INFORMATION-BASED INDICIA PROGRAM (IBIP)

PERFORMANCE CRITERIA FOR INFORMATION-BASED INDICIA AND SECURITY ARCHITECTURE FOR CLOSED IBI POSTAGE METERING SYSTEMS

(PCIBI-C)

UNITED STATES
POSTAL SERVICE

January 12, 1999

The United States Postal Service (USPS)

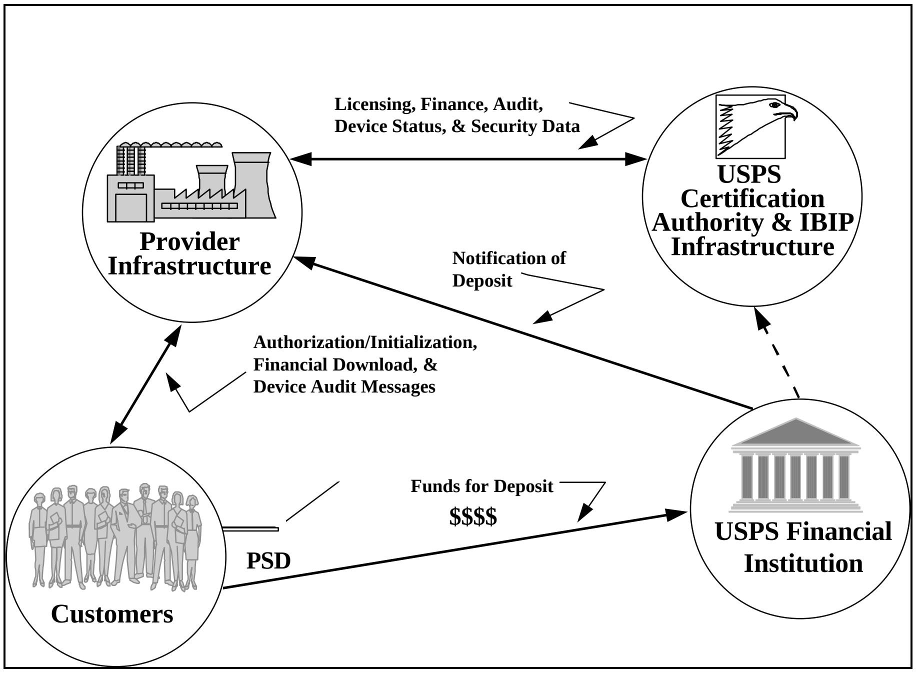
Introduction

The United States Postal Service (USPS) initiated the Information-Based Indicia Program (IBIP) to enhance the security of postage metering by supporting new methods of applying postage to mail. This document, "Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems (PCIBI-C)," defines the requirements for the Closed System elements of IBIP. A Closed System is a system whose basic components are dedicated to the production of information-based indicia and related functions, similar to an existing, traditional postage meter. A Closed System, which may be a proprietary device used alone or in conjunction with other closely related, specialized equipment, includes the indicia print mechanism.

System Overview

From a system context, IBIP is designed to support customer, Product/Service Provider ("Provider"), and USPS operations. The IBIP architecture will support differing implementations by various Providers and customers of the functions identified in this document.

The target IBIP functions and their interactions are shown in the accompanying figure. The customer authorization and initialization process is expected to be supported by both Providers and the USPS. Under current USPS regulations, postage payments are sent from customers directly to the USPS (via its cash management processor). Only information will flow between customers and Providers, and between Providers and the USPS. Postage payment processes and the resulting PSD (Postal Security Device) postage value download process shall be performed by authenticated electronic means between the USPS, Providers, and customers. The USPS Certificate Authority may provide the authentication for these electronic transactions.


Licensing, Finance, Audit,
Device Status, & Security Data
Provider Infrastructure
USPS Certification Authority & IBIP Infrastructure
Notification of Deposit
Authorization/Initialization, Financial Download, & Device Audit Messages
Funds for Deposit
$$$$
PSD
Customers
USPS Financial Institution

Target System Architecture

Structure of the Performance Criteria

The “Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems (PCIBI-C)” is composed of four major parts. The parts correspond to the sections of the previously released “Performance Criteria for Information-Based Indicia and Security Architecture for IBI Postage Metering Systems (PCIBISAIBIPMS),” Draft, namely: Indicium, Postal Security Device, Host System, and Key Management Plan. The current document organizes all of the relevant IBIP performance criteria needed for a Provider to participate in the IBIP program for Closed Systems. The following overview describes each of the parts:

- **Part A — PCIBI-C Indicium:** This section of the PCIBI-C defines the requirements for the indicium (i.e., postage mark) to be applied to mail produced by Closed Systems of the Information-Based Indicia Program.
- **Part B — PCIBI-C Postal Security Device (PSD):** This section of the PCIBI-C defines the requirements for a Postal Security Device (PSD) that shall provide security services to support the creation of the new indicium to be applied to mail using a Closed System.
- **Part C — PCIBI-C User Interface:** This section of the PCIBI-C is reserved.
- **Part D — PCIBI-C Key Management Plan:** This section of the PCIBI-C is reserved.

Parts A through D are followed by an Acronym List and a Glossary.

Interpretation of Requirements

The requirements presented in this document are composed of statements containing the words “shall” or “must.” Requirements using the words “shall” or “must” are mandatory. Other statements use the words “should” or “may.” Statements using the word “should” are recommendations; statements using the word “may” are design-related or functional options to consider for implementation purposes.

Reference Documents and Resources

The proposed requirements and performance criteria included in this document are supported by a number of published resources. A summary of the primary resources supporting this document follows:

- **Federal Register,** Vol. 63, No. 170, pages 46719–46728, September 2, 1998, “Proposed Rule on Manufacture, Distribution, and Use of Postal Security Devices and Information-Based Indicia,” 39 CFR Parts 111 and 502.
- **“Performance Criteria for Information-Based Indicia and Security Architecture for IBI Postage Metering Systems (PCIBISAIBIPMS),” Draft,** August 19, 1998.
- **USPS Domestic Mail Manual** (DMM), Issue 53, January 1, 1998.
- “Uniform Symbology Specification PDF417,” July 1994.

- “Digital Signature Standard — FIPS PUB 186,” May 19, 1994 and Change 1, December 30, 1996.
- “Secure Hash Standard — FIPS PUB 180-1,” April 17, 1995.
- “PKCS #1: RSA Encryption Standard,” Version 1.5, December 1, 1993.
- “ANSI X9.62, Elliptic Curve Digital Signature Algorithm Standard (ECDSA),” Working Draft, January 15, 1997.
- “Security Requirements for Cryptographic Modules — FIPS PUB 140-1,” January 11, 1994.
- “Cryptographic Module Validation Program Announcement,” July 17, 1995.
- “Coding Accuracy Support System, AMS-II, Technical Guide,” March 1996.
- “ISO/IEC 9594-8 (1995). Information Technology — Open Systems Interconnection — The Directory: Authentication Framework.”
- “PKCS #10: Certification Request Syntax Standard, An RSA Laboratories Technical Note,” Version 1.0, December 1993.
- Publication 25, *Designing Letter Mail*, August 1995
- “Directory Authentication Framework Recommendation X.509”

Intellectual Property and License Considerations

Requirements contained in this document may be subject to intellectual property claims by various individuals or organizations. It shall be the responsibility of the Provider to obtain required rights, such as licenses. It shall be the responsibility of the Provider to indemnify and hold harmless the USPS with respect to intellectual property rights of third parties.

Part

A

Indicium

TABLE OF CONTENTS

A.1 INTRODUCTION TO INDICIUM PERFORMANCE CRITERIA

A.1.1 Introduction

This part of the PCIBI-C defines the requirements for the indicium to be applied to mail produced by Closed Systems of the Information-Based Indicia Program (IBIP). The indicium shall consist of a two-dimensional (2 D) barcode and certain human-readable information. The barcode format for the indicium shall be the PDF417 barcode or any other USPS-approved 2 D barcode standard. The information required in the barcode and human-readable portions of the indicium is defined in this part. Providers and customers will have some flexibility in the appearance of the indicium, provided that the basic requirements contained in these performance criteria are satisfied.

The indicium will provide the following features:

- Printing Technology Alternatives — The new indicium will support a number of printing technology alternatives (e.g., laser, inkjet, thermal).
- Machine Readable — Through the use of a two-dimensional barcode, the new indicium shall be readable using automated equipment.
- Standard Ink — The new indicium no longer requires the special fluorescent ink required for current postage meter indicia, and may be printed using standard black ink or toner, provided it meets reflectance standards defined in Section A.5. However, a facing identification mark (FIM) shall be required on the mailpiece if a fluorescent ink meeting USPS requirements is not used.
- Fraud Mitigation — The new indicium will support various fraud mitigation strategies that will be incorporated into the overall IBIP security architecture. These strategies require an increased amount of information as compared with that provided by current indicia.
- Support for Future Services — The new indicium offers the flexibility to provide support for new services that the USPS may wish to offer its customers in the future. (These performance criteria do not specifically provide for these services.)

The IBIP is expected to support new methods of applying postage in lieu of the current approach that typically relies on a postage meter mechanically printing the indicium on a mailpiece. In general, these new methods will involve the use of a user interface and printer to create and print the indicia on mailpieces, envelopes, or labels.

A.1.2 Overview of Indicium Performance Criteria

The remainder of this part is organized as shown below. The following presents an overview and general description of each of the remaining sections:

- **Section A.2 — Indicium Data Contents:** This section specifies the human-readable and barcode data. This section also identifies the data formats, output characteristics, and order of the data elements within the indicium.
- **Section A.3 — Special Purpose Indicia:** This section specifies the requirements for special purpose indicia for postage correction and postage redate.

- **Section A.4 — Digital Signature Requirements:** This section documents the various approaches for providing a digital signature within the indicium.
- **Section A.5 — Indicium Design Requirements:** This section addresses the sizing and placement of the indicium on a mailpiece. Readability requirements (e.g., reflectivity) also appear in this section.

A.2 INDICIUM DATA CONTENTS

The proposed indicium shall consist of both human-readable and barcode data. The human-readable information shall show the minimum information as specified in DMM P030.4.6. The barcoded information shall meet the requirements for IBIP specified in this section. The following paragraphs detail the data elements included in the indicium. Their formats, output characteristics, and the order of the data elements within the indicium are specified in Table A-1. Two additional indicia types to address special cases are Redate and Postage Correction indicia. The data content for these special purpose indicia is discussed in Section A.3. Barcode data shall include machine-readable ASCII format, as well as binary format in the case of the digital signature.

It is the intent of the USPS to support multiple cryptographic digital signature algorithms. As necessary to support Provider implementations, the USPS will support use of the Digital Signature Algorithm (DSA), Rivest Shamir Adleman (RSA) Algorithm, and the Elliptic Curve Digital Signature Algorithm (ECDSA) systems to generate the digital signature for the indicium. The length of the digital signature field depends on the choice of signature algorithm, as shown in Table A-1. DES and RSA, as encryption techniques, shall not be used in indicia.

Table A-1. Indicium Data Elements

Data Elements	Barcode Data	Human-Readable Data	Length (bytes)	Field Number
Indicia Version Number	Yes	No	1	1
Algorithm ID	Yes	No	1	2
Certificate Serial Number	Yes	No	4	3
Device ID				
- PSD Manufacturer ID	Yes	Yes	2	4
- PSD Model ID	Yes	Yes	2	5
- PSD Serial Number	Yes	Yes	4	6
Ascending Register	Yes	No	5	7
Postage	Yes	Yes	3	8
Date of Mailing	Yes	Yes	4	9
Originating Address:				
- City, State, ZIP Code	No	Yes	---	---
- Licensing ZIP Code	Yes	No	4	10
Reserved Field 1	Yes	No	5	11
Software ID	Yes	No	6	12
Descending Register	Yes	No	4	13
Rate Category	Yes	No	4	14
Digital Signature	Yes	No	DSA 40 RSA 128 ECDSA 40	15
Reserve Field 2	Yes	No	Variable Size	16

The data elements listed in Table A-1 shall be included in the indicium. The format of each human-readable data element shall be as specified in the DMM. These required elements are:

- **Indicia Version Number** — This data element represents the version number assigned by the USPS to this indicia data set. It shall be represented by a 1-byte binary value.
- **Algorithm ID —** This data element identifies the digital signature algorithm used to create the digital signature on the indicium. It shall be represented by a 1-byte binary value.
- **Certificate Serial Number** — This data element represents the unique serial number of the PSD certificate issued by the IBIP Certificate Authority. It shall be represented by a 4-byte binary value.
- **Device ID: PSD Manufacturer ID** — This field represents the USPS-assigned 2 character ID for each Provider. The data shall be ASCII text.
- **Device ID: PSD Model ID** — This field represents the Provider's 2 character assigned model number for this PSD. This model number is furnished by the Provider and approved by the USPS. The data shall be ASCII text with the first character being numeric (0 to 9) and the second alpha (A to Z).
- **Device ID: PSD Serial Number** — This field represents the serial number assigned by the Provider to the given PSD. The data shall be represented by a 4-byte binary value.
- **Ascending Register** — This data element represents the total monetary value of all indicia ever produced by the PSD. The data shall be represented in a 5-byte binary value.
- **Postage —** This data element represents the amount of postage applied for this specific mailpiece. Postage applied is in accordance with then current USPS postage rates and DMM. The postage amount shall be represented in a 3-byte binary value in the numeric format XX.XXX. This field size supports any valid postage amount that is less than US$ 100.00.
- **Date of Mailing** — This data element represents the date of mailing for a mailpiece. The date of mailing shall be represented in a 4-byte binary value and has the numeric format YYYYMMDD in the barcode. The format of the date in the human-readable portion of the indicium is at the discretion of the Provider, except for the year, which shall be represented by 4 digits.
- **Originating Address: City, State, ZIP Code —** This field represents the city, state and 5-digit ZIP Code for the licensing post office. The indicium may display the ZIP Code rather than the city/state designation. In this case, the words "Mailed From ZIP Code" and the mailer's delivery address ZIP Code must appear in place of the city designation and state, respectively.

- **Originating Address: Licensing ZIP Code —** This data element represents the licensing delivery point identification. The format shall be a 5-digit numeric value represented by a 4-byte binary value in the indicium.
- **Reserved Field 1 —** This field in the indicium is included to preserve congruence between the Open System and Closed System indicia. This binary field shall be 5 bytes with a zero value each.
- **Software ID —** This data element represents the host system software 12-digit identification number. It shall be represented by a 6-byte binary value.
- **Descending Register** — This data element represents the postage value remaining on the PSD. It shall be represented as a 4-byte binary value.
- **Rate Category —** This data element represents the postage class, including any presort discount level, and rate. Values for this field are provided by the USPS. This shall be a 4-byte alphanumeric ASCII value.
- **Digital Signature** — This data element represents the digital signature. The size of this data element is a function of the digital signature algorithm. If additional algorithms are approved for use by USPS, in addition to those shown in Table A-1, the length of this field will be appropriately specified for those algorithms.
- **Reserve Field 2** — This field is included to allow for the future addition of data to the indicium. The field size shall be variable based upon the data content. The field shall have an ASCII value of zero.

The data that comprises the indicium must be input from either the PSD, the host application/user interface, or by the customer. The Provider shall obtain the necessary values for the indicia version number, algorithm ID, and software ID fields from the USPS. The licensing ZIP Code shall be assigned as part of the USPS licensing process.

A.3 SPECIAL PURPOSE INDICIA

In addition to the standard mailpiece indicium discussed in Section A.2, two additional indicia, Redate and Postage Correction indicia, may be required to address special cases. The requirements for these special purpose indicia are specified in Sections A.3.1 and A.3.2 below.

A.3.1 Redate Indicium

A complete and accurate date shall be printed on the mailpiece. The complete date shall include the year, month and day. The date of the indicium shall represent the actual date of deposit of the mailpiece. An exception to this would be a case where mail deposited after the day's last scheduled collection would bear the next scheduled collection date. In some cases, a correction of the date may be needed. In order to correct the date, the following data shall be included, in human-readable format only, on the mailpiece: the corrected date and the word "REDATE." The complete date shall include the month, day, and year with the year being represented as 4 digits. There is no barcode portion in the redate indicium. The location of the redate indicium is specified in the DMM.

A.3.2 Postage Correction Indicium

The correct postage value shall be included in both the human-readable and barcode portion of the mailpiece indicium. Therefore, if additional postage is to be added, a postage correction indicium shall be placed on the mailpiece. The postage correction indicium shall contain both barcode and human-readable information. The data elements shall be the same as for the regular indicium, as specified in Table A-1. The location of the postage correction indicium on the mailpiece is specified in the DMM.

A.4 DIGITAL SIGNATURE REQUIREMENTS

A.4.1 Introduction

The digital signature required for the indicium is specified in this section. A digital signature shall be created by the PSD for each mailpiece and shall be placed in the digital signature field of the barcode. Multiple digital signature algorithms will be supported by the IBIP. Providers are at liberty to choose the digital signature algorithm most appropriate for their product. As of the date of these performance criteria, the IBIP supports the following algorithms:

- Digital Signature Algorithm (DSA)
- Rivest Shamir Adleman (RSA) Algorithm
- Elliptic Curve Digital Signature Algorithm (ECDSA)

If other digital signature algorithms are proposed, they will be considered by the USPS in accordance with the requirements in section A.4.5. It shall be the responsibility of the Provider to obtain any required rights from third parties, such as licenses, to use the approach chosen.

A.4.2 Digital Signature Algorithm (DSA) Approach

One approach to providing the digital signature is the Digital Signature Standard (DSS), which incorporates the DSA algorithm, as specified in FIPS PUB 186. For a detailed discussion of the DSA signature creation and verification processes, see Part B, Postal Security Device.

A.4.3 RSA Signature Approach

Another method for digital signature generation is by means of an algorithm known as the RSA algorithm, in accordance with PKCS #1: RSA Encryption Standard version 1.5, dated December 1, 1993. For a detailed discussion of the RSA signature creation and verification processes, see Part B, Postal Security Device.

A.4.4 Elliptic Curve Digital Signature Algorithm Approach

Another approach to providing the signature functionality is to use the Elliptic Curve Digital Signature Algorithm (ECDSA), as specified in ANSI X9.62 Standard (Working Draft), Elliptic Curve Digital Signature Algorithm. For a detailed discussion of the ECDSA signature creation and verification processes, see Part B, Postal Security Device.

A.4.5 Other Digital Signature Methods

Digital, public-key signature methods, other than those addressed in these performance criteria, will be considered by the USPS if:

- The proposed method is shown to have a cryptographic strength equal to or greater than approaches delineated in these performance criteria.
- The proposed method can be supported by the planned USPS infrastructure with minimal or no increase in cost.
- The proposed method meets industry standards.

A.5 INDICIUM DESIGN REQUIREMENTS

This section addresses the requirements for the composition, position, printing resolution, error detection and correction, design layout, and reflectance standards for the indicium.

A.5.1 Indicium Composition

The following requirements address design-related issues concerning the composition of the indicium:

- The indicium shall consist of both human-readable information and barcoded information in accordance with the requirements specified in Section A.2, Indicium Data Contents.
- The human-readable information shall consist of, at a minimum, the Device ID (comprising the PSD Manufacture ID, PSD Model ID, and PSD Serial Number); the amount of the applied postage; the date of mailing; and the city, state, and 5-digit ZIP Code of the licensing post office. The indicium may display the ZIP Code rather than the city/state designation. In this case, the words “Mailed From ZIP Code” and the mailer’s delivery address ZIP Code must appear in place of the city designation and state, respectively.
- The human-readable portion of the indicium shall be in accordance with DMM P030.1.8, Documentation and Marking; P030.4.13, Other Matter Printed on Meter Stamps; and P030.4.14, Postal Markings. These requirements also provide guidelines for including postal markings and slogans as part of the mailpiece.
- The barcode region of the indicium shall be in accordance with the USPS-approved symbology.

A.5.2 Indicium Position

The requirements for positioning of the indicium on the mailpiece are applicable to mailpieces meeting the dimensions as specified in DMM C800, Automation-Compatible Mail, as follows:

- The indicium shall be printed or applied on the upper-right corner of the mailpiece, address label, or tag. It shall have a minimum distance of 1/4" from the right edge of the mailpiece and 1/4" from the top edge of the mailpiece. The barcode portion of the indicium shall be horizontally oriented.
- The positioning of the indicium shall not infringe on the areas allocated for the FIM or optical character reader (OCR) processing. As a reference, the general guidelines defining the dimensions for the FIM clear zones are detailed in DMM S922 and Publication 25, *Designing Letter Mail*. General guidelines defining the dimensions for the OCR read area are contained in DMM C830.
- If a FIM is printed with the indicium, the requirements for FIM type and placement are in accordance with the DMM.

A.5.3 Indicium Printing

The minimum printing resolution for the barcode portion of the indicium shall be 200 dots per inch. Readability of the barcode portion of the indicia must assure a minimum USPS acceptance rate of 99.5%. For PDF417, a minimum 15 mil feature size shall be used for the “x” dimension. No dimension of the barcode portion of the indicium shall exceed 4 inches.

A.5.4 Error Detection and Correction

By adding error correction code words to the data message, the PDF417 symbology supports the detection and correction of lost or missing data. This symbology provides selectable levels of error protection by adding from 2 to 512 error correction code words. The error correction level shall be chosen to achieve a minimum USPS acceptance rate of 99.5%. The error correction code word level shall be a minimum of Level 4 as specified in the Uniform Symbology Specification PDF417. A higher error correction level shall be selected if needed to achieve the required USPS acceptance rate. If a USPS-approved symbology other than PDF417 is chosen, an equivalent level of error correction shall be applied by the chosen symbology.

A.5.5 Indicium Design Layout

The specific design layout of the indicium is at the discretion of the Provider. However, the indicium design shall conform to the guidelines as contained in DMM P030.4, Meter Stamps. All indicia used in IBIP must be preapproved by the Manager, Metering Technology Management.

A.5.6 Reflectance Standards

The requirements for the minimal standards for achieving acceptable reflectance measurements concerning the indicium and the background material shall be as specified in the Uniform Symbology Specification PDF417. If a symbology other than PDF417 is chosen, the requirements for the minimal standards for achieving acceptable reflectance measurements and the background material shall be as specified in the Uniform Symbology Specification of the chosen symbology. In addition, the mailpiece is required to meet USPS reflectance standards, as specified in the DMM, section C840.5.

Part

B

Postal Security Device (PSD)

TABLE OF CONTENTS

B.1 INTRODUCTION TO POSTAL SECURITY DEVICE (PSD) PERFORMANCE CRITERIA

B.1.1 Introduction

This part of the PCIBI-C defines the requirements for a Postal Security Device (PSD) to provide security services to support the creation of the new IBIP Closed System indicium.

The IBIP supports new methods of applying postage. The term “host” is used in these performance criteria to refer to the user interface.

B.1.2 Overview of Postal Security Device Performance Criteria

This part is organized as shown below. The following is an overview and general description of each of the remaining sections.

- **Section B.2 — PSD Overview:** This section presents an overview of PSD functions.
- **Section B.3 — PSD Functional Requirements:** This section specifies the PSD core functions, including initialization, digital signature, and register management. This section also describes the role that the PSD plays in IBIP-specific functions including device authorization, finance, indicium creation, and device audit.
- **Section B.4 — PSD Physical Requirements:** This section documents the physical requirements for the PSD. It covers PSD security, contents, internal storage, software, watchdog timer, tamper resistance, access control, key handling, and input/output requirements.
- **Section B.5 — PSD Testing Requirements:** This section specifies the test requirements for the PSD.

B.2 POSTAL SECURITY DEVICE (PSD) OVERVIEW

The Postal Security Device (PSD) provides security-critical functions for IBIP. The PSD shall be a hardware component and each PSD shall be a unique security device. The PSD core security functions are PSD initialization, cryptographic digital signature generation and verification, and the secure management of the registers that track the remaining amount of money available for indicium creation (descending register) and the total postage value used by this PSD (ascending register). To ensure the security of IBIP processes, these core security functions, which are further described in Section B.2.1, must be performed by the PSD. In order to perform these functions securely, the PSD shall be a tamper-resistant device that shall contain an internal random number generator, various storage registers, a date/time clock, and other circuits necessary to perform these functions. See section B.4 for details. The PSD shall be compliant with FIPS 140-1, as described in Section B.4.1. Compliance shall be validated through the National Institute of Standards and Technology (NIST) Computer Systems Laboratory's Cryptographic Module Validation Program. Additionally, the PSD shall be compliant with USPS criteria as detailed in this document. Where there are conflicts between FIPS standards and USPS criteria, the USPS criteria take precedence.

The PSD core security functions shall support the implementation of the IBIP device authorization, finance, indicium creation, and device audit functions, which are further described in Section B.2.2. The PSD ensures that only authorized IBIP devices are able to apply a valid indicium to a mailpiece. Figure B-1 illustrates the role the PSD plays in the creation of indicia.

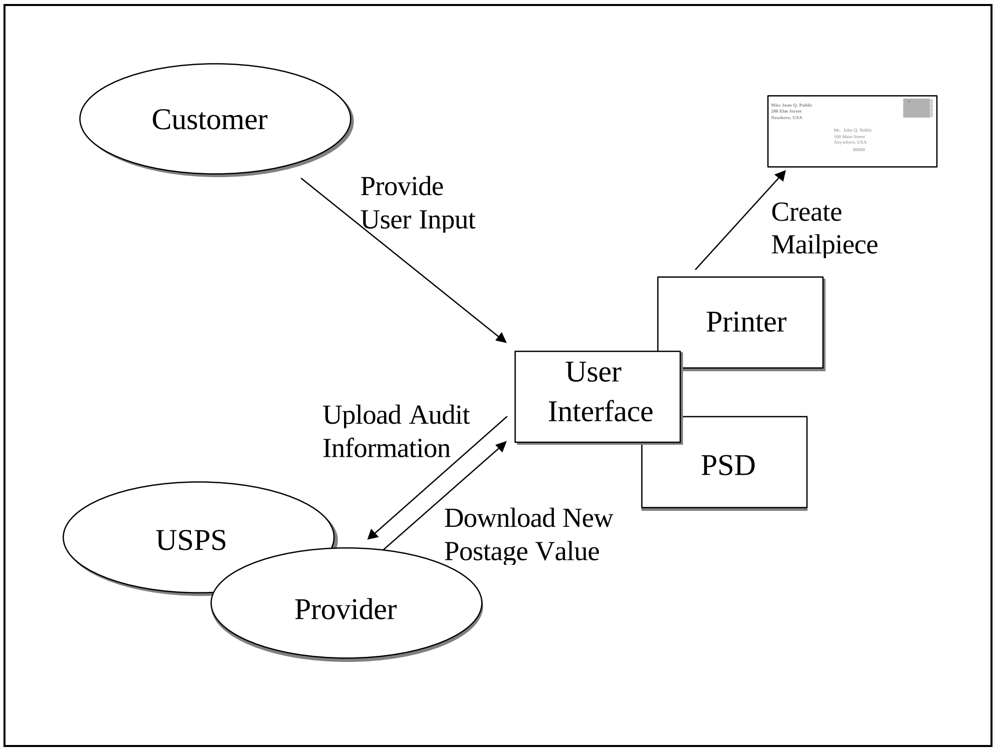


Figure B-1. PSD Role in IBIP Indicia Creation

B.2.1 Core PSD Security Functions

There are three core security functions of the PSD (i.e., initialization, digital signature, and register management) that are used to support four of the IBIP functions (i.e., device authorization, finance, indicium creation, and device audit). The IBIP functions supported by each of the PSD core security functions are identified in Table B-1.

Table B-1. PSD Security Functions and IBIP Functions Matrix

PSD Security Functions	IBIP Device Authorization	IBIP Financial Functions	IBIP Indicium Creation	IBIP Device Audit
Initialization	✓			
Digital Signature*	✓*	✓*	✓	✓*
Register Management		✓	✓	

*Use of the Digital Signature function is optional, except for IBIP Indicium Creation, provided another secure method is used.

A brief introduction into each PSD core security function is provided in this section. Detailed requirements for each of these functions are presented in Section B.3.1 of this document.

B.2.1.1 PSD Initialization Function

The PSD initialization function is the process used to load device-specific information that is loaded once and only once for a given PSD. The process includes loading the device serial number and initializing the ascending and descending registers.

B.2.1.2 PSD Digital Signature Function

The PSD digital signature function uses the signing key generated by the IBIP Certificate Authority (CA). This function shall provide data integrity and non-repudiation security services for IBIP indicia. Several alternatives for the digital signature function are identified in these performance criteria. Each of these alternatives implements a “public key” cryptographic algorithm for the digital signature function. Providers may choose to implement one of the defined alternatives or may propose additional alternatives for consideration by the USPS. The PSD shall also provide data integrity and security services on other selected IBIP and non-IBIP communications messages by using the signing key generated by the CA, or an alternative approach that is equally secure.

B.2.1.3 PSD Register Management Function

The intent of the register management function is to ensure that the financial registers in the PSD (i.e., the ascending and descending registers) operate correctly and protect the revenue of the USPS appropriately. Providers shall choose the technology used to implement these registers such that even a sophisticated, knowledgeable attacker could not alter the register values or successfully defraud the USPS.

B.2.2 IBIP Functions

The four IBIP functions (device authorization, finance, indicium creation, and device audit), in conjunction with the PSD initialization function, ensure that only authorized PSDs support the creation of valid indicia on mailpieces. Additionally, these functions provide the means to detect illicit use of a PSD. A brief introduction to each IBIP function is provided in this section. Detailed requirements for the PSD, in support of each of these functions, are presented in Section B.3.2.

B.2.2.1 IBIP Device Authorization

The IBIP authorization process ensures that only an authorized device can support the creation of a valid indicium. The Provider shall authorize a PSD for use by a specific licensed customer. Once a PSD is authorized, the finance functions must be performed before the first indicium is created.

B.2.2.2 IBIP Finance

The IBIP finance function shall download postage value into the PSD. In order to download postage into the PSD, the customer must have sufficient funds on deposit with the USPS.

B.2.2.3 IBIP Indicium Creation

The PSD and the host system shall jointly perform functions necessary to create a valid indicium in accordance with the performance criteria for the indicium in Part A. The PSD shall accept input from the host system and use data internal to the device itself to create signed data elements for selected fields in the indicium.

B.2.2.4 IBIP Device Audit

The device audit function allows the USPS to ensure proper use of the PSD. To ensure such use, the PSD shall create an appropriate device audit message and output it to the host system for transfer to the Provider. Upon receipt of a device audit message, the Provider shall assess the continued integrity of the register values and other associated data. If appropriate, the Provider responds with a device audit response message which results in the resetting of the PSD’s watchdog timer. The watchdog timer precludes indicia creation if the PSD has not been adequately audited, or if the Provider has not responded to a device audit with a device audit response message resulting in the resetting of the watchdog timer.

B.2.3 Other Digital Signature Capability

For security reasons, the PSD shall not be a generalized digital signature device. Only USPS-approved messages shall be signed by the PSD.

B.3 PSD FUNCTIONAL REQUIREMENTS

Functional requirements for the PSD are specified in two subsections below. Section B.3.1 identifies core PSD functional security requirements. Section B.3.2 identifies how the core PSD security functions are to be applied to satisfy overall IBIP requirements.

B.3.1 Core PSD Functional Security Requirements

This section presents requirements for the core PSD security functions that shall be applied in various combinations to implement security services for the IBIP functions presented in Section B.3.2.

B.3.1.1 PSD Initialization

In order to initialize the PSD, the Provider must load device-specific information that shall not change over the life-cycle of the device.

The Provider shall assign a unique 4-byte PSD serial number to each PSD during the manufacturing process. The serial number shall be written to nonvolatile memory in the PSD during device initialization.

During the initialization process, the PSD shall explicitly initialize all internal registers and counters to their intended initial values. When the PSD is initialized by the PSD manufacturer, the value of the ascending register shall be set to US$ 000,000,000.000 and the value of the descending register shall be set to US$ 000,000.000. PSD-resident software used for initialization shall be permanently disabled after the operation is complete to ensure the registers cannot be reinitialized after the one-time process.

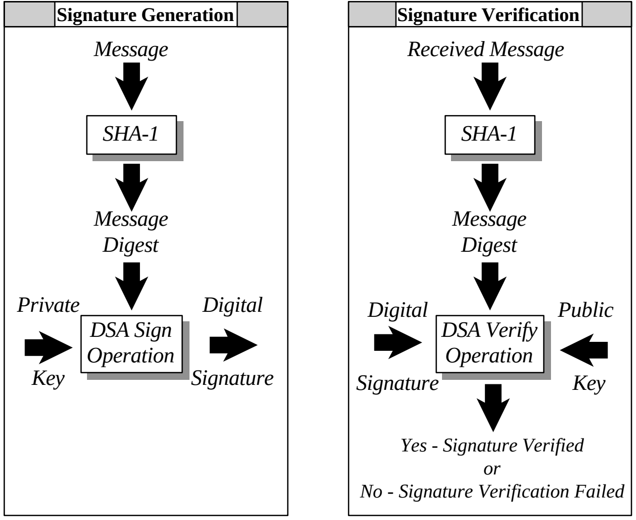
B.3.1.2 PSD Digital Signature Functions

The PSD shall implement either DSA, RSA, ECDSA, or another Provider-suggested and USPS-approved method for the generation and verification of digital signatures for the creation of indicia. The digital signature methodology used shall provide data integrity and non-repudiation services. If DSA, RSA, or ECDSA is used, the PSD must adhere to the requirements specified in Section B.3.1.2.1 for DSA, Section B.3.1.2.2 for RSA, or Section B.3.1.2.3 for ECDSA, as well as the appropriate government and/or commercial standards. Requirements for other approved digital signature methods, if any, will be documented in future versions of the PCIBI-C.

B.3.1.2.1 DSA Requirements

If the Provider chooses to use DSA, the PSD shall implement the DSA as specified in FIPS PUB 186, to provide digital signature generation and verification functions. The PSD shall use the standard DSA parameters that are defined in FIPS PUB 186. Figure B-2 illustrates the generic DSA signature generation and verification processes. Applications of these processes to satisfy IBIP requirements are defined in Section B.3.2.

Figure B-2. DSA Signature Generation and Verification



The following subsections detail requirements and parameters for the use of DSA. A PSD must adhere to the requirements addressed in these sections only if it implements DSA for IBIP. Wherever there are any conflicts, the requirements in these sections take precedence over those in the referenced published standards.

B.3.1.2.1.1 PSD DSA Parameters

Using the default, standard parameters specified in FIPS PUB 186, the PSD shall obtain or generate, as appropriate, the DSA parameters listed in Table B-2 for signature generation, and in Table B-3 for signature verification.

Table B-2. DSA Parameters for Signature Generation

Parameter	Source	PSD Storage	Comments
p	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs
q	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs
g	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs
x	Generated by the PSD during device authorization	Stored in nonvolatile memory until replaced or erased	PSD private key
y	Calculated by the PSD and output to host system during device authorization	Stored in the PSD IBIP certificate	PSD public key
M	Message created by the PSD based on host system inputs and internal register contents	Stored in the PSD only for the duration of DSA signature generation	Output to host system by the PSD
k	Generated by the PSD	Used for a single signature; erased after use	A new random value must be generated for each digital signature
r	Calculated by the PSD during the DSA sign operation	Result of DSA signature generation; erased after use	Output to host system by the PSD
s	Calculated by the PSD during the DSA sign operation	Result of DSA signature generation; erased after use	Output to host system by the PSD

Table B-3. DSA Parameters for Signature Verification

Parameter	Source	PSD Storage	Comments
p	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs; same as parameter *p* in Table B-2
q	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs; same as parameter *q* in Table B-2
g	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	DSA standard parameter common for all PSDs; same as parameter *g* in Table B-2
y	Loaded into the PSD from the host system	Stored in nonvolatile memory until replaced or erased	Public key of message originator
M'	Message as received from message originator	Stored in PSD only for duration of DSA signature verification	Input from the host system to the PSD
r'	*r* value received from message originator	Stored in PSD only for duration of DSA signature verification	Input from the host system to the PSD
s'	*s* value received from message originator	Stored in PSD only for duration of DSA signature verification	Input from the host system to the PSD
w, u_1, u_2, v	Generated by the PSD during signature verification process	Stored in PSD only for duration of DSA signature verification	The signature is verified if $v = r'$ PSD actions upon verification (or failure of verification) are specified in Section 3.2

B.3.1.2.1.2 Creation of the DSA Digital Signature

If the DSA is used, the PSD shall create the digital signature, using the standard DSA parameters, as specified in the Digital Signature Standard, FIPS PUB 186. In accordance with that standard, the Secure Hash Algorithm (SHA-1), as specified in the Secure Hash Standard, FIPS PUB 180-1, shall be used to create a 160-bit message digest. This is used in conjunction with the private key as inputs to the DSA signing operation and results in the digital signature as output. The input message for the SHA-1 shall be formatted as shown in Table B-4. Although SHA-1 requires input to be blocked as multiples of 64 bytes, any required message pad is added by the algorithm itself and must not be included in the input data.

Table B-4. SHA-1 Message Input Format

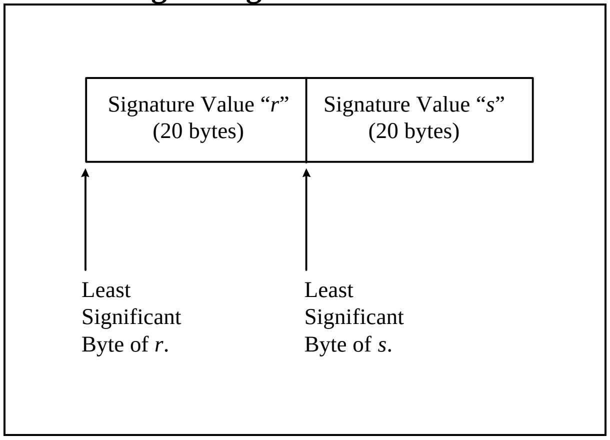
Field Number	Field Name	Number of Bytes	Order*
1	Indicia Version Number	1	N/A
2	Algorithm ID	1	N/A
3	Certificate Serial Number	4	Start with least significant byte
4	PSD Manufacturer ID	2	N/A (text field)
5	PSD Model Number	2	N/A (text field)
6	PSD Serial Number	4	Start with least significant byte
7	Ascending Register	5	Start with least significant byte
8	Postage	3	Start with least significant byte
9	Date of Mailing	4	Start with least significant byte
10	Licensing ZIP Code	4	Start with least significant byte
11	Reserved	5	N/A
12	Software ID	6	Start with least significant byte
13	Descending Register	4	Start with least significant byte
14	Rate Category	4	N/A (text field)

*All binary fields are little endian format with least significant byte first, most significant byte last.

B.3.1.2.1.3 Digital Signature Algorithm Message Digest

The PSD shall perform the hash function using the Secure Hash Algorithm (SHA-1), as specified in the Secure Hash Standard, FIPS PUB 180-1. The result of that operation shall be a 160-bit message digest that the PSD shall use in the creation of the DSA digital signature. The DSA algorithm generates two parameter values resulting from the DSA signing operation, which are referred to as "*r*" and "*s*." Each parameter is 160 bits in length. These two values shall be placed into the digital signature field of the barcode as shown in Figure B-3.

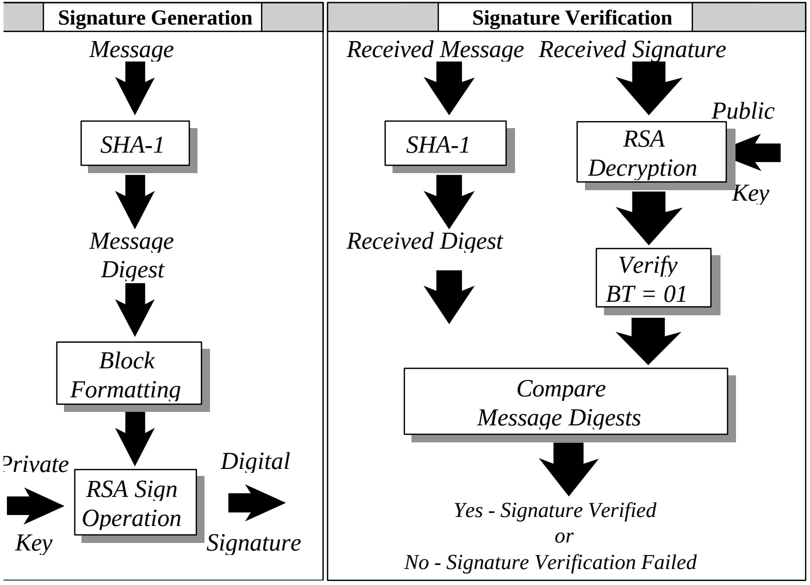
Figure B-3. Digital Signature Field Format for DSA



B.3.1.2.2 RSA Requirements

If RSA is chosen, the PSD shall use RSA as specified in PKCS #1, Section 10, to implement digital signature generation and verification functions, using the standard RSA parameters as defined in PKCS #1: RSA Encryption Standard. Figure B-4 illustrates the generic RSA signature generation and verification processes.

Figure B-4. RSA Digital Signature Generation and Verification



The PSD shall create a digital signature by inputting the data to be signed to the SHA-1 and obtaining a message digest of 160 bits in length. Since the process of using the RSA algorithm to create a digital signature utilizes the SHA-1 hashing algorithm, as did DSA in the previous section, the input message for SHA-1 shall be the same as that illustrated in Table B-4. However, in this case the 160-bit SHA-1 output shall be block formatted in accordance with the RSA Data Security Standard, PKCS #1, Section 8. That is, the SHA-1 output is placed in the data field (D) of the signature block (SB), as follows:

SB = 00 || BT || PS || 00 || D

The block type (BT) shall be a single octet with the value of 01 indicating a private key operation. The padding string (PS) shall be 105 octets with each octet being set to the value FF. This then makes the length of the signature block equal to the length of the public-key modulus (1024 bits). This resulting block is then transformed using the private key and the result is place in the digital signature field of the indicium. Applications of these processes to satisfy IBIP requirements are defined in Section B.3.2.

The following subsections detail requirements and parameters for the use of RSA. A PSD must adhere to the requirements addressed in these sections only if it implements the RSA signature method for IBIP. Wherever there are any conflicts, the requirements in these sections take precedence over those in the referenced published standards..

B.3.1.2.2.1 PSD RSA Digital Signature Parameters

If RSA is used, the PSD shall generate the parameters listed in Table B-5 for RSA signature generation and Table B-6 for RSA signature verification.

Table B-5. RSA Parameters for Signature Generation

Parameter	Source	PSD Storage	Comments
p	Generated by the PSD during device authorization	N/A	Needed to calculate the PSD’s modulus *n*
q	Generated by the PSD during device authorization	N/A	Needed to calculate the PSD’s modulus *n*
n	Modulus for the PSD, calculated during authorization	Stored in nonvolatile memory until replaced or erased	*n* = *pq*, stored as part of the PSD’s public key
d	Generated by the PSD during device authorization	Stored in nonvolatile memory until replaced or erased	PSD’s private key
e	IBIP established parameter (shall be set = 65537)	Stored in nonvolatile memory until replaced or erased	RSA exponential value used in the signature verification process; part of PSD’s public key
S	Generated during the RSA signature generation process	Stored in PSD only for duration of RSA signature generation	Result of the RSA signature generation that is output to the host system

Table B-6. RSA Parameters for Signature Verification

Parameter	Source	PSD Storage	Comments
n	X.509 Certificate of the signer	Stored in nonvolatile memory until replaced or erased	Part of the signer's public key
e	IBIP established parameter (shall be set = 65537)	Stored in nonvolatile memory until replaced or erased	
M	Message generated by the sender	Stored in PSD only for duration of RSA signature verification	*n* = *pq*, stored as part of the PSD's public key
S	Generated by the message originator during message creation	Stored in PSD only for duration of RSA signature verification	Input from the host system to the PSD
MD	Message digest resulting from processing the signature of the message	Stored in PSD only for duration of RSA signature verification	
MD'	Generated using the received message during the RSA signature verification process	Stored in PSD only for duration of RSA signature verification	RSA signature is verified if *MD'* = *MD*

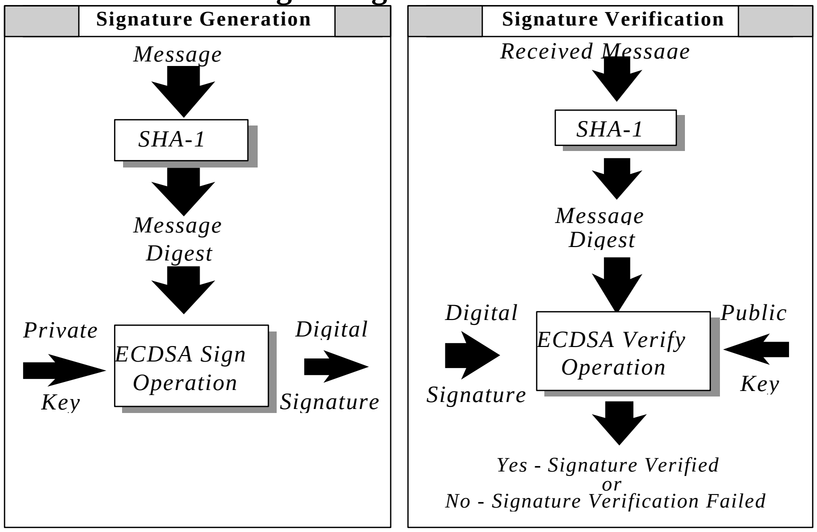
B.3.1.2.2.2 RSA Message Digest

The PSD shall perform the hash function using the Secure Hash Algorithm (SHA-1), as specified in the Secure Hash Standard, FIPS PUB 180-1. The result of that operation shall be a 160-bit message digest that the PSD shall use in the creation of the RSA digital signature. If the RSA methodology is used, the signature block generated by application of the RSA is signed using the private key and the result is placed into the digital signature field of the indicium.

B.3.1.2.3 Elliptic Curve Digital Signature Algorithm Requirements

If Elliptic Curve technology is chosen, the PSD shall use the ECDSA algorithm as specified in the ANSI X9.62 Standard to implement digital signature generation and verification functions. Figure B-5 illustrates the generic ECDSA signature generation and verification processes. Applications of these processes to satisfy IBIP requirements are defined in Section B.3.2.

Figure B-5. ECDSA Digital Signature Generation and Verification



The following subsections detail requirements and parameters for the use of the ECDSA algorithm. A PSD must adhere to the requirements addressed in these sections only if it implements ECDSA for IBIP. Wherever there are any conflicts, the requirements in these sections take precedence over those in the referenced published standards.

B.3.1.2.3.1 PSD Elliptic Curve Digital Signature Algorithm Parameters

If the ECDSA algorithm is used, the PSD shall generate or obtain, as appropriate, the parameters listed in Table B-7 for ECDSA signature generation and Table B-8 for ECDSA signature verification.

Table B-7. ECDSA Parameters for Signature Generation

Parameter	Source	PSD Storage	Comments
q	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	ECDSA standard parameter common for all PSDs; defines the underlying finite field
f	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	ECDSA standard parameter common for all PSDs; defines the basis for field representation
a, *b*	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	Two ECDSA standard parameters common for all PSDs; defines the elliptic curve to be used
P	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	ECDSA standard parameter common for all PSDs; defines a point of the curve of prime order
n	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	ECDSA standard parameter common for all PSDs; the order of the point *P*; must be a prime which is greater than 2^{150}
d	Generated by the PSD during device authorization.	Stored in nonvolatile memory until replaced or erased	PSD private key
Q	Calculated by the PSD and output to the host system during device authorization	Stored in the PSD IBIP certificate	PSD public key
M	Message created by the PSD based on host system input and internal register contents	Stored in the PSD only for the duration of the ECDSA signature generation calculation	Output to host system by the PSD
k	Generated by the PSD	Used for a single signature; erased after use	A new random value generated for each signing operation
r, *s*	Calculated by the PSD during the ECDSA sign operation	Result of ECDSA signature generation; erased after use	Output to host system by the PSD

Table B-8. ECDSA Parameters for Signature Verification

Parameter	Source	PSD Storage	Comments
q	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	ECDSA standard parameter common for all PSDs; defines the underlying finite field; same as parameter q in Table B-7
f	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	ECDSA standard parameter common for all PSDs; defines the basis for field representation; same as parameter f in Table B-7
a, b	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	Two ECDSA standard parameters common for all PSDs; defines the elliptic curve to be used; same as parameters a and b in Table B-7
P	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	ECDSA standard parameter common for all PSDs; defines a point of the curve of prime order; same as parameter P in Table B-7
n	Loaded into the PSD during device initialization	Stored in nonvolatile memory until replaced or erased	ECDSA standard parameter common for all PSDs; the order of the point P; same as parameter n in Table B-7
Q	Loaded into the PSD from the host system	Stored in PSD only for duration of ECDSA signature verification	Public key of message originator
M'	Message as received from message originator	Stored in PSD only for duration of ECDSA signature verification	Input from the host system to the PSD
r', s'	r, s values received from message originator	Stored in PSD only for duration of ECDSA signature verification	Input from the host system to the PSD
w, u_1, u_2, v	Intermediate values generated by the PSD during signature verification	Stored in PSD only for duration of ECDSA signature verification	The signature is verified if $v = r'$

B.3.1.2.3.2 Elliptic Curve Digital Signature Algorithm Message Digest

The PSD shall perform the hash function using the Secure Hash Algorithm (SHA-1), as specified in the Secure Hash Standard, FIPS PUB 180-1. The result of that operation shall be a 160-bit message digest that the PSD shall use in the creation of the ECDSA digital signature. Since the process of using the ECDSA algorithm to create a digital signature utilizes the SHA-1 hashing algorithm, as did DSA above, the input message for SHA-1 shall be the same as that illustrated in Table B-4. This message digest and the private key are then input to the ECDSA signing operation and the resulting output is the digital signature.

The ECDSA algorithm generates two parameter values resulting from the ECDSA signing operation, which are referred to as “r” and “s.” Each parameter is 160 bits in length.

These two values shall be placed into the digital signature field of the barcode in the same manner as for DSA, as shown in Figure B-3.

B.3.1.3 PSD Register Management Functions

The PSD shall store and manage ascending and descending registers in nonvolatile memory to support the IBIP finance, indicia creation, and device audit functions as discussed in Section B.3.2. The management of these registers is specified in this section.

B.3.1.3.1 PSD Register Formats

Each register shall represent a monetary value. The monetary values shall be measured in 1/10 of 1-cent increments. The ascending register shall consist of 5 bytes of binary data. The descending register shall consist of 4 bytes of binary data. Therefore, the register values shall be interpreted as follows:

- Ascending Register: US$ XXX,XXX,XXX.XXX
- Descending Register: US$ XXX,XXX.XXX

The ascending register shall support any postage usage value less than US$ 1 billion; the descending register shall support any postage value less than US$ 1 million. The maximum value of the ascending register in binary format is 5 bytes of packed binary data, which, reading left to right from the most significant byte to the least significant byte, neglecting decimal placement, shall be:

11111111 11110000 10100101 00101011 00010111.

Similarly, the maximum value of the descending register in binary format, neglecting decimal placement, shall be

00111111 11100100 11010110 01110111.

The PSD shall be designed such that neither the ascending register nor the descending register shall ever exceed the maximum allowable value. In the event that the ascending register reaches its maximum value, further indicia creation operations shall be disabled. The sum of the ascending and descending registers shall not be able to exceed US$ 1 billion.

B.3.1.3.2 PSD Register Operations

When the PSD receives a postage value download message resulting from the IBIP finance function, and that message has been validated as discussed in Section B.3.2, the PSD shall check for the replay of prior postage value download messages by comparing the old control total field in the postage value download message with the sum of the ascending and descending registers in the PSD. When the old control total in the download message equals the sum of the values of the ascending and descending registers, the descending register value shall be increased by the amount of the postage value contained in the download message. If the old control total in the download message does not equal the sum of the values in the ascending and descending registers, the PSD shall abort the download process and send an appropriate message to the host system.

When the host system requests the creation of an indicium, the PSD shall perform several operations using the ascending and descending registers. First, the PSD shall compare the requested postage amount input from the host system with the allowable limits currently in effect for the PSD for printing postage. If the requested postage amount is greater than or equal to the minimum limit and less than or equal to the maximum limit, the PSD shall proceed with its register management functions. If the requested postage amount is not within the allowable limits, an appropriate error message shall be returned to the host system. The allowable requested postage amount shall be compared to the value contained in the descending register. When the descending register contains sufficient value, the register values shall change in accordance with Table B-9. If an insufficient value remains in the descending register, the PSD shall return an appropriate message to the host system and abort the indicium creation function.

Table B-9. Ascending and Descending Register Operations

IBIP Function	Ascending Register Operation	Descending Register Operation
Indicium Creation	The value contained in the ascending register shall increase by the postage amount specified by the host system.	The value contained in the descending register shall decrease by the postage amount specified by the host system.
Finance (Upon receipt of postage value download message by the PSD)	The value contained in the ascending register shall be unchanged by the finance function.	The value contained in the descending register shall increase by the amount of postage value contained in a valid postage value download message.

B.3.1.3.3 Register Integrity

After completion of PSD initialization, the PSD shall have no mechanism available to alter the value contained in the ascending register except as specified in Section B.3.1.3.2. The PSD shall have no mechanism to alter the value contained in the descending register except as specified in Section B.3.1.3.2.

Upon request of the host system, the current values of the ascending and descending registers shall be output to the host system for display to the customer. This function allows the customer to determine the remaining postage value contained in the PSD and the total amount of postage applied by that PSD. The host system shall have no mechanism to alter the ascending or descending register values in the PSD.

B.3.2 PSD Requirements to Implement IBIP Functions

This section presents the requirements for the proper implementation of IBIP functions. Where appropriate, reference is made to the core PSD functional requirements presented in Section B.3.1.

B.3.2.1 IBIP Device Authorization Requirements

The authorization of a PSD is the process used to load customer-specific information into the PSD. It includes generating all cryptographic keys, loading certificates, setting the initial value of the watchdog timer, and loading the manufacture identification number and model identification number components of the device identity.

During the IBIP device authorization process, the Provider shall tailor the PSD for a particular customer and fully enable it to perform IBIP functions. Prior to performing the device authorization functions, the PSD must have been initialized in accordance with Section B.3.1.1. PSD device authorization shall include the steps identified in the following subsections.

A Provider may reprogram a PSD with new device authorization information if the relevant customer authorization information changes, such as a change to the licensing ZIP Code. The Provider must reprogram a PSD with the appropriate device authorization information if the PSD is issued to a different customer by the Provider, or if there is an upgrade to the PSD. When customer authorization information changes, the Provider must interface with the USPS infrastructure to ensure customer information is updated as required.

B.3.2.1.1 Load Device ID Elements

During device authorization, each PSD shall be loaded with the 2-character manufacturer ID, and a 2-character model identification. The USPS will assign the manufacturer ID. The USPS will assign the model numbers based on recommendations made by the Provider. The model number is 2 characters with the first character being numeric, and the second character being alpha.

B.3.2.1.2 Load Customer Authorization Information

During device authorization, each PSD shall be loaded with customer-specific information including the licensing ZIP Code.

B.3.2.1.3 Private/Public Key Processing

The PSD shall handle public and private key processing as detailed below in Table B-10. The Provider shall be responsible for passing the public key to the IBIP certificate authority and obtaining the certificate containing the PSD's public key.

Table B-10. Private/Public Key Processing

Step	DSA or ECDSA	RSA
1	PSD shall internally generate the private key.	PSD shall internally generate the public key.
2	PSD shall calculate the public key.	PSD shall calculate the private key.
3	PSD shall store the private and public keys in nonvolatile memory.	Same
4	PSD shall output the public key to the Provider.	Same
5	PSD shall accept the certificate from the Provider.	Same
6	PSD shall compare the stored public key with the received certificate's public key.	Same
7	If the comparison in step 6 fails, go to step 1.	Same
8	If the comparison in step 6 is successful, store certificate.	Same

B.3.2.1.4 Load Maximum/Minimum Postage Amount

The PSD shall be loaded with the maximum and minimum postage values that the PSD is allowed to process. The Provider determines the minimum value. In accordance with section A.2, the maximum value of the indicium must be less than $100.00.

The PSD shall have a mechanism to update the range of maximum and minimum allowable postage when the USPS changes applicable regulations.

B.3.2.1.5 Load Watchdog Timer Values

The PSD shall be loaded with a value, which is measured in days, that shall be used as the reset value of the watchdog timer. The initial value of the watchdog time shall be set to day one of the reset period.

B.3.2.1.6 PSD Upgrades

Any revisions to the PSD, including software upgrades to existing PSDs, shall result in a new 2-character model number, making it necessary to reauthorize the device by loading the new model identification number into the PSD. However, at no time shall any revisions to the PSD result in changing the PSD’s register values or serial number. Any revision to the PSD, including software upgrades of existing PSDs must be approved by the USPS. The USPS must also approve the process for implementing the upgrade.

B.3.2.2 IBIP Finance Functions

The fundamental role of the PSD in the implementation of the IBIP finance functions is to request, accept, and process postage value downloads and to perform security-critical functions in the creation of the indicium. To support IBIP finance functions, all communications from the PSD to the Provider infrastructure and all communications from the Provider infrastructure to the PSD must authenticate the sender and verify the message. The specific authentication/verification methods for these transactions are Provider-specific, and are beyond the scope of this document. The authentication methods may vary from Provider to Provider, but must be approved by the USPS.

B.3.2.2.1 Postage Value Download Transaction (PVDT)

When a customer needs to add postage value to their PSD, the customer must have sufficient funds on deposit with the USPS. If necessary, the customer shall execute a funds transfer to the USPS.

The Postage Value Download Transaction (PVDT) is the transaction required to complete a postage value download. A PVDT contains a series of messages transmitted between the PSD/host system and the Provider infrastructure. At a minimum, this transaction contains at least two messages, the postage value download request message and the postage value download message. It shall be the Provider’s responsibility to determine the authentication and verification method and the data contained in these messages, however such methods and the message data must be approved by the USPS. It shall be the Provider’s responsibility to ensure that all messages and transmissions are completed without error and any erroneous messages are trapped and handled properly.

B.3.2.2.1.1 Postage Value Download Request Message

The PSD shall initiate the postage download process by creating a request message, and passing that message to the host system for transmission to the Provider infrastructure. The Provider infrastructure must authenticate the PSD as the sender, and must verify the data transmitted to detect data modification and replay.

B.3.2.2.1.2 Postage Value Download Message

After the Provider infrastructure successfully authenticates the sender and verifies the request message, the Provider infrastructure shall prepare a postage value download message. The Provider infrastructure shall then transmit this message to the host system. Upon receipt of a postage value download message from the host system, the PSD shall authenticate the sender and verify the message. Only when the sender has been authenticated and the message verified, may the postage value download be applied to the PSD registers.

B.3.2.3 Indicium Creation Function

The role of the PSD in the indicium creation function is to perform security-critical processes as described in this section. It is the responsibility of the host system to use the information provided by the PSD to create the indicium. Upon failure of any of the processes described in this section, the PSD shall issue an appropriate error message to the host system.

B.3.2.3.1 Indicium Creation Host Request

The PSD shall accept a request from the host system to perform the security functions necessary for the host to create an indicium. The format of this request is at the discretion of the PSD Provider.

B.3.2.3.2 Indicium Creation Register Operations

The PSD shall perform the register operations in accordance with Section B.3.1.3.2 before signing the indicium data.

B.3.2.3.3 Indicium Creation Signature Generation

The PSD shall generate a digital signature for the indicium as defined in Part A, Indicium, and Section B.3.1.2.

B.3.2.3.4 Indicium Creation Results Output

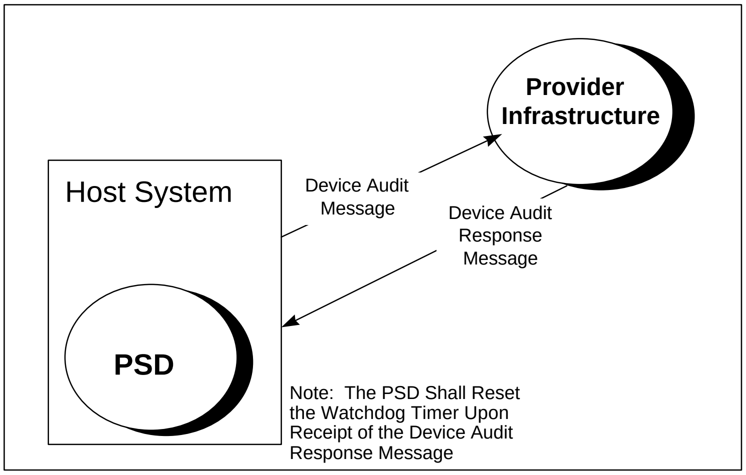
Upon successful completion of the processes defined in Sections B.3.2.3.1 through B.3.2.3.3, the PSD shall output the value of the ascending register, descending register, and the digital signature to the host system. Other indicium data may also be output to the host system at the discretion of the Provider. The host system shall generate the indicium.

B.3.2.4 Device Audit Function

The primary role of the PSD in the device audit function is to create device audit messages and pass those messages to the host system for transmission to the Provider. The PSD shall initiate the device audit function upon host request and to request the reset of a "timed out" watchdog timer. The overall device audit process is illustrated in Figure B-6.

Upon receipt of a device audit message, the Provider infrastructure shall create a device audit response message and return that message to the PSD. After validating the response message, the PSD shall reset the watchdog timer to its initial value.

Figure B-6. Device Audit Process


Provider Infrastructure
Host System
Device Audit Message
Device Audit Response Message
PSD
Note: The PSD Shall Reset the Watchdog Timer Upon Receipt of the Device Audit Response Message

B.3.2.4.1 Device Audit Message

The host system/PSD shall prepare a device audit message for transmission to the Provider infrastructure. The contents and format of this message are at the discretion of the Provider, but must contain enough information to ensure that inconsistencies within the PSD are detected by the Provider infrastructure. Sender authentication and data validation are required, as is required for all financial transactions.

B.3.2.4.2 Device Audit Response Message

The Provider infrastructure shall return a device audit response message to the PSD in response to the receipt of a device audit message. Upon receipt of a device audit response message from the host system, the PSD shall authenticate the sender and verify the data. If the authentication and verification process succeeds, the PSD shall reset its watchdog timer to its initial value. If the authentication or verification process fails, the PSD shall discard the device audit response message without further processing and shall return an appropriate error indication to the host system.

B.3.3 PSD Requirements to Implement Other Digital Signature Capabilities

The PSD is required to create digital signatures signed by the public key generated by the IBIP CA to complete the indicium creation process. The PSD may use the same public key for other IBIP authentication and verification requirements at the discretion of the Provider, and approval of the USPS.

B.4 PSD PHYSICAL REQUIREMENTS

This section describes the physical requirements to which the PSD shall conform. It is not the intent of these performance criteria to require a particular physical design. The requirements presented in this section are those necessary to ensure the integrity of the PSD and the IBIP system.

B.4.1 PSD Security

The PSD shall be designed and implemented in accordance with FIPS PUB 140-1. The PSD shall conform to the FIPS requirements for overall security level 2, and as specified in Table B-11. In instances where there is a conflict between the FIPS requirements and the table, Table B-11 takes precedence.

Table B-11. FIPS 140-1 PSD Requirements

FIPS 140-1 Design Category	Proposed PSD Performance Criteria/ FIPS 140-1 Requirements	Comment
Crypto Module	Documentation Required: • PSD Module Description (by Provider). • Specification of PSD cryptographic module and its cryptographic boundary (by Provider). • PSD security policy (by Provider).	Provider PSD description and performance criteria must comply with these PSD performance criteria; Provider PSD security policy must comply with IBIP Security Policy.
Module Interfaces	Paths explicitly defined (by Provider): • Power and control paths (from host system). • Input data (through host system). • Separate inputs for data and plaintext security parameters (keys and access control data), or single input if security parameters are protected. • Output data and status (to host system). • Optional: maintenance access (Provider proprietary).	Message and data formats must be approved by the USPS, as described in these performance criteria.
Roles	Authorized roles: • Customer (through host system). • Crypto officer (Provider). • Maintenance (Provider-required if optional maintenance port is implemented). Access control — authentication by role for customer, Provider, individual (optional).	• Minimum access control shall satisfy security level 2 (role-based) access; security level 3 and 4 (individual) access is optional. • At least a PIN/password entry is needed for access control for either case.
Services	• Initiate and run self-tests. • Output module status to host system. • Output module alarms to host system. • Accept host system controls. • PSD core and IBIP functions. • No bypass capability.	Self-tests — see below
Finite State Machine Model	Comply with FIPS PUB 140-1, Section 4.4 design and documentation requirements.	Required documentation from Provider/manufacturer.

FIPS 140-1 Design Category	Proposed PSD Performance Criteria/ FIPS 140-1 Requirements	Comment
Physical Security	PSD Physical Security requirements.	Security level 3.
Environmental Failure Protection or Testing (EFP/EFT)	Employ environmental failure protection features or undergo environmental failure protection testing for accreditation.	Implemented to counter a potential tampering mode (especially voltage and temperature). Security level 4.
Software Security	Required documentation: • Software design. • Relationship of design to security policy. • Annotated complete source code. Implement in high-level language unless low-level language essential or high-level language not available.	Additional documentation required from Provider/ manufacturer.
Operating System Security	Not applicable.	Required only if operator has means of loading device software.
Key Management	• Key generation — Only internal generation of PSD's public and private keys. • Key distribution — PSD public key sent to CA upon generation for inclusion in certificate.	No key extraction except PSD public key.
Crypto Algorithms	Implement either DSA, RSA, ECDSA, or other USPS-approved signature generation and verification algorithm.	Provider may need to obtain necessary rights to use.
Electromagnetic Interference and Compatibility (EMI/EMC)	Comply with EMI/EMC requirements specified by FCC Part 15, Subpart J, Class B (i.e., for home use); conforms to security levels 3 and 4.	Primarily for compatibility with other electronic devices.
Self-Tests	Statistical random number generator test performed during initialization and again at authorization. Power-up self-tests: • Crypto algorithm (known answer). • Error detection code or authentication. • Critical functions. Conditional tests: TBD by Provider (pair-wise consistency, software/firmware load, manual key entry, continuous random number generator)	Testing must ensure proper operation of PSD functions.

B.4.2 PSD Contents

The PSD shall include a FIPS 140-1-compliant random number generator.

The PSD shall include a real-time clock. A mechanism must be available to reset the real-time clock value to match the current time.

The PSD shall include a watchdog timer.

The PSD shall include a backup battery capable of maintaining the real-time clock for a minimum of 5 years from installation. Other means of ensuring the retention of PSD data, and continued operation of the real-time clock in the absence of primary input power, which is in lieu of a battery, will be evaluated, if proposed.

The PSD shall output an alarm signal indication in the event of a low battery power level condition.

B.4.3 PSD Internal Storage

PSD internal storage shall satisfy the data requirements of Sections B.3.1 and B.3.2. The minimum data required by IBIP in nonvolatile storage are as follows:

- Device ID (PSD Manufacturer ID, PSD Model ID, PSD Serial Number)
- PSD Private Key
- IBIP Common Parameters
- Originating Address
- Ascending Register
- Descending Register
- Maximum/Minimum Postage Values
- PSD X.509 Certificate Serial Number
- Any other required authentication/verification data for the Provider product.

B.4.4 PSD Software

The PSD shall comply with the FIPS PUB 140-1 software security requirements appropriate for its security level. Additionally, if applicable, the PSD shall comply with the operating system requirements in accordance with FIPS PUB 140-1.

B.4.5 Watchdog Timer

The initial value of the watchdog timer shall be set by the Provider at authorization. This value shall be measured in calendar days and shall range between 1 and 366. The watchdog timer shall be tied to the real-time clock in the PSD. Once each day, the value contained in the watchdog timer shall be decremented by 1 (one). When the timer expires (i.e., reaches a zero value), the PSD shall be unable to create additional indicia. A PSD that is disabled shall be reset only upon receipt of a valid device audit response message as discussed in Section B.3.2.4. A PSD that is disabled shall retain its memory and shall not “zeroize,” but it cannot be used to create indicia until audited by the Provider.

B.4.6 PSD Tamper Resistance

The PSD shall have an explicitly defined perimeter that establishes the physical bounds of the cryptographic module and the cryptographic boundary, including the processor for the software and/or firmware that executes the code. The requirements for different format options are summarized in Table B-12.

Table B-12. PSD Physical Security Requirements (per FIPS PUB 140-1)

Single Chip Module (stand-alone or embedded)	**Multi-Chip Module**	**Multi-Chip Stand-Alone Module**
Inherently tamper resistant (e.g., smart card)	ICs with interconnections, not within a protected enclosure (e.g., expansion boards/adapters)	ICs interconnected within protected enclosure (e.g., IC printed circuit board or ceramic substrate)
• Hard, opaque, removal-resistant coating including or covering passivation • Tamper response and zeroization active when keyed • Include environmental failure protection (shutdown or zeroization, especially for temperature and voltage), or undergo environmental failure testing	• Strong, non-removable enclosure • Completely within tamper detection envelope • Tamper response and zeroization circuitry active when keyed • Any ventilation holes/slits to include anti-probe design (e.g., 90 degree bends) completely within tamper detection envelope • Include environmental failure protection (shutdown or zeroization, especially for temperature and voltage), or undergo environmental failure testing	• Strong, removal-resistant enclosure, with tamper detection for entire envelope • Tamper response and zeroization circuitry active when keyed • Any ventilation holes/slits to include anti-probe design (e.g., 90 degree bends) • Include environmental failure protection (shutdown or zeroization, especially for temperature and voltage), or undergo environmental failure testing

The PSD shall use tamper detection countermeasures that respond to tampering by disabling the PSD from further use until completion of a physical inspection by USPS. The PSD ascending and descending register values shall be retained at the values present when the tampering was detected.

The PSD shall not provide any capability to bypass the security services of the cryptographic module.

B.4.7 PSD Access Control

The PSD shall employ security mechanisms to restrict unauthorized physical access to the contents of the module, thereby deterring unauthorized use and unauthorized modification (including substitution) of the PSD.

The PSD shall directly, or through the host system, authenticate any person who is authorized to perform the role of operator of the PSD, for example, by using a password and PIN, to meet FIPS PUB 140-1, Security Level 4 minimum requirement.

B.4.8 PSD Key Handling

PSD key entry and output, distribution, and storage shall be in conformance with FIPS-approved methodologies and with the IBIP Key Management Plan.

PSD keys shall be stored in plaintext form in the cryptographic module and shall not be accessible from outside the device.

The PSD shall include a mechanism to ensure that stored keys shall remain associated with the correct device ID and the customer to whom the key was issued.

The PSD shall provide the capability to zeroize all plaintext cryptographic keys and other unprotected security parameters within the module. There shall be no capability to zeroize the ascending or descending registers after initialization.

The PSD shall not output its private keys.

B.4.9 PSD Input and Output Requirements

The data ports for unencrypted, critical PSD-security parameters shall be physically separated from other data ports.

If plaintext authentication data (e.g., password or PIN) is used, the entry port shall be physically separate from any other cryptographic module data entry port and allow for direct entry of the data.

The PSD shall provide an output to indicate the status of the device.

B.5 PSD TESTING REQUIREMENTS

This section describes the testing requirements for the PSD.

The PSD shall be tested for conformance with FIPS PUB 140-1, Level 4 through the Cryptographic Module Validation Program by a cryptographic module testing laboratory that is a member of an accredited National Voluntary Laboratory Accreditation Program. When the PSD is shown to be in conformance with FIPS PUB 140-1 as required by these performance criteria, it shall receive a validation certificate. In addition, the PSD shall be evaluated and approved by the USPS, and receive IBIP approval. The PSD shall either employ environmental failure protection features or undergo environmental testing, as required by FIPS PUB 140-1, to the extent appropriate for its security level. Upon authorization for service to a customer, the PSD shall be tested for proper time stamping, signature generation, indicium data creation and output, signature validation, and maintenance of required data in its data storage registers. The PSD shall initiate and run self-tests to ensure proper operation in accordance with FIPS PUB 140-1.

Part
C
User Interface

(RESERVED)

Part
D
Key Management Plan

(RESERVED)

APPENDIX A

LIST OF ACRONYMS

AMS	Address Matching System
ANSI	American National Standards Institute
API	Application Program Interface
CA	Certificate Authority
CASS	Coding Accuracy Support System
CMLS	Centralized Meter Licensing System
CPU	Central Processing Unit
CRL	Certificate Revocation List
DMM	Domestic Mail Manual
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EC	Elliptic Curve
ECDSA	Elliptic Curve Digital Signature Algorithm
FIM	Facing Identification Mark
FIPS	Federal Information Processing Standard
IBI	Information-Based Indicia
IBIP	Information-Based Indicia Program
NIST	National Institute of Standards and Technology
OCR	Optical Character Reader
PCR	Print Contrast Ratio
PKCS	Public Key Cryptographic Standard
PKI	Public Key Infrastructure
PPKI	Postal Public Key Infrastructure
PRD	Print Reflective Difference
PSD	Postal Security Device
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
USPS	United States Postal Service
2 D	two-dimensional

APPENDIX B

GLOSSARY

Address Matching System (AMS) — used in conjunction with USPS ZIP+4 National Directory File to improve accuracy of mailpiece delivery. Also see "Code Accuracy Support System, AMS-II, Technical Guide." USPS National Customer Support Center (1-800-238-3150).

Alphanumeric — consists of the set of digits, letters, and some special characters such as spaces.

Ascending register — the register that keeps track of the total monetary value of all indicia ever produced by a specific meter or PSD.

ASCII (American Standard Code for Information Interchange) — a coding scheme using 7 or 8 characters to assign numeric values to up to 256 characters.

Background reflectance — the ability of the background portion of paper (as it relates to the surface containing the address, whether envelope, card, label, or insert) to be light enough in color to reflect a sufficient amount of light to the OCR's scanner.

Certificate Authority (CA) — an entity trusted by one or more users to create and assign certificates.

Closed System — a system whose basic components are dedicated to the production of information-based indicia and related functions, similar to an existing, traditional, postage meter; may be a proprietary device used alone or in conjunction with other closely related, specialized equipment; the Closed System device includes the indicium print mechanism.

Coding Accuracy Support System (CASS) — a process to improve the accuracy of ZIP Codes including ZIP+4 and delivery point (DP) codes appearing on mailpieces. Also see "Code Accuracy Support System, AMS-II, Technical Guide." USPS National Customer Support Center (1-800-238-3150).

Cryptographic — of or relating to codes that convert data so that a recipient shall only be able to read it using a specified decoding key. When cryptographic techniques are used for encryption, the specified decoding key is kept secret. When public key cryptographic techniques are used for authentication, the "private" encoding key is usually kept secret, but the corresponding "public" decoding key is publicly available to facilitate authentication of messages digitally signed using the private key.

Descending register — the register that keeps track of how much postage is remaining on a specific PSD or meter.

Digital Signature — a personal authentication method based on encryption and secret authorization codes used for signing electronic documents.

Digital Signature Algorithm (DSA) — an encryption algorithm based on the Digital Signature Standard; see FIPS PUB 186.

Elliptic Curve Digital Signature Algorithm (ECDSA) **—** an encryption algorithm using elliptic curves; see ANSI X9.62 for details.

FIM (Facing Identification Mark) — a pattern of vertical bars printed in the upper right portion of the mailpiece just to the left of the indicia, used to identify business reply mail and certain barcoded mail. The FIM is an orientation mark for automated facing and canceling equipment.

Firmware — software routines stored in read-only memory (ROM). Unlike random access memory (RAM), read-only memory stays intact even in the absence of electrical power. Startup routines and low-level input/output instructions are stored in firmware. It falls between software and hardware in terms of ease of modification.

Hashing — creating a map from a set of elements to a set of numbers based upon a hashing algorithm.

Host — the control logic that performs the functions required by the performance criteria. In the Open System version, the host is software, and, in the Closed System version, the host may be implemented in hardware, software, firmware, or a combination.

Information-Based Indicia Program (IBI/IBIP) — a program to support new methods of applying postage in lieu of the current approach that typically relies on a postage meter mechanically printing the indicium on mailpieces. In general, these new methods shall involve the use of a computer and printer to create and print indicia on mailpieces and labels.

Indicia/Indicium — the imprinted designations used on mailpieces denoting evidence of postage payment.

OCR (Optical Character Reader) — for the USPS, a piece of computer-controlled automated equipment that locates, reads, and interprets address information (contained on the face of a mailpiece), sprays a barcode, and sorts the mailpiece into a stacker.

Opacity — the ratio of the intensity of the light incident on a sample or object to that of the light transmitted through it.

Open System — a general purpose computer used for printing information-based indicia, but not dedicated to the printing of those indicia.

Padding string — a string of bits, usually zeros, that are added to force the data bits into a certain position.

PDF417 — a stacked 2 D barcode symbology developed by Symbol Technologies, Inc.

Print Reflectance Difference (PRD) — the background reflectance minus print reflectance and expressed as a percentage.

Private key — one of two keys used in the digital signature; the private is not shared and is used to create the digital signature.

Provider (also, Product/Service Provider) — the company providing the products and/or services, such as the different types of meters or forms of metering postage with the USPS.

Postal Security Device (PSD) — the device that provides security-critical functions for IBIP customers.

POSTNET (POSTal Numeric Encoding Technique) — the barcode used to encode ZIP Code information on letter and flat mail.

Public key — one of two keys used in the digital signature; the public key is the key that is released to the public and that can be used to verify the digital signature.

Reflectance — amount of or type of light reflected by envelopes that are able to be scanned by an OCR scanner to find out if the postage material is acceptable.

Rivest Shamir Adleman (RSA) — an encryption algorithm based on the difficulty of factoring large numbers.

Secure Hashing Algorithm-1 (SHA-1) — an algorithm that computes a 160-bit representation of a message which is useful in creating and verifying digital signatures.

Watchdog timer — as a function of the PSD, a process that precludes indicia creation by a PSD that has not been adequately audited; resets to its original value upon successful receipt of the device audit response message from the Provider.

Zeroize — to return to a zero value.

2 D Barcode — a two-dimensional barcode is a barcode that is read both horizontally and vertically.