UNITED STATES POSTAL SERVICE

United States Postal Service Policy for In-Person Proofing

Publication 364
August 2003

Contents

1 Introduction

1-1 Background

In recent years, several new federal statutes have sought to preserve the ability of the public and private sectors to use the efficiency of the Internet to exchange time-sensitive communications rapidly while ensuring that people receiving and sending messages are in fact who they say they are. A number of top-quality private-sector businesses have mastered the technology of secure digital signatures, and this has increased the demand for improved identity verification for individuals seeking to use digital signatures.

One of the growth strategies presented in the Postal Service's Transformation Plan is to "continue to seek opportunities to leverage our brand and assets to create new products and services with minimal investment." The need for improved "online identity" creates just such an opportunity. Numerous organizations have approached the Postal Service about conducting In-Person Proofing (IPP) — an identity verification procedure in which an Applicant for a digital signature certificate has to go to a Post Office, physically present identification documents, and attest to their authenticity — before the organization will issue the Applicant a certificate. By offering this service, the Postal Service will provide value to the public and enable Internet communications to enjoy a new level of security and reliability.

1-2 Purpose

IPP is a Postal Service program designed to improve the nation's public-key infrastructure. The public-key infrastructure has emerged as an accepted infrastructure component for protecting and facilitating the nation's electronic communications.

1-3 Overview

In this document, the Postal Service establishes the following:

- Requirements for Service Providers to include IPP within an identity verification process.

- Policy and procedures for individuals who perform IPP.
- Requirements for Applicants.
- Policy for the use of digital certificates issued pursuant to the policy contained in this document by Applicants and Relying Parties.

Terms and abbreviations used in this publication are defined in Section 12, Terms and Definitions.

1-3.1 IPP Registration Agent (RA)

An IPP Registration Agent (RA) is an authorized employee of the Postal Service, who verifies the identity of Applicants consistent with the policy contained in this document.

1-3.2 Service Provider

A Service Provider is an entity that has entered into a service agreement with the Postal Service for the use of the IPP service.

1-3.3 Applicant

An Applicant is an individual who is directed by a Service Provider to present his or her registration and identification documents to an IPP RA in accordance with a Service Provider's identity validation process.

The Postal Service has established the following minimum criteria for Applicants:

a. An Applicant must be under no legal disability to execute a legally binding and enforceable contract.

b. An Applicant must present at least one of the following *non-expired* photo IDs to an IPP RA during IPP:
   (1) United States passport.
   (2) State-issued driver's license.
   (3) Federal driver's license.
   (4) State-issued (non-driver's) ID card.
   (5) Active-duty U.S.-military-issued ID card.

c. An Applicant must present one of the following documents to an IPP RA during IPP that has been received by the Applicant at his or her residential mailing address (identified on the IDVF form):
   (1) A current electric bill.
   (2) A current water bill.
   (3) A current telephone bill.
   (4) A state-issued voter registration card (non-expired).
   (5) An active insurance policy.

The Postal Service reserves the right to amend the above list of required documents at its discretion.

1-4 Guidelines for Determining Usage

The Postal Service does not determine the required levels of assurance for usage or claims of suitability for specific applications.

To determine the required level of assurance for an application, relying parties should consider various risk factors and conditions, as well as the value of the information, operating environment, and existing mitigating controls placed in practice. Determining the required levels of assurance is the sole responsibility of the Relying Party.

This page intentionally left blank

2 Contact Details

2-1 Specification Administration Organization

The management team of the chief marketing officer (or its successor organization) of the Postal Service administers the policy contained in this document.

2-2 Contact Person

The United States Postal Service developed the policy contained in this document. Direct questions about this policy to the following address:

UNITED STATES POSTAL SERVICE
ATTN PROGRAM MANAGER IPP
1735 N LYNN ST RM 4034
ARLINGTON VA 22209-6354

This page intentionally left blank

3 Obligations

This section provides a general overview of the responsibilities of the Postal Service RAs, Service Providers, Applicants, and Relying Parties in the context of IPP. Additional obligations may be set forth in other contracts or in policies promulgated by a Service Provider. Applicants and Relying Parties must read all relevant documentation before applying for, accepting, using, or relying on digital certificates.

3-1 United States Postal Service IPP Registration Agent Obligations

The Postal Service will provide that IPP is performed only by IPP RAs who are obligated to comply with this policy.

The Postal Service shall provide a specification for the creation of identity verification (IDVF) forms (PS Form 2001, forthcoming) by Service Providers.

The IPP RA is responsible for the performance of IPP in accordance with the policy contained in this document and the procedure specified below.

For each IDVF form presented by an Applicant at a participating retail office, an IPP RA will do the following:

a. Compare the identifying documents listed on the IDVF form with those presented by the Applicant, and compare the Applicant's physical appearance with the photographic image contained on the identifying documents.

b. Observe the Applicant's signing of the IDVF form.

c. Apply a round date stamp to the IDVF form.

d. Initial the IDVF form.

e. Place the IDVF form (PS Form 2001, forthcoming) in the accountable mail bin.

At the end of each day, the unit manager (or his or her designee) retrieves all IDVF forms, scans the barcode on each form with the Mobile Data Collection Device (MDCD) scanner, and mails the original IDVF forms to the appropriate Service Provider at the address preprinted on the IDVF form using a letter-sized window envelope with G-10 permit.

On a nightly basis, the Postal Service transmits to each Service Provider a record of all barcodes scanned at participating retail offices from IDVF forms generated by that Service Provider.

3-2 Service Provider Obligations

A Service Provider shall do the following:

a. Enter into an IPP Service Agreement with the Postal Service before offering the IPP service.

b. Require all Applicants to meet the requirements of Section 1.3.3 of this document.

c. Retain the original signed IDVF forms mailed by the Postal Service to the Service Provider for a period of 7 years.

d. Provide access to the completed IDVF forms, Applicant data, and IPP-related financial activity information at the request of United States Postal Inspection Service or the Postal Service Office of Inspector General for review, audit, and investigative purposes.

e. Maintain IPP financial activity records sufficient to produce and reconcile monthly reports and payments to the Postal Service.

f. Incorporate this policy by reference into the primary policy document (e.g., certificate policy) used by the Service Provider to govern the operation of its service.

g. Incorporate the IDVF form specification defined by the Postal Service into the design and operation of the Service Provider's identity verification process.

h. Produce sample IDVF forms to be used by the Postal Service for compliance testing.

i. Issue IDVF barcodes within the defined range of sequence numbers supplied by the Postal Service and listed in the IPP Service Agreement.

j. Provide customer support for Applicants.

k. Include the following in its identity verification process:

   (1) A verification of the Applicant's physical residential address via First-Class Mail® with a "Return Service Requested" endorsement.

   (2) Use of a Patriot Act-compliant database vetting process to gain initial assurance of an Applicant's identity before sending the Applicant to the Post Office for IPP.

l. Verify that the Applicant has undergone IPP within the 4 years immediately preceding the issuance of any digital certificate supported by IPP.

m. Publish its certificate policy related to its issuance of digital certificates supported by IPP and make that policy freely available so that Relying Parties and Applicants can determine whether the digital certificate is suitable for an intended use.

n. Enter into an agreement with the Postal Service that includes standard pricing, service level commitments, IPP Policy compliance, and liability and service termination provisions, as well as such other terms and conditions as may be included.

o. Have sufficient privacy and security safeguards that meet the approval of the Postal Service.

p. Operate the CA to enable the broadest practical use of IPP-based digital certificates. This includes the following:

(1) Issuing, at a minimum, a daily certificate revocation list to better allow users to rely upon the certificates.

(2) Passing an external CA audit in accordance with industry best practices, such as “AICPA/CICA WebTrust Program for Certificate Authorities.”

(3) Achieving interoperability with the Federal Bridge for Certificate Authorities.

(4) Mapping the common object identifier (USPS-registered OID) for IPP-based digital certificates into the policy mapping extension of the digital certificate. The official OID is as follows:

2.16.840.1.113901.175 - ID Verified by the US Postal Service

3-3 Applicant Obligations

An Applicant must do the following:

a. Agree to abide by the policy contained in this document and the Service Provider’s policies and related agreements, which incorporate this policy.

b. Attest to the accuracy of any information provided by the Applicant and the authenticity of the identification documents presented by the Applicant to an IPP RA by signing the IDVF form in the presence of the IPP RA.

3-4 Relying Party Obligations

Before relying on a digital certificate supported by IPP a Relying Party must do the following:

a. Read this document and the Service Provider’s published policies, which incorporate the policy contained in this document.

b. Abide by any restrictions imposed by the Service Provider in its published policies regarding who may rely on a digital certificate and the purposes for which a digital certificate supported by IPP may be used.

This page intentionally left blank

4 Liability

4-1 Warranties and Limitations on Warranties

The Postal Service makes no warranties or representations, express or implied, concerning the use of IPP and IPP-supported digital certificates under the policy contained in this document by Service Providers, Applicants, Relying Parties, or any other person. The Postal Service is not liable for any of the following:

a. Loss due to the unavailability of IPP services due to war, natural disasters, or other uncontrollable forces.

b. Loss due to nonauthorized use of IPP services or a digital certificate supported by IPP or use of IPP services or a digital certificate supported by IPP not consistent with the prescribed use defined in this document or in a policy promulgated by a Service Provider that incorporates the policy contained in this document.

c. Loss of profits, data, or other indirect, consequential, or punitive damages arising from or in connection with the IPP service or the use or reliance on a digital certificate supported by IPP.

The Postal Service disclaims all other warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of the accuracy of information provided, unless expressly stated otherwise in this document.

4-2 Loss Limitations

The Postal Service is not liable to any person or entity, including Applicants, Service Providers, and Relying Parties, for any direct, indirect, consequential, or punitive damages arising from any use of a digital certificate supported by IPP issued pursuant to the policy contained in this document. If the Postal Service fails to conform to the procedures in this policy, the sole and exclusive remedy is a refund of the fee, or a prorated portion thereof that the Postal Service charged to perform the IPP event.

This page intentionally left blank

5 Financial Responsibility

5-1 Indemnification by Relying Parties and Applicants

The Relying Parties, Service Providers, and Applicants must indemnify the Postal Service, holding it harmless in accordance with section 4.2, Loss Limitations, if the loss incurred from the transaction is found to be at the fault of the Relying Party, Service Provider, or Applicant. The Postal Service is not responsible for loss due to the failure of the Applicants, Service Providers, and Relying Parties to fulfill their obligations under the policy contained in this document as described in Sections 3.2, Service Provider Obligations, 3.3, Applicant Obligations, and 3.4, Relying Party Obligations.

5-2 Fiduciary Relationships

Issuance of a digital certificate supported by IPP in accordance with the policy contained in this document does not make the Postal Service or an IPP RA an agent, fiduciary, trustee, or other kind of representative to Applicants, Service Providers, or Relying Parties.

This policy does not create a partnership or a relationship of principal and agent between the Postal Service and any Service Provider, Applicant, or Relying Party.

This page intentionally left blank

6 Interpretation and Enforcement

6-1 Governing Law

The laws of the United States govern the enforceability, construction, interpretation, and validity of the policy contained in this document. If no such law is applicable, the laws of the state of New York govern.

6-2 Jurisdiction

The federal courts of the District of Columbia have jurisdiction over any disputes arising in connection with the policy contained in this document.

6-3 Severability, Survival, Merger, Notice

Entire Agreement. This policy, applicable Postal Service regulations, IPP Service Agreements, and Applicant agreements constitute the entire agreement between the Parties with respect to the subject matter in this publication and merge all prior and contemporaneous communications. It must not be modified except by a written agreement dated after the date of this document and signed on behalf of the Postal Service by a duly authorized representative.

Construction. If for any reason a court of competent jurisdiction finds any provision of the policy contained in this document, or portion thereof, to be unenforceable, that provision of this policy is enforced to the maximum extent permissible so as to affect its intent, and the remainder of this policy will continue in full force and effect. Failure by the Postal Service to enforce any provision of this policy will not be deemed a waiver of future enforcement of that or any other provision.

Notices. All notices and requests in connection with the policy contained in this document are deemed given on the day they are received either by messenger, nationally recognized delivery service, or in the U.S. mail, postage prepaid, certified or registered, return receipt requested, and addressed as follows:

UNITED STATES POSTAL SERVICE
ATTN PROGRAM MGR IPP
1735 N LYNN ST RM 4034
ARLINGTON VA 22209-6354

6-4 Arbitration

In any dispute regarding the Postal Service IPP Service, any Party may request arbitration for any controversy or claim involving any aspect of the policy contained in this document. Each Party bears its own fees associated with such action. Arbitration is presided over by an individual agreed to by each Party, trained and capable of such arbitration, and organizationally separate from the Postal Service, Service Provider, Applicant, and Relying Party.

6-5 Dispute Resolution Procedures

The management team, under the direction of the Chief Marketing Officer (or its successor organization), is responsible for resolving any disputes associated with the use of IPP services. In the event that the management team is unable to resolve the dispute, any party may request arbitration pursuant to Section 6.4, Arbitration.

7 Fees

7-1 In-Person Proofing Fee

Fees for IPP services are defined in the IPP Service Agreement.

This page intentionally left blank

8 Confidentiality

8-1 Types of Information to Be Kept Confidential

Applicant Data. For the purpose of proper administration of IPP, the Postal Service, a Service Provider, or their respective agents may request information (e.g., credit card number, home phone number, social security number, or shared secret) for use in identity verification processes or the collection of fees payable by an Applicant. In the event that this type of information is required, it is handled as confidential information, and access is restricted to those with an official need to access that information in performance of their official duties. The Postal Service will protect data in accordance with the Privacy Act and related Postal Service policies. The Service Provider is responsible for managing data under its applicable privacy policies.

8-2 Types of Information Not Considered Confidential

The following information is not confidential:

a. Any information that can be obtained from public sources.

b. This document.

c. Information defined as not confidential in a Service Provider's published policies or related agreements.

8-3 Release of Confidential Information to Law Enforcement Officials

The Postal Service will not disclose confidential information except as provided in the Privacy Notice of the IDVF, or unless required by legal process or statute.

8-4 Disclosure upon Owner's Request

Confidential information may be released, if the Applicant submits written consent.

This page intentionally left blank

9 Intellectual Property Rights

The intellectual property in this document is the exclusive property of the Postal Service:

Applicants represent and warrant that the information that they provide to Service Providers and IPP RAs does not infringe upon or violate in any way the trademarks, service marks, trade names, company names, or any other intellectual property rights of any third party. Applicants will defend, indemnify, and absolve the Postal Service and Service Providers from all financial responsibility and any claims of loss or damage resulting from such an infringement or violation. An Applicant who brings about a claim of loss or damage by violating or infringing upon the intellectual property right of any third party pays all legal fees incurred by the Postal Service and the Service Provider as a result of such claim.

This page intentionally left blank

10 Administrative Controls

All employees, contractors, and consultants of the Postal Service (collectively, “personnel”) that have access to or control over operations that may materially affect the Postal Service IPP barcode processing systems, serve in a Trusted Role. Such personnel include, but are not limited to, system administration personnel, database administration personnel, data handling and support staff, and security staff who are designated to oversee the Postal Service network operations.

All employees, consultants, and contractors of the Postal Service that have access to or control over operations of Postal Service networks must have a Postal Service sensitive security clearance issued by the United States Postal Inspection Service. The Postal Service sensitive clearance must be issued before access is permitted to Postal Service systems.

This page intentionally left blank

11 Computer Security Controls

The Postal Service provides an information technology infrastructure that implements security controls based upon policies identified in Handbook AS-805, *Information Security*, and industry best practices.

The barcode scanning contains cyclic redundancy checks to ensure accurate data acquisition. The barcode data collected from the use of IPP services is segregated by Service Provider, and access is controlled for file transfer pickup by the Service Provider.

This page intentionally left blank

12 Terms and Definitions

Applicant. An Applicant is an individual who is directed by a Service Provider to present his or her registration and identification documents to an IPP RA in accordance with a Service Provider's identity validation process.

Digital Certificate. A type of identity credential, defined by ITU standard x.509 v3, used in systems that employ public-key encryption technology, that (a) names or otherwise identifies a person or entity, (b) binds the identity of that person or entity to the public key contained in the digital certificate, and (c) identifies and is digitally signed by the issuer of the digital certificate.

In-Person Proofing (IPP). An in-person identity verification procedure provided by the Postal Service wherein an Applicant (a) physically presents two specified identification documents to an IPP RA and (b) attests to the accuracy and authenticity of the documents presented. IPP is performed by an IPP RA under the terms of an IPP service agreement concluded between the Postal Service and the service provider.

IPP Registration Agent (RA). An IPP Registration Agent (RA) is an authorized employee of the Postal Service who verifies the identity of Applicants consistent with this IPP Policy.

IPP Service Agreement. A contract that defines the terms and conditions for use of IPP by a Service Provider. IPP Service Agreements will include terms related to the availability and performance of specific functions to be performed by the Postal Service and the service provider as well as financial terms related to the fees that will be collected by the service provider and remitted to the Postal Service for IPP services.

Public-Key Infrastructure. A system of digital certificates, certificate authorities, and registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Relying Party. A person or legal entity that relies on a Service Provider's identity verification process or any digital certificate supported by IPP for any purpose.

Service Provider. An entity that has entered into a service agreement with the Postal Service for the use of the IPP service.

Trusted Role. One whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.

This page intentionally left blank

13 Acronyms

EPM	Electronic Postmark Service
IDVF	ID Verification Form
IPP	In-Person Proofing
ITU	International Telecommunications Union
RA	Registration Agent
USPS	United States Postal Service

This page intentionally left blank