

White Paper

The next generation of secure email delivery

Andrew Kemshall
Co-Founder SecurEnvoy

Date: April 2008

Email has evolved into one of the most important methods of communication in the business world today, enabling organisations to share information and interact with customers, employees, clients and partners. However, the growth of email traffic has been matched by an increasing security threat, and email has become a serious potential weak spot in corporate IT systems. As a number of high-profile cases in recent months have demonstrated, the exposure of an organisation's most sensitive information can result in financial loss, legal ramifications, and brand damage.

Securing email communication, therefore, has to be a priority for any IT department especially as email, no matter how well protected, is more easily hacked than well-secured web sites. Traditionally, the only way organisations have been able to guarantee that the content of their emails are not intercepted during transition between email servers has been to encrypt the contents using public key infrastructure (PKI). This uses a key to encrypt or "lock" a message, so that only the complementary private key can be used to "unlock" it.

However, what it adds in terms of security, it loses in flexibility. The recipient of the email typically has to pre-enrol for the keys. Both sender and recipient have to agree to mutually trust one or more Certificate Authorities, and both parties have to download and install a root certificate from each of the trusted Certificate Authorities that they choose to use. Once that has been done, they each must create a private key and enrol for their digital certificate. Next they need to exchange their trusted public keys typically by sending each other digitally signed e-mail messages. Finally they may need to setup certificate revocation list checking to block any compromised certificates. Only then can they exchange trusted and encrypted emails.

Not surprisingly, this rather drawn out and cumbersome method of securing emails presents a number of problems. Firstly, you have to know the identity of the person you are sending the encrypted email to and have had prior communication with them. It isn't possible to send email securely to any recipient unless that person has agreed to install a similar technology at their end.

Not surprisingly this is an unrealistic scenario for most business-to-business communication. Aside from the time involved in establishing the framework for exchanging encrypted emails, most individuals don't have the authority to download software on to their desktop and even when they do, with so many different PKI solutions on the market, the chances of them happily co-existing with one another are slim.

Aside from the fact that the average office worker has neither the time nor the interest in managing authentication keys, the other major issue you have with encrypting emails is making sure they get through the recipient's email filter system. Most organisations today have an email content management system to control the huge number of unauthorised spam and virus emails in circulation. As these systems are not capable of decrypting emails they have no way of identifying what they are and whether or not they are safe – and automatically class them as a potential threat. Since organisations simply cannot risk letting an uncontrolled virus into their systems all encrypted content is inevitably blocked or quarantined.

The only way to get round this is for the sender of the email to contact the recipient in advance and let them know they are sending an encrypted email so they, in turn, can alert their IT department that the email needs to be released from the email filter system - hardly a convenient solution, especially for larger organisations.

An alternative to PKI and web-based email encryption is to adapt the idea behind tokenless two-factor authentication to securing emails. To deliver the email securely with this method, the only information required is the recipient's email address and mobile telephone number. The recipient is sent an email which contains a web address where the content of the email is securely stored and a 8 digit PIN (the first factor of authentication). The recipient is then sent a six digit code to their phone via SMS which they must use in order to access that web address.

In this scenario the recipient's mobile phone is used as the second authentication factor to prove they are in fact the person for whom the email is intended.

Using tokenless two-factor authentication to send emails securely overcomes the problem of not knowing the identity of the person you are sending to as there is no need for software to be preinstalled at the recipient's end and no need to exchange a password or secret key. All that is required is their email address and mobile telephone number and there is no issue with the email getting through a spam filter. For the same reason it overcomes all the problems associated with using PKI in large organisations or between a business and its customers.

With all the obstacles organisations have to overcome in order to use PKI or a web-based system to send email securely, and with the growing security risk that email communication presents, it won't be long before organisations look for an alternative, safer and more effective solution. Tokenless two-factor authentication looks likely to be the most obvious alternative.

For more details see SecurEnvoy SecurMail (www.securenvoy.com)