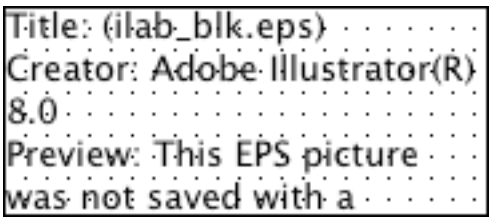

How do I use Certificates with Email?

There are two ways that most people use certificates and PKI with their email. The first way is at the session level, when your mail reader connects to the mail server, with SSLv3/TLS. You can run the popular standardized email protocols SMTP, IMAP, and POP all over SSLv3/TLS. This secures and protects your data stream so that no one can eavesdrop on your mail, but does not secure the mail on the mail server. The second way is by doing end-to-end encryption of your email message using a standard such as S/MIME or a product such as PGP. This protects your message at all times.

You may want to use either one or both of these techniques to protect your email, depending on your needs. The table below shows some common threats and the best technology to protect them.

Someone stealing your IMAP or POP password	SSL/TLS
Someone reading your mail as you download it over the Internet	SSL/TLS
Someone reading your mail as it is transported over the Internet	SSL/TLS or S/MIME
Someone reading a very important message at any time, even after you've read it	S/MIME
Someone pretending to be someone you know via email	S/MIME
Your ISP reading your mail	S/MIME

What is S/MIME?

S/MIME (Secure/Multipurpose Internet Mail Extensions) can be used by email user agents to provide authentication (by signing) and privacy (by encrypting) for email messages. In the iLabs we are showing S/MIME as implemented by Netscape, Microsoft, and Baltimore Technologies (as a plug-in to Eudora).

How does S/MIME compare to PGP?

PGP (Pretty Good Privacy) provide fairly similar capabilities to S/MIME. One of the many differences in implementation is that S/MIME relies on the use of the X.509 format for certificates and PGP uses a unique PGP format for certificates. In the iLabs we are demonstrating public key infrastructures based on X.509 certificates, so we are showing S/MIME.

How does S/MIME signing work?

S/MIME is based on public key technology. That is, a person's private key can decrypt what the public key has encrypted and vice versa. To sign a message, the sender computes a cryptographic hash (checksum) of the message and encrypts the hash with the sender's private key. The recipient, knowing the sender's public key can decrypt the hash and verify that the hash is indeed correct for the message received. If that matches, only the correct sender could have signed the message.

How does S/MIME encryption work?

A random encryption key (called the 'session key') is chosen by the sender application to encrypt the message to be sent. The sender, knowing the recipient's public key, can encrypt the session key so that only the recipient can decrypt the session key and then use that key to decrypt the message. The reason for the extra step with the extra (session) key is because symmetric encryption algorithms, such as DES, are much more efficient than public key algorithms, such as RSA. To be more efficient in encrypting large messages, symmetric algorithms are used first.

How do I sign an email message using Netscape 4?

Let's assume you already have your certificate and private key stored for Netscape. In a Composition window, click the padlock icon. The Security Info window displays information about digitally signing this message. Check the option to sign the message and select [OK]. When you actually send the message, you may be prompted for the password that you chose to protect your private key.

How do I encrypt an email message using Netscape 4?

In a Composition window, click the padlock icon. The Security Info window displays information about whether you can encrypt this message. Select the option to encrypt the message if you already have certificates for all of the recipients or follow the instructions for getting a recipient's certificate. Netscape will give you the option to look up the recipient in an LDAP directory. However, the easiest way to obtain a recipient's certificate is to have the recipient first send you a signed message. The recipient's certificate will be included in the signed message and Netscape will store the certificate for you to use later.

How do I decrypt or verify a signature on a received message?

Netscape does this automatically for you. When you open a message with Netscape, it will display an icon in the upper right corner of the message window and will specify if the message was signed, encrypted or both. To decrypt the message, Netscape may have to ask you for the password that you chose to protect your private key.

How do I see what certificates Netscape has stored that can be used to encrypt email?

Open the Security Info window by clicking the padlock icon, select Certificates, then People. Choose a certificate from the list, then click View/Edit, Verify, or Delete.