

Dated: June 12, 2003.

D.L. Gamberoni,

*Technical Coordinator, Office of the
Secretary.*

[FR Doc. 03-15347 Filed 6-13-03; 11:53 am]

BILLING CODE 7590-01-M

POSTAL SERVICE

In-Person Proofing at Post Offices (IPP) Program

AGENCY: U.S. Postal Service.

ACTION: Notice.

SUMMARY: The USPS is announcing the availability of an In-Person Proofing at Post Offices (IPP) Program to support the activities of U.S. Certificate Authorities and government organizations.

EFFECTIVE DATE: June 9, 2003.

FOR FURTHER INFORMATION CONTACT:

Chuck Chamberlain at 703-292-4172, or
Brad Reck at 703-292-3530

SUPPLEMENTARY INFORMATION: In recent years, a number of new federal statutes have sought to preserve the ability of the public and private sectors to use the efficiency of the internet to rapidly exchange time sensitive communications while assuring 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 around the use of secure digital signatures, yielding a greater demand for improved identity verification for individuals seeking to use digital signatures.

This need for improved "online identity" creates a unique service opportunity for the Postal Service to provide value to the public, leverage our retail network and enable internet communications to enjoy a new level of security and reliability. Numerous organizations have approached the U.S. Postal Service to conduct In-Person Proofing (IPP) of customers nationwide for physically authenticating an individual's identification at a post office before the organization issues a digital signature certificate to the individual.

IPP supports efficient, affordable, trusted communications through the use of identification verification at Post Offices, incorporation of process enhancements required by the Postal Service, active management of the IPP program by the USPS, and use of a First Class U.S. Mail piece to verify physical addresses of applicants. We believe that IPP conducted at local post offices will create a new broad based capability for

the Nation that promotes improved public trust and greater efficiency in the electronic delivery of a wide range of services. These efforts support achieving the goals of the Government Paperwork Elimination Act of 1998, Electronic Signature in Global and National Commerce Act of 2000, Health Insurance Portability and Accountability Act of 1996, Sarbanes-Oxley Act of 2002, and Gramm-Leach-Bliley Act of 1999 and numerous Presidential Directives on eGovernment.

The following is a brief description of how IPP would work. An organization can establish a relationship with a qualified U.S. Certificate Authority to integrate digital signing with improved identity verification into an online application. Any individual desiring to use digital certificates that include USPS IPP will complete an application online. The online system will verify the individual's identity via commercial data base checking. The system will then produce a standard Postal Service form to be printed out at the "applicant's" personal computer. The individual requesting the service will present this form to a participating post office where the "In Person Proofing" process is conducted. After successful completion of the IPP event, the CA will notify the applicant to download their digital certificate. For clarity, the steps in the IPP process are outlined below.

1.0 DESCRIPTION

1.1 Purpose

IPP is a postal program to improve the public key infrastructure of the Nation. The public key infrastructure has emerged as an accepted infrastructure component for protecting and facilitating the electronic communications of the Nation.

2.0 BASIC STANDARDS

2.1 Eligibility

For a Certificate Authority (CA) to use IPP, the CA must incorporate the U.S. Postal Service In-Person Proofing Policy into their Certificate Policy. Conformance to the Postal policy includes:

1. Use of a Patriot Act compliant database vetting process to gain initial assurance of an applicant's identity before sending the applicant to the Postal Office for IPP.
2. Perform a verification of the applicant's physical residential address via First Class U.S. Mail with an "Address Correction Requested" and "Do Not Forward" endorsement.
3. Restrict the expiration date of an IPP based Digital Certificate such that it does not surpass the expiration of the 4

year validity period of an IPP verification event. A new IPP event will be required every 4 years.

4. Facilitate IPP processing by using standard forms and barcodes as directed by the USPS and exchanging of information as necessary for the efficient operation of IPP. This includes:

A. Using the standard ID Verification Form (IDVF),

B. Maintaining a secure repository of IDVF forms,

C. Providing access to IDVF forms and customer account information as necessary for investigative purposes by USPS Inspection Service and the USPS Office of Inspector General,

D. Submitting the processes and operations of the CA to security audits and compliance reviews as required by the USPS, and

E. Restricting the generation of unique barcodes for each IPP event to those expressly permitted by the USPS.

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

A. Issuing, at a minimum, a daily Certificate Revocation List to better allow users to rely upon the certificates,

B. Passing an external CA audit in accordance with industry best practices such as "AICPA/CICA WebTrust Program for Certificate Authorities",

C. Achieving interoperability with the Federal Bridge for Certificate Authorities, and

D. Incorporating a new common object identifier (USPS registered OID) for IPP based digital certificates.

6. Successfully enter into an agreement with the USPS that includes standard pricing, service level commitments, IPP Policy compliance, liability and service termination provisions, as well as such other terms and conditions as may be included.

2.2 Minimum Volume

IPP transactions are to be purchased in pre-paid blocks of 10,000 transactions by either the CA or a government customer on behalf of the CA.

2.3 Labeling

Each digital certificate must contain the statement "ID Verified by the U.S. Postal Service" within the certificate profile to let any user or relying party know that:

- The issuer of the digital certificate authority operates in compliance with IPP Policy, and

- The holder of the credential did physically appear before a postal employee and had their hardcopy identification successfully verified.

Applications should interrogate the digital certificate presented during an