

BEFORE THE
POSTAL RATE COMMISSION
WASHINGTON, D.C. 20268-0001

Complaint on Electronic Postmark®

Docket No. C2004-2

RESPONSE OF UNITED STATES POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA
(OCA/USPS-RT-1.a – b., i – k, 2-11, 13 – 23.a, 24-28)
(August 4, 2006)

The United States Postal Service hereby provides the response of witness Foti to the following interrogatories of the OCA, filed on July 21, 2006: OCA/USPS- RT-1.a – b., i – k, 2-11, 13 – 23.a, 24-28. Objections to 1.c. – h., 5, 12, and 23.b. – d. were filed on July 31, 2006. The objection to question 5 only covered part of the request, so a partial answer is provided. With respect to question 12, a review of Federal Registers indicates that any responsive material would only have been distributed at a closed session of a Board of Governors meeting, so the objection stands.

Each interrogatory is stated verbatim and is followed by the response.

Respectfully submitted,

UNITED STATES POSTAL SERVICE

By its attorneys:

Daniel J. Foucheaux, Jr.
Chief Counsel, Ratemaking

Eric P. Koetting

475 L'Enfant Plaza West, S.W.
Washington, D.C. 20260-1137
(202) 268-2992, FAX -5402
August 4, 2006

RESPONSE OF POSTAL SERVICE WITNESS FOTI TO INTERROGATORIES OF THE OCA

OCA/USPS-RT1-1. At page 3 of your testimony, you make the statement that the Technology Applications group was tasked with developing technology-based applications products, or services-oriented capabilities that would enable the Postal Service to better serve its customers. The following questions are limited to domestic (non-international) activities of the Postal Service.

a. Please provide a detailed description of the Postal Service's "customers" as used at page 3, line 7. Address, in this description, whether the Postal Service views its customers as limited to those individuals and businesses that send or receive "personal, educational, literary, and business correspondence," as well as packages.

b. If the Postal Service customer base is limited to individuals and businesses that send or receive "personal, educational, literary, and business correspondence," and packages, then does the Postal Service view Electronic Postmark (EPM) customers as part of the set of individuals and businesses that send or receive "personal, educational, literary, and business correspondence" and packages. Explain in full.

c. If the Postal Service customer base includes other types of "customers," additional to individuals and businesses that send or receive "personal, educational, literary, and business correspondence," and packages, are there any limits on whom the Postal Service might view as a customer? If there are limits, what are they?

d. Are there any limits on the types of commercial or retail services that the Postal Service might decide to provide to its customers, e.g., selling doughnuts? Selling shoes? Selling homeowners insurance to non-employees? Providing a full array of banking services (for a fee) to non-employees? Explain fully. If there are limits, what are they?

e. Is it the policy of the Postal Service to limit the commercial or retail services it provides to mail-related services? If not, why not?

f. Is it the policy of the Postal Service to limit the commercial or retail services it provides to services that are close substitutes for mail, e.g. PostECS? If not, why not?

g. Does the Postal Service take the view that it may provide any type of commercial/retail product or service solely to earn additional revenues, without regard to the nature of the service and whether it has a close relationship to mail? Please explain fully.

h. Does the Postal Service take the view that there are any limitations on its ability to provide "nonpostal" services to its customers? Please explain fully.

i. Is EPM a postal service? Please explain

j. Or is EPM a "nonpostal" service? Please explain.

k. How does EPM relate to the Postal Service's core mission to provide *mail* services and services incidental to *mail* services?

i. Is EPM a mail service?

ii. Is EPM incidental to a mail service?

iii. Is it the Postal Service's position that EPM has nothing whatsoever to do with mail?

iv. Is EPM a service that comes within the Postal Service's fundamental mission because it is a substitute for/functions like a mail service?

v. Explain your answers to k.i. – iv. fully.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

RESPONSE:

a. I am unaware of any intent to use the term “customer” in any other than the generic sense of the term – “one that purchases a commodity or service” (Webster’s Ninth New Collegiate Dictionary). Therefore, I have no reason to believe that the term as used incorporated any limitation of the type described in your question.

b. Not applicable.

c.-h Objection filed.

i.-j. USPS EPM is a nonpostal service, as it is not a postal service. It is not a postal service because, although I am not a lawyer, it is my understanding that it does not fall within any operative definition of a postal service.

k. USPS EPM relates to the basic function of the Postal Service in that, while postal services bind the Nation together through personal, educational, literary, and business correspondence, USPS EPM has the potential to bind the Nation together through provision of a widely-available, standardized, and commonly-accepted means to establish the integrity of the contents of an electronic file at a particular time and date. In that sense, it is a similar type of service to a postal service.

i. No, it is not a mail service.

ii. No, it is not incidental to a mail service.

iii. Yes, it has nothing whatsoever to do with customary hard-copy mail.

iv. No, it does not substitute for/function like a mail service, although, as noted above, it is in some sense a similar type of service.

v. Those answers are self-explanatory.

RESPONSE OF POSTAL SERVICE WITNESS FOTI TO INTERROGATORIES OF THE OCA

OCA/USPS-RT1-2. At page 3 of your testimony, you state that in a 1991 report commissioned by the Postal Service and prepared by a consulting firm, the consultant used the name “electronic postmark” and clearly described the function of the electronic postmark as “a secure time and date applied to electronic messages and documents.” Further down the page, you describe a 1995 Technology Applications focus group that discussed “the notion of electronically time and date stamping electronic documents and messages.” Are these descriptions still applicable to describe the functions of Electronic Postmark (EPM)? If not, explain fully and provide the current description. Provide all Postal Service documents that support any description different from that used in the 1991 consulting report or 1995 focus group.

RESPONSE

Below is the relevant description of the USPS EPM which can be found on the USPS internet site:

The USPS Electronic Postmark™ (EPM) protects the integrity of your electronic data through the use of auditable time stamps, digital signatures and hash codes. Through the USPS EPM web-based service, any third-party can verify the authenticity of electronic content. The EPM provides evidence to support non-repudiation of electronic transactions. The EPM is designed to deter and detect any fraudulent tampering or altering of electronic data.

Additionally, the Postal Service has provided USPS EPM description with previous filings to the Commission concerning Nonpostal Programs. On June 1, 2006, in response to Commission Order No. 1449 (Docket No. RM2004-1), and again on July 25, 2006 in response to OCA/USPS-58 (Docket No. R2006-1), the Postal Service provided the following description of the USPS EPM:

“ELECTRONIC POSTMARK (EPM)

The USPS Electronic Postmark (EPM) is currently an out-sourced all-electronic service giving customers a way to time-stamp electronic files. The EPM provides evidence that a document or file existed at a specific time and date and detects changes made to the postmarked document. Since January of 2003, the service has been performed as a strategic alliance with an outside vendor, Authentidate,

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

under postal direction, policies, and branding. The Postal Service shares a portion of the EPM fees collected. The service is sold over the internet via online sales, or via a hardcopy sales agreement.”

Finally a more detailed description of the USPS EPM can be found in the attached USPS EPM White Paper which is available on our provider’s internet site at <http://www.authentidate.com/index.php/content/view/35/62/>



USPS[®] Electronic Postmark[™] (USPS[®] EPM[™])
White Paper

September, 2003

Contents

Contents	1
Introduction	1
Highlights of the USPS Electronic Postmark	1
Legal Strength of the USPS EPM.....	1
Benefits of USPS EPM	2
Start Using the USPS EPM Today	2
Developers.....	2
End Users	2
Technology Overview	3
Non-Repudiation – Proving WHO did WHAT and WHEN	3
Hash Codes prove WHAT	3
Digital Certificates Prove WHO.....	4
Digital Signatures Prove WHO did WHAT	4
Time Stamps Prove WHAT and WHEN	4
Trusted Third Party for Long Term Non-Repudiation	4
How does USPS EPM work with PKI?	4
Putting it all together - The EPM Process	5
USPS EPM Extension for Microsoft Office	5
ESIGN and Signing.....	5
How EPM Works	6
Overview	6
Authentication	6
Verification	6
USPS EPM Specifications	7
Features	8
Software Development Kits	9
USPS EPM Enabled Applications.....	9
Security Standards.....	10
USPS EPM Related Services	11
In-Person Proofing at Post Offices (IPP) Program	11

Introduction

Highlights of the USPS Electronic Postmark

The advent of the Internet increased the need for efficient communication of electronic information with the same level of trust and value that the public has come to expect from the USPS® in the physical environment. The USPS® Electronic Postmark™ (USPS® EPM™) was created to facilitate secure electronic communication for government and commercial systems and has the potential to strengthen the security, privacy, and productivity of communication in the nation's electronic future.

The USPS EPM is a web-based security service. It includes trusted time stamps and content authentication technology, as well as aspects of non-repudiation. The trusted time stamps are derived from the National Institute of Standards and Technology (NIST), the official US source of time for commerce. These time stamps are auditable such that for each time stamp issued, the system is able to produce upon demand the bracketing time synchronization events starting from NIST and following a secure chain of custody through any intermediary clocks.

The USPS EPM service combines trusted time stamps with content authentication technology. This combination proves document authenticity when a resulting USPS EPM is associated with a document or transaction that can later be verified using the USPS EPM repository. Finally, the service enables digital signing applications by including support for digital certificates. The combination of these technologies maintained in the USPS EPM repository provides third party evidence to support non-repudiation of electronic transactions and is designed to detect the fraudulent tampering or inadvertent altering of electronic data.

Additionally, the USPS EPM supports applications so that they can comply with the E-SIGN legislation (Public Law 106-229 – enacted in June 2000) which made electronic signatures the legal equivalent of their paper counterparts in many situations. The E-SIGN law, which is technology neutral, provides general performance based guidelines eliminating legal barriers to using electronic technology to form and sign contracts, collect and store documents, and send and receive notices and disclosures. The USPS EPM is consistent with these guidelines, and enables corporations and individuals to take advantage of online contracts and commerce with a trusted USPS service.

The USPS has contracted with Authentidate to provide the sales, marketing, technology and services for customers to purchase and use the USPS EPM. Authentidate is currently the sole provider of the USPS EPM. By bringing the EPM to market with Authentidate, the USPS provides an important service to the public which combines the long standing integrity of the Postal Service with Authentidate's content authentication technology.

Legal Strength of the USPS EPM

Security experts agree that trusted time stamps and trusted third party archival of signatures and receipts are necessary to ensure long-term non-repudiation. A wide body of knowledge suggests that even today's best PKI technologies may be capable of being "broken" in the future, rendering signatures and receipts that are not archived by a trusted third party, untrustworthy (unless they are re-signed). Additionally, to ensure completeness and enable non-repudiation, e-commerce systems must have a third-party time-stamping system in place because it is simply too easy to alter dates on computer systems. Government and industry reporting requirements specifying that information must be submitted by a certain date and time can also be satisfied through the USPS EPM service.

In addition, a well-established body of federal law exists which support the USPS and its operations and services. The United States Postal Inspection Service protects the integrity of USPS operations and is authorized to investigate a variety of criminal activity. Any attempt to criminally interfere with the operation of the USPS EPM may be subject to investigation and prosecution under several federal statutes.

Benefits of USPS EPM

The USPS offering of the EPM is significant for a variety of reasons. In light of recent economic conditions affecting the technology marketplace, the longevity of an organization and its ability to continue offering and supporting services into the future is of primary concern to customers. USPS policies for long term archival and retrieval of EPM receipts mean that these receipts will be available to satisfy legal retention requirements for years to come.

Equally important to the general marketplace is the fact that the USPS EPM offering provides a web-based service with an affordable, volume-based, transactional pricing model. This egalitarian approach provides a cost effective means by which companies large and small, as well as individuals, can utilize this non-repudiation service for trusted applications.

Additionally, where government agencies in particular are seeking ways to reduce the burden on citizens and businesses, the USPS EPM provides a service by which organizations can implement a receipting process to facilitate a basic system of records of all electronic transactions for a customer of that agency. A standard manifest will save countless hours of organizational and retrieval activities for organizations and individual customers alike.

As one of the most trusted government agencies in the United States today, the USPS offering of the EPM has the ability to stimulate electronic contracting and transactions by encouraging people who may be reluctant to use the Internet or technology to do business electronically. By stimulating widespread use of electronic systems, the USPS EPM has enormous potential to significantly increase government and commercial adoption of such systems. In turn, increased adoption of electronic systems facilitated by the USPS EPM will enhance national productivity by stimulating the technology industry and eliminating the costs associated with preparing, shipping, and storing paperwork.

Start Using the USPS EPM Today

Developers

EPM Software Development Kits (SDKs) allow developers to easily build applications incorporating USPS EPM functionality. The SDK's are available for both the Microsoft Windows development environment (using the COM EPM SDK), as well as for a variety of other development platforms (using the Java EPM SDK).

End Users

Because the USPS EPM is provided as a web service, end users will find that the USPS EPM easily fits their business needs. The USPS EPM service will soon be (planned fall 2003) integrated with Microsoft Office Professional Edition 2003 (part of the Microsoft Office System) and Microsoft Office XP as an Extension to Microsoft Office for Word. See more discussion about the details of the USPS EPM Extension for Microsoft® Office on page 7. For more information about these services, contact information is provided here.

United States Postal Service
USPS EPM Program Manager
475 L'Enfant Plaza, SW Suite 3300
Washington, DC 20260
202-268-7455
www.uspsepm.com

Authentidate
Connell Corporate Center
300 Connell Drive 5th Floor
Berkeley Heights, NJ 07922
800-870-5348
www.authentidate.com

Technology Overview

Electronic commerce enhances business efficiencies, enabling electronic data to be stored, accessed or transmitted with great ease. These efficiencies, however, and the dramatic growth of the Internet as a medium for communication, have raised new issues and concerns related to the security of electronic information. For example, when exchanging documents over the Internet, users (both corporate and individual) are concerned by such factors as eavesdropping (information remains intact, but privacy is compromised), tampering (information in transit is changed or replaced) and impersonation (information passes to a person who poses as the intended recipient).

Non-Repudiation – Proving WHO did WHAT and WHEN

The fact that electronic data can be easily altered necessitates a system by which parties can trust the information they share and use in everyday transactions. This requirement for trust is referred to in both the legal and crypto-technical worlds as non-repudiation. Non-repudiation is important in e-commerce to prevent parties to a transaction from disputing or denying the transaction after the fact. The primary goal of a non-repudiation system is to prove WHO did WHAT and WHEN, and maintain evidence of such information to resolve disputes, or for auditing and compliance.

Non-repudiation should be viewed from both a legal and a technical perspective. From a legal perspective, the American Bar Association PKI Assessment Guidelines define the term non-repudiation as "...sufficient evidence to persuade the ultimate authority (judge, jury or arbiter) as to such origin, submission, delivery, and integrity, despite an attempted denial by the purported sender." (p. 281)

In general terms, to repudiate something is to deny its existence, and therefore non-repudiation services use cryptographic methods which prevent an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority, providing proof of origin; for proof of obligation, intent, or commitment; or for proof of ownership.) From a technical perspective, the term non-repudiation is used within authentication technology to describe a service which "...provides proof of the integrity and origin of data, both in an unforgeable [not able to be forged] relationship, which can be verified by any third party at any time; or, ... [provides a] high assurance ... [that data is] genuine, and that can not subsequently be refuted." (W. Caelli, D. Longley, and M. Shain, 1991. *Information Security Handbook*. London: Macmillan.)

Time stamping services are an aspect of non-repudiation services which provide "...a strong and verifiable cryptographic statement that a specific digital record existed at a specific moment in time. Time stamping a digital record provides the relevant parties with a verifiable statement of when the digital record was known to exist. Time stamping a digitally-signed record can further provide the relevant parties with a verifiable statement that the digital record was signed while the signing certificate was valid e.g., that the signature was formed before the expiration date of the signing certificate." ... [T]ime-stamping services thus provide the technical basis for general non-repudiation services, and for both Common Law – and Latin-derived notarial services." (p.182 ABA PKI Assessment Guidelines).

Hash Codes prove WHAT

To prove that the contents of a file have not been tampered with, USPS stores a *hash code* of the file, without actually seeing or storing the file. A hash code, also referred to as a "file signature" or "message digest", is a number that uniquely represents (is sufficient to identify) a particular file. Hash codes are unique in the sense that two different files will never have the same hash code, except in the unlikely event of a *hash collision*. The likelihood of a hash collision decreases exponentially as the bit length of the hash code increases. With the 160 bit SHA-1 hashing algorithm (the industry standard) used by the USPS EPM, the odds of a hash collision are exceedingly remote (1 in 2^{80}). And because the hashing function is 'one-way', no portion of the original data can be reconstructed from the file signature (in the same way an individual cannot be "reconstructed" from his signature or fingerprint). Hashing functions are superior to their technical counterpart the checksum, in that it is not possible (or at least extremely unlikely using today's technology) to find a second file with different contents that has the same hash code. Thus, if a user can present the EPM Service with a hash code, it can be assumed that the person who computed that hash code had in their possession a certain file.

Digital Certificates Prove WHO

PKI (Public Key Infrastructure) uses the concept of public and private keys to prove identity at a distance in the electronic world, where “face to face” authentication is impractical. A digital certificate is comprised of two “keys”, one public and one private key. The public key is freely distributed, and serves to verify a signature as being created by its matching private key. The private key is held secret by the owner, and is used to sign digital transactions. Certificate Authorities (CAs) control the issuance of digital certificates, and are responsible for properly identifying the owner (also known as *vetting*).

Digital Signatures Prove WHO did WHAT

A digital signature is created by signing a hash code of a file with the user’s private key. Since the public key is distributed as part of the digital signature anyone viewing the signature can now verify that it was signed by the corresponding private key. In this way, both senders and receivers can associate the sender’s identity with a specific file. The E-SIGN act, signed into law in 2000, gives electronic signatures the same legal strength as paper signatures for most documents.

Time Stamps Prove WHAT and WHEN

Time-Stamping is a process whereby a trusted third party signs a hash code with the current time. There is a protocol for time stamping – the Internet Engineering Task Force (IETF) 3161, that defines how hash codes are signed with a time stamp. This protocol is an *anonymous* protocol, meaning the identity of the submitter of the hash code is not associated with the file. The private key used for signing is that of the Time Stamping Authority (TSA). The TSA certifies (in the case of the USPS EPM, the TSA is the United States Postal Service) that the time stamp issued is accurate. This avoids the problem of relying on an individual computer clock for time stamping, since the time and date functions in a computer are relatively easy to manipulate. The USPS EPM derives trusted time stamps from the National Institute of Standards and Technology (NIST), the official US source of time for commerce.

Trusted Third Party for Long Term Non-Repudiation

All the techniques described above are today’s industry standard techniques for proving identity, signing, and time stamping. According to RFC 3126, Electronic Signature Formats for Long Term Electronic Signatures, one of the best ways to ensure successful long term non-repudiation is to store signatures and time stamps in a trusted third party repository, which can vouch for their integrity. The USPS EPM service stores a signed hash of the file or transaction and an associated time stamp signed by the USPS. Should there ever be a need to utilize newer, stronger algorithms, a trusted third party could *re-sign* the signatures and time stamps, thus preserving a *chain of trust* from the original as far into the future as required.

How does USPS EPM work with PKI?

The core strength of PKI is strong user-level authentication and digital signing (proving WHO did WHAT). The USPS EPM actually extends the trust of PKI by adding trusted time stamps, checking that the signing certificate is not expired, and archiving the transaction for long term non-repudiation. Therefore, the USPS EPM service is *complementary* to PKI, but the EPM user does not need to use PKI in order to use the EPM. USPS also uses PKI to establish a secure, tamper-proof connection between the customer’s network and the USPS EPM repository. The USPS EPM repository is issued server-level PKI digital certificates so that users can trust the service maintaining their file/document digital signatures.

Putting it all together - The EPM Process

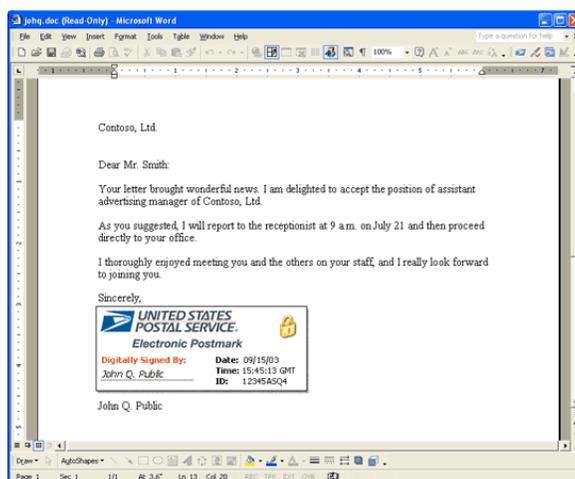
Where digital signature technology proves WHO did WHAT, and time stamping technology proves WHAT and WHEN, these technologies are all combined in the USPS EPM service to provide the necessary evidence to enable non-repudiation of electronic data. Now let's take a look at just one example of how the EPM works.

USPS EPM Extension for Microsoft Office

The USPS EPM, which enables users to verify authenticity, provide tamper detection, and date and time stamp their electronic documents and files, will be integrated with Microsoft Office Professional Edition 2003 (part of the Microsoft Office System) and Microsoft Office XP as an Extension to Microsoft Office for Word. The USPS EPM Extension for Microsoft Office software, co-developed by Authentidate and Microsoft Corp., will be available for download from <http://office.microsoft.com> in Fall 2003, where users will receive instructions on how to establish a USPS EPM account.

The USPS EPM Extension for Microsoft Office, an extra feature added to the standard Microsoft Word application, consists of an integrated set of capabilities, including: 1) digital signing of a Word document using digital certificates, 2) electronic content sealing and time/date stamping with the USPS EPM, and 3) the ability to subsequently verify the Word document's validity, authenticity and integrity.

Figure 1.0 Sample Postmarked Word Document



ESIGN and Signing

The USPS EPM service supports applications so that they can comply with the ESIGN legislation (June 2000) which made electronic signatures a legally viable option for conducting business. The USPS EPM Extension for Microsoft Office is an application that makes it possible.

The ESIGN law, which is technology neutral, provides general performance based guidelines eliminating legal barriers to using electronic technology to form and sign contracts, collect and store documents, and send and receive notices and disclosures. ESIGN also requires that electronically signed records are retained in a manner that: 1) accurately reflects the information set forth in the contract or other record; and 2) remains accessible to all persons who are legally entitled to access in a form that is capable of being accurately reproduced for later reference, whether by transmission, printing or otherwise.

The USPS EPM Extension for Microsoft Office allows users of the USPS EPM service to digitally sign, electronically postmark and verify Word documents so that documents stay protected, auditable and secure – allowing detection of alterations. The USPS EPM service is consistent with the ESIGN guidelines, allows content to be verified by users over the web, and maintains evidence of document authenticity for later reference for seven years.

How EPM Works

Overview

As a web-based service, the USPS EPM enables companies large and small as well as individuals to take advantage of the efficiency of the Internet for everything from correspondence to contracting with the ability to verify the authenticity of data.

The USPS EPM employs a secure time stamping clock, synchronized to the National Institute of Standards Technology (NIST), the official US source of time. A trusted time stamp is obtained from the time stamping clock and signed by the USPS to the unique hash code (associated with each customer's original file) to produce a combined USPS EPM receipt.

The USPS EPM cannot be changed by end users — or even by the USPS or Authentidate. In fact, attempting to tamper with an EPM in the USPS EPM repository could be prosecuted as a violation of federal law.

Authentication

The USPS EPM protects the integrity of your electronic data by providing third-party verification (via the USPS) of electronic content against the secure USPS EPM Data Center to establish that content has not been altered or changed since the time of electronic postmarking. This service provides the foundation for non-repudiation services by enabling non-repudiation of electronic content. The USPS EPM also allows for digital signing, whereby users can apply their identity to electronic content through access to digital certificates for signing as well as including declarations of intent when signing.

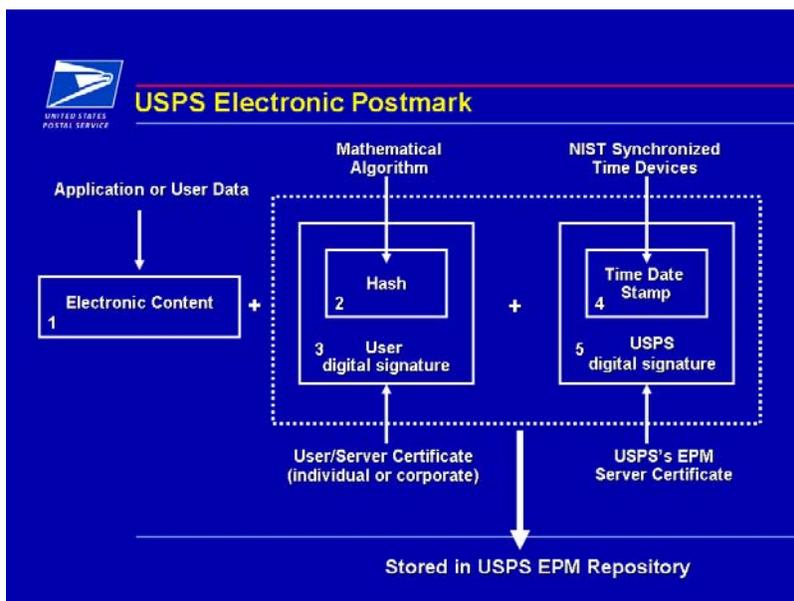
Verification

All documents, web forms, email, etc. that have been electronically postmarked by the USPS include the USPS EPM digital signature and a signed date/time stamp. The attributes of the digital signature and date/time stamp are made available for users to view as evidence of authenticity. The attributes of the USPS EPM include information illustrating that:

1. The contents of the document have not been modified in any way since the EPM was applied.
2. The EPM signature has not been modified or tampered with since it was signed.
3. The certificate used to sign the EPM was not expired at the time the EPM date/time stamp was issued.
4. The EPM date/time stamp denotes the exact time and date at which the EPM was issued by the USPS EPM Service.
5. The EPM date/time stamp has not been modified or tampered with.

The following diagram illustrates how the USPS EPM process works:

Figure 2.0 USPS EPM Process



1. Electronic content is created from any application.
2. The electronic content is submitted for an EPM through the USPS EPM SDK. The USPS EPM SDK then creates a hash code of the electronic content (a unique fingerprint of the file, but does not include the file itself (proves WHAT)).
3. The hash code is signed by the user/server digital certificate.
4. The signed hash code is sent by the USPS EPM SDK to the USPS EPM Data Center for time stamping. Once the Data Center receives the signed hash, the user/server's digital certificate is checked for validity against a Certificate Revocation List (CRL). Next, a trusted time stamp is obtained from the EPM Time Stamp Server (which is synchronized to the National Institute for Standards and Technology). The time synchronization events are logged by the time stamping hardware and can be used to prove that the time stamp issued for each EPM is accurate.
5. The resulting time stamp is then signed by the USPS digital certificate to produce an EPM, which is stored in the USPS EPM repository along with the user's signature of the file's hash to provide verifiable evidence of content for seven years. (WHO, WHAT and WHEN). The actual content of a file is never stored by the USPS EPM repository.

This electronic proof, signed by the Postal Service, provides evidence to support non-repudiation of electronic transactions. The EPM is designed to detect the tampering or altering of electronic data.

USPS EPM Specifications

The USPS EPM is a web-based service that is available in the form of a software development kit (SDK) for developers to use to build applications incorporating USPS EPM functionality. The SDK's are available for both the Microsoft Windows developing environment (COM SDK), as well as for a variety of other development platforms (Java SDK). The USPS EPM service is also available in an application, as an extension to Microsoft Office XP for Word documents.

Features

Features	
USPS EPM Service	<ul style="list-style-type: none"> ❑ Web-based service allows third-parties to verify authenticity of electronic content (documents, web forms, email, etc.) from USPS EPM repository ❑ Detects whether data has been modified or altered from time of USPS EPM applied to data ❑ Enables applications to include digital signing functionality, with a signing ceremony ❑ Technology consistent with the American Bar Association PKI Assessment Guidelines 2001* (See more information below) ❑ Consistent with Electronic Signatures in Global and National Commerce Act (ESIGN) performance-based requirements for electronic signing ❑ Compatible with all X.509 digital certificates ❑ Requires no modification or transmission of content (only a hash code of the file is logged as evidence of authenticity) ❑ Stores hash of data for 7 years

* According to the American Bar Association PKI Assessment Guidelines (June 2001), "A time-stamping service generally provides a strong and verifiable cryptographic statement that a specific digital record existed at a specific moment in time. Time stamping a digital record provides the relevant parties with a verifiable statement of when the digital record was known to exist. Time stamping a digital record can further provide the relevant parties with a verifiable statement that the digital record was signed while the signing certificate was valid, e.g., that the signature was formed before the expiration date of the signing certificate. Time-stamping certificate revocation lists and other revocation data corresponding to a signing certificate provides the relevant parties with additional assurances that the signing certificate was not revoked at the time of signing. Time-stamping services thus provide the technical basis for general non-repudiation services, and for both Common Law and Latin-derived notarial services." (PAG p.182)

Software Development Kits

Software Development Kits	
SDKs	<ul style="list-style-type: none"> <input type="checkbox"/> Obtain USPS EPMs <input type="checkbox"/> Verify USPS EPMs against USPS EPM repository <input type="checkbox"/> Verify USPS EPMs locally <input type="checkbox"/> Obtain verification receipts <input type="checkbox"/> Sample applications provided for easy integration and configuration into existing applications <input type="checkbox"/> User guides provided (Use of objects in EPM service and code samples) <input type="checkbox"/> All transaction secured by SSL communication with USPS EPM server
	<p>COM SDK</p> <ul style="list-style-type: none"> <input type="checkbox"/> Enables Windows applications to use USPS EPM service <input type="checkbox"/> Organized as a set of COM objects that can be used from any language or development tool that supports COM (Microsoft C++, Visual Basic, ASP, C#, etc.) <input type="checkbox"/> Shipped with extensive code samples in a variety of programs (C++, Visual Basic, ASP, C#, MFC, .NET, etc.), both GUI and command-line
	<p>Java SDK</p> <ul style="list-style-type: none"> <input type="checkbox"/> Java SDK is platform independent <input type="checkbox"/> Enables developers to integrate USPS EPM service into any platform <input type="checkbox"/> Java SDK can be used from any stand-alone Java and J2EE applications <input type="checkbox"/> Java SDK is packaged as a jar file for easy integration and configuration

USPS EPM Enabled Applications

Applications	
USPS EPM Extension For Microsoft Office	<ul style="list-style-type: none"> <input type="checkbox"/> Application for applying USPS EPMs to Word documents <input type="checkbox"/> Enables use of digital certificates for identity and signing <input type="checkbox"/> Compatible with all X.509 digital certificates <input type="checkbox"/> Web based verification of EPM's against USPS EPM repository <input type="checkbox"/> Option to verify USPS EPMs locally <input type="checkbox"/> Ability to include multiple USPS EPMs within a single document <input type="checkbox"/> Obtain verification receipts

Security Standards

The USPS EPM embraces a wide range of industry security standards, as well as technical and legal performance-based guidelines that are available today with respect to electronic data. The list below includes various standards and guidelines with which the USPS EPM is technically compliant. At present, these standards and guidelines include:

- ❑ **Fault Tolerant.** The EPM Data Center, including firewalls, routers, switches, servers, and storage, is designed to be 100% fault tolerant to any single component or connection failure. Disk mirroring is used in all servers. Multiple ISP connections are designed to assure continuous availability of the service.
- ❑ **Federal Information Processing Standards Publications (FIPS).** Time stamp server and time stamp private signing key are protected to FIPS PUB 140-2 Level 3.
- ❑ **Firewall.** Service is able to tunnel through all standard firewalls as HTTP-S traffic through port 443. The EPM service is also able to pass through both non-authenticated and password-authenticated proxy servers without modification or reconfiguration of the firewall or proxy servers.
- ❑ **Hashing.** System uses the SHA-1 hashing algorithm for each file processed.
- ❑ **Non-Repudiation.** All USPS EPMs issued are stored in a central USPS EPM repository for seven years to provide non-repudiation.
- ❑ **Operating Systems.** EPM SDK software runs on the following operating systems: Windows®, Solaris, Linux.
- ❑ **Public-Key Cryptography Standards (PKCS).** System supports the PKCS#7 Cryptographic Message Syntax Standard.
- ❑ **Secure Data Center.** The USPS EPM Data Center is housed in AT&T's secure hosting facility, including physically secured cages for servers and strict access control.
- ❑ **Secure Socket Layers (SSL).** EPM uses SSL for secure communications between the customer and the Central Server. Server-level digital certificates are used to authenticate the SSL connection.
- ❑ **Simple Object Access Protocol (SOAP)/Extensible Markup Language (XML).** EPM uses an XML-based SOAP protocol to communicate between the client-side SDK and the EPM Data Center.
- ❑ **Software Development Kits (SDKs).** Software Developer Kits are available and support the following languages: C++, COM, Java (JVM).
- ❑ **Time Stamping.** EPM time stamp servers are compliant with RFC 3161 Internet X.509 Public Key Infrastructure Time Stamp Protocol.
- ❑ **Trusted Time™ Auditable Timing Source.** The source of time is the National Institute of Standards and Technology (NIST), the official US source of time for commerce. These time stamps are auditable – that is, for each time stamp issued, the system is able to produce upon demand the bracketing time synchronization events starting from NIST and following a secure chain of custody through any intermediary clocks. (Trusted Time™ is a trademark of Symmetricom).
- ❑ **Web Services Development Language (WSDL)/Universal Description, Discovery and Integration (UDDI).** EPM is a Web Service, using the latest standard protocols. The Web services Description Language provides a way of describing the specific interfaces of Web services and APIs, and is used by UDDI. UDDI is a repository that stores the descriptions of Web services.
- ❑ **X.509 Digital Certificates.** USPS EPM uses X.509 digital certificates for strong authentication and identity purposes. At the end user level, an individual's private key may be used to sign the hash of a file or document. At the server level, the EPM time stamp server's private key (signed by the USPS) is used to re-sign the combined digital certificate containing the hash of the file or document and the secure time stamp.

Other product or service names mentioned herein are the trademarks of their respective owners.

USPS EPM Related Services

In-Person Proofing at Post Offices (IPP) Program

Similar to the goals of the USPS EPM service in facilitating secure electronic communication for government and commercial systems by providing verifiable evidence of electronic content, the USPS announced In-Person Proofing at Post Offices (IPP) Program, which is a related trusted service supporting the activities of U.S. Certificate Authorities and government organizations. (*Federal Register / Vol. 68, No. 116 / Tuesday, June 17, 2003*) [FR Doc. 03-153470]

The IPP Program is an operation by which the USPS conducts In-Person-Proofing of customers nationwide for physically authenticating an individual's identification at a post office before that individual is issued a digital certificate.

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 First Class U.S. Mail to verify physical addresses of applicants.

The IPP program begins when an organization establishes a relationship with a qualified U.S. Certificate Authority to integrate digital signing with improved identity verification into an online application. Then, any individual wanting to use digital certificates that include USPS IPP completes an application online. The online system will then verify the individual's identity via commercial database checking. Next, the system produces a standard Postal Service form that can be printed out by the individual. That individual then presents the form, and accompanying identification such as a driver's license and home utility bill, 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.

IPP creates 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. Similar to the USPS EPM, the IPP efforts support 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, Gramm-Leach-Bliley Act of 1999 as well as other Presidential directives on e-government.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-3. Please provide the Statement of Work for the 1991 report commissioned by the Postal Service (USPS-T-1 at 3, l. 4 -11). Also, provide the resulting report and any memoranda produced by the consultant or Postal Service in connection with this report.

RESPONSE

There were a number of activities mentioned in the History section of my rebuttal testimony to clearly establish that the Postal Service was active in developing electronic services (including the USPS Electronic Postmark) for over ten years. The main purpose of providing this background was to highlight Witness Borgers' inaccurate claim that the Postal Service entered the market in 2004, and to show that the Postal Service had already established itself in this emerging industry prior to 1998 when the concept occurred to Witness Borger. I have tried to provide the information requested in this and similar interrogatories. Because many of the activities mentioned took place many years ago, however, some of the information or documents being requested are no longer available. What is being provided, though, will clearly support my testimony that the Postal Service has been at this for a long time.

We were unable to locate the Statement of Work for the 1991 report commissioned, or to find the final report by the consultant.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-4. Please provide the internal documentation that led to the creation of the Technology Applications group (USPS-T-1 at 3, l. 13 – 17). Also provide any documentation describing the functions, goals, and mission of the Technology Applications group.

RESPONSE

Attached is an excerpt from the Fiscal Year 1994 Comprehensive Statement of Postal Operations discussing the creation and activities of this group.



Comprehensive Statement
on Postal Operations

FY 1994

HE6315 .A29 1994

United States. Postal
Service.

Comprehensive statement
on postal operations.

2. Retail Operations

a. Postal Lobby Improvements. The Postal Service continued to add computer-based Integrated Retail Terminals (IRTs) to retail operations.

In addition, Postage Validation Imprinters (PVI)s have been added to IRT systems at retail windows. PVIs have replaced postage meters and produce postage labels that validate the collection of postage and include the barcoded destination address of the mailpiece.

National standards for furniture, display fixtures, graphics, and signage that will be used in all future lobby upgrades are being developed. The first pilot sites completed in fiscal year 1994 included five sites in Van Nuys, California; three sites in Washington, DC; two sites in Northern Virginia; and five sites in Kansas City, Missouri. The test will be completed with 48 additional pilot sites throughout the country in fiscal year 1995.

b. Debit/Credit Card Acceptance. During 1993-94, market testing of USPS acceptance of credit and debit (bank/ATM) cards continued successfully in five districts (Ft. Worth, Dallas, Orlando, Capital, and Northern Virginia). The decision analysis report (DAR) for a national rollout of the program was approved in October 1994 by the Board of Governors. National implementation is scheduled to begin in April 1995 and continue during 1995-96.

c. Self-Service Equipment. Deployment of the first new Booklet Stamp machines began in fiscal year 1994. More than 1,000 will be deployed in postal lobbies during the first phase in the overhaul of the self-service program. The new machines sell basic postage stamps in booklet form or separately from coils, and customers can use debit cards as well as cash when purchasing stamps.

A contract was awarded for the production of a new single-stamp and small-booklet vending machine. One thousand machines will be purchased initially to replace old equipment. Each will return complete change, to include pennies, instead of stamps.

The number of Postage and Mailing Centers (PMCs) will be expanded to 40, while field testing continues. The PMC offers customers convenience and fast service for obtaining mailing information and costs. The PMC prints and dispenses stamps of the exact postage required at the time of purchase. Customers desiring change-of-address service will be able to enter their COA information on the PMC's keyboard. The information is then mailed to the customer at his old address for verification and, if correct, is forwarded to address management for incorporation into the system.

d. Philatelic Programs. Net philatelic revenue was approximately \$285 million in fiscal year 1994 — a 15 percent increase over the previous year. In conjunction with the issuance of stamps featuring popular singers and jazz and blues greats, the Postal Service conducted the first American Music Stamp Festival during the month of September and followed up with National Stamp Collecting Month's promotion centering around the Wonders of the Seas stamps. A nationwide stamp design contest co-sponsored by McDonald's generated 150,000 submissions by children. The four winning designs will be issued as stamps in 1995.

Consumer response to self-adhesive stamps has been overwhelmingly positive. The Postal Service introduced seven new "no lick" stamp designs in 1994, including two ATM stamps available through bank automated teller machines.

3. Information and Research Programs

I. Technology and the Future

As the Postal Service continues to be the leader in the delivery of hard copy communications, it is also seeking opportunities to leverage its technological base to create new products and services that will deliver value to customers. The Technology Applications department has been chartered to identify enabling technologies that will serve the needs of customers, help perform the Postal Service's core business activities more efficiently and reliably, and offer it the opportunity to become an innovative leader in the future electronic-services marketplace.

Technology Applications is meeting this challenge by focusing on three critical strategies: improving the existing mail flow by creating new hybrid mail services (electronic to paper and paper

to electronic); identifying and implementing new services in the emerging electronic commerce arena; and positioning the Postal Service in those new media markets. Taken together, these strategies will help carry the Postal Service into the next century and provide the next generation of communications products customers will need.

The following initiatives are examples of the Postal Service's commitment to provide technology-based services that are responsive to changing customer needs and expectations:

a. Reply Card Scanning. Reply Card Scanning is a hybrid service that captures scanned video images of customer information on business reply cards at the originating post office. The data is then electronically delivered to the recipient in a matter of hours, rather than the normal two- to four-day period, thereby reducing overall customer costs while improving postal operating efficiencies and speed of service.

b. Electronic Commerce. Working with other federal agencies, the Postal Service is evaluating the provision of electronic commerce services such as certification, authentication, encryption, electronic messaging, and value-added services based on its established role as a trusted third party to maintain security and protect individual privacy.

c. Kiosks. The National Performance Review team has asked the Postal Service to lead an interagency effort to electronically provide government information and services to the public. Working with federal, state, and local entities, Technology Applications is developing an interactive information kiosk to provide a single point of contact for government services, as well as ensuring fast, easy, and universal access to all citizens.

d. Address Recognition. A continuing area of contract research activity by the State University of New York (SUNY) is the recognition of handwritten addresses. During fiscal year 1994, earlier investigations were integrated into a prototype system that could completely process script addresses to the delivery point level. This requires that the system recognize delivery-line information in addition to the handwritten ZIP Code. Tests conducted in the laboratory of actual mail piece images indicated that more than 20 percent of the handwritten letters could be finalized. During the next year, computer processes developed by SUNY will be integrated with the remote computer reader (RCR) to further increase the performance of the entire remote bar coding system.

There have also been research efforts to increase the performance of the MLOCRs. These efforts have concentrated on designing improved address matching techniques. Using an addressing matching directory developed under earlier research programs, an MLOCR was converted to one that had two directory matching systems with software to arbitrate the results. Testing of this system saw increased delivery point coding results and a reduction in errors. Five additional systems are in the process of being field tested to confirm that the results can be replicated across the nation with the addressing peculiarities that exist in various locales.

Success with the co-directory also revealed that significant performance improvements should be possible by adding parallel recognition processing to the MLOCRs. A co-processing recognition system has been built and integrated with an MLOCR in the laboratory. Testing of live mail has begun and initial results of an arbitrated output look very promising.

Looking further into the future, a development is underway on a low-cost optical character reader. A full system — including a gray-scale camera, processing electronics, and address directory — is being developed for installation on small bar code sorters installed in delivery units. This effort is being undertaken by the University of Arkansas — the original developers of the wide area bar code reader — and will allow local OCR processing of letter mail that has originated at that delivery office.

2. Information Systems

a. Field Distributed Computing Infrastructure. As the Postal Service implements distributed computing on the workroom floor, at the retail window, on the loading dock, and in vehicles, it is moving to a standard information technology (IT) infrastructure. The dominant computing model is the small powerful computer — distributed throughout the organization and linked to an enterprise network. This business model emphasizes satisfaction of customer needs, decentralization

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-5. Please provide the Statement of Work for the 1995 focus group research (USPS-T-1 at 3, L. 19 – p. 4, l. 8). Provide the results of the focus group, including any reports that describe the results of the research.

RESPONSE

We are unable to locate the Statement of Work. Objection filed on providing report.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-6. Please provide copies of the 1994 and 1995 speeches of postal officials cited at USPS-T-1 at 4, l. 10 – 12.

RESPONSE

We no longer have copies of every speech from this period, but attached is a August 3, 1994 speech by Richard Rothwell, Senior Director of Technology Integration, on this subject, which I am informed is typical of the speeches at that time.

Address to Information Security Committee, EDI/IT Division
American Bar Association Section of Science and Technology
Quebec City, Canada, August 3, 1994

Good afternoon.

My name is Richard Rothwell. I am senior director of technology integration for the United States Postal Service.

I doubt there are many groups more aware of the sweeping changes taking place in communications than this one, or how those changes affect the way that all of us will do business in the future. Today I want to share with you my thoughts on the role of the postal service in this new age, and particularly, the role that we are being asked to assume in helping to facilitate the emerging world of electronic commerce.

The postal service was established, at the birth of the United States, with the mission of binding together a diverse and far-flung nation through the correspondence of the people. It was, and is, a broad-based mission. Over a century ago, then acting Attorney General William Howard Taft wrote that "the makers of the constitution ... had in mind the comprehensive view which regarded post offices ... as instruments for the transmission of intelligence," a mission they expressed "in very comprehensive terms..." Today we are being asked by our customers to consider new ways of carrying out this mission. Today we live in a complex, cost conscious, interdependent society which is developing new electronic communication systems and re-inventing commercial practices. For many applications, the new efficiencies of electronic data communication, the benefits that it has provided to its early adopters, and the competitive pressures that this evolution has created are driving corporations, governments, and individuals to explore new ways of conducting business, and serving their customers and constituents.

Yet, as many experts have noted, including many of you in this room, digital files as a rule are neither as secure nor as reliable as their paper counterparts. Digital files are designed to be easily manipulated by users on different computers. This is, of course, an essential element of the efficiency that electronic commerce conveys. But without some method of sealing a digital file to establish its contents, author, and time of

transmittal, the benefits of electronic commerce will inevitably be limited to highly structured transactions between parties that know and trust on another. Such limits will severely constrain or wipe out the benefits of electronic data interchange. A recent article in *Government Computer News* noted that the use of trading partner agreements to structure EDI agreements could require the services of hundreds of lawyers to negotiate, write, and argue about the agreements just for government procurement. This is evidence of the great degree of transactional friction that must inevitably accompany such an approach.

If electronic commerce is not going to be limited to highly structured transactions between well known and trusted parties, other solutions must be developed to create an effective legal framework and electronic infrastructure. Electronic communication media cannot become a reliable basis for widespread business use without a trusted method of sealing digital contents, verifying the parties involved, and establishing an official date and time for the transaction.

Government has similar needs. Trust and security are essential to the success of the national information infrastructure, the reform of government performance, and a number of other critical functions, such as the implementation of health care reform. Personal, educational, literary, and business correspondence traveling on the information superhighway must be electronically guarded so that all citizens are reasonably assured of the integrity of their records. The timely delivery of important electronic information, and the identity and authority of the people with whom they communicate are equally important. Without trust and security, all of the supercomputers and all of the high-speed networks in the world cannot make the NII succeed on the broad functional basis for which it was conceived.

As one of the nation's largest organizations, the United States postal service shares many of the concerns of both business and government. The Postal Service must manage transactions with thousands of organizations on a daily basis in the process of annually doing \$49 billion of business moving 171 billion pieces of mail. But our concerns are no different from those of any large enterprise in the world today trying to make its operations more efficient.

There are not likely to be many in this room who do not believe in the need for a mechanism for establishing the reliability of an electronic transmission, and binding an individual to it. I

therefore do not believe that it will be necessary to conduct a detailed exploration of the advantages of building a public key infrastructure as a solution to the technical problems of providing security for electronic documents. What I will talk to you about is the role the postal service can play in providing these technical solutions where they are needed.

There are several reasons why the postal service is developing platforms for providing solutions to these problems. First, our general duty to "bind the nation together through the personal, educational, literary, and business correspondence of the people" has taken on new meaning now that a hybrid information highway, part paper and part electronic, has become a reality and will continue to be for at least the next decade. Second, not surprisingly, our customers are asking us to play an expanded role in facilitating paper and electronic commerce because we have unique legal and institutional resources to accomplish the task. And third, we have to develop electronic services to meet our customers' needs for faster, more efficient handling of their products.

A core function of the Postal Service will remain the transmission of hard copy messages to and from residences and businesses in America. As I've noted, that function flows out of our core mission to bind the nation together. The Postal Service has other missions as well. We are tasked to provide service on a universal basis to patrons in all areas and to all communities. We are required to use every effort to provide efficient and expeditious delivery of correspondence. We are charged with protecting the privacy of postal customers and may not make available to the public by any means or for any purpose any mailing or other list of names or addresses, past or present, of postal patrons or other persons. And we are charged with maintaining the security and integrity of the mails, and investigating postal offenses and civil matters relating to the Postal Service.

As a consequence of these missions, the Postal Service has at least three assets which make us a likely candidate to play a role in this emerging field. First, the Postal Service already has much of the legal and institutional infrastructure necessary to assist in the development of widespread electronic commerce. Second, our size and widely distributed resources give us the practical tools to provide a much-needed service on a universal basis. Third, we are uniquely situated to protect core values

such as security and individual privacy as well as universal access to the tools of electronic commerce.

Let me discuss these one at a time.

First, the Postal Service has the legal structure to perform the duties of managing a certificate authority. The Post Office was originally established by the Continental Congress as the United State's first information highway. For over two hundred years, a sophisticated regime of statutes, regulations, and policies has developed to provide the infrastructure which enables secure, efficient, and inexpensive transmission of paper communications. For 200 years, the United States Postal Service has certified mail, sealed it with the power and authority of law, provided responsible and timely mail delivery, and insured patrons against loss or theft. A reliable and trusted mail system remarkably free of corruption or abuse has accompanied the development of a system of commerce in the United States which is second to none in the world.

For hardcopy communications, the legal framework is already in place to handle issues such as liability, indemnity, confidentiality, fraudulent use, theft, definite dating, etc. A similar framework will be required to support electronic commerce. Customers have suggested that the Postal Service may be in a unique position to provide part of that structure. For example, some customers have suggested that they are concerned with their own capacity to handle liability issues, and that the postal service provides a ready-made solution to this problem. Others have expressed concern about the confidentiality problems inherent in dealing with other companies, while still others have asked for a regime for controlling fraud which is as strong and convenient as that in place for mail fraud. Thus, the strong legal framework established for handling paper communications can provide similar benefits for electronic commerce.

Second, our customers are asking for our assistance in this area because we have unique practical assets, including:

- * The 40,000 retail facilities distributed nationwide.
- * Universal presence and the capacity to achieve significant scale.
- * The resources of an existing national information infrastructure.
- * A very strong verification process currently used for passports, that involves proof of id and other

information to a federal employee.

* The experience, policies, and ability to archive records without risk that they would be used for collateral commercial purposes.

The Postal Service is also a remarkably long-lived organization, and those of you who have struggled with archiving policies will recognize that to be an important advantage. As Bob Jueneman has said on the Internet, "Certificates 'R Us" may be gone tomorrow. If you have to prove that a certificate was registered on a certain date, and you are seeking an appropriate archiving facility, you can have confidence the postal service will still be around to support your request.

A third strength the Postal Service brings to enabling electronic commerce, and another reason that our customers have asked for help, is our capacity to create certificate management systems that can reach virtually every community in America, because we already have a substantial presence in those communities. We can therefore provide a solution to the question of how to put the tools of electronic commerce, such as certificates, into the hands of everyone. There are many obstacles to prevent citizens from taking advantage of the benefits of electronic commerce. Currently there are technological, geographic, economic, and knowledge barriers which prevent people from participating in the benefits of electronic commerce. To provide universal service to electronic commerce we must provide access which is universally usable and ubiquitous and scalable. By providing a solution to some of these access problems, the Postal Service may have an important role to play in ensuring that future communications in America provide a continuing framework for sustaining a democratic, participatory society.

Thus, many of the institutional features needed by an entity wishing to take part in certificate issuance and management already exist in the United States Postal Service. The Postal Service was established to provide very similar services for the support of correspondence when the physical frontier was chaotic and hard to reach. It is ready to provide similar services on the electronic frontier.

As the Postmaster General has informed Congress, we are actively supporting the development of the NII to facilitate the development of our own business and to help us carry out our mission. On March 24, the Postmaster General testified before the Senate affairs committee that "working with other federal

agencies, we may be able to develop an electronic commerce system." He also noted that, through the development of a kiosk program that might carry out postal transactions and perhaps also disseminate information from other agencies, our postal lobbies could become "on-ramps" to the electronic super highway. The Postmaster General highlighted two important areas in which the Postal Service may be helpful: serving the requirements of other government agencies, and providing universal service to those citizens who are in danger of being left out of the information revolution. To these he might have added a third, equally important area: protecting the privacy of American citizens. This concern is deeply embedded in postal tradition and statute. When we speak of the security of electronic commerce we should not miss the way in which commercial security and individual privacy are interconnected concepts.

While it is too early to know what precisely lies ahead, let me share with you a general description of the systems we are developing, both for our own use and for that of our customers.

The postal service is using public key encryption technology, and related technologies, to develop a public key certification authority and a set of associated trusted third party services which we call Postal Electronic Commerce Services (Postal ECS). When initially deployed, Postal ECS will provide a basis for electronic assurances within and among government agencies, and between government agencies and their constituents. In particular, the postal service has developed the ability to:

- * Issue public key certificates and store them in a public directory;
- * Provide for the "sealing" of selected documents or other electronic objects and associating them with a digital signature and a trusted time and date stamp;
- * Provide services for public key certificate publication and revocation; and,
- * Provide the ability to encrypt confidential information moving between the user environment and the Postal ECS management system.
- * Finally, provide near real-time access to certificates and their status.

The certification authority will issue and manage X.509 public key certificates containing a person's X.500 distinguished name, public key, and other identifying information. Users can then retrieve a certificate from the postal service, and use its

public key to authenticate a digital signature generated by the complementary private key.

The correspondence service provided by the system is the postal ecs seal which provides users with a validation of the originator based on his or her digital signature. We also provide a postal service digital signature on the digest of an electronic object that assures that it cannot be changed without detection. We also provide the postal service digital signature on a date and time stamp that we supply to enable proof of existence at a point in time and we provide archiving for those date and time stamps. Finally, we provide near real-time access to certificates and their status. This allows a user to get up-to-date information on the validity of certificates, and removes the need for users to maintain their own certificate revocation lists.

The postal service has implemented the certificate authority services, the correspondence services and the supporting directory on a host computer system in one of our major production data centers. We have also developed three postal service-licensed user agents as reference models to be installed on end user workstations that will provide access to postal ecs services. They run on Microsoft Windows-based PC's and access Postal ECS services via e-mail (either internet or X.400). We are also working on an interactive dial-up communication alternative and expect this to be available shortly.

These user agents contain standard programming interfaces that link user applications, cryptographic routines, and ecs services together. Our initial implementation is based on the Digital Signature Standard (DSS) algorithm set; but our plan is to support other cryptographic options such as RSA in the near future.

We are now moving from developmental work to actual proof of concept pilot testing of these services both internally in the usps and with our government agency partners. Our plans will evolve as we gain experience from these initial pilot tests and continue to talk with customers, and experts in encryption, software development, and computer science. We have shared our plans with congress, the administration, and the media. And we have asked ourselves three key questions:

- * Is this initiative critical to our mission and our responsibility to the public?
- * Do our customers have a need for our participation?

And,

*** Would the costs of providing these services be balanced by potential revenues?**

Certainly the responses that we have received to date more than justifies our view that this is an area in which we should continue to be an active participant.

Before concluding, let me directly address a controversial philosophical discussion about certificate management so you can understand what we see as the future world of electronic commerce. There has been a great deal of debate about the relative advantages of hierarchial versus peer-to-peer or one-level models for management of digital signature. To some extent, I believe this debate misses the point. The system for managing X.500 certificates that will eventually be adopted will be adopted only because it meets the business needs of the users. Because the complex communication needs of the future will require flexibility to meet individual desires, some mix of hierarchial and peer-to-peer or flat management schemes will be adopted.

What the recipient of an electronic document signed with a digital signature needs to know is how much weight to give that signature -- or, in other words, what actions to take based on an evaluation of the sender. This is exactly the same thing that is decided every day by people -- should we sell securities to a voice over the phone? Should we place an order with a new salesman? Given the infinite variety of possible transactions and encounters, there is no point in trying to impose on electronic transactions a single paradigm for authentication. Different levels of assurance, and different architectures, will be necessary for different uses. What is important is that the parties to the transaction are aware of the level of assurance provided.

The Postal Service can be of assistance in filling some specific needs in the certificate arena, but it has no intention of controlling or dominating that arena. For the near future the universe of electronic commerce will continue to have many different galaxies. Many varying concepts and services will be able to make valuable contributions. Many other entities will provide services in this area: as Vice President Gore has noted in numerous speeches, there is a role for both private and public entities. We plan to provide services based upon identified needs, which customers will decide whether or not they will use.

In keeping with the philosophy I have articulated, let me say that the Postal Service, in any development of these products, intends to support multiple cryptographic products in the market place. In addition, we will not compete with network service providers, nor will we become a network or carrier.

In developing these services, we are keenly interested in the work of this group. While the technology and scale issues seem to us to be manageable, we recognize that there are still many legal questions concerning the way in which the design of a public key infrastructure management service might best work. The liability issues are not yet completely clear, and the duties of each entity in such an infrastructure need to be articulated. As customers seek our services, we will have to face questions of scalability, investment, and the regulatory issues associated with the introduction of a new service. Can the service be managed? What investment will be required? How will regulators have us present the service to the public and at what price?

We greatly appreciate the exchange of views that this forum makes possible. We all have much to learn in this area, and I believe we should welcome the fact that we live in such interesting times.

[end]

----- End Included Message -----

- **Next message:** hallam@dxal18.cern.ch: "Re: OBCSCR"
- **Previous message:** [Nick Szabo](#): "The ultimate in trust"

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-7. Please provide the Statement of Work for the CygnaCom Solutions contract cited at USPS-T-1 at 4, l. 13 – p. 5, l. 5.

RESPONSE

The original Statement of Work for the Cygnacom Solutions, Inc., contract is no longer available, although the Postal Service does have the Statement of Work for 1997 for a later phase of the contract. It is attached. The only copy located contains text that was previously highlighted by unknown persons for unknown reasons, but the resulting shading on the attached copy is not to my knowledge intended to be a redaction. To provide a more legible copy, the page with the highlighting (page 1) has been retyped, and the retyped page is inserted behind the original page 1, in case the original is not sufficiently clear.

ATTACHMENT TO RESPONSE, OCA/USPS-RT-7
Amendment to the
Statement of Work
Order No. 102590-96-F-1247

Statement of Work for Phase V. Software Changes

OVERVIEW

The United States Postal Service (USPS) has begun piloting an infrastructure designed to provide Electronic Commerce Services to users of electronic networks. These services include an electronic postmark (similar attributes to the paper postmark) and other services required for the authentication and privacy of electronic documents. Initially, a partnership was formed between the USPS and a commercial firm to provide electronic postmarking and archival services. The commercial firm is located in Palo Alto, California. As the project progressed, it became more difficult and expensive for the commercial partner to provide operation support services. The USPS has decided that it would be more advantageous to develop, modify and operate an electronic postmarking service in the Washington, DC metropolitan area. The system must be constructed quickly, must provide reliable services, and be sufficiently flexible to offer and implement new services to meet customer demands.

The new electronic postmarking services allow the USPS to experiment with more innovative concepts in electronic commerce. For example, the postmark processor pilot will allow the introduction of return receipts for USPS electronic mail. It also offers the capability for the USPS to form new partnerships that do not rely on proprietary software from a single vendor.

PURPOSE

The purpose of this document is to identify the technical tasks and roles necessary to release a pilot electronic postmarking system.

EXISTING ELECTRONIC POSTMARKING SYSTEM

The electronic postmarking system is currently in operation at AegisStar's facility in San Jose, California. It consists of a Sun Sparc 20 serving as a USPS Postmarking Processor, and client software for the verification of USPS postmarks. In the current implementation, postmarks are generated using a software cryptographic engine and a hard-coded private key. Verification is performed on the client side using a dynamic link library (DLL) with the public key hard coded into the DLL. There is no support for standard X.509 certificates and no mechanism for key exchange.

PILOT ELECTRONIC POSTMARKING SYSTEM

In the Pilot implementation, the USPS Postmark Processor will provide mail services. The initial system will duplicate the electronic mail and postmarking services currently offered by AegisStar, with the exception of the archiving and billing. As new opportunities for partnerships between the USPS and commercial billing and archival services become available, modifications to the system may be made to accommodate these services.

Subsequent versions of the postmarker may include access to non-SMTP mail services (MCI, AT&T, etc.). As part of this effort, client software will be provided to perform verification of the electronic postmark at

**Amendment to the
Statement of Work
Order No. 102590-96-F-1247**

Statement of Work for Phase V. Software Changes

OVERVIEW

The United States Postal Service (USPS) has begun piloting an Infrastructure designed to provide Electronic Commerce Services to users of electronic networks. These services include an electronic postmark (similar attributes to the paper postmark), and other services required for the authentication and privacy of electronic documents. Initially, a partnership was formed between the USPS and a commercial firm to provide electronic postmarking and archival services. The commercial firm is located in Palo Alto, California. As the project progressed, it became more difficult and expensive for the commercial partner to provide operation support services. The USPS has decided that it would be more advantageous to develop, modify and operate an electronic postmarking service in the Washington, DC metropolitan area. The system must be constructed quickly, must provide reliable services, and be sufficiently flexible to offer and implement new services to meet customer demands.

The new electronic postmarking services allow the USPS to experiment with more innovative concepts in electronic commerce. For example, the postmark processor pilot will allow the introduction of return receipts for USPS electronic mail, it also offers the capability for the USPS to form new partnerships that do not rely on proprietary software from a single vendor.

PURPOSE

The purpose of this document is to identify the technical tasks and roles necessary to release a pilot electronic postmarking system

EXISTING ELECTRONIC POSTMARKING SYSTEM

The electronic postmarking system is currently in operation at AegisStar's facility in San Jose, California. It consists of a Sun Sparc 20 serving as a USPS Postmarking processor, and client software for the verification of USPS postmarks. In the current implementation, postmarks are generated using a software cryptographic engine and a hard coded private key. Verification is performed on the client side using a dynamic link library (DLL) with the public key hard coded into the DLL. There is no support for standard X509 certificates and no mechanism for key exchange.

PILOT ELECTRONIC POSTMARKING SYSTEM

In the Pilot implementation, the USPS Postmark Processor will provide mail services. The initial system will duplicate the electronic mail and postmarking services currently offered by AegisStar, with the exception of file archiving and billing. As new opportunities for partnerships between the USPS and commercial billing and archival services become available, modifications to the system may be made to accommodate these services.

Subsequent versions of the postmarker may include access to non-SMTP mail services (MCI, AT&T, etc). As part of this effort, client software will be provided to perform verification of the electronic postmark at

ATTACHMENT TO RESPONSE, OCA/USPS-RT-7

the client's personal computer. The software will be compatible with the postmarks generated by the pilot system. This software will be easily modified to meet customer demands and expectations.

On an as-needed basis and at the request of the USPS, the contractor will provide support to USPS customers who have special requirements or wish to integrate postmarking services into their existing structures.

The Pilot also increases security of the system. A hardware-signing device will replace the software cryptographic engine. The private key will be restricted to this hardware device. Access to the device will eventually be limited to USPS-authorized personnel.

Mail Reader

A mail "reader" will be constructed that is compatible with the current postmark implementation. The reader shall be user friendly, providing an easy to use graphical user interface (GUI). The reader will be suitable for distribution via floppy disk or the Internet. It shall provide the ability to verify an electronic postmark, decode and detach mail attachments. It is intended for use with the customer's existing mail package. The mail reader will process postmarks generated by either the current AegisStar system or the Pilot system.

Pilot Electronic Postmarker

A postmark processor will be constructed that provides SMTP-based mail and postmarking services. To provide the most compatible and reliable SMTP mail services, SendMail Version 8.5 will be employed to send mail to recipients. (One drawback of the current implementation is that a proprietary mailer was modified for this purpose, yielding incompatibilities with some Internet mail packages.) This system is intended to provide reliable services with minimal support.

The postmark processor shall use an Atalla Websafe for signature generation, and an Odetics GPS as a stable timebase. Initially, BASE64, UUENCODE, and text encoding will be supported for all messages. Other modules may be added as the need arises. Unlike the current AegisStar implementation, the pilot postmark processor will allow users to specify recipients using the tag USPOST or any reasonable derivation (e.g., U.S.POST, USpost, U S post, etc.). Like the current implementation, the pilot postmarker will support the following formatting tags: /text, /ccMail, /UUENCODE, /SUN, /Eudora, etc. Other switches will be supported, as new features become available.

The postmark processor may include an interface to MCI electronic Mail Service. This will consist of a server that transfers mail destined to/from the postmark server to MCI, providing native MCI users with USPS Electronic Postmarking services. Alternatives to this implementation will be evaluated prior the commencement of this effort.

Pilot Return Receipt

The postmark processor will include a return receipt function. The postmark processor will hold postmark messages in local storage and forward a message to the recipient indicating that the USPS has an electronic message for the recipient. The recipient will retrieve the message, causing a return receipt to be forwarded to the message originator.

Pilot Integrated Mail Sender

An integrated mail sender will be constructed that integrates the pilot mail reader and a SMTP mail sender capability. The mail sender will be designed for the Windows 3.1/95 environment. Mail will be sent using the SMTP protocol to send mail and POP3 to receive mail. Multiple attachments to email will be

ATTACHMENT TO RESPONSE, OCA/USPS-RT-7

supported. The mail sender will enable calculation of charges based upon the prices for postmarking and other services as required. The mail sender will display the value of these charges to the user prior to message submission. The mail sender may be required to provide encryption and digital signatures. A window will be displayed requesting that the user select the security services desired, including document archive, priority mail, express mail, and electronic postmark. Once any option is selected and a price is calculated, the USPOST (or other) tag will then be generated for the original address and all other addresses. The user will not be required to use the USPOST tag to generate electronic postmarks. The mail sender will perform this service transparently to the user.

Pilot Additional Modifications

Additional modifications to the postmark processor may be requested to support the USPS effort to establish electronic commerce. These may include providing software for commercial electronic mail vendors, integrating the postmark process in commercial electronic mail packages and systems, the development of an API for integration into commercial products, the development of a distributed architecture, and integration with other USPS projects, as required.

Pilot "Brainstorming Sessions"

The contractor will participate with USPS Marketing planners in a series of brainstorming sessions to define the Postmark process, sender and reader. The sessions will include freeform discussions, analysis, and alternatives to proposed solutions. The contractor will be responsible for documenting or assembling documentation on the session discussion and results.

ATTACHMENT TO RESPONSE, OCA/USPS-RT-7

Deliverables

1. Software deliverables
 - Pilot Mail Reader*
 - Pilot Mail Sender*
 - Pilot Return Receipt
 - Pilot Electronic Postmarker
 - Pilot Additional Modifications (as required)
2. Other deliverables
 - Pilot "Brainstorming Sessions"

In addition, the following will also apply:

- All client software used in development of the Postal Application must, to the greatest extent possible, be of commercial usage and must, to the greatest extent possible, comply with Postal standards.
- All rights to this software will revert to the United States Postal Service'
- All deliverables for technical documentation shall include source and object code, as well as printer/hardcopy deliverables.

*Note: the Pilot Mail Reader and Pilot Mail Sender may be combined into one user interface

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-8. Please provide any slides or handouts that were presented at the May 1996 meeting at Aegis Star (USPS-T-1 at 5, l. 7 -9)

RESPONSE

I am unaware of whether any slides or handouts were used in this meeting.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-9. Please provide any slides or handouts that were presented at the June 1996 demonstration at Foote, Cohn, Belding (USPS-T-1 at 5, l. 9 - 10). What was the purpose of the demonstration at Foote, Cohn, Belding?

RESPONSE

My understanding is the purpose of the meeting was to demonstrate a prototype EPM application. I am unaware of whether any slides or handouts were used in this meeting.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPSRT1-10. Please provide the Statement of Work for the Cylink project (USPS-T-1 at 5, l. 12 – 21).

RESPONSE

The original Statement of Work for this project is no longer available. A Statement of Work in connection with an extension of the contract for 2000 is attached.

IDIQ Contract No. 102590-00-B-1651

Statement of Work for Multi Algorithm PPKI Development and Support

Contractor: Cylink Corporation

1) Background

The U.S. Postal Service development of electronic commerce continues to be in an environment where requirements and technology are changing quickly. Several vendors are currently in beta test offering services requiring encryption software or public key software. The USPS is providing the Public Key Infrastructure and Certificate Authority (PKI/CA) services required by these vendors. These services include:

- electronic time and date postmarking and delivery confirmation
- certification of sender identity; and
- assurance that received document has not been altered en route
- identity validation for system/application access

This PKI/CA service provides digital certificates that qualify a device or user digital identity and establishes the premise that "I am who I say I am" when that device or user conducts an electronic transaction on the Internet. USPS PKI is currently being used for applications including the Information Based Indicia Program (IBIP) postal secure device (PSD), by issuing certificates for vendors deploying PSDs. The current number of IBIP certificates issued is approximately 400,000.

Other applications depending on this program to provide digital certificates include: Mailing Online requires digital certificates to identify non-profit mailers when submitting electronic documents for non-profit mailing; Post.CS™ (an international postal electronic document and file delivery service) requires digital certificates for both electronic signatures and encryption for both non-repudiation and privacy. This program is currently in pilot. Digital certificates will provide protection of Postal customer's financial transactions, personal correspondence, and non-repudiation of legal and other messages sent over the Internet.

Cylink Corporation is the developer of the Postal Public Key Infrastructure and Certificate Authority (PPKI/CA) software used to support IBIP and other Internet Business initiatives. This system provides digital certificates and an authentication architecture to enable these new businesses. There are two systems for which Cylink is responsible on site at Cylink:

- A development system used by Cylink to develop new functionality and
- a PPKI testbed system used by the USPS to pilot new enhancements

Cylink Corporation Proprietary Information

Revised 04/19/00

before they are transitioned to the production system.

The USPS has finalized a Certification & Accreditation on the Cylink production system which is located at the USPS San Mateo COSC. There has also been a complete security review and audit of the software prior to the move.

2) Objectives

- Operation of a PPKI Testbed
Infrastructure support of development by USPS and its vendors by the operation of a test/pilot PPKI system on Cylink's premises.
- Architecture Consulting and Development
- Support for Pilot phase
during the testing and deployment of PPKI software
- Support of Production Phase Installation
- Disaster Recovery system support
- Program Management and Coordination

3) Scope of Work

Cylink's specific obligations shall be as detailed below:

a) Operation of PPKI Testbed

Operation of a test/pilot Postal Public Key Infrastructure/Certificate Authority (PPKI) server on Cylink premises. This system shall support development and pilot activities. The system shall be available nominally from 7:00 a.m. until 7:00 p.m. PST, Monday to Friday, except Government holidays.

b) Architecture Consulting and Development:

All development activities shall be undertaken according to a mutually-agreed technical specification and initiated by task orders that may be issued from time to time by the USPS.

Cylink shall perform testing and validate the operation of new releases of PPKI server software prior to installation in the USPS San Mateo facility. Testing and software validation shall be conducted against the requirements specified and agreed between Cylink and USPS prior to starting development. Cylink shall provide on-site support of the CAT at the San Mateo COSC facility.

Cylink shall continue the development of enhancements to the IBIP system as required by the IBIP program manager such as:

- Allow authenticated users to perform a "real time" message authentication.

- Produce a downloadable file (updated at some specific interval) that lists all IBIP PSD certificates issued to allow USPS to perform a comparison against MATS and have a full loop audit on PSDs.
- Provide for a batch download of PSD certificates to allow for signature verification "off line".

Cylink shall provide support for PKI-enabled applications developed by the USPS or its vendors. Cylink shall provide system design consultation by the Cylink PPKI/CA System Engineer, software development, testing, end-user documentation and programming documentation. These PKI-enabled applications may include.

- eProof - a business-to-government secure authenticated electronic document interchange service. Delivery of the documents is proven via an electronic return receipt containing the USPS electronic postmark.
- NetPost - a multi-channel (hard copy and electronic) document delivery service messaging suite. This mailing online service requires USPS digital certificates for authentication of non-profit mailers prior to national launch, encryption for customer privacy, and controlling access to sensitive databases
- Shipping Online -- an Internet package delivery service that will require digital certificates for controlled data base access as well as user authentication.
- Electronic Mail Box - digital certificates will be needed for both authentication and encryption to ensure the users privacy and protect access to the mailbox.
- Internet Bill Delivery and Presentment - a secure financial transaction application requiring certificates for authentication and for digitally signing documents. Electronic Postmark to apply a time/date stamp and check for any evidence of tampering. Encryption certificates for privacy may also be considered for this application.
- An archiving service which provides ability to store and transfer as a just-in-time function. Such a service might be a component which enhances secure email and postmarked applications.

c) Support for Pilot Phase at COSC

Cylink shall provide continuing support for San Mateo operations personnel as needed during pilot projects. Operational support shall be for USPS business days only, beginning at 7:00 a.m. through 7:00 pm Pacific time, and would require a telephone response from Cylink within 4 hours. Note that unless problems can be solved by walking COSC support personnel through problems via phone, Cylink will either have to come on site at San Mateo or access through a secure system (not in place at this point in time.) If future expansion to hours or days is

necessary, additional funding will have to be negotiated. Support outside of the 7:00 a.m. to 7:00 p.m. window can be provided with 48 hours notice, for a limited period of time.

Cylink shall provide training as requested to USPS personnel.

d) *Support for Production Phase Installation*

Cylink shall support the production phase installation of PPKI according to its "Standard Safe" service level agreement, in the document entitled *Cylink's Worldwide Support and Maintenance Agreement* attached hereto.

Cylink shall deliver its standard commercial product training course to USPS personnel as requested.

e) *Disaster Recovery Site Operation*

The pilot test PPKI system that is maintained by Cylink in support of pilot applications and testing by USPS and USPS vendors shall be maintained in a state of readiness such that it could be brought online to support the continuing operation of the certificate issuing, revocation, and directory publishing of the operational PPKI at COSC.

The service level agreement describing Cylink's obligations for providing disaster recovery backup site are to be determined.

f) *Program Management and Coordination*

Cylink shall attend meetings with the USPS Program Managers and other contractors involved in the development effort for the purpose of updating all team members and to track the delivery of interdependent components of the system. Provide management reports to the Program Manager with detail program status (including procurement purchases to date and/or needs, and problem analysis/suggested solutions report).

4) Deliverables

The specific project deliverables relate to the requirements of the individual programs. The delivery dates will be determined after agreement on the technical requirements. Specific deliverables will include:

Technical Manuals – User's Guide and Installation Guide, distributed in .pdf format with software distribution media.

Software Deliverables - Based on the agreed requirements.

5) Schedule of Deliverables

Technical Manuals – User's Guide and Installation Guide

Cylink Corporation Proprietary Information

Revised 04/19/00

Statement of Work for Multi Algorithm PPKI Development and Support
ATTACHMENT TO RESPONSE, OCA/USPS-RT-10

Draft	Provided at each Customer Acceptance Test (CAT)
Final Version	Provided with final version of each delivery of Cylink's commercial PKI product
Software Deliverables	To be mutually agreed for each task order

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-11. Please provide all public announcements, speeches, and press releases concerning Electronic Postmark (EPM) (USPS-T-1 at 6, l. 1 – 4).

RESPONSE

Attached is the August 14, 1996, Federal Register Notice. I have been unable to locate any other public material from the Postal Service in this time frame.

POSTAL SERVICE**39 CFR Part 701****Postal Electronic Commerce Service**

AGENCY: Postal Service.

ACTION: Proposed rule electronic postmark test; request for comments.

SUMMARY: The United States Postal Service is developing "Postal Electronic Commerce Services" that will provide security and integrity to electronic correspondence and transactions, giving them attributes usually associated with First-Class Mail. As part of this effort, the United States Postal Service is testing a limited prototype of an Electronic Postmarking Service that will offer customers a third-party validation of the time and date that an electronic mail document was received by the Postal Service, and validate the existence of a document by ensuring that it was not changed after its handling by the Postal Service. The test is intended to be concluded within 60 days of its start, although it may be extended. To provide guidance for implementing the test, the Postal Service is proposing to add new regulations to title 39 of the Code of Federal Regulations.

DATES: Comments must be received on or before September 13, 1996.

ADDRESSES: Written comments should be directed to the Manager, Electronic Commerce Services, Room 5636, 475 L'Enfant Plaza, SW., Washington, DC 20260-2427. Copies of all written documents will be available at that address for inspection and photocopying between 9 a.m. and 4 p.m., Monday through Friday.

FOR FURTHER INFORMATION CONTACT: Leo Campbell (202) 268-6837.

SUPPLEMENTARY INFORMATION: To further its mission of "binding the Nation together through the correspondence of the people," 39 U.S.C. 101, the United States Postal Service is developing services which, through an extension of its traditional paper mail services, will enable and enhance the development of commerce by electronic means. These "Postal Electronic Commerce Services" will provide security and integrity to electronic correspondence and transactions, giving them attributes usually associated with First-Class Mail. As a first step in this effort, the Postal Service is testing a limited prototype pilot of an "Electronic Postmarking Service." Under this new service, the Postal Service will apply a trusted time and date stamp to a document that has been electronically submitted to the Postal Service ("Electronic Postmark"), and then digitally signs the document with a Postal Service private key (defined by a CCITT X.509 Version 3 certificate). This Electronic Postmark provides evidence of the document's existence at a specific point in time, allows any subsequent change in the document to be identified, and shows that the Electronic Postmarked version of the document was no longer in the possession of the originator at the time of marking.

This Electronic Postmark is a valuable third-party validation of the official character of some documents. For users of electronic commerce, the Electronic Postmark is a way to send important information in a manner that combines the security of postmarked paper with the speed and convenience of an electronic network. Further, the Electronic Postmark, if offered in combination with a public key infrastructure, can be used to validate the digital signature of a sender of documents. At this time, this certification capability is an additional service that the Postal Service will offer only in the event that there is clear demand from its customers.

Although the prototype system for the Electronic Postmark is still in development, it will be FIPS 140-1 compliant and will incorporate U.S. Postal Service Software Process Standards and Security Management Procedures. The Electronic Postmark will use Digital Signature Standard (DSS) as the signing algorithm. Future implementations may incorporate additional or different algorithms. For the prototype test, the service will be provided by contract with an Authorized Computer Service Provider.

This prototype pilot test is intended to last 60 days, although it may be

extended if necessary to achieve more complete test results.

Although exempt from the notice and comment requirements of the Administrative Procedure Act (5 U.S.C. §§ 553 (b), (c)) regarding proposed rulemaking by 39 U.S.C. § 410(a), the Postal Service invites public comment on the following revisions to the Title 39 of the Code of Federal Regulations.

List of Subjects in 39 CFR Part 701

Communications, Electronic Commerce Services, Postal Service, Telecommunications.

It is proposed that chapter I of title 39 be amended as set forth below.

SUBCHAPTER I—ELECTRONIC AND COMPUTER-BASED SERVICES

Part 701 in Subchapter I will be added to read as follows:

PART 701—POSTAL ELECTRONIC POSTMARK

Authority: 5 U.S.C. 552(a); 39 U.S.C. 101, 401, 403, 404, 3001-3011.

§ 701.1 Policy and objective.

The Postal Service seeks to offer Electronic Postmark Services that will offer Senders of Messages a third-party validation of the time and date that the Message was received by the Postal Service, and that will validate the existence of the Message by enabling Recipients to determine whether it was changed after its handling by the Postal Service.

§ 701.2 Trial period.

The Electronic Postmarking Services (defined in § 701.4) are being provided via a prototype system and will be made available to selected Senders as part of a pilot test that is intended to be concluded within 60 days of its start, although it may be extended if necessary to achieve more complete test results. The Regulations in this part will govern that pilot test.

§ 701.3 Definitions.

For purposes of this part, the following definitions shall apply:

(a) *Authorized Computer Service Provider* means a third party authorized by the Postal Service to accept and process Messages to be Electronically Postmarked and to forward the Postmarked Messages to the Recipient(s).

(b) *Authorized Value-Added Network* means a private computer-based value-added network designated by the Postal Service as authorized to carry Messages to the Postal Service for Electronic Postmarking.

(c) *Certificate* means a computer-based record that identifies the Postal

Service public key to be used for purposes of authenticating Postal Service Electronic Postmarks. The certificate will be in CCITT X.509 version 3 format.

(d) *Digital Signature* means a transformation of a Message using the Digital Signature Standard (DSS) and the DSA algorithm that allows recipients of the Message to authenticate the Message and determine whether the Message has been altered since it was received by the Postal Service.

(e) *Digitally Sign* means to apply a Digital Signature to a Message.

(f) *Electronic Address* means an alphanumeric or other designation corresponding a location on a computer network.

(g) *Electronic Mail Software* means any commercially available software product capable of sending and receiving electronic mail Messages.

(h) *Electronic Postmark* means data incorporated within a Message by the Postal Service that includes the following information:

(1) Postal Service branding.

(2) Date and time in Greenwich Mean Time (GMT) down to the second the Message was received by the Postal Service Mail Processor, as determined by the Mail Processor's internal clock.

(3) Postal Service Certificate serial number.

(4) Postal Service's distinguished name.

(5) Postal Service's Digital Signature consisting of the DSA R component and the DSA S component.

(i) *Mail Processor* means the computer system operated by an Authorized Computer Service Provider that is designed to handle the processing of Messages intended to be Electronically Postmarked in accordance with this Regulation.

(j) *Message* means any data in electronic machine-readable form directed to one or more Electronic Addresses to which it can be communicated via a computer network. A "Message" is not a "letter" for purposes of part 310.

(k) *Postmark Address* means the e-mail address to which a Message must be sent in order to obtain an Electronic Postmark.

(l) *Postmarked Message* means a Message, submitted to the Postal Service by a Sender in accordance with these Regulations, to which an Electronic Postmark has been added to the body of the Message as text, and which is attached to another Message containing a graphical representation of the Electronic Postmark.

(m) *Postmark Processor* means the computer system operated by or on

behalf of the Postal Service for the purpose of applying an Electronic Postmark to a Message.

(n) *Recipient(s)* means the person(s) designated by an Electronic Address in a Message prepared by the Sender to receive the Electronic Postmarked Message.

(o) *Sender* means an individual or entity that submits a Message to the Postal Service via an Authorized Value-Added Network for Electronic Postmarking under part 701.

(p) *USPS Mail Reader* means software developed or licensed by the Postal Service that enables a Recipient to view an Electronic Postmarked Message, view the Electronic Postmark, and authenticate the Electronic Postmark for such Message.

§ 701.4 Description of Electronic Postmark Services.

(a) The Postal Service will provide the following Electronic Postmark Services for Messages sent to the Postmark Address at its Mail Processor via an Authorized Value-Added Network:

(1) The Postal Service will apply an Electronic Postmark to the Message using a private key corresponding to the public key specified in its Certificate.

(2) The Postal Service will forward the Postmarked Message to the recipient(s) designated by the Sender, using the same Authorized Value-Added Network from which the Message was originally received.

(b) The Electronic Postmarking Services will be available on demand, on a 24-hour, 7-day-a-week basis, subject to equipment, software, and communications problems.

(c) The Electronic Postmarking Services do not include any undertaking by the Postal Service to deliver Messages to any intended Recipient. The Postal Service's obligation is limited to communicating the Electronic Postmarked Message, using each Recipient's Electronic Address as specified by the Sender, to the Authorized Value-Added Network from which it was received, for further communication to the intended Recipient by such Authorized Value-Added Network. The Postal Service shall have no obligation or liability with respect to the performance of any Authorized Value-Added Network.

(d) The Postal Service may subcontract the foregoing Electronic Postmark Services to an Authorized Computer Service Provider.

§ 701.5 Requirements for submitting messages to be postmarked.

Any person whether or not a U.S. citizen and whether or not located in

the United States may submit a Message to the Postal Service to be Electronically Postmarked in accordance with these Regulations, provided the following requirements are met:

(a) the Message must be in the format prescribed by § 701.6;

(b) the Message must be submitted to the Postmark Address at the Postal Service Mail Processor via an Authorized Value-Added Network; and

(c) the Sender must have an account with an Authorized Computer Service Provider for the purpose of obtaining Electronic Postmarks, and must pay the fee provided in § 701.8 to such Authorized Computer Service Provider.

§ 701.6 Message format.

(a) Messages shall be submitted electronically in a binary-encoded file.

(b) Messages must include: (i) the Postmark Address at the Postal Service's Mail Processor; (ii) a valid account number against which the Authorized Computer Service Provider may charge applicable fees for Electronic Postmarking Services, and (iii) the Electronic Addresses of any Recipients to whom the Electronic Postmarked Message should be forwarded after the Electronic Postmark is applied.

(c) For the purposes of this test, the specific format shall be specified by the Authorized Computer Service Provider.

§ 701.7 Authorized Value-Added Network and Authorized Computer Service Provider.

(a) All Messages to be Electronically Postmarked must be submitted to the Postmark Address through an Authorized Value-Added Network, and the corresponding Electronic Postmarked Message will be forwarded to the Recipient(s) by the Postal Service using the same Authorized Value-Added Network. Senders must make necessary arrangements with the Authorized Value-Added Network.

(b) The Authorized Computer Service Provider is responsible for issuing account numbers, billing Senders for the Electronic Postmarking Services, and supplying Senders and Recipients with the USPS Mail Reader software.

(c) The Authorized Computer Service Provider and Authorized Value-Added Networks may by contract or otherwise specify other protocols, formats, procedures, terms, conditions, and requirements not inconsistent with these Regulations with respect to the generation, structure, submission and receipt of Messages, the assignment, use, and authentication of account numbers, and the payment of charges assessed against account numbers.

(d) A list of Authorized Computer Service Providers and Authorized

Value-Added Networks may be obtained by contacting the Postal Service via electronic mail at: LCAMPBELL@EMAIL.USPS.GOV, or by writing to: Leo Campbell, New Electronic Businesses, 475 L'Enfant Plaza SW, Room 5670, Washington, DC 20260-2427. Requests sent by regular mail should include a self-addressed stamped return envelope.

§ 701.8 Fees.

(a) Senders submitting Messages shall be charged in accordance with fee schedules to be developed by the Postal Service. The fee shall be assessed against the Sender account number. Sender will be billed for the amount of the fee by the Authorized Computer Service Provider that issued the account number.

(b) A person submitting an account number in connection with a Message is representing to the Postal Service that he or she has authority to use the account number to pay for the Electronic Postmarking of the Message. Persons using account numbers without proper authority may be subject to fines and imprisonment.

§ 701.9 Specifications for recipients.

(a) When a Recipient receives a Postmarked Message, Recipient will need a USPS Mail Reader to read it. The USPS Mail Reader will include the public key file (and may include the Postal Service Certificate) for verifying the Postal Service Digital Signature on the Electronic Postmarked Message.

(b) The USPS Mail Reader is available from the Authorized Service Provider and will be licensed to Recipients on terms specified by the Authorized Service Provider. Use of the USPS Mail Reader constitutes acceptance of these terms.

§ 701.10 Electronic Postmark.

(a) Application of Electronic Postmark. Messages submitted for Electronic Postmarks will be processed substantially as follows:

(1) Upon receipt of the Message by the Mail Processor, the format of the information specified in § 701.6 and the Sender's account with the Authorized Computer Service Provider is verified. Messages that are not in proper format, and Messages received from Senders who do not designate valid account numbers, will be returned.

(2) Messages received in proper format from Senders with valid accounts will be readdressed to the intended Recipient(s) and passed to the Electronic Postmark Processor.

(3) The Electronic Postmark Processor will create an Electronic Postmark for

the Message. It will then create a new Message, with the body being a graphical representation of the Electronic Postmark and with the original Message attached to the new Message using Mime base 64. The new Message, with attachment, is then sent back to the Mail Processor as the Postmarked Message.

(4) The Mail Processor will then forward the Electronic Postmarked Message to the Recipient(s) designated in the original Message via the same Authorized Value-Added Network from which it was received.

(b) Security Policy. The Electronic Postmark will be FIPS 140-1 compliant and will incorporate U.S. Postal Service Software Process Standards and Security Management Procedures. Implementation of the Electronic Postmark will also be governed by the Postal Services Electronic Commerce Services Security Policy. The Electronic Postmark will use Digital Signature Standard (DSS) as the signing algorithm.

§ 701.11 Digital signatures and certificates.

(a) All Postmarked Messages will be Digitally Signed by the Postal Service.

(b) The Digital Signature shall be based on the original Message, plus the Electronic Postmark, using the Digital Signature Standard (DSS).

(c) All Digital Signatures will be generated using a private key held by the Postal Service corresponding to a public key specified in the Certificate located in the United States Postal Service Prototype Certificate Authority in the Information Systems Service Center (ISSC) in San Mateo, CA.

§ 701.12 Message handling generally.

(a) Except as provided in § 701.10, the Postal Service will not undertake to verify the format or integrity of any Message received for Electronic Postmark Processing. Messages shall be Postmarked as received, regardless of condition.

(b) Messages will be processed for Electronic Postmarking and forwarding to the intended Recipient within a reasonable time after receipt by the Mail Processor. However, the Postal Service does not guarantee any specific response time.

(c) Messages with invalid account numbers will not be Electronic Postmarked or forwarded to the Recipient. They will be returned to Sender.

(d) Electronic Postmarked Messages will be forwarded to the Recipient identified by the Sender using the same Authorized Value-Added Network as that from which the Message was

originally received by the Mail Processor. The Postal Service shall have no responsibility for delivery of the Message by the Authorized Value-Added Network.

§ 701.13 Terms and condition of service.

(a) The Electronic Postmark Services are offered subject to the terms of this part, which Senders are deemed to accept by submitting any Message to the Postmark Address at the Postal Service Mail Processor.

(b) The Postal Service shall have no liability to the Sender or any Recipient for any indirect, incidental, special, or consequential damages (including damages for loss of profits or revenue by the Sender, Recipient, or any third party), or for damages arising from lost or corrupted Messages or other data, delayed or incorrect forwarding of Messages, or any other failure or error on the part of the Postal Service, whether in an action in contract or tort, even if the Postal Service has been advised of the possibility of such damages.

(c) The Postal Service's entire liability for any damages claim (regardless of legal theory) arising from the provision of Electronic Postmarking Services shall not exceed the amount of fees paid by the applicable Sender for the Electronic Postmarking Services giving rise to the liability.

(d) Each Sender shall indemnify and hold the Postal Service and its Governors, officers, employees, subcontractors and agents (the "Indemnified Parties") harmless from and against any and all liabilities, losses, damages, costs, and expenses (including legal fees and expenses) associated with, or incurred as a result of, any claim or action brought against an Indemnified Party either for actual or alleged infringement of any patent, copyright, trademark, service mark, trade secret, or other property right based on the processing, or communication of any Message submitted to the Postal Service by the Sender.

(e) A Sender shall not submit Messages or otherwise use Electronic Postmarking Services in any manner that violates any federal or state law or regulations.

§ 701.14 Security provisions.

(a) Policy. The Postal Service will preserve and protect the security of all Messages and Postmarked Messages in its custody from unauthorized interception, inspection or reading of contents, or tampering, delay, or other unauthorized acts. Any postal employee committing or allowing any of these

unauthorized acts is subject to administrative discipline and may be subject to criminal prosecution leading to fine, imprisonment, or both. An employee having a question about proper security procedures that is not clearly and specifically answered by postal regulations or by written direction of the Inspection Service or Law Department shall resolve the question by protecting the Messages in all respects and delivering them, or letting them be delivered, without interruption to their destination.

(b) Interception, Searching, or Reading of Messages Generally Prohibited.

(1) General.

In general, no employee may intercept, search, read, or divulge the contents of any Message submitted for Electronic Postmarking, even though such Message may be believed to contain criminal matter or evidence of the commission of a crime. The only exception to this general rule is for a person executing a search warrant duly issued under Rule 41 of the Federal Rules of Criminal Procedure. Usually, a warrant issued by a Federal Court or service by a Federal Officer is issued under Rule 41, and is duly issued if signed and dated within the past 10 days. No employee shall permit the execution of a search warrant issued by a state court and served by a state officer.

(2) Disclosure of Information Collected from Messages Sent or Received by Customers. Except as provided in § 701.14(b)(1), no employee in the performance of official duties may disclose information collected from Messages processed by the Postal Service Electronic Postmark Processor, including any information about a Message processed by the Postal Service.

(3) Interference with Operation of Postal Computers.

Interference by any person with the operation of Postal Service data processing equipment, including the Postmark Processor, is strictly prohibited.

Stanley F. Mires,

Chief Counsel, Legislative.

[FR Doc. 96-19102 Filed 8-13-96; 8:45 am]

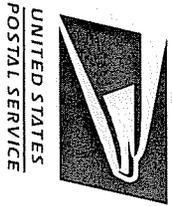
BILLING CODE 7710-12-P

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-13. Please provide any slides, handouts or other materials distributed in connection with the briefings for members of Congress, The Electronic Frontier Foundation, and any other groups (USPS-T-1 at 6, l. 5 -6).

RESPONSE

Attached is a presentation of the USPS Electronic Commerce Services to the San Jose Postal Customer Council. I have been unable to locate any other material during this timeframe.



UNITED STATES POSTAL SERVICE ELECTRONIC COMMERCE SERVICES

Customer Benefits of the Electronic Postmark

**Presentation to:
San Jose - PCC**

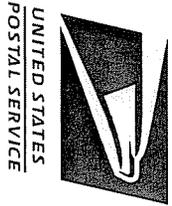
June 19, 1997

**Leo Campbell
Manager, ECS**

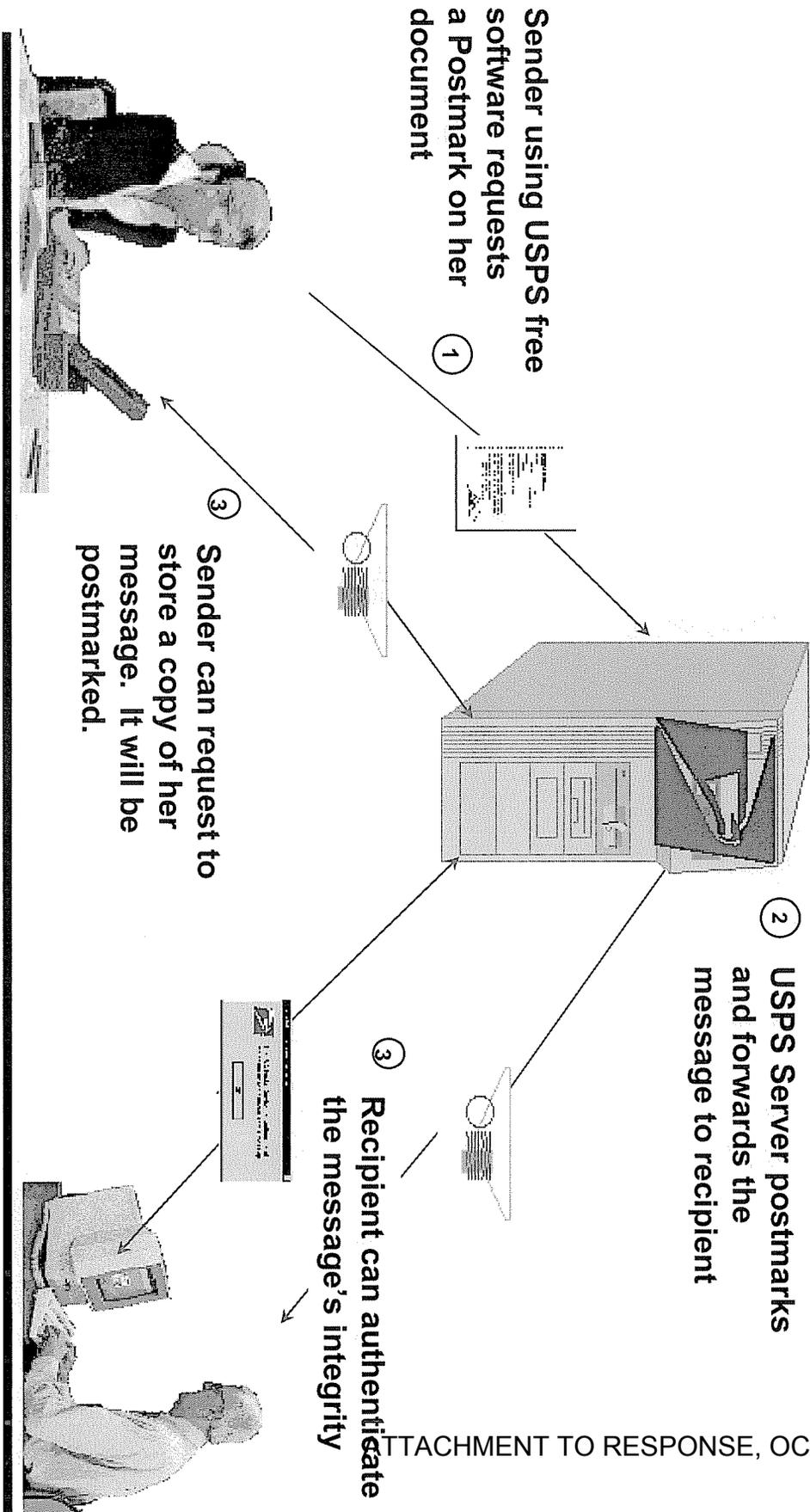


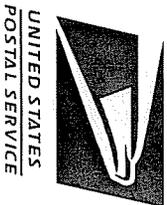
What is a postmark?

- **A time and date stamp**
But also -----
 - **Proof of existence**
 - **Third Party temporary possession**
 - **Chain of possession**
 - **Disinterested party handling**
 - **Generally Accepted practices and procedures**
-



How The USPS Postmarking Service Works





What You Get When You Postmark:

Attribute: Your document existed at a certain point in time

Benefit: Neither sender, receiver, nor third party can deny the document's existence



What You Get When You Postmark:

Attribute: Your document was no longer in the originator's control nor yet under receiver's possession

Benefit: Coupled with the first attribute, a verifiable chain of possession can be established



What You Get When You Postmark:

Attribute: Universally accepted date and time stamp assures all parties 'When' the document existed

Benefit: Coupled with both earlier attributes, all interested parties can now link chain of possession with time and dates of possession



What You Get When You Postmark:

**Attribute: Digitally applied USPS signature
validates contents have not been
altered**

**Benefit: The USPS signature assures the
recipient that the received
message is what was sent**



What You Get When You Postmark:

Attribute: Postal Service authentication continues a long uninterrupted history of legal standing and authority to authenticate

Benefit: Universal recognition by all parties (including courts) of the validity and authority associated with Postal involvement



What You Get When You Postmark:

Attribute: All USPS records of transactions undergo frequent and periodic internal and external audit

Benefit: These audits provide adequate proof to all interested parties that USPS procedures and practices adhere to stringent regulations that have consistently been upheld in many legal and audit venues



What You Get When You Postmark:

Attribute: For those documents you voluntarily choose to archive, postmarks are applied on all transactions which store and retrieve your document

Benefit: This additional postmarking adds a more thorough temporal chain of possession and evidence about your document's existence



CONCLUSIONS

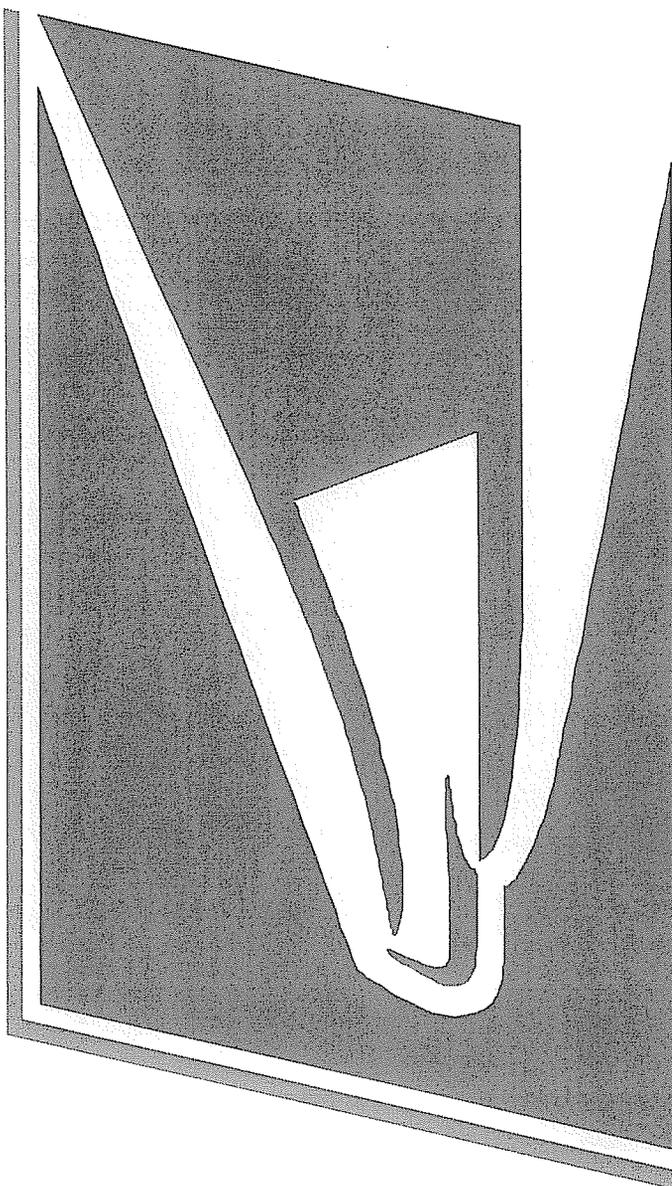
Email and web-based electronic transactions often require a proof of existence in time. While most systems can provide, literally, a time and date stamp, the USPS Electronic Postmark brings with it legal standing, enforcement, and security.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-14. Please provide copies of all materials used to demonstrate Electronic Postmark (EPM) at the San Jose, Chicago, and Boston trade shows, as well as multiple Postal Forum trade shows (USPS-T-1 at 6, l. 11-15).

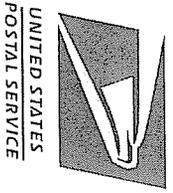
RESPONSE

To my knowledge, the only material that may exist is the attached presentation believed to have been used at the Boston trade show.

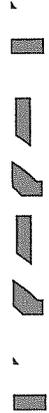


UNITED STATES
POSTAL SERVICE

*Boston DCI Trade Show
1998*



LONGEVITY



225 Years

1984

1991

1993

1994

1995

1996

1997

1998

1999

2000

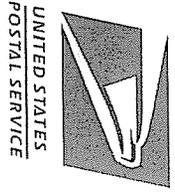
2001

2002

2003

2004

2005

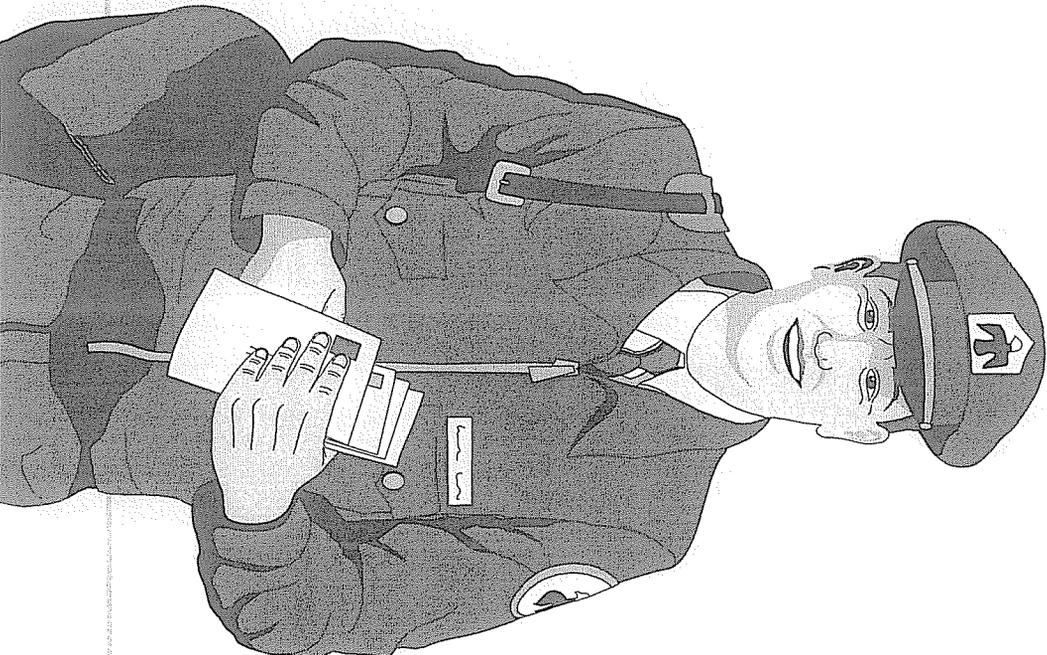


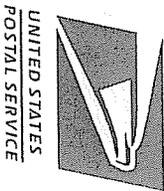
LONGEVITY

225 Years

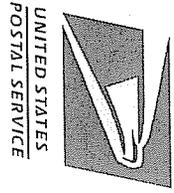
800,000

Employees



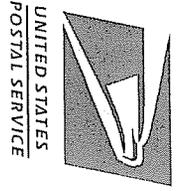


**“To bind the nation
together through the
personal, educational,
literary, and business
correspondence of
the people.”**

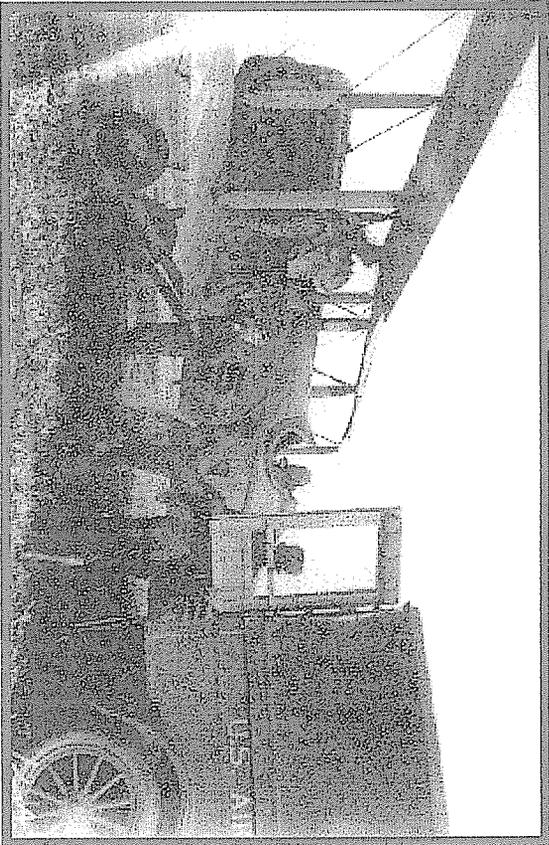
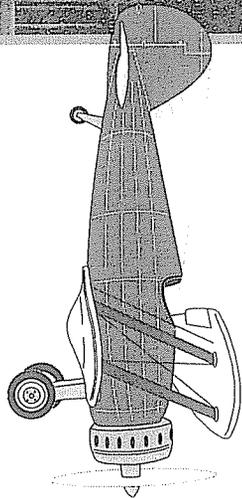
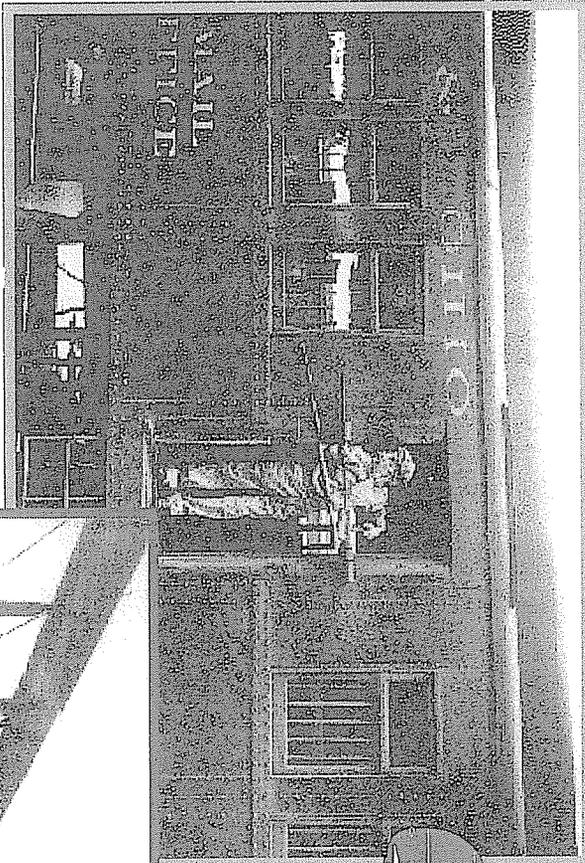


TRUST

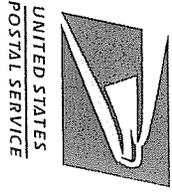
UNITED STATES POSTAL SERVICE



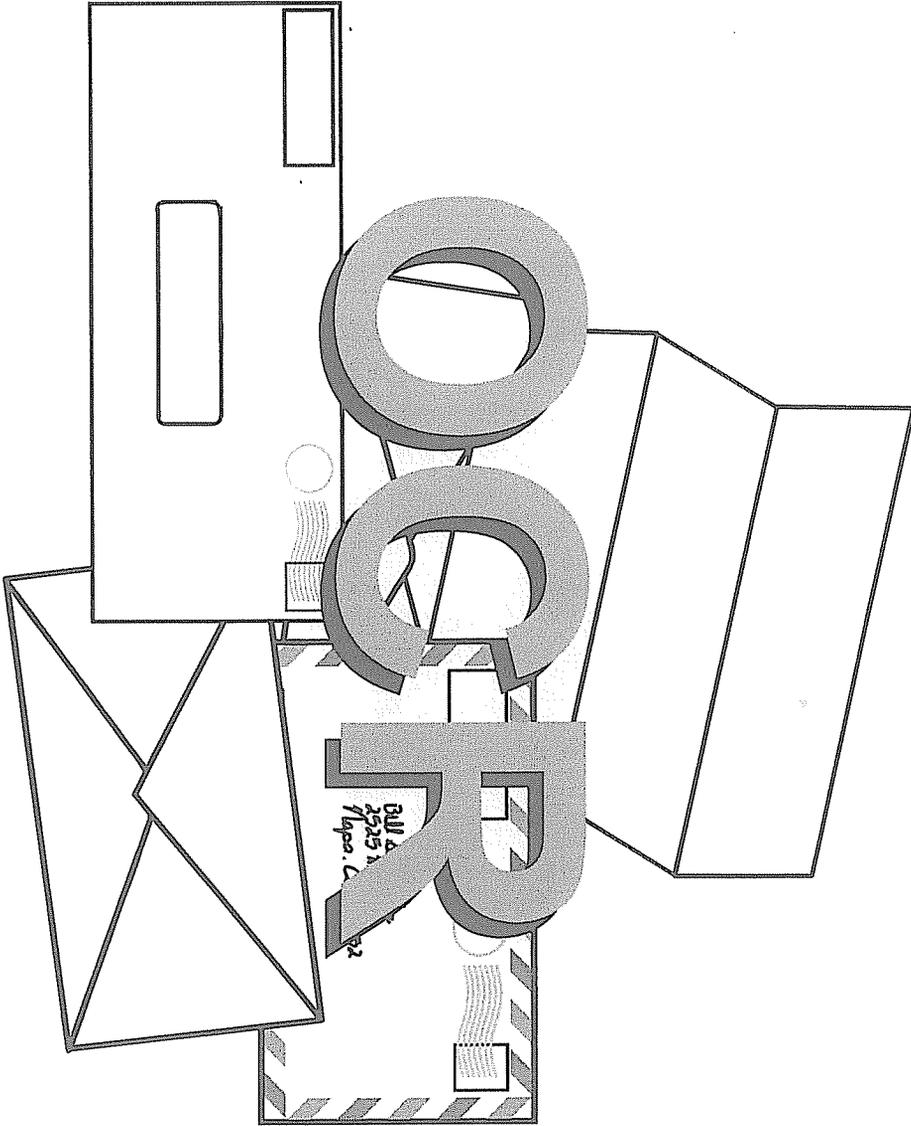
TECHNOLOGY

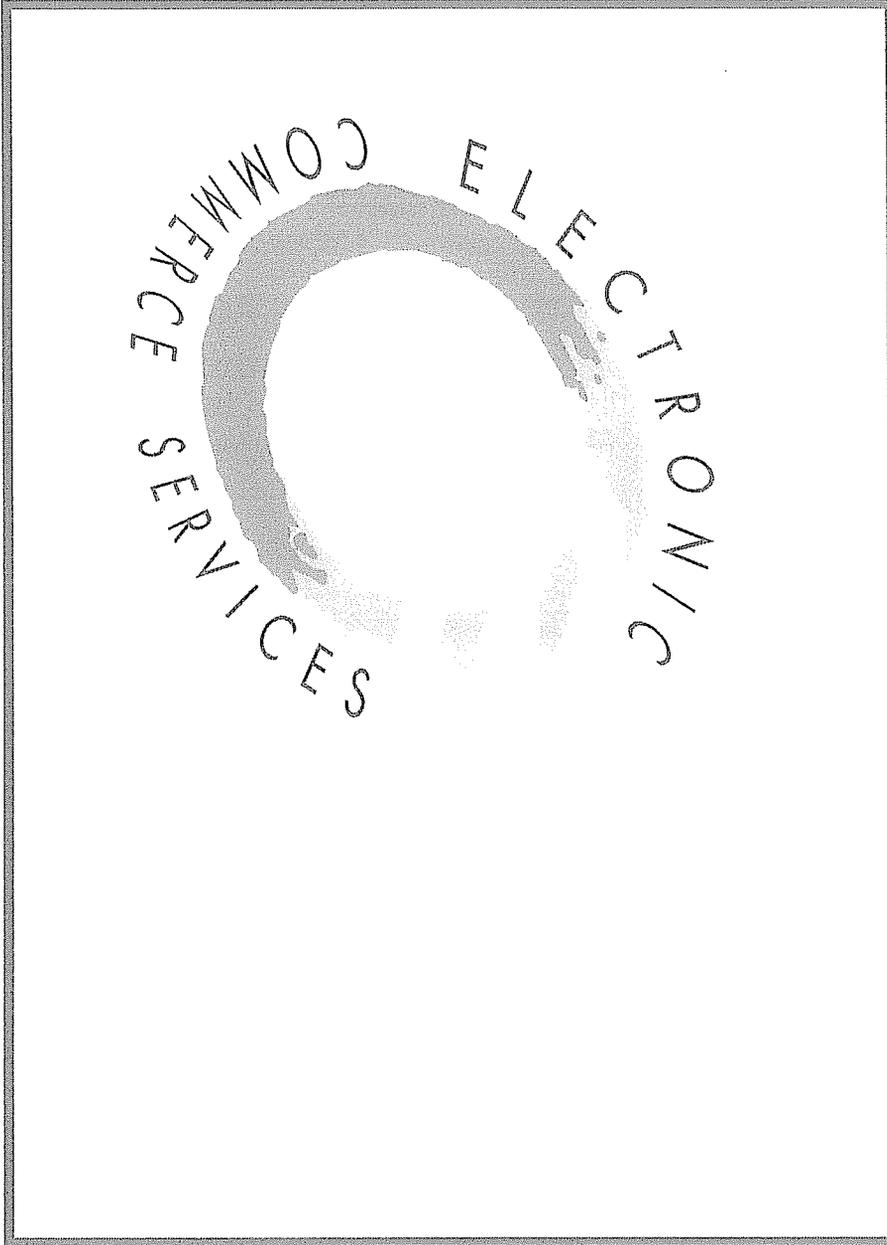
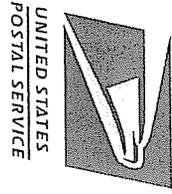


-  **Telegraph**
-  **Railroads**
-  **Aviation**

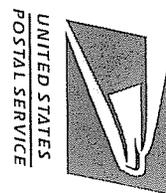


TECHNOLOGY

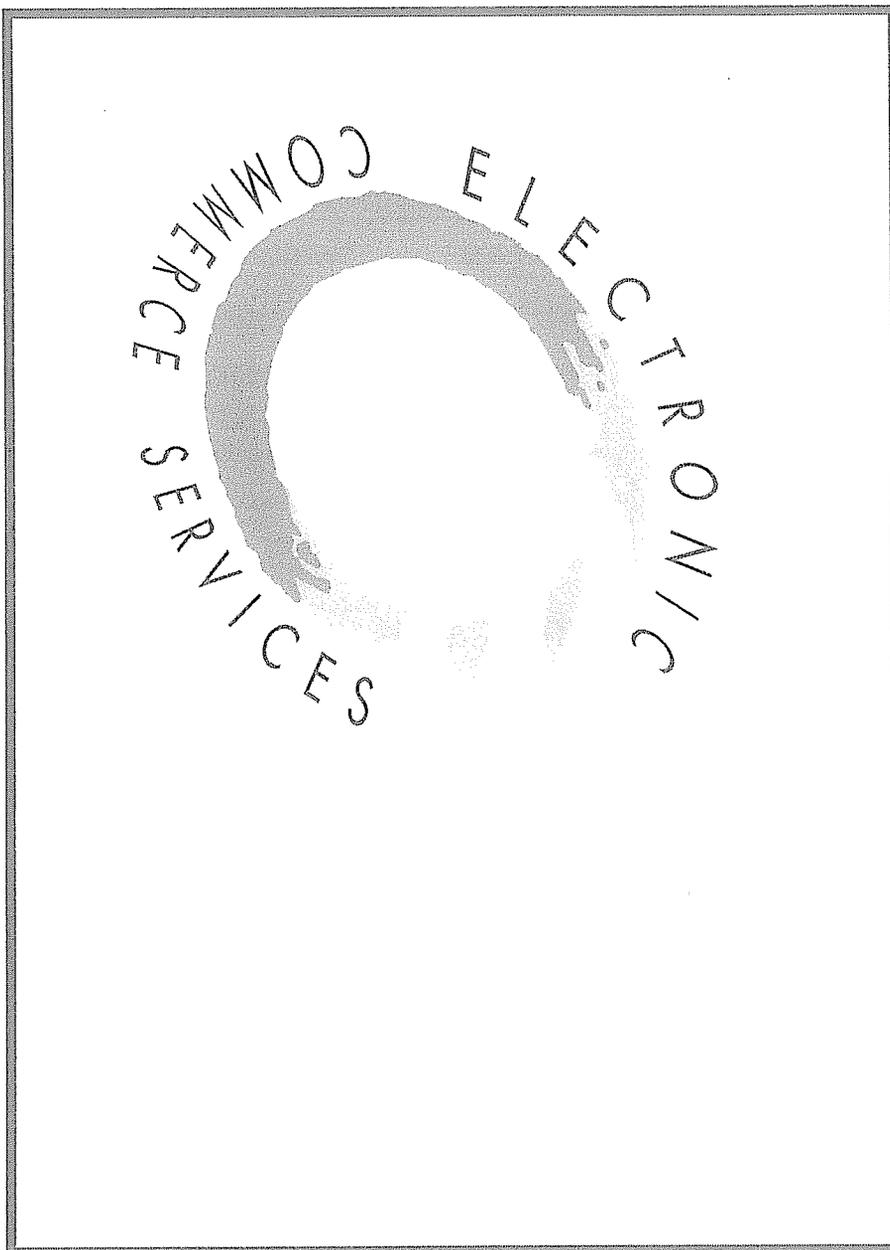


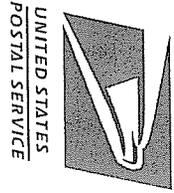


UNITED STATES POSTAL SERVICE

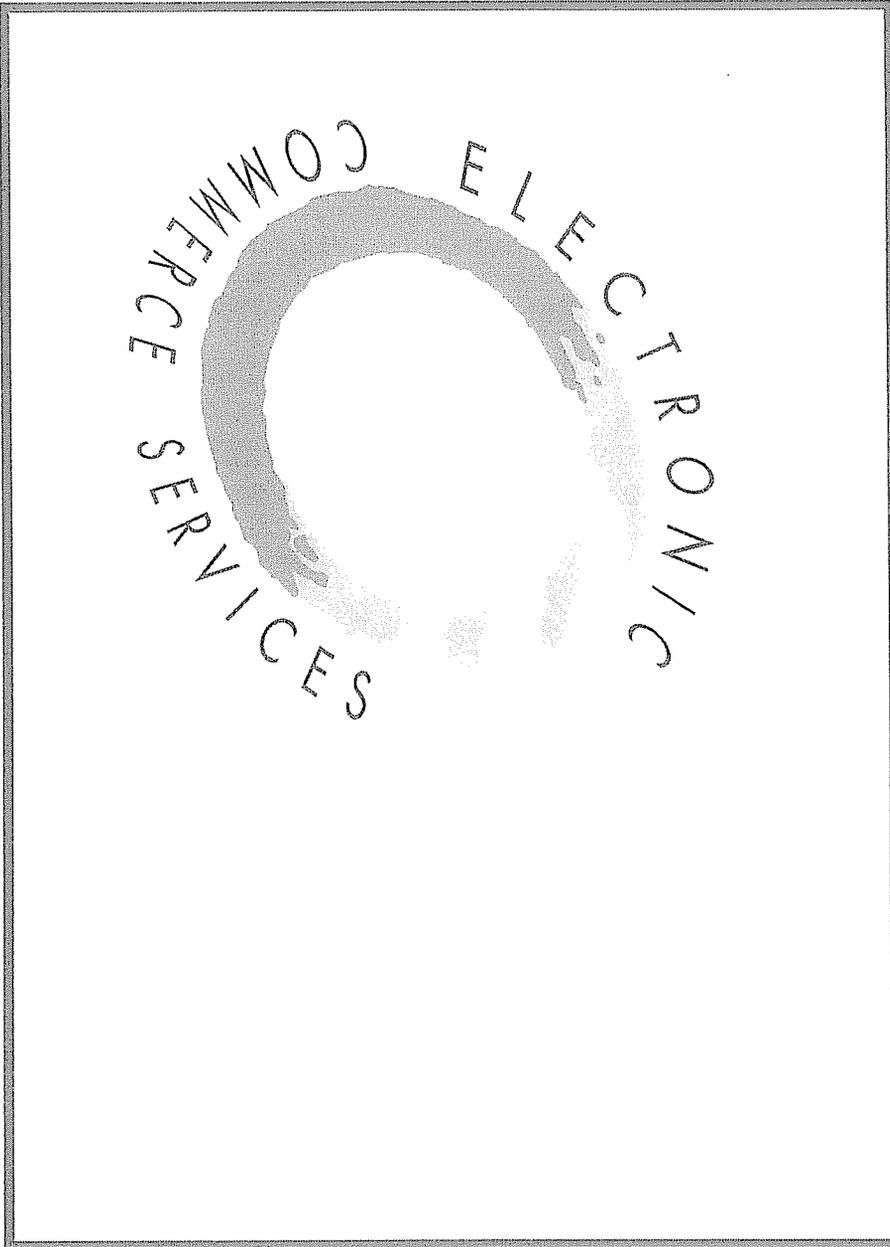


Time & Date Stamp

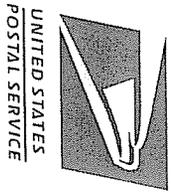




Easy To Use



Small vertical text on the left side of the page, likely a page number or reference code.



Applications



Contracts



Notarized Documents

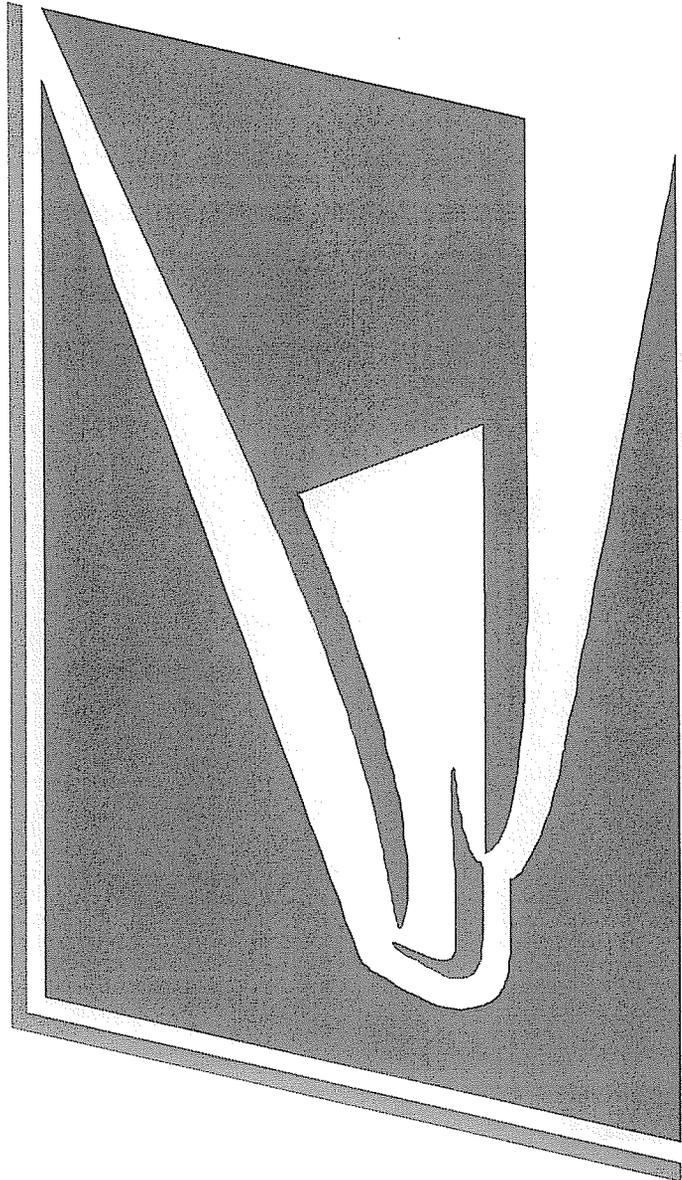


Purchase Orders

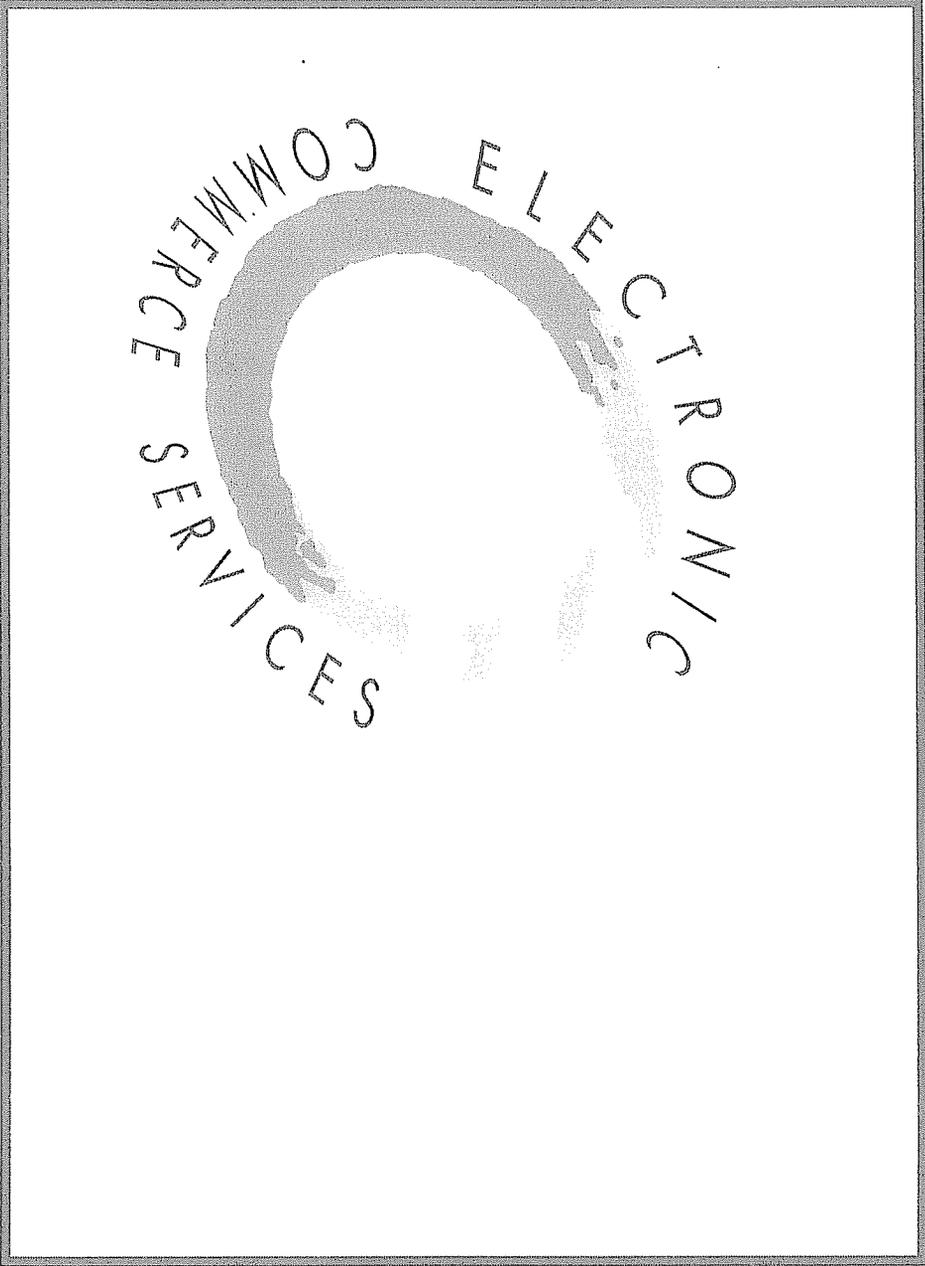
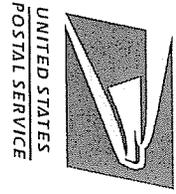


Medical Records

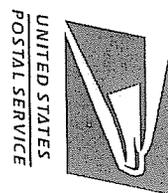
Billing Information



UNITED STATES
POSTAL SERVICE



UNITED STATES POSTAL SERVICE
1450 K STREET, N.W.
WASHINGTON, D.C. 20504
PH: 202-268-2000
WWW.USPS.COM

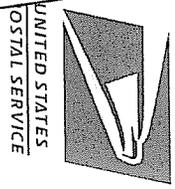


SECURITY

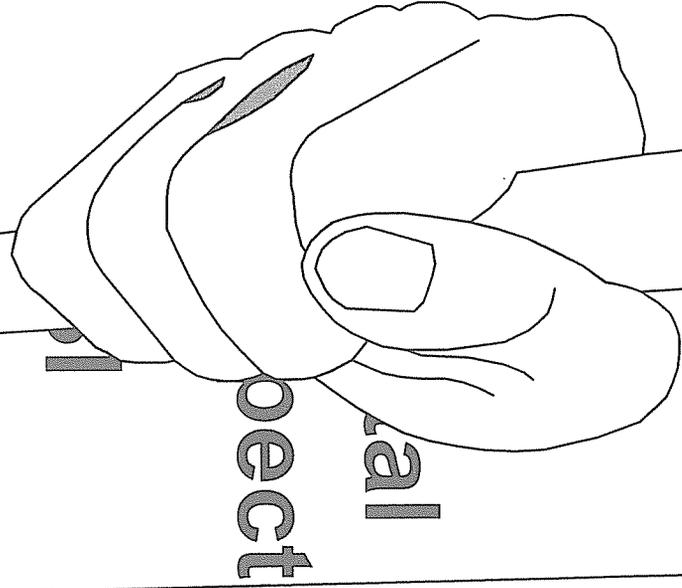
Postal

Inspectors

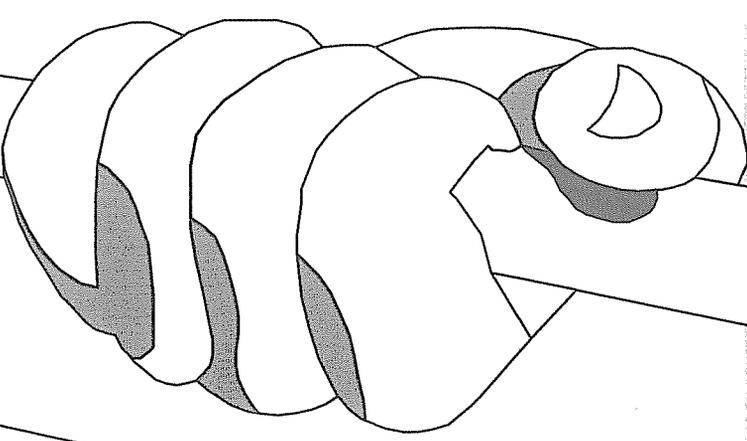
FBI

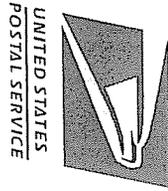


SECURITY

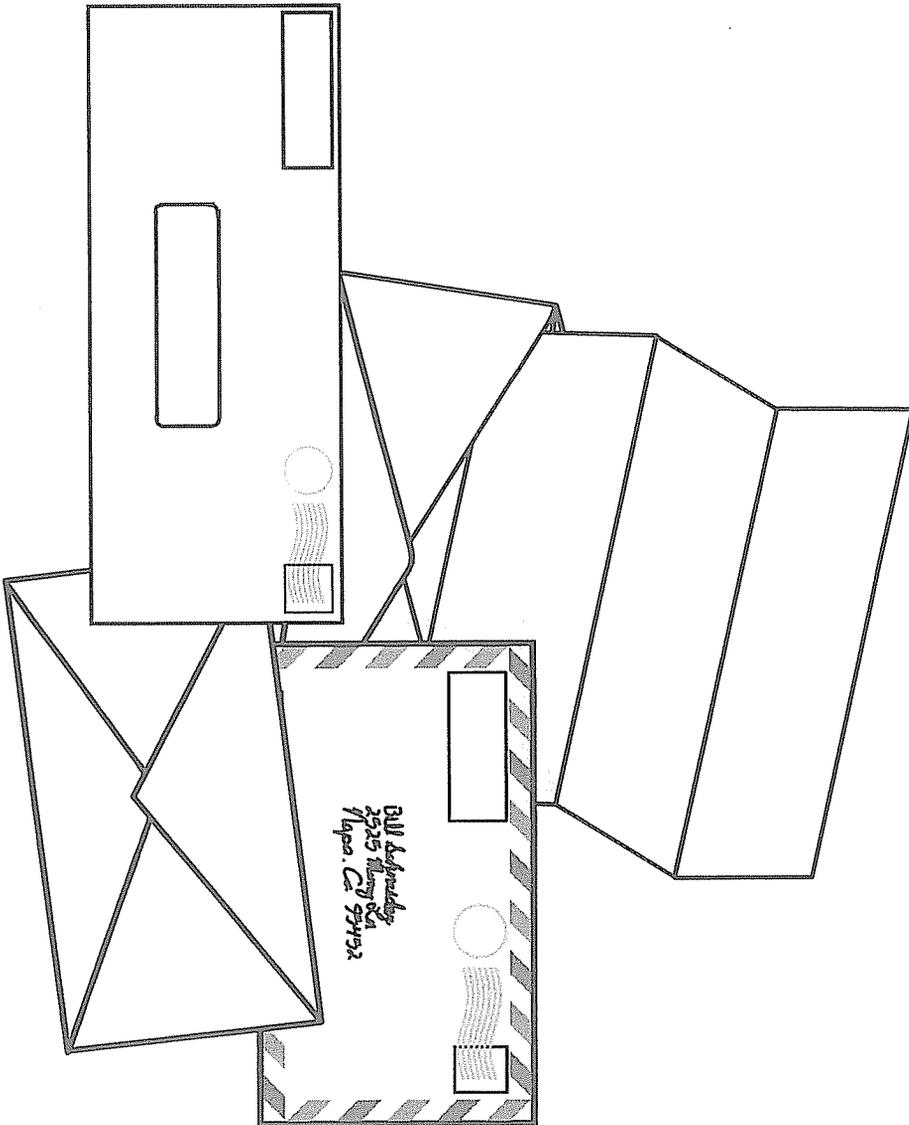


Project
Final
S





TECHNOLOGY



**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-15. Please provide copies of materials and exhibits used at all “eCommerce’ trade shows” (USPS-T-1-6, l. 15 – 17).

RESPONSE

To my knowledge, this material no longer exists.

RESPONSE OF POSTAL SERVICE WITNESS FOTI TO INTERROGATORIES OF THE OCA

OCA/USPS-RT1-16. Please provide all communications from the Postal Service to hundreds of companies and organizations describing Electronic Postmark (EPM)'s functions and how EPM might be applied to their specific needs (USPS-T-1 at 7, I. 1 – 3). (Identifying information may be redacted. However, please indicate the type of work the company or organization performs).

RESPONSE

To my knowledge, most of the communication was done through informal channels, such as through conversations and business card exchanges at trade shows. From available materials, I can tell the following.

At the 1996 Boston Trade show, contacts were made with approximately 500 people. In many instances, it is not possible to tell directly from the company or organization name (which is all we have) what type of work the company or organization performs. Based on what can be discerned from the more recognizable names, however, the types of outfits represented include computer companies, consulting companies, financial sector companies, telecommunications companies, public utilities, federal agencies, state and local governments, higher educational institutions, nonprofit organizations, manufacturing companies, technology companies, and members of the media.

At the 1996 Chicago Trade Show, contacts were made with approximately 720 people. In addition to the types represented at the Boston Trade Show, other types included insurance companies, health care companies, and publishing companies.

At the 1996 EMA Conference, contacts were made with approximately 60 people. In addition to the above types, petroleum companies were also represented.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

At the 1997 San Jose conference, contacts were made with approximately 540 people.

In addition to the above types, aviation companies were also represented.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-17. Please provide all communications from the Postal Service to “dozens . . . of IT developers” describing Electronic Postmark (EPM)’s functions and how EPM might be utilized by their customers (USPS-T-1 at 7, l. 4 – 6). (Identifying information may be redacted. However, please indicate the type of work the company or organization performs).

RESPONSE

Attached is a request for information for IT services. To my knowledge, the majority of this communication was done through phone conversations. It is believed that many of these people or companies potentially could be those whose contacts at trade shows are referenced in response to your question 16.

ATTACHMENT TO RESPONSE, OCA/USPS-RT-17

[Commerce Business Daily: Posted April 25, 1997]
[Printed Issue Date: April 29, 1997]
From the Commerce Business Daily Online via GPO Access
[cbdnet.access.gpo.gov]

PART: U.S. GOVERNMENT PROCUREMENTS

SUBPART: SERVICES

CLASSCOD: D--Information Technology Services, including Telecommunication
Services--Potential Sources Sought

OFFADD: U.S. Postal Service, Headquarters Purchasing, Room 4541,
475 L'Enfant Plaza, SW., Washington, DC 20260-6230

SUBJECT: D--**ELECTRONIC POSTMARK SERVICES**

SOL N/A

DUE 051297

POC Booker Weaver (202) 268-5669

DESC: As a part of a strategy to expand the range of systems that could incorporate the USPS' postmarking code (enabling privacy, tamper detection/prevention, and official time/date stamp), the United States Postal Service (USPS) is seeking qualified firms that currently offer either an Internet based email service, a Web-based **electronic** document transmission service, and/or an archival service (which may be web or email-based). The USPS is seeking responses from only those firms that are currently operating such a service, so that we might explore with them the feasibility of adapting these systems to accommodate the USPS' software code to **postmark** email messages, **electronic** document transmissions, attachments, and files/documents messages in and out of, an **electronic** archive. We encourage responses from vendors who have the ability to pass messages as generic ASCII text and/or Web based HTML, RFT, PDF, or other industry standard messaging formats. We are not seeking responses from software and/or hardware firms, unless these firms are currently offering a service such as described above. If you are unsure as to whether your current service can integrate with our software, please submit your credentials. All submittals should include the following: a description of the services you are currently offering, with flow diagrams (or other graphics aids) showing how the system routes mail/messages; a short history of how long the system has been operating, and how many iterations it has gone through; whether customers are currently using it, how many, etc.; a brief description of your current pricing/rate schedules; a description of the physical processing facilities you currently are using; and a description of your system features; and corporate qualifications. In the corporate qualifications section please identify and provide the following: 1) A statement of the years of experience the company, as currently organized has had in delivering the required products or services, including a list of current contract with estimated completion dates, dollar values, purchasers, and telephone numbers of purchasers' representatives. 2) Whether you are privately funded; including references with length of service, average savings and checking balances; outstanding loans, type and limit of credit and the bank's rating of your company as a customer. 3) A description of the company's organization and capabilities, including brief biographies of key personnel, expertise in marketing and business development within your respective industry, staff available for the specific project or projects, project control systems, manpower and equipment resources, and current physical locations and places of business. If your company is interested in being considered for participation, should a solicitation be

ATTACHMENT TO RESPONSE, OCA/USPS-RT-17

issued, you should submit the requested written information NOT LATER THAN MAY 12,1997. In addition to the requested information, your cover letter must include company name, address, telephone number, federal tax ID number, name(s) of the contact person(s), signature by an officer of the company, and sufficient information to enable the U. S. Postal Service determine if your company is qualified to perform. You should also identify whether your company is large, small, women or minority owned. Responses should be sent to Booker Weaver, Room 4541, 475 L'Enfant Plaza, SW., Washington, DC 20260-6238. There will be no other announcement for this requirement. THIS IS NOT A SOLICITATION. U.S. POSTAL SERVICE, 475 L'ENFANT PLAZA, SW, ROOM 4541,WASHINGTON, DC (202) 268-5669.

CITE: (W-115 SN066361)

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-18. Please provide all communications from the Postal Service to Microsoft, IBM, Lotus, Digital, Hewlett-Packard, Verisign, eTRade, and Entrust describing EPM's functions and how Electronic Postmark (EPM) might be applied to their specific needs or the needs of their customers (USPS-T-1 at 7, l. 1 – 3).

RESPONSE

To my knowledge, this material no longer exists.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-19. Please provide all communications from the Postal Service to “a dozen top law firms” describing Electronic Postmark (EPM)’s functions and how EPM might be utilized by their customers (USPS-T-1 at 7, l. 9). (Identifying information may be redacted. However, please indicate the type of work the company or organization performs).

RESPONSE

To my knowledge, these communications no longer exist. The firms were engaged in the general practice of law.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-20. Please provide all communications from the Postal Service to “the EDI community” describing Electronic Postmark (EPM)’s functions and how EPM might be utilized by their customers (USPS-T-1 at 7, l. 9). (Identifying information may be redacted. However, please indicate the type of work the company or organization performs).

RESPONSE

To my knowledge, these communications no longer exists.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-21. Please provide all communications from the Postal Service to each of the "host of government agencies" describing Electronic Postmark (EPM)'s functions and how each agency might utilize EPM (USPS-T-1 at 7, l. 9).

RESPONSE

To my knowledge, this communications no longer exists.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-22. Please list the “two dozen active participants in this sector” (USPS-T-1 at 7, l. 20- 21).

RESPONSE

An internet search would indicate many companies in this sector. The Postal Service’s internal list may be viewed as subjective.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-23. Please provide a copy of the October 2001 Request for Information (RFI) published in the Commerce Business Daily concerning Electronic Postmark (EPM) (USPS-T-1 at 10, l. 10 -12).

- a. How many companies responded?
- b. Which companies responded?
- c. Why did the Postal Service choose Authentidate?
- d. What were the reasons for not choosing the other applicants?

RESPONSE

Attached is the October 2001 RFI.

a. Four

b-d. Objection filed.

ATTACHMENT TO RESPONSE, OCA/USPS-RT-23

[Commerce Business Daily: Posted in CBDNet on October 17, 2001]

[Printed Issue Date: October 19, 2001]

From the Commerce Business Daily Online via GPO Access

[cbdnet.access.gpo.gov]

PART: U.S. GOVERNMENT PROCUREMENTS

SUBPART: SERVICES

CLASSCOD: D--Information Technology Services, including Telecommunication Services--Potential Sources Sought

OFFADD: United States Postal Service, Supplies and Services Purchasing, Alliance and Innovations Group, Room 4541, 475 L'Enfant Plaza SW, Washington, DC, 20260-6230

SUBJECT: D--USPS **ELECTRONIC** POST MARK ALLIANCE OPPORTUNITY ANNOUNCEMENT

SOL 106590-001

DUE 110701

POC Mark Guilfoil, Manager, Alliance & Innovations, Headquarters

Purchasing, Phone 202-268-8951, Fax 202-268-3677, Email mguilfoil@email.usps.gov

DESC: United States Postal Service T&DS / EPM Alliance Opportunity

Announcement. This notice serves as public announcement that the United States Postal Service (USPS) is commencing a business alliance process focused in the product area of Time and Date Stamp (T&DS) Technology. The USPS is seeking firms with existing T&DS technology solutions to extend the functionality or offer an alternative to our current USPS **Electronic Postmark?** (EPM) service. Interested parties may obtain detailed information concerning our current USPS EPM at www.usps.com and searching under EP M. Such a developed solution might include additional functional components of **electronic** mail (email) software for electronic content delivery, Internet service for business or home consumers, or other developed Internet services or products. USPS customers confidently count on the delivery of secure correspondence through our traditional paper mail systems. Today the USPS is expanding this same trust and security in the **electronic** world. Our USPS EPM has been targeted to address Internet security and privacy concerns while supporting the USPS in our trusted third-party status and brand name. The specific USPS business purpose of the initiative announced herein is to mutually expand both a USPS product and the supplier's service to provide and/or complement authentication, privacy, and non-repudiation of **electronic** content delivery. Suppliers should note that this announcement and its next steps will not result in a request for proposal (RFP), but rather initiation of alliance activities which may result in the identification and implementation of a contractual relationship with an alliance partner. The USPS alliance process is not equivalent to a procurement process, and will not be conducted under the USPS Purchasing Manual. If you have questions about the T&DS / EPM alliance process, please contact Mr. Mark A. Guilfoil, Headquarters Purchasing, Alliance and Innovations Group, 475 L'Enfant Plaza, Washington, D.C. 20260-6230, Tel: (202) 268-8951. The USPS anticipates a two phased technology review process consisting of a pilot test, and if successful, market implementation with a selected alliance partner. Should an internal pilot phase successfully demonstrate commercial viability and a clear potential for mutual financial benefit, the USPS would expect to proceed with alliance discussions with the identified supplier. Any resulting alliance instrument would provide for a nonexclusive business relationship which would require mutual risks and rewards, including revenue sharing of the jointly offered product(s) or service(s). If your firm is interested

ATTACHMENT TO RESPONSE, OCA/USPS-RT-23

in participating in this T&DS alliance selection process with the USPS, please provide information concerning your product, service, and business. Respondents should state how their product(s) or service(s) would enhance the USPS EPM?. Additionally, the following list of criteria should be addressed for purposes of USPS review of organizational compatibility and strength. These criteria will form the basis for further discussions and issuance of a Request for Information (RFI) to identified participants. Criterion #1; Demonstration of an existing product solution, current usage, and market potential. #2; Information concerning corporate history, current customer base, and product deployment. #3; Brief introductory discussion of the applicable technology platform, and how it meets emerging Internet Engineering Task Force (IETF) Standards for Date/Time Stamps. #4; Provide product history, number of customers, average number of transactions per day, and plans for future enhancements and releases. #5; Discuss number of dedicated staff for your product. #6; Describe the competitive advantages your company and current product(s) can provide to the USPS vis-à-vis other competitors. This should include a discussion on speed to market and short/long term solutions. #7; Show security standards in use and any assessment concerning penetration testing. Submissions should be limited to 30 pages and provided to Ms. Priscilla A. Hicks, EPM Program Manager, E-Business Technology Solutions, Room 2140, L'Enfant Plaza S.W., Washington, D.C. 20260-1530 no later than 2:30 p.m. on November 7, 2001. One original and two copies of all materials submitted are requested.

LINKURL: <http://www.eps.gov/spg/USPS/SSP/AIHQ/106590-001/listing.html>

LINKDESC: Visit this URL for the latest information about this notice

CITE: (A-290 SN510876)

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-24. Please provide the Strategic Alliance Agreement between the Postal Service and Authentidate (USPS-T-1 at 10, l. 15 -18).

RESPONSE

A copy of the Strategic Alliance Agreement, partly redacted for confidential commercial information, is available on the Securities and Exchange Commission EDGAR web site under ADAT documents (ADAT is the securities symbol for Authentidate).

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-25. Please provide the number of transactions that underlie the 97 percent figure set forth at USPS-T-1 at 11, l. 12 – 14. Break down the number given into the 10 most numerous types of usage, and rank these uses by amount of volume for the usage type.

RESPONSE

To provide this level of detail, an updated customer usage analysis was performed. The results of this analysis is based on the time period of mid-2002 through mid-2006. The total volume of USPS EPM used was over 3.1 million. Based on our understanding of how customers are using the USPS EPM, the results of this analysis show non-message application exceeding 99 percent. Below is break-out the most common applications of the USPS EPM:

	<u>% of EPMs Used</u>
Non-Messaging_Applications	
Authenticating doctors' orders	85%
Auditing archived records	10%
Signing medical necessity forms	2%
Certifying drivers records	2%
Other	<1%
Potential Message Applications	<1%

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-26. Please refer to your testimony at 11, l. 16 -22. You mention the use of a fax at line 19.

- a. Does the "largest customer" ("A") send the referenced fax to itself?
- b. Or to another entity ("B")?
- c. What is the nature of A's business?
- d. If the fax is sent to a different entity, what is the nature of the recipient's business ("B")?
- e. What kind of information is contained in the fax?
- f. Before the availability of Electronic Postmark (EPM) and like services, how did A transmit the information contained in the fax to B?
 - i. Was mail a suitable means of transmitting the contents of the fax from A to B? If not, please explain.
 - ii. Are you aware of businesses such as A today sending information such as that contained in the fax to recipients such as B? If not, please explain.
 - iii. Are you aware of businesses such as A sending information such as that contained in the fax to recipients such as B prior to the availability of EPM and like services? If not, please explain.
- g. If A preferred to use hardcopy mail, could it print the fax (or the information contained in the fax), put it in an envelope, and mail it to B? If not, why not?

RESPONSE

a.-g. This customer referenced (and referred to as "A") in this set of questions does not send a fax. This customer receives a doctor's order (or prescription) via fax. Upon receipt of the electronic document, the file is presented to the USPS EPM Server for authentication through a customized application which was developed and integrated into the customer's business process. After authentication of the document, the customer's fulfillment process, including billing, can be initiated. Prior to integrating the customized application with USPS EPM functionality, I believe the customer's business process was that it received the fax and directly processed the order without authentication. Due to the urgency to get the product to the patient, using mail for this purpose generally is not considered suitable.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-27. An example of a “second customer’s” use of Electronic Postmark (EPM) is given at page 12 of your testimony at lines 1 – 4.

- a. What is the nature of the customer’s business?
- b. Will the Worker Compensation claim forms be sent to another entity or entities? If so, what is the nature of the other entities?
- c. Before the availability of EPM, did businesses like this (i.e., the “second customer’s” business) often use mail to achieve what is now done through EPM? If not, why not?
- d. Would hardcopy mail be a good substitute for the second customer’s use of EPM? If not, why not? How could the second customer use mail to achieve comparable results?
- e. For the doctor example set forth at page 12, l. 6 – 11, you emphasize that the doctors “keep this record” and “don’t forward it to anyone.” However, you do not make the same claim for the second customer. Is that because the second customer does forward the Worker Compensation forms to another entity? If not, then please explain.

RESPONSE

- a. The customer's business is a Managed Care Utilization Review Office
- b. Yes - A third-party administrator
- c. I ’m not clear on what is meant by saying “done through EPM,” but I do not know how businesses like these previously authenticated electronic files.
- D . No. The EPM provides third-party authentication of electronic files.
- e. Yes.

**RESPONSE OF POSTAL SERVICE WITNESS FOTI
TO INTERROGATORIES OF THE OCA**

OCA/USPS-RT1-28. Please refer to the 3 examples set forth on page 12 of your testimony. Isn't it correct that businesses that want to prove they have not altered a document could print the document, seal it in an envelope, address to themselves, have it postmarked by mailing it, and keep the unopened envelope as proof that the document contained in the envelope had not been modified since the time of mailing?

a. If not, why not?

b. Are you aware of current examples of such mail use? If so, please describe your understanding of this practice.

c. Are you aware of past examples of such mail use? If so, please describe your understanding of this practice.

RESPONSE

a.-c. I am familiar with anecdotes suggesting the process you describe as a means by which aspiring writers, inventors, and the like could prove the existence of their written work product at a given date. I am personally unaware of any previous or current attempts to use this procedure, or, if there were any, whether this process was viewed as satisfactory proof of anything. While this procedure conceivably could work for an individual with the need to "postmark" a relatively few pieces of work, it would seem totally unacceptable for any business with a significant volume of transactions to document. Not only would there be the problem of storing and retrieving multiple copies, but the process may be viewed as susceptible to manipulation, and once the envelope is unsealed, the postmark can never again be used to prove anything.

CERTIFICATE OF SERVICE

I hereby certify that I have this date served the foregoing document in accordance with Section 12 of the Rules of Practice and Procedure.

Eric P. Koetting

475 L'Enfant Plaza West, S.W.
Washington, D.C. 20260-1137
(202) 268-2992, FAX: -5402
August 4, 2006