FP InovoLabs GmbH
Postal xRevenector US 2023

FIPS 140-3 Non-Proprietary Security Policy

Version 1.0

TABLE OF CONTENTS

1 General 6

1.1 Overview 6

1.2 Security Levels 6

2 Cryptographic Module Specification 7

2.1 Description 7

2.2 Tested and Vendor Affirmed Module Version and Identification 8

2.3 Excluded Components 9

2.4 Modes of Operation 9

2.5 Algorithms 10

2.6 Security Function Implementations 11

2.7 Algorithm Specific Information 15

2.8 RBG and Entropy 15

2.9 Key Generation 16

2.10 Key Establishment 16

2.11 Industry Protocols 16

3 Cryptographic Module Interfaces 17

3.1 Ports and Interfaces 17

4 Roles, Services, and Authentication 18

4.1 Authentication Methods 18

4.2 Roles 18

4.3 Approved Services 19

4.4 Non-Approved Services 30

4.5 External Software/Firmware Loaded 31

5 Software/Firmware Security 31

5.1 Integrity Techniques 31

5.2 Initiate on Demand 31

6 Operational Environment 31

6.1 Operational Environment Type and Requirements 31

7 Physical Security 32

7.1 Mechanisms and Actions Required 32

7.2 EFP/EFT Information 32

7.3 Hardness Testing Temperature Ranges 32
8 Non-Invasive Security 33
8.1 Mitigation Techniques 33
9 Sensitive Security Parameters Management 33
9.1 Storage Areas 33
9.2 SSP Input-Output Methods 33
9.3 SSP Zeroization Methods 34
9.4 SSPs 35
10 Self-Tests 42
10.1 Pre-Operational Self-Tests 42
10.2 Conditional Self-Tests 42
10.3 Periodic Self-Test Information 44
10.4 Error States 45
10.5 Operator Initiation of Self-Tests 46
11 Life-Cycle Assurance 46
11.1 Installation, Initialization, and Startup Procedures 46
11.2 Administrator Guidance 46
11.3 Non-Administrator Guidance 46
11.4 Design and Rules 46
11.5 End of Life 47
12 Mitigation of Other Attacks 47
12.1 Attack List 47
12.2 Mitigation Effectiveness 47
12.3 Guidance and Constraints 47

List of Tables

Table 1: Security Levels 6

Table 2: Tested Module Identification – Hardware 9

Table 3: Modes List and Description 9

Table 4: Approved Algorithms 10

Table 5: Vendor-Affirmed Algorithms 10

Table 6: Security Function Implementations 14

Table 7: Ports and Interfaces 17

Table 8: Authentication Methods 18

Table 9: Roles 18

Table 10: Approved Services 30

Table 11: Mechanisms and Actions Required 32

Table 12: EFP/EFT Information 32

Table 13: Hardness Testing Temperatures 32

Table 14: Storage Areas 33

Table 15: SSP Input-Output Methods 33

Table 16: SSP Zeroization Methods 34

Table 17: SSP Table 1 37

Table 18: SSP Table 2 41

Table 19: Pre-Operational Self-Tests 42

Table 20: Conditional Self-Tests 44

Table 21: Pre-Operational Periodic Information 44

Table 22: Conditional Periodic Information 45

Table 23: Error States 46

List of Figures

Figure 1 – Postal xRevenector US 2023 7

Figure 2: Block Diagram 8

1 GENERAL

1.1 OVERVIEW

This document forms a Cryptographic Module Security Policy for Francotyp Postalia's Postal xRevenector US 2023 Postal Security Device (PSD) under the terms of NIST FIPS 140-3.

The Postal xRevenector US 2023 is a Postal Security Device (PSD) designed and manufactured by FP InovoLabs GmbH for use in Postage Evidencing Systems (PES) produced by the Francotyp-Postalia group. PSDs perform the cryptographic and postal security functions required by the postage evidencing systems and protect both Sensitive Security Parameters (SSPs) and Postal Relevant Data Items (PRDIs) from unauthorized access.

This Security Policy specifies the security rules under which this device operates. It covers both the operation of the device's bootloader and its postal application, which has been designed to meet the requirements of the corresponding postal authority.

1.2 SECURITY LEVELS

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

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	3
	Overall Level	3

Table 1: Security Levels

2 CRYPTOGRAPHIC MODULE SPECIFICATION

2.1 DESCRIPTION

The Postal xRevenector US 2023 is illustrated in Figure 1 below. The device's cryptographic boundary is designated by the extent of the potted area.

Figure 1 – Postal xRevenector US 2023

The Postal xRevenector US 2023 is a multiple chip embedded cryptographic module, based around a cryptographic integrated circuit, together with a small number of support components. The components, mounted on a PCB, are covered by hard opaque potting material. The extent of the potting forms the cryptographic boundary of the module. The module has a proprietary electrical connector forming the interface to it. The module does not contain a modifiable operational environment. A block diagram of the module is shown in Figure 2 below.

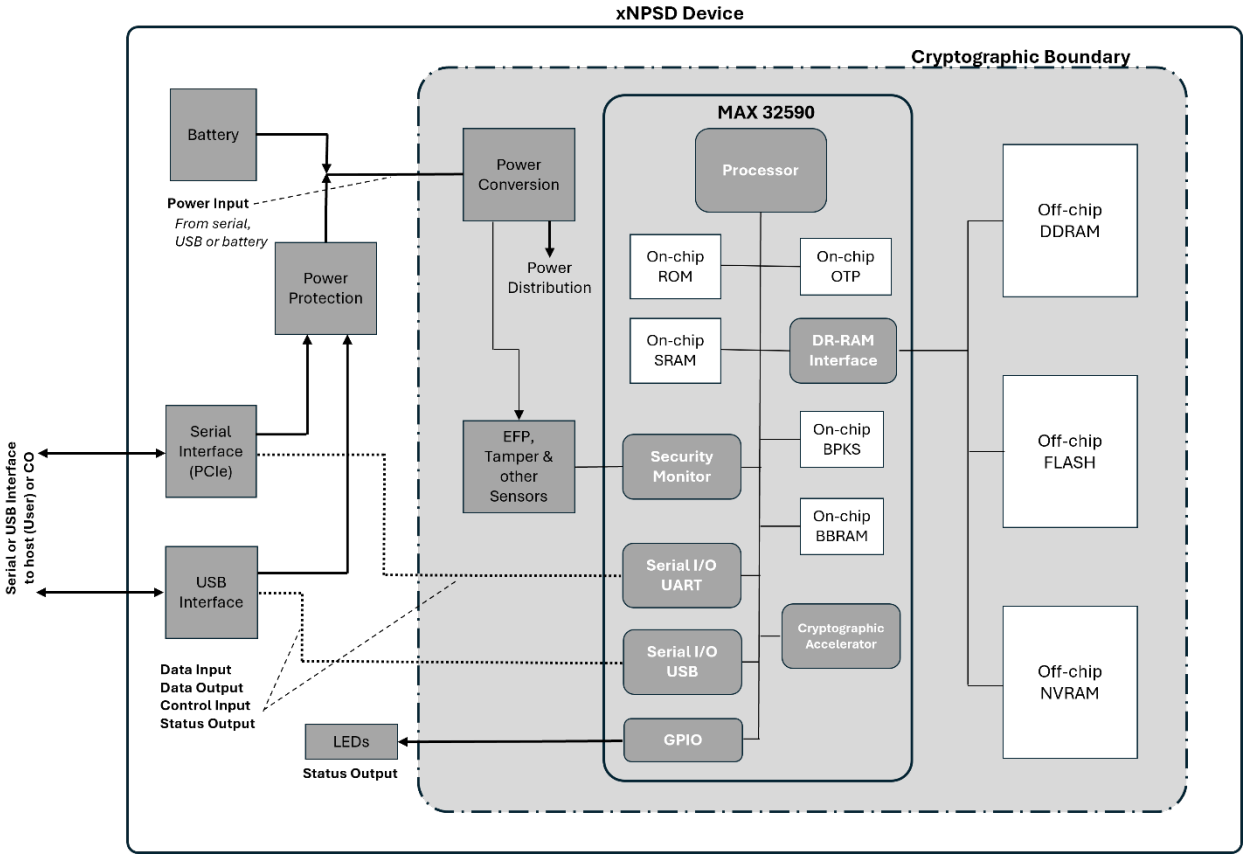

Figure 2: Block Diagram

Purpose and Use:

The module acts as the core security module with Postage Evidencing Systems (PES). It is responsible for producing digitally signed postage evidence in the form of an indicium. It secures financial registers and facilitates secure postal transactions.

Module Type: Hardware

The Postal xRevenector US 2023 is defined as hardware module (*refer to ISO/IEC 19790, Section 7.2.2*).

Module Embodiment: MultiChipEmbed

The Postal xRevenector US 2023 is a multiple chip embedded cryptographic module, based upon the Maxim Integrated MAX32590 DeepCover Secure Microcontroller together with a small number of other components.

Module Characteristics:

The critical components within the module are encapsulated inside a hard, opaque, production grade epoxy.

Cryptographic Boundary:

The cryptographic boundary is defined as the perimeter of the epoxy that encapsulates all the module's components on both sides of the printed circuit board (PCB).

2.2 TESTED AND VENDOR AFFIRMED MODULE VERSION AND IDENTIFICATION

The Postal xRevenector US 2023 cryptographic 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:

Tested Module Identification – Hardware:

Model and/or Part Number	Hardware Version	Firmware Version	Processors	Features
Postal xRevenector US 2023 (58.0036.0301.00)	1	90.0036.0616.00/2023.32.5.003	Maxim Integrated MAX32590 DeepCover Secure Microcontroller	Includes PCIe Interface only
Postal xRevenector US 2023 (58.0036.0302.00)	2	90.0036.0616.00/2023.32.5.003	Maxim Integrated MAX32590 DeepCover Secure Microcontroller	Includes USB and PCIe Interfaces

Table 2: Tested Module Identification – Hardware

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

The module does not exclude any components from the requirements of FIPS 140-3.

2.4 MODES OF OPERATION

Modes List and Description:

The module supports a single, approved mode of operation with only approved services. There are no non-approved modes, degraded modes, or non-approved services available to the module. Upon successful completion of the pre-operational and conditional self-tests on power-up, the module provides an indicator of the approved mode output to LEDs. Upon completion of each service an explicit, separate indicator is written to the module's event log (accessible via the module's 'Get Log Information' service) that indicates success or failure of each approved service.

Mode Name	Description	Type	Status Indicator
Approved Mode	The module incorporates a single, Approved mode of operation	Approved	LED

Table 3: Modes List and Description

The device will not respond to service calls before it has entered its approved mode of operation.

2.5 ALGORITHMS

The Postal xRevenector US 2023 cryptographic module supports the approved cryptographic algorithms shown in Table 4.

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

Algorithm	CAVP Cert	Properties	Reference
AES-CBC	A3256	-	SP 800-38A
AES-CTR	AES 5662	-	SP 800-38A
AES-ECB	A3256	-	SP 800-38A
AES-KW	A3257	-	SP 800-38F
Counter DRBG	A3939	-	SP 800-90A Rev. 1
DSA KeyGen (FIPS186-4)	A3259	-	FIPS 186-4
ECDSA KeyGen (FIPS186-4)	A3260	-	FIPS 186-4
ECDSA SigGen (FIPS186-4)	A3260	-	FIPS 186-4
ECDSA SigVer (FIPS186-4)	A3260	-	FIPS 186-4
HMAC-SHA2-256	A3262	-	FIPS 198-1
KAS-FFC-SSC Sp800-56Ar3	A3263	-	SP 800-56A Rev. 3
KDA OneStep Sp800-56Cr1	A3264	-	SP 800-56C Rev. 2
KDF SP800-108	A3938	-	SP 800-108 Rev. 1
RSA KeyGen (FIPS186-4)	A3265	-	FIPS 186-4
RSA SigGen (FIPS186-4)	A3265	-	FIPS 186-4
RSA SigVer (FIPS186-4)	A3265	-	FIPS 186-4
SHA2-256	A3267	-	FIPS 180-4

Table 4: Approved Algorithms

Vendor-Affirmed Algorithms:

The module supports the following vendor affirmed algorithms.

Name	Properties	Implementation	Reference
CKG	Key Type:Symmetric and Asymmetric	N/A	NIST SP 800-133r2 and IG D.G per Section 4 example 1, Sections 5.1, 5.2, and 6.1.

Table 5: Vendor-Affirmed Algorithms

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:

N/A for this module.

2.6 SECURITY FUNCTION IMPLEMENTATIONS

Name	Type	Description	Properties	Algorithms
CSP Decryption	BC-UnAuth	CSP Decryption in NVRAM	Key:128 Direction:Decrypt	AES-CTR: (AES 5662) Key Size: 128
CSP Encryption	BC-UnAuth	CSP encryption in NVRAM	Key:128 Direction:Encrypt	AES-CTR: (AES 5662) Key Size: 128
Data Decryption	BC-UnAuth	AES CBC Data Decryption	Key:128 Direction:Decrypt	AES-CBC: (A3256) Direction: Encrypt, Decrypt Key Size: 128
Data Encryption	BC-UnAuth	AES CBC Data Encryption	Key:128 Direction:Encrypt	AES-CBC: (A3256) Direction: Encrypt, Decrypt Key Size: 128
DRBG Generate Function	DRBG	NIST SP 800-90A CTR_DRBG generate function for delivering random bits on demand	Returned Bits:2048	Counter DRBG: (A3939) Mode: AES 128 Derivation Function: Enabled Prediction Resistance: Disabled AES-ECB: (A3256) Key Size: 128-bit
DSA Key Generation	AsymKeyPair-KeyGen CKG	DH Key Generation during KAS	L:2048 N:224	DSA KeyGen (FIPS186-4): (A3259) L: 2048 N: 224 CKG: () Key Type: Symmetric and Asymmetric

Name	Type	Description	Properties	Algorithms
ECDSA Key Generation	AsymKeyPair-KeyGen CKG	FIPS 186-4 ECDSA P-224 Key Generation	Curve:P-224	ECDSA KeyGen (FIPS186-4): (A3260) Curves: P-224, P256 Secret Generation Mode: Testing Candidates CKG: () Key Type: Symmetric and Asymmetric
ECDSA Signature Generation	DigSig-SigGen	FIPS 186-4 ECDSA P-224 digital signature generation of postal relevant data	Curve:P-224	ECDSA SigGen (FIPS186-4): (A3260) Curves: P-224, P-256 SHA2-256: (A3267)
ECDSA Signature Verification	DigSig-SigVer	FIPS 186-4 ECDSA P-224 digital signature verification	Curve:P-224	ECDSA SigVer (FIPS186-4): (A3260) Curves: P-224, P256 SHA2-256: (A3267)
Hash Function	SHA	SHA-256 data integrity for digital signatures	SHA:SHA-256	SHA2-256: (A3267) Message Length Min: 8 bits Message Length Max: 51200 bits
KAS (dhEphem C(2e, 0s, FFC DH))	KAS-Full	NIST SP 800-56Arev3. KAS-FFC per IG D.F Scenario 2 path (2)	IG:IG D.F Scenario 2, path 2, split Key confirmation:No Key derivation:KDA (separately tested) Caveat:Key establishment methodology provides 112 bits of security strength	KAS-FFC-SSC Sp800-56Ar3: (A3263) Scheme: Ephemeral Diffie Hellman KAS Role: Responder KDA OneStep Sp800-56Cr1: (A3264) Derived Key Length: 2048 Shared Secret Length: 2048
Key Based Key Derivation	KBKDF	NIST SP 800-108 Key Based Key Derivation used to derive authentication keys to authenticate		KDF SP800-108: (A3938) KDF Mode: Counter Min Length: 128 Max Length: 4096

Name	Type	Description	Properties	Algorithms
		Cryptographic Officer (Local) role		
Key Transport	KTS-Wrap	Key Transport using AES KW	Standard:SP800-38F IG D.G:Approved method from IG D.G Caveat:Key establishment methodology provides 112 bits of security strength	AES-KW: (A3257) Direction: Wrap, Unwrap Key Size: 128
Message Authentication	MAC	HMAC-SHA-256 used for authentication for secure sessions	Key:128	HMAC-SHA2-256: (A3262) Key Length Min: 128 bit Key Length Max: 512-bit
Seed DRBG	DRBG	Instantiate the DRBG	Entropy Input:256 bits Nonce:256 bits Personalization String:256 bits	Counter DRBG: (A3939) Prediction Resistance: Disabled Derivation Function: Enabled Mode: AES 128
SSP Encryption	BC-UnAuth	SSP encryption in NVRAM	Key:128	AES-CBC: (A3256) Key Size: 128-bit
RSA Key Generation	AsymKeyPair-KeyGen CKG	FIPS 186-4 RSA 2048 Key Generation	Key:2048	RSA KeyGen (FIPS186-4): (A3265) Key Generation Mode: B.3.3 Modulo: 2048 Hash Algorithm: SHA-256 Primality Tests: Table C.3 Private Key Format: Standard CKG: () Key Type: Symmetric and Asymmetric
RSA Signature Generation	DigSig-SigGen	FIPS 186-4 RSA 2048 Digital Signature Generation	Modulus:2048	RSA SigGen (FIPS186-4): (A3265) Signature Type:

Name	Type	Description	Properties	Algorithms
				PKCS1 v1.5 Modulo: 2048 SHA2-256: (A3267)
RSA Signature Verification (Auth)	DigSig-SigVer	FIPS 186-4 RSA 2048 digital signature verification used for authentication of the Cryptographic Officer (Remote)	Key:2048	RSA SigVer (FIPS186-4): (A3265) Signature Type: PKCS1 v1.5 Modulo: 2048 SHA2-256: (A3267)
RSA Sig Ver (FW Integrity - App)	DigSig-SigVer	FIPS 186-4 RSA 2048 digital signature verification used to verify the firmware integrity	Key:2048	RSA SigVer (FIPS186-4): (A3265) Signature Type: PKCS1 v1.5 Modulo: 2048 SHA2-256: (A3267)
RSA Sig Ver (FW Integrity - BL)	DigSig-SigVer	FIPS 186-4 RSA 2048 digital signature verification used to verify the firmware integrity	Signature Type:RSA PSS Key:2048	RSA SigVer (FIPS186-4): (A3265) Signature Type: RSA PSS Modulo: 2048 SHA2-256: (A3267)
RSA Sig Ver (FW Load Test)	DigSig-SigVer	FIPS 186-4 RSA 2048 digital signature verification used to verify the firmware during FW load	Key:2048 Signature Type:PKCS1 v1.5	RSA SigVer (FIPS186-4): (A3265) Signature Type: PKCS1 v1.5 Modulo: 2048 SHA2-256: (A3267)
SSP Authentication	MAC	Message authentication code applied to stored SSPs	Key:128	HMAC-SHA2-256: (A3262) Key Length: 128-bit
SSP Decryption	BC-UnAuth	SSP Decryption in NVRAM	Key:128	AES-CBC: (A3256) Key Size: 128-bit
Symmetric Key Generation	CKG	Symmetric Key Generation	Key:256 bit	CKG: () Key Type: Symmetric and Asymmetric

Table 6: Security Function Implementations

2.7 ALGORITHM SPECIFIC INFORMATION

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

The module complies with IG D.L Comment 2. A derivation function is used during a Counter DRBG (Cert. #A3939) instantiation. No reseeding is supported. The module does not contain an entropy source.

The module complies with IG D.M. All of the key derivation keys generated through KDF SP800-108 (Cert. #A3938) (i.e., Local Session Authentication Key (LSAK), Local Session Encryption Key (LSEK), Local Session Wrapping Key (LSWK)) are derived from the Local User Key (LUK), which in turn has been generated using an approved method, namely, Counter DRBG (Cert. #A3939) or CKG per NIST SP 800-133r2, in the approved mode. The encoding of the data fields (i.e., Label, Context, and Length L) is complaint to Section 6.4 of NIST SP 800-133r1. No asymmetric keys are generated through KBKDF.

The module complies with IG C.K. DSA KeyGen (Cert. #A3259) is used exclusively for KAS-FFC-SSC SP800-56Ar3 (Cert. #A3263). This usage is allowed per IG C.K Resolution 3. The strength of the DSA key pairs thus generated is 112 per NIST SP 800-57Part1r5, Section 5.6.1.1, Table 2. These DSA keys are ephemeral keys. No DSA static keys are generated.

For ECDSA KeyGen (FIPS 186-4) (Cert. #A3260), ECDSA SigGen (FIPS 186-4) (Cert. #A3260), ECDSA SigVer (FIPS 186-4) (Cert. #A3260), RSA KeyGen (FIPS186-4) (Cert. #A3265), RSA SigGen (FIPS186-4) (Cert. #A3265), and RSA SigVer (FIPS186-4) (Cert. #A3265), IG C.K Additional Comment 3 is applicable. Specifically, the validation date of January 30, 2023 preceded February 5, 2024. The CAVP tests conducted for the said certificates are mathematically identical to the FIPS 186-5 CAVP tests.

Compliance to SP 800-56Ar3 assurances:

For KAS-FFC, the module satisfies IG D.F Scenario 2 path (2). The key derivation functions comply with NIST SP 800-56Cr2 (i.e., KDA NIST SP 800-56Cr2 (Cert. #A3264)). Furthermore, the module obtained the appropriate assurances, as required in Sections 5.6.2 of NIST SP 800-56Ar3. Full public key validation (NIST SP 800-56Ar3 Section 5.6.2.3.1) is implemented. No key confirmation is implemented.

2.8 RBG AND ENTROPY

The module incorporates a NIST SP 800-90A CTR-DRBG (Cert. #A3939) that is seeded during manufacturing with an Entropy String, a nonce, and a personalization string of length 256 bits each. Entropy of 112 bits is claimed of only the Entropy String. The unmodified output of the DRBG is used for generating cryptographic key material or random nonces. The module's source of randomness corresponds to IG 9.3.A scenario 2(a), i.e., the module is a hardware module that passively receives the entropy from an entropy source outside the TOEPP.

The claimed minimum number of bits of loaded entropy is 112. The entropy source is provided by FP InovoLabs infrastructure during device manufacturing. The caller of the module shall ensure that the entropy input provided has a minimum of 112 bits of entropy.

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

2.9 KEY GENERATION

The module generates symmetric cryptographic keys in conformance with NIST SP 800-133r2 using a NIST SP 800-90A conforming DRBG (Cert. #A3939) for the encryption and protection of data and cryptographic keys. The module generates asymmetric cryptographic key pairs in conformance with FIPS 186-4 for the generation or verification of digital signature, or for the facilitation of key agreement in conformance with NIST SP 800-56ar3.

2.10 KEY ESTABLISHMENT

The module supports the establishment of cryptographic keys using Finite Field Cryptography (FFC) ephemeral Diffie Hellman (DH) in conformance with NIST SP 800-56ar3. The module implements KAS-FFC-SSC per NIST SP 800-56A Rev3 (Cert. #A3263) Model C (2e, 0s, FFC DH) using DSA KeyGen (Cert. #A3259), used in conjunction with KDA per NIST SP 800-56Cr2 (Cert. #A3264). Key establishment methodology provides at least 112 bits of encryption strength. This is used to establish secure communication sessions.

2.11 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 physical ports are defined within Table 7 below and include the primary communication serial ports:

- 36-Pin Serial I/O card edge connector (PCIe x1)
- USB (micro-USB)

There is also an optical interface leading from the module to LEDs that provides operational state of the module.

Physical Port	Logical Interface(s)	Data That Passes
36-pin Serial I/O card edge connector (PCIe)	Data Input Data Output Control Input Status Output Power	Primary (PCIe) serial interface for communicating with module.
USB	Data Input Data Output Control Input Status Output Power	Alternate interface for communicating with module.
LED Interface	Status Output	Module status
Battery	Power	Additional power

Table 7: Ports and Interfaces

4 ROLES, SERVICES, AND AUTHENTICATION

4.1 AUTHENTICATION METHODS

The module supports authentication methods for the Cryptographic Officer roles. These roles have separate authentication methods as indicated in Table 8.

Method Name	Description	Security Mechanism	Strength Each Attempt	Strength per Minute
Local Login	Identity-based. Allows the Cryptographic Officer (Local) to authenticate to the module. Sets up a local session with host.	Challenge response mechanism.	128 bits	A delay of 1 second is added after any failed login attempt, resulting in a maximum of 60 attempts per minute. The probability of a successful random attempt per minute is therefore 60/2^128, which is less than 1/1,000,000.
Remote Login	Identity-based. Allows the Cryptographic Officer (Remote) to authenticate themselves. Sets up a remote session with CO.	RSA SigVer (FIPS186-4) (A3265)	112 bits	A delay of 1 second is added after any failed login attempt, resulting in a maximum of 60 attempts per minute. The probability of a successful random attempt per minute is therefore 60/2^112, which is less than 1/100,000.

Table 8: Authentication Methods

4.2 ROLES

Name	Type	Operator Type	Authentication Methods
Cryptographic Officer (Remote)	Identity	Cryptographic Officer	Remote Login
Cryptographic Officer (Local)	Identity	Cryptographic Officer	Local Login
User	Role	Unauthenticated	None

Table 9: Roles

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

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Accounting	Debits the postal funds and returns indicia content.	Event Log	Postal data to be digitally signed	Digitally signed data stream	ECDSA Signature Generation Hash Function CSP Decryption SSP Decryption SSP Authentication	Cryptographic Officer (Local) - Indicia Signing Key : E - Local Session Authentication Key (LSAK): E - Local Session Encryption Key (LSEK): E - Master Key Encryption Key (MKEK): E - Data Encryption Key (NVDEK): E - Data Authentication Key (NVDAK): E
Dump Memory	Dumps memory contents to a log file.	Event Log	Memory parameters	Memory data	None	User
Echo	Echoes back data payload	Service response	Input pattern	Output pattern	None	User
Generate Indicia Keypair	Generating the Indicia Signing Key and Indicia Verifying Key	Event Log	Key ID, Key Expiration	Key Version #, Public Key	ECDSA Key Generation DRBG Generate Function CSP Decryption SSP Encryption	Cryptographic Officer (Remote) - Indicia Signing Key : G - Indicia Verifying Key: G - Remote Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					SSP Authentication	Authentication Key (RSAK): E - DRBG State: G,E - Data Encryption Key (NVDEK): E - Data Authentication Key (NVDAK): E - Master Key Encryption Key (MKEK): E
Generate PSV Keypair	Generating PSV Keypair	Event Log	Key ID, Key Expiration	Key Version #, Public Key	ECDSA Key Generation DRBG Generate Function CSP Decryption SSP Encryption SSP Authentication	Cryptographic Officer (Remote) - PSV Signing Key: G - PSV Verifying Key: G - Remote Session Authentication Key (RSAK): E - DRBG State: G,E - Data Encryption Key (NVDEK): E - Data Authentication Key (NVDAK): E - Master Key Encryption Key (MKEK): E
Get Device Status	Gets module status information	Service response	Required status data	Module information, status and versioning	None	User
Get Certificate Information	Retrieves certificate data	Service response	Required certificate data	Certificate data (X509 format)	None	User

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Get Log Information	Reads log data	Service response	Log Information	Log record data	None	User
Instantiate DRBG	Loads entropy and seeds DRBG	Event Log	Entropy string	Entropy size	Seed DRBG	Cryptographic Officer (Remote) - Entropy String: W - DRBG State: G - DRBG Seed: G - Master Key Encryption Key (MKEK): E - Data Encryption Key (NVDEK): G - Data Authentication Key (NVDAK): G
Load Firmware	Receives firmware from an external source and programs it into the cryptographic module's FLASH memory	Event Log	Digitally signed firmware	Status	Message Authentication RSA Sig Ver (FW Load Test)	Cryptographic Officer (Local) - Local Session Authentication Key (LSAK): E - Firmware Verification Key: E
Local Login	Authenticates the Cryptographic Officer (Local) using a challenge-response protocol	Event Log	User ID, Response to challenge	Device Info, Nonce, Role ID	DRBG Generate Function Key Based Key Derivation Message Authentication CSP Decryption	Cryptographic Officer (Local) - Local Session Authentication Key (LSAK): G - Local Session Encryption Key (LSEK): G - Local Session Wrapping Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(LSWK): G,E - Local User Key (LUK): E - Master Key Encryption Key (MKEK): E
Lockout	Changes the state in the postage lifecycle	Event Log	None	Status	None	User
Logoff	Logout function for CO	RFU LED, Event Log	None	Status	None	Cryptographic Officer (Remote) - Remote Session Authentication Key (RSAK): Z - Remote Session Encryption Key (RSEK): Z - Remote Session Wrapping Key (RSWK): Z Cryptographic Officer (Local) - Local Session Authentication Key (LSAK): Z - Local Session Encryption Key (LSEK): Z - Local Session Wrapping Key (LSWK): Z

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Postage Value Download (PVD)	Finance service required to load funds	Event Log, Postal Registers	Postage value data	Postage value response data	RSA Signature Generation Message Authentication RSA Signature Verification (Auth) Data Encryption CSP Decryption Data Decryption SSP Decryption SSP Authentication	Cryptographic Officer (Remote) - Remote Session Authentication Key (RSAK): E - Remote Session Encryption Key (RSEK): E - Master Key Encryption Key (MKEK): E - Data Encryption Key (NVDEK): E - Data Authentication Key (NVDAK): E - PKMCert: E - PSD Private Key: E
Postage Value Refund	Finance service managing postal funds	Event Log, Postal Registers	Postage refund data	Postage refund response data	RSA Signature Generation Message Authentication RSA Signature Verification (Auth) Data Encryption CSP Decryption Data Decryption SSP Decryption SSP Authentication	Cryptographic Officer (Remote) - Remote Session Authentication Key (RSAK): E - Remote Session Encryption Key (RSEK): E - Master Key Encryption Key (MKEK): E - Data Encryption Key (NVDEK): E - Data

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Key (NVDAK): E - PSD Private Key: E - PKMCert: E
Postal Authorization	Authorize the device according to the USPS - Intelligent Mail Indicia - Performance Criteria requirements	Event Log	Postal data	Postal data	Message Authentication	Cryptographic Officer (Remote) - Remote Session Authentication Key (RSAK): E
Postal Initialization	Initialize the device according to the USPS - Intelligent Mail Indicia - Performance Criteria requirements	Event Log	Signed certificate	Certificate request	DRBG Generate Function RSA Key Generation Message Authentication CSP Encryption SSP Encryption SSP Authentication	Cryptographic Officer (Remote) - PSD Private Key: G - Remote Session Authentication Key (RSAK): E - DRBG State: G,E - Data Encryption Key (NVDEK): E - Transport Signing Key: E - Transport Verifying Key: E - Data Authentication Key (NVDAK): E - Master Key Encryption Key (MKEK): E
Re-Authorization	Updates customer configuration data	Event Log	Postal data	Status	Message Authentication	Cryptographic Officer (Remote) - Remote Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Key (RSAK): E
Reboot Device	Reboots the module	Event Log	None	Status	None	Cryptographic Officer (Remote) Cryptographic Officer (Local) User
ReKey Local User Key	Sets up an individual key between the module and host	Event Log	Encrypted local user key	Encrypted local user key, Nonce	DRBG Generate Function Symmetric Key Generation Message Authentication Key Transport CSP Encryption	Cryptographic Officer (Local) - Local User Key (LUK): G,Z - Local Session Authentication Key (LSAK): E - Local Session Wrapping Key (LSWK): E - Master Key Encryption Key (MKEK): E
Rekey PSD Key	Generation of a new PSD Key Pair and exchange with infrastructure	Event Log	Signed Certificate	Certificate Request	DRBG Generate Function RSA Key Generation Message Authentication CSP Decryption SSP Encryption SSP Authentication	Cryptographic Officer (Remote) - PSD Private Key: G,Z - PSD Public Key: G,Z - Remote Session Authentication Key (RSAK): E - DRBG State: G,E - Data Encryption Key (NVDEK): E - Data

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						Authentication Key (NVDAK): E - Master Key Encryption Key (MKEK): E
Remote Login	Cryptographic Officer (Remote) login service	Event Log	PSD-Name, Random Bits, Domain parameters, CO-DH-public-key, Signature	CO-Name, Random Bits, Domain parameters, Module-DH-public-key, Signature	KAS (dhEphem C(2e, 0s, FFC DH)) DRBG Generate Function Hash Function RSA Signature Generation DSA Key Generation RSA Signature Verification (Auth) CSP Decryption SSP Decryption SSP Authentication	Cryptographic Officer (Remote) - Ephemeral Diffie-Hellman Client (Private) Key: G,Z - Transport Signing Key: E - PSD Private Key: E - Remote Session Authentication Key (RSAK): G - Remote Session Encryption Key (RSEK): G - Remote Session Wrapping Key (RSWK): G - DRBG State: G,E - Ephemeral Diffie-Hellman Client (Public) Key: G,R,Z - Ephemeral Diffie-Hellman Server (Public) Key: W,E,Z - PKMCert: E - Shared Secret: G,E

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
Renew PKM Key	Load signed PKM certificate	Event Log	Signed certificate	Certificate Request	RSA Signature Verification (Auth)	Cryptographic Officer (Remote) - PKMCert: W,E,Z
Scrap	Zeroizes all plaintext CSPs	Event Log	None	Status	None	Cryptographic Officer (Local) - Master Key Encryption Key (MKEK): Z - Data Encryption Key (NVDEK): Z - Data Authentication Key (NVDAK): Z - DRBG State: Z - Local User Key (LUK): Z User - Master Key Encryption Key (MKEK): Z - Data Encryption Key (NVDEK): Z - Data Authentication Key (NVDAK): Z - DRBG State: Z - Local User Key (LUK): Z
Secure Echo	Echoes back data payload within a secure session	Event Log	Encrypted data, MAC	Encrypted data, MAC	Message Authentication Data Encryption Data Decryption	Cryptographic Officer (Remote) - Remote Session Authentication Key

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
						(RSAK): E - Remote Session Encryption Key (RSEK): E Cryptographic Officer (Local) - Local Session Authentication Key (LSAK): E - Local Session Encryption Key (LSEK): E
Secure Get Status	Provides status within a secure session	Event Log	Status data	Module information, status and versioning	Message Authentication	Cryptographic Officer (Remote) - Remote Session Authentication Key (RSAK): E
Secure Set Time	Synchronizes the RTC within a secure session	Event Log	Time data	Status	Message Authentication	Cryptographic Officer (Remote) - Remote Session Authentication Key (RSAK): E
Self-Test	Runs all self-tests (Pre-operational and Conditional)	Event Log	None	Status	RSA Sig Ver (FW Integrity - App) RSA Sig Ver (FW Integrity - BL)	User
Set Meter Parameter	Enters postal config data	Event Log	Postal configuration data	Status	None	User
Sign PMD Data	Sign postal related items and communication data	Event Log	Postal data	Digital signature	Hash Function RSA Signature Generation	Cryptographic Officer (Local) - Local Session

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Message Authentication Data Encryption CSP Decryption Data Decryption SSP Decryption SSP Authentication	Authentication Key (LSAK): E - Local Session Encryption Key (LSEK): E - PMD Signing Key: E - Master Key Encryption Key (MKEK): E - Data Encryption Key (NVDEK): E - Data Authentication Key (NVDAK): E
Sign PSV Data	Signs postal related data for storage in hosts PSD Secured Vault	Event Log	Postal data	Digital signature	ECDSA Signature Generation Hash Function Message Authentication CSP Decryption SSP Decryption SSP Authentication	Cryptographic Officer (Local) - PSV Signing Key: E - Local Session Authentication Key (LSAK): E - DRBG State: G,E
Setup Parameters	Enters other postal-related data	Event Log	Postal data	Status	None	Cryptographic Officer (Local) - Local Session Authentication Key (LSAK): E User
Verify PSV Data	Verify postal related items stored (using Public PSV Key)	Event Log	Postal data, digital signature	Status (true or false)	Hash Function ECDSA Signature Verification	Cryptographic Officer (Local) - PSV Verifying Key:

Name	Description	Indicator	Inputs	Outputs	Security Functions	SSP Access
					Message Authentication CSP Decryption SSP Decryption SSP Authentication	E - Local Session Authentication Key (LSAK): E
Re-Initialization	Initialize the device according to the USPS - Intelligent Mail Indicia - Performance Criteria requirements	Event Log	Postal data	Status	Message Authentication	Cryptographic Officer (Remote) - Remote Session Authentication Key (RSAK): E

Table 10: Approved Services

4.4 NON-APPROVED SERVICES

N/A for this module.

4.5 EXTERNAL SOFTWARE/FIRMWARE LOADED

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

The postal application firmware is signed by FP, with a signature of form RSA-2048-SHA-256-PKCS #1 V1.5. On downloading, the device verifies the firmware, including: the type, version, CRC and signature of the new firmware package. On loading the firmware for execution, the signature is verified again by the FP Bootloader.

5 SOFTWARE/FIRMWARE SECURITY

5.1 INTEGRITY TECHNIQUES

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

- Bootloader - RSA 2048 RSA-PSS digital signature verification using an FP Customer Root Key
- Postal Application - RSA 2048 PKCS1 v1.5 digital signature verification using the Firmware Verification Key

The module will transition to its error state upon the failure of either firmware integrity test. Both public verification keys are non-SSP. The pre-calculated digital signatures for the Bootloader and the Postal Application are stored in the FLASH memory within the cryptographic module boundary.

5.2 INITIATE ON DEMAND

The module's pre-operational FW integrity tests can be initiated on demand via the 'Self-Test' service.

6 OPERATIONAL ENVIRONMENT

6.1 OPERATIONAL ENVIRONMENT TYPE AND REQUIREMENTS

Type of Operational Environment: Limited

How Requirements are Satisfied:

The module operational environment is defined as limited. The module has the ability to load its firmware from Flash memory. Only the firmware versions identified on the module's validation certificate are included in the scope of this validation. Any other firmware loaded onto the module is not validated and would require a separate FIPS 140-3 validation.

7 PHYSICAL SECURITY

All the components within the cryptographic boundary of the device are covered with a hard, tamper-evident potting material, which is tamper evident and opaque within the visible spectrum, deterring direct observation, probing, and manipulation. The module is inspected for tamper evidence each time it is retrieved from the field. Because of the potting material it is not possible to physically access any internal components without seriously damaging the module or causing zeroization. Hardness testing has been performed at ambient temperature and at the extremes of the module's operating, storage and distribution temperature ranges.

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 FP.

Mechanism	Inspection Frequency	Inspection Guidance
Tamper Evidence	During installation, re-installation, decommissioning, and servicing.	Inspect device for obvious damage or other evidence of tamper.

Table 11: Mechanisms and Actions Required

7.2 EFP/EFT INFORMATION

The module supports Environmental Failure Protection (EFP) mechanisms for high/low voltage and temperature extremes (refer to Table 12).

Temp/Voltage Type	Temperature or Voltage	EFP or EFT	Result
LowTemperature	-35°C	EFP	Zeroization
HighTemperature	70°C	EFP	The module shuts down
LowVoltage	3.7V	EFP	The module shuts down
HighVoltage	6.1V	EFP	The module shuts down

Table 12: EFP/EFT Information

7.3 HARDNESS TESTING TEMPERATURE RANGES

The module supports and has been tested at the operation, storage and distribution temperatures listed in Table 13. The module's epoxy hardness is assured within these ranges.

Temperature Type	Temperature
LowTemperature	-25°C
HighTemperature	70°C

Table 13: Hardness Testing Temperatures

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 Data Encryption Key is encrypted with the Data Encryption Master Key and is rendered inaccessible when this is zeroized. All other stored CSPs are encrypted with the Data Encryption Key and are rendered inaccessible when this is zeroized.

The AES-KW key-wrapping algorithm is used to protect any CSPs that are input or output. Only a single CSP, the Local User Key, is input or output and this is wrapped for transport using the AES-KW key-wrapping algorithm with the Local Session Wrapping Key (LSWK).

Storage Area Name	Description	Persistence Type
Battery Protected Key Storage (BPKS)	On-chip memory that is zeroized on tamper detection.	Static
Battery Backed RAM (BBRAM)	Plaintext and encrypted	Static
FLASH	Plaintext	Static
NVRAM	Plaintext and encrypted	Static
SRAM	Plaintext	Static

Table 14: Storage Areas

9.2 SSP INPUT-OUTPUT METHODS

Name	From	To	Format Type	Distribution Type	Entry Type	SFI or Algorithm
Manufacturing	Manufacturing	SRAM	Plaintext	N/A	Electronic	
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))

Table 15: SSP Input-Output Methods

9.3 SSP ZEROIZATION METHODS

The zeroization methods described within Table 16 are supported by the module. Zeroization services explicitly overwrite SSPs with zero values.

Zeroization Method	Description	Rationale	Operator Initiation
Scrap	Service	Forces a zeroisation of the Master Key Encryption Key (MKEK) 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 zeroisation of the Master 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

Table 16: SSP Zeroization Methods

9.4 SSPS

The following two tables list the SSPs used in the module. The tables include a non-SSP, namely Firmware Verification Key, used for integrity verification of the Postal Application.

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Data Authentication Key (NVDAK)	Authenticate internally stored CSPs	128-bit - 112-bit	Symmetric Key - CSP	DRBG Generate Function Symmetric Key Generation		SSP Authentication
Data Encryption Key (NVDEK)	Encrypt and decrypt internally stored CSPs	128-bit - 112-bit	Symmetric Key - CSP	DRBG Generate Function Symmetric Key Generation		SSP Encryption SSP Decryption
DRBG Seed	Instantiate the DRBG	768-bit - 112-bit	Entropy - CSP	Seed DRBG		Seed DRBG
DRBG State	Key and V	N/A - N/A	N/A - CSP	DRBG Generate Function		DRBG Generate Function
Entropy String	Instantiate the DRBG	256-bit - 112-bit	Entropy - CSP	Externally		Seed DRBG
Ephemeral Diffie-Hellman Client (Private) Key	Private DH Key used during KAS	224-bit - 112-bit	Asymmetric Private Key - CSP	DSA Key Generation		KAS (dhEphem C(2e, 0s, FFC DH))
Ephemeral Diffie-Hellman Client (Public) Key	Public DH Key used during KAS	2048 - 112-bit	Asymmetric Public Key - PSP	DSA Key Generation		KAS (dhEphem C(2e, 0s, FFC DH))
Ephemeral Diffie-Hellman Server (Public) Key	Server's Public DH Key imported during KAS	2048 - 112-bit	Asymmetric Public Key - PSP	Externally		KAS (dhEphem C(2e, 0s, FFC DH))

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
Firmware Verification Key	Firmware verification key for RSA PKCS#1 V1.5 signature verification (Non-SSP)	2048-bit - 112-bit	Asymmetric Public Key - PSP	Externally		RSA Sig Ver (FW Load Test)
Indicia Signing Key	Indicia Signing Key	P-224 - 112-bit	Asymmetric Private Key - CSP	ECDSA Key Generation		ECDSA Signature Generation
Indicia Verifying Key	Indicia Verifying Key	P-224 - 112-bit	Asymmetric Public Key - PSP	ECDSA Key Generation		ECDSA Signature Verification
Local Session Authentication Key (LSAK)	Authentication of data transfer in a local secure session	128-bit - 112-bit	Symmetric Key - CSP	Externally	Key Based Key Derivation	Message Authentication
Local Session Encryption Key (LSEK)	Authentication of data transfer in a local secure session (User role)	128-bit - 112-bit	Symmetric Key - CSP	Externally	Key Based Key Derivation	Data Encryption
Local Session Wrapping Key (LSWK)	Securing CSP data transfer in a local secure session (User role)	128-bit - 112-bit	Symmetric Key - CSP	Externally	Key Based Key Derivation	Key Transport
Local User Key (LUK)	Cryptographic Officer (Local) authentication key	256-bit - 112-bit	Symmetric Key - CSP	DRBG Generate Function Symmetric Key Generation		Key Based Key Derivation
Master Key Encryption Key (MKEK)	Encrypt and decrypt CSPs	128-bit - 112-bit	Symmetric Key - CSP	DRBG Generate Function Symmetric Key Generation		CSP Encryption CSP Decryption
PKMCert	PKMCert	2048-bit - 112-bit	Asymmetric Public Key - PSP	Externally		RSA Signature Verification (Auth)
PMD Signing Key	RSA PKCS#1 V1.5	2048-bit - 112-bit	Asymmetric Private Key - CSP	RSA Key Generation		RSA Key Generation

Name	Description	Size - Strength	Type - Category	Generated By	Established By	Used By
PSD Private Key	RSA PKCS#1 V1.5	2048-bit - 112-bit	Asymmetric Private Key - CSP	RSA Key Generation		RSA Signature Generation
PSD Public Key	RSA PKCS#1 V1.5	2048-bit - 112-bit	Asymmetric Public Key - PSP	RSA Key Generation		RSA Signature Verification (Auth)
PSV Signing Key	PSV Signing Key	P-224 - 112-bit	Asymmetric Private Key - CSP	ECDSA Key Generation		ECDSA Signature Generation
PSV Verifying Key	PSV Verifying Key	P-224 - 112-bit	Asymmetric Public Key - PSP	ECDSA Key Generation		ECDSA Signature Verification
Remote Session Authentication Key (RSAK)	Encryption of data transfer in a remote secure session	128-bit - 112-bit	Symmetric Key - CSP	Externally	KAS (dhEphem C(2e, 0s, FFC DH))	Message Authentication
Remote Session Encryption Key (RSEK)	Encryption of data transfer in a remote secure session	128-bit - 112-bit	Symmetric Key - CSP	Externally	KAS (dhEphem C(2e, 0s, FFC DH))	Data Encryption
Remote Session Wrapping Key (RSWK)	Securing CSP data transfer in a remote secure session	128-bit - 112-bit	Symmetric Key - CSP	Externally	KAS (dhEphem C(2e, 0s, FFC DH))	Key Transport
Shared Secret	Shared Secret	2048-bit - 112-bit	Shared Secret - CSP	KAS (dhEphem C(2e, 0s, FFC DH))		KAS (dhEphem C(2e, 0s, FFC DH))
Transport Signing Key	RSA PKCS#1 V1.5	2048-bit - 112-bit	Asymmetric Private - CSP	RSA Key Generation		RSA Signature Generation
Transport Verifying Key	RSA PKCS#1 V1.5	2048-bit - 112-bit	Asymmetric Public Key - PSP	RSA Key Generation		RSA Signature Verification (Auth)

Table 17: SSP Table 1

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Data Authentication Key (NVDAK)		Battery Backed RAM (BBRAM):Encrypted		Scrap Removal of Battery/Tamper	Data Encryption Key (NVDEK):Used With Master Key Encryption Key (MKEK):Encrypted By
Data Encryption Key (NVDEK)		Battery Backed RAM (BBRAM):Encrypted		Scrap Removal of Battery/Tamper	Transport Signing Key:Encrypts Transport Verifying Key:Encrypts PMD Signing Key:Encrypts PSD Private Key:Encrypts PSD Public Key:Encrypts Indicia Signing Key :Encrypts Indicia Verifying Key:Encrypts PSV Signing Key:Encrypts PSV Verifying Key:Encrypts Master Key Encryption Key (MKEK):Encrypted By
DRBG Seed		Battery Backed RAM (BBRAM):Encrypted		Automatically	Entropy String:Derived From
DRBG State		Battery Backed RAM (BBRAM):Encrypted		Scrap Removal of Battery/Tamper	DRBG Seed:Derived From Master Key Encryption Key (MKEK):Encrypted By
Entropy String	Manufacturing	SRAM:Plaintext		Automatically	DRBG Seed:Derives
Ephemeral Diffie-Hellman Client (Private) Key		SRAM:Plaintext	Persists only for the life of the Key Agreement process	End of session	Ephemeral Diffie-Hellman Client (Public) Key:Paired With Shared Secret:Derives

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Ephemeral Diffie-Hellman Client (Public) Key	Output (Plaintext)	SRAM:Plaintext	Persists only for the life of the Key Agreement process	End of session	Ephemeral Diffie-Hellman Client (Private) Key:Paired With
Ephemeral Diffie-Hellman Server (Public) Key	Input (Plaintext)	SRAM:Plaintext	Persists only for the life of the Key Agreement process	End of session	Shared Secret:Derives
Firmware Verification Key	Manufacturing	FLASH:Plaintext		Automatically	
Indicia Signing Key		NVRAM:Encrypted		Automatically	Indicia Verifying Key:Paired With Data Encryption Key (NVDEK):Encrypted By
Indicia Verifying Key		NVRAM:Encrypted		Automatically	Indicia Signing Key :Paired With Data Encryption Key (NVDEK):Encrypted By
Local Session Authentication Key (LSAK)		SRAM:Plaintext	Persists only for the life of the active Cryptographic Officer (Local) session	End of session	Local User Key (LUK):Derived From
Local Session Encryption Key (LSEK)		SRAM:Plaintext	Persists only for the life of the active Cryptographic Officer (Local) session	End of session	Local User Key (LUK):Derived From
Local Session Wrapping Key (LSWK)		SRAM:Plaintext	Persists only for the life of the active Cryptographic Officer (Local) session	End of session	Local User Key (LUK):Derived From
Local User Key (LUK)	Manufacturing Output (Encrypted)	Battery Backed RAM (BBRAM):Encrypted		Automatically	Local Session Authentication Key (LSAK):Derives Local Session Encryption Key (LSEK):Derives Local Session Wrapping Key

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
					(LSWK):Derives Master Key Encryption Key (MKEK):Encrypted By
Master Key Encryption Key (MKEK)		Battery Protected Key Storage (BPKS):Plaintext		Scrap Removal of Battery/Tamper	Data Encryption Key (NVDEK):Encrypts Data Authentication Key (NVDAK):Encrypts DRBG State:Encrypts Local User Key (LUK):Encrypts
PKMCert	Manufacturing Input (Plaintext)	NVRAM:Plaintext		Automatically	Data Encryption Key (NVDEK):Encrypted By
PMD Signing Key		NVRAM:Encrypted		Automatically	Data Encryption Key (NVDEK):Encrypted By
PSD Private Key		NVRAM:Encrypted		Automatically	PSD Public Key:Paired With Data Encryption Key (NVDEK):Encrypted By
PSD Public Key		NVRAM:Encrypted		Automatically	PSD Private Key:Paired With Data Encryption Key (NVDEK):Encrypted By
PSV Signing Key		NVRAM:Encrypted		Automatically	PSV Verifying Key:Paired With Data Encryption Key (NVDEK):Encrypted By
PSV Verifying Key		NVRAM:Encrypted		Automatically	PSV Signing Key:Paired With Data Encryption Key (NVDEK):Encrypted By
Remote Session Authentication Key (RSAK)		SRAM:Plaintext	Persists only for the life of the active Cryptographic Officer (Remote) session	End of session	Shared Secret:Derived From

Name	Input - Output	Storage	Storage Duration	Zeroization	Related SSPs
Remote Session Encryption Key (RSEK)		SRAM:Plaintext	Persists only for the life of the active Cryptographic Officer (Remote) session	End of session	Shared Secret:Derived From
Remote Session Wrapping Key (RSWK)		SRAM:Plaintext	Persists only for the life of the active Cryptographic Officer (Remote) session	End of session	Shared Secret:Derived From
Shared Secret		SRAM:Plaintext		Automatically	Remote Session Authentication Key (RSAK):Derives Remote Session Encryption Key (RSEK):Derives Remote Session Wrapping Key (RSWK):Derives Ephemeral Diffie-Hellman Client (Private) Key:Derived From Ephemeral Diffie-Hellman Server (Public) Key:Derived From
Transport Signing Key		NVRAM:Encrypted		Automatically	Transport Verifying Key:Paired With Data Encryption Key (NVDEK):Encrypted By
Transport Verifying Key		NVRAM:Plaintext		Automatically	Transport Signing Key:Paired With Data Encryption Key (NVDEK):Encrypted By

Table 18: SSP Table 2

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 self-tests being performed, the module performs the required known answer test (KAT) on the RSA implementation.

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details
Application Firmware Integrity Test	2048 bits	KAT	SW/FW Integrity	LED	RSA-PKCS1 v1.5 Signature Verification
Bootloader Firmware Integrity Test	2048 bits	KAT	SW/FW Integrity	LED	RSA-PSS Signature Verification

Table 19: Pre-Operational Self-Tests

10.2 CONDITIONAL SELF-TESTS

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

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-CBC Encrypt (A3256)	128-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Encrypt KAT	Power-up, Periodically & on-demand
AES-CBC Decrypt (A3256)	128-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Decrypt KAT	Power-up, Periodically & on-demand
AES-ECB Encrypt (A3256)	128-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Encrypt KAT	Power-up, Periodically & on-demand
AES-ECB Decrypt (A3256)	128-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Decrypt KAT	Power-up, Periodically & on-demand
AES-KW Encrypt (A3257)	128-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Encrypt KAT	Power-up, Periodically & on-demand

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
AES-KW Decrypt (A3257)	128-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Decrypt KAT	Power-up, Periodically & on-demand
Counter DRBG (A3939)	N/A	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Instantiate and Generate KAT	Power-up, Periodically & on-demand
DSA KeyGen (FIPS186-4) (A3259)	2048-bit	PCT	PCT	Success or Failure written to Event Log	PCT	DH Key Generation
ECDSA SigGen (FIPS186-4) (A3260)	P-224	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Signature Generation KAT	Power-up, Periodically & on-demand
ECDSA SigVer (FIPS186-4) (A3260)	P-224	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Signature Verification KAT	Power-up, Periodically & on-demand
ECDSA KeyGen (FIPS186-4) (A3260)	P-224	PCT	PCT	Success or Failure written to Event Log. ERR LED illuminates on error.	PCT	ECDSA Key Generation
HMAC-SHA2-256 (A3262)	256-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	HMAC Generation KAT	Power-up, Periodically & on-demand
KDF SP800-108 (A3938)	256-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	Key Based KDF Generation KAT	Power-up, Periodically & on-demand
KDA OneStep Sp800-56Cr1 (A3264)	2048-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	KDA KAT	Power-up, Periodically & on-demand
KAS-FFC-SSC Sp800-56Ar3 (A3263)	2048-bit	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	KAS-SSC KAT	Power-up, Periodically & on-demand
RSA KeyGen (FIPS186-4) (A3265)	2048 bits	PCT	PCT	Success or Failure written to Event Log. ERR LED illuminates on error.	RSA Key Gen	RSA Key Generation

Algorithm or Test	Test Properties	Test Method	Test Type	Indicator	Details	Conditions
RSA SigGen (FIPS186-4) (A3265)	2048 bits	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	RSA Signature Generation KAT	Power-up, Periodically & on-demand
RSA SigVer (FIPS186-4) (A3265)	2048 bits	KAT	CAST	Success or Failure written to Event Log. ERR LED illuminates on error.	RSA Signature Verification KAT	Power-up, Periodically & on-demand

Table 20: Conditional Self-Tests

Note:

- The 'Get Device Status' service provides self-test status.
- Conditional tests are performed at power up, on-demand (via the 'Self-Test' service) and periodically.

10.3 PERIODIC SELF-TEST INFORMATION

The running of a periodic self-test is indicated by an extended response time for the first message when running the Local- or Remote Login services. This can be confirmed later by a self-test timestamp available via the 'Get Device Status' service.

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
Application Firmware Integrity Test	KAT	SW/FW Integrity	<=90 days	Automatically
Bootloader Firmware Integrity Test	KAT	SW/FW Integrity	On demand	On Demand - Conforms with IG 10.3.E Resolution 3C.

Table 21: Pre-Operational Periodic Information

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-CBC Encrypt (A3256)	KAT	CAST	<=90 days	Automatically
AES-CBC Decrypt (A3256)	KAT	CAST	<=90 days	Automatically
AES-ECB Encrypt (A3256)	KAT	CAST	<=90 days	Automatically
AES-ECB Decrypt (A3256)	KAT	CAST	<=90 days	Automatically
AES-KW Encrypt (A3257)	KAT	CAST	<=90 days	Automatically

Algorithm or Test	Test Method	Test Type	Period	Periodic Method
AES-KW Decrypt (A3257)	KAT	CAST	<=90 days	Automatically
Counter DRBG (A3939)	KAT	CAST	<=90 days	Automatically
DSA KeyGen (FIPS186-4) (A3259)	PCT	PCT	N/A	Programmatically - Upon Key Generation
ECDSA SigGen (FIPS186-4) (A3260)	KAT	CAST	<=90 days	Automatically
ECDSA SigVer (FIPS186-4) (A3260)	KAT	CAST	<=90 days	Automatically
ECDSA KeyGen (FIPS186-4) (A3260)	PCT	PCT	N/A	Programmatically - Upon Key Generation
HMAC-SHA2-256 (A3262)	KAT	CAST	<=90 days	Automatically
KDF SP800-108 (A3938)	KAT	CAST	<=90 days	Automatically
KDA OneStep Sp800-56Cr1 (A3264)	KAT	CAST	<=90 days	Automatically
KAS-FFC-SSC Sp800-56Ar3 (A3263)	KAT	CAST	<=90 days	Automatically
RSA KeyGen (FIPS186-4) (A3265)	PCT	PCT	N/A	Programmatically - Upon Key Generation
RSA SigGen (FIPS186-4) (A3265)	KAT	CAST	<=90 days	Automatically
RSA SigVer (FIPS186-4) (A3265)	KAT	CAST	<=90 days	Automatically

Table 22: Conditional Periodic Information

10.4 ERROR STATES

On entering an error state, the module will output a signal to illuminate the ERR LED (Status Output). The reason for the error is obtainable using the 'Get Device Status' service. All data via the data output interface is inhibited whilst within an error state. No cryptographic functions are available whilst the module is in an error state.

Name	Description	Conditions	Recovery Method	Indicator
Defect (Hard Error)	Non recoverable error	Fatal error caused by self-test failure Fatal error caused by physical tamper e.g. removal of battery	Non recoverable error	LED (Red)
Soft Error	Recoverable Error	General Application errors	Power-cycle	LED (Yellow)

Table 23: Error States

10.5 OPERATOR INITIATION OF SELF-TESTS

Self-tests may be triggered by the user using the 'Self-Test' service, which allows either individual or all tests to be run.

11 LIFE-CYCLE ASSURANCE

There are no specific maintenance requirements. Care should be taken to ensure that the device is not left without an external source of power for more than 10 years.

11.1 INSTALLATION, INITIALIZATION, AND STARTUP PROCEDURES

The module is initialized within FP manufacturing and installed into an FP 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 FP customers as part of a postage evidencing system. Administration guidance, in the form of API definitions, exists for FP 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.

The Postal xRevenector US 2023

1. Supports only an Approved mode of operation. The Approved mode indicator is returned via the 'Get Device Status' service or by examining the module status LEDs.
2. Does not allow unauthenticated operators to have any access to the module's cryptographic services.
3. Inhibits data output during self-tests, firmware load, zeroization and error states.
4. Logically disconnects data output from the processes performing zeroization and key generation.

5. Excludes the overwriting of an unprotected SSP with another unprotected SSP for zeroization.
6. Enforces identity-based authentication for roles that access approved algorithms and CSPs.
7. Does not retain the authentication of an operator following power-off or reboot.
8. Supports the following roles: Cryptographic Officer (Remote), Cryptographic Officer (Local) and User.
9. Does not permit the input or output of plaintext cryptographic keys or other CSPs.
10. Does not support a bypass mode or maintenance mode.
11. Supports the following logically distinct interfaces:
    - Data input interface
    - Data output interface
    - Control input interface
    - Status output interface
    - Power interface
12. Implements all firmware using a high-level language, except the limited use of low-level languages to enhance performance.
13. Protects critical security parameters from unauthorized disclosure, modification and substitution.
14. Provides means to ensure that a key entered into or stored within the module is associated with the correct entities to which the key is assigned.
15. Supports an approved deterministic random bit generator (DRBG) as specified in NIST SP 800-90A section 10.2.1.
16. Performs self-tests as listed in Section 10 during power-on and on-demand when the corresponding service is used.
17. Stores an error indication whenever an error state is entered.
18. Does not perform any cryptographic functions while in an error state.
19. Does not support multiple concurrent operators.

11.5 END OF LIFE

Upon end of life, the module is withdrawn from service and returned to FP manufacturing for decommissioning, redeployment or scrapping. At the end of the device's life, the Scrap service should be run.

12 MITIGATION OF OTHER ATTACKS

12.1 ATTACK LIST

The module incorporates additional protections against removing the module's epoxy to gain access to the underlying components via a tamper detection and response mechanism. The module zeroizes all plaintext SSPs upon tamper detection.

12.2 MITIGATION EFFECTIVENESS

The module will zeroize all SSPs upon the removal of its epoxy. The module will transition to a permanent error state.

12.3 GUIDANCE AND CONSTRAINTS

Upon a physical tamper event, the module will zeroize all SSPs and will transition to a permanent error state.