


REV	EN NO.	SECTION	DESCRIPTION	BY	DATE
A		All	Initial Review	J.Hurd	10-Nov-14
B		All	Updates from submission review	B. Hannigan	2-Dec-14
C		1, 3, 4, 5	Update from CMVP comments	B. Hannigan	20-May-15
D		3, 9	Update from CMVP comments	B. Hannigan	1-Sept-15
E		All	Update to fix typos, minor errors	B. Hannigan	10-Apr-18

PRODUCT CODE NO. 4W00		 <b>Pitney Bowes, Inc.</b>
APPROVALS		
BY	DATE	TITLE <b>MS1 X4 PSD Security Device (PSD) Policy</b>
		PREPARED J. Hurd DATE 10-Apr-18
		CHECKED B. Hannigan DATE
<b>SHEET 1 OF 27 SHEETS</b>		EN NO. DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.		
55019		

## TABLE OF CONTENTS

1	MODULE OVERVIEW .....	3
2	SECURITY LEVEL.....	4
3	MODES OF OPERATION .....	5
	3.1 FIPS MODE INDICATOR.....	6
4	PORTS AND INTERFACES .....	7
5	IDENTIFICATION AND AUTHENTICATION POLICY .....	7
6	ACCESS CONTROL POLICY .....	9
7	SOFTWARE UPDATE ACCESS CONTROL POLICY .....	15
	7.1 PSD SOFTWARE UPDATE.....	15
8	DEFINITION OF CRITICAL SECURITY PARAMETERS (CSPS) .....	16
9	FUNDS RELEVANT DATA ITEMS.....	22
10	OPERATIONAL ENVIRONMENT .....	22
11	SECURITY RULES .....	23
12	PHYSICAL SECURITY POLICY.....	25
13	MITIGATION OF OTHER ATTACKS POLICY .....	25
14	REFERENCES.....	25
15	ACRONYMS .....	27

<b>SHEET 2</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

# 1 Module Overview

This document describes the Security Policy for the Pitney Bowes MS1 X4 Postal Security Device (PSD) Cryptographic Module created by Pitney Bowes, Inc.

**Table 1 – Pitney Bowes X4 MS1 Postal Security Device (PSD) components**

Item	Version
Pitney Bowes MS1 X4 Postal Security Device Cryptographic Module	Part # 4W84001 Rev AAA
Hardware: MAX32590 Secure Microcontroller	Revision B4
Firmware components:	
Device Abstraction Layer (DAL)	01.01.00F4
PRNG Library	01.01.0009
AES Library	01.01.0008
ECDSA Library	01.01.000A
DSA Library	01.01.000A
HMAC Library	01.01.0008
DESMAC Library	01.01.0008
KAS Library	01.01.0008
DH Library	01.01.0008
RSA Library	01.01.000C
Hash Library	01.01.0008
Common Crypto Library	01.01.000A
Bootloader Interface Library	00.00.000C
PB Bootloader	00.00.0016
PSD Application	21.04.007E

Digital postal payment systems, such as the Digital Meter Program, rely on secure accounting of postage funds and printing a cryptographic digital postage evidence mark on a mail piece in the form of an indicium. 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

<b>SHEET 3</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

relevant data items (FRDIs) such as accounting data. CSPs and FRDIs reside inside the physical protections of the PSD.

The MS1 X4 PSD is defined as a single chip cryptographic module

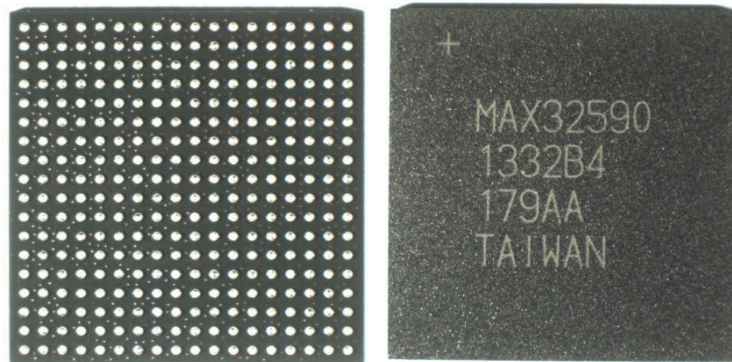


Figure 1 - MAX32590 Secure Processor

The MS1 X4 PSD’s cryptographic boundary is defined as the package that comprises the Maxim Integrated MAX32590 secure microcontroller. PB executable code is stored in external memory and copied to internal SRAM to be executed. On each power-up the firmware components listed in Table 1 are authenticated via digital signatures and then copied to internal SRAM for execution:

1. The ROM Bootloader validates the PB Bootloader using RSA-PSS 2048 signature verification. The RSA-PSS 2048 SigVer function part of the ROM Bootloader has been validated (Cert. #1539).
2. Once the PB Bootloader has been authenticated, the PB Bootloader bootstraps and authenticates the Device Abstraction Layer (DAL) and its firmware components using an ECDSA P-256 with SHA-256 signature verification. The ECDSA P-256 SigVer function part of the PB Bootloader has been validated (Cert. #529).

## 2 Security Level

The MS1 X4 PSD cryptographic module meets the overall requirements applicable to Level 3 security of FIPS 140-2.

Table 2 - Module Security Level Specification

Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3

<b>SHEET 4</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
----------------	----------	-----------------------	-----------	------------

© Copyright 2018 Pitney Bowes, Inc.  
 May be reproduced only in its original entirety (without revision) including this copyright notice.

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

### 3 Modes of Operation

The PSD uses FIPS approved algorithms contained in the DAL. The DAL module supports the following FIPS Approved algorithms:

**Table 3 – Approved Algorithms**

Algorithm	Usage
FIPS 197 AES (Cert. #2826)	Used to encrypt data output from the module and decrypt data input into the module. Key sizes supported are 128 bits and 256 bits.
SP 800-38F AES Key Wrapping (KTS) (Cert #2936)	Used to protect secret data. Key sizes supported are 128 bits and 256 bits.
FIPS 186-4 CVL (Cert. #254)	ECDSA component for signature generation.
SP 800-90A DRBG (Cert. #487)	Hash-Based Deterministic Random Bit Generator using SHA-256.
FIPS 186-4 DSA (Cert. #871)	Used to generate cryptographic key pairs, generation of digital signatures and digital signature verification for L=2048, N=256 & SHA-256.  Also, supports legacy systems when used to verify signatures for L=1024, N=160 & SHA-1.
FIPS 186-4 ECDSA (Cert. #529)	Used to generate cryptographic key pairs, generation of digital signatures and digital signature verification for P-256 curves (SHA-256). Cryptographic key pair generation per FIPS 186-4 Section B.4.2.  Also, supports legacy systems when used to verify signatures for P-192 curves (SHA-1).
HMAC (Cert. #1769)	Used to generate HMAC-SHA-1 and HMAC-SHA-256 Message Authentication Codes. Minimum key size is 160 bit.
KAS (Cert. #49)	Key Agreement Protocol used to establish a session key (Ephemeral Unified Model C (2, 0, ECC CDH))

<b>SHEET 5</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

FIPS 186-4 RSA (Cert #1539)	Used for key generation, digital signature generation and encryption (key encapsulation) with key size of 2048.  Also, supports legacy systems when used to verify signatures for key size = 1024.
SHS (Cert. #2369)	SHA-1 provides the hashing algorithm used as part of the digital signature verification process for DSA and ECDSA. It is also used in the generation of HMAC-SHA-1 message authentication codes.  SHA-256 provides the hashing algorithm used as part of the digital signature process for RSA, DSA and ECDSA and in the generation of HMAC SHA-256 message authentication codes.
Triple-DES (Cert. #1690)	Legacy encryption support 2-key Triple-DES and 3-key Triple-DES keys. Life of the module is designed to perform fewer than 2 <sup>20</sup> blocks of data encryption.
Triple-DES MAC (Cert. #1690, vendor affirmed)	Legacy SP 800-57 Part 1 (Revision 3) message authentication.

The module supports the following non-Approved but Allowed security functions:

**Table 4 – Non-Approved but Allowed Security Functions**

Diffie Hellman	Key establishment methodology provides 112 bits of security using 2048 bit keys
NDRNG	The hardware RNG is used to initially seed the Approved DRBG

The module supports the following non-Approved security functions while operating in non-FIPS mode:

**Table 5 - Non-Approved Security Functions**

Diffie Hellman (non-compliant)	Key Agreement Protocol used to establish a session key. Key agreement using 1024 bit keys
DSA (non-compliant)	This algorithm is used to generate key pairs and generate signatures for L=1024, N=160 & SHA-1.
ECDSA (non-compliant)	This algorithm is used to generate key pairs, digital signatures for P-160 (SHA-1) and P-192 (SHA-1) curves.
RSA (non-compliant)	This algorithm is used to digitally sign using schemes PKCS 1.5, X9.31 and PSS, PKCS 1 version 2.1 for 1024 bit modulus using SHA-1.

### 3.1 FIPS Mode Indicator

The module supports a single mode of operation in which the module alternates service by service between Approved and non-Approved modes of operation. When the module executes the services not relying on cryptographic functions or relying on Approved algorithms it is said to operate in an Approved mode of operation. Corollary, when the services relying on non-Approved algorithms are executed, the module is said to operate in a non-Approved mode of operation.

<b>SHEET 6</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

The MS1 X4 PSD has a Non Fips Mode Parameter that can be set via a Load Parameters message. If the non-FIPS Mode Parameters is set, the most significant bit of the status word in each message response is set, reflecting that the MS1 X4 PSD is operating in a non-FIPS Mode.

## 4 Ports and Interfaces

The MAX32590 is supplied in a 324-pin BGA package where all power input, data input, data output, control input, and status output interfaces are supported.

		<i>Ball Grid Array Pin Horizontal from "x"</i>																	
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
<i>Ball Grid Array Pin Vertical from "y"</i>	<b>A</b>	-	-	-	-	-	-	O	-	-	-	-	-	-	-	-	-	-	-
	<b>B</b>	-	-	-	-	-	-	I	-	-	-	-	-	-	-	-	-	-	-
	<b>C</b>	-	-	P	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	<b>D</b>	-	-	P	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	<b>E</b>	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-
	<b>F</b>	-	-	-	-	-	P	P	P	P	P	P	P	P	IO	IO	-	-	-
	<b>G</b>	-	-	-	-	S	P	-	-	-	-	-	P	C	-	-	-	-	-
	<b>H</b>	-	-	-	-	P	P	-	-	-	-	-	P	S	-	-	-	-	-
	<b>J</b>	-	-	-	-	C	P	-	-	-	-	-	P	C	-	-	-	-	-
	<b>K</b>	-	-	-	-	C	P	-	-	-	-	-	P	C	-	-	-	-	-
	<b>L</b>	-	-	-	-	-	P	-	-	-	-	-	P	-	-	-	-	-	-
	<b>M</b>	-	-	-	S	-	P	-	-	-	-	-	P	-	-	-	-	-	-
	<b>N</b>	-	-	-	-	-	P	P	P	P	P	P	P	-	S	-	-	S	S
	<b>P</b>	-	-	-	O	-	O	O	O	O	O	O	-	O	O	O	O	O	O
	<b>R</b>	-	-	-	-	-	-	-	-	-	IO	IO	IO	IO	O	O	O	O	O
	<b>T</b>	-	-	-	-	-	-	-	-	-	IO	IO	IO	IO	-	O	O	O	O
	<b>U</b>	-	-	-	-	-	-	-	-	-	IO	IO	IO	IO	-	-	O	O	O
	<b>V</b>	-	-	-	-	-	-	-	-	-	IO	IO	IO	IO	-	-	O	O	O

I = Data In      O = Data Out      S = Status Out      C = Control In      P = Power      - = Disabled

Figure 2 – Interface Mapping

## 5 Identification and Authentication Policy

There is no traditional login process for an operator for any role in the MS1 X4 PSD design. No role or identity is active other than during the processing of a valid authorized transaction. Each request sent to the MS1 X4 PSD is digitally signed with a particular key. The MS1 X4 PSD authenticates the entity by verifying the digital signature with the associated public certificate.

<b>SHEET 7</b>	REV <b>E</b>	REV DATE <b>17-Apr-18</b>	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

**Table 6 - Roles and Authentication Type**

<b>Role</b>	<b>Authentication Method</b>	<b>Authentication Type</b>
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

**Table 7 - Authentication Strength**

<b>Authentication Mechanism</b>	<b>Strength of Mechanism</b>
Digital Signature	<p>Based on number of protected bits in the key or signature, the probability is 1 in <math>2^x</math> tries, where x is the number of protected bits and thus, less than 1 in 1,000,000.</p> <p>External entities are authenticated using digital signatures based on the ECDSA P-256 curve. This provides 128 bits of key strength or a probability of random success in 1 in <math>2^{128}</math>. The module can execute 17.85 ECDSA P-256 Signature Verifications per second therefore the probability of a success in a one minute period is 1 in <math>3.2 \times 10^{35}</math> which is less than 1/100,000.</p>

<b>SHEET 8</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
----------------	----------	-----------------------	-----------	------------

© Copyright 2018 Pitney Bowes, Inc.  
 May be reproduced only in its original entirety (without revision) including this copyright notice.



## 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 PSD. The primary functions are to load keys into the MS1 X4 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 and ECDSA. The algorithm used is determined by the Key Descriptor in the Signed Parameter Record and is based on postal requirements.
- **Load PRNG Seed:** The Crypto Officer sends this block to instruct the PSD initialize the Pseudo Random Bit Generator. The PSD shall retrieve data from the TRNG to create the DRBG-V, Key Encryption Key, Key Authentication Key and DRBG-WS.
- **Load Certificate Key:** The Crypto Officer sends this certificate to instruct the PSD to load the Domain MS1 Auth Certificate Key from the host or PB Infrastructure systems in a certificate signed by the Domain MS1 Auth Vendor ECDSA P-256 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 MS1 Certificate Key Certificate with the Domain MS1 Authentication Vendor Key. If valid, the PSD shall store the Domain MS1 Auth Certificate Key. The Domain MS1 Auth Certificate Key is an ECDSA P-256 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 MS1 Vendor Key from the host or PB Infrastructure systems in a certificate signed by the Domain Comet Auth Sigma Mfg ECDSA FP256 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 MS1 Vendor Key Certificate with the Domain Comet Auth Sigma Mfg Key. If valid, PSD shall store the Domain MS1 Authentication Vendor Key. Otherwise an error message shall be generated. The Domain MS1 Authentication Vendor Key is an ECDSA P-256 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 MS1 Authentication Vendor Key. The version of

<b>SHEET 9</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

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-Dbt
  - KUPsdA-Dbt

### PSD Administrator (PSDA):

The PSD Administrator manages non-key data used to set internal parameters and settings in the MS1 X4 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 MS1 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 MS1 X4 PSD to transition to operational state. This shall place the MS1 X4 PSD in the Operational State.
- Transition to Base State: Triggers an event to transition the PSD 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
- Disable PSD: This command shall place the MS1 X4 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 MS1 X4 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.

<b>SHEET 10</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
-----------------	----------	-----------------------	-----------	------------

© Copyright 2018 Pitney Bowes, Inc.  
May be reproduced only in its original entirety (without revision) including this copyright notice.

- 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 MS1 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 MS1 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 software 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 7.1 Software Update

<b>SHEET 11</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				

## 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 MS1 binary SHA 256 Hash Block.

The PSD shall receive the MS1 Download Certificate and MS1 Binary Hash Block and then validate the message header and data content. If accepted as valid, the PSD shall verify the MS1 Download Certificate with the Domain MS1 Authentication Vendor Key. If valid, the PSD will extract the Domain MS1 Auth Download key from the download certificate. This key will be used in verifying the input MS1 Binary Hash Block. Otherwise, an error message is returned.

The PSD shall validate the message header and data content of the I\_BLK\_MS1\_BIN\_HASH\_BLK binary hash block. If accepted as valid, the PSD shall verify the MS1 Binary Hash Block with the Domain MS1 Auth Download Key that was previously loaded. Otherwise, an error message is returned

## Financial Officer (FO):

Funds transfer into and out of the MS1 X4 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 MS1 PVD Response Block with the Domain MS1 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 containing 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 MS1 Withdraw Response Block. This block is signed to verify the integrity and authenticity of the content using the Domain MS1 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 MS1 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

<b>SHEET 12</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

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 command to the PSD so that it may process the MS1 Audit Response Block returned from the Pitney Bowes infrastructure in response to the immediate previous Audit Request command. The MS1 PSD shall verify the signature of the MS1 Audit Response Block with the Domain MS1 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

<b>SHEET 13</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
<p>© Copyright 2018 Pitney Bowes, Inc.          May be reproduced only in its original entirety (without revision) including this copyright notice.</p>				

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 MS1 X4 PSD authentication of the entity; Unauthenticated Services are available to all roles, both authenticated and unauthenticated.

- Get Challenge: The Host shall instruct the MS1 X4 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 MS1 X4 PSD clock offset values
- Get Local Time: This command shall cause the MS1 X4 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 MS1 X4 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: 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),

<b>SHEET 14</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
-----------------	----------	-----------------------	-----------	------------

© Copyright 2018 Pitney Bowes, Inc.  
May be reproduced only in its original entirety (without revision) including this copyright notice.

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 MS1 X4 PSD is in a state where a specified command is expected, this command is used to return the MS1 X4 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, the PSD must relinquish control to DAL. The DAL contains a Software Update Utility which is used to update the PSD application in a safe manner. This layer is referred to as the Software Update Utility.

### 7.1 PSD Software Update

The Start Software Update event triggers the software update process. This event instructs the PSD relinquish control to the Software Download Utility in the DAL. PSD Software applications are loaded in chunks. Each chunk is signed by the Domain MS1 Authentication PSD 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 MS1 Authentication PSD Software Key.

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 Domain MS1 Authentication 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.

<b>SHEET 15</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

## 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 X4 Manufacturing DAL Interface Specification (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 1 second, then resets the MAX32590.
- **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:

Table 8 – CSPs

Key	Key Name	Description / Usage	Generation / Agreement	Storage	Entry / Output	Destruction
KEK	Unique HSM Key Encryption Key	AES256 Key Encryption Key	Internally by FIPS approved DRBG	cleartext in BBREG, ciphertext in BRAM	Entry: N/A Output: N/A	Zeroized on Tamper or Reinitialize or removal of all power
KAK	Unique HSM Key Authentication Key	HMAC256 Key Authentication Key	Internally by FIPS approved DRBG	Ciphertext in BRAM	Entry: N/A Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power
P' <sub>UPsdA-Dbt</sub>	Unique PSD Authentication Debit Private Key	ECDSA or DSA key used sign debit records	Internally by a FIPS Approved DRBG	cleartext in SRAM	Entry: N/A Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power

<b>SHEET 16</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				



Key	Key Name	Description / Usage	Generation / Agreement	Storage	Entry / Output	Destruction
K <sub>UPSDA-DBT</sub>	Unique PSD Authentication Debit Secret Key	AES, TDES, HMAC key used to generate Message Authentication codes on debit Records	External	cleartext in SRAM	Entry: Encrypted Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power
P' <sub>UPSDA-Op</sub>	Unique PSD Authentication Operational Private Key	ECDSA keys used to communicate with the infrastructure	Internally by a FIPS Approved DRBG	cleartext in SRAM	Entry: N/A Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power
P' <sub>UPSDP-DBt</sub>	Unique PSD Privacy Debit Key	RSA public keys used to encapsulate postal generated debit keys	External	cleartext in SRAM	Entry: Encrypted Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power
K <sub>UPSDP-DBt</sub>	Unique PSD Privacy Debit Key	TDES key used to encrypt postal security related parameters to the PSD	External	cleartext in SRAM	Entry: Encrypted Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power
K <sub>SPSDA-Prt</sub>	Session PSD Authentication Printer Key	HMAC Key used to authenticate messages sent to the system controller	Key Agreement per SP 800-56A	cleartext in SRAM	Entry: N/A Output: N/A	End of session or zeroized on Tamper or Reinitialize or removal of all power
K <sub>UPSDP-Op</sub>	Session PSD Privacy Operation Key	AES Key used to wrap secret or private key data sent from the infrastructure	Key Agreement per SP 800-56A	cleartext in SRAM	Entry: N/A Output: N/A	End of session or zeroized on Tamper or Reinitialize or removal of all power
DRBG WS	DRBG Working State	Values for V and C of the DRBG	Updated during each internal call to the DRBG	ciphertext in BRAM	Entry: N/A Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power

<b>SHEET 17</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

Key	Key Name	Description / Usage	Generation / Agreement	Storage	Entry / Output	Destruction
DRBG V	DRBG Entropy Input	Random bits obtained from the Hardware RNG	Hardware RNG	ciphertext in BRAM	Entry: N/A Output: N/A	Encrypting key zeroized on Tamper or Reinitialize or removal of all power

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

**Table 9 - Public Keys**

Key	Key Name	Description / Usage	Generation / Agreement	Storage	Entry / Output
MRK	Maxim Root Key	RSA PSS 2048 public key used to validate CRK when it is loaded.	Externally	cleartext in OTP	Entry: Hard Coded in MAX32590 ROM Output: N/A
CRK	Customer Root Key	RSA PSS 2048 public key used to validate PB Bootloader	Externally	cleartext in OTP	Entry: Authenticated Output: N/A
SWAK	HSM Software Authentication Download Key	ECDSA P-256 public key used to validate firmware	Externally	cleartext in SRAM	Entry: Hard coded in BL SDU Output: N/A
P <sub>DCmtA-SigMfg</sub>	Domain Comet Authentication Sigma Manufacturing Key	ECDSA used to validate Software Download Utility and Vendor Certificate	Externally	cleartext in SRAM	Entry: Certificate form Output: N/A
P <sub>DMS1A-C</sub>	Domain MS1 Authentication Certificate Key	ECDSA used to validate Authority Data	Externally	cleartext in SRAM	Entry: Certificate form Output: N/A
P <sub>DMS1A-DI</sub>	Domain MS1 Authentication Download Key	ECDSA used to validate data blocks for the Trusted Printer from the infrastructure	Externally	cleartext in SRAM	Entry: Certificate form Output: N/A
P <sub>DMS1A-PsdS</sub>	Domain MS1 Authentication PSD Software Key	ECDSA key used to authenticate PSD application Software	Externally	cleartext in SRAM	Entry: Embedded with DAL Software Update Utility form Output: N/A
P <sub>DMS1A-V</sub>	Domain MS1 Authentication Vendor Key	ECDSA vendor authentication	Externally	cleartext in SRAM	Entry: Certificate form Output: N/A

<b>SHEET 18</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

Key	Key Name	Description / Usage	Generation / Agreement	Storage	Entry / Output
P <sub>UMS1KA-B</sub>	Unique MS1 Key Agreement Base Key	ECDH Key used in key agreement between the Base an PSD	Externally	cleartext in SRAM	Entry: Certificate form Output: N/A
P <sub>UMS1KA-Op</sub>	Unique MS1 Key Agreement Operation Key	ECDH Key used in Key Agreement between Infrastructure and PSD	Externally	cleartext in SRAM	Entry: Certificate Form Output: N/A
P <sub>UPsdA-Dbt</sub>	Unique PSD Authentication Debit Key	ECDSA or DSA key used sign debit records	Internally by a FIPS Approved DRBG	cleartext in SRAM	Entry: N/A Output: Certificate Form
P <sub>UPSDA-Op</sub>	Unique PSD Authentication Operational Key	ECDSA keys used to communicate with the infrastructure	Internally by a FIPS Approved DRBG	cleartext in SRAM	Entry: N/A Output: Certificate Form

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.
- **Revokes:** Revokes a key based on identifiers in the CRL.

**Table 10 – Modes of Access**

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
X					Generate PSD Key	Generates P' <sub>UPsdA-Op</sub> and P' <sub>UPsdA-Dbt</sub> corresponding public key is output signed by current version of P' <sub>UPsdA-Op</sub> P' <sub>UPsdA-I</sub> , Encrypt with KEK
X					Load CRL	Revokes the key(s) identified in the CRL
X					Load Vendor Key	Verifies and loads P <sub>DMS1A-V</sub>
X					Load Certificate Key	Verifies and loads P <sub>DMS1A-C</sub>

<b>SHEET 19</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
X					Load Encrypted Key	Verifies and loads $K_{UPsdA-DBT}$ , $P'_{UPSDP-Dbt}$ , $K_{UPSDP-Dbt}$ , $P_{DCmtA-SigMfg}$ , $P_{DMS1A-DI}$ , $P_{DMS1A-PsdS}$ , $P_{UMS1KA-B}$ , $P_{UMS1KA-Op}$ ,
X					Load PRNG Seed	Triggers generation of DRBG V, KEK, KAK and intial DRBG WS
			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 Debit Block	N/A
	X				Disable PSD	N/A
	X				Enable PSD	N/A
	X				Reinitialize PSD	Zeroizes all Secret and Private key data
	X				Transition to Base State	N/A
	X				Transition to Operational State	N/A
	X				Generate Session	Loads $P_{UMS1KA-Op}$ , generates $K_{UPSDP-Op}$

<b>SHEET 20</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
-----------------	----------	-----------------------	-----------	------------

© Copyright 2018 Pitney Bowes, Inc.  
 May be reproduced only in its original entirety (without revision) including this copyright notice.

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
					Key	or Loads P <sub>UMS1KA-B</sub> , generates K <sub>SPSDA-Prt</sub>
	X				Start Software Update	N/A
	X				Setup Download Data	N/A
	X				Setup Download Chunk	N/A
	X				Download Chunk	N/A
				X	Finalize Debit	Sign with P'UPsdA-I
				X	Precompute r for Debit	N/A
				X	Create Debit Certificate	Sign with P' <sub>UPsdA-Dbt</sub>
				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
X	X	X	X	X	Get PSD Status	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

<b>SHEET 21</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
-----------------	----------	-----------------------	-----------	------------

© Copyright 2018 Pitney Bowes, Inc.  
May be reproduced only in its original entirety (without revision) including this copyright notice.

Roles					Services	CSP Modes of Access
CO	PSDA	PHA	FO	CU		
X	X	X	X	X	Set GMT Offset	N/A

## 9 Funds Relevant Data Items

FRDIs are data items (reflecting financial data) whose authenticity and integrity are critical; however, 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 MS1 X4 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.

<b>SHEET 22</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

## 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 signatures.
- All keys generated in the module shall have at least 112 bits of strength for FIPS Approved operation
- 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 input of 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
- The module shall support the following conditional tests:
  - Pairwise consistency test for DSA2048 key pair generation
  - Pairwise consistency test for ECDSA P-256 key pair generation
  - Continuous RNG test for the DBRG – Stuck Seed, Stuck Number

<b>SHEET 23</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

- Continuous RNG test for internal hardware Random Number Generator
- ECDSA P-256 Signature Verification - Firmware Load Test
- ECDSA P-256 Public Key Validation as part of SP 800-56A Key Agreement Protocol
- The module shall support power up self-tests, which can also be run as requested by the user, include:
  - Firmware Integrity Tests:
    - Digital Signature - ECDSA P-256
  - Bootloader Power On Self-Tests (POST)
    - ECDSA P-256 Verification Known Answer Test
    - SHA-256 Known Answer Test
  - Critical functions tests:
    - RTC Test
    - Bootloader Test
    - BRAM Pattern Test
  - Cryptographic Algorithm Known Answer Tests: (DAL POST)
    - 2-key and 3-key Triple DES Known Answer Test
    - DSA1024 and DSA2048 Verification Known Answer Test
    - SHA-1 and SHA-256 Known Answer Test
    - AES256 Key Wrap / Unwrap Known Answer Test
    - AES256 Encrypt / Decrypt Known Answer Test
    - RSA2048 Sign/Verify Known Answer Test
    - DSA2048 Pairwise Consistency Test
    - ECDSA P-256 Pairwise consistency
    - 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

<b>SHEET 24</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				



- 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 MAX32590 is a single chip cryptographic module which protects key material from unauthorized disclosure. The security features in the module include real time environmental monitoring (temperature, battery, voltage) and tamper detection. Triggering the environmental monitors or damaging the tamper shield results in a destructive result, which halts the processor and automatically zeroizes the internal encrypting key.

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 186-4, July, 2013
- 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, Jan 2012.
- The Keyed-Hash Message Authentication Code (HMAC), Federal Information Processing Standards Publication 198-1, July 2008

<b>SHEET 25</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				

- Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Special Publication 800-90A, January 2012.
- AES Key Wrap – NIST Special Publication 800-38F - December 21, 2012
- International Postage Meter Approval Requirements (IPMAR) - S30 UPU Standard
- Secure Hash Standard – FIPS PUB 180-4, March 2012
- NIST SP 800-56A Rev 2., Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography – May 2013
- Security Requirements for Cryptographic Modules – FIPS PUB 140-2, Change Notices December 3, 2002

<b>SHEET 26</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
<p>© Copyright 2018 Pitney Bowes, Inc.          May be reproduced only in its original entirety (without revision) including this copyright notice.</p>				

## 15 Acronyms

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
BBREG	Internal Battery-backed Key Register (auto zeroizable).
BRAM	Internal Battery-backed Random Access Memory
CM	Cryptographic Module
CRL	Certificate Revocation List
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
GMT	Greenwich Mean Time
IPMAR	International Postal Meter Approval Requirements
ISO	International Standards Organization
NVM	Nonvolatile Memory
OTP	One-Time Programmable Memory
PB	Pitney Bowes
PCN	Product Code Number
PHC	Print Head Controller
PSD	Postal Security Device
PSS	Probabilistic Signature Scheme
PVD	Postage Value Download
SDR	Signed Data Record
SDU	Software Download Utility
SHA	Secure Hash Algorithm
SKR	Signed Key Record
SRAM	Internal Random Access Memory
TDEA	Triple Data Encryption Algorithm
TDES	Triple Data Encryption Standard
UIC	User Interface Controller

<b>SHEET 27</b>	REV E	REV DATE 17-Apr-18	EN NO.	DWG NO.
© Copyright 2018 Pitney Bowes, Inc. May be reproduced only in its original entirety (without revision) including this copyright notice.				
55019				