

Policy-Based Email Encryption now Easier and More Affordable

INTRODUCTION

As email has evolved into a common—and mission critical—communications tool, so has the value of the information and transactions conveyed by email and the threats to its extensive use. The “open” nature of email messages that helped propel its universal interoperability also makes these messages vulnerable to interception, viewing and even altering by parties other than the sender and recipient. Often compared with “sending a postcard through the mail,” email messages have not typically been secured in their transfer over the Internet. Yet, in a time when identity theft, industrial espionage and privacy concerns dominate the headlines, securing email messages has become more important than ever before.

As the risks to the privacy and security of email communications have grown, so have efforts to protect it. Highly sensitive government communications initially helped to spur efforts to secure email messages through encryption. Encryption involves highly complex mathematical algorithms that scramble messages before they are sent over the Internet, and then unscramble them once they are delivered to the recipient.

Email is encrypted by the sender's email program, which makes it unreadable until it is de-scrambled or decrypted by its intended recipient. If an unencrypted email message is like a “postcard”, then an encrypted message is like a sealed envelope which can't be viewed until its rightful recipient opens it.

Over the past several years, various individuals and companies have developed proprietary encryption methods, and the means to implement them. Standards such as PKI, S/MIME, and OpenPGP were developed to enable organizations to secure their emails, but at a relatively high cost in time, effort and expense, and often with unpredictable results.

EMAIL ENCRYPTION EARNS REPUTATION AS COMPLEX, COSTLY AND CUMBERSOME

While many email clients, such as Microsoft Outlook, allow senders and receivers to encrypt and decrypt email, to do so requires a PKI or Public Key Infrastructure that uses digital certificates to authorize individuals to send and receive encrypted messages. But as one reviewer of PKI alternatives for secure messaging noted, “For the enterprise, trying to create, distribute, and maintain digital certificates for large numbers of users isn't very practical. Try to extend the PKI to outside business partners, and the problem only gets worse.”⁽¹⁾

Because the market offers a virtual alphabet soup of PKI vendors and encryption protocols (OpenPGP, IBE, S/MIME), the implementation of PKI infrastructure is a complex task for any enterprise to undertake, often costing hundreds of thousands of dollars. Third party PKI vendors offer desktop-to-desktop encryption, for example, based on public key technology that requires users to manage keys, certificates and extra passwords. Analysts at one major research firm, however, note that their application remains limited because of

the difficulty in managing desktop configurations, and the inherent complications of managing public/private keys.⁽²⁾

Thus, encryption using these methods has not gained widespread usage for several reasons.

- **Complexity:** Most current encryption methods are complicated and cumbersome to use because of multiple standards and multiple proprietary solutions/gateways, and desktops. Several steps on the part of both sender and receiver may be required to secure a message. Both sender and receiver need to be authenticated which may require software not only on host, but on desktop and mobile computer systems.
- **Cost:** Proprietary systems available were developed at considerable expense and are priced accordingly. Licensing costs and administrative overhead to maintain desktop systems have meant only the most sensitive communications would justify the expense. In many cases this is priced outside the reach of the small business.
- **Scale:** In many cases these encryption methods do not scale to today's large, highly diverse computing environments. Keeping every component of a secure messaging system in sync and up-to-date for just a few hundred users creates an administrative nightmare not to mention what it would require for organizations with tens of thousands of users.

Experts debate the strength of encryption delivered by PKI technology vendors, and product/vendor reviews go into great detail trying to explain the different techniques. For the vast majority of companies, however, seeking to secure email communications—especially those in healthcare and financial services—the difficulties and costs of implementing PKI often outweigh the benefits. Because traditional encryption methods are so complex and costly, requiring extensive user education and technical support, few organizations can afford to implement and maintain them.

WHY EMAIL ENCRYPTION NOW?

As new regulations and compliance issues have moved front and center more organizations than ever are seeking to secure their messages: to avoid legal penalties, meet the requirements of their business partners, reduce risk of lost or stolen information, and satisfy public law over privacy and identity theft/fraud.

In regulated industries such as healthcare and financial services, companies are required by law to protect messages that contain sensitive information such as patient records or personal financial data. In the U.S., the Health Insurance Portability and Accountability Act (HIPAA), mandates that personally identifiable patient data must travel through secure channels. The Graham-Leach-Bliley Act requires that confidential information must be sent securely. Likewise, Canada and Europe have similar and in some cases more stringent regulations for transmitting data. The UK for example, has the “Data Protection Act” and the “Companies Act” designed to protect personal information, as well as “EC Directive 95/46” indicating personal data should be handled with appropriate care.⁽³⁾

Beyond regulatory mandates, businesses have become more aware of consumer fears and concerns about the privacy and confidentiality of their data transmitted over the Internet. And, as business relationships and partnerships are increasingly forged over the Internet, securing those partner communications has become a basic requirement for many corporations.

OVERCOMING THE BARRIERS TO ENCRYPTED EMAIL

Until recently, a practical and affordable method to encrypt and thus secure email transmission over the Internet has been lacking. Postini, the leader in Integrated Message Management, addressed this problem by becoming the first managed service to provide secure email transmission through its

support of Transport Layer Security (TLS) (RFC 3546). Introduced as a feature of Postini Perimeter Manager® Enterprise Edition in 2004, Postini’s connection level security of email is based upon this standard critical components.

TLS is an Internet Engineering Task Force (IETF) sponsored protocol designed to secure and authenticate communications across a public network such as the Internet using data encryption. TLS is a universal and open standard successor to SSL or Secure Socket Layer, the protocol used to secure e-commerce transactions across the World Wide Web.

Another advantage of the TLS protocol stems from its application independence, allowing application or higher-level protocol developers to choose the best way of initiating TLS “handshaking” and interpreting authentication. In fact, TLS is already built into most MTA (Mail Transfer Agent)

technology used by MS Exchange and Notes/Domino mail servers, so that TLS can be utilized for secure email transmission with a simple activation in the Mail Transfer Agent.

POSTINI TLS SUPPORT PROVIDES A PRACTICAL, SECURE FOUNDATION FOR EMAIL ENCRYPTION

Postini has built support for TLS on top of its Enterprise Edition managed service and currently processes millions of encrypted messages each day. In most cases, enabling Postini Default TLS support simply means making sure TLS is “turned on” at the sending and receiving Mail Transfer Agent. For senders of encrypted email such as trusted partners and others using the TLS protocol, Postini recognizes the TLS “handshake” and ensures proper receipt by the customer.

POSTINI ENCRYPTION MANAGER

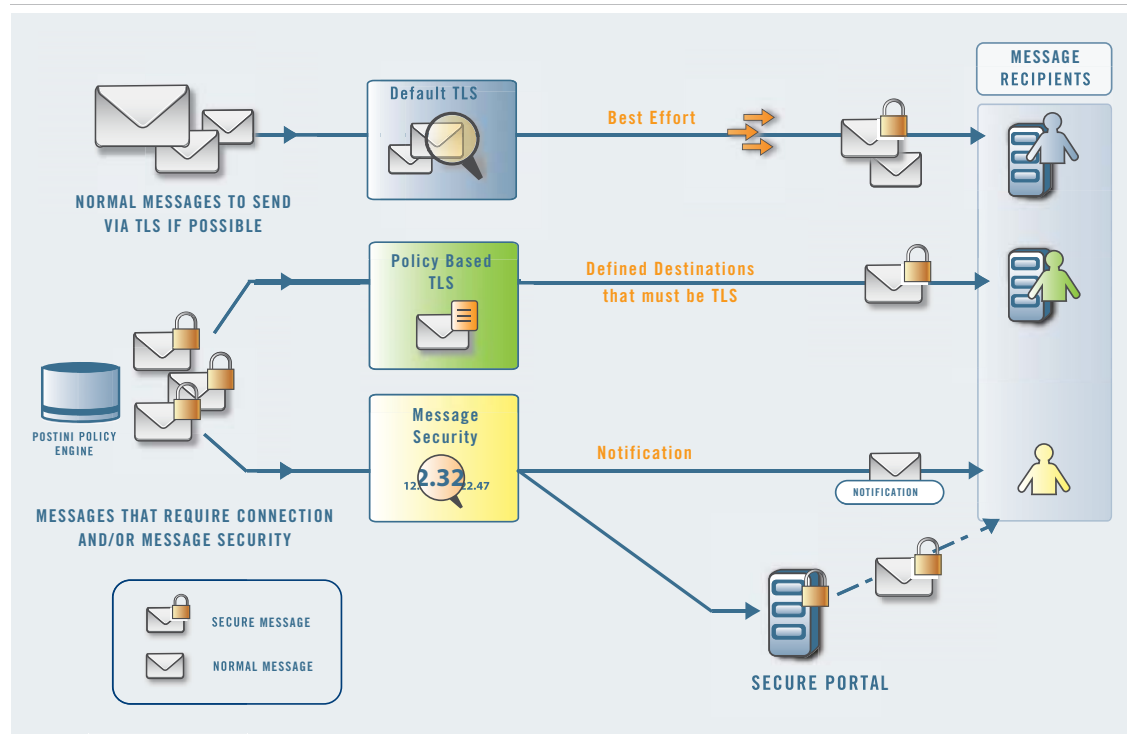


Figure 1: Assuring secure email transmission via the Internet: Postini assures that emails are delivered via a secure connection when traversing the Internet through its built in support of the TLS protocol. Additional encryption options pictured are described below.

As an added benefit, encrypted emails sent in or out of an organization pass through the Postini managed service data centers and are automatically scanned to block spam, viruses, and enforce content policy and compliance. In contrast, encrypted emails cannot be screened with many PKI implementations. Having invested years of effort and considerable expense to gain the ability to scan and filter their organizations' email, many administrators would not want to use an encryption system that would "lock them out" from screening encrypted emails. Just because an email has been encrypted does not necessarily mean it is safe or should be excluded from screening for viruses or malicious code. Or, that the encrypted message should not be screened for email content policy violations.

Postini's support of the TLS protocol was an important step in securing email transmission while preserving the administrator's ability to filter out unwanted or malicious messages and prevent email content policy violations. Because of Postini's patented MTA technology, encrypted messages are screened in memory, in real-time, compared with other managed services that use industry standard MTA technology and must first store messages to disk, screen them and then forward them to the recipient.

THE NEXT GENERATION IN EMAIL ENCRYPTION: POLICY-BASED ENCRYPTION ON DEMAND

One of the issues surrounding the use of email encryption has been a desire to not just encrypt email to those who mutually support and accept the TLS protocol but to extend the value and security of encryption to communications with all types of email recipients, including trusted partners, outside vendors, and remote employees and those that cannot support the TLS protocol.

As a result, most organizations today are seeking a more flexible, policy-based encryption solution for email that allows them to send an encrypted message to anyone, regardless of any pre-existing encryption solution they may or may not be

using. This requires a "federated" approach to encrypting emails that enables encryption to work with all types of authentication and proprietary systems. Just as important, email encryption needs to be managed according to company policies and regulatory mandates that govern its various relationships with customers, employees, trading partners, vendors and others.

INTRODUCING POSTINI ENCRYPTION MANAGER: POLICY-BASED ENCRYPTION AS A SERVICE

With the introduction of Postini Encryption Manager™, a suite of managed security services, organizations now have an easy and affordable method of securing email connections and email content anytime, for any recipient, according to specified policies. Postini Encryption Manager thus gives message administrators the flexibility and control to manage and enforce policy-based encryption without the cost and complexity typically associated with traditional PKI solutions. Postini Encryption Manager achieves this new level of security and flexibility through two transmission methods that can be used separately or bundled together.

SECURING THE EMAIL CONNECTION

First, Postini has extended its industry-leading support for the TLS encryption standard by providing comprehensive management tools that enable and maintain secure transmission between network servers according to established policies. Using the Postini Encryption Manager Connection Security, organizations can now enforce mandatory domain-level TLS connections, restrict connections that cannot be encrypted, and generate alerts when TLS policy cannot be enforced. This means message administrators retain full control over which messages can be delivered via mandatory TLS to domains they specify.

Available to Postini customers, Postini Encryption Manager Connection Security provides a convenient, automatic method for assuring secure email connections with customers and business or

trading partners that communicate directly with the organization via “mail server to mail server,” or “gateway-to-gateway.”

ENCRYPT THE EMAIL MESSAGE ITSELF

For situations where server-to-server connections cannot be established, or where the sender seeks more than connection level security, Postini Encryption Manager provides the option to encrypt the actual message content. Encryption Manager Message Security provides the ability to send encrypted messages to any recipient regardless of any pre-existing encryption solution they may be using.

Eliminating the cost and complexity of PKI software installation and ongoing key management, Encryption Manager Message Security allows the message administrator to enforce policies that encrypt all messages from a specified individual sender, or group of senders, as well as encrypting messages flagged as “sensitive” or “confidential.”

HOW MESSAGE SECURITY WORKS

Using proven encryption technology, the Postini Message Security automatically ensures that an email from a specified sender or type of message is encrypted and held in one of Postini’s secure global data centers. The recipient is notified that he or she has an email message from the sender and directs the recipient to a secure web portal to authenticate themselves through the Postini system, read and reply to the message via the secure portal and download the message if they need to. See Figure 2.

This type of “secure-and-post” messaging is particularly well-suited to banks or other financial institutions that want to communicate securely with customers that do not have encryption know-how, but still require a safe, yet convenient receipt of account statements or other privileged communications.

HOW POSTINI ENCRYPTION MANAGER MESSAGE SECURITY WORKS

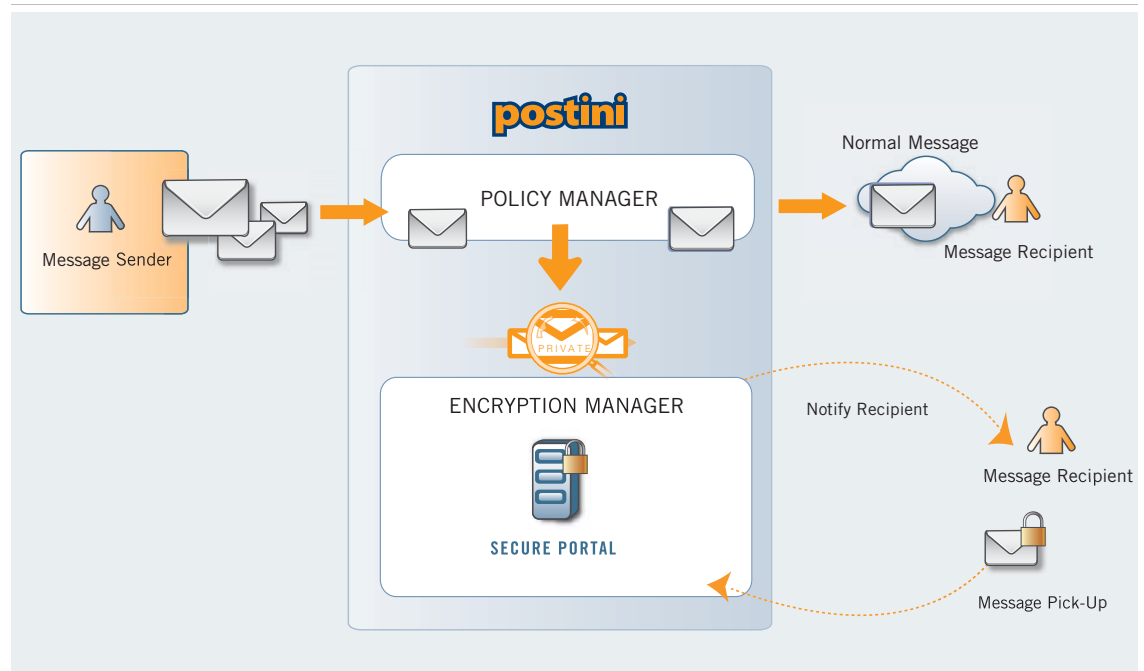


Figure 1: Assuring secure email transmission via the Internet: Postini assures that emails are delivered via a secure connection when traversing the Internet through its built in support of the TLS protocol. Additional encryption options pictured are described below.

COMMON POLICY FRAMEWORK AND MANAGEMENT ENABLES FEDERATED EXPANSION AND REPORTING

The Postini Encryption Manager suite of services is built upon a common policy framework and common management platform that allows it to employ multiple encryption options regardless of the recipient's encryption solution or preferences. Postini Encryption Manager Message Security can support multiple encryption solutions such as ZixCorp's encryption technology. Additional support for OpenPGP, S/MIME and other market encryption solutions are planned.

By utilizing Postini's common policy framework and management platform, message administrators, security and compliance officers can automatically assure enforcement of policies and mandates, reducing the risk of human error in the transmission of privileged and private information. Security managers, compliance officers and message administrators can readily manage encryption policies for individual users, user groups or domains, conveniently and effectively from a secure web interface. In addition, Postini Encryption Manager provides security intelligence reporting to help administrators track the number of users, quantity of messages, and analyze activity trends.

KEY ADVANTAGES OF AN INTEGRATED MANAGED SERVICE APPROACH TO EMAIL ENCRYPTION

- **Immediate deployment:** no infrastructure required: Selecting Postini Encryption Manager means there is no additional hardware or software to install or

maintain on either desktops or email servers, and no key management burden. The service can be activated in a matter of hours.

- **Automatic, real-time protection:** Postini provides comprehensive, automatic email encryption for both Connection Security and Message Security that scales easily and effectively across any size organization.
- **Much easier for users and administrators to use:** Because the TLS protocol encryption of email is built into Postini's Integrated Message Management Framework, there is no need to manage PKI certificates, keys, or passwords to assure encryption of messages, and all complexity is hidden from end users.
- **Significantly lower cost compared to conventional PKI solutions:** Using Postini Encryption Manager's suite of services means that organizations do not have to build or maintain dedicated secure networks such as VPN's between partners, while at the same time maximizing "federated" interoperability across technologies.

References:

- (1) "Locking Down E-mail," Keith Schultz, *InfoWorld Special Report*, September 20, 2004.
- (2) "No Vendor Can Fulfill All of Your Encrypted E-Mail Needs," Wheatman, Hallawell, Grey, Pescatore, Wagner, Kreizman, *Research Note*, October 13, 2004
- (3) "Secure E-Mail and Public Key Cryptography: Together At Last?" Andrew Conry-Murray, *Security Pipeline*, October 1, 2004
- (3) "Big Gamble: Decade of ECommerce," Laurie Sullivan, *InformationWeek*, November 8, 2004.



ABOUT POSTINI

As the leader in Integrated Message Management, Postini managed services protect businesses from a wide range of IM and email threats, provide message archiving and encryption, and enable the management and enforcement of enterprise policies to meet regulatory compliance requirements.

Corporate Headquarters

San Carlos, CA USA
Toll-free: 1-866-767-8461
Email: info@postini.com
www.postini.com

EMEA Headquarters

London, UK
Tel: +44 (0)207 082 2000
Email: info_emea@postini.com

Asia Pacific Headquarters

Tokyo, Japan
Tel: +81 80 3089 7470
Email: info_apac@postini.com