

# Secure Messaging

Contrary to popular belief, email is not a private or secure means of communication. With normal SMTP email, once you press the SEND button, your email travels over the Internet in an open format and can be read by anyone who puts their mind to intercepting your messages.

Your email travels through Internet Service Providers, routers and other servers on its journey, where it is often copied or logged. Anyone with access to these servers can acquire a copy of your email. Anyone with the will and the know-how can even intercept your message, preventing it from reaching its intended destination. They can then forge the details of the message and forward it on, making it appear that it has come from you or someone else. This process of making email appear as though it has come from another person is known as spoofing.

Spoofing and gaining access to other people's email is much easier than you might think and this is where "secure email" plays a major role.

Secure messaging has two key elements:

1. Encryption – this is the process of making information unreadable to those without special knowledge. The only person who should have the special knowledge, or the key required, to decipher your message is the intended recipient. This renders the message useless and illegible to others.
2. Digital Signing – this is the process of attaching a message with a special

code that is unique to you. The result is that the recipient of a message that bears your unique signature can be assured that the message has come from you. The additional benefits of digital signing are that not only does the recipient know that the message has come from you, they also know the message is unaltered and has not been tampered with.

## Why is Secure Messaging Important?

Email is one of the great technology success stories of the last 20 years. It has grown to become the most common form of business communication today. Email has surpassed the fax and postal mail, and is now relied upon for critical communications thanks to its ease of use, speed and low cost. Email is used for everything from parts orders, to sending contracts and legal documents, to sharing confidential information like patient records, patent applications and business plans.

Sending sensitive information and documents via email is tantamount to sending your most closely guarded secrets on the back of a postcard – anyone that handles the message can read its contents.

There have been many high-profile examples over the years where emails have been leaked or stolen and then turned up in the hands of reporters. Enron is one such example where the company's emails came back to haunt them.

In 2001, a disgruntled customer sent spoofed emails to employees at Samsung Electronics, USA, accusing them of hacking and other crimes. The emails appeared to be sent by Samsung's attorney, causing employees to panic.

Numerous political leaders have been exposed and embarrassed after their private emails were stolen and then used against them.

Secure messaging ensures that messages remain private between the parties concerned and minimizes the risk of confidentiality breaches and data theft. It also creates a high level of trust and assurance that communications are genuine and dependable. Within this framework of secure messaging, organizations can communicate freely and with confidence that unsecured email simply cannot provide.

*Secure messaging ensures that messages remain private between the parties concerned and minimizes the risk of confidentiality breaches and data theft.*



# Secure Messaging

## How does Secure Messaging Work?

In terms of actually encrypting a message between two parties, there are multiple methods of encryption available. These include PGP (Pretty Good Privacy), TLS (Transport Layer Security) and S/MIME (Secure/Multipurpose Internet Mail Extensions). One of the most secure email frameworks is known as PKI (Public Key Infrastructure).

PKI essentially involves asymmetric key pairs known as Public Keys and Private Keys. Company A generates a key pair or is issued a key pair by an authentication authority such as Verisign. Company A retains their Private Key and keeps this private. Company A then posts their Public Key on their restricted website, or issues it to another company that they wish to communicate with securely; Company B for example.

Company A and Company B exchange Public Keys with each other. When A wants to send B a message, Company A will digitally sign the email with their Private Key (no one else has this key, so it is unique to Company A). At the same time, the process of encryption occurs, using the Public Key for Company B. Only Company B will be able to decrypt the message now as only they have the matching Private Key required to decipher the message.

This is the PKI process in simple terms between two companies. In reality there

are a lot of practical complications to this process when it is scaled up to include multiple companies encrypting email to each other. How do you ensure that every email between companies is encrypted? How do you store, maintain and organize keys for other companies? How do you know when keys have expired or been invalidated?

This is where Marshal's solution for secure email comes in, with answers for all of these questions and many more.

## The Marshal Solution for Secure Messaging

Marshal has been developing solutions for secure messaging for more than six years. MailMarshal Secure is used by more than 900 organizations and is one of only two solutions accredited for use by the New Zealand e-Government S.E.E. Program (Secure Electronic Environment).

Marshal has developed solutions to manage keys for hundreds of communication partners and ensure policies for encryption are adhered to. Today, MailMarshal provides one of the most complete, scalable and easy-to-manage secure email solutions available in the world.

Marshal's solutions for secure messaging provide the following features and benefits:

- TLS Encryption – MailMarshal provides a simple option for secure

email in TLS encryption, or Transport Layer Security. Transport Layer Security is a method of email encryption that allows two servers to create a secure SMTP connection between them. TLS is effectively SSL (Secure Socket Layer) for SMTP email connections and ensures that any communications between two TLS-enabled servers remain private and confidential. TLS is easy and cost-effective to establish, providing an ideal way for organizations to communicate securely.

- S/MIME PKI – MailMarshal Secure's S/MIME PKI solution for secure email offers a more robust and scalable framework than TLS. TLS is ideal for organizations that wish to "test the waters" for secure email with one or two other companies. MailMarshal Secure is for when you want to develop trusted communities of secure email partners. Most typically, MailMarshal Secure is used for compliance situations such as HIPAA or adherence to government secure email protocols.

- Policy-Based Secure Email – One of MailMarshal's key benefits is applying a policy-based infrastructure to secure email which is absolutely crucial for compliance. For example, in the case of HIPAA, you may be required to keep any communications between a hospital and a healthcare insurer confidential. With MailMarshal, you can set policies that all emails between the hospital and the insurer must be encrypted and signed. This means no email can be sent unless it is encrypted. You can

*Today, MailMarshal provides one of the most complete, scalable and easy-to-manage secure messaging solutions available in the world.*

# Secure Messaging

also set policy-based standards on the level of encryption – no message shall be sent with less than 168bit Triple DES encryption, for example.

- **Certificate Management** – MailMarshal Secure's most impressive features are arguably in certificate management. Most of the usual pitfalls and disadvantages with PKI are in managing certificates. Certificates are authenticated digital signatures that combine a company's public key with identification credentials. When issued by a certificate authority such as Thawte or Verisign, the certificate is verified accurately by the issuing authority and confirms the company's details as true and accurate. MailMarshal provides multiple advantages in Certificate Management:

- **Community Manager** – Allows you to establish secure email member groups. These groups can then be automatically managed and synchronized via LDAP member lists and certificate stores. This means that all certificate management for the community is centralized, easily maintained and always up-to-date. These communities can consist of hundreds of member organizations. Normally maintaining and exchanging certificates between multiple companies can be a nightmarish task, exponentially multiplied every time you add a new member. But, with MailMarshal, it is as easy as simply adding a new member's certificate details into the LDAP server. All other members then synchronize

with LDAP and have all the latest information required for secure email with the newest member.

- **CRL Support** – CRL, or Certificate Revocation Lists, are part of any sound secure email environment. Industry best practice dictates that certificates should be issued with an expiration date. This helps to ensure that keys cannot be cracked or that compromised certificates can be invalidated. Typically, certificates will be set to expire every 12 months. CRL's are posted lists of certificates that have expired or been compromised. With MailMarshal, when an encrypted message arrives, it is cross-referenced against a CRL. If the certificate is found to be invalid, MailMarshal can quarantine or reject the message, or flag it as untrustworthy and signed with a revoked certificate. When combined with MailMarshal's Community Manager feature, MailMarshal can automatically check for, and retrieve the new certificate from the LDAP server when the old certificate is posted on the CRL. The system maintains itself without any administrative overhead.

- **Certificate Harvesting** – MailMarshal Secure can automatically gather and catalogue digital certificates. It can use information-rich certificates to store options such as update locations, CRL locations, and expiry dates for administrative notifications. Additional functionality allows MailMarshal to identify certificates that are due to expire on a specific date. By default,

MailMarshal Secure will automatically retrieve a new certificate to replace an old one five days before the set expiry date.

- **Content-Based Encryption Policies** – As previously mentioned, MailMarshal can apply secure email in a policy-based framework. This goes beyond assured encryption between companies to the actual content of the message. With MailMarshal, you can set policies that specify any message should be encrypted based on the presence of keywords, files, numerical patterns or sequences such as with social security numbers or credit card numbers. This ensures that no message containing sensitive or confidential information can leave your organization without being encrypted first. This provides significant benefits in achieving compliance with regulations such as HIPAA or SEC Rule 17 a-4.

- **Interoperability** – MailMarshal Secure follows industry standard secure email protocols. This allows MailMarshal to communicate with other compatible S/MIME gateways or clients. MailMarshal Secure also follows standards for the importation and expiration of Public Keys and Certificates, allowing MailMarshal to work with all major certificate authorities.

The Marshal solution for secure messaging is designed to be self-maintaining. Once you have set up

*With MailMarshal, you can set policies that specify any message should be encrypted based on the presence of keywords, files, numerical patterns or sequences such as with social security numbers or credit card numbers.*

# Secure Messaging

your infrastructure and rules for secure messaging, MailMarshal Secure can manage changes with very little manual intervention. If MailMarshal is unable to resolve an issue automatically, it can notify the network administrator or another appropriate party.

There are many reasons to implement secure messaging. Privacy, confidentiality, compliance, protection of Intellectual Property and corporate reputation are perhaps the most obvious reasons. The confidence and trust gained through utilizing secure messaging is also a key advantage.

In addition to this, Marshal's centralized, server-based solution for secure messaging provides other advantages. Management of encryption is far easier and there is no training required for end users. Deployment is simple as there is no need to install software on individual PCs.

Another point to consider is that secure messaging dilutes a lot of other email disadvantages. Spam and phishing messages do not come from secure email partners. Viruses often come in emails with forged details, like an incorrect FROM address. Secure

messaging can help to identify malicious or unwanted email.

Using unsecured email is like playing poker with your cards out on the table for all to see. When you want to keep your cards close to your chest, Marshal provides the solution.

## Why Marshal?

Today, Marshal is the solution of choice for more than 18,000 organizations worldwide, protecting in excess of 7 million users.

- 10 years experience in total content security solutions
- Solutions for companies from 10 to 100,000+ users
- Global 24/7 support team
- TRACE team insights and updates
- More than 40% of the Global Fortune 500 companies rely on Marshal solutions for email and Internet security needs
- More than 60% of the European Fortune Top 50 Companies use Marshal
- 45% of the USA's Fortune Top 170 Companies use Marshal
- 40% of Asia's Fortune Top 50 Companies use Marshal



Marshal's Worldwide and EMEA HQ  
Marshal Limited,  
Renaissance 2200,  
Basing View,  
Basingstoke,  
Hampshire RG21 4EQ  
United Kingdom

Phone: +44 (0) 1256 848080  
Fax: +44 (0) 1256 848060

Email: [emea.sales@marshal.com](mailto:emea.sales@marshal.com)

Americas  
Marshal, Inc.  
5909 Peachtree-Dunwoody Rd  
Suite 770  
Atlanta  
GA 30328  
USA

Phone: +1 404 564 5800  
Fax: +1 404 564 5801

Email: [americas.sales@marshal.com](mailto:americas.sales@marshal.com)  
[info@marshal.com](mailto:info@marshal.com) | [www.marshal.com](http://www.marshal.com)

Asia-Pacific  
Marshal Software (NZ) Ltd  
Suite 1, Level 1, Building C  
Millennium Centre  
600 Great South Road  
Greenlane, Auckland  
New Zealand

Phone: +64 9 984 5700  
Fax: +64 9 984 5720

Email: [apac.sales@marshal.com](mailto:apac.sales@marshal.com)