A “Trusted Internet Delivery Service”

providing users the ability to conduct a secure, authenticated, electronic exchange of documents and transactions.

Featuring:

Nationwide In-Person Proofing

USPS Electronic Postmark™(EPM)
"[t]he Postal Service should assist in developing future messaging systems and seek to leverage its comprehensive directory, messaging security, and addressing directory management capabilities in a manner that promotes universal access to the benefits of these new technologies for all citizens who desire them.

- President George W. Bush, Budget Message - March 7, 2001
NetPost.Certified Infrastructure

- Registration Authority
  - Nationwide Availability Planned
  - Currently Available at 63 Sites

- Certificate Authority
  - X509 v3 Digital Certificates

- Validation Authority
  - CRL
  - OCSP v1 (Planned)

- Electronic Postmark
  - Time/Date Stamp

- National Customer Support

- Transport SW for Integrated Secure Delivery

- Inspection Service for Wire Fraud Protection
Potential Applications for NetPost.Certified

- Wage Reports
- Tax Data
- Vital Statistics
- Health Insurance
- Benefits Data
- Medical Records
- Patient Care Data
- Laboratory Data
- Research Data

- X-Rays
- Investigative Reports
- License Applications
- Security Filings
- Bids & Proposals
- Video Files
- Geographic Images
- Voice Files
Delivering Postal Quality to the Internet

Enables people to send electronic information with the same security, privacy and business quality as traditional U.S. Mail.

Physical Mail-Like Attributes

- Privacy within Envelopes ...................... Encryption
- Restricted Del. to Addressee Only ........ Digital Signatures
- Time-Date-Place Postmark ..................... USPS Electronic Postmark™
- Return Receipts .................................. e-Receipts
- Universal Service ................................. Nationwide Availability to Federal and State Govt.
- Postal Protections ............................... e-Crimes Program
Solution Definition

At the highest level, NPC allows customers to send and receive an electronic communication incorporating key features of USPS Registered and Certified Mail.

- **Physical Identification** – one time in person identification proofing of users at Post Offices nationwide;

- **Electronic Authentication** – cryptographically verifies the identity of the sender and receiver of each transaction;

- **Integrity** – tamper detection assures and certifies that what was sent is the same as what was received;

- **Confidentiality** – encrypts contents so only the intended recipient can read the contents to enhance privacy and ensure restricted access;

- **Proof-of-Service** – non-repudiation of the transaction between the sender and receiver when the Electronic Postmark (EPM) is posted on the receipt; and

- **Fraud Protection** – USPS Inspection Service to protect and resolve transaction disputes.
NetPost.Certified™ Transaction Process

1) (Optionally) Smart Card inserted into Smart Card Reader
2) Sender identifies files to send (may be any type of file)
3) NPC software creates manifest, signs using the sender’s private key, and includes manifest in package
4) NPC software signs package with sender private key and “wraps” (encrypts) package with recipient’s certificate key so only the recipient can decrypt.
5) "Package" sent to destination site via Internet/Extranet.
6) Package "opened" by recipient.
7) NPC software “unwraps” (decrypts) package, manifest inspected, manifest signed with recipient’s private key.
8) Signed manifest (a.k.a receipt) encrypted and sent to USPS Electronic Postmark service
9) Receipt inspected and Electronic Postmark applied. Receipt archived for at least 5 years.
10) Postmarked receipt is returned to the sender
11) User or end-application accesses and processes transaction data.
The Identity Validation Process for USPS Digital Certificates

**STEP 1**
On-line Registration

Customer registers on-line...receives installs SmartCard/Kit...USPS generates IDV Form...mailed to customer address.

**STEP 2**
Identity Validation

undergoes Identity Validation...goes to the Post Office...the customer

**STEP 3**
Downloading the Digital Certificate

The customer...receives an email notification...Digital...which authenticates the customer when using secure USPS eCommerce Services

1. On-line Registration
2. Identity Validation
3. Downloading the Digital Certificate
4. USPS generates IDV Form
5. Mailed to customer address
6. Customer processes Identity Validation
7. Goes to the Post Office
8. undergoes Identity Validation
9. Receives an email notification
10. Digital Certification
11. Authenticates the customer
12. Secure USPS eCommerce Services

Step 1 will take approx 3-5 days. Step 2 must be completed by the customer in 20 days from the date of on-line registration. Step 3 takes 48 hours after Identity Validation at the Retail counter.
NetPost.Certified™ - Value Added

- Postal Protection and Branding
- USPS Electronic Postmark™ (EPM)
- Nationwide In-Person Proofing
- Efficient Large File/Large Volume Transfer
- Multiple Encryption Options
- Postal Return Receipts
- End-to-End Security Certification
- ID Validation
  - Smart Card
- USPS Electronic Postmark™ USPS Certificate Authority
- Internet
- Encrypted Message
Enables GPEA¹, HIPAA², GLBA³, E-Sign Compliance

<table>
<thead>
<tr>
<th>Compliance with...</th>
<th>NetPost Certified</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GPEA</strong>: Allow citizens to use electronic technologies when filing information with, or retrieving it from the Federal Government</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>GPEA</strong>: Provide the legal framework for agencies to accept electronically submitted forms and documents</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>GPEA</strong>: Electronic signatures and other measures will be used to authenticate citizens as they transact business with the Government</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>HIPAA</strong>: Improved efficiency in healthcare delivery by standardizing electronic data interchange</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>HIPAA</strong>: Protection of confidentiality and security of health data through setting and enforcing standards</td>
<td>Enables</td>
</tr>
<tr>
<td><strong>HIPAA</strong>: Security standards protecting the confidentiality and integrity of &quot;individually identifiable health information&quot; past, present, or future</td>
<td>Enables</td>
</tr>
<tr>
<td><strong>HIPAA</strong>: Organizations will be required to implement one of more security authentication access mechanisms: user-based, role-based, and or context-based access (depending on organization's environment)</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>GLBA</strong>: Protect security and confidentiality of customers' non-public personal information</td>
<td>Yes</td>
</tr>
<tr>
<td><strong>E-SIGN</strong>: Permit private parties to conduct business and retain records electronically, using electronic signatures</td>
<td>Yes</td>
</tr>
</tbody>
</table>

¹Government Paperwork Elimination Act of 1998
²Health Insurance Portability and Accountability Act of 1996
³Gramm-Leach-Bliley Act of 1999
## Addresses CFO Council Issues

<table>
<thead>
<tr>
<th>CFO Council Issues</th>
<th>NetPost. Certified</th>
</tr>
</thead>
<tbody>
<tr>
<td>Systems should provide improved auditing capabilities</td>
<td>Yes</td>
</tr>
<tr>
<td>Provide for electronic submission of forms and data to facilitate prompt payment and reduced cycle times</td>
<td>Yes</td>
</tr>
<tr>
<td>Authentication of users (senders and receivers)</td>
<td>Yes</td>
</tr>
<tr>
<td>Protection from fraud</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Value For Our Customers

- Cost Reduction
- Nationwide In Person Proofing at Post Offices
- Nationwide Customer Support
- National Scalability
- Fraud Prevention & Prosecution
- Security and Privacy Safeguards
- Assists with Legislative Compliance