	N/A

Figure 8 – CSP Modes of Access

9 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.
- Zero Piece Count: The number of indicia containing zero for the postage value.

10 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.

11 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 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
- Once a module has been zeroized, it must be returned to the factory for software loading and parameterizing prior to being usable by a customer.
- 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 the DBRG – Stuck Seed, Stuck Number
    - ECDSA Known Answer Test – Signature Verification prior to Software Load Test

    - ECDSA Public Key Validation as part of SP 800-56A Key Agreement Protocol
- The module shall support power up self-tests, which include:
    - Software/Firmware Integrity Tests:
        - EDC for firmware, PSD Application Verification and SW Download Utility (SHA-256)
    - Sigma ASIC Power On Self-Tests (POST) (Critical functions test)
        - TDES Known Answer Test
        - DSA Verification Known Answer Test
        - ECDSA Verification Known Answer Test
        - SHA-1 Known Answer Test
        - SHA-256 Known Answer Test
        - SHA-224
        - AES Engine Known Answer Test (128, 192, 256)
        - Crypto Engine 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
        - Sigma ASIC POST
    - Cryptographic Algorithm Known Answer Tests:
        - DSA Pairwise Consistency Test
        - ECDSA Pairwise consistency
        - AES Key Wrap / Unwrap Known Answer Test
        - AES Encrypt / Decrypt Known Answer Test
        - AES CBC MAC Known Answer Test
        - HMAC SHA-1 Known Answer Test
        - HMAC SHA-256 Known Answer Test
        - KAS SP800-56A (C(2, 0, ECC CDH)) Known Answer Test
        - HASH DRBG SP800-90 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.

12 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).

13 Mitigation of Other Attacks Policy

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

14 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
- Digital Signature Standard (DSA) – FIPS PUB 186-3, November 2008
- Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems, PCIBI-C, Draft January 12, 1999
- Advanced Encryption Standard (AES) FIPS PUB 197, November 26, 2001
- Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, December 2001.
- Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Special Publication 800-67, May 2004.
- The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198, March 06, 2002

- Recommendation for Random Number Generation Using Deterministic Random Bit Generators (Revised), Special Publication 800-90, March 2007.
- AES Key Wrap Specification, November 2001
- International Postage Meter Approval Requirements (IPMAR) - S30 UPU Standard
- Secure Hash Standard – FIPS PUB 180-3, October 2008
- NIST SP 800-56A, Recommendation for Pair-Wise Key Establishment SchemesUsing Discrete Logarithm Cryptography – March 2007
- 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.

15 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
EC-DH	Elliptic Curve Diffie Hellman
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 ***