Pitney Bowes, Inc.

X4i Hardware Security Module (HSM)

FIPS 140-2 Non-Proprietary Security Policy

Version 1.0

Pitney Bowes, Inc.
27 Waterview Drive
Shelton, CT 06484

TABLE OF CONTENTS

TABLE OF TABLES

1. CRYPTOGRAPHIC MODULE SPECIFICATION

1.1 OVERVIEW

This document describes the Security Policy for the X4i Hardware Security Module (HSM) (the X4i HSM). The X4i HSM is a single-chip cryptographic module designed by Pitney Bowes, Inc. (PB) to conform with FIPS 140-2 Level 3 + EFP requirements.

Table 1 – X4i Hardware Security Module (HSM) Component Versions

Item	Version	
Hardware Components:		
MAX32590 Secure Microcontroller	Revision B4	
Firmware Components:		
PB Bootloader	00.00.0016	
HSM Application Device Abstraction Layer (DAL)	21.02.000F 01.02.0018	21.03.0001 01.02.0024

The HSM Application and DAL are compiled into a single firmware and integrity tested together. This single firmware is referred to as the HSM Application hereafter.

The X4i HSM provides cryptographic services to a host device, including authentication, privacy, and key protection.

The X4i HSM is defined as a single chip cryptographic module.

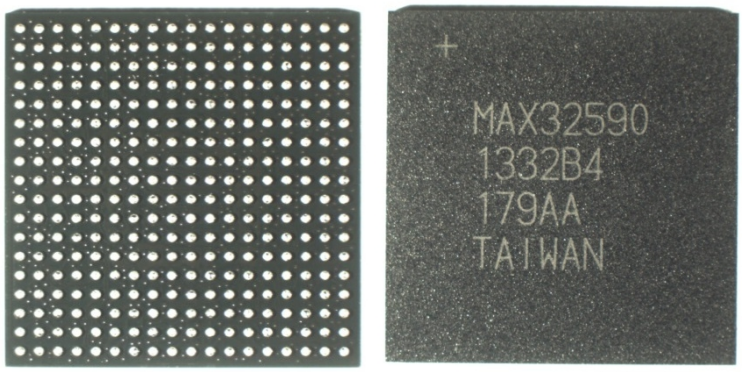

Figure 1 – MAX32590 (Back and Front)

The X4i HSM's cryptographic boundary is defined as the IC package that comprises the Maxim Integrated MAX32590 DeepCover Secure Microcontroller (refer to Figure 1). 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 copied to internal SRAM and then authenticated via digital signatures.

The PB Bootloader is authenticated by verification of the "CRK" key using RSA 2048 with SHA-256 (Cert. #C477). Once the PB Bootloader has been loaded and authenticated, the PB Bootloader copies HSM Application (i.e. the combined Device Abstraction Layer (DAL) and HSM Application) to SRAM and authenticates it by verification of the "SWAK" Key using ECDSA P-256 with SHA-256 (Cert. #C476).

1.2 SECURITY LEVEL

The module meets the overall requirements of FIPS 140-2 Security Level 3 +EFP

Table 2 – Module Security Level

FIPS Area	FIPS Security Requirement	Level
1	Cryptographic Module Specification	3
2	Module Ports and Interfaces	3
3	Roles, Services, and Authentication	3
4	Finite State Model	3
5	Physical Security	3 +EFP
6	Operational Environment	N/A
7	Cryptographic Key Management	3
8	EMI/EMC	3
9	Self-Tests	3
10	Design Assurance	3
11	Mitigation of Other Attacks	3

1.3 MODES OF OPERATION

The module supports both an Approved mode and a non-Approved mode of operation. The module provides an explicit mode of operation indicator: the FIPS mode status flag is returned in every response from the module. The FIPS mode flag is set to zero for an Approved mode of operation or to one for non-Approved mode of operation.

2. MODULE 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.

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

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

Figure 2 – X4i HSM Interface Mapping

3. ROLES, SERVICES, AND AUTHENTICATION

3.1 ROLES

The module supports three authenticated roles that are either categorized as Crypto-Officer (CO), or User roles. Additionally, the module has a single unauthenticated role. The CO Admin role is implicitly selected and authenticated via digital signature. The CO Op and TU identities are implicitly selected by ID and possession of the respective HMAC key used for authentication.

Table 3 – Roles and Authentication

Role	Authentication Method	Authentication Type
Crypto-Officer (Administrator) (CO Admin)	Digital Signature (ECDSA P-256) authenticated by PAK	Identity-based
Crypto-Officer (Operator) (CO Op)	Uniquely Assigned ID in conjunction with HMAC-SHA-256 (MAC truncated to 128 bits)	Identity-based
Trusted User (TU)	Uniquely Assigned ID in conjunction with HMAC-SHA-256 (MAC truncated to 128 bits and different than the CO Op Secret Key)	Identity-based

Unauthenticated	None	None

Table 4 – Strength of Authentication

Authentication Mechanism	Probability of False Acceptance (Single Attempt)	Probability of False Acceptance (One Minute)
Digital Signature	The probability of a random access or false acceptance occurring is 1 in 2^128 for ECDSA P-256, which is less than 1 in 1,000,000.	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.
Uniquely Assigned ID and HMAC	A 256-bit HMAC key (DAK) with the MAC truncated to 128 bits is used for authentication. The probability of a random access or false acceptance occurring is 1 in 2^128 for a given ID, which is less than 1 in 1,000,000.	The module can execute at most 3,000 HMAC authentication attempts per second. Therefore, the probability of a successful random attempt in a one-minute period is 1 in 1.9 x 10^33, which is far less than 1 in 100,000

3.1.1 INITIALIZATION

During manufacturing, the PB Bootloader (verified by CRK key) and HSM application (verified by the SWAK key) are loaded at secure vendor facilities. The system is initialized. The DRBG seed, KEK (Key Encryption Key) and KAK (Key Authentication Key) are generated. The mode of operation is locked to Approved mode unless changed via a HSMLoadParameter command before additional keys are loaded or generated. Signed public keys, the Device Authentication Keys (DAK) and Device Privacy Key (DPK) are loaded and verified[1]. The module is now configured.

3.2 SERVICES

Crypto-Officer (Administrator):

The services allocated to this role are as follows:

Load Parameters: Load a set of parameters into the HSM.

Firmware Update[2]: Secure firmware update process using the Software Download Utility (SDU) within the Device Abstraction Layer (DAL). The PB Bootloader verifies the ECDSA P-256 (Cert. #C476) signature on the combined HSM Application and DAL firmware.

The Software Download Utility supports the following authenticated sub-services.

- **Setup Download Data**: The Host sends this signed record to make the SDU aware of the parameters of the software (application) to be downloaded. Receipt of this message triggers a transition to the state required to load chunk information.
- **Setup Download Chunk**: The Host sends this signed record to make the SDU 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 DAL has received a valid Setup Download Data message. The downloaded firmware is authenticated with the Software Authentication Key (SWAK).

[1] The DAK and DPK are generated for modules configured as a Key Root Authority (KRA) HSMs
[2] Any firmware loaded into this module that is not shown on the module certificate, is out of the scope of this validation and requires a separate FIPS 140-2 validation

- **Download Chunk**: This message contains the data referenced in the Setup Download Chunk message.

Crypto-Officer (Operator) and Trusted User:

The same services are allocated to both these roles. These services are as follows:

- **Decrypt**: Decrypt data.
- **Decrypt Compare**: Decrypt encrypted data and compare to expected result.
- **Decrypt Encrypt**: Decrypt encrypted data and re-encrypt with another key.
- **Delay Echo**: Respond with input message after delay.
- **Delete Key**: Remove a key from the HSM.
- **Delete Key Parameter**: Remove a key parameter from the HSM.
- **Derive Key Agreement**: Establish a key to be used to exchange secure information with the HSM (AES 128/192/256 KW or HMAC-SHA-256).
- **Encrypt**: Encrypt data.
- **Encrypt Nonce**: Generate a nonce (if not passed in) and then encrypt the nonce.
- **Export Key**: Securely export a key for storage / use in another location.
- **Generate**: Generate a public/private key pair or a secret key. The message specifies the cryptographic algorithm and the parameters for use in the generation of the key(s).
- **Generate PSD RSA Record**: Generate an RSA public/private key pair for a Postal Security Device (PSD).
- **Generate RSA Primes**: Generate a pair of prime numbers used for RSA key generation.
- **Get Counters**: Output a copy of the current values of the internal counters.
- **Get Entropy**: Retrieves data from the hardware TRNG.
- **Join Key**: Assemble a key that has been previously split.
- **Load Key**: Load an encrypted or public key for later use. The command specifies the storage type:
    - Volatile: Store in RAM, can be replaced if space is needed.
    - Sticky: Store in RAM, can NOT be replaced until it is deleted by the host.
    - Static: Store in NVM
- **Load Key Parameters** – Load a set of key parameters for later use, stored in NVM.
- **Load Parameters**: Load a set of parameters into the HSM.
- **Set Counter**: Set an internal counter to a specific value.
- **Sign**: Apply a cryptographic signature to a set of data.
- **Split:** Divide a key into 2 or more parts.
- **Update Counters**: Update specific internal counters
- **Verify**: Verify a cryptographic signature on a set of data.

Unauthenticated Services:

Miscellaneous functions that do not require the HSM authentication of the entity. Unauthenticated Services (listed below) are available to all roles, both authenticated and unauthenticated.

- **Get HW Status**: Get the hardware specific status data of the HSM.
- **Get Key List**: Return a list of all active keys stored in the HSM.
- **Get Key Parameters**: Retrieve list of key parameters loaded into HSM.
- **Get Key Table**: Retrieves data of key and key parameters stored in key table.
- **Get Parameters**: Retrieve parameter values from the HSM. The Host can request individual parameter IDs or all of the stored parameters in the HSM.
- **Get Random**: Get a pseudo-random number from the HSM.
- **Get Status**: Get HSM status information.
- **Get Versions:** Get the versions of the components in the HSM
- **Perform Diagnostic Test**: Perform one or more diagnostic tests.
- **Perform Full Diagnostics:** Run power up tests and perform other maintenance activities.
- **Read Log**: 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.
- **Reboot**: Reboot the device.
- **Reinit**: Reinitialize HSM by erasing all NVM data except for HW Mfg Data and 'persistent' data (total device cycles, reinit count) and then invalidates the HSM Application. This command zeroizes the unique HSM Key Encryption Key (KEK), which results in the loss of all other private and secret keys. Used to 'clean' the HSM so it can be re-configured.

3.2.1 Service Access to Security Functions and CSPs

Critical Security Parameter (CSP) and Public Security Parameter (PSP) access by services is classified as Read (R), Write (W), or Zeroize (Z) in the table below.

Table 5 – Services Available in FIPS Approved Mode

Role(s) with Service Access	Service	Security Functions Used	CSP Access	PSP Access
CO Admin	All services with CSP access	HMAC-SHA-256 AES 256 KW	KAK: R KEK: R	-
	Load Parameters	HMAC-SHA-256 ECDSA P-256 SigVer	DAK: R	PAK: R
	Firmware Update: Setup Download Data	HMAC-SHA-256 ECDSA P-256 SigVer	DAK: R	SWAK: R
	Firmware Update: Setup Download Chunk	HMAC-SHA-256 ECDSA P-256 SigVer	DAK: R	SWAK: R
	Firmware Update: Download Chunk	HMAC-SHA-256	DAK: R	None

Role(s) with Service Access	Service	Security Functions Used	CSP Access	PSP Access
CO Op or TU	All services	HMAC-SHA-256	DAK: R	-
	All services with CSP access	HMAC-SHA-256 AES 256 KW	KAK: R KEK: R	-
	Decrypt	HMAC-SHA-256 or AES 128/192/256 or RSA 2048	Session Key: R or PK: R or DPK: R	None
	Decrypt Compare	HMAC-SHA-256 or AES 128/192/256 or RSA 2048	Session Key: R or PK: R or DPK: R	None
	Decrypt Encrypt	HMAC-SHA-256 or AES 128/192/256 or RSA 2048	Session Key: R or PK: R or DPK: R	PK Public: R
	Delay Echo	No additional	No additional	None
	Delete Key	No additional	All static keys except DAK, KEK, KEK', KAK: Z	All static public keys: Z
	Delete Key Parameter	No additional	No additional	None
	Derive Key Agreement	DRBG KAS-SSC KDA HMAC-SHA-256 or AES 128/192/256 (KW only)	DRBG Working State: R, W ECC-CDH Key: W, R, Z Shared Secret: W, R, Z Session Key: W, R	ECC-CDH Peer Public Key: W, R ECC-CDH Public Key: W, R
	Encrypt	HMAC-SHA-256 or AES 128/192/256 or RSA 2048	Session Key: R or PK: R or DPK: R	PK Public: R
	Encrypt Nonce	DRBG HMAC-SHA-256 or AES 128/192/256 or RSA 2048	DRBG Working State: R, W Session Key: R or PK: R or DPK: R	PK Public: R
	Export Key	HMAC-SHA-256 AES 128/192/256 (KW only)	All static keys except KEK, KEK', KAK: R	All static public keys: R
	Generate	DRBG ECDSA P-224/P-256 KeyGen or DSA 2048 KeyGen or RSA 2048 Key Gen or AES 128/192/256 Key Gen or HMAC-SHA-256 Key Gen	DRBG Working State: R, W AK: W or PK: W or DAK: W[3] or DPK: W or CRK Private: W or SWAK Private: W or PAK Private: W	AK Public: W or PK Public: W or CRK Public: W[4] or SWAK Public: W or PAK Public: W

[3] DAK, DPK, CRK, SWAK, and PAK keys are only generated in modules configured as KRA HSMs

[4] CRK, SWAK, and PAK keys are only generated in modules configured as KRA HSMs

Role(s) with Service Access	Service	Security Functions Used	CSP Access	PSP Access
	Generate PSD RSA Record	DRBG RSA 2048 SigGen HMAC-SHA-256 AES 128/192/256 (KW only)	DRBG Working State: R, W DPAG Private: W Session Key: R	DPAG Public: W
	Generate RSA Primes	DRBG RSA 2048 SigGen HMAC-SHA-256 AES 128/192/256 (KW only)	DRBG Working State: R, W RSA Primes: W Session Key: R	None
	Get Counters	HMAC-SHA-256 ECDSA P-224/P-256 SigGen or DSA 2048 SigGen or RSA 2048 SigGen	AK: R	AK Public: R
	Get Entropy	NDRNG HMAC-SHA-256 AES 128/192/256 (KW only)	Session Key: R	None
	Join Key	AES 256 KW ECDSA P-256 SigVer	PK: W	AK: R
	Load Key	HMAC-SHA-256 or AES 128/192/256 ECDSA P-224/P-256 SigVer	Session Key: R or PK: R or DPK: R All static keys except KEK, KEK', KAK: W[5] RSA primes: W	AK Public: R All static public keys: W[6]
	Load Key Parameters	HMAC-SHA-256 or AES 128/192/256 ECDSA P-224/P-256 SigVer	Session Key: R or PK: R or DPK: R	AK Public: R
	Load Parameters	ECDSA P-256 SigVer	No additional	PAK: R
	Set Counter	No additional	No additional	None
	Sign	DRBG ECDSA P-224/P-256 SigGen or DSA 2048 SigGen or RSA 2048 SigGen or HMAC-SHA-256	DRBG Working State: R, W AK: R or CRK Private: R or SWAK: R or PAK: R	None
	Split	DRBG ECDSA P-256 SigGen	DRBG Working State: R, W AK: R PK: W	None
	Update Counters	No additional	No additional	None

[5] DAK, DPK, CRK, SWAK, and PAK keys are only loaded in Manufacturing

[6] CRK, SWAK, and PAK keys are only loaded in Manufacturing

Role(s) with Service Access	Service	Security Functions Used	CSP Access	PSP Access
	Verify	ECDSA P-224/P-256 SigVer or DSA 2048 SigVer or RSA 2048 SigVer or HMAC-SHA-256	AK: R	AK Public: R or CRK Public: R or SWAK Public: R or PAK Public: R
Unauthenticated User	Get HW Status	None	None	None
	Get Key List	None	None	None
	Get Key Parameters	None	None	None
	Get Key Table	None	None	None
	Get Parameters	None	None	None
	Get Random	DRBG	DRBG Working State: R, W	None
	Get Status	None	None	None
	Get Versions	None	None	None
	Perform Diagnostic Test	None	None	None
	Perform Full Diagnostics	None	None	None
	Read Log	None	None	None
	Reboot	None	None	None
	Reinit	None	KEK: Z	None

3.3 Non-Approved Mode Roles and 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 7.3 FIPS Non-Approved Algorithms. Additionally, non-Approved mode includes the following services:

Crypto-Officer (Operator) and Trusted User:

- **Decrypt Conv Encrypt**: Decrypts, converts legacy records and re-encrypts.
- **Derive Key**: Establish a Triple DES key to be used to exchange information between a PSD and a Post.

3.4 Security Rules

This section documents the security rules enforced by the cryptographic module to implement the security requirements of a 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 or unique IDs and Message Authentication Codes (MACs) using unique HMAC keys for each identity

- All keys generated in the module shall have at least 112 bits of cryptographic security strength for an Approved mode of operation.
- The module shall not provide a bypass state where plaintext information is passed through the module.
- The module shall not support a maintenance mode.
- The module shall not output any secret or private key in plaintext form.
- The module shall not accept any secret or private key in plaintext form outside of manufacturing.
- There shall be no manual entry of keys into the system.
- There shall be no entry or output of split shared keys from the module except when it is configured as a Key Root Authority (KRA).
- Keys shall be established via an Approved method or entered into the system through FIPS Approved processes.
- 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.

4. PHYSICAL SECURITY

The X4i HSM utilizes the Maxim Semi-Conductor MAX32590 micro-controller, a single chip cryptographic module that protects key material from unauthorized disclosure, modification or substitution. The module is conformant to FIPS 140-2 Level 3 physical security requirements and is protected by an encapsulant. The hardness of the module encapsulant was tested at room temperature and over the module's documented operating temperature range from -40˚C to + 85˚C.

In addition to Level 3 physical security features, the module includes real time environmental monitoring (temperature, battery, voltage), and tamper detection and response. Triggering the environmental failure protection mechanisms or damaging the active shield (tamper detection) that protects the entire module results in a tamper event. A tamper event halts the processor and automatically zeroizes the master key encryption key (KEK).

The operator should periodically inspect the module for evidence of tampering.

5. MITIGATION OF OTHER ATTACKS

The module has been designed to mitigate specific attacks outside the scope of FIPS 140-2, Level 3. It incorporates environmental failure protection mechanisms inherent to a Level 4 module. The module is designed to defend against out of bound voltage and temperature extremes. Additionally, the module provides a tamper detection and response mechanism.

6. 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.

7. CRYPTOGRAPHIC KEY MANAGEMENT

7.1 FIPS APPROVED ALGORITHMS

The following FIPS Approved cryptographic algorithms listed in Table 6 are supported by the module.

Table 6 – FIPS Approved Algorithms

CAVP Certs	Algorithm	Standards	Modes/ Methods	Key Lengths, Curves, or Moduli	Use
5954	AES	FIPS 197 SP 800-38A SP 800-38F	CBC, ECB, KW	256, 192, 128	Data encryption and decryption Cryptographic key wrapping and unwrapping (KTS key establishment providing 256 bits of encryption)
Vendor Affirmed	CKG	SP 800-133			Symmetric key generation and asymmetric seed generation from the unmodified output of the DRBG
C472	DRBG	SP 800-90A	HASH-based		Deterministic Random Bit Generator with 256-bit security strength (seeded with full entropy). DRBG does not support reseed.
C475	DSA	FIPS 186-4	KeyGen SigGen SigVer	(2048, 224)[7] (2048, 256) (2048, 224, SHA-224) (2048, 256, SHA-256) (2048, 224, SHA-224) (2048, 256, SHA-256)	Generation of cryptographic key pairs, and digital signature generation and verification.
C476	ECDSA	FIPS 186-4	KeyGen SigGen SigVer	P-224[8] P-256 P-224, SHA-256 P-256, SHA-256 P-224, SHA-256 P-256, SHA-256	Generation of cryptographic key pairs, and digital signature generation and verification.

[7] The following DSA functionality is included in the algorithm certificate, but is not used in Approved mode: SigVer (1024, 160, SHA-1)
[8] The following ECDSA functionality is included in the algorithm certificate, but is not used in Approved mode: SigGen Component; SigVer (P-192, SHA-1)

CAVP Certs	Algorithm	Standards	Modes/ Methods	Key Lengths, Curves, or Moduli	Use
C464	HMAC	FIPS 198-1	HMAC-SHA-256[9]	256 bits	Used to generate Message Authentication Codes (MACs). Truncated MACs (at least 128 bits) are used for some applications.
n/a	KAS	SP 800-56Ar3 and SP 800-56Cr1	C (2e, 0s, ECC CDH)	P-256	The KAS consists of KAS-SSC (vendor affirmed) and KDA (vendor affirmed)
Vendor Affirmed	KAS-SSC	SP 800-56Ar3	ECC	P-256	Key Agreement Protocol used to establish a session key (Ephemeral Unified Model C (2e, 0s, ECC CDH)). Provides 128 bits of encryption strength.
Vendor Affirmed	KDA	SP 800-56Cr1	One-Step KDF	HMAC-SHA-256	Key Derivation Function used with KAS-SSC to establish a session key
KTS (AES Cert. #5954)		SP 800-38F	AES KW	128, 192, 256	Protects exported keys. Key establishment methodology provides between 128 and 256 bits of encryption strength.
KTS (AES Cert. #5954 and HMAC Cert. #C464)		SP 800-38F	AES CBC 256 HMAC-SHA-256	256	Protects CSPs stored in Non-Volatile Memory (NVM) external to the module (using KEK and KAK keys)
C477	RSA	FIPS 186-4	KeyGen SigGen (ANSI X9.31, PKCS 1.5, PKCSPSS) SigVer (ANSI X9.31, PKCS 1.5, PKCSPSS)	2048[10] 2048, SHA-256 2048, SHA-256	Generation of cryptographic key pairs, digital signature generation and verification, and data encryption and decryption.
C295	SHS	FIPS 180-4	SHA-224 SHA-256[11]		SHS provides the hashing algorithm necessary for DSA, ECDSA and RSA digital signature generation/ verification and for the key derivation function

[9] HMAC-SHA-1 is included in the algorithm certificate, but is not used in Approved mode

[10] The following RSA functionality is included in the algorithm certificate, but is not used in Approved mode: SigVer ANSI X9.31 (1024, SHA-1 and SHA-256); SigVer PKCS 1.5 (1024, SHA-1 and SHA-256); SigVer PKCSPSS (1024, SHA-1 and SHA-256) and (2048, SHA-1)

[11] SHA-1 is included in the algorithm certificate, but is not used in Approved mode

7.2 FIPS ALLOWED ALGORITHMS

The module supports the following non-Approved but Allowed security functions listed in Table 7.

Table 7 – FIPS Allowed Algorithms

Algorithm	Strength	Use
NDRNG	The NDRNG entropy rate and the DRBG implementation ensure that the DRBG is seeded with full entropy (256 bits)	Seeding the DRBG

7.3 FIPS NON-APPROVED ALGORITHMS

The following cryptographic algorithms listed in Table 8 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 8 – FIPS Non-Approved Algorithms

Algorithm	Key Lengths, Curves, or Moduli	Use
KAS (non-compliant)	1024	FFC KAS used to establish a Triple DES session key
DSA (non-compliant)	KeyGen: (1024, 160) SigGen: (1024, 160, SHA-1) SigVer: (1024, 160, SHA-1)	Used to generate key pairs and generate/verify digital signatures. Legacy verification validated by CAVP DSA Cert. #475.
ECDSA (non-compliant)	KeyGen: P-160 P-192 SigGen: P-160, SHA-1 P-192, SHA-1 SigVer: P-160, SHA-1 P-192, SHA-1	Used to generate key pairs and generate/verify digital signatures. Legacy verification of P-192, SHA-1 validated by CAVP Cert. #C476.
HMAC (non-compliant)	HMAC-SHA-1	Validated by CAVP Cert. #C464
RSA (non-compliant)	KeyGen: 1024 SigGen ANSI X9.31, PKCS 1.5, PKCSPSS: (1024, SHA-1) SigVer ANSI X9.31, PKCS 1.5, PKCSPSS: (1024, SHA-1)	Used to generate keys and digital signatures. Legacy verification validated by CAVP Cert. #C477
SHS (non-compliant)	SHA-1	Hashing for digital signatures and key derivation. Validated by CAVP Cert. #C295

Algorithm	Key Lengths, Curves, or Moduli	Use
Triple-DES (non-compliant)	2 key and 3 key encrypt/decrypt	Data encryption and decryption. Validated by CAVP TDES Cert. #2900.
Triple-DES MAC (non-compliant)	128-bit, 192-bit	Used to generate Message Authentication Codes (MACs).

7.4 CSPs and Keys

7.4.1 Critical Security Parameters

All CSPs except the KEK are stored in battery-backed memory encrypted by the KEK, or in Non-Volatile Memory (NVM) external to the module encrypted by the KEK and additionally protected by the KAK. Therefore, zeroizing the KEK destroys access to all CSPs. All CSPs that are input or output are wrapped in conformance to SP 800-38F by an AES KW key (128-256 bits).

Table 9 – Secret Keys, Private Keys, Cryptographic Key Components, and Other CSPs

CSP/Key	Security Function	Use	Establishment	Entry/Output	Storage	Destruction
KEK (256-bit) (Key Encryption Key)	AES KW 256 (Cert. #5954)	Protect all keys stored internally or in NVM	Generated Internally by FIPS approved DRBG (during manufacturing)	Entry: N/A Output: N/A	Plaintext	Zeroization, Tamper or removal of all power
KEK' (256-bit) (Backup Key Encryption Key)	AES KW 256 (Cert. #5954)	Backup KEK	Generated Internally by FIPS approved DRBG (during manufacturing)	Entry: N/A Output: N/A	Encrypted with KEK	Zeroization, Tamper or removal of all power
KAK (256-bit) (Key Authentication Key)	HMAC-SHA-256 (Cert. #C464)	Protect keys externally stored in NVM	Generated Internally by FIPS approved DRBG (during manufacturing)	Entry: N/A Output: N/A	Encrypted with KEK	Zeroization, Tamper or removal of all power
DAK (Device Authentication Keys)	HMAC-SHA-256 (Cert. #C464)	Keys used to authenticate CO Op and TU identities	Generated Internally by FIPS approved DRBG (KRA HSM only) Entered in manufacturing	Entry: N/A Output: Encrypted by AES KW	Encrypted with KEK	Zeroization, Tamper or removal of all power
DPK (Device Privacy Key)	AES CBC 256 or AES KW 256 (Cert. #5954)	Keys used to encrypt data or keys	Generated Internally by FIPS approved DRBG (KRA HSM only) Entered in manufacturing	Entry: N/A Output: Encrypted by AES KW	Encrypted with KEK	Zeroization, Tamper or removal of all power

CSP/Key	Security Function	Use	Establishment	Entry/Output	Storage	Destruction
DRBG Seed (1024-bit)	NDRNG	Seeding the DRBG	Generated Internally by NDRNG (during manufacturing)	Entry: N/A Output: N/A	Encrypted with KEK	Zeroization, Tamper or removal of all power
DRBG Working State (1024-bit)	DRBG (Cert. #C472)	Internal working state of the DRBG	Generated Internally by FIPS approved DRBG	Entry: N/A Output: N/A	Encrypted with KEK	Zeroization, Tamper or removal of all power
AK (Authentication Key)	HMAC-SHA-256 (Cert. #C464)	Used to provide Authentication	Generated Internally by FIPS approved DRBG Or loaded as needed	Entry: Encrypted by AES KW Output: Encrypted by AES KW	Encrypted with KEK	Zeroization, Tamper or removal of all power
	DSA 2048 (Cert. #C475)	Used to provide Authentication			Encrypted with KEK	
	ECDSA P-224 or P-256 (Cert. #C476)	Used to provide Authentication			Encrypted with KEK	
	RSA 2048 (Cert. #C477)	Used to provide Authentication			Encrypted with KEK	
PK (Privacy Key)	AES CBC 128, 192, 256 or AES KW 128, 192, 256 (Cert. #5954)	Keys used to encrypt data or keys	Generated Internally by FIPS approved DRBG Or loaded as needed	Entry: Encrypted by AES KW Output: Encrypted by AES KW	Encrypted with KEK	Zeroization, Tamper or removal of all power
	RSA 2048 (Cert. #C477)	Keys used to decrypt data			Encrypted with KEK	
DPAG Private (DPAG Private Key)	RSA 2048 (Cert. #C477)	RSA Keys generated for PSDs	Generated Internally by FIPS approved DRBG Or loaded as needed	Entry: Encrypted by AES KW Output: Encrypted by AES KW	Encrypted with KEK	Zeroization, Tamper or removal of all power
ECC-CDH Key (256-bit)	KAS-SSC (vendor affirmed)	Ephemeral ECC-CDH private key used in KAS-SSC	Generated Internally by FIPS approved DRBG	Entry: N/A Output: N/A	Destroyed immediately after session established	Zeroization, Tamper or removal of all power
Shared Secret (256-bit)	KDA (vendor affirmed)	Used to derive session keys	KAS-SSC per SP 800-56Ar3	Entry: N/A Output: N/A	Destroyed immediately after session established	Zeroization, Tamper or removal of all power
Session Key (256-bit)	AES KW 128, 292, 256 (Cert. #5954)	Encrypt data or wrap keys transported to infrastructure	KAS-SSC per SP 800-56Ar3 + KDF per SP 800-56Cr1	Entry: N/A Output: N/A	Encrypted with KEK	Zeroization, Tamper or removal of all power
	HMAC-SHA-256 (Cert. #C464)	Provide message Authentication				

CSP/Key	Security Function	Use	Establishment	Entry/Output	Storage	Destruction
CRK Private	Customer Root Key (RSA PSS 2048)	Signs the PB Bootloader firmware	Generated Internally by FIPS approved DRBG (KRA HSM only) Or loaded as needed	Entry: Encrypted by AES KW Output: Encrypted by AES KW	Encrypted with KEK	Zeroization, Tamper or removal of all power
SWAK Private	Software Authentication Key (ECDSA P-256)	Signs the HSM firmware	Generated Internally by FIPS approved DRBG (KRA HSM only) Or loaded as needed	Entry: Encrypted by AES KW Output: Encrypted by AES KW	Encrypted with KEK	Zeroization, Tamper or removal of all power
PAK Private	Parameter Authentication Key (ECDSA P-256)	Signs the HSM parameters	Generated Internally by FIPS approved DRBG (KRA HSM only) Or loaded as needed	Entry: Encrypted by AES KW Output: Encrypted by AES KW	Encrypted with KEK	Zeroization, Tamper or removal of all power
RSA Primes	Primes for RSA PSS 2048	Primes used to speed up RSA key generation	Generated Internally by FIPS approved DRBG Or loaded as needed	Entry: Encrypted by AES KW Output: Encrypted by AES KW	Encrypted with KEK	Zeroization, Tamper or removal of all power

7.4.2 PUBLIC SECURITY PARAMETERS KEYS

Table 10 – Public Security Parameters

Public Key	Description	Use	Establishment	Entry/Output	Storage
CRK	Customer Root Key (RSA PSS 2048)	Validates the PB Bootloader firmware integrity on power-on	Loaded in Manufacturing	Entry: N/A Output: Plaintext	Plaintext
SWAK	Software Authentication Key (ECDSA P-256)	Validates the HSM Application firmware integrity on power-on	Loaded in Manufacturing	Entry: N/A Output: Plaintext	Plaintext
PAK	Parameter Authentication Key (ECDSA P-256)	Validated loaded Parameters	Loaded in Manufacturing	Entry: N/A Output: Plaintext	Plaintext
ECC-CDH Peer Public Key	ECC-CDH KAS Public counterpart received during the DH handshake	ECDH public counterpart received as part of the EC DH exchange.	Externally (Loaded during KAS-SSC)	Entry: Authenticated per 56A Output: N/A	Plaintext

Public Key	Description	Use	Establishment	Entry/Output	Storage
ECC-CDH Public Key	ECC-CDH KAS Public key generated during the DH handshake	ECDH public key transmitted as part of the EC DH exchange	Generated Internally	Entry: N/A Output: Plaintext	Plaintext
AK Public (Public Authentication Key)	DSA 2048 Public Key	Used to provide Authentication	Generated Internally by FIPS approved DRBG Or loaded as needed	Entry: Plaintext Output: Plaintext	Plaintext
	ECDSA P-224 or P-256 Public Key	Used to provide Authentication			
	RSA 2048 Public Key	Used to provide Authentication			
PK Public (Public Privacy Key)	RSA 2048 Public Key	Keys used to encrypt data	Generated Internally by FIPS approved DRBG Or loaded as needed	Entry: Plaintext Output: Plaintext	Plaintext
DPAG Public (DPAG Public Key)	RSA 2048 Public Key	Used to provide Authentication	Generated Internally by FIPS approved DRBG Or loaded as needed	Entry: Plaintext Output: Plaintext	Plaintext

7.4.3 ZEROIZATION

The module is a single-chip, cryptographic module that incorporates an Active Shield that provides a tamper detection and response mechanism. When this mechanism is triggered, the module immediately zeroizes the KEK, which renders all encrypted keys non-operational. The module transitions to a hard error state in which it must be returned to manufacturing.

Zeroization of the module can also be performed by the operator via the *Reinit* service.

8. SELF-TESTS

The module supports the following self-tests.

Power on self-tests (POSTs) can be run on demand by an unauthenticated operator by either power-cycling the module or via the *Reboot* service. Additionally, they may be executed via *Perform Diagnostic Test* or *Perform Full Diagnostics* services.

Upon the failure of any of the self-tests the module transitions to an error state. All data output via the data output interface is inhibited while in the error state. No cryptographic operations can be performed while in the error state. To transition from the error state the module must be power-cycled.

8.1 POWER ON SELF-TESTS

Firmware Integrity Tests:

The module conducts the following digital signature verifications on power-up.

- PB Bootloader
  - RSA 2048 (Cert. #C477) Digital Signature Verification
- HSM Application
  - ECDSA P-256 (Cert. #C476) Digital Signature Verification

Algorithm Tests:
The module conducts the following Known Answer Tests (KATs) and Pairwise Consistency Tests (PWCT) on power-up.

- AES (Cert. #5954)
  - AES-256 ECB Encrypt KAT
  - AES-256 ECB Decrypt KAT
  - AES-256 KW Encrypt KAT
  - AES-256 KW Decrypt KAT
- DRBG (Cert. #C472) [12]
  - Instantiate KAT
  - Generate KAT
- DSA (Cert. #C475)
  - 2048 Signature Generation and Verification PWCT
- ECDSA (Cert. #C476)
  - P-256 Signature Generation and Verification PWCT
- HMAC (Cert. #C464) and SHS (Cert. #C295)
  - HMAC-SHA-256 KAT
- Key Agreement: KAS-SSC (vendor affirmed, C(2e, 0s, ECC CDH)) and KDA (vendor affirmed)
  - Primitive "Z" Computation KAT
  - KDF KAT covered by HMAC-SHA-256 KAT
- RSA (Cert. #C477)
  - 2048 Signature Generation KAT
  - 2048 Signature Verification KAT

Critical Function Tests:
- RTC Test
- BRAM Pattern Test

8.2 CONDITIONAL TESTS

The module conducts the following conditional tests.

- NDRNG
  - Repetition Count Test (per IG 9.8)
- PWCT upon cryptographic key pair generation:
  - DSA 2048 PWCT
  - ECDSA P-224 or P-256 PWCT
  - RSA 2048 PWCT
- KAS-SSC (vendor affirmed, C(2e, 0s, ECC CDH))

[12] Per IG 9.8, the SP 800-90A-compliant DRBG does not perform the test described in AS.09.42 and AS.09.43

    - ECC Full Public Key Validation per SP 800-56Arev 3: 5.6.2.3.3
- Software/Firmware Load Test:
    - ECDSA P-256 Signature Verification (Cert. #C476)

APPENDIX A: REFERENCES

Table 11 – References

Reference Title	Publishing Entity	Publication Date
Digital Signature Standard (DSA) – FIPS PUB 186-4	NIST	July 2013
Advanced Encryption Standard (AES) – FIPS PUB 197	NIST	November 2001
The Keyed-Hash Message Authentication Code (HMAC) – FIPS PUB 198-1	NIST	July 2008
Secure Hash Standard – FIPS PUB 180-4	NIST	March 2012
Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography - Special Publication 800-56A Revision 3	NIST	April 2018
Recommendation for Key-Derivation Methods in Key-Establishment Schemes - Special Publication 800-56C Revision 1	NIST	April 2018
Recommendation for Block Cipher Modes of Operation, Methods and Techniques – Special Publication 800-38A	NIST	December 2001
Recommendation for Random Number Generation Using Deterministic Random Bit Generators – Special Publication 800-90A	NIST	January 2012
FIPS PUB 140-2, Security Requirements for Cryptographic Modules	NIST	May 2001
Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules	NIST	January 2011
FIPS PUB 140-2, Annex A – Approved Security Functions for FIPS PUB 140-2	NIST	January 2018
FIPS PUB 140-2, Annex B – Approved Protection Profiles for FIPS PUB 140-2	NIST	December 2016
FIPS PUB 140-2, Annex C – Approved Random Number Generators for FIPS PUB 140-2	NIST	January 2016
FIPS PUB 140-2, Annex D – Approved Key Establishment Techniques for FIPS PUB 140-2	NIST	May 2018
Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program	NIST	December 2019

APPENDIX B: ABBREVIATIONS AND DEFINITIONS

Table 12 – Abbreviations and Definitions

Term	Definition
AES	Advanced Encryption Standard
BRAM	Battery Backed RAM
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CO	Crypto Officer
CSP	Critical Security Parameters
CVL	Component Validation List
DAL	Device Abstraction Layer
DH	Diffie-Hellman
DRBG	Deterministic Random Bit Generator
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ECC CDH	Elliptic Curve Cryptography Cofactor Diffie-Hellman
EC-DH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
EFP	Environmental Failure Protection
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FIPS	Federal Information Processing Standards
HMAC	Hashed Message Authentication Code
HSM	Hardware Security Module
KAS	Key Agreement Scheme
KRA	Key Root Authority
NDRNG	Non-Deterministic Random Number Generator
NVM	Non-Volatile Memory
PB	Pitney Bowes
POST	Power-on Self-test
PSD	Postal Security Device
PSS	Probabilistic Signature Scheme
PVD	Postage Value Download
RAM	Random Access Memory

Term	Definition
ROM	Read-Only Memory
RSA	Rivest Shamir Adleman
RTC	Real Time Clock
SDU	Software Download Utility
SHA	Secure Hash Algorithm
SSC	Shared Secret Computation
SRAM	Static RAM