



Seal Your Email™

Combining the Convenience of E-Mail with Complete Client Protection

Email Encryption More Accessible Now for Legal Firms of All Sizes

Are you confident that your email is safe from being read by someone other than you and the person to whom it is addressed? Not sure? In recent studies conducted by email analyst firm Radicati, 97% of business people surveyed were aware that email is insecure. More than two thirds of those surveyed worry about the privacy of email, and the same number agree that they would use email to send confidential information if they had access to email encryption technology.

Stick With Standards

Encryption based on industry trusted public key infrastructure (PKI) standards is undoubtedly the most trusted option for protecting the privacy of email content, but until recently, the cost, complexity and inflexibility of commercially available solutions have kept all but the truly dedicated from making use of them.

“There are many email encryption technologies to choose from,” says Theo Ling, partner and member of the Information Technology/Communications group at Baker & McKenzie, one of the largest global law firms. “The problem is finding a single technology that gives me the ability to exchange email with all of my clients simply, easily and cost effectively.”

New PKI-based encryption products are now being offered by Internet service providers (ISPs), carriers and other large service providers that give everyone an easy and cost efficient option of enclosing email in the digital equivalent of tamper-proof envelopes. As these new encryption products become more prevalent, no longer will we be able to rely on the excuse that encrypting sensitive email is too difficult, or too expensive.

Email Tampering

Email has become one of the most important communications channels for lawyers. Fifteen years ago, when lawyers first started to communicate with clients, the head of IT for law firms small and large warned of the dangers of email. Email travels from the sender to the receiver as a virtual postcard, and as email is stored and forwarded through the Internet, there is a real risk that someone other than the sender or the intended receiver can intercept and either read it or tamper with it. Client-solicitor privilege, liability for breach of confidentiality obligations and damage to a firm's reputation were all reasons originally cited for stopping the use of email at law firms before it even started. Convenience and responsiveness to clients became

justification enough to ignore the basic issue that email was inherently insecure. The standard form disclaimer that we now see at the end of every lawyer's email became the solution to protecting the confidential nature of client-solicitor communications. Is it sufficient today?

Is a Disclaimer Sufficient Protection?

Lawyers decided in the early days of email that there was a commercially reasonable expectation that email would not be read by those not authorized to read it. That was then. Now email is read multiple times by filtering programs that test for viruses and spam. Law enforcement authorities are intercepting email which means that email interception is a generally available capability for anyone interested in email content. The fact is that we use email so much and that email contains vast quantities of sensitive and private information that intercepting email is a lucrative endeavour for hackers. The fact that large volumes of email can be collected, scanned, filtered, read and altered makes email an easier target for illegal interception than regular physical mail. Also, unlike regular mail, you would never know that your email has been intercepted.

Professional Obligation

Everyone should take positive steps to protect this vital communications channel. Lawyers, financial advisors, accountants, educators, health care providers and other professional advisors have ethical, legal and fiduciary duties to protect confidential information of their clients. Lawyers are also subject to their own Rules of Professional Conduct.

Complying with Legislation

Clients too have started to require that lawyers adopt measures to protect the privacy of email communications, either because of common sense, or because of privacy legislation and legislation that generally requires that they take "reasonable measures" to protect the privacy of third party information and ensure the integrity and authenticity of corporate information. The *Heath Insurance Portability and Accountability Act* (HIPAA) is an example of legislation that protects personal information sent amongst health care professionals. The *Sarbanes-Oxley Act* (SOX) governs integrity of financial operations of publicly traded companies. The *Gramm-Leach-Bliley Act* (GLBA) requires that all financial institutions protect customer information. The *California Security Breach Notification Act* (CB 1386) requires disclosure when private personal information of a California resident has been compromised, except if the information was encrypted. Legal reasons aside - doesn't it just make sense to put email into envelopes if it can be done easily and inexpensively?

Encrypting email is a logical, and until recently, a daunting option for protecting the privacy of email communications. "I am looking forward to someday having the digital equivalent of an envelope", says Mr. Ling. "Protecting the privacy of email communications is not easy because of the variety of limited encryption products that

I've seen. We cannot afford to accommodate all of the encryption options that our clients will demand in the long run. A single, effective and ubiquitous solution that is a simple plug-in download to your email client would be dearly welcome.”

Previous Approaches No Longer Sufficient

Protecting files with passwords provides a level of protection, but is often inconvenient and is less secure. Establishing the equivalent of VPN connections to allow the secure movement of email from the law firm to particular client servers is not scalable. Catering to client requests to establish and administer multiple non-standard encryption systems quickly becomes prohibitively expensive.

PKI Email Encryption for the Mass Market

Adopting an encryption mechanism based on standard PKI-based technology and designed with the mass market in mind is the most cost effective and efficient option. PKI-based encryption products also give both the sender and recipient confidence that the email and its content can only be unlocked and read by the intended recipient; that the email was not altered en-route to its destination; and that the sender was in fact the sender.

In a PKI system, each subject user (or principal) is issued a digital certificate for the public key that is used to encrypt a message and/or verify a digital signature on a message; such a key is the public component of a public/private key-pair securely generated by the principal. Until recently, you had to understand the details of PKI to some degree, and had to buy and administer specialized hardware and software. Keys have to be generated, registered, backed up and lifecycle-managed (renewed, re-keyed, re-certified, revoked, etc.); and public keys have to be made available to everyone with whom you want to communicate. Large ISPs (like Verizon), and technology and service providers (like Sun Microsystems and Lucent who operate PKI infrastructure on behalf of Verizon and other well known carriers) now offer secure e-mail services, targeting small and medium businesses, relieving them from the ongoing lifecycle and infrastructure costs for managing keys and certificates. (See: <http://securemail.verizon.net>)

Encryption Doesn't Have to Be Hard to Use

An effective PKI-based encryption product must ensure that the privacy of the email is protected and allow users to send encrypted email to everyone. The products must also be cost effective, easy to use and easy to support. The latest PKI-based encryption products offered by carriers such as Verizon (<http://securemail.verizon.net>) are designed to provide everyone with an email account the ability to send email which is encrypted on the sender's desktop and decrypted by the recipient, without the need for the sender or recipient to know any of the details.

Offered on a subscription basis like anti-virus and anti-spam security products, these products provide a full PKI-based encryption solution without the need for a law firm to acquire and manage expensive equipment and infrastructure software. Lawyers that subscribe for such a service, for example, are not required to change their email address and their firms are not required to interfere with their email infrastructure. Lawyers are able to send “secure email” to anyone, whether or not they are also subscribers to Verizon Secure Mail, without having to exchange credentials or requiring non-subscribers to download specialized software or register for any service.

Existing Products Have Impeded the Adoption of Email Encryption

Traditional encryption products all have their drawbacks.

Firms can establish secure connections with client mail servers on a case-by-case basis. This solution is not scalable and is of limited usefulness because only email from the firm to that particular client is protected.

Hosted encryption solutions that require that users subscribe for a new secure email address, and communicate with the hosted secure email service through a browser using a SSL encrypted connection is inconvenient and of limited use. Such products significantly restrict the way users can send email messages, and create “walled gardens” in which only members can send messages securely to other members.

Gateway or “boundary” solutions consist of hardware and software systems installed at the firm, and at every other entity with which the firm wishes to communicate. Email is routed through these gateways, encrypted, and forwarded on to a compatible gateway on which decrypts the message before sending the unencrypted email on to the intended recipient. These systems are suitable for intra-corporate email communications and not the needs of lawyers who have no control over their clients’ email infrastructure. In addition, email remains open for interception from the sender to the gateway, and from the gateway to the recipient.

Non-standard encryption products have been developed that try to simplify the process of encrypting and decrypting email. These non-PKI based products often fall short of the security and confidence that industry trusted PKI-based solutions offer. In addition, these products may not permit the revocation of subscribers credentials if they have been compromised; email addresses may have to be changed if credentials have been compromised; it may not be possible for a firm to acquire the decryption key for an employee alone; and non-subscribers who receive secure mail messages may be required to register for multiple userids and passwords just to receive secure mail messages.

One last option is to simply have each person who wishes to exchange encrypted email acquire a PKI digital certificate, manually install the certificate in their computer’s certificate store, and then manually exchange public keys with everyone that the user wishes to exchange encrypted email. This option is simply too complicated and a significant administrative burden which to date, has not caught on.

Don't Re-Invent the Wheel

Underlying each of these other solutions is the issue that smaller firms and even larger firms do not have the resources or the desire to build their own encryption infrastructure. “Lawyers should not be expected to build and maintain platforms for managing digital identities nor should they be expected to establish customized secure email links with all of their clients. The cost is just too high, and the complexity of the task is just too great,” explains Mr. Ling. “Subscription products like Verizon Secure Mail which require no upfront investment or ongoing management have got to be the solution. Clients and lawyers alike will benefit by this mass market approach to encrypting email.”

Email Protection for Everyone

Now that email encryption products are being made available to the mass market, we should no longer rely on the outdated excuse that encryption products are too complex and expensive to implement and are therefore not commercially reasonable to adopt. We protect ourselves against viruses and spam, but until recently, have not been offered email encryption products that would justify taking action. Next time you exchange with a client email containing a draft statement of defense, litigation opinion, advice on deal negotiations or other sensitive or privileged information, consider whether it should be placed in a the digital equivalent of a tamper-proof envelope. Carriers, ISPs and trusted technology providers are now offering cost effective email encryption products that are geared to the mass market. Encrypting email is no longer limited to rocket scientists.

About the Author

Chris Erickson, P.Eng, LLB
Executive Vice President, Echoworx Corporation

Chris Erickson obtained a BAsC degree in Computer Engineering from the University of Waterloo, and an LLB from the University of Toronto Law School. Prior to joining Echoworx, Mr. Erickson was President and CEO of Tira Wireless. Previously, he founded and served as President and General Counsel for 724 Solutions, and practiced law at Fasken Martineau.