Why you need secure email

WHITE PAPER

CONTENTS

PURPOSE

This white paper is intended to provide the reader with a brief overview of relevant email security issues and technologies, as well as introducing the sslpost **secure email solution.**

Communication in the modern world has been revolutionised by email. Most businesses would simply not function without the medium of email and the opportunities it has created. However, for all its benefits, email has encountered some major problems. Although it is commonly known that email is not the securest means of communication, most people are completely unaware of the extent to which email is insecure. Messages, meant for a specific recipient could have been read and used by many different people, modified in transit, or could even be sitting on one or many servers all over the world. Information that is vital for your business could therefore be in the hands of competitors and fraudsters without your knowledge.

Security and information integrity are becoming increasingly important in business as more and more business is being conducted by email. Five fundamental security criteria must be met in order to provide more effective protection for the delivery of electronic documents:

1. Confidentiality – protecting content from unauthorised access.
2. Authorization – assigning permissions to the user working with the document.
3. Integrity – detecting unintentional or malicious document alteration.
4. Authenticity – proving that the document comes from true sender.
5. Non-repudiation – preventing senders and recipients from refuting delivery and receipt respectively.

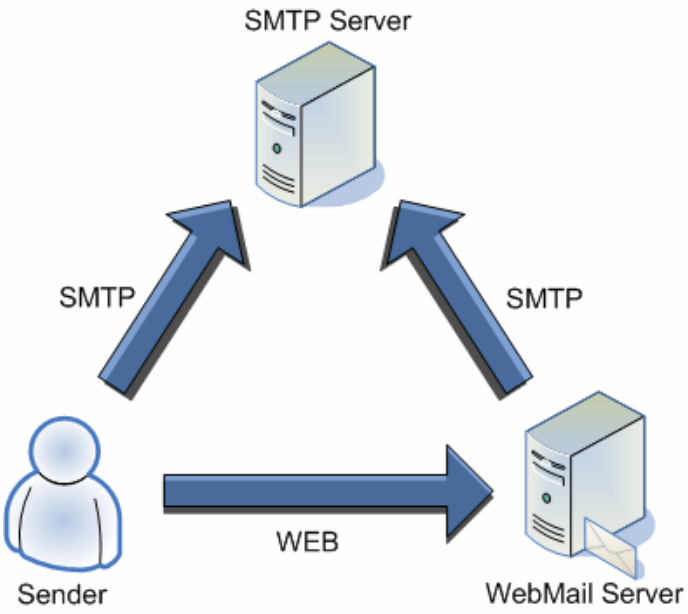
The sslpost secure email delivery and management solution is a sophisticated system of processes which encrypt and deliver electronic mail in a highly secure environment. SSLPOST can be supplied to organizations either as an easy to use ASP[1] solution or as a self-hosted and self-managed solution.

[1] Application Service Provider

This section describes the general mechanisms and paths taken by an email message on its route from sender to recipient. This should give you an overview of the different protocols involved, the different types of servers involved, and the distributed non-instantaneous nature of email. The examples herein are representative of most common email solutions, but are by no means exhaustive.

Sending an Email Message

In order to fully understand the process of sending and receiving an email, it is useful to make a direct comparison to the sending of a letter. Following this analogy we can consider our computers as the post offices and the 'Simple Mail Transport Protocol' (SMTP) as the course of action that the postal system follows. SMTP can be compared to a post office which has received a letter and who forwards the letter onto the nearest post office so that this post office can ultimately post it through the recipients' letterbox. Like the post office that sends the letter on its journey, SMTP is used by any program that relays an email message towards its final destination.



Most email users will be use one of two methods for sending email – either via a web-based interface, (such as Hotmail), or via an 'email client program' which runs on their personal computer or server, (such as Outlook or Lotus Notes).

In the case of an 'email client program', all external messages will be sent to an SMTP server, as the priority servers such as Microsoft Exchange will only deliver internal emails. All other emails will be passed onto the SMTP servers on your behalf, via the computer protocol SMTP.

When using WebMail, a web connection is used to communicate between your personal computer and the WebMail server. This in turn begins the first step of the delivery process, as the server contacts the SMTP server,

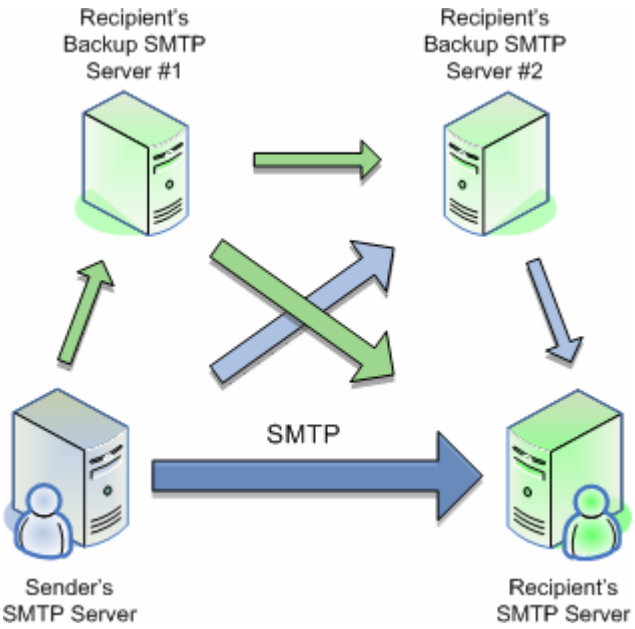
Delivery of email from your SMTP Server to your recipient's SMTP Server:

When a SMTP Server receives an email message addressed to someone whose email box is not located in that SMTP Server, it should "relay" that email message to another SMTP server closer

to the recipient (it may choose not to relay in which case an error message will be sent to the recipient). This is very much analogous to the postal service. When you drop off a letter and they notice that the address is for someone in a different location, the postal service ships off the letter to another post office in or near its destination. In the virtual world of emails this process is known as "email relaying".

But how does your SMTP Server know where to relay the message to?

If the recipient's email address is "mha@sslpost.com", then the recipient's domain name would be "sslpost.com". In order to ensure that the email is received an ordered list of SMTP servers are included in the 'DNS Settings' of the recipients' domain. These servers are all expected to receive emails for the recipient. However, the recipient's actual server is the highest priority receiver, and the others on the list are backup SMTP Servers. The roles of the backup servers are to queue the email for later delivery to the actual SMTP server for that particular domain.



On its journey from the sender to the recipient, an email can take several routes. Some of the following are examples of how an email may finally reach its destination.

1. The sender's server manages to contact the recipient's server directly and the email message is simply passed directly from sender to recipient (thick blue line in the figure).

2. The sender's server is unable to contact the recipient's server. This can occur for many reasons; although the most common reason is simply that the server is busy other reasons include the server being down or a problem with the internet connection between the two servers. In this scenario, the sender's server will attempt to contact the recipient's backup servers and deliver the message to the back up server.

3. The sender's server is unable to contact either the recipient's actual SMTP server or the backup server. The email will then be delivered to the second backup server.

4. The sender's server may be unable to connect to any of the recipient's servers (the sender's server could be too busy or unable to connect to the internet at that actual point). The message will then be stored by the server, which will try to send it at a later time or date. It will keep attempting to send the message until it has succeeded or given up.

In instances 2-4 above, an email message delivered to one of the backup servers could go through any of the above when trying to be passed to the recipient's actual SMTP server. The backup servers will queue any emails sent to them until they are all sent to the recipient's actual server.

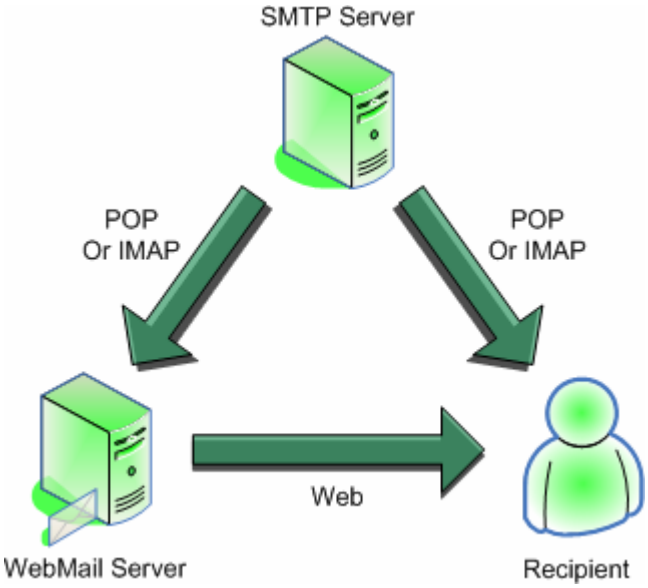
The recipient will only be able to read the email once it has arrived in their SMTP Server and has been moved into their email inbox. The recipient will then be able to see the history of the email's journey by the stamp that identifies which servers have received the message and at what time.

Summary so far:

- SMTP (Simple Mail Transport Protocol) is the system used by all email servers to communicate with each other.
- Many factors contribute to the length of time an email will take to be sent and received. These include internet traffic, servers that are too busy or are undergoing maintenance.
- Recipients can establish where from and when the email was sent, by the identification stamp on every email. This will also give them the internet address and the name of the sender's computer.

Retrieving Email from an SMTP Server

Once an email has been received by your SMTP Server, it is passed straight into a file. In order to then read the email, this file must be accessed with a program that can speak the same language as the SMTP Server.



The two main languages used to retrieve emails stored in this file are "Internet Message Access Protocol" (IMAP) and "Post Office Protocol" (POP).

Most recipients view their mail by using either a WebMail interface (such as Hotmail) or an Email Client Program (such as Outlook or Lotus Notes). The email client program and the WebMail will interface with the file using either IMAP or POP, thereby allowing you to read the email.

The Lack of Security in Email

The bullet points below highlight some of the inherent security issues involved with sending and receiving email. It is important to remember that privacy and encryption were not part of the original design of email. Security is therefore not a prominent feature.

- SMTP, used by all email servers to communicate, does not use encryption for messages. This means that SMTP Servers send all messages in plain text, open for anyone to see. It also means that if the server requires you to log in with a username and password to send emails, this too can also be seen. SMTP also includes in all messages information about which computer they came from and what email program was used.

- WebMail does not use encryption either. All information including the username and password used to get into the account is open to anyone who wishes to see it, as it moves from the WebMail Server and personal computers. The connection to WebMail servers is http:// and not https://, thereby determining their inherent insecurity.

- IMAP and POP require users to login with a private username and password. Again these credentials are not encrypted or secured. Anyone with adequate knowledge of eavesdropping in computer systems can therefore view this information.

- Most messages are stored on SMTP Servers in plain text and are free to be read by anyone. Backups can also be made on the servers, meaning data held anywhere on those machines can be read. Messages you thought had been deleted could be saved and being read by people you don't even know.

The Internet is used by millions people all over the world. The Internet has improved business communications and opened new business opportunities by cutting costs and speeding up the communication process. However it has also allowed for fraudsters to benefit from the lack of common knowledge of most Internet users of even the most basic Internet security.

The following section is designed to highlight the security problems involved in email in order to then show how one can mitigate against such security weaknesses.

EAVESDROPPING is a fundamental problem on the 'Information Super-Highway'. It is very easy for people to access information held on computers and servers not intended for sharing. Email, although in many aspects the most efficient form of communication, has the potential to spread private information to both unwanted and unknown recipients.

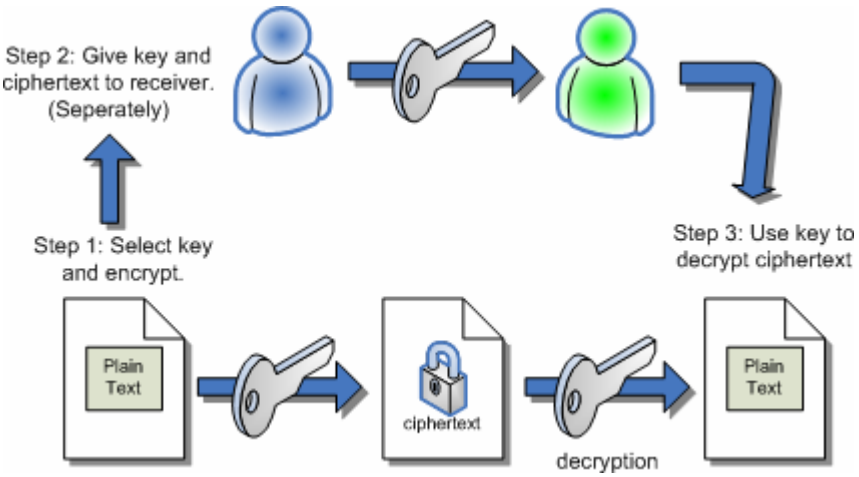
THEFT OF LOGIN DETAILS is the one of the outcomes that may result from Eavesdropping on connections such as SMTP, POP or IMAP. If a person obtains the username and password of an email server, they can gain access to any emails or information held on them.

MESSAGE ALTERATION or even email deletion can occur at many points during an email's journey to the intended recipient. Anyone who can access the SMTP Servers that a message visits is able to read and change the message before it is forwarded onto its intended destination. The recipient has therefore no way of knowing whether the email has been tampered with. Furthermore if the message was deleted it would never arrive and the intended recipient would be none the wiser.

FALSE MESSAGING has created the perfect environment for the spreading of viruses. It is very easy to construct an email that looks as if it has come from someone that the recipient would normally trust. Many people open emails appearing to be from someone they know only to find they have inadvertently infected their computer.

THE IMPLICATIONS OF FALSE EMAILS can cause huge problems in business communications. Forged and false emails circulating the Internet have made it almost impossible to tell whether someone did or did not send you a message. It is very possible for someone to deny that they sent you a message, when they did, or say they sent you a message when they didn't. This has obvious repercussions for businesses which rely heavily on email.

In order to show how the security problems with email (described in sections 2 and 3) can be solved it is vital to understand how the two main types of encryption operate.



Symmetric Key Encryption (single key system)

Symmetric key encryption helps to erase the problem of eavesdropping and unwanted backups. It does this by creating a "secret key" for the sender and the recipient of the email to share. Both parties will be able to use this key to encrypt and then decrypt the message. Cyphertext is used for encryption, as it looks like a totally random sequence of characters, and appears meaningless to those who do not have the "secret key". It is very hard to change the message in transit, as any modification of the email will mean that it cannot be decrypted by the key.

In theory this method would be perfect for keeping emails secure. However, the fact that both parties share the same key can cause problems. Unless the two parties meet in person, there is no real way to securely communicate the key. If you wish to send a secure message to someone around the world, you would need to find a way to get the "secret key" to the recipient in an efficient and expeditious manner.

Message Digests / Authentication Codes

'Message Digest' or 'Message Authentication Code' is a simple concept to solve the issue of message modification. Before it is sent, the message is passed through an algorithm (a series or mathematical processes), which determines a short sequence of numbers that only correlate to that specific message. This is called a unique 'fingerprint' as any change in the message would create a totally different sequence. No two messages will yield the same sequence.

Comparing the digest and the message will automatically tell you whether an email has been altered in any way. If the digest matches the message, then you know that it has been received by you exactly the same as it was sent by the sender.

Asymmetric Key Encryption (two key system)

Asymmetric key encryption, also known as "Public Key Encryption" differs from Symmetric Key encryption as it involves two keys. Both the sender and the recipient are given separate keys, one to encrypt the message and the other to decrypt. Any text encrypted into cyphertext by one of the keys can only be decrypted by the other, and likewise, (e.g. If Pi encrypts a message, then only Pii can decrypt it. If Pii encrypts the message, then only Pi can decrypt it).

The two keys in Asymmetric encryption are commonly known as the “Private” and “Public” keys, whereby the Public key is given out to anyone who wants one, and the Private key is kept secret for only the sender. The security of Asymmetric encryption depends upon the Secret Key being kept securely.

Asymmetric Key Encryption allows you to do the following:

SEND A SECURE ENCRYPTED MESSAGE

To ensure that the message being sent will only be seen by the intended recipient, it can be encrypted by their public key. It will only be the intended recipient able to decrypt the message with their Private Key, removing the possibility that eavesdroppers will be able to see the information and tamper with it.

PROVE THAT A MESSAGE WAS SENT ONLY BY YOU

If your public key decrypts a message, it means that it must have only been encrypted with your private key. This proves that it was you alone who sent the message, as your private key is kept only to yourself. This is a simple and obvious way of showing that a message has come from you.

SIGN A MESSAGE

This process can be used to determine aids in determining whether an email has been modified whilst being sent from the sender to the recipient and proves that you sent the message. This is done by encrypting a digest of the message with the senders’ secret key. The recipient can decrypt this and compare it to the digest of the actual message. If the two match then the message has not been altered and was sent by you.

Combining these three features together gives the most secure form of email communication. Security benefits such as removing the possibility of eavesdropping, proof of sender and proof of message integrity are vital in any business relying on email communication.

Note

Symmetric encryption is a type of encryption where the same key is used to encrypt and decrypt the message. This differs from asymmetric (or public-key) encryption, which uses one key to encrypt a message and another to decrypt the message.

Using an email provider that utilises a "Secure Socket Layer" (SSL) when connecting to WebMail, POP, IMAP or an SMTP Server, is one of the simplest ways to increase the security of your email system.

SSL in combination with Asymmetric and Symmetric key encryption has two main benefits. It will not only ensure that you have been connected to the right server, but it will also ensure that all the subsequent communications between the user and the server is secure. This is done through the following features:

- In order to make sure that the user is in fact connecting to their SMTP Server and not a 'middleman' attempting to intercept communications, the SSL uses the 'Private/Public' key method. The server uses the private key to prove to the user that it is the correct sever.
- The user then generates a 'secret key'.
- This 'secret key' is then shared with the server by encrypting it with the server's public key.
- The user and the sever can then securely communicate using Symmetric encryption using the shared 'secret key'

SSL certificates prove that the user is going through the above process and thereby negates some of the security risks associated with email communication. The SSL certificates are issued by companies, such as Verisign or Thawte.com, who are known globally as trusted certificate issuers. These third party agencies will run several background checks on those requesting SSL certificates to ensure that they have the right to use it. The issued certificate will then contain the name of the company or person, the issuing company and the name of the server to which it is issued. When the user then connects to the server they can view this information and thereby confirm that the certificate was issued by a company and to a company that they can trust.

WARNING MESSAGES

Warning messages often pop up when using SSL to connect to a server. Although these can be caused by small issues with the provider, they could also be caused by the user's communications being intercepted by a third party. These warning messages should therefore not be ignored.

Any of the following could be reasons for a warning message appearing:

- The SSL certificate has expired and must be renewed.
- The user could be inadvertently connecting to the wrong server, in which case the information on the SSL certificate, such as the server name, will be different to that expected.
- The certificate was issued by an agency that cannot be trusted.

Using an SSL certificate ensures that all communications, using WebMail, POP, IMAP and SMTP, between the user and the server will be secure. The username and password to retrieve messages and the actual message content will also be hidden from third parties. However, this is only secure while on your own server. SSL does not protect your private emails and as soon as they leave the secure SMTP Server and make their way to the recipient they become insecure. On leaving the secure SMTP server the emails are capable of being read by any eavesdropper.

Using SSL is a very simple and straightforward procedure. It only involves a change in the configuration of your email client and is totally transparent. It can also be used even if the recipients of your emails do not have a SSL certificate of their own. Although the email id is not protected once it leaves your server, SSL will completely protect your username and password from detection. This is important in preventing identity theft and the sending of false messages.

SSL can only protect the path between the users' personal computer and their SMTP Server and whilst this does help to keep login details and messages secure to some extent, it does not deal with all email security issues.

In order to truly protect email communication, Asymmetric key encryption must be used. This solves the following issues:

EAVESDROPPING – All information is encrypted and therefore looks like a seemingly random selection of characters.

MESSAGE ALTERATION – Message digests (see page 7) mean that the message will be illegible if changed.

FALSE MESSAGES – Signatures and timestamps prove that the message is exactly from who it claims to be.

To maximise the security surrounding email communication, Asymmetric key encryption should be used with SSL. Although the message will be protected by the asymmetric encryption, login details, (username and password), will not. With SSL, the login details will be encrypted along with the message and the whole process, from sending to receiving the mail will therefore be secure.

The two most widely used forms of encryption for adding encryption and signatures to email are S/MIME and PGP.

PGP can be acquired from PGP.com and is compatible with most modern email systems.

S/MIME is pre-built into email systems, such as Microsoft Outlook, but in order to use it, an S/MIME certificate from a third party must be obtained.

Interoperability Problems

Although encrypting and signing your messages through PGP and S/MIME alleviates the security issues of email messaging, it does have some drawbacks. The main problem is that PGP and S/MIME are incompatible. This obviously means that people using PGP and S/MIME are unable to send each other secure emails. PGP currently accounts for over 90% of encrypted email traffic, so most people using the encryption method are compatible with one-another. However, this does still leave a large number of users who prefer to use S/MIME, and in today's business world no business can afford to exclude such a large user base. There are email clients that can be configured to use both PGP and S/MIME so that secure correspondence can occur no matter which security format is being used.

However the other and more important interoperability issue is caused by the main feature of encryption, which is 'key exchange'. In order to send an encrypted message, you first need the recipients' public key. For the recipient to then prove that it was in fact you who sent the message and that it is unchanged in transition, they need your public key. So, before any secure communication can get underway, trading of keys must first take place. There are various ways of doing this, such as PGP's Key servers from which the recipient and the sender can both download each others key information. However, not every person has access to the keys on the servers, let alone the authority to use PGP, so the key exchange issue is a significant problem.

The SSLPOST encryption wrapper software offers all the advantages of symmetric encryption, asymmetric encryption, SSL and message digests in one simple and easy to use software package with no need for trading public keys.

Using SSLPOST the sender no longer has to know the public key of the recipient and in fact the recipient does not even need their own key.

As a result no interoperability issues arise between the sender and the recipient.

SSLPOST:

- Prevents message modification during transit
- Allows recipient to store the message forever in a highly secure fashion on their server
- Prevents eavesdropping of your email
- Allows a time stamp to be included in the signature thereby preventing the problems associated with message replay
- Prevents repudiation of the email by the recipient as SSLPOST records the date and time of all attempted and actual openings
- SSLPOST can prevent a brute force password attack by limiting the number of attempted openings. Furthermore SSLPOST is capable of restricting the recipient from opening a SSLPOST email by time and/or IP address of the recipient.
- No interoperability problems
- Recipient does not need their own certificate
- Works with all well known client software
- Allows recipient to verify the identity of the sender thereby verifying the authenticity of the email from the sender
- Communication between the sender and recipient is always secure
- Allows the sender to know when the recipient opened the email and how many times they opened the email

Definition of terms

Encryption -	The translation of data into a secret code (cipher text). Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text.
Decryption -	Is the reverse process that transforms cipher text back to the original plain text.
Key -	A password or table needed to decipher encoded data.
Plain Text -	Plain text refers to any message that is not encrypted.
Ciphertext -	Data that has been encrypted. Cipher text is unreadable until it has been converted into plain text (decrypted) with a key.
Symmetric Encryption -	A type of encryption where the same key is used to encrypt and decrypt the message.
Asymmetric Encryption -	A cryptographic system that uses two keys -- a public key known to everyone and a private or secret key known only to the recipient of the message.

	Proves integrity of content	Secures the Message	Private and public key encryption	Repudiation	Protects against unwanted backups	Simple key exchange	Protects Username and password	No Interoperability issues
Symetric Encryption		●						
Asymmetric Encryption	●	●	●	●	●	●		
Message Digests	●							
SSL							●	
PGP	●	●	●	●	●		●	
S/MIME	●	●	●	●	●		●	
SSLPOST	●	●	●	●	●	●	●	●

Email is by its nature highly insecure

These security issues include:

- Eavesdropping
- Identity Theft
- Invasion of Privacy
- Message Modification
- False Messages
- Message Replay
- Unprotected backups
- Repudiation (Sender denies that they sent it)

Solutions:

SSL: Simple and easy to use, SSL will secure communications between your computers and your email service provider's computers. This works no matter who your recipients are. Using SSL provides the following benefits:

- Trust, in that you are contacting your service provider's computers and not someone else's
- Encryption to protect the username and password that you use to login to these servers. This mitigates identity theft.
- Protection from eavesdropping during this leg of the email message's path to the intended recipients.

PGP and S/MIME: These additions to your email allow you to use the features of asymmetric key encryption to protect the contents of your messages throughout their entire path of transit from you to your recipient. They provide:

- Encryption to protect against eavesdropping and unwanted backups
- Message Digests to allow the recipient to see if the message has been altered in transit
- Signatures to prove that the apparent sender is in fact the one who sent the message

Only a very few companies are utilising the full benefits of PGP or S/MIME for encryption.

The resistance in adopting these encryption protocols is often due to the effort required to setup the PKI infrastructure, enforce usage, and in training employees. These costs are often much greater than any perceived benefit derived from PKI.

Clearly the cost savings gained by using secure email messaging will be in having less information leakage or modification. However such losses are extremely difficult to quantify financially, especially as most companies assume that they don't or won't have any significant financial problems from sending or receiving insecure emails.

SSLPOST: The assumptions above will change as SSLPOST becomes more widely adopted. The cost of setting up SSLPOST, using SSLPOST and training staff to use SSLPOST is small when compared to full PKI infrastructures.

More importantly SSLPOST simply requires the recipient to have an email account and access to a web browser and nothing more.

Unlike computer break-ins and other security problems, problems with email security are very hard to detect. You cannot tell if someone is reading your email or modifying messages subtly until it is too late.

You cannot quantify the cost of email and information security problems until it is too late.