



# >KEEP EMAILS PRIVATE

>WHY BUSINESSES NEED EMAIL ENCRYPTION



## >CONTENTS

>KEEP EMAILS PRIVATE	>P1
>THE CASE FOR EMAIL ENCRYPTION	>P1
>LEGAL AND REGULATORY CONCERNS	>P2
>APPROACHES TO EMAIL ENCRYPTION	>P3
>MANAGING ENCRYPTION	>P5
>THE SERVICE APPROACH TO EMAIL ENCRYPTION	>P5

## >KEEP EMAILS PRIVATE

An accountant wants to email her clients their tax returns but needs to be sure that no one else can open the attachments. A doctor wants to send an insurance report by email but is nervous about protecting the confidentiality of his client. The Procurement director needs to exchange pricing information with the supply chain but must be sure that this market-sensitive information doesn't leak.

Email is at the heart of business today. The Radicati Group, a technology market research firm, estimated in August 2008 that there are 1.3 billion email users worldwide. In earlier research, they counted 516 million business email inboxes worldwide<sup>1</sup>. It's easy to ground these big numbers in your own everyday experience – just imagine what would happen if your own email link were switched off.

Email may be ubiquitous but it is far from secret. The vast majority of emails are unencrypted which means that they are not secure during transit and can ultimately be read by anyone. With so much at stake, what are the risks of sending unencrypted emails, what are the options for keeping emails private and what are the benefits of the MessageLabs Policy Based Encryption service? This white paper addresses these important questions.

## >THE CASE FOR EMAIL ENCRYPTION

Email encryption addresses three business issues. It reduces the risk of data loss. It helps companies comply with legal and professional requirements. Lastly, it builds trust by demonstrating a company's commitment to data security.

Data loss is in the news. The government seems to lose laptops, CDs and memory sticks with personal data on a regular basis. Businesses face the same risks but perhaps less pressure to go public about each incident. Email is another conduit for data loss. Consider these possibilities:

- Customers assume that the financial information that they share by email with a business is secure, only to learn that their messages have been intercepted, harming the company's reputation.
- A law firm loses business because it can't guarantee that email messages between clients and lawyers are secure.
- Client emails containing medical, legal or tax paperwork fall into unauthorised hands.

<sup>1</sup>Radicati data: [http://email.about.com/od/emailtrivia/f/how\\_many\\_email.htm](http://email.about.com/od/emailtrivia/f/how_many_email.htm)

The risks are obvious:

- Reputation damage through negative PR
- The legal risk that someone might sue you for breach of confidentiality
- Loss of company secrets and intellectual property
- The risk of identity theft or other security problems
- Failure to live up to regulatory requirements

Once it has leaked, data is very hard to put back into the bottle. It can be shared easily online and it is difficult to trace who has seen it or who is responsible for leaking it. For example, information can find its way onto internet sites that are very difficult or impossible to shut down. An ounce of prevention is worth a pound of cure.

Conversely, a proactive approach to data security that embraces email encryption can demonstrate to employees, partners and customers that you value their trust – a valuable business asset. While it may be difficult to quantify, imagine the business benefits of increased trust in your company's email. For example, you could send wage slips, invoices, pin numbers and other sensitive information via encrypted email and save money on printing and postage.

Being able to exchange sensitive information safely is a competitive advantage. It is more efficient for your customers, employees and partners. It is cheaper for you. Using email is also greener than sending things by post. Secure, trustworthy, efficient email could be a key differentiator for companies that use it.

### **>LEGAL AND REGULATORY CONCERNS**

Email privacy is especially important to regulated professions including the legal, finance, medical and insurance sectors. However, in the UK, the Data Protection Act 1998 applies to all businesses. Among other provisions, it requires companies to take appropriate technical and organisational measures against unauthorised or unlawful processing of personal data and to protect against its accidental loss. Companies must take care to make sure that information sent by email is protected in transit.

Besides the risks of legal action arising from wrongful disclosure, the Information Commissioner can issue a very public enforcement notice. For example, in January 2008, the Information Commissioner required that a leading high street retailer encrypt all the hard drives of its laptop computers by April 2008. It almost goes without saying that such a notice would be very damaging to a company's reputation.

Regulation is also a concern. Different professions have different rules and regulations. However, sanctions can be severe. In February 2006, for example, the Financial Services Authority fined one of the UK's largest building societies £980,000 when a computer containing unencrypted customer files was stolen from an employee's home. On a personal level, failure to take reasonable precautions in similar circumstances could be career-limiting, to say the least.

### **>APPROACHES TO EMAIL ENCRYPTION**

Encryption is not just for spooks and the military. It's part of everyday life but it goes unnoticed most of the time. Millions of people use SSL certificates to encrypt ecommerce and other online transactions. Mobile phone conversations are encrypted to prevent eavesdropping and, with the right settings, so are wireless networks.

It is possible to make encryption a seamless and near-invisible part of the email experience. There are different ways to do it and the choice depends on a variety of factors: what you need to protect, the level of control you want, how much time and skill your IT department has and the level of automation you need. There are four main choices:

Desktop vs. gateway.

As the name suggests, with desktop encryption the actual encoding takes place on each user's own PC, typically on a message-by-message basis within the email client and requires desktop software to be installed. This approach gives individual users more flexibility and allows for additional features such as non-repudiation and sender authentication. However, keeping track of encryption keys and enforcing company policies creates headaches for the IT department. Gateway encryption lets IT departments define policies at a corporate level and encrypt emails as they pass through the email system, removing the need for users to decide what to protect. Gateway encryption also makes it easier to implement email archiving, content control and anti-virus protection because messages are not encrypted until they pass through these systems.

## Types of encryption.

Having decided where in the email pipeline to do your encryption, you then have to decide how to do it. There are several encryption protocols, including TLS, S/MIME and OpenPGP. TLS is like a permanent encrypted tunnel between two email systems. S/MIME is supported by many email clients but requires each user to have their own certificate and unique encryption key. (S/MIME Gateway technology can make it easier to manage.) OpenPGP is an open standard based on the commercial PGP encryption protocol. It also requires that individual users have certificates and unique keys. It requires sender and recipient to use compatible versions of the encryption software.

## Push vs. pull.

These encryption options support the “send-to-anyone” capability. Once the email has been encrypted and sent to the recipient, how do they read it? This is the choice between push and pull. With push emails, the encrypted message appears in the recipient’s normal inbox. The push solution requires no special software and has the benefit of storing the encrypted message directly in the recipient’s inbox. With pull emails, the recipient is ‘pulled’ to a secure website to read encrypted messages. The pull option does not require special software either and, in addition, it can support other unique features including automatic expiration of messages and read receipts.

## Software, appliance or service.

The final choice determines how companies implement encryption. An in-house software solution requires dedicated servers, including a Public Key Infrastructure key server, and dedicated software and maintenance. Some vendors pre-package all this technology into stand-alone appliances. This makes it simpler to install and maintain but still requires capital expenditure and in-house technical expertise. The other option, encryption as a service, is the fastest and easiest way to implement encryption. A trusted third party handles the whole process using their servers, eliminating the need for capital-intensive hardware and technical expertise on the client’s premises.

## **>MANAGING ENCRYPTION**

The technology is only part of the puzzle. It raises several management challenges. For the IT department, encryption has a reputation for being difficult both to implement and manage. For example, with a software-based, in-house solution, if a user loses their encryption key, they cannot read their old email. So keeping track of everyone's keys and providing the means to issue replacements is vital, if burdensome. An effective encryption system needs to minimise the burden on the IT department.

Traditional approaches to encryption are not always intuitive and easy to use for non-technical users. Many users who deal with confidential information – call centre workers or frontline medical personnel, for example – may not have the computer skills to use desktop encryption software properly and consistently. What is more, most encryption techniques require that users pre-share their public keys so that they can decrypt one another's emails. This means that both the sender and the recipient have to know what they are doing. Under pressure of time or faced with 'computer problems', users may simply bypass encryption altogether.

To be worthwhile, encryption must work for all users in compliance with all company policies, otherwise it provides a false sense of security. It may be better to know that all your emails are unencrypted than to have some secure and some not, but not to know which is which.

## **>THE SERVICE APPROACH TO EMAIL ENCRYPTION**

The MessageLabs Policy Based Encryption service makes it easy for companies to deploy email encryption. It is an online service that doesn't require any dedicated hardware or expertise on site. Because it is a gateway service, outgoing email is encrypted automatically according to your company's policies. You can decide, for example, that all emails to certain recipients or containing certain words must be encrypted and the MessageLabs service will enforce the policies consistently across every outgoing email.

It integrates seamlessly with other other MessageLabs Email Security Services (including Anti-Spam, Anti-Virus, Content Control) and the MessageLabs Email Archiving Service. It provides full key management, which is completely transparent, with an easy to use web interface for systems administrators to adjust policies. Like other MessageLabs services, there is no upfront capital expense – just an affordable per-user fee.

Senders don't need to do anything to make this happen and they don't require any training or technical skills to use the MessageLabs service.

The recipients will either log into a secure website to read their incoming secure emails or double click the attachment to their email message and enter their password to have the message decrypted for them. Which method is used depends on which option the sending company configured.

MessageLabs Policy Based Encryption service helps you maintain the privacy of your email. It applies your policies consistently to ensure compliance with legislation, regulations and best practice. When customers, employees and business partners see that you value their privacy, it can build trust. It can also enable new email-based opportunities and efficiencies. Email encryption isn't just the right thing to do, it's good for business.

For more information please visit: [www.messagelabs.co.uk/products](http://www.messagelabs.co.uk/products)

>**WWW.MESSAGELABS.CO.UK**  
>**INFO@MESSAGELABS.COM**  
>**FREEPHONE UK: 0800 917 7733**

>**EUROPE**

>**HEADQUARTERS**

1270 Lansdowne Court  
Gloucester Business Park  
Gloucester, GL3 4AB  
United Kingdom  
Tel +44 (0) 1452 627 627  
Fax +44 (0) 1452 627 628  
Freephone 0800 917 7733  
Support: +44 (0) 1452 627 766

>**LONDON**

3rd Floor  
40 Whitfield Street  
London, W1T 2RH  
United Kingdom  
Tel +44 (0) 20 7291 1960  
Fax +44 (0) 20 7291 1937  
Support +44 (0) 1452 627 766

>**NETHERLANDS**

WTC Amsterdam  
Zuidplein 36/H-Tower  
NL-1077 XV  
Amsterdam  
Netherlands  
Tel +31 (0) 20 799 7929  
Fax +31 (0) 20 799 7801  
Support +44 (0) 1452 627 766

>**BELGIUM/LUXEMBOURG**

Culliganlaan 1B  
B-1831 Diegem  
Belgium  
Tel +32 (0) 2 403 12 61  
Fax +32 (0) 2 403 12 12  
Support +44 (0) 1452 627 766

>**DACH**

Feringastraße 9a  
85774 Unterföhring  
Munich  
Germany  
Tel +49 (0) 89 203 010 300  
Support +44 (0) 1452 627 766

>**AMERICAS**

>**HEADQUARTERS**

512 Seventh Avenue  
6th Floor  
New York, NY 10018  
USA  
Tel +1 646 519 8100  
Fax +1 646 452 6570  
Toll-free +1 866 460 0000  
Support +1 866 807 6047

>**CENTRAL REGION**

7760 France Avenue South  
Suite 1100  
Bloomington, MN 55435  
USA  
Tel +1 952 886 7541  
Fax +1 952 886 7498  
Toll-free +1 877 324 4913  
Support +1 866 807 6047

>**CANADA**

First Canadian Place  
100 Kings Street West,  
37th floor  
Toronto, ON M5X 1C9  
Tel+1 646 519 8100  
Fax +1 646 452 6570  
Toll-free +1 866 460 0000  
Support +1 866 807 6047

>**ASIA PACIFIC**

>**HONG KONG**

Room 3006, Central Plaza  
18 Harbour Road  
Wanchai  
Hong Kong  
Tel +852 2528 6206  
Fax +852 2111 9061

>**AUSTRALIA**

Level 6  
107 Mount Street,  
North Sydney  
NSW 2060  
Australia  
Tel +61 2 8208 7100  
Fax +61 2 9954 9500  
Support +1 800 088 099

>**SINGAPORE**

Level 14  
Prudential Tower  
30 Cecil Street  
Singapore 049712  
Tel +65 6232 2855  
Fax +65 6232 2300  
Support +852 2111 3658

>**JAPAN**

Bureau Toranomom 3rd Floor  
2-7-16 Toranomom Minato-ku  
Tokyo 105-0001  
Japan  
Tel +81 3 3539 1681  
Fax +81 3 3539 1682  
Support +852 2111 3658

© MessageLabs 2008  
All rights reserved



Confidence in a connected world.