



Simple, Secure Messaging: Eliminating Barriers to Customer Adoption

Contents

Executive Summary	3
Capsule History of Secure Messaging Approaches	3
S/MIME.....	4
Public Key Infrastructure (PKI).....	4
Proprietary Push Solutions.....	4
Web-Based Pull Solutions.....	4
Optimal Characteristics of Secure Messaging	5
Flexibility of PostX Universal Transport	5
Extensive Cross-Platform Support	6
No Recipient Software Installation Needed	6
Using Electronic Postmarks for Verification	6
Universal Transport Delivery Methods	7
PostX Platform Interoperability	7
Case Study: Charles Schwab	7
Case Study: JP Morgan Chase	8
Confronting E-mail Fraud	9
Quantifying the Identity Theft Problem.....	9
Combating the Problem.....	9
Choosing a Successful Approach	10
Conclusion	10

Executive Summary

Despite nearly a decade of effort to establish secure e-mail as a replacement for paper-based communication, businesses still tend to rely on physical delivery methods for exchanging sensitive information with customers, partners, and employees. The slow acceptance of secure e-mail within enterprises is less a factor of poor technologies and products than the result of individual approaches that often fail to achieve a balance between secure communication and ease of use.

As additional threats of identity theft and fraudulent e-mail attacks challenge the industry, promising technologies and advanced strategies offer real-world answers to successfully meet the twin challenges of secure data delivery and authentication.

This paper traces the evolution of secure messaging, illuminates the factors that make certain approaches viable, provides case studies, and presents the PostX Trusted E-Business solution as a model for simple, secure messaging.

Capsule History of Secure Messaging Approaches

E-mail offers the potential to move a giant step closer to the promise of the efficient paperless office. However, there is one enormous drawback—security. Sending business communications by conventional e-mail is akin to putting sensitive information on a postcard and dropping it in a mailbox. Just as anyone can read the contents of a freely circulated postcard, a variety of techniques exist to identify and extract the contents of messages transferred through packets on the Internet.

Savvy IT security professionals have known for years that encryption, when properly applied, can ensure the privacy of message transfer. Although tools and technologies to encrypt e-mail messages are readily available, widespread adoption by businesses has lagged because of a number of obstacles. Until recently, US intelligence gathering and law enforcement agencies have opposed widespread use of encryption, fearing that criminal elements would take advantage of private message transfer to evade detection. In a substantial turnabout, as more government agencies and large enterprises in the financial sector have begun to rely on e-mail communication, legislation mandating privacy has made encryption both necessary and desirable.

Early efforts to apply encryption to large-scale e-mail communication ran into another barrier—processing power. The algorithms required to encrypt hundreds or thousands of messages a day place a substantial burden on enterprise servers. Encrypting and decrypting message streams at enterprise volumes demands very expensive, high-performance servers to keep operations from slowing to a crawl during peak message periods.

Today's high-performance commodity servers feature processors with capabilities that rival supercomputers of years past and functionality that accelerates processing of the algorithms that perform encryption and decryption. The architectural model for business computing has evolved from a monolithic to a distributed approach, where computing proxies perform many of the key tasks, shifting the burden away from a single processor. Complex tasks, such as those required for encryption, can be accomplished with greater efficiency within the enterprise workflow.

Another issue that has impeded widespread adoption of secure e-mail is authentication. Without a definitive means for identifying the sender of a message, the potential for fraud is significant. Many of the approaches to authentication have involved cumbersome technologies that burden both the senders and recipients of messages, discouraging widespread use. While authentication is indisputably necessary if e-mail is to continue to make inroads in today's security-conscious business world, the authentication method must fit comfortably within the realm of normal business operations if it is to be accepted.

Given this history and framework, a number of companies have created proprietary products and standards-based solutions designed to circumvent obstacles while protecting privacy and ensuring the veracity of messages. These approaches have had varying degrees of success, as discussed in the following sections.

S/MIME

Secure Multi-Purpose Internet Mail Extensions (S/MIME) arose from the need to create a standards-based approach to sending secure e-mail. Currently being slated for adoption by the Internet Engineering Task Force (IETF), S/MIME uses the Rivest-Shamir-Adelman encryption system and employs the syntax defined by the Public-Key Cryptography Standard format number 7.

S/MIME includes mechanisms for delivering encrypted messages and authenticating senders through a single set of credentials. Instead of requiring a global encryption and authentication system deployed at the enterprise level, S/MIME sends secure individual e-mails to a limited number of recipients. S/MIME also addresses the issue of verifying message integrity. In practical use, however, S/MIME creates a number of complications and can be cumbersome to use. Interoperability problems reduce the effectiveness of this approach in cross-platform message exchanges.

Although S/MIME is built into current generation e-mail systems, such as those from Microsoft and Lotus, there is currently no way to use it with consumer-focused Web-based e-mail systems, such as those provided by Yahoo!, Hotmail, and America Online. These restrictions and the inherent complexities of S/MIME have resulted in limited adoption of this approach.

Public Key Infrastructure (PKI)

PKI—Public Key Infrastructure—provides a mechanism for users of an inherently insecure network, such as the Internet, to exchange messages securely by means of public and private cryptography keys. Although PKI's certificate-based approach is sound, it has limitations in enterprise environments. It was never designed to deal with today's volumes of data communication, the multiple types of computing devices in use, nor the IT requirements of enterprises that service hundreds or thousands of users.

Before message exchange can be completed using PKI, the client must locate the appropriate certificate for the recipient, a process made difficult by the lack of universal certificate directories. Certificates must be validated based on corporate-wide or personal policy decisions, which adds overhead to the process. Circulation of certificates, which contain sensitive information, represents a security risk. Secure

business communications must be conducted online; for the mobile workforce trying to perform useful work offline, access to message content is possible only by transporting a set of certificates. PKI offers security, but it does so at the cost of time, effort, and administrative overhead.

Proprietary Push Solutions

While offering fewer complexities than S/MIME, proprietary push solutions require software to be installed by the recipient. Although problems with certificates are eliminated, this approach has limited client support, both in terms of operating systems and e-mail platforms. The less-than-universal support and the somewhat cumbersome aspects of proprietary push solutions have limited their acceptance.

Proprietary push solutions require the use of unique, proprietary plug-ins that must be downloaded and installed by users in their e-mail clients. In many enterprise environments, security guidelines and administrative practices prohibit individual installations of software. These requirements make proprietary push solutions impractical for most IT organizations at the enterprise level.

Web-Based Pull Solutions

Secure e-mail and information access solutions based on Web browser access have a clear advantage—they can reach anyone on any platform with a Web browser. Any usability issues with this approach involve the message recipient. The Web host bears the burden of maintaining the storage resources and ensuring the bandwidth availability for the users accessing the system. Although it has advantages in some areas, the Web-based pull solution has made limited penetration in the market for business users.

In circumstances where a financial institution or similar enterprise delivers information with Web-based pull techniques, high-volume bandwidth demands at particular times of the day may result in slow response or error messages from the Web host. Load-balancing techniques and other approaches can minimize these problems, but ensuring unfettered access to system information can still be challenging for IT organizations.

Optimal Characteristics of Secure Messaging

To meet the needs of security-conscious enterprises, the optimal secure messaging solution should fulfill these requirements:

- **Simplified requirements for the message recipient:** The solution should require no additional software installation for the recipient. It should reach virtually 100 percent of users and be convenient and easy to use.
- **Streamlined sender requirements:** From the perspective of the sender, an optimal secure messaging system should be easy to deploy and maintain. It should also support the vast majority of message types.
- **Flexible options for security and authentication models:** To meet the requirements of the widest range of enterprises, the solution should provide choices in the security and authentication techniques used. The selected approach should be easily integrated into the existing IT infrastructure, using those proven components already in use within the enterprise.
- **Scalable to meet enterprise growth:** The solution must be adaptable to the increasing demands and transaction volumes that are associated with enterprise growth. As the user base increases, the system should not exhibit significant performance reduction or diminished information availability.
- **Minimal limitations to deployment and use:** First-generation messaging platforms typically present numerous restrictions in terms of transports, supported e-mail clients, and other factors. However, second-generation approaches offer much more flexibility, more operating systems are supported, integration with middleware components is more flexible, and hardware requirements for the messaging system are more open. Mechanisms for sending messages are also more open, encompassing Web delivery, S/MIME, and other methods of push and pull delivery. In general, second-generation messaging platforms are more suitable for wide scale enterprise use, with more flexibility and better integration into existing systems.

Flexibility of PostX Universal Transport

To meet the dual challenges of flexible integration and ease of deployment, the PostX Universal Transport, a component of the PostX Trusted E-Business solution, provides a wide choice of secure messaging delivery approaches that enable straightforward and rapid implementation. Recipient usability and satisfaction are the top priorities of these approaches, which feature several patented innovations.

The PostX Universal Transport provides options for security architecture, the user interface, and delivery requirements. Delivery options should be selected based on the overall security consideration and the needs of the recipient.

	Considerations	Delivery Options
Security	What type of security will be used to protect documents and messages?	<ul style="list-style-type: none"> • Symmetric (using passwords or hardened keys) • Asymmetric (using PKI)
Delivery Model	Will documents be delivered by means of e-mail or will notification URL's be sent instead?	<ul style="list-style-type: none"> • Push (using PostX Envelopes or S/MIME) • Pull (using WebSafe)
Usability	Which message viewing requirements will have priority?	<ul style="list-style-type: none"> • Opening offline • Opening online
Message Integrity	Should options to ensure message integrity, such as date/time verification, tamper detection, and legal protection, be implemented?	<ul style="list-style-type: none"> • US Postal Service Electronic Post Mark (USPS EPM) • Enterprise Postmark

	Considerations	Delivery Options
Customer Service	How will users retrieve keys for PostX Offline Envelopes after password changes?	<ul style="list-style-type: none"> • Fallback Key Retrieval™ • Ad-hoc message resend capabilities

PostX Universal Transport lets enterprises match security and usability requirements to the appropriate messaging methodologies. With a unified recipient-side architecture, PostX presents a simple interface for e-mail recipients to authenticate and decrypt their messages. The primary objective of PostX Universal Transport is to ensure a consistent and rewarding user experience, regardless of the complexities associated with the underlying security model. To provide a consistent framework, the PostX Offline Envelope (providing password-based encryption) uses the same user interface as the PostX Registered Envelope (using online authentication).

All PostX Universal Transport methods draw upon field-proven, audited encryption principles and techniques. Ultimately, the simplicity of the end-user experience masks the complexity and variety of secure delivery methods employed to support the secure messaging experience. This approach eliminates significant barriers to the adoption of secure messaging, creating a seamless framework to support the mass deployment of secure messaging applications.

Extensive Cross-Platform Support

Enterprises recognize that e-mail users rely on a wide variety of Web-based and desktop e-mail applications. Any viable secure messaging solution requires robust cross-platform compatibility. PostX Universal Transport's server-side and recipient-side technologies are designed from their cores to work in all major distributed IT environments. The delivery technology is entirely e-mail client- and platform-agnostic. This ensures that a message sent to a Windows user will work as flawlessly as one sent to a Mac or Linux user, and will work equally well on AOL, Outlook, Lotus Notes, Yahoo! Mail, or Microsoft Hotmail. The sender does not need advance knowledge of the e-mail client, which greatly simplifies the secure messaging application. PostX Universal Transport methods make secure messaging work as simply as normal e-mail. The

approach used does not require any advance knowledge of what type of system the message recipient is using.

No Recipient Software Installation Needed

The PostX Universal Transport solutions embrace a model that eliminates the need for software to be installed on the recipient desktop. This design requirement was driven by the following market realities:

- Enterprises are not in the business of software distribution and/or software support. Consumers do not want to install software to conduct business.
- Software installation typically requires administrative rights. More and more organizations prevent their employees from installing software on their machines by not giving them administrative rights.
- Software depends on the operating system, and, if e-mail client plug-ins are used, on the e-mail client. The matrix of operating systems, e-mail clients, and versions in use can be so large and complex that the recipient software installation approach is difficult or impossible to deploy and support.

Using Electronic Postmarks for Verification

USPS Electronic Postmark

PostX offers the USPS Electronic Postmark (EPM) in conjunction with the US Postal Service. This technology provides complete message tamper-detection, an official USPS timestamp, and the guarantee of the USPS to investigate any fraud and to prosecute to the full extent of the law. These are powerful enterprise-level incentives to improve the security and credibility of e-mail messages.

PostX Universal Transport has the ability to generate EPMs and the built-in tools to enable both recipients and enterprises to verify the postmarks.

Enterprise Postmark

The Enterprise Postmark allows enterprises to generate postmarks using their own private key, thus providing detection of message tampering.

Universal Transport Delivery Methods

One of the underlying goals of the PostX architecture model is to provide transparent support for a variety of delivery methods and to minimize the complexities of each of these mechanisms. PostX Universal Transport supports these delivery methods:

- PostX Envelope™ (Push)
 - PostX Registered Envelope™
 - PostX Offline Envelope™
- B2B Standards-based S/MIME
- PostX WebSafe™ (Pull)

PostX Trusted E-Business integrates these delivery methods into the system architecture, reaching the widest possible audience by reducing restrictions on the methods chosen. Messages meeting specific criteria, from individual applications, or targeted to particular recipients can be sent through any one of the methods by means of messaging routing rules that dictate encryption algorithms and delivery methods.

PostX Platform Interoperability

PostX Trusted E-Business is based on the enterprise-class PostX Platform, which is a J2EE-compliant application that provides maximum flexibility of platform and application server selection. The PostX Platform integrates fluidly into any enterprise software environment to support the widest variety of secure messaging applications. The platform includes robust support for the SOAP protocol in order to leverage the various services that customers may have developed in a Microsoft .NET environment.

The PostX Platform currently supports the following platform options:

- Operating Systems
 - Solaris
 - Linux
 - Windows
 - AIX
- J2EE Application Servers
 - IBM WebSphere
 - BEA WebLogic
 - JBoss (an open source application server)
 - Database support (through Java Database Connectivity)
 - Oracle
 - IBM DB2
 - Microsoft SQL Server
 - MySQL

Case Study: Charles Schwab

Within the competitive financial services industry, Charles Schwab needed a way to differentiate their services. They wanted to increase customer satisfaction while controlling rising customer service costs, including the substantial costs associated with postal delivery of account statements. One clear objective was the creation of a system for the SchwabPlan that would let customers to receive their 401(k) information electronically.

Charles Schwab mapped out the parameters for an improved information delivery system that had to meet these criteria:

- Provide 100 percent reach to their customer base.
- Be accessible without the installation of additional client software.
- Support offline viewing.
- Deliver high-value content to customers.

Customers stated a preference for having information delivered directly to their computer desktops. They also wanted a means to download statements into financial management tools such as Microsoft Money and Quicken. Customers emphasized the need for simplicity—they did

not want to install special document viewers, deal with multiple passwords, or log on to retrieve their data.

Charles Schwab considered a variety of solutions. These included developing a Web site “pull” approach, creating a mechanism for pushing Adobe Acrobat documents to customers, and using the PostX activeSTATEMENTS component to deliver statements securely for offline viewing while maintaining image and print fidelity.

The selected solution, PostX activeSTATEMENTS, uses this sequence to provide data to customers:

- The system pulls 401(k) data from the internal Charles Schwab systems.
- The data is added to the print stream workflow.
- Additional relevant customer advice and fund ratings are retrieved from external data sources and used to supplement the 401(k) data.
- PostX activeSTATEMENTS generates a personalized, dynamic statement from the applicable data.
- The information, presented in Macromedia Flash format, is secured in a PostX envelope.
- PostX activeSTATEMENTS delivers an expanding interactive visual representation of the current statement for offline viewing. The system tracks and manages this delivery.

Through the use of PostX activeSTATEMENTS, Charles Schwab achieved significant savings in delivering personalized information to its customers while meeting strict security protocols. The net savings for each customer equals \$120 per year, with an additional profit of \$275 per year per customer. The secure delivery mechanism has been deployed within the existing IT infrastructure at Charles Schwab and requires very little maintenance or oversight.

The resulting system also met customer expectations. Customers can now receive statements through secure e-mail, whether they use a desktop client application or Web-based e-mail. The approach lets customers access information offline without having to download documents and with simplified, single sign-on access methods. The success of PostX activeSTATEMENTS has encouraged Charles Schwab

to pursue additional PostX solutions, including trade confirmations and other types of banking and brokerage statements.

Case Study: JP Morgan Chase

As an early adopter of Customer Relationship Management (CRM) technologies, JP Morgan Chase recognized the benefits of improving service transactions through automation. The increase in the number of online customers, however, presented a growing challenge, particularly as e-mail requests to customer service rose beyond 2-million messages per year. Many of these messages required responses that contained sensitive information, making it essential that the content be encrypted to meet current regulatory and compliance mandates. Without a secure messaging system in place, JP Morgan Chase had to rely on telephone contact to convey sensitive information, a costly and inefficient process.

Having invested heavily in their Kana CRM system, JP Morgan Chase needed an approach that could coordinate communication throughout six lines of business and integrate successfully with their enterprise infrastructure. Netegrity SiteMinder was being used as the access management tool and JP Morgan Chase required a single point of entry for management of the banking portal. The customer-facing portion of this system had to provide a single sign-on for ease of use, a comprehensive online message center, dynamic inquiry forms, and accurate routing of queries.

JP Morgan Chase considered the following solutions: developing an in-house implementation using IT department staff members; engaging a development firm to design a custom messaging system; and implementing PostX activeEnterprise.

JP Morgan Chase concluded that the most cost-efficient and comprehensive solution was PostX activeEnterprise. They opted to include the optional WebSafe™ component, which provides secure document retrieval through push and pull technology to support on-demand request from customers.

The deployment of PostX activeEnterprise successfully met or exceeded all compliance, privacy, and regulatory requirements for the industry. Customers gained the flexibility of having their requests met through telephone, postal mail service or secure e-mail. The efficiency of the call center increased because customer service representatives were able to focus on more personalized service. The PostX solution enables JP

Morgan Chase to provide timelier, better customer service while reducing the overall costs of its service operation.

Confronting E-mail Fraud

As described in the previous sections, the primary obstacles to the adoption of secure e-mail within enterprises can only be met by combining rigorous security with outstanding ease of use. This is the prevailing design approach incorporated in the PostX Trusted E-Business solution.

As one set of challenges is successfully addressed, however, another set emerges. Spoofing and phishing, two new forms of e-mail fraud, have become increasingly widespread. The nature of these threats makes it necessary for enterprises to deal with them forcefully and effectively.

Both spoofing and phishing are forms of identity theft. The stolen identity is that of the enterprise itself, and it affects any consumer who accepts the bait. In *spoofing*, the contents of an e-mail header are forged to make it appear that the e-mail came from a legitimate source, such as a bank or other institution. Spoofing encourages recipients to open and respond to a message they might otherwise ignore.

Phishing consists of attempting to obtain sensitive personal data, such as credit card numbers, by misdirecting a mail recipient to a fraudulent Web site. Using highly recognizable logos and replicating site characteristics (another form of spoofing), unwary consumers are urged to “update their personal information” or “verify their credit card numbers.” This information is then harvested and often used illegally.

Quantifying the Identity Theft Problem

According to the Federal Trade Commission, identity theft in all its forms results in \$50 billion in losses each year. The Public Interest Research Group (PIRG) calculated that occurrences of identity theft have increased by 500 percent in the past 3 years. In 2003, the amount of time devoted to resolving identity theft issues in the United States reached nearly 300 million hours. In the same year, various forms of identity theft affected nearly 10-million people in the U.S.

By all indicators, the problem is substantial and growing. No practical method of secure e-mail exchange implemented at the enterprise level

can ignore the risks of spoofing, phishing, and other forms of identity theft.

Combating the Problem

Authentication lies at the heart of the e-mail identity theft problem. Verifying both the sender of a particular e-mail message and the owner of an enterprise Web site is critical to eliminating the problem of identity theft. The approaches that have evolved include:

- **Enterprise Alerting Services:** These services monitor and detect fraudulent site operations, as well as illicit e-mail campaigns, and notify the enterprises being spoofed. Companies such as Brightmail, Cyota, Cyveillance, and Envisional offer this type of service. This early warning services help shut down illegal operations quickly, but cannot eliminate phishing or spoofing. The alerts are provided only to the enterprise involved—not the customers of the enterprise.
- **E-mail Verification:** PostX employs an e-mail verification system to combat e-mail fraud. This allows the e-mail gateway and client to verify whether a received message originated from a particular sender. The same framework that supports this approach can be expanded to encompass message privacy through encryption. This approach works with any e-mail client that supports it, but message recipients must be trained to look for the message validation.
- **Sender Validation:** This promising approach equips the e-mail gateway to determine whether a received message originated from the purported sender. America Online relies on DNS registration verification through Sender Policy Framework (SPF). Microsoft applies a caller-ID approach, also capitalizing on DNS registration. Two other techniques, IMAP from IETF and domain keys from Yahoo!, address the same issue, but there is no unified agreement within the industry as to which approach to use. The validation approach must be supported by the customer’s e-mail gateway and must provide a mechanism to indicate the status of individual messages. There are potential incompatibilities with e-mail forwarding services.
- **Web Site Verification:** Services offered by companies such as Passmark and Geotrust let customers determine whether a Web site is properly registered. For this approach to work,

customers must be trained to look for the validation and recognize the difference between an authentic validation and a spoofed validation. Since the approach is not proactive, it relies on customer knowledge to quantify the risks and it doesn't prevent spoofed e-mail forms.

Choosing a Successful Approach

The messaging approach most likely to gain industry traction will be the one that places the least deployment and maintenance burden on the enterprise while minimizing the inconvenience and involvement of the e-mail users. The mechanism for verifying e-mail senders and Web sites must embrace the widest range of platforms and offer a simple, direct means of relieving e-mail users and IT organizations from the responsibility of manually assessing the degree of risk.

PostX continues to refine its Trusted E-Business solution to address emerging threats and identity theft risks, offering approaches that ensure security without hampering daily enterprise operations.

As a board member of the Trusted Electronic Communications Forum (TECF), PostX works with knowledge leaders in industries such as retail, telecommunications, financial services, and online service providers to establish guidelines and best practices for trusted communication.

The goals of TECF include:

- Collaborating with industry participants to establish standard solutions to identity theft and electronic fraud
- Expanding educational campaigns related to online identity theft for improved consumer protection
- Promoting technologies and self-help options that help cope with the identity theft problem
- Distributing relevant information to alert consumers about emerging forms of identity theft
- Working closely with the Federal Trade Commission (FTC) to ensure that perpetrators of cyber crimes are punished

PostX offers a solution to the spoofing and phishing problem with a recently released product, PostX Trusted Dialog. Trusted Dialog gives e-mail users a mechanism for identifying fraudulent e-mail, and gives enterprises a way to protect the legitimacy of their brand. The unique

PostX technology authenticates and validates e-mail as a background process that does not unduly burden enterprise messaging systems. Each enterprise can attach distinct digital signatures to e-mail messages and then use the Web to distribute a plug-in that can be embedded in their e-mail system for certifying signed messages. This approach works for Web-based message systems, such as Yahoo!, and conventional message clients, such as Microsoft Outlook.

Conclusion

Acceptance of secure e-mail as part of everyday business workflow requires attention to well-understood risks, and recognition of emerging threats. Enterprises have many individual characteristics and requirements. The chosen approach to secure e-mail must be flexible, interoperable, scalable, and compatible with existing systems and standard business practices.

No company is willing to sacrifice the efficiency of business operations for security. Effective security measures must fit within the realm of mainstream workflow without burdening e-mail users or the IT staff members who implement and maintain the system. The PostX Trusted E-Business solution embraces these requirements and offers an approach that can be flexibly adapted to a wide range of businesses—ensuring the benefits of secure messaging in an efficient, cost-effective manner.



Copyright © 2004 PostX Corporation

All Rights Reserved

PostX Envelope, PostX Registered Envelope, PostX Offline Envelope, and PostX WebSafe are trademarks of PostX Corporation. All other brands, product names, company names, trademarks, and service names are the properties of their respective holders.

PostX Corporation

3 Results Way

Cupertino, CA 95014

U.S.A.