A Guide to Secure Email

ABOUT THIS WHITE PAPER AND TARGET AUDIENCE

This document is a whitepaper discussing the concept of secure email and the way in which M86 Security enables secure email with its solutions. The central focus in this whitepaper is on Public Key Infrastructure (PKI); how it works, what it does and how it provides the platform for M86's secure email solution. It also covers other aspects of secure email such as encryption and digital signing, Transport Layer Security (TLS), and the ongoing management of secure email systems.

The intended target audience for this whitepaper is anyone who is interested in the concept of secure email. This document provides an elementary introduction to these concepts that can be appreciated by almost any level of reader, from IT administrator to CEO to end user. Having a basic understanding of SMTP email and how it works is advantageous but not required.

WHAT IS SECURE EMAIL

Depending on who you talk to, the term 'secure email' can have different meanings. In M86, when we refer to secure email, we are essentially talking about email encryption and digital signing.

SMTP email is an open protocol in that a message can be intercepted and read by any number of third parties. When you send an email message, that message can be seen and read by anyone who comes in contact with the message; just like a postcard. For example, your message may pass through a number of Internet Service Providers on its journey and administrators for these ISPs will almost undoubtedly have access to the contents of messages that you send.

When we talk about secure email, we are talking about the ability to secure a message in such a way that the contents of that message remain private between you and your intended recipient and visa versa. This is achieved through encryption.

A second (and arguably more important) issue with SMTP email is that it is open to abuse and manipulation. It is very easy for a third party to forge an SMTP message and make up its content and address details. This act of impersonation is commonly known as spoofing. From this perspective, SMTP email is also unsecure. Therefore, any solution for secure email should not only provide encryption for privacy but also ideally authentication and validation that messages are genuine and can be guaranteed to have originated from the apparent sender.

The act of validating the authenticity of a message is known as digital signing.

THE M86 SOLUTION FOR SECURE EMAIL

M86 Security effectively has two solutions for providing secure email:

1. TLS secure communications with MailMarshal SMTP
2. PKI using S/MIME with MailMarshal Secure Email Server

This whitepaper primarily addresses the second, stronger, solution around S/ MIME and PKI. TLS secure communications is M86's introductory secure email solution and is well suited to typical small business requirements. TLS only provides encryption for the privacy of message content; it does not provide any form of signing to indicate the message originated from the apparent sender.

TRANSPORT LAYER SECURITY – TLS

TLS or Transport Layer Security is a standard feature with MailMarshal SMTP and is available for use at no additional cost. TLS works in a similar manner to SSL security for HTTPS secured websites. Effectively, TLS establishes a secure communications channel between two TLS enabled email servers allowing email messages to pass between the servers in a secure fashion. In this regard, messages are not individually encrypted and authentication is supplied by the inherent trust in the link between the two TLS enabled servers.

We won't be exploring the details of TLS in this whitepaper. It is suffice to say that PKI provides greater levels of privacy and authentication than TLS and is more scalable and manageable in a business context. TLS offers an excellent means of setting up a good secure link between two organizations but it doesn't achieve the level of secure email required to meet the compliance standards for several major pieces of legislation. TLS will likely meet the secure email needs of many organizations however in this whitepaper we will be exploring the advantages of the stronger PKI method of providing secure email.

PKI and S/MIME

M86's more advanced solution for secure email is Public Key Infrastructure (PKI) based on the S/MIME email encryption standard. The name of this solution is MailMarshal Secure Email Server which is a dedicated S/MIME gateway designed to be compatible with any SMTP server capable of routing S/ MIME encrypted messages.

MailMarshal Secure Email Server is also designed to work with M86 email content security solutions, MailMarshal SMTP and MailMarshal for Exchange, to provide deep content inspection of encrypted messages.

WHAT IS S/MIME?

Secure / Multi-purpose Internet Mail Extensions (S/MIME) is an industry standard for providing public key encryption and signing of MIME encapsulated email. MIME is a standard format for SMTP email which allows message attributes such as rich text, attachments and message bodies with multiple parts. S/MIME is simply a secure extension of that format in a similar way to how HTTPS is a secured form of the HTTP protocol for Web.

S/MIME is a widely supported standard that provides both cryptographic security and digital signing. The significant majority of today's email applications support S/MIME including Microsoft Outlook. S/MIME is arguably the mostly widely supported standard for Public Key Infrastructure (PKI) available.

*PKI is described in depth further on in this document

OTHER SECURE EMAIL CONCEPTS

- B2B or Business to Business – Describes a system where two companies agree on a mutual encryption standard such as S/Mime and then begin exchanging email directly between each other using this method

- B2C or Business to Consumer – Describes a system where a business does not need to decide on a common encryption method but instead sends the message to a secured website where the consumer first must authenticate to prove who they are and then retrieve the message typically through a SSL secured browsing session. This means the consumer does not require any compatible encryption product but does need to manually retrieve each message

- Gateway to Gateway Encryption – Describes where an email message is encrypted only between the sending and receiving hosts but not between the hosts and the email client used to compose or read the message. This means the email is encrypted on the Internet but not on a company's internal network. The advantage of this is that you only need one certificate for all users but the disadvantage is that if security is paramount, even internally within a company this does not protect that email on the internal network.

- Desktop to Desktop Encryption – Describes where an email message is encrypted all the way from the client used to compose the email message to the email client used to read the email message. The advantage of this is that the email message is encrypted at all times providing paramount security but the disadvantage is that individual certificates are required for each user. Products such as MailMarshal Secure Email Server can still de-crypt a desktop to desktop encrypted email message, scan it to ensure it meets defined policy and then reencrypt and send on to the email client if configured correctly.

WHAT IS OPENPGP & PGP?

PGP stands for 'Pretty Good Privacy' and is an encryption standard developed byv Philip Zimmermann in 1991 primarily for Email encryption. It is regarded as a defacto industry standard because, although fairly widely deployed (mainly in America), it has been officially accepted by the Internet Standards board. OpenPGP is a freely available interface for independent developers to create solutions based on PGP.

PGP corporation is separate from these and develops extended products based on the original PGP standard. OpenPGP is available typically as a gateway to gateway solution, as it has limited client support.

WHAT IS PKI?

Public Key Infrastructure (PKI) is a framework for secure communications using a pair of encryption keys; one public key and one private key. This is known as asymmetric cryptography which is basically a technical way of describing two different but interrelated digital keys. One way to think of this relationship is to think of the public key as a child and the private key as its parent – the public key can only come from its parent/private key.

To understand what PKI is all about and why it is such an excellent form of secure email, it is helpful to appreciate some of the difficult questions about secure email that PKI answers.

1. How do you code a message for another person without revealing the decryption secret to anyone else?

2. How do you ensure that when you code a message, only the person (or organization) you want to be able to open it has the unique ability to decrypt it?

3. How do you ensure that the person receiving a coded message knows for sure that it is from you and the message can be trusted?

HOW DOES PKI WORK?

In essence, encryption is basically a code. In World War II, armies needed secure communications to prevent the enemy from discovering their battle plans. Messages were coded and intended recipients were only supposed to be able to decode the message if they knew the secret way to decode the message. To decode the message you either needed to know the code, or you had to have a special machine that could decode the message.

In the modern Internet age the idea of cryptography is the same as it was in World War II but the logistical problems and communication mediums have changed. Often you meet new people or organizations that you need to communicate with securely. You need to be able to share the details of how you will be providing secure email between each other without revealing to anyone else how you are doing it.

A common analogy to this problem (as described on Wikipedia. org) is to imagine two people who wish to exchange secret messages. Alice wants to send her friend Bob a secret message and then wants to receive a secret reply back from Bob.

With a physical letter, Alice puts the letter in a lockbox and locks it (encrypting the message). She then sends the box to Bob who unlocks it with an identical key that he has to the box (decrypting it). Bob can read the message, write a response and send the letter back to Alice, locked in the same box, to which she also has a key. This scenario is known as a symmetric key system of encryption. The problem with this system is that anyone with a copy of the key can unlock the box, so it is not very secure. It also fails to answer the question of how does Bob know that the message is from Alice – the letter could have been written by anyone with a copy of the key.

PKI uses a pair of keys to solve these issues. The way PKI works is that Alice and Bob each have separate padlocks and keys. Alice exchanges her padlock with Bob but keeps her key to herself (private key). Bob does the same. Now Alice has Bob's padlock and Bob has Alice's padlock. When Alice wants to send Bob a letter, she puts it in the lockbox and secures it with Bob's padlock. Bob has the one and only copy of the key to this padlock so only he can open it. Effectively, the padlock is the public key while the key to the padlock is the private key.

The main advantage in this scenario is that there are no copies of the private key to the padlock, so no third party has had an opportunity to make a copy of the key.

Another aspect to this analogy is that because only Alice's key can open her padlock she can use this unique key to sign or mark her message to Bob. Let's say that Alice leaves the imprint of her private key on the message to Bob (like a wax seal). Alice places the letter in the lockbox and locks it with Bob's padlock. When Bob opens the padlock at the other end with his key and takes out the letter, he can see the mark of

Alice's unique key and can compare it to the padlock (public key) that he has for Alice. If they match, Bob knows that the letter has come from Alice because only her private key is compatible with her padlock (public key).

This analogy is a simplification of how PKI works to convey the basic principles involved. With PKI, Bob doesn't actually need to physically compare Alice's key sign with her padlock. The comparison and verification is done automatically. The issue that is still unresolved is how do Bob and Alice really know that each is who they claim to be when they first exchange public keys with each other? This question introduces the concept of certification and identity verification when first setting up secure email between two parties. We will cover this particular aspect of PKI in the next section.

LIMITATIONS OF PKI

On paper, and in simple analogies to a postal system, PKI appears to work well. However, there are a number of 'what if' scenarios with PKI that are mostly associated with scalability and ongoing maintenance:

1. How do you verify that a person who gives you their public key is who they say they are without meeting them face-to-face?
2. What if you want to set up PKI with 100 organizations rather than just one?
3. What if someone's private key is compromised, enabling a third party to decrypt their messages and forge their digital signature?

With the first question the answer is related to identity confirmation. This is provided in the form of a certificate, which is signed by a respected and trusted agency, verifying an organization's identity claims. These agencies are known as Certificate Authorities. It may help to think of Certificate Authorities as reference checkers who do background investigation on organizations before issuing them with an identity card.

Certificate Authorities (CA) will investigate and verify a company's identity claims and issue them with a certificate. When Alice gives Bob her public key, she also gives Bob her certificate validated by a trusted Certificate Authority. Often these certificates have an expiry date (typically about 12 months). When the certificate expires, Alice needs to re-confirm her identity credentials with the Certificate Authority who issues her with a new, valid certificate. Alice then needs to re-issue her updated public key with the new certificate to Bob so that he can continue to trust Alice's digital signature.

This idea of certificates expiring and being re-issued on a regular basis can create logistical challenges. These challenges are not significant when it is just Alice and Bob using secure email between each other. It just means that once a year they have to update their secure email system to use the latest keys and certificates. The challenges become more apparent when Alice and Bob also need to establish secure email with Claire and Daniel (A, B, C, and D). This means, once a year, Alice will need to exchange credentials with Bob, Claire and Daniel and each of them will need to do the same. This means 4 x 4 = 16 key exchanges per year. If another person is introduced the problem becomes exponential. When 10 parties are involved there will be 10 x 10 = 100 key exchanges per year.

This scenario shows that PKI can have a potential scalability issue. Every time you introduce a new secure email contact you square the number of manual key exchanges required by the number of secure email contacts involved.

At the point where you have 100 contacts (100 x 100 = 10,000 key exchanges) the problem of maintaining up-to-date credentials for everyone becomes unmanageable. We will address how M86 solves this challenge later in this whitepaper.

There is still another question about PKI limitations that we haven't yet answered. What happens when one of your secure email contacts is compromised and their private key obtained by a third party? Trying to deal with scheduled updates of key credentials is challenging enough, but what happens when an unforeseen and random breach in secure email occurs? Clearly there needs to be a mechanism by which you can notify all of your secure email contacts that your public key can no longer be trusted and should be discarded. The answer to this problem is called a CRL or Certificate Revocation List which is a standard feature available with certificates.

A CRL is a list of published public keys which have been revoked and should no longer be trusted. The reasons for revoking a public key do not have to be for security breaches. It could be a list of expired certificates. Or, if a company is sold and their identity credentials have changed, a CRL might list a revoked key for such simple reasons as a change of address.

HOW DO M86 SOLUTIONS SOLVE PKI LIMITATIONS?

As we have explored, PKI introduces some pretty big challenges if you want to use if for secure email with many, geographically dispersed contacts. Yet, this is typically the exact kind of scenario where secure email is needed. A key element of secure email is to allow a group of organizations to communicate and collaborate in private. MailMarshal Secure Email Server has been specifically designed to address these challenges; providing a cost effective, easy to maintain and scalable platform for secure email.

Certificate Authorities are one way to solve the issue of identity verification. The problem with these is that they can be expensive. It can cost thousands of dollars to have a CA perform a background check and issue you with a certificate. Plus, there are ongoing costs if you follow secure email best practices and retire your certificate each year.

Some organizations choose to self-sign their certificates and obviously this defeats the purpose of validating your credentials. The key ingredient here is that a CA is essentially a referral from a trusted source.
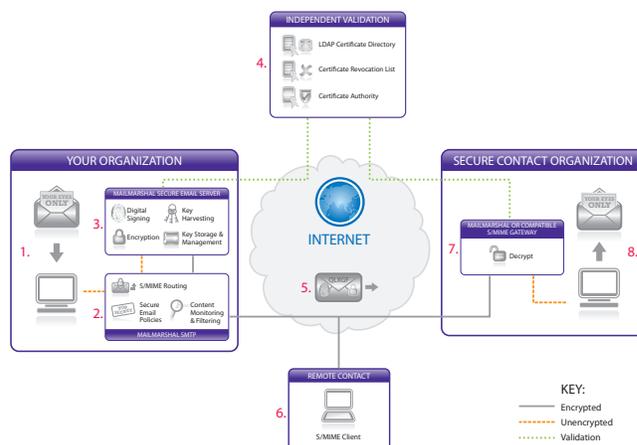
MailMarshal Secure Email Server provides a simple but very effective means for organizations to set up their own trusted referral source. Let's say that Alice, Bob, Claire and Daniel want to set up a secure email collaboration group between them. They can use a Certificate Authority to validate their certificates or, they can nominate one trusted source. What if Alice knows and can vouch for Bob, Claire and Daniel, having independently met all of them. Alice is then in a position where she can then act as the Certificate Authority for the group.

With MailMarshal Secure Email Server, you can nominate a central trusted authority who oversees your group. They can then establish a central validation server which Alice, Bob, Claire and Daniel all connect to. This server can then be used for a variety of functions including centrally managing automatic key/certificate updates, CRLs and as the trusted source to validate new secure email contacts if you want to expand the group. This framework is used by the New Zealand Government's eGovernment Secure Electronic Environment (SEE) Mail program to facilitate and maintain secure email between government departments and agencies.

MailMarshal Secure Email Server can use Lightweight Directory Access Protocol (LDAP) to update from a central authentication server. This mechanism allows for completely autonomous maintenance of secure email contacts, key exchanges and CRL look-ups, thus solving the various historic scalability and management limitations of PKI. Furthermore, MailMarshal Secure Email Server is a policy-based solution. It ensures that any private communication between secure email contacts is always encrypted. If it doesn't have all of the valid and current ingredients to encrypt a message for an intended recipient it will not transmit the message.

HOW MAILMARSHAL SECURE EMAIL SERVER WORKS

MailMarshal Secure Email Server works with MailMarshal SMTP or MailMarshal for Exchange to provide centralized, policy-based secure email as well as content monitoring & filtering. It provides a framework which requires no desktop encryption software and no end-user training. MailMarshal Secure Email Server automatically and seamlessly enforces encryption, decryption and digital signing policies, along with deep content inspection, certificate management, harvesting and secure storage of public keys for email contacts.

STEP-BY-STEP

1. Confidential Email – an authorized user within your organization sends a confidential email to a secure contact.

2. MailMarshal SMTP – MailMarshal SMTP evaluates the message and automatically determines that based on policy, such as confidential content and/ or the intended recipient, the message must be encrypted before leaving your organization. It routes the message to MailMarshal Secure Email Server for encryption and signing. NOTE: In the reverse scenario where your MailMarshal SMTP server receives an encrypted message from a secure contact, it routes the message to MailMarshal Secure Email Server for decryption in order to perform the content filtering required before delivery to the internal recipient. It may also be re-encrypted before being sent to the internal recipient if Desktop to Desktop encryption is supported.

3. MailMarshal Secure Email Server – the confidential email is accepted by MailMarshal Secure Email Server which then signs the message with your organization's Private Key and automatically encrypts the message content with the intended recipient's public key/certificate. If the right certificate is unavailable, has expired or been revoked, MailMarshal Secure Email Server can be configured to automatically retrieve the right certificate from a central LDAP server or independent Certificate Authority (see Step 4). MailMarshal Secure Email Server will also automatically harvest and store Public Keys from incoming digitally signed messages.

4. Independent Validation – MailMarshal Secure Email Server can interface with a central LDAP server that you and your secure contacts establish together to maintain credentials such as certificates/public keys and certificate revocation lists. This makes it easy to add new members and share key updates without any manual administration. MailMarshal can also work with independent Certificate Authorities such as VeriSign or Comodo.

5. Encrypted & Signed Email – Once the message has been signed and encrypted by MailMarshal Secure Email Server, it is then routed back to MailMarshal SMTP where it is re-checked against policy before transmission. Once the email leaves your organization it can only be opened by the intended recipient.

6. RemoTe Contact – The intended recipient can be an individual such as one of your own staff working out of the office or an external party such as a contractor or lawyer. These individuals can use a standard S/MIME email client such as Microsoft Outlook to communicate with your organization securely.

7. Secure Contact Organization – Your secure email partners can use MailMarshal or any other suitable S/MIME gateway or a standard S/MIME client such as Outlook to decrypt the message.

8. Intended Recipient – Whether the email is decrypted by an S/MIME gateway or S/MIME client, the intended recipient is the only person able to view the message. The recipient can also trust that the message is authentic and unaltered as it is digitally signed by MailMarshal Secure Email Server with your company's Private Key.

SUMMARY AND FURTHER READING

In this paper we have discussed the PKI framework for secure email and how MailMarshal Secure Email Server leverages this technology. We have also explored the traditional objections and limitations around PKI when utilized for large scale secure business collaboration. Finally, we have detailed how MailMarshal Secure Email Server acknowledges and overcomes these issues with smart automation and centralized updates.

MailMarshal Secure Email Server offers a policy-based, centralized and totally seamless secure email solution.

MailMarshal Secure Email Server is accredited for use by the New Zealand Government SEE Mail standard. If you would like more information about the SEE Mail accreditation standards please visit the eGovernment website at http://www.e.govt.nz/services/see/see-mail-prod-cred-2-1.

If you would like to know more detailed information about Public Key Infrastructure, please visit Wikipedia's reference pages at http://en.wikipedia.org/wiki/Public_key_infrastructure.

Additional information on S/MIME is also available on Wikipedia at http://en.wikipedia.org/wiki/S/MIME.

ABOUT M86 SECURITY

M86 Security is a global provider of Web and messaging security products, delivering comprehensive protection to more than 20,000 customers and over 16 million users worldwide. As one of the largest independent internet security companies, we have the expertise, product breadth and technology to protect organizations from both current and emerging threats. Our appliance, software and cloud-based solutions leverage real-time threat data to proactively secure customers' networks from malware and spam; protect their sensitive information; and maintain employee productivity. The company is based in Orange, California with international headquarters in London and offices worldwide. For more information about M86 Security, please visit www.m86security.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit **www.m86security.com/downloads**

M86
™
SECURITY

Corporate Headquarters	International Headquarters	Asia-Pacific
828 West Taft Avenue	Renaissance 2200	Suite 1, Level 1, Building C
Orange, CA 92865	Basing View, Basingstoke	Millennium Centre
United States	Hampshire RG21 4EQ	600 Great South Road
	United Kingdom	Auckland, New Zealand
Phone: +1 (714) 282-6111	Phone: +44 (0) 1256 848080	Phone: +64 (0) 9 984 5700
Fax: +1 (714) 282-6116	Fax: +44 (0) 1256 848060	Fax: +64 (0) 9 984 5720

Version 09.01.09