Pitney Bowes, Inc.
X5 Postal Security Device (PSD)

FIPS 140-3 Non-Proprietary Security Policy

Version 1.0

TABLE OF CONTENTS

List of Tables

List of Figures

1 GENERAL

1.1 OVERVIEW

This document defines the Security Policy for the Pitney Bowes, Inc. (PB) X5 Postal Security Device (PSD) cryptographic module, hereafter "the module".

The physical form of the module is depicted in Figure 1. The module is a single-chip embodiment as defined by FIPS 140-3 and conforms to Security Level 3.

1.2 SECURITY LEVELS

The module meets the overall requirements of FIPS 140-3 Security Level 3.

Table 1: Security Levels

Section	Title	Security Level
1	General	3
2	Cryptographic Module Specification	3
3	Cryptographic Module Interfaces	3
4	Roles, Services, and Authentication	3
5	Software/Firmware Security	3
6	Operational Environment	N/A
7	Physical Security	3
8	Non-Invasive Security	N/A
9	Sensitive Security Parameter Management	3
10	Self-Tests	3
11	Life-Cycle Assurance	3
12	Mitigation of Other Attacks	N/A
	Overall Level	**3**

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 DESCRIPTION

The X5 Postal Security Device (PSD) is a single-chip (hardware) cryptographic module designed by PB to conform with FIPS 140-3 Security Level 3 requirements. The module provides cryptographic services to a host device (i.e., Digital Postage Meter), to support postage evidence in the form of an indicium. A PSD provides protection that includes ensuring the secrecy of critical security parameters (CSPs) such as cryptographic keys and providing data

integrity protection for funds relevant data items (FRDIs[1]) such as accounting data. CSPs and FRDIs reside inside the strong physical protection of the PSD.

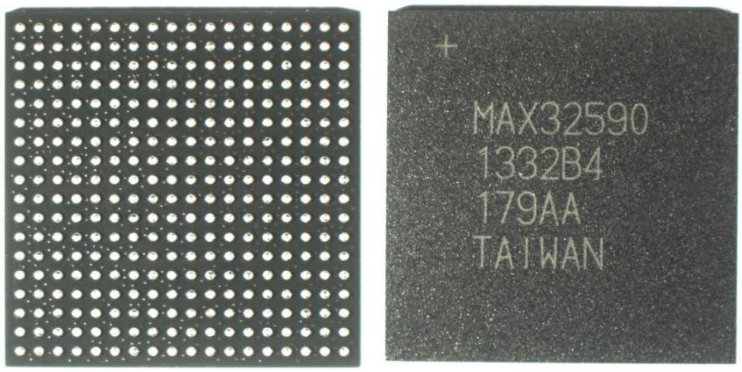

Figure 1 – X5 Postal Security Device (PSD)

Purpose and Use:
The module is designed to function as a postal security device. Postal security devices act as the core security component within postage evidencing systems (PES).

Module Type:
The module is defined as hardware module (*refer to ISO/IEC 19790, Section 7.2.2*).

Module Embodiment:
The module is defined as a single-chip cryptographic module.

Module Characteristics:
The critical components within the module are encapsulated within a single, integrated circuit.

Cryptographic Boundary:
The module's cryptographic boundary is defined as the IC package that comprises the Maxim Integrated MAX32590 DeepCover Secure Microcontroller.

[1] FRDIs are not applicable to FIPS 140-3 and are not CSPs. The FRDIs' authenticity and integrity are critical for postal functionality, and they should never be zeroized.

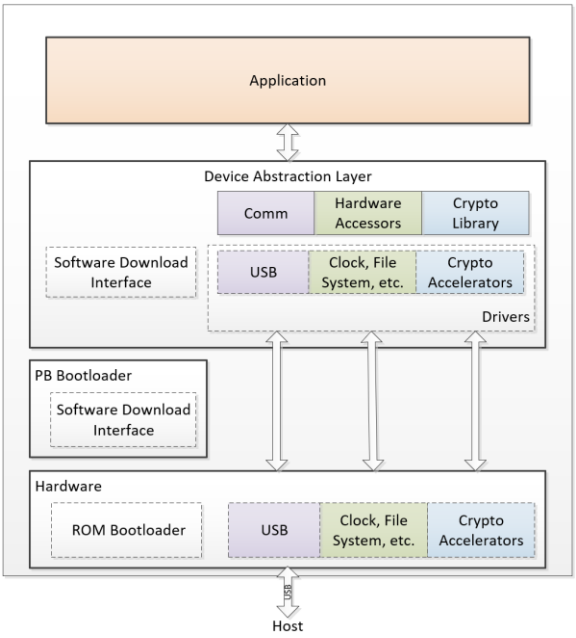

Figure 2: Block Diagram

2.2 TESTED AND VENDOR AFFIRMED MODULE VERSION AND IDENTIFICATION

The module is designed to meet the requirements of FIPS 140-3 Security Level 3 (*refer to Table 1*). The module is available in the following configuration (*refer to Table 2*):

Tested Module Identification – Hardware:

Table 2: Tested Module Identification – Hardware

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
X5 Postal Security Device (PSD)	Maxim Integrated MAX32590 DeepCover Secure Microcontroller - Revision B4	PSD Application: 22.01.000D & 22.01.000F Device Abstraction Layer (DAL): 02.01.000F & 02.01.0013	Maxim Integrated MAX32590 DeepCover Secure Microcontroller	ARM926EJ-S™ Processor Core with 16KB Data Cache and 32KB Instruction Cache

N.B. The module versioning can be verified using the 'Get Module Versions' command which returns the module's hardware ID (00000005) and firmware versions.

Tested Module Identification – Software, Firmware, Hybrid (Executable Code Sets):

N/A for this module.

Tested Module Identification – Hybrid Disjoint Hardware:

N/A for this module.

Tested Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

Vendor-Affirmed Operational Environments - Software, Firmware, Hybrid:

N/A for this module.

2.3 EXCLUDED COMPONENTS

N/A for this module.

2.4 MODES OF OPERATION

Modes List and Description:

The module only supports an Approved and non-Approved mode of operation. The module provides an explicit mode of operation indicator: the 'Approved mode status flag' is returned in every response from the module. The Approved Mode Status Flag is set to zero when a service utilizes an approved cryptographic algorithm, security function or process in an approved manner or to one for non-Approved cryptographic algorithms, security functions or process in a non-approved manner.

The module's mode of operation can only be configured within manufacturing. Once configured, the module does not have the ability to change modes.

Table 3: Modes List and Description

Mode Name	Description	Type	Status Indicator
Approved Mode	Only Approved services are supported	Approved	Approved Mode Status Flag returns '0'.
Non-Approved Mode	Non-Approved Configuration	Non-Approved	Approved Mode Status Flag returns '1'.

2.5 ALGORITHMS

The module supports the approved cryptographic algorithms shown in Table 4.

Approved Algorithms:
The module supports the following approved cryptographic algorithms.

Table 4: Approved Algorithms

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	Cert. #A2435	**Direction:** Encrypt, Decrypt **Key Length**: 256[2]	FIPS 197, NIST SP 800-38A

[2] Key sizes 128 and 192 are included in the algorithm certificate, but are not used in Approved mode.

Algorithm	CAVP Cert	Properties	Reference
AES-ECB	Cert. #A2435	**Direction:** Encrypt, Decrypt **Key Length**: 256[3]	FIPS 197, NIST SP 800-38A
AES KW	Cert. #A2435	**Direction:** Wrap, Unwrap **Key Length**: 256[4]	NIST SP 800-38F
ECDSA Key Generation	Cert. #A2437	**Curves:** P-224, P-256 **SHA Size:** 224, 256	FIPS 186-4
ECDSA Signature Generation	Cert. #A2437	**Curves:** P-224, P-256 **SHA Size:** 224, 256	FIPS 186-4
ECDSA Signature Verification	Cert. #A2437	**Curves:** P-224, P-256 **SHA Size:** 224, 256	FIPS 186-4
Hash DRBG	Cert. #A2436	**Function:** Hash_DRBG	NIST SP 800-90A Rev. 1
HMAC-SHA2-256	Cert. #A2438	**Function:** Generate Message Authentication Codes **SHA Size:** 256	FIPS 198-1
KAS-ECC-SSC NIST SP 800-56Ar3	Cert. #A2439	**Scheme:** Ephemeral Unified Model C (2e, 0s, ECC CDH) **Curve:** P-256	NIST SP 800-56A Rev. 3
KDA OneStep NIST SP 800-56Cr1	Cert. #A2439	**Function:** One-Step KDF (Session Key) **SHA Size:** 256	NIST SP 800-56C Rev. 2
KTS	Cert. #A2435	**Function:** Wrap, Unwrap **Key Length:** 256	NIST SP 800-38F
KTS	Cert. #A2435 Cert. #A2438	**AES Function:** Encrypt, Decrypt **HMAC Function:** Generate HMAC **Key Length:** 256 **SHA Size:** 256	NIST SP 800-38F; FIPS 197; FIPS 198-1
RSA Signature Verification	Cert. #A2440[5]	**Function:** Signature Verification (PKCS PSS) **Key Length:** 2048 **SHA Size:** 256	FIPS 186-4
SHA2-224	Cert. #A2441	**SHA Size:** 224	FIPS 180-4

[3] Key sizes 128 and 192 are included in the algorithm certificate, but are not used in Approved mode.
[4] Key sizes 128 and 192 are included in the algorithm certificate, but are not used in Approved mode.
[5] RSA PKCS1 v1.5 and ANSI X9.31 are not used by the module in Approved mode. Only the modulus size of 2048 is supported by the module in Approved mode.

Algorithm	CAVP Cert	Properties	Reference
SHA2-256	Cert. #A2441	**SHA Size:** 256	FIPS 180-4

Vendor-Affirmed Algorithms:

The module supports the following vendor affirmed algorithms in accordance with IG D.H (refer to Table 5).

Table 5: Vendor-Affirmed Algorithms

Name	Properties	Implementation	Reference
CKG - Asymmetric	Key Type: Asymmetric	N/A	NIST SP 800-133r2 Section 4 and Section 5.1 - The unmodified output of the DRBG is used for generation of asymmetric keys.
CKG - Symmetric	Key Type: Symmetric	N/A	NIST SP 800-133r2 Section 4 and Section 6.1 - The unmodified output of the DRBG is used for generation of symmetric keys.
CKG - Establishment	Key Type: Asymmetric	N/A	NIST SP 800-133r2 Section 4 and Section 5.2 - The unmodified output of the DRBG is used for key pair generation for key establishment.

Non-Approved, Allowed Algorithms:

N/A for this module.

Non-Approved, Allowed Algorithms with No Security Claimed:

N/A for this module.

Non-Approved, Not Allowed Algorithms:

The following cryptographic algorithms are used solely in a non-Approved mode of operation (this includes specified CAVP-validated algorithms). There exists no mechanism to allow the use of these algorithms in an Approved mode of operation.

Table 6 – FIPS Non-Approved, Not Allowed Algorithms

Algorithm	Use/Function
KAS (non-compliant)	FFC KAS used to establish a Triple DES session key.
DSA (non-compliant)	Used to generate key pairs and generate/verify digital signatures.
ECDSA (non-compliant)	Used to generate key pairs and generate/verify digital signatures.
HMAC (non-compliant)	Secondary security mechanism on Canada Indicia.
RSA (non-compliant)	Used to generate keys and digital signatures.
SHS (non-compliant)	Hashing for digital signatures and key derivation.
Triple-DES (non-compliant)	Data encryption and decryption.
Triple-DES MAC (non-compliant)	Used to generate Message Authentication Codes (MACs).

2.6 SECURITY FUNCTION IMPLEMENTATIONS

Table 7: Security Function Implementations

Name	Type	Description	Properties	Algorithms
DRBG Generate Function	DRBG	NIST SP 800-90A CTR_DRBG generate function for delivering random bits on demand	Returned Bits:1024	Hash DRBG/A2436
ECDSA Key Generation	AsymKeyPair-KeyGen CKG	FIPS 186-4 ECDSA P-224/P-256 Key Generation	Curve:P-224 Curve:P-256	ECDSA KeyGen (FIPS186-4) Curves: P-224, P256 Secret Generation Mode: Testing Candidates CKG - Asymmetric Key Type: Asymmetric
ECDSA Signature Generation	DigSig-SigGen	FIPS 186-4 ECDSA P-224/P-256 digital signature generation of postal relevant data	Curve:P-224 Curve:P-256	ECDSA SigGen (FIPS186-4) Curves: P-224, P-256 SHA2-224, SHA2-256
ECDSA Signature Verification	DigSig-SigVer	FIPS 186-4 ECDSA P-224/P-256 digital signature verification	Curve:P-224 Curve:P-256	ECDSA SigVer (FIPS186-4) Curves: P-224, P256 SHA2-224, SHA2-256
Hash Function	SHA	SHA2-224 and SHA2-256 data integrity for ECDSA digital signatures	SHA2-224, SHA2-256	SHA2-224 and SHA2-256 Message Length Min: 8 bits Message Length Max: 51200 bits
KAS	KAS	NIST SP 800-56Ar3 KAS-SSC Per IG D.F Scenario 2 path (2)	ECC P-256 providing strength of 128 bits	KAS-ECC-SSC SP800-56Ar3/A2439 KDA OneStep SP800-56Cr1/A2439
KTS_1	KTS	NIST SP 800-38F key wrapping and unwrapping per IG D.G	256-bit key providing strength of 256 bits	AES-KW/A2435
KTS_2	KTS	NIST SP 800-38F key wrapping and unwrapping per IG D.G	256-bit key providing strength of 256 bits	AES-CBC/A2435 HMAC-SHA2-256/A2438
Message Authentication	MAC	HMAC-SHA-256 used for authentication for secure sessions	Key: 256-bit	HMAC-SHA2-256 Key Length Min: 128-bit Key Length Max: 512-bit
RSA Signature Verification (Auth)	DigSig-SigVer	FIPS 186-4 RSA 2048 digital signature verification	Key:2048-bit	RSA SigVer (FIPS186-4) Signature Type: PKCS PSS Modulo: 2048 SHA2-256

Seed DRBG	DRBG	Instantiate the DRBG	Length: 1024 bits	Hash DRBG/A2436
SSP Authentication	MAC	Message authentication code applied to stored SSPs	Key: 256-bit	HMAC-SHA2-256 Key Length: 128-bit
SSP Decryption	BC-UnAuth	SSP Decryption in NVRAM	Key:256-bit	AES-CBC Key Size: 128-bit
SSP Encryption	BC-UnAuth	SSP encryption in NVRAM	Key:256-bit	AES-CBC Key Size: 128-bit
Symmetric Key Generation	CKG	Symmetric Key Generation	Key: 256-bit	CKG Key Type: Symmetric

The module utilizes only approved algorithms that are tested and validated under the Cryptographic Algorithm Validation Program (CAVP).

2.7 RBG AND ENTROPY

The module incorporates a NIST SP 800-90A Hash-DRBG (Cert. #A2436) that is seeded with 512 bits of entropy and a 512-bit nonce from an external source during manufacturing of the module. The unmodified output of the DRBG is used for generating cryptographic key material or random nonces.

Given that the entropy is imported from outside the device, there is no assurance of the minimum strength of generated SSPs.

2.8 KEY GENERATION

The module generates symmetric cryptographic keys in conformance with NIST SP 800-133r2 using a NIST SP 800-90A conforming DRBG (Cert. #A5176) for the encryption and protection of data and cryptographic keys. The module generates asymmetric cryptographic key pairs in conformance with FIPS 186-5 for the verification of digital signatures, or for the facilitation of key agreement in conformance with NIST SP 800-56ar3.

2.9 KEY ESTABLISHMENT

The module supports the establishment of cryptographic keys using elliptic curve cryptography (ECC) in conformance with NIST SP 800-56ar3 and IG D.F – Scenario #2. The module implements KAS-ECC-SSC per NIST SP 800-56A Rev3 (Cert. #A2439), used in conjunction with KDA per NIST SP 800-56Cr1 (Cert. #A2439). Key establishment methodology provides at least 128 bits of encryption strength. This is used to establish secure communication sessions.

The module also incorporates KTS in conformance with NIST SP 800-38F using AES-KW (Cert. #A2435), or when using AES-CBC (Cert. #A2435) with HMAC-SHA2-256 (Cert. #A2438).

2.10 INDUSTRY PROTOCOLS

The module relies upon the standard USB and other serial protocols for communication with general purpose computer (GPC) systems.

3 CRYPTOGRAPHIC MODULE INTERFACES

3.1 PORTS AND INTERFACES

The module incorporates physical ports and logical interfaces. The MAX32590 is supplied in a 324-pin Ball Grid Array (BGA) package where all power input, data input, data output, control input, and status output interfaces are supported. The module does not support a control output interface. The physical ports are defined within Table 8 below:

Table 8: Ports and Interfaces

Physical Port	Logical Interface(s)	Data That Passes
G13, J5, J13, K5, K13	Control Input	Reset Input, RTC, Commands.
B7, F13, F14, R10, R11, R12, R13, T10, T11, T12, T13, U10, U11, U12, U13, V10, V11, V12, V13	Control Input Data Input	Serial UART and USB interfaces for inputting postal relevant data items, configuration or sensitive security parameters (SSPs).
A7, F13, F14, P4, P6, P7, P8, P9, P10, P11, P13, P14, P15, P16, P17, P18, R10, R11, R12, R13, R14, R15, R16, R17, R18, T10, T11, T12, T13, T15, T16, T17, T18, U10, U11, U12, U13, U16, U17, U18, V10, V11, V12, V13, V16, V17, V18	Data Output, Status Output	Serial UART and USB interfaces for outputting postal relevant data items, sensitive security parameters (SSPs), error codes and module status.
G5, H13, M4, N14, N17, N18	Status Output	USB Detect, Reset Output, module status.
C3, D3, F6, F7, F8, F9, F10, F11, F12, G6, G12, H5, H6, H12, J6, J12, K6, K12, L6, L12, M6, M12, N6, N7, N8, N9, N10, N11, N12	Power	Power input.

4 ROLES, SERVICES, AND AUTHENTICATION

4.1 AUTHENTICATION METHODS

The module supports authentication methods for the Cryptographic Officer (CO) or User roles. These roles have separate authentication methods as indicated in Table 9.

Table 9: Authentication Methods

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Cryptographic Officer (CO)	Identity-based. Allows the Cryptographic Officer to authenticate themselves. Sets up a remote session with CO.	ECDSA P-256 SigVer (FIPS 186-4) (A2437)	128 bits	The module can execute at most 17.85 ECDSA verifications per second. Therefore, the probability of a successful random attempt in a one-minute period is 1 in 3.2 x 10^35 for ECDSA, which is far less than 1 in 100,000.
User	Identity-based. Allows the User to authenticate to the module.	Challenge response mechanism.	128 bits	The module can execute at most 40 password authentication attempts per minute. Therefore, the probability of a successful random attempt in a one-minute period is 1 in 8.5 x 10^36, which is far less than 1 in 100,000.

4.2 ROLES

Table 10: Roles

Name	Type	Operator Type	Authentication Methods
Cryptographic Officer (CO)	Identity	Cryptographic Officer	Digital Signature (ECDSA P-256, authenticated with Vendor, Download or Certificate Keys)
User	Identity	User	Uniquely Assigned ID in conjunction with 128-bit password
Unauthenticated	N/A	Unauthenticated	None

The module does not support concurrent operators. Only one operator is allowed to access the device at any time. Operator authentication does not persist beyond power-cycling the module. The selection of roles is implicit.

4.3 APPROVED SERVICES

Table 11: Approved Services

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Generate PSD Key	Instructs the PSD to generate its Unique ECDSA P-256 Operation Key pair or the Unique ECDSA P-256 Debit Key pair.	Approved Service ID, Success or Error ID	Command Block:0x203F00BD + Signed Key Record with the parameters for use in the generation of the private and public key values.	PSD Certificate Request block after the key has been generated or an error condition has been detected	ECDSA P-256/P-224 KeyGen, Hash-DRBG, AES 256, HMAC-SHA-256, CKG	Cryptographic Officer - Operation Private/Public Keys: G - Or Debit Private/Public Keys: G - DRBG Working State: E, G - Vendor Key: E - KEK: E - KAK: E
Generate Session Key	Instructs the PSD to generate an AES 256-bit and a HMAC 256-bit session key via NIST SP 800-56A and NIST SP 800-56C.	Approved Service ID, Success or Error ID	Command Block:0x203F00C3 + Signed Key Block with an ECDH key for generating the shared secret key.	Status bits, Session Key	Hash-DRBG, NIST SP 800-56A KAS-SSC, NIST SP 800-56C KDA, ECDSA P-256 SigVer, AES KW 256, HMAC-SHA-256 Or AES 256, CKG	Cryptographic Officer - DRBG Working State: E, G - Shared Secret: G, E - ECC-CDH PSD KAS Private Key: G, E - Operation Private Key: E, Session - Authentication Key: G, E - Or Session Privacy Key: G, E - KEK: E, KAK: E - Certificate Key: E, ECC-CDH - Infrastructure KAS Public Key: E - ECC-CDH PSD KAS Public Key: G, E, R
Load Certificate Key	Instructs the PSD to load the (ECDSA P-256) Certificate Key.	Approved Service ID, Success or Error ID	Command Block: 0x203F00BA + Certificate Key	Status bits (Success or Error ID)	HMAC-SHA-256, ECDSA P-256 SigVer	Cryptographic Officer - KAK: E, Vendor Key: E - Certificate Key: W
Load CRL	Loads the Certificate Revocation List and the CRL version.	Approved Service ID, Success or Error ID	Command Block: 0x203F00B8 + CRL	Status bits (Success or Error ID)	ECDSA P-256 SigVer	Cryptographic Officer - Download Key: E
Load Download Key	Instructs the PSD to load the (ECDSA P-256) Download Key Certificate.	Approved Service ID, Success or Error ID	Command Block:0x203F00BB + Download Key	Status bits (Success or Error ID)	HMAC-SHA-256 ECDSA P-256 SigVer	Cryptographic Officer - KAK: E - Certificate Key: E - Download Key: W

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Load Encrypted Key	The Crypto Officer instructs the PSD to load a signed key record containing an encrypted symmetric or private key.	Approved Service ID, Success or Error ID	Command Block:0x203F00AD + Encrypted Secret Key	Status bits (Success or Error ID)	HMAC-SHA-256 AES KW 256 AES 256 ECDSA P-256 SigVer	Cryptographic Officer - Debit Secret Key: W - Session Privacy Key: E - KEK: E - KAK: E - Certificate Key: E
Load Key Acknowledgement	Acknowledge that the generated PSD Key has been successfully registered and that the PSD can activate that key.	Approved Service ID, Success or Error ID	Command Block: 0x203F00AE + Affirmation from server with Key Acknowledgement	N/A	ECDSA P-256 SigVer	Cryptographic Officer - Certificate Key: E
Load Parameters: Transition to Operational State	Causes the PSD to transition to the PSD Operational lifecycle state.	Approved Service ID, Success or Error ID	Command Block:0x203F00B5 + parameter value	Status bits (Success or Error ID)	ECDSA P-256 Sig Ver	Cryptographic Officer - Certificate Key: E
Load Parameters: Transition to Base State	Transitions the PSD from its Manufacturing lifecycle state to Base lifecycle state.	Approved Service ID, Success or Error ID	Command Block:0x203F00B5 + parameter value	Status bits (Success or Error ID)	ECDSA P-256 Sig Ver	Cryptographic Officer - Certificate Key: E
Load Parameters: Disable PSD	Places the PSD in the Disabled lifecycle state. In the Disabled lifecycle state, further financial functions are prohibited.	Approved Service ID, Success or Error ID	Command Block:0x203F00B5 + parameter value	Status bits (Success or Error ID)	ECDSA P-256 Sig Ver	Cryptographic Officer - Certificate Key: E
Load Parameters: Enable PSD	Transition the PSD from Disabled lifecycle state to Operational lifecycle state.	Approved Service ID, Success or Error ID	Command Block:0x203F00B5 + parameter value	Status bits (Success or Error ID)	ECDSA P-256 Sig Ver	Cryptographic Officer - Certificate Key: E
Load Parameters: Reinitialize PSD	Causes PSD to zeroize all plaintext cryptographic keys and CSPs, and then invalidates the PSD Application.	Approved Service ID, Success or Error ID	Command Block:0x203F00B5 + parameter value	Status bits (Success or Error ID)	ECDSA P-256 Sig Ver	Cryptographic Officer - Certificate Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Load Parameters: Software Update	Update utility that allows start of firmware download.	Approved Service ID, Success or Error ID	Command Block:0x203F00B5 + parameter value	Status bits (Success or Error ID)	ECDSA P-256 Sig Ver	Cryptographic Officer - SWAK: E - Certificate Key: E
Load Parameters: Transaction Start (Commit, Rollback)	Triggers event to have the PSD prepare for a multi-message transaction that must be completed successfully as a unit (atomic transaction).	Approved Service ID, Success or Error ID	Command Block:0x203F00B5 + parameter value	Status bits (Success or Error ID)	ECDSA P-256 Sig Ver	Cryptographic Officer - Certificate Key: E
Wipe PSD	Causes PSD to zeroize all plaintext cryptographic keys and CSPs.	Approved Service ID, Success or Error ID	None	Status bits (Success or Error ID)	ECDSA P-256 Sig Ver	Cryptographic Officer - KEK: Z - Certificate Key: E
Load Vendor Key	Instructs the PSD to load the (ECDSA-P256) Vendor Key Certificate.	Approved Service ID, Success or Error ID	Command Block:0x203F00BC + Vendor Key	Status bits (Success or Error ID)	HMAC-SHA-256, ECDSA P-256 SigVer	Cryptographic Officer - KAK: E - Manufacturing Key: E - Vendor Key: W
Process Audit Response	Instructs the PSD to process the Horizon Audit Response Block returned from the Pitney Bowes infrastructure.	Approved Service ID, Success or Error ID	Command Block:0x203F00B2 + Audit Response Block	Status Bits	ECDSA P-256 Sig Ver	Cryptographic Officer - Certificate Key: E
Process Postage Value Download	Instructs the PSD to perform a postage value download operation.	Approved Service ID, Success or Error ID	Command Block:0x203F00B9	Status bits (Success or Error ID)	ECDSA P-256 Sig Ver	Cryptographic Officer - Certificate Key: E
Process Withdraw Response	Instructs the PSD to complete the withdraw process.	Approved Service ID, Success or Error ID	Command Block:0x203F00B0	Status Bits	ECDSA P-256/P-224 Sig Ver	Cryptographic Officer - Debit Private Key: E - Certificate Key: E
Audit Request	Instructs the PSD to prepare a signed Audit Request Block.	Approved Service ID, Success or Error ID	Command Block:0x204E0007 - initiates an Audit Request	Audit block	Hash-DRBG, AES-256, ECDSA P-256 SigGen	User - DRBG Working State: E, G - KEK:E - Operation Key: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Clear Upload Interval	Instructs the PSD to clear the Upload Interval Timer.	Approved Service ID, Success or Error ID	Command Block: 0x204E0032 - clears the upload interval	Status bits (Success or Error ID)	None	User - None
Create Debit Certificate	Instructs the PSD to create a debit certificate in the format defined by the Flex Debit Certificate Template.	Approved Service ID, Success or Error ID	Command Block:0x204E0029 + Postal data for signing	Status bits, Signed data block	DRBG, AES 256, ECDSA P-256/P-224 SigGen or HMAC-SHA-256	User - DRBG Working State: E, G - KEK: E - Debit Secret Key: E, or Debit Private Key: E or Mail Piece Key: E
Create PVD Request	Instructs the PSD to create a Postage Value Download Request Block.	Approved Service ID, Success or Error ID	Command Block:0x204E0033 - initiates an PVD Request	Status bits (Success or Error ID)	Hash-DRBG, AES 256, ECDSA P-256 SigGen	User - DRBG Working State: E, G - KEK: E - Operation Key: E
Finalize Debit	Performs post-debit housekeeping and prepare for the next Debit operation by precomputing the 'r' signature parameter if necessary	Approved Service ID, Success or Error ID	Command Block:0x204E0008 + data to perform a debit transaction	Status Bits	None	User - None
Log Permit	Logs the permit and the data capture recovery information.	Approved Service ID, Success or Error ID	Command Block:0x204E002B	Status Bits and Register Values	None	User - None
Login Request	Authenticates the User with the PSD. If the authentication is successful, the PSD allows debit operations.	Approved Service ID, Success or Error ID	Command Block:0x204E002F + Login data	Status Bits with login success or failure	AES 256	User - KEK: E - Password: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Precompute r for Debit	Pre-computes the 'r' signature component for the PSD Key signature (ECDSA). This message is used for countries whose debit certificate is signed by an ECDSA key.	Approved Service ID, Success or Error ID	Command Block:0x204E0009	Status bits (Success or Error ID)	Hash-DRBG, AES-256	User - DRBG Working State: E, G - KEK: E
Process Flex Debit Block	Loads a flex debit template into the PSD. The flex debit template defines the indicia content for debit operations.	Approved Service ID, Success or Error ID	Command Block:0x203F00B4 + debit template data	Status bits (Success or Error ID)	ECDSA P-256 SigVer	User - Download Key: E
Sign Transaction Data	Generates a signature on the included hash.	Approved Service ID, Success or Error ID	Command Block:0x204E0030 + Data to be hashed	Digital Signature	Hash-DRBG, AES 256, ECDSA P-256 SigGen	User - DRBG Working State: E, G - KEK: E - Operation Key: E
Verify Hash Block	Validates the included hash.	Approved Service ID, Success or Error ID	Command Block:0x203F00B3 + data and hash to be verified	Status bits (Success or Error ID)	ECDSA P-256 SigVer	User - Download Key: E
Verify Mail Piece Data	Verifies the hash of the transaction data for a mail piece.	Approved Service ID, Success or Error ID	Command Block:0x204E0031 + Data to be verified	Status bits (Success or Error ID)	HMAC-SHA-256	User - MailPiece Key: E
Withdraw Request	Instructs the PSD to initiate a Withdrawal operation.	Approved Service ID, Success or Error ID	Command Block:0x204E000A	Status bits (Success or Error ID)	ECDSA P-256 SigGen	User - Operation Key: E
Get Challenge	Returns an 8-byte nonce (random number) from the DRBG.	Approved Service ID, Success or Error ID	Command Block:0x204E0003	Nonce (8 bytes from DRBG)	Hash-DRBG, AES-256	Unauthenticated - DRBG Working State: E, G - KEK: E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Clock Offsets	Returns the drift and GMT offset values.	Approved Service ID, Success or Error ID	Command Block:0x204E0020	Status bits, + value of offsets	None	Unauthenticated - None
Get Flex Debit Template	Returns the loaded flex debit template.	Approved Service ID, Success or Error ID	Command Block:0x204E002E	Status bits + Debit Template	None	Unauthenticated - None
Get GMT Time	Returns the real time clock value with only the drift correction applied.	Approved Service ID, Success or Error ID	Command Block:0x204E001C	Time YYYYMMDDhhmmss	None	Unauthenticated - None
Get Key List	Returns a list of all active keys stored in the PSD.	Approved Service ID, Success or Error ID	Command Block:0x204E0004	Key List	None	Unauthenticated - None
Get Local Time	Returns the real time clock with drift and GMT offsets applied.	Approved Service ID, Success or Error ID	Command Block:0x204E001E	Time YYYYMMDDhhmmss	None	Unauthenticated - None
Get ML Attributes	Returns device versions and unique device serial number.	Approved Service ID, Success or Error ID	Command Block:0x204E002D	DAL Layer versions	None	Unauthenticated - None
Get Parameters	Returns parameter values stored in the PSD. The Host can request individual parameter IDs or all the Parameters in the PSD.	Approved Service ID, Success or Error ID	Command Block:0x204E0005	Status bits + parameter information	None	Unauthenticated - None
Get PSD Attributes	Returns PSD attribute data, including firmware and hardware versions.	Approved Service ID, Success or Error ID	Command Block:0x204E0021	PSD versioning information	None	Unauthenticated - None

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get PSD Status	Returns PSD status information that includes the module's mode of operation indicator.	Approved Service ID, Success or Error ID	Command Block:0x204E0022	Status of the PSD	None	Unauthenticated - None
Get PSD Versions	Retrieves the versions of the hardware, software and cryptographic libraries.	Approved Service ID, Success or Error ID	Command Block:0x204E0037	PSD Versioning information (includes HW ID and FW versions)	None	Unauthenticated - None
Get Withdraw Certificate	Retrieves the Withdraw Certificate created at the successful completion of the Withdraw process.	Approved Service ID, Success or Error ID	Command Block:0x204E0034	Signed withdrawal certificate	None	Unauthenticated - None
Perform Diagnostic Test	The User sends this message to request that the PSD perform a diagnostic test.	Approved Service ID, Success or Error ID	Command Block:0x204E0026	Status bits (Success or Error ID	None	Unauthenticated - None
Perform Full Diagnostics	The User sends this command to request the PSD perform its diagnostic processing.	Approved Service ID, Success or Error ID	Command Block:0x204E0024	Status bits (Success or Error ID	None	Unauthenticated - None
Read Log File	Returns Log Data stored in the PSD.	Approved Service ID, Success or Error ID	Command Block:0x204E0028	Log data	None	Unauthenticated - None
Reboot PSD	Restarts the PSD application. The PSD will run its power up tests.	Approved Service ID, Success or Error ID	Command Block:0x204E0006	N/A	None	Unauthenticated - None
Set Clock	Sets the real time clock in the PSD. The real time clock can only be set when the PSD is in manufacturing state.	Approved Service ID, Success or Error ID	Command Block:0x204E0002 + clock data YYYYMMDDhhmmss	Status bits (Success or Error ID	None	Unauthenticated - None

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Set GMT Offset	Sets the GMT offset in the PSD. The GMT offset is a combination of time zone offset and daylight savings time offset (if applicable).	Approved Service ID, Success or Error ID	Command Block:0x204E001D + 4-byte offset	Time with offset	None	Unauthenticated - None

4.4 NON-APPROVED SERVICES

The non-Approved Mode of the module implements the same roles and services as the Approved Mode of operations, but this mode also allows the use of the algorithms specified in Section 2.10.

Table 12 - Non-Approved Services

Name	Description	Algorithms Accessed	Role
General Postal Services	Postal services for countries that utilize non-approved algorithms (e.g. France, Germany, etc.)	DSA, ECDSA, HMAC, KAS, RSA, SHS, Triple-DES	CO/User

4.5 EXTERNAL SOFTWARE/FIRMWARE LOADED

There is no complete image replacement process. New firmware may be downloaded by the module for the country-specific postal application.

The postal application firmware is signed by PB, with an ECDSA P-256 digital signature. On downloading, the device verifies the firmware digital signature.

5 SOFTWARE/FIRMWARE SECURITY

5.1 INTEGRITY TECHNIQUES

The module includes the following firmware components that include separate firmware integrity tests:

- Bootloader: RSA 2048 Digital Signature Verification (RSA, Cert. #A2440)
- Postal Application Firmware: ECDSA P-256 Digital Signature Verification (ECDSA, Cert. #A2437)

The module will transition to its error state upon the failure of either firmware integrity test.

5.2 INITIATE ON DEMAND

Self-tests may be initiated on demand by power cycling the module ('Reboot PSD') or invoking the 'Perform Diagnostic Test' or 'Perform Full Diagnostics' services.

6 OPERATIONAL ENVIRONMENT

6.1 OPERATIONAL ENVIRONMENT TYPE AND REQUIREMENTS

Type of Operational Environment: Limited

How Requirements are Satisfied:

The module does not contain a modifiable operational environment. The module's operational environment is limited. The module includes a firmware load service to support necessary updates. Firmware versions validated through the FIPS 140-3 CMVP will be explicitly identified on a validation certificate. Any firmware not identified in this Security Policy does not constitute the module defined by this Security Policy or covered by this validation.

7 PHYSICAL SECURITY

7.1 MECHANISMS AND ACTIONS REQUIRED

The device includes automatic tamper detection and response. CSPs are zeroized automatically and immediately upon a tamper event being detected. On detection of a tamper event, the device is to be returned to PB.

Table 13: Mechanisms and Actions Required

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evidence	During installation, re-installation, decommissioning, and servicing.	Inspect device for obvious damage or other evidence of tamper.
Tamper Detection	Every 30 days	The module HW status flag is submitted every 30 days to the PB servers to check for tamper.

7.2 EFP/EFT INFORMATION

The module supports environmental failure protection (EFP) mechanisms for high/low voltage and temperature extremes (refer to Table 14).

Table 14: EFP/EFT Information

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
Low Temperature	-65°C	EFP	Zeroization
High Temperature	117°C	EFP	Zeroization
Low Voltage	2.9V	EFP	Zeroization
High Voltage	3.6V	EFP	Zeroization

7.3 HARDNESS TESTING TEMPERATURE RANGES

The module has been tested at the operational, storage and distribution temperatures listed in Table 15. The module's epoxy hardness is assured within these ranges.

Table 15: Hardness Testing Temperatures

Temperature Type	Temperature
Low Temperature	-65°C
High Temperature	150°C

8 NON-INVASIVE SECURITY

8.1 MITIGATION TECHNIQUES

The module does not provide protections against non-invasive security methods.

9 SENSITIVE SECURITY PARAMETERS MANAGEMENT

9.1 STORAGE AREAS

The module supports both volatile and persistent storage of SSPs.

Table 16: Storage Areas

Storage Area Name	Description	Persistence Type
Battery Backed RAM Register (BBREG)	On-chip memory that is zeroized on tamper detection.	Static
NVRAM	On-chip memory that is zeroized on tamper detection.	Static
SRAM	Volatile memory	Dynamic
FLASH	Persistent long-term storage	Static

9.2 SSP INPUT-OUTPUT METHODS

Table 17: SSP Input-Output Methods

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Input (Encrypted)	Outside the Module	NVRAM	Encrypted	Automated	Electronic	Key Transport
Output (Encrypted)	NVRAM	Outside the Module	Encrypted	Automated	Electronic	Key Transport
Input (Plaintext)	Outside the Module	SRAM	Plaintext	Automated	Electronic	KAS (dhEphem C(2e, 0s, FFC DH))
Output (Plaintext)	SRAM	Outside the Module	Plaintext	Automated	Electronic	KAS (dhEphem C(2e, 0s, FFC DH))

9.3 SSP ZEROIZATION METHODS

The zeroization methods described within Table 18 are supported by the module. Zeroization services explicitly overwrite SSPs with zero values.

Table 18: SSP Zeroization Methods

Zeroization Method	Description	Rationale	Operator Initiation
Reinitialize PSD	Service	Forces a zeroization of the KEK (Key Encryption Key) and NVRAM memory components. N.B. This process is irreversible.	Host device calls the service
Wipe PSD	Service	Forces a zeroization of the KEK (Key Encryption Key) and NVRAM memory components. N.B. This process is irreversible.	Host device calls the service
End of session	Automatic	Firmware programmed zeroization of ephemeral SSPs used in secure session	N/A
Removal of Battery/Tamper	Physical	Forces a zeroization of the KEK (Key Encryption Key) and removal of power from battery-backed memory.	Removal of battery power or a tamper event
Automatically	Automatic	Immediately after use.	N/A

9.4 SSPS

Table 19: SSP Table 1

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
KEK (Key Encryption Key)	Protect all keys stored internally or in NVM	256-bit	Symmetric Key - CSP	Generated Internally by DRBG (during manufacturing)	N/A	SSP Encryption SSP Decryption
KEK' (Backup Key Encryption Key)	Backup KEK	256-bit	Symmetric Key - CSP	Generated Internally by DRBG (during manufacturing)	N/A	SSP Encryption SSP Decryption
KAK (Key Authentication Key)	Authenticate keys externally stored in NVM	256-bit	Symmetric Key - CSP	Generated Internally by DRBG (during manufacturing)	N/A	SSP Authentication
Debit Private Key	Digitally sign debit records (indicia data)	112-bit or 128-bit	Asymmetric Private Key - CSP	Generated Internally by DRBG	N/A	ECDSA Signature Generation
Debit Secret Key	Digitally authenticate debit records (indicia data)	256-bit	Symmetric Key - CSP	Externally	N/A	Message Authentication
Operation Private Key	Authenticate to the communicating infrastructure	128-bit	Asymmetric Private Key - CSP	Generated Internally by DRBG	N/A	ECDSA Signature Generation
Session Authentication Key	Used to authenticate messages sent between the Host and the PSD	256-bit	Symmetric Key - CSP	N/A	KAS (dhEphem C(2e, 0s, FFC DH))	Message Authentication
Session Privacy Key	Encrypt data or wrap keys transported to infrastructure	256-bit	Symmetric Key - CSP	N/A	KAS (dhEphem C(2e, 0s, FFC DH))	KTS_1 KTS_2
ECC-CDH PSD KAS Key	Ephemeral ECC-CDH private key used in KAS	256-bit	Asymmetric Private Key - CSP	Generated Internally by DRBG	N/A	KAS
Shared Secret	Used to derive session keys	256 bits	Shared Secret - CSP	N/A	KAS (dhEphem C(2e, 0s, FFC DH))	KAS
Entropy Input	Instantiate the DRBG	512 bits	Entropy - CSP	Externally	N/A	DRBG Generate
DRBG Seed	Seeding the DRBG	1024 bits	Entropy - CSP	Generated Internally by DRBG (during manufacturing)	N/A	DRBG Generate

DRBG Working State	Internal working state of the DRBG	N/A	N/A - CSP	Generated Internally by DRBG	N/A	DRBG Generate
Mail Piece Key	Authenticate stored mail piece data	256-bit	Symmetric Key - CSP	Generated Internally by DRBG	N/A	Message Authentication
Password	Authenticate User Role	128-bit	N/A - CSP	Externally	N/A	
SWAK (Software Authentication Key)	Used to verify loaded application code	128-bit	Asymmetric Public Key - PSP	Externally	N/A	ECDSA Signature Verification
Manufacturing Key	Validates Vendor Certificate	128-bit	Asymmetric Public Key - PSP	Externally	N/A	ECDSA Signature Verification
Vendor Key	Authenticates CO role	128-bit	Asymmetric Public Key - PSP	Externally	N/A	ECDSA Signature Verification
Certificate Key	Authenticates CO role. Validates Authority Data, including other public keys	128-bit	Asymmetric Public Key - PSP	Externally	N/A	ECDSA Signature Verification
Download Key	Authenticates CO role	128-bit	Asymmetric Public Key - PSP	Externally	N/A	ECDSA Signature Verification
ECC-CDH Infrastructure KAS Public Key	ECDH public counterpart received as part of tKAS	128-bit	Asymmetric Public Key - PSP	Externally	N/A	KAS
ECC-CDH PSD KAS Public Key	ECDH public key transmitted as part of KAS	128-bit	Asymmetric Public Key - PSP	Generated Internally by DRBG	N/A	KAS
Debit Public Key	Output to the CO. Used to allow the CO to authenticate the debit records	112-bit or 128-bit	N/A - PSP	Generated Internally by DRBG	N/A	KTS_1, KTS_2
Operation Public Key	Output to the CO. Used to allow the CO to authenticate the PSD	128-bit	Asymmetric Public Key - PSP	Generated Internally by DRBG	N/A	KTS_1, KTS_2

Table 20: SSP Table 2

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
KEK (Key Encryption Key)	N/A	NVRAM: Plaintext	N/A	Zeroization, Tamper or removal of all power	DRBG Working State: Generated from

KEK' (Backup Key Encryption Key)	N/A	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	DRBG Working State: Generated from KEK (Key Encryption Key): Encrypted by
KAK (Key Authentication Key)	N/A	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	DRBG Working State: Generated from KEK (Key Encryption Key): Encrypted by
Debit Private Key	N/A	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	DRBG Working State: Generated from Debit Public Key: Paired with KEK (Key Encryption Key): Encrypted by
Debit Secret Key	Input (Encrypted)	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	KEK (Key Encryption Key): Encrypted by
Operation Private Key	N/A	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	DRBG Working State: Generated from Operation Public Key: Paired with KEK (Key Encryption Key): Encrypted by
Session Authentication Key	N/A	SRAM: Plaintext	For the life of the Secure Session	Zeroization, Tamper or removal of all power	Shared Secret (Z): Derived from
Session Privacy Key	N/A	SRAM: Plaintext	For the life of the Secure Session	Zeroization, Tamper or removal of all power	Shared Secret (Z): Derived from
ECC-CDH PSD KAS Key	N/A	SRAM: Plaintext	Until Use	Immediately after use	ECC-CDH PSD KAS Public Key: Paired with DRBG Working State: Generated from Shared Secret (Z): Derives
Shared Secret (Z)	N/A	SRAM: Plaintext	Until Use	Immediately after use	Session Authentication Key: Derives Session Privacy Key: Derives ECC-CDH Infrastructure KAS Public Key: Derived From ECC-CDH PSD KAS Key: Derived From
Entropy Input	N/A	SRAM: Plaintext	Until Use	Immediately after use	DRBG Working State: Derives
DRBG Seed	N/A	SRAM: Plaintext	Until Use	Immediately after use	DRBG Working State: Derives
DRBG Working State	N/A	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	Entropy Input: Derived from KEK (Key Encryption Key): Encrypted by
Mail Piece Key	N/A	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	KEK (Key Encryption Key): Encrypted by
Password	N/A	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	KEK (Key Encryption Key): Encrypted by
SWAK (Software Authentication Key)	N/A	Plaintext	N/A	N/A	N/A
Manufacturing Key	N/A	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	KEK (Key Encryption Key): Encrypted by
Vendor Key	Input (Encrypted)	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	KEK (Key Encryption Key): Encrypted by

Certificate Key	Input (Encrypted)	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	KEK (Key Encryption Key): Encrypted by
Download Key	Input (Encrypted)	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	KEK (Key Encryption Key): Encrypted by
ECC-CDH Infrastructure KAS Public Key	Input (Plaintext)	SRAM: Plaintext	Until Use	Zeroization, Tamper or removal of all power	Shared Secret (Z): Derives
ECC-CDH PSD KAS Public Key	Output (Plaintext)	SRAM: Plaintext	Until Use	Zeroization, Tamper or removal of all power	ECC-CDH PSD KAS Key: Paired with DRBG Working State: Generated from
Debit Public Key	Output (Encrypted)	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	DRBG Working State: Generated from Debit Private Key: Paired With KEK (Key Encryption Key): Encrypted by
Operation Public Key	Output (Encrypted)	NVRAM: Encrypted	N/A	Zeroization, Tamper or removal of all power	DRBG Working State: Generated from Operation Private Key: Paired with KEK (Key Encryption Key): Encrypted by

10 SELF-TESTS

10.1 PRE-OPERATIONAL SELF-TESTS

The following pre-operational tests are performed upon power-up, on-demand and periodically. Prior to the Pre-Operational firmware integrity self-tests being performed, the module performs the required known answer test (KAT) on the implementation.

Table 21: Pre-Operational Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Firmware Integrity of Bootloader	RSA 2048 (Cert. #A2440)	RSA Signature Verification	SW/FW Integrity	Success: No Error Code; Failure: Error Code	RSA 2048 Digital Signature Verification
Firmware Integrity of Firmware	ECDSA P-256 (Cert. #A2437)	ECDSA Signature Verification	SW/FW Integrity	Success: No Error Code; Failure: Error Code	ECDSA P-256 Digital Signature Verification

The module also includes critical function tests that test the real time clock (RTC) and BRAM.

10.2 CONDITIONAL SELF-TESTS

The following conditional tests are performed upon power-up, on-demand and periodically.

Table 22: Conditional Self-Tests

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-ECB (Cert. #A2435)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	Encrypt and Decrypt KATs	Power-up, Periodically & on-demand
AES-KW (Cert. #A2435)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	Encrypt and Decrypt KATs	Power-up, Periodically & on-demand
ECDSA (Cert. #A2437)	P-256	KAT	CAST	Success: No Error Code; Failure: Error Code	Signature Generation and Verification KATs	Power-up, Periodically & on-demand
Hash DRBG (Cert. #A2436)	N/A	KAT	CAST	Success: No Error Code; Failure: Error Code	Instantiate and Generate KAT	Power-up, Periodically & on-demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
HMAC (Cert. #A2438)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	HMAC-SHA-256 KAT	Power-up, Periodically & on-demand
KAS-ECC-SSC SP800-56Ar3 (Cert. #A2439)	P-256	KAT	CAST	Success: No Error Code; Failure: Error Code	KAS-ECC Shared Secret Computation KAT per IG D. F	Power-up, Periodically & on-demand
KDA OneStep SP800-56Cr1 (Cert. #A2439)	256-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	KDA KAT	Power-up, Periodically & on-demand
RSA (Cert. #A2440)	2048-bit	KAT	CAST	Success: No Error Code; Failure: Error Code	Signature Verification KAT	Power-up, Periodically & on-demand
Firmware Load Test	ECDSA P-256	Digital Signature Verification	SW/FW Load	Success: No Error Code; Failure: Error Code	Firmware load test occurs during *'Load Parameters Software Update'* service	During Firmware Updates
Public Key Validation	P-256	N/A	Critical Function	Success: No Error Code; Failure: Error Code	Occurs during KAS upon receipt of the connected host application public key	During key agreement
ECC Pairwise Consistency Test	P-256	PCT	PCT	Success: No Error Code; Failure: Error Code	Pairwise consistency test	During key agreement
ECDSA Key Generation	P-256	PCT	PCT	Success: No Error Code; Failure: Error Code	Pairwise consistency test	After key pair generation

10.3 PERIODIC SELF-TEST INFORMATION

The pre-operational and conditional algorithm self-tests are also automatically run on a periodic basis every 24 hrs.

Table 23: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Firmware Integrity of Bootloader	RSA Signature Verification	SW/FW Integrity	Every Power-On	Automatic invocation of self-test service
Firmware Integrity of Firmware	ECDSA Signature Verification	SW/FW Integrity	Every Power-On	Automatic invocation of self-test service

Table 24: Conditional Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-ECB (Cert. #A2435)	KAT	CAST	24 hours	Automatic invocation of self-test service
AES-KW (Cert. #A2435)	KAT	CAST	24 hours	Automatic invocation of self-test service
ECDSA (Cert. #A2437)	KAT	CAST	24 hours	Automatic invocation of self-test service
Hash DRBG (Cert. #A2436)	KAT	CAST	24 hours	Automatic invocation of self-test service
HMAC (Cert. #A2438)	KAT	CAST	24 hours	Automatic invocation of self-test service
KAS-ECC-SSC NIST SP 800-56Ar3 (Cert. #A2439)	KAT	CAST	24 hours	Automatic invocation of self-test service
KDA OneStep NIST SP 800-56Cr1 (Cert. #A2439)	KAT	CAST	24 hours	Automatic invocation of self-test service
RSA (Cert. #A2440)	KAT	CAST	24 hours	Automatic invocation of self-test service

ERROR STATES

The module incorporates a single error state (refer to Table 25).

Table 25: Error States

Name	Description	Conditions	Recovery Method	Indicator
Tampered	Occurs in the event of a physical tamper event e.g. removal of battery power, physical breach.	Tamper Event	None	Error Code
Hard Error	An error condition that is not recoverable.	Self-Test Failure	None	Error Code
Soft Error	Non-critical, recoverable errors that allow the module to transition back to operation.	Non-Critical Error Occurrences	Automated or Power-Cycle	Error Code

10.4 OPERATOR INITIATION OF SELF-TESTS

Self-tests may be triggered by the user on demand by power cycling the module ('Reboot PSD') or invoking the 'Perform Diagnostic Test' or 'Perform Full Diagnostics' services, which allows either individual or all tests to be run.

11 LIFE-CYCLE ASSURANCE

There are no specific maintenance requirements.

11.1 INSTALLATION, INITIALIZATION, AND STARTUP PROCEDURES

The module is initialized within PB manufacturing and installed into a PB manufactured PES. The PES is authorized and shipped to an end customer.

11.2 ADMINISTRATOR GUIDANCE

The device will only be provided to or retrieved from PB customers as part of a postage evidencing system. Administration guidance, in the form of API definitions, exists for PB engineers involved in the development of PES equipment.

11.3 NON-ADMINISTRATOR GUIDANCE

The device will only be provided to customers as part of a postage meter. Any user guidance will be provided as part of that equipment.

11.4 DESIGN AND RULES

The following security rules are enforced by the cryptographic module to ensure the FIPS 140-3 security requirements are met.

1. The module must support an Approved and non-Approved mode of operation. The Approved mode indicator must be returned to the end user.
2. The module must not allow unauthenticated operators to have any access to the module's cryptographic services.
3. The module must inhibit data output during self-tests, firmware load, zeroization and error states.
4. The module must logically disconnect data output from the processes performing zeroization and key generation.
5. The module must enforce identity-based authentication.
6. The module must not retain the authentication of an operator following power-off or reboot.
7. The module must support the following roles: Cryptographic Officer and User.
8. The module must not permit the input or output of plaintext cryptographic keys or other CSPs.
9. The module must not support a bypass mode or maintenance mode.
10. The module must not support the following logically distinct interfaces:
    - Data input interface
    - Data output interface
    - Control input interface
    - Status output interface
    - Power interface.
11. The module must protect critical security parameters from unauthorized disclosure, modification and substitution.
12. The module must perform power-on, on-demand and periodic self-testing.
13. The module must log errors whenever an error state is entered.
14. The module must not perform any cryptographic functions while in an error state.
15. The module must not support multiple concurrent operators.

11.5 END OF LIFE

Once a module is no longer needed by a customer, they will walk through a process called withdrawal and return the PSD to PB where an operator will perform the "re-initialize" operation, zeroizing the KEK. 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.

12 MITIGATION OF OTHER ATTACKS

The module is not purposefully designed to mitigate any attacks beyond the scope of FIPS 140-3 requirements.