

Secure Mail as a Service By Keith Pasley, CISSP

One of the biggest challenges to the increased use of encrypted email is the sheer complexity of it all. Designing and managing a secure email infrastructure includes anti-virus, antispam / content management, secure web mail, DNS protection, and related policy. However, a potentially high value opportunity that is often missed by enterprises is the use of encrypted email. While there are many approaches to encrypting email, they all have drawbacks. One of the most glaring challenges to wider use is ongoing management of the cryptologic elements of the system. The basic legwork of receiving requests for user certificates, processing the requests, issuing certificates, revoking expired certificates, and providing a revocation list to users software agents. Add to this list the administrative overhead of distributing the authority down an organizational hierarchy for a decentralized approach. And then there is hardware and software to be bought. There are operating systems licenses, application software licenses, maintenance licenses, cost of training of employees, network infrastructure equipment and servers that may be purchased. All of this represents a potentially large up front costs to get started with an encrypted email system.

Increased security regulations by governments, litigious society, high costs of recovery from cyber attacks, and competitive pressures are some contributors to recent interest in encrypted email. As in most everything in the IT world, there are two basic choices of deployment to consider, build it yourself or subscribe to a service provider. The build it yourself approach described earlier does not work for all businesses. However, for those businesses that require an out-sourced service provider option, there are alternatives.

The Co-Mail secure mail service, offered by Ireland based NR Lab LTD, provides a web based secure email system that anyone can use. Co-Mail implements the concept of a virtual server. The virtual server concept allows for assignment of physical email file space being divided into logical separate parts of the platform file system, a sort of apartment house analogy.

The web based user and administrator interface proved to be user friendly, highly intuitive, well-documented, and well thought out with the user in mind. Supported browsers include Netscape Navigator/Communicator and Internet Microsoft Explore. Security professional will especially interested in the application and system level security components employed by the service. The outstanding design and implementation leaves little to be desired from a security perspective. The use and proper implementation of well-known security protocols, such SSL and OpenPGP (RFC 2440), provides additional confidence and credibility to the service. Details of the cryptologic framework employed by the service is available online at <http://www.co-mail.com/data.html>. Briefly, operational security characteristics of the service are impressive. They include:

1. All messages carry 1024-bit DSA digital signatures
2. Automatic encryption of emails and attachments.
3. Automatic electronic signature.
4. Web-interface session protection
5. Secure file storage
6. File protection
7. Password change
8. Virtual keyboard (to prevent keyboard logging and other recording of activity)
9. iKey support
10. Encrypted email storage

The Co-Mail services designed to provide communities of users, large and small enterprises to communicate securely via encrypted email with strong user authentication and high data integrity. A company email administrator would sign up for the service by pointing a browser to the Co-Mail registration web page. After completing registration and entering an activation code a company is ready to login and start using the service. Offers one month free trial with 10 mailboxes.

Initial email policy configuration is web based, simple, and intuitive. From the web-based administrative interface can be viewed the service statistics, by both service and by user. Logo / branding can be applied by an upload feature of the administrative interface. The domain defaults to company_name.co-mail.com but can be changed to reflect an existing domain or a company can register for a brand new domain name through partnerships held by the Co-Mail service. Help information provided in surprisingly through detail such that special knowledge about mail box configuration and operations is encapsulated within the actual screens. A handy feature for users is the option to drop a shortcut to the service onto the user desktop for easy access.

User registration is a snap. There are two ways a user mail box can get registered and configured: 1) administratively or 2) user created. In the case of an admin initiated mail box creation, the admin would establish a new user name, generate the secret keys (via random mouse movements), and create the user pass-phrase. All of this is accomplished in two three insanely easy steps. The administrator can then notify the user of the creation and login information for the new mail box. The second method for creating a new mail box is to let the actual users register and create mail boxes themselves. Of course, appropriate user authentication is mandatory. From a management perspective, Co-Mail administrative interface is at once very informative yet ridiculously easy to manage, almost infinitely scalable, and quite response over the web.

The user-initiated approach may be appropriate in such cases where there is a large user community or in the case of integrating into a human resource process. In any event, the process starts with the administrator authorizing and sending an email to the user's current mail box with instructions on accessing the service. The user is also sent a time-based expiring URL pointing to the same registration page as was used by the admin. This time, though, the end user has

to cooperate to get the mailbox set up using the same insanely simple two step process.

Another handy component of the Co-Mail service is the optional mail client, Co-Mail Express. Co-Mail Express lays a bridge between a user's favorite e-mail client program and the corporate mail server. Co-Mail Express automatically encrypts/decrypts all incoming and outgoing data, automatically configures the member's favorite mail client to work with the company mail system via POP/SMTP, and shows statistics of the user's communications. Co-Mail Express also can protect, via encryption, any files on the user's desktop or removable disks. Supported platforms include Windows 95/98/Me/2000/NT/XP™ or Linux.

The administrator can have the Co-Mail Express software installed on user PCs in order for them to be able to access Co-Mail using their favorite email clients such as Outlook, Eudora and others. Again, there are two distribution methods, administrative sending of the executable as attachment through the corporate Co-Mail environment using the included address book or by sending to the file to any discrete email address. Co-Mail provides customizable user instruction text. This is another helpful element to make setup easier at the same time lowering the amount of administrative busy work.

Co-Mail Express can be configured to download and install in one step. Co-Mail Express then effortlessly installs on the user's computer without any user significant user intervention or need for special knowledge. A short cut is installed on the user's Windows Desktop for easy, quick access.

As for user experience, easy to learn interface and uncluttered are words that immediately come to mind. However, the user interface does pack a decidedly strong punch, in terms of capabilities. For starters, the Co-Mail provides the user with directly accessible encrypted file storage, the ability to verify signatures of both the sender and the message, option to save attachments in encrypted form right after downloading, automatically open the file after save, or the combination of both. The user's private key is used to encrypt or decrypt a file on the users computer. However, the private key cryptographic functions reside on the Co-Mail servers. A benefit of this is, potentially, increased security with the separation of key and target file. An attacker would have to subvert the Co-Mail servers that store the users private key. However, a drawback is the potential of wide scale access to secret key if the Co-Mail servers that store the private key is subverted. Thanks to airtight security of the Co-Mail application environment, there is a very low probably of attacker success in this regard.

Additional features include user controlled anti-spam capability, user mail box address book export function, a option to specify a preferred language (great for businesses with international-based users), and the usual mail box user-based administrative house keeping items. Users can also be assigned on-line **file** storage space via Co-Mail's secure storage platform, S-Mail. However, there is a separate fee for using this service. What

Overall, Co-Mail answers the challenge of getting more users comfortable with using encrypted email as a service. In today's competitive market, with companies looking for top line and bottom line productivity, Co-Mail secure email service provides an out-sourced model that takes the cost, and the fear out secure email systems. It does this by providing low up front costs (\$1/user/per month), fast and simple implementation, no appreciable user technical expertise needed, and flexible branding options and reliable service. The backend cryptologic framework is based on server implementations of OpenPGP and SSL.

The diagram illustrates the Co-Mail architecture. At the center is the 'Co-Mail server' (Mail.your-company.com) with 'Secure disk storage' and 'Co-Mail Express software'. It connects to 'Your company's branch' (employee1@your-company.com, employee2@your-company.com, employee3@your-company.com) and 'Your company's partner' (your-partner@your-company.com). Both branches use 'Co-Mail Express software' and a 'WEB interface'. A 'Manager@your-company.com' is also shown with a 'WEB interface' for 'Remote access'.

The screenshot shows the 'Secure mail admin interface' in Microsoft Internet Explorer. The address bar shows 'https://mail.co-mail.com/admin/workplace.html'. The page title is 'ADMIN INTERFACE'. The navigation menu includes 'Home', 'New user', 'Co-Mail Express', 'Options', 'Shortcuts', 'Logout', 'Print', and 'Support'. The main content area is titled 'Corporate mail: summary information' for domain 'kpassociates.co-mail.com'. It contains a table with the following data:

Maximum number of accounts on a corporate mail server:	10
Total number of users (including incomplete registrations):	10
Number of accounts (completed registrations only):	10
Number of active accounts (used at least once):	4
Average number of messages:	0.200
Average message size:	0.836 Kb

On the left, there is a 'Users' list with a tree view showing 'k' (kpasley) and 'u' (user10 through user9). On the right, there is an 'F.A.Q. for administrator' section with 6 questions and answers.