INFORMATION-BASED INDICIA PROGRAM (IBIP)

PERFORMANCE CRITERIA FOR INFORMATION-BASED INDICIA AND SECURITY ARCHITECTURE FOR OPEN IBI POSTAGE EVIDENCING SYSTEMS

(PCIBI-O)

UNITED STATES
POSTAL SERVICE

February 23, 2000

The United States Postal Service (USPS)

Introduction

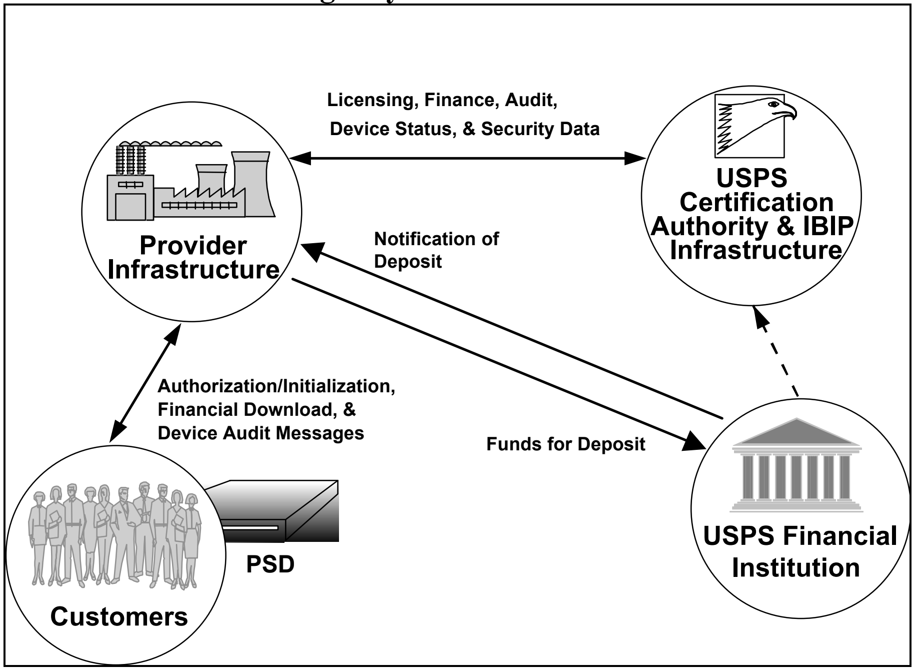
The United States Postal Service (USPS) initiated the Information-Based Indicia Program (IBIP) to enhance the security of postage evidencing[*] by supporting new methods of applying postage to mail. This document, "Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidencing Systems (PCIBI-O)," defines the requirements for the Open System elements of IBIP. An Open System is a system that uses a general-purpose computer and a printer which is not dedicated to the printing of indicia for printing information-based indicia.

System Overview

From a system context, the IBIP is designed to support customer, Product/Service Provider ("Provider"), and USPS operations. The IBIP architecture supports 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 following diagram. 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.

Target System Architecture


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

[*] The Postal Service is developing policies, procedures, and systems that will distinguish between postage meter and IBI postage evidencing systems.

Structure of the Performance Criteria

This document is a revision of the "Performance Criteria for Information-Based Indicia and Security Architecture for Open IBI Postage Evidencing Systems (PCIBI-O)," released July 15, 1999, and is composed of four major parts: Indicium, Postal Security Device, Host System, and IBIP Key Infrastructure. The current document organizes all of the relevant IBIP performance criteria needed for a Provider to participate in the IBI program for Open Systems. The following overview describes each of the parts:

- **Part A — Indicium:** This section of the PCIBI-O defines the requirements for the indicium (i.e., postage mark) to be applied to mail produced by Open Systems of the Information-Based Indicia Program.
- **Part B — Postal Security Device (PSD):** This section of the PCIBI-O 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 an Open System.
- **Part C — Host System:** This section of the PCIBI-O describes the performance criteria for the host system that supports an IBI Open System.
- **Part D — IBIP Key Infrastructure:** This section of the PCIBI-O describes the key registration process and attributes of the keys used in the IBIP digital signatures.

An Acronym List and a Glossary follow parts A through D.

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.

Year 2000 Compliance

All components of a system used to produce information-based indicia shall be year 2000 compliant. Year 2000 compliant means that the system shall accurately process date and time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations. The system shall properly exchange date and time data with other systems with which it must interface to meet the Performance Criteria.

Reference Documents and Resources

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

- "Performance Criteria for Information-Based Indicia and Security Architecture for Closed IBI Postage Metering Systems (PCIBI-C)," Draft, January 12, 1999.
- **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.

- **USPS Domestic Mail Manual** (DMM), Issue 55, January 10, 2000.
- **USPS International Mail Manual** (IMM), Issue 21, May 30, 1999.
- "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

Product Service Providers who choose to produce a postage evidencing product or service must comply with USPS Intellectual Property (IP) Requirements as a condition for receiving and maintaining regulatory approval. If a Product Service Provider is unable or unwilling to meet the IP Requirements, it should not offer the product or service.

Product Service Providers do not have authorization or consent from the USPS under 28 U.S.C. 1498(a) or otherwise to make or use any patented invention.

The USPS reserves the right and authority to discontinue a Product Service Provider's authorization to distribute a postage evidencing device or service if the USPS or a court determines that the manufacture of the device or service, the use of the device or service by mailers, or the validation of the indicia produced by the device or service, requires use of patented inventions for which Product Service Provider has not procured appropriate licenses.

This requirement applies to all aspects of the Product Service Provider's product or service, including those required or specified under applicable performance criteria.

TABLE OF CONTENTS

Part
A
Indicium

A.1 INTRODUCTION TO INDICIUM PERFORMANCE CRITERIA

A.1.1 Introduction

This part of the PCIBI-O defines the requirements for the indicium that is applied to mail produced by Open 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 in the human-readable portions of the indicium is defined in this part. Providershave some flexibility in the appearance of the indicium, provided the basic requirements contained in these performance criteria are satisfied.

The indicium provides the following features:

- <u>Printing Technology Alternatives</u> — The new indicium supports a number of printing technology alternatives (e.g., laser, inkjet, thermal).
- <u>Machine Readable</u> — Through the use of a two-dimensional barcode, the new indicium shall be readable using automated equipment.
- <u>Standard Ink</u> — 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 the reflectance standards defined in section A.5.6.
- <u>Fraud Mitigation</u> — The new indicium supports various fraud mitigation strategies that are incorporated into the overall IBIP security architecture. These strategies require an increased amount of information as compared with that provided by current indicia.
- <u>Support for Future Services</u> — The new indicium offers the flexibility to provide support for new services that the USPS may wish to offer in the future. (These performance criteria do not specifically provide for these services.)

The IBIP supports new methods of applying postage in lieu of the traditional approachthat typically relies on a postage meter mechanically printing often-identical indicia on mailpieces. In general, these new methods involve the use of the host system and a printer to create and print unique indicia on mailpieces, envelopes, or labels.

A.1.2 Overview of Indicium Performance Criteria

The following presents an overview and general description of each of the remaining sections of the indicium performance criteria:

- **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, such as reflectance, 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 the DMM. The barcoded information shall meet the requirements for the IBI 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 data, as well as binary format data for 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 supports 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	—	—
- Registration ZIP Code	Yes	No	4	10
Destination Delivery Point	Yes	No	5	11
Software ID	Yes	No	6	12
Descending Register	Yes	No	4	13
Mail Class or Category				
- Rate Category	Yes	No	4	14
- Endorsement (Mail Class)	No	Yes	—	—
Digital Signature	Yes	No	DSA 40 RSA 128 ECDSA 40	15
Reserved Field	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 in 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 – 9) and the second alpha (A – 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 during the life cycle of the PSD. The data shall be represented in a 5-byte binary value.
- **Postage** — This data element represents the amount of postage applied to this specific mailpiece. Postage applied is in accordance with the then-current USPS postage rates in the DMM or the IMM The postage amount shall be represented in a 3-byte binary value in the numeric format 999.999. This field size supports the maximum amount of postage due on a single piece of mail in any mail class supported by the system.
- **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 human-readable field represents the city, state, and 5-digit ZIP Code for the registration 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 registration post office ZIP Code must appear in place of the city designation and state, respectively.

- **Originating Address: Registration ZIP Code** — This data element represents the registration post office delivery point identification. The format shall be a 5-digit numeric value represented by a 4-byte binary value in the indicium.
- **Destination Delivery Point** — This data element represents the destination delivery point. The format shall be a 5-byte binary value in the indicium. For domestic mail, the destination ZIP Code shall be used for this data element.

  Formail with an international destination, the first 2 bytes of this data element are the two-character country code, per ISO 3166-1 Alpha-2 code, of the destinating country. The next 2 bytes of the data element shall contain the 16-bit little endian value of the total number of characters in the address block. The last byte shall contain a binary zero.
- **Software ID** — This data element represents the host system software identification number, which has a length of no more than 12 digits. It shall be represented by a 6-byte binary value in the indicium.
- **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 classand rate. The USPS provides values for this field. 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, beyond those shown in Table A-1, the length of this field will be appropriately specified for those algorithms.
- **Reserved Field** — 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 a binary value of zero.

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

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 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 portions of the mailpiece indicium. If additional postage is to be added, a postage correction indicium maybe placed on the mailpiece. The postage correction indicium shall contain both barcode and human-readable information. The data elements shall be as specified in Table A-2, with the addition of the word "CORRECTION" to the human readable information The location of the postage correction indicium on the mailpiece is specified in the DMM

Table A-2. Correction 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	—	—
- Registration 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
Mail Class or Category				
- Rate Category	Yes	No	4	14
- Endorsement (Mail Class)	No	Yes	—	—
Digital Signature	Yes	No	DSA 40 RSA 128 ECDSA 40	15
Reserved Field 2	Yes	No	Variable Size	16

The first reserved field in the correction indicium replaces the Destination Delivery Point field in the standard indicium, and is the same length. This field shall have a binary value of zero.

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 are supported by the IBIP. A Provider is at liberty to choose the digital signature algorithm most appropriate for its 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 from third parties any required rights, 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, *Digital Signature Standard*. 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

Cryptographic, 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 registration post office, as well as the endorsement (mail class). 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 the DMM.
- 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 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 inch from the right edge of the mailpiece and 1/4 inch 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 for First-Class Mail, the requirements for FIM type and placement are in accordance with the DMM.

A.5.3 Indicium Printing

As a general guideline, the barcode portion of the indicium should be printed using 300 dots per inch; however, indicium readability is the ultimate determining factor of whether or not the system is usable for printing postage. Readability requirements could increase, or decrease, the printed dots per inch requirement. Readability of the barcode portion of the indicium 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 the DMM. All indicia used in an IBI product must be preapproved by the Manager, Postage Technology Management. This approval includes all elements in the indicium as defined by these performance criteria and includes the entire area within the following boundaries:

- The right hand edge of the envelope.
- The top edge of the envelope.
- The bottom edge of the 2 D barcode or any other indicium element.
- The left most edge of the 2 D barcode or any other indicium element.
- A one-half inch (1/2") clear zone to the left of and below these indicium boundaries.

An approved indicium must not include any image or text within the boundaries defined above that is not required by the IBI Performance Criteria or is not a postal marking required or recommended by postal regulation.

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)

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

B.1.1 Introduction

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

B.1.2 Overview of Postal Security Device Performance Criteria

The following is an overview and general description of each of the remaining sections of the PSD performance criteria:

- **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.

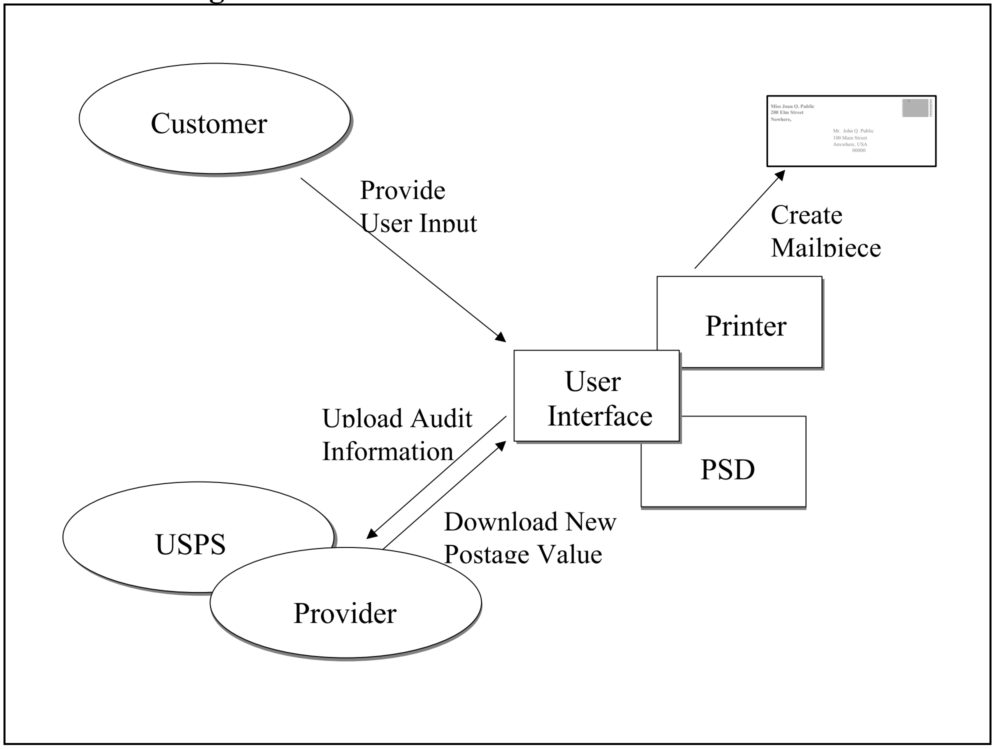
B.2 POSTAL SECURITY DEVICE (PSD) OVERVIEW

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 shall have no functions except as related to the generation of approved information-based indicia and as described in these performance criteria.

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 during the life cycle of thePSD (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, *Security Requirements for Cryptographic Modules,* 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 implementation of the IBIP device authorization, finance, indicium creation, and device audit functions, which are further described in section B.2.2.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 to 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 for a given PSD. The process includes loading the device serial number and initializing the ascending and descending registers.

B.2.1.1.1 PSD Reinitialization Function

A PSD that is in the possession of the Provider can be reinitialized if the serial number of the device is changed and the ascending and descending registers are reset to zero. Reinitialization, with its assignment of a new serial number, ends the life cycle of the device with the previous serial number.

B.2.1.2 PSD Digital Signature Function

The PSD digital signature function uses the signing key generated in the PSD. 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 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 registered 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 initiated payment for the amount to be downloaded. When an IBIP system is withdrawn from use, the IBIP finance function also allows the user to obtain a refund of the postage value remaining on the PSD.

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 that 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 this section. 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. Section B.3.3 describes requirements for implementation of other digital signature capabilities.

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 and Reinitialization

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 or during Reinitialization The serial number shall be written to nonvolatile memory in the PSD during device initialization or reinitialization.

During the initialization (or reinitialization) process, all internal registers and counters in the PSD shall be explicitly initialized to their intended initial values When the PSD is initialized by the PSD manufacturer or IBI Provider 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 disabled after the operation is complete to ensure the registers cannot be reinitialized by the user

The Provider may reinitialize a PSD only when it is in the Provider's possession. Reinitialization of the PSD is accomplished by assigning a new serial number to the PSD.

When the new serial number is assigned to the PSD, the ascending register showing total postage used shall be reinitialized and the old serial number for the PSD shall be reported to the Postal Service as a scrapped device

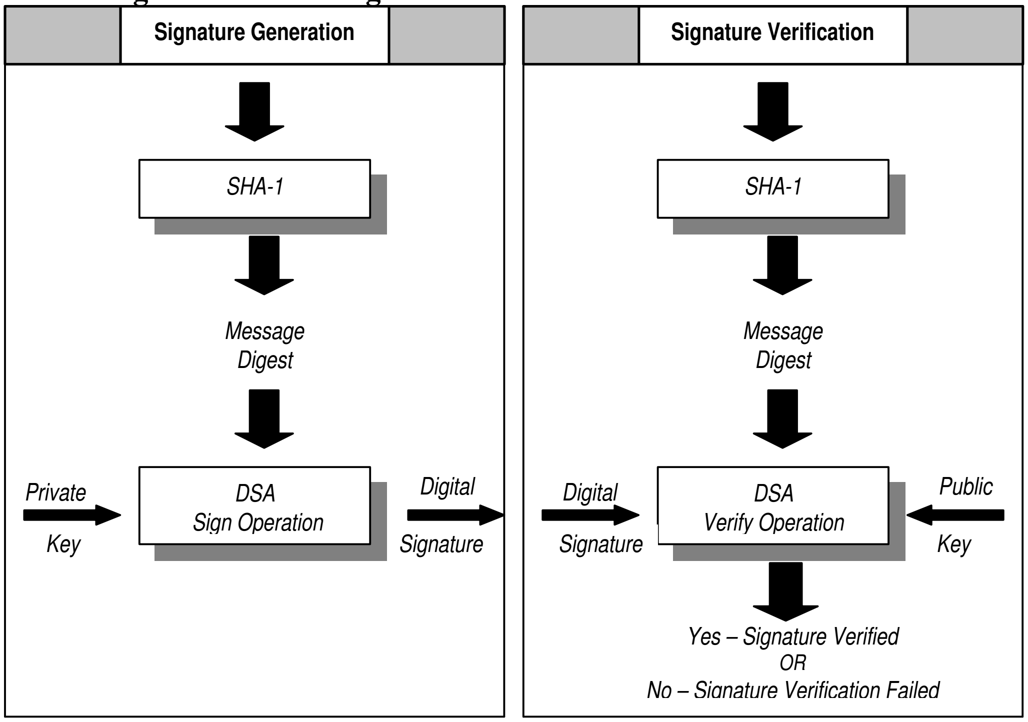
B.3.1.2 PSD Digital Signature Functions

The PSD shall implement DSA, RSA, or 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-O.

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, *Digital Signature Standard*, 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 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 in FIPS PUB 186. In accordance with that standard, the Secure Hash Algorithm (SHA-1), as specified in FIPS PUB 180-1, *Secure Hash Standard*, 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

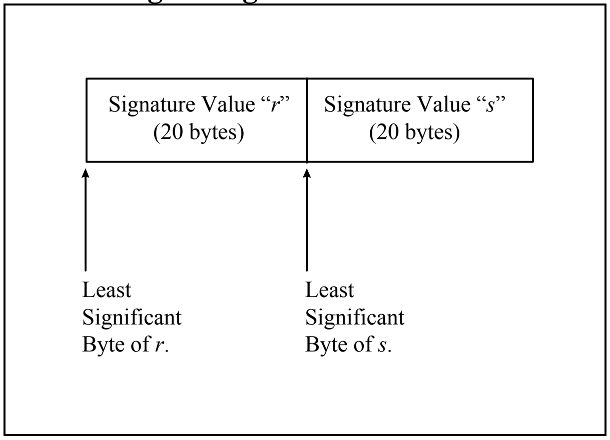
Field Number	Field Name	Number of Bytes	Order*
1	Indicia Version Number	1	N/A
2	Algorithm ID	1	N/A
3	Certificate Serial Number	4	Start with least significant byte
4	PSD Manufacturer ID	2	N/A (text field)
5	PSD Model Number	2	N/A (text field)
6	PSD Serial Number	4	Start with least significant byte
7	Ascending 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	Registration ZIP Code	4	Start with least significant byte
11	Destination Delivery Point	5	Start with least significant byte
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.

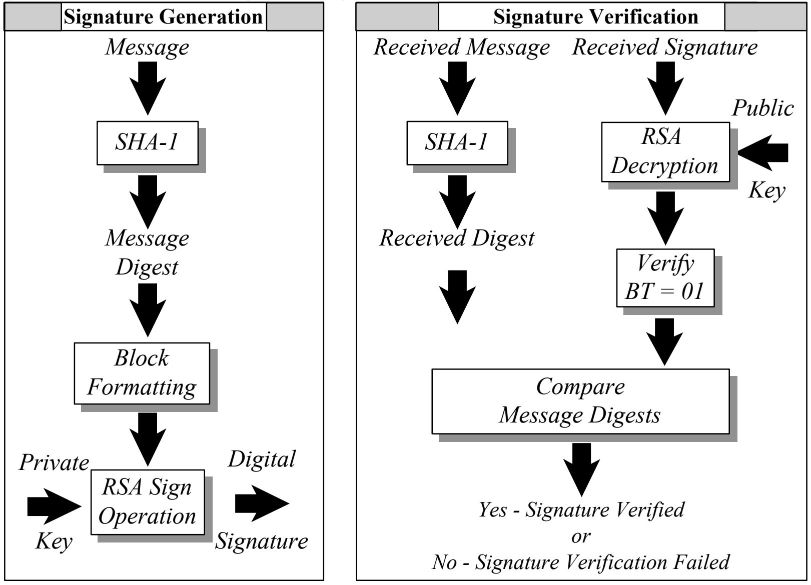
Figure B-3. Digital Signature Field Format for DSA


Signature Value "*r*" (20 bytes)
Signature Value "*s*" (20 bytes)
Least Significant Byte of *r*.
Least Significant Byte of *s*.

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. Specifically, 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 placed 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 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*

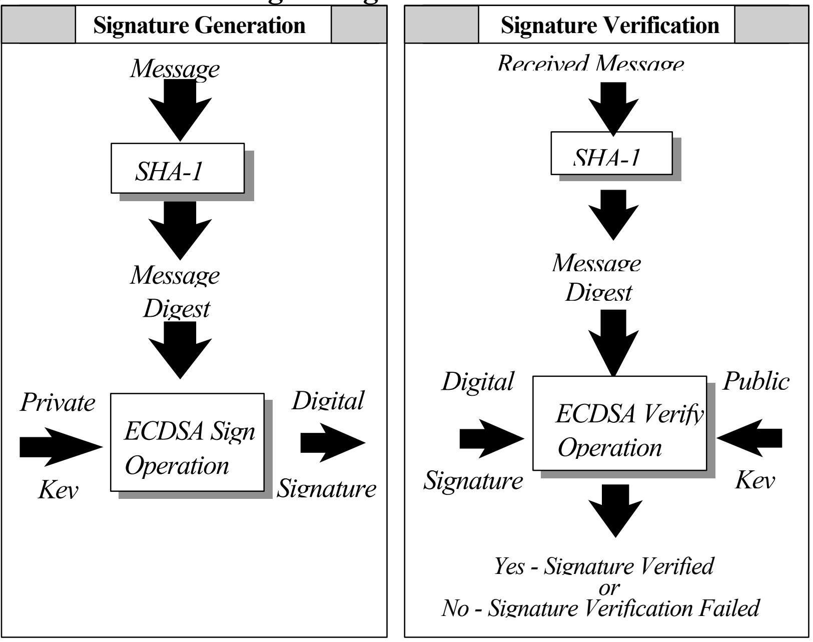
B.3.1.2.2.2 RSA Message Digest

The PSD shall perform the hash function using the Secure Hash Algorithm (SHA-1), as specified in the Secure Hash Standard in 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 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$ 999,999,999.999
- Descending Register: US$ 999,999.999

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 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.3.2.2 Similarly, 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 or reinitialized 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 registration ZIP Code. The Provider must reprogram a PSD with the appropriate device authorization information if the Provider issues the PSD to a different customer, 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. Device authorization does not include resetting the value in the ascending or the descending register. These values can only be set when the device is initialized or reinitialized.

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 registration ZIP Code.

B.3.2.1.3 Private/Public Key Processing

The PSD shall handle public and private key processing as detailed 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 the number of the 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. The maximum value is in accordance with section A.2.

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, unless the PSD is in the Provider's possession and is reinitialized 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.

In addition, the IBIP finance functions allow the user to obtain a refund of all postage remaining when the PSD is withdrawn from service. The automated process for obtaining a refund requires the PSD and host system to work with the user and the Provider infrastructure to produce a message containing the required data elements and digital signature to ensure a proper refund.

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 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.3.2.2.2 Remaining Postage Refund Transaction

When a PSD is withdrawn from service, the PSD shall support the process of obtaining refunds for the postage value balance remaining on the PSD.

The host system prepares the postage value refund request message and transmits it to the PSD. The PSD shall then sign the message and zeroize the descending register The watchdog timer shall also be "timed out" so that no further transactions are possible

The postage value request message shall then be returned 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 modifications and replay.

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.

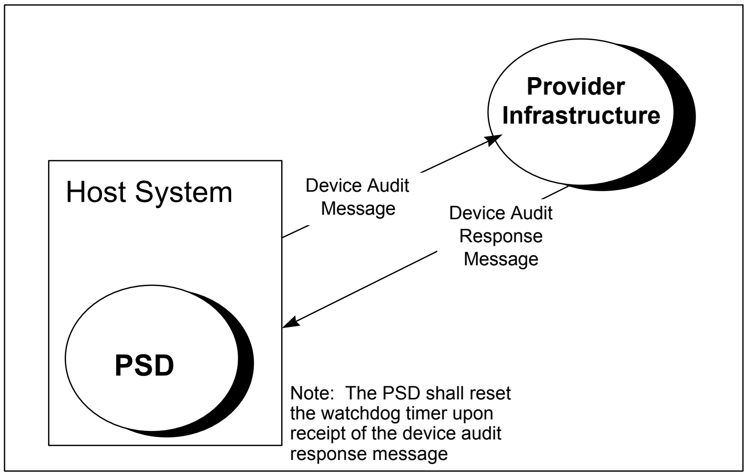
B.3.2.3.4 Indicium Creation Results Output

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 private key generated by the PSD to complete the indicium creation process. The PSD may use the same private key for other IBIP authentication and verification requirements at the discretion of the Provider, and approval of the USPS. The USPS must approve the contents of all messages signed by the PSD. All digital signature functions of the PSD shall be related to the generation of postage, as described in these performance criteria.

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, physical security level 3, 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 levels 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.
Physical Security	PSD Physical Security requirements.	Security level 3.

FIPS 140-1 Design Category	Proposed PSD Performance Criteria/ FIPS 140-1 Requirements	Comment
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 DSA, RSA, or 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 authentication/verification data required 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 module. Included within this boundary shall be all cryptographic components, all processors, software, firmware, and other components that implement IBIP required PSD processes and functionality. The physical security requirements for different PSD module implementations 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

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 (EFP) (shutdown or zeroization, especially for temperature and voltage), or undergo environmental failure testing (EFT).	• Production-grade chips. • Strong, opaque, 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 (EFP) (shutdown or zeroization, especially for temperature and voltage), or undergo environmental failure testing (EFT).	• Production-grade chips. • Strong, opaque, non-removable 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 (EFP) (shutdown or zeroization, especially for temperature and voltage), or undergo environmental failure testing (EFT).

*If a single-chip cryptographic module is used to meet some or all of the IBIP Performance Criteria, the associated PSD must meet the requirements in this Table for Multi-Chip or Multi-Chip Stand-Alone implementations.

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. The physical security protections of the PSD must not be easily tampered, circumvented, or disabled.

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 Infrastructure.

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 except during initialization or reinitialization,which shall only occur when the PSD is in the possession of the Provider.

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

The PSD shall be tested for conformance with FIPS PUB 140-1, physical security level 3, and FIPS PUB 140-1 EFP/EFT Requirements. Testing shall be 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.

This testing shall include any attack procedures known to the USPS, whether or not such procedures are included in the current FIPS PUB 140-1 requirements. In addition, the PSD shall be evaluated and approved by the USPS and receive IBIP approval. 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
Host System

C.1 INTRODUCTION TO HOST SYSTEM PERFORMANCE CRITERIA

C.1.1 Introduction

This part of the Open System Performance Criteria defines the requirements for the open system host element of the IBIP. The host shall assist users in creating the new information-based indicia. The host system serves as one of the three basic components (host, printer, PSD) required to produce the information-based indicia and to provide the interface between the user, the PSD, and the Provider, as shown in Figure B-1, in part B of this document.

C.1.2 Overview of Host System Performance Criteria

The following is an overview of each of the remaining sections of the host system performance criteria:

- **Section C.2 — Host System Overview:** This section specifies the host system core functions and the role the host system plays in the implementation of IBIP-specific functions.
- **Section C.3 — Host System Functional Requirements:** This section specifies the functional requirements to implement the host system core functions and to support the implementation of IBIP-specific functions.

C.2 HOST SYSTEM OVERVIEW

The host system is defined as the control logic that performs the host system core functions as described in the performance criteria. The core functions of the host system are user authentication, configuration management, operational status checks, mailpiece production, communications management, log file and safe-store management user interface, and user education and support. The location of each element of the host system, whether on the user's computer or the Provider's computer, is product-specific.

The host system core functions support implementation of IBIP-specific functions including device authorization, finance, indicia creation, device audit, and the security functions of the PSD.

C.2.1 General

The following general comments regarding the customer and Provider infrastructure, tailoring the functional capabilities of the host system, and additional host system functionality apply to the overall host design.

C.2.1.1 Customer and Provider Infrastructures

The host system and the PSD comprise the customer infrastructure and may reside at the user's site or the Provider's site, as determined by the Provider's concept of operations for the product. The host functions contribute to the overall IBIP functions of device authorization, finance, indicia creation, and device audit, and, in addition, support the security functions of the PSD. The PSD is a NIST-certified, secure device that maintains financial records for postage and provides essential security elements, including the digital signature for the indicia. For a complete discussion of the functions of the PSD, see part B of this document.

The Provider shall supply an infrastructure consisting of information systems as well as Provider processes, policies, and personnel to support installed systems at customer sites. The host communicates with the Provider infrastructure as necessary to support postage value download and device audits. The host system also receives software and critical information updates. The host system does not communicate directly with the USPS infrastructure. The Provider infrastructure may interact with the USPS infrastructure either in the course of, or as a result of, interactions with the host system. For example, the Provider infrastructure interacts with the USPS infrastructure to obtain registrations for users on behalf of the Postal Service and to provide reports of postage value downloads.

C.2.1.2 Host System Functional Capability Tailoring

Providers may have differing business models for distributing and supporting IBI products. These performance criteria apply to all business models. The Provider may propose to satisfy a given requirement by means of a procedure based on the Provider's business model, rather than by means of a function performed by the host component of the system.

C.2.1.3 Additional Functionality

These performance criteria identify the minimum set of functions a product must perform before gaining approval under the IBI program. The Provider may desire to offer comprehensive mail systems that include additional capabilities beyond the functions described in these performance criteria. The Provider is not prevented from offering added features. However, any features affecting the preparation or processing of mail must comply with appropriate USPS regulations.

C.2.2 Host Functional Requirements

This section presents requirements for the minimum host system functions. The functions are defined briefly in the following sections. Figure C-1, Host System Functions, illustrates the interactions between the user interface and communications management functions and the remaining core host functions.

Figure C-1. Host System Functions

User Interface					
User Authentication	Configuration Management	Operational Status Checks	Mailpiece Production	Log File and Safe-Store	User Education and Support
Communications Management					

C.2.2.1 User Authentication

The user authentication function of the host, in conjunction with the PSD, shall provide the means to prevent unauthorized access to the PSD.

C.2.2.2 Configuration Management

The configuration management function ensures the user's system configuration is current. Some of the functions of configuration management include configuring the host system for initial installation and setup, system modifications, and system uninstall; host system software update; and host system critical information update for the postal rate table USPS ZIP+4 National Directory CD-ROM, public-key certificates, and user profile.

C.2.2.3 Operational Status Checks

The operational status check functions ensure the PSD is operational; the host software is properly configured; the user profile data is current; all values of registers, dates, and timers are within accepted ranges; and the essential hardware and software elements are functioning properly. These checks generally occur at the start of each user session.

C.2.2.4 Mailpiece Production

The mailpiece production function of the host system is responsible for generating the elements of a properly formatted mailpiece front, including the USPS-approved indicia, the FIM (where required, a valid delivery address, and a POSTNET barcode (where required. These elements shall be formatted and positioned on the mailpiece or label in accordance with USPS requirements.

C.2.2.5 Communications Management

The communications management function is responsible for relaying messages among the various components of the system, including the PSD, the Provider infrastructure, and the host; and for establishing communications to support configuration management.

C.2.2.6 Log File and Safe-Store Maintenance

The log file and safe-store maintenance function of the host system shall maintain log files with entries relating to user activity, and shall provide a safe-store function to protect selected, critical information against loss. The log files record use of the system and provide automated records containing information required by the USPS. The safe-store function involves creating copies of critical information, including log files, which can survive catastrophic system failures.

C.2.2.7 User Interface

User interface functions shall allow the user to control and operate the system, obtain status information, and perform quality assurance functions. The user interface may also provide the means for the user to apply for and update user registrations and leases.

C.2.2.8 User Education and Support

The user education and support function provides users with information on how to use and operate the system and informs them of their responsibilities with respect to the use of information-based indicia.

C.2.3 IBIP-Specific Functions

The host system functions support the IBIP-specific functions, namely device authorization, finance, indicia creation, and device audit, as well as the PSD security functions. The IBIP-specific functions supported by each of the host system functions are identified in Table C-1, Relationship of Host and IBIP Functions. A brief introduction to each of the IBIP-specific functions follows the table. See section C-3 for the functional requirements the host system shall meet in support of each of these functions.

Table C-1. Relationship of Host and IBIP Functions

	IBIP Functions				
Host Functions	**Device Authorization**	**Finance**	**Indicia Creation**	**Device Audit**	**PSD Security Functions**
User Authentication		√	√		√
Configuration Management	√	√	√	√	√
Operational Status Checks		√	√	√	√
Mailpiece Production			√		√
Communications Management	√	√	√	√	√
Log File and Safe-Store Maintenance		√	√	√	
User Interface	√	√	√	√	
User Education and Support	√	√	√	√	√

C.2.3.1 IBIP Device Authorization

The host system supports the IBIP authorization process to ensure only an authorized device can support the creation of valid indicia.

C.2.3.2 IBIP Finance

The host system communicates with the Provider infrastructure, as necessary, to support the IBIP finance functions, which allow the user to obtain postage. In order to download postage into the PSD, the customer must have initiated payment for the amount to be downloaded The finance function also allows the user to obtain refunds for remaining postage value when the PSD is withdrawn from service.

C.2.3.3 IBIP Indicia Creation

The host system and the PSD shall jointly perform functions necessary to create valid indicia in accordance with the performance criteria for the indicia in part A.

C.2.3.4 IBIP Device Audit

The device audit function allows the USPS to ensure proper use of the system.

C.2.3.5 IBIP Security Functions

The host system core functions support implementation of the core security functions of the PSD, namely, initialization, digital signature generation and verification, and register management.

C.3 HOST SYSTEM REQUIREMENTS

This section identifies the minimum functional requirements a host system must meet.

C.3.1 General

The following general requirements affect the overall host design.

C.3.1.1 Single and Multiple PSD Operations

These performance criteria are written as if host system interacts only with a single PSD. That is, the performance criteria presume that the user neither changes the PSD during a session of use, nor uses a different PSD from one invocation of the host to another. If the system concept allows the use of only one PSD, Providers shall document their concepts for preventing use of the host with multiple PSDs.

However, if the use of multiple PSDs by a given user is essential to the system concept, the Provider shall show how the system satisfies all the other requirements of these performance criteria. The Provider must develop a concept of operations and product design for the multi-PSD environment that protects Postal Service revenue and ensures the security and integrity of the system functions in accordance with the performance criteria for single PSD systems, as described in this document. Specifically, transactions involving the PSD and the host system shall ensure that a transaction initiated by any one given PSD can affect only that PSD, and that all host system records, such as log files, shall be related to the responsible PSD.

C.3.1.2 Single and Multiple User Operations

Similarly, these performance criteria are written as if the host system operates on a single user workstation operated by a single individual. If, however, the Provider develops a host system that is to be shared by a community of users, the Provider must develop a concept of operations and product design for the multi-user environment that protects Postal Service revenue and ensures the security and integrity of system functions in accordance with the performance criteria for single user systems described in this document.

C.3.1.3 Reliability and Robustness of Communications

Host system functions may involve a sequence of communications between the host system, the PSD, and/or the Provider infrastructure. The purpose of the communications sequence is to provide for the consistent update of user, Provider, and USPS databases. The Provider shall ensure updates affecting the host system occur if, and only if, all corresponding updates occur to corresponding Provider and USPS records. The Provider shall ensure consistency of database updates regardless of system and communication failures.

C.3.1.4 Millennium Change

The host shall maintain the proper ordering and relationship of all dates, both those prior to the year 2000 and those in the year 2000 or later.

C.3.2 Host System Functional Performance Criteria

C.3.2.1 User Authentication

The host, in conjunction with the PSD, shall prevent unauthorized access to the PSD by use of passwords, PINs, or other means approved by the USPS. The intent is to prevent a stolen PSD from being depleted of its remaining postage.

C.3.2.2 Configuration Management

The configuration management functions shall ensure the proper installation and configuration of the host system. The configuration management function shall ensure that updates and modifications to the host system are made in accordance with the performance criteria.

C.3.2.2.1 Host System Configuration

The host system, or a USPS-approved Provider procedure, shall be employed to ensure the IBIP system configuration in use is current. Specifically, the system shall be configured for the underlying software and hardware and all components shall have current USPS approval.

The major software components are the host system programs and the databases. The host system software shall have an identification number consisting of up to 12 digits. This number is the "Software ID" field included in indicium. See part A of this document. The specific database components are the USPS Address Matching System (AMS), consisting of software and the ZIP+4 National Directory CD-ROM; the postal rates associated with the mailing classes and rate categories supported by the system; and the user profile consisting of information from the user registration file and user system information.

The host system shall verify the configuration to ensure host system resident programs and critical information are as approved by the USPS and have not been modified.

C.3.2.2.1.1 Initial Installation and Setup

The host system shall provide functions and capabilities to allow the user to install host system software that is appropriately configured for the underlying software and hardware. The host system shall automatically detect, or query the user for, information regarding system resources and peripherals used by the host system. The host system shall determine whether the available resources and devices satisfy the stated minimum configuration requirements. The host system shall determine whether the system can perform the essential functions of indicia preparation. During the installation process, the system shall verify the host can communicate with the PSD and the Provider infrastructure and is able to send and receive information.

Configuration and installation of the system may involve selection of device driver software appropriate for the specific devices and/or copying appropriate software components and data from the distribution media for incorporation in the host system.

C.3.2.2.1.2 System Modifications

The host system shall be capable of modifying the installation and configuration of the host system at the user's request or upon detecting substantive changes to the configuration. The host shall perform all necessary actions to change the configuration, including changing the Provider infrastructure records and updating user registration and user profile information, as appropriate for the configuration change. The host system shall have the capability to roll back to the previous configuration in the event it cannot confirm the integrity of an attempted configuration update.

C.3.2.2.1.3 Uninstall

The host system shall be capable of removing software and databases. The system shall provide the capability for either the user or the Provider infrastructure to initiate the uninstall function.

Performing the uninstall function immediately after completing the install function should return the host system to its state prior to the install. If the uninstall function is invoked after at least one log file has been created, then the uninstall function should not delete any log files containing postage download or mailpiece creation records without first providing for the transmission of existing log files to the Provider infrastructure and then giving the user the opportunity to safe-store or retain the log files.

C.3.2.2.2 Host System Software Update

Upon each communication with the Provider infrastructure, the host system, through interaction with the Provider infrastructure, shall determine whether any changes to the host software configuration are required. If changes are required, they shall be made before producing any more indicia or increasing the postage value available. Acting under the direction of the Provider infrastructure, the host shall receive modifications from the Provider infrastructure and install them or else instruct the user regarding actions necessary to update the host configuration.

If the software update mandates a resultant change to the software identification number, the change shall be made in the user profile.

C.3.2.2.3 Host System Critical Information Update

The host shall ensure critical system information is current. The critical information that shall be kept current includes the postal rate table, the USPS Address Matching System ZIP+4 Directory, public-key certificate information and the user profile. Upon each communication with the Provider infrastructure, the host system, through interaction with the Provider infrastructure, shall determine whether any critical system information needs to be updated. If an update is required, it shall be made before producing any more indicia, completing a postage value download transaction, or performing a device audit resulting in the resetting of the watchdog timer.

C.3.2.2.3.1 Postal Rate Table Update

If the postal rate table is not current, the host system shall either update the rate table or inform the user of any action necessary to obtain a current version. The Provider shall ensure users have a reliable method of obtaining the new postal rate table before the current table expires.

C.3.2.2.3.2 USPS ZIP+4 National Directory (CD-ROM) Revision

If the USPS ZIP+4 National Directory is not current, the open system host shall either update the Directory, or inform the user of any action necessary to obtain a current version. The Provider shall ensure users have a reliable method of obtaining a new directory for the USPS ZIP+4 CD-ROM before their current directory expires.

C.3.2.2.3.3 Public-Key Certificate Update

If a public-key certificate has expired, action shall be initiated by the host system to obtain a current certificate, or the user shall be informed of the actions necessary to obtain a current certificate. If a certificate expiration is pending, the host system shall so inform the user and advise of any action necessary to obtain a new certificate. If a public-key certificate has expired, the host system shall prevent the PSD from performing any IBIP functions other than obtaining a new certificate.

C.3.2.2.3.4 User Profile

The host shall maintain a user profile that contains critical information about the host installation and the responsible owner or user of the system. The user and installation information shall include, at a minimum, the information the USPS requires in the *Application or Update for a Registration to Lease and Use Postage Evidencing Systems* (PS Form 3601-A), the information returned with the *Registration to Lease and Use Postage Evidencing Systems* (PS Form 3601-B), as well as the software identification number and the PSD serial number.[*]

C.3.2.3 Operational Status Checks

The host system, upon start-up, shall perform general checks to ensure the configuration is proper and essential hardware and software items are functioning. These checks shall:

- Verify host system software programs are current in accordance with configuration management requirements.
- Verify the USPS ZIP+4 National Directory CD-ROM is current and has not changed.
- Verify the user profile data, including user registration and user system information, is current and has not changed.
- Verify the current date is neither on nor after the effective date of any previously noted pending rate change, and the postal rate table is current and has not changed.
- Verify no significant, detectable changes have occurred in the system hardware configuration. Changes are significant if there is reason to expect the host could not perform any of its required functions.
- Verify the PSD is operational and is the expected PSD.
- Verify the PSD watchdog timer has not expired.

[*] The Postal Service is developing policies, procedures, and systems that will distinguish between postage meter and IBI postage evidencing systems.

- Verify the maximum values of the ascending and descending registers in the PSD do not exceed the maximum allowable values, as given in the performance criteria.
- Verify public-key certificates have not expired
- Verify the Provider infrastructure had not previously notified the host system of a user registration revocation.

If the host fails any of these verifications, it shall prevent indicia printing, postage value downloads, or a device audit to reset the watchdog timer, until the cause of the verification failure is corrected. The host shall inform the user regarding the nature of the verification failure and the actions necessary to correct the situation.

The operational status check shall determine if the previous session terminated while communications were in progress, and, if so, note the status of the disrupted activity. The disrupted activity should be completed, undone, or rolled back.

The host system should inform the user of any operational status checks that indicate there will be problems in the near future, such as an approaching expiration date.

C.3.2.4 Mailpiece Production

C.3.2.4.1 Standard Services

The host shall produce the mailpiece front, including the delivery address, the POSTNET barcode (where required), the FIM (where required), and the indicium, as an integral unit. The host may print this unit on the actual mailpiece stock or on label(s) for later attachment to the mailpiece. The host shall indicate to the user when the FIM is required on the mailpiece, but shall also provide the user with an option to omit the FIM in those instances when the FIM is preprinted on the mailpiece, or it is not required for the given mail class, or is not required for another reason

The location of the various mailpiece components (indicium, POSTNET barcode, delivery address, and FIM), and the overall appearance of the mailpiece, shall comply with the requirements in the DMM and Publication 25, *Designing Letter Mail*, for the given class of mail and size of mailpiece, for mail with a domestic destination. For mail with an international destination, the overall appearance of the mailpiece shall comply with the requirements in part 145.3 of the IMM for the given class of mail and size of mailpiece.

The indicium component of the mailpiece shall comply with the performance criteria for the indicium as given in part A of this document. The user shall only print a USPS-authorized indicium that has been preapproved by the Manager, Postage Technology Management.

A complete and accurate date shall be printed on the mailpiece. The host system shall not allow mailpiece generation with a mailing date earlier than the current calendar date. The date of the indicium shall represent the actual date of deposit of the mailpiece. In some cases, a correction of the date may be needed. See part A of this document for the criteria for the redate indicium.

A mailpiece may be generated with a date of mailing in the indicium not exceeding 30 days in advance of the date on which the mail is to be deposited with the Postal Service. The host system shall ask the user to actively acknowledge a notification that mail will not be accepted by the Postal Service prior to the mailing date in the indicium when that date is more than one day in advance of the date of deposit of the mailpiece

For domestic mail the host shall integrate and use the USPS Address Matching System (AMS) Application Program Interface (API) to produce a standardized address for the mailpiece. The host may perform the ZIP+4 validation at the time of indicia creation or may provide another method that satisfies USPS requirements for the proper ZIP+4 coding. The standardized address shall include the standard POSTNET delivery point barcode.

For mail with an international destination, the formats of the origination and destination addresses are in accordance with part 122 of the IMM.

C.3.2.4.2 Expedited and Special Mail Services

The host system shall assist the user in the preparation of mailpieces that take full advantage of expedited and special mail services Expedited services include Express and Priority Mail, as well as International Express Mail, Global Priority Mail, and Priority Mail Global Guaranteed. Special services include Certified Mail and other services, such as delivery confirmation, as they become available.

In addition to preparing the indicia to indicate payment for expedited and special mail services, the host system shall complete the special forms for these products, including the generation of a one-dimensional barcode and a tracking number. The USPS will supply the allowable tracking numbers to the Provider. The format of the special forms and generation of the tracking information will be addressed in a future version of this document

C.3.2.5 Communications Management

The host system shall provide communications with the Provider infrastructure for downloading postage, performing device audits, obtaining software and critical information updates, replacing expired or revoked certificate information and transmitting log files. The selection of the transmission media and security protocol is left to the Provider.

If the given system supports the ability to obtain or maintain a user registration through the host system, communications shall be provided to support that function as well. Communications involving user registration require strong identification and authentication of the host or PSD to the Provider infrastructure, and of the Provider infrastructure to the PSD and the host.

The host system shall implement effective communication between the user and the Provider infrastructure. The host system shall select the connection method from those supported by the USPS as part of the initial system setup and subsequently establish the communications channel as needed to support the functions described in these performance criteria

The host system shall be designed to recover from communications failures that could occur at any point in the process, including any supporting interaction between the USPS and the Provider infrastructure. Possible actions to take when a failure occurs include restart or rollback. In the event of lost communications, and if communications cannot be reestablished during the current user session, the host system shall be capable of returning the system to the state existing at the time of the interruption.

C.3.2.6 Log File and Safe-Store Maintenance

The host shall maintain a log file that records significant events. All transactions relating to indicia creation, funds transfer, or device audits must be logged. The host system shall provide for automatic transmission of log files from the host system to the Provider infrastructure. The host system shall also provide a capability to safe-store information.

C.3.2.6.1 Log File Entries

Postage value downloads, indicia creation, and PSD audit messages are specific event entries that shall be included in the log file. Additional events may be logged at the Provider's discretion. The log file must be designed to prevent easy access from any software other than the host system. The following sections detail the fields required for each of the required log file entries.

C.3.2.6.1.1 Postage Value Download Log File Entry

An entry shall be made to the log file to record each postage value download. The postage download message, showing the transaction amount, shall be included in the entry. The entry shall contain a result code that indicates whether the download succeeded or failed and the reason(s) for any failure. Table C-2, Postage Value Download Log File Entry, lists the specific fields required. The register values recorded in the log file are those at the completion of the download process.

Table C-2. Postage Value Download Log File Entry

Fields	Format or Value			
PSD Device ID: Manufacturer ID Model ID Serial Number	 ASCII, 2 characters ASCII, 2 characters Numeric, 10 digits			
Date and Time of Log Entry	YYYYMMDD/HH:mm:SS			
Log Entry Type	06			
Transaction Amount—Postage Download Message	Numeric, 999.99			
Ascending Register	Numeric, 999,999,999.999			
Descending Register	Numeric, 999,999.999			
Result Code	Successful Event 00	Failed Event 01	Pending Event 02	Unknown Event 03

C.3.2.6.1.2 PSD Audit Messages Log File Entry

An entry shall be made to the log file to record each PSD audit message. The PSD audit message shall be included in the entry. As indicated in Table C-3, PSD Audit Message Log File Entry, the audit message itself, showing the control total and the values of the ascending and descending registers, and identifying data is all that is included in the entry.

Table C-3. PSD Audit Message Log File Entry

Fields	Format or Value			
PSD Device ID: Manufacturer ID Model ID Serial Number	 ASCII, 2 characters ASCII, 2 characters Numeric, 10 digits			
Date and Time of Log Entry	YYYYMMDD/HH:mm:SS			
Log Entry Type	99			
Audit Message: Control Total Ascending Register Descending Register	 Numeric, 999,999,999.999 Numeric, 999,999,999.999 Numeric, 999,999.999			
Result Code	Successful Event 00	Failed Event 01	Pending Event 02	Unknown Event 03

C.3.2.6.1.3 Indicia Creation Log File Entry

An entry shall be made to the log file to record each indicium created. Table C-4, Indicia Creation Log File Entry, shows the required fields are a subset of those required for the indicium, with some added identifying information. The order and formatting of this data are defined in Table C-4.

Table C-4. Indicia Creation Log File Entry

Fields	Format or Value			
Date and Time of Indicia Creation	YYYYMMDD/HH:mm:SS			
Log Entry Type (A log file entry for the redate indicium is optional	Standard Indicia 07	Postage Correction 08	Redate Indicia 09	Refund Indicia 10
Indicia Version Number	ASCII, 1 character			
Algorithm ID	ASCII, 1 character			
Certificate Serial Number	Alphanumeric, 9,999,999,999			
PSD Device ID: Manufacturer ID Model ID Serial Number	 Alphanumeric, 2 characters Alphanumeric, 2 characters Numeric, 10 digits			
Ascending Register	Numeric, 999,999,999.999			
Postage	Numeric, 99.999			
Date of Mailing	YYYYMMDD			
Originating Address (Registration ZIP Code)	Alphanumeric, 99999			
Destination Delivery Point 5-digit ZIP Code	Alphanumeric, 99999-0000 (This field has zero value for correction indicia and international mail			
Software ID	Numeric, 12 digits			
Descending Register	Numeric, 999,999.999			
Rate Category	Numeric, 4 digits			

C.3.2.6.2 Log File Management and Review

The host system shall provide capabilities to create new log files, safe-store log files, and view log files. The log files shall be assigned names in the underlying system file structure to provide insight into the sequence of log entries across multiple files. The log file must be designed to prevent the user from directly manipulating the log file entries.

The host system shall provide an automated means to transmit log file entries to the Provider's infrastructure with every connection, including the connection for transmittal of the refund request indicium. The entire contents of the log file need not be transmitted, only those entries not previously transmitted. It is the responsibility of the host system to maintain accurate records of which entries have been transmitted. Once each Postal Accounting period, the Provider shall submit to the Postal Service infrastructure all user log files not previously transmitted.

C.3.2.6.3 Safe-Store

The host system shall provide a capability to safe-store information. Critical information that is necessary for the operation of the system, and is not otherwise recoverable, shall be safe-stored when created or updated. Following a catastrophic hardware or software failure, an inadvertent accident, or any loss or detected corruption, the host system shall be able to restore information that has been safe-stored Information shall be safe-stored by making copies on storage media that may be removed and physically separated from the host system, or by copying to a remote location accessible over a network.

C.3.2.7 User Interface

The host system shall provide an interface to allow the user to initiate, control, and interact with the functions and operations described in these performance criteria. The user interface should comply with standard human engineering practices and should prompt and help users to provide complete, accurate input data. The host should provide informative responses that clearly indicate the success or failure of each request. Error messages should inform the user clearly of the nature of the error and the corrective action required. The remaining paragraphs describe additional interface requirements.

C.3.2.7.1 General Information Displays

The host system shall provide the user with the means to request information on the current status of the host system. The information the host shall provide to the user is listed in Table C-5, Information Display Items. The host may offer several displays that collectively provide the indicated information.

Table C-5. Information Display Items

Information Display Items
Device ID/Type
Cumulative Postage (Ascending Register)
Remaining Postage (Descending Register)
Expiration Date of Watchdog Timer
User Registration Application Information, including Registration Number
Current Rate Table Version
Current AMS ZIP+4 CD-ROM Version
Public-Key Certificate and Expiration Date
Software ID Number
Provider Name and Contact Information

C.3.2.7.2 Advisory Messages

During user interaction with the functions and operations of the system, the host system shall report to the user any errors that occur. Such errors would include insufficient postage available to print the requested indicium, or the postage amount requested for the indicium is out of the allowable range.

The host system should advise the user of near-term conditions that could cause the PSD to stop operating. For example, the host should advise the user of an impending expiration of the PSD's watchdog timer or of a public-key certificate. The advisory message, along with information on how to correct the problem, should give the user sufficient time to take the required action.

C.3.2.7.3 Indicia Quality Assurance

Periodically, the host shall produce indicia for Provider review and quality assurance. The user interface shall instruct the user to mail the quality assurance indicium to the Provider. The Provider shall inspect the indicium for compliance with USPS policy and IBIP requirements to ensure the indicium components are readable and properly oriented and positioned The Provider shall inform users of any problems found and advise them of corrective action they need to take.

The first quality assurance indicium shall be produced for Provider review in conjunction with the initial installation of the system. It shall be produced after completion of the product initialization and authorization and after obtaining a user registration. Subsequently, the schedule for production of the quality assurance indicia shall be as required by the USPS.

C.3.2.7.4 Postage Evidencing System Lease and User Registration Application and Update[*]

If the host system provides the means to request or update a registration for use of a postage evidencing system, the host shall collect the required information in accordance with requirements of the USPS Centralized Registration System (CRS). If the host system does not provide the means to request or update the postage evidencing system user registration, it is the Provider's responsibility to ensure the user registration information is accurate and complete prior to producing indicia.

The host shall print a hardcopy of the lease for appropriate signature and instruct the user to mail the signed document to the Provider In lieu of a hard copy lease, the host may allow the user to actively acknowledge the terms and conditions of an electronic service agreement, and to transmit the acceptance to the Provider infrastructure using a process that authenticates the user. The terms and conditions of the electronic service agreement must be approved by the Postal Service before implementation.

The host shall provide the user a copy of any Postal Service privacy policy applicable to IBI products. The Provider is responsible for ensuring the user reads and actively accepts the conditions of any privacy policy prior to producing indicia.

C.3.2.8 User Training and Support

The host system, or supporting documentation, shall provide training and support material to allow users to install and operate the system without assistance. The training and support shall include the Postal Service's general rules for IBI use and related federal laws and their consequences. The training material should highlight the proper position and location for the indicium and other elements of mailpiece design, especially the FIM (where required). The Provider may use or reproduce existing USPS materials intended for IBI users. It is recommended that an on-line help file be included for the user as part of the host system.

C.3.3 Host Requirements to Implement IBIP-Specific Functions

This section presents the host requirements for the proper implementation of IBIP functions. Where appropriate, reference is made to the core host functional requirements presented in section C.3.2.

[*] The Postal Service is developing policies, procedures, and systems that will distinguish between postage meter and IBI postage evidencing systems.

C.3.3.1 Device Authorization

The host system provides the interface between the Provider's infrastructure and the PSD to load customer-specific information for device authorization, in accordance with the performance criteria in section B of this document.

The host system also provides the interface between the Provider's infrastructure and the PSD to update the device authorization information with all relevant changes to the user profile or other authorization information.

C.3.3.2 Finance

The host shall provide necessary functions to allow the user to obtain postage. The financial management process involves the electronic transfer of funds to the USPS for downloading to the PSD.

The host system finance function also allows the user to obtain a refund of the remaining postage value when the PSD is withdrawn from service, as described in section C.3.3.2.2.

C.3.3.2.1 Obtaining Postage

C.3.3.2.1.1 Payment to USPS

The host system shall provide or direct the user to informationon how to transfer funds to the USPS for postage value downloads. The host system shall enable the user to verify the amount. The host system may provide the user with the necessary functions to transfer funds electronically to the USPS. The need for and nature of these payment functions is dependent on the Provider business model and USPS policy.

C.3.3.2.1.2 Postage Value Download

The host system shall provide an interface between the PSD and the Provider infrastructure for initiating and completing a postage value download. The interface should allow the user to specify the amount of the download. The host system user interface should provide information such as the before and after postage-remaining values to assist the user in formulating the download and then verifying its completion. The host communicates the user request for a postage value download to the PSD. The PSD subsequently controls the postage value download process, in accordance with the performance criteria in part B of this document. The host receives messages regarding the status of the postage value download from the PSD and the Provider infrastructure for communication to the user.

C.3.3.2.2 Remaining Postage Value Refund

C.3.3.2.2.1 Remaining Postage Value Refund Process

The host system shall provide the interface between the user, the PSD, and the Provider infrastructure for the refund of remaining postage value.

The user can obtain a refund of postage value in the PSD only when the PSD is withdrawn from service. The refund request must be for the entire postage value remaining in the PSD, as shown on the descending register at the initiation of the refund process. There shall be no mechanism for processing a partial refund of an amount remaining on the PSD.

The request for postage value refund shall be the last transaction permitted for the PSD. To ensure this, the watchdog timer shall be set to show it has expired at the completion of the postage value refund process.

C.3.3.2.2.2 Remaining Postage Value Refund Request Message

The user initiates the request for a refund through the host system. The host system verifies the amount of postage remaining on the PSD and collects the data required for transmission of the refund request to the Provider.

The host system collects all data elements in Table C-6, except for the digital signature, which shall be added by the PSD. The elements collected by the host system shall be formatted as an indicium for transmittal to the PSD for signature. There shall be no mechanism available for the user to print the refund indicium

Table C-6. Data Elements for Refund Request Indicium

Data Elements	Barcode	Human Readable	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
Remaining Postage Value	Yes	No	3	8
Date of Refund Request	Yes	Yes	4	9
Registration 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
Reserved Field 2	Yes	No	4	14
Digital Signature (field added by PSD)	Yes	No	DSA 40 RSA 128 ECDSA 40	15
"Refund Message Only"	No	Yes	N/A	

When the PSD returns the signed refund indicium to the host system, the host will transmit it to the Provider. The Provider is responsible for collecting any additional data required to process the refund. The host system shall inform the user of the success or failure of the transmission of the refund indicium to the Provider

C.3.3.2.2.3 Submitting Postage Value Refund Request to USPS

The Provider infrastructure is responsible for verifying the postage value refund request and for issuing a refund to the individual customer. On a regular basis, the Provider will submit to the Postal Service an aggregate total of all refunds issued to customers. The Postal Service will issue a refund to the Provider for the aggregate total of all refunds for unused postage or for postage value remaining on the PSD that were issued by the Provider during the period covered. The Provider is required to maintain documentation supporting all individual refunds to customers for periodic Postal Service audits. The supporting documentation shall include a copy of the Refund Request Indicium.

C.3.3.3 Indicia Creation

The host system shall create indicia and transmit indicia to the printer. The host system shall provide the PSD with the mailpiece-specific data elements necessary to prepare the indicia and the mailpiece. The host system shall provide input to the PSD for use in creating the signed data elements for selected fields in the indicia. The host system shall prevent the printing of multiple copies of an indicium, and shall restrict printing to only one image.

The host shall provide the capability to produce and print four types of indicia: the standard indicium, the date correction indicium, the postage correction indicium, and the test indicium. Part A of this document provides specific detailed requirements regarding the content, position, readability, and print characteristics for the standard, date correction, and postage correction indicia.

C.3.3.3.1 Date Correction and Postage Correction Indicia

The host shall be capable of producing date correction and postage correction indicia. The host shall be capable of printing these indicia on either the non-addressed side of the mailpiece or on a label that will be affixed to the mailpiece, in accordance with the requirements of the DMM. The host shall produce the date correction indicium without employing the PSD.

The production of the postage correction indicium does require use of the PSD. The data elements to be included in the postage correction indicia are found in part A of this document. The host shall provide the data elements to the PSD to produce the additional postage value and to digitally sign the indicia.

C.3.3.3.2 Test Indicia

The host shall be capable of producing test indicia. The host must produce the test indicia without employing the PSD. The user generates a test indicium to verify location of the indicium on the mailpiece and to check on print quality and other aesthetic features prior to printing valid indicia. The test indicium shall clearly indicate it is not usable as evidence of postage. There are no other specific performance criteria associated with the test indicium

C.3.3.4 Device Audit

The device audit function allows the USPS to ensure proper use of the system. During the device audit process, the host system manages the transactions between the PSD and the Provider infrastructure. For more information on device audits, see part B, PSD.

C.3.3.5 PSD Security Functions

The host system core functions support implementation of the core security functions of the PSD, namely initialization, digital signature generation and verification, and register management.

C.3.3.5.1 Initialization

The host system provides the interface between the Provider's infrastructure and the PSD to initialize the PSD, in accordance with the Provider's concept of operations.

C.3.3.5.2 Digital Signature

The host system shall request the PSD to perform the security functions necessary for the host to create the indicium. The host system shall provide the data required to generate the digital signature and shall request the PSD to digitally sign the indicium data. Data from the digital signature generation process in the PSD is output to the host system in accordance with the specifications of the selected digital signature algorithm. If the digital signature request is successful, the host system shall prepare the mailpiece. If the request is unsuccessful, an appropriate error message shall be displayed to the user.

C.3.3.5.3 Register Management

The host system has no role in register management. The host system shall have no mechanism to alter the ascending or descending register values in the PSD.

Part
D
IBIP Key Infrastructure

D.1 INTRODUCTION

D.1.1 Overview

Digital signatures based on public-key cryptography are required in the IBI program for the creation of the indicium, in accordance with the performance criteria in part A, Indicium, and part B, Postal Security Device. This approach relies on a pair of cryptographic keys, a private key and a public key. The private key is used by the signatory for creating the signature. The recipient uses the public key for verifying that signature. Multiple digital signature algorithms are supported by the IBIP, see part B, Postal Security Device. A Provider is at liberty to choose the digital signature algorithm(s) most appropriate for its product(s).

IBIP uses X.509 Version 3 certificates as the vehicle for distributing the necessary cryptographic keys to the IBIP elements requiring them. The IBIP Certificate Authority (CA) is responsible for the creation and distribution of these certificates.

A USPS-supplied interface supports the IBIP key infrastructure for Providers. The IBIP key infrastructure services, which include trust evaluation, key registration and key selection, key distribution, and certificate revocation, support the applications of public-key cryptography to the IBI program for Open Systems. The IBIP standard is based on the use of X.509 certificates. The USPS will supply all qualified IBI Providers with additional details of the key interface and of the key management plan.

D.1.2 Structure of This Document

The following is an overview and general description of each of the remaining sections of the performance criteria for the IBIP key infrastructure:

- **Section D.2 — Key Registration:** This section describes the IBIP trusted keying hierarchy, the generation of the certificates for the Provider, and the PSD certificate registration procedure.
- **Section D.3 — Key Attributes:** This section discusses the length of the public key and the cryptoperiod for IBIP keys.

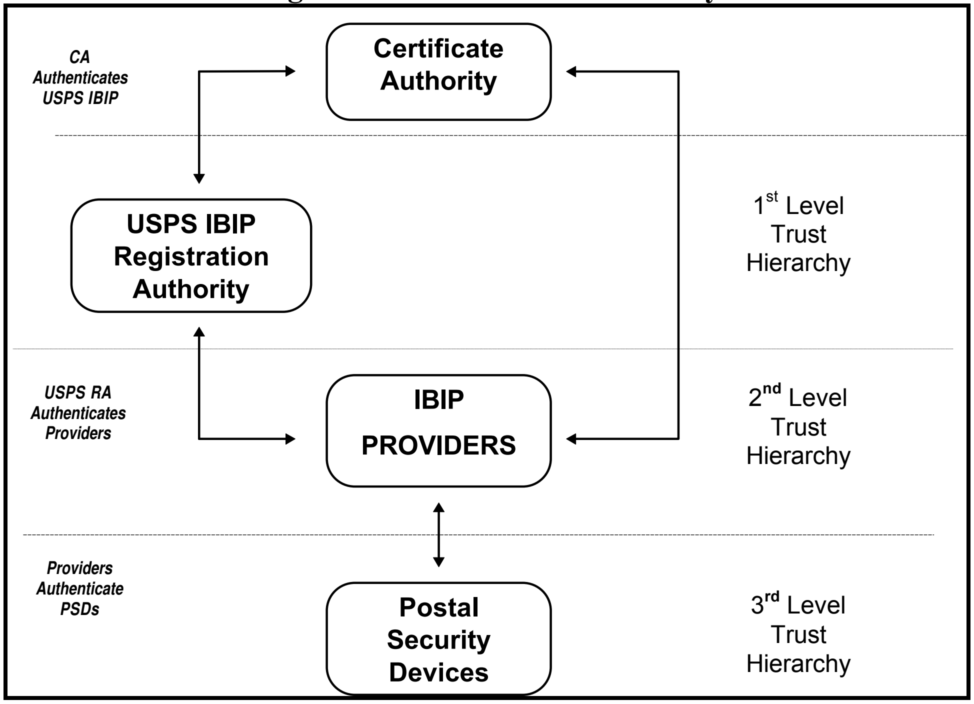
D.2 KEY REGISTRATION

D.2.1 IBIP Trusted Hierarchy

There are four IBIP entities that use digital signatures and require cryptographic keys and digital signature certificates, namely the CA, the USPS IBIP Registration Authority (RA), the Providers, and the PSDs. The certificates are required to verify the indicia objects issued by each authorized PSD.

IBIP has a single Certificate Authority. The organization of the IBIP trusted keying hierarchy, based on the public-key certificates, is depicted in Figure D-1.

Figure D-1. IBIP Trust Hierarchy


CA Authenticates USPS IBIP
Certificate Authority
USPS IBIP Registration Authority
1st Level Trust Hierarchy
USPS RA Authenticates Providers
IBIP PROVIDERS
2nd Level Trust Hierarchy
Providers Authenticate PSDs
Postal Security Devices
3rd Level Trust Hierarchy

The CA generates and distributes the CA Certificate to the first level of the keying hierarchy, the USPS IBIP Registration Authority (RA). The USPS IBIP RA must authenticate the IBIP Provider to the CA before the CA generates a certificate for the second level of the keying hierarchy, the Provider. The IBIP Provider, in turn, authenticates each PSD to the CA. The CA then generates a certificate that is transmitted through the Provider to the third level of the keying hierarchy, the PSDs.

D.2.2 Provider Certificate Registration Procedure

Before a Provider can request certificates for its PSDs, it must have its own Provider certificate. The Provider receives its certificate from the IBIP Registration Authority (RA. As part of the process for obtaining this certificate:

- The IBIP RA authenticates the identity of the Provider's representative.

- The IBIP RA generates the key pair.
- The IBIP RA submits a certificate request to the CA for the Provider.

The USPS conducts this process in the presence of the Provider. The Provider's private key is stored on a token selected by the USPS. This token is used to sign the PSD certificate requests. All software or tool kits required to perform this function are provided by the USPS.

D.2.3 PSD Certificate Registration Procedure

Once the Provider receives its token, the Provider may thereafter request certificates for its PSDs from the CA.This process can be accomplished in one of the following ways:

- Provider uses the USPS-supplied single-request registration authority application.
- Provider develops an application using the USPS-supplied IBIP Public-Key Infrastructure application program interface (API).

For each of the methods described above, the Provider signs the PSD certificate requests with the token obtained during the Provider certificate registration procedure and receives an X.509 certificate in return. The actual implementation and data requirements for the certificate request are beyond the scope of this document but will be supplied to qualified Providers.

D.3 KEY ATTRIBUTES

Attributes for the public keys in the algorithms currently approved for use in the IBI program, namely DSA, RSA, and ECDSA, are described in the following sections.

D.3.1 Key Lengths

The key length, in bytes, for the public key for each of the approved algorithms is shown in Table D-1.

Table D-1: Key Lengths

Algorithm	Key Length (bytes)
DSA	1024
RSA	1024
ECDSA	21

D.3.2 Cryptoperiods

The cryptoperiod of a key is the length of time for which that key is valid. The cryptoperiods established by the USPS for the various IBIP entities are shown in Table D-2.

Table D-2. IBIP Cryptoperiods

IBIP Entity	Cryptoperiod
USPS IBIP Element / Provider	3 years
Postal Security Device	3 years

When the cryptoperiod expires, a new certificate (containing a new key) must be created and distributed.

D.3.3 Additional Attributes

The USPS will make additional details of IBIP key management available to all qualified product Providers

APPENDIX A

LIST OF ACRONYMS

2 D	Two-dimensional
AMS	Address Matching System
ANSI	American National Standards Institute
CA	Certificate Authority
CASS	Coding Accuracy Support System
CRS	Centralized Registration System
DMM	*Domestic Mail Manual*
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDSA	Elliptic Curve Digital Signature Algorithm
EFRS	Electronic Funds Resetting System
FIM	Facing Identification Mark
FIPS	Federal Information Processing Standard
IBI	Information-Based Indicia
IBIP	Information-Based Indicia Program
IMM	*International Mail Manual*
NIST	National Institute of Standards and Technology
OCR	Optical Character Reader
PKCS	Public-Key Cryptographic Standard
PROM	Programmable Read-Only Memory
PSD	Postal Security Device
ROM	Read-Only Memory
RSA	Rivest Shamir Adleman
SHA	Secure Hash Algorithm
USPS	United States Postal Service

APPENDIX B
GLOSSARY

2 D Barcode (Two-Dimensional Barcode) — a barcode that is read both horizontally and vertically.

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.

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 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 codes appearing on mailpieces. Also see Code Accuracy Support System, AMS-II, Technical Guide.

Cooperating software — software programs with which the host system interfaces but which do not perform any functions required of these performance criteria.

Cryptographic — of or relating to codes that convert data so 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 secret authorization codes used for signing electronic documents.

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

Elliptic Curve Digital Signature Algorithm (ECDSA) — a cryptographic 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 indicium, as an orientation mark for automated facing and canceling equipment.

Firmware — software routines or data permanently stored in hardware (e.g., in ROM, or PROM), such that the programs and data cannot be dynamically written or modified during execution and stay intact even in the absence of electrical power.

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, the new methods shall use a computer and printer to create and print an indicium 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.

PC Postage — the Postal Service trademark for Postal Service-approved secure postage evidencing products using information-based indicia that have been developed by commercial providers to allow customers to purchase and print postage onto envelopes and labels using their personal computers and the Internet.

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

Private key — one of two keys used in the digital signature; the private key 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 IBI systems.

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 released to the public and 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.

Remaining postage — the value representing the remaining cumulative amount of postage that the PSD may produce before needing to download additional postage from the Provider. This value is the value maintained in the descending register in the mechanical meter era.

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

Safe-Store — action taken to protect selected information from catastrophic system failures. The critical information can be restored following a system failure. Off-line storage using floppy disks or tape or on-line storage on a remote network node often serves as the media for safe-storage.

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

Strong identification and authentication — a process for performing user, workstation, or network node authentication that involves measures resistant to compromise, tampering, spoofing, or playback. Strong identification and authentication generally involve cryptographic techniques.

Underlying hardware — the complete collection of hardware that comprises the hardware available for use by the host system and upon which the host system relies to perform its necessary functions. This hardware includes components such as the central processing unit (CPU), main memory, on-line storage, modems, network interfaces, data ports, and printers. It includes the PSD interface, connector, or holder but excludes the actual PSD.

Underlying software — the collection of programs that is not part of the host system software distribution but upon which the host system depends to perform its required functions. Operating systems and device-unique drivers are possible examples of underlying software.

User System — the collection of the host system, the underlying hardware and software, and the cooperating software. It includes the PSD.

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.

Zeroization — a method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data.