

Re: OE Encryption

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.inetexplorer.ie6_outlookexpress/2006-03/m

- *From:* "Vanguard" <vanguard.news@xxxxxxxxxxxxx>
 - *Date:* Wed, 22 Mar 2006 12:30:01 -0600
-

"Dennis_H" <DennisH@xxxxxxxxxxxxxxxxxxxxxxxxxxxxx> wrote in message
news:A680FB8D-FC9A-47EA-A7AC-1C78B3A3701C@xxxxxxxxxxxxxxxxxxxx

How difficult is it to encrypt something?

"Dennis_H" wrote:

Any help out there on encryption with OE? Do I need a digital signature. Are there any that are free?

To sign a message (this is NOT the same as adding a signature text string at the end of your message):

– Add the cert to your outbound message. It will include identification of your cert (so others can do a lookup on it, automatically or manually, to get info on the sender). It will also include your public key which will be needed by anyone who wants to send you an encrypted message.

To encrypt a message:

– To send an encrypted message to someone else, you need that someone else's public key (from their cert). That is because they will use their private key to let them decrypt your message.

– To have someone else send you an encrypted message, you need to send them your public key. They use your public key to encrypt their message and you use your private key to decrypt it.

The public key is, well, public. You distribute it to whomever you want to allow to send you encrypted messages. The public key cannot be used by itself to decrypt a message. The private key is required for decryption. You give your public key to someone else by sending them a digitally signed message (so it includes the cert with the public key). They then have to save and use your public key. They cannot send you encrypted mails (that you can decrypt) unless you gave them your public key.

Since you are divulging a key to the public (to the recipient and whomever else may intercept the message or to whomever the recipient gives your public key), obviously it would not be a secure mechanism if everyone could use your public key to decrypt your messages. You keep your private key to yourself and it is the second half of the pair of keys needed to decrypt a message. If only one key were needed for encryption and decryption, how could you give out that key and know that only you could decrypt a mail that used that key?

Re: OE Encryption

That's why 2 keys are needed that are paired together: the public one you give out for others to encrypt messages that they send you (and which allows no one to decrypt the message), and the private one that you use to decrypt the message.

Once you get the certificate installed in your e-mail client, all you have to do is select an option to encrypt your message using the recipient's certificate that you must've saved from a prior digitally signed e-mail that they sent to you. If you don't have their public key, you cannot encrypt a message that you send to them. Once the cert is installed, you can digitally sign any or all of your e-mails. Usually you get the option to add the cert on a per-item basis or to enable a global option to always add your cert to your outbound mails. There is usually little need to enable the global option since it will be rare when you need or want to digitally sign your outbound mails. The Thawte cert only provides identification by e-mail address. The recipient still doesn't know who you are but only what is your e-mail address, and what good is that e-mail only identification if you are using a freebie Hotmail or Yahoo e-mail account which doesn't require trackability (by following the money) or registration (other than a confirmation e-mail)? Even if you buy a full cert that contains all your ID details, or you use Thawte's web-of-trust mechanism to get more details added, the info only shows what you claimed was true when you got the cert. Certs are nice but they don't provide 100% proof of identity, but neither does any other form of ID.

Adding a digital signature to every outbound e-mail adds bloat to each one. There may also be lookup problems, like the recipient's e-mail client cannot automatically find and query the CA (certificate authority) for your cert and reports the problem which makes the recipient wonder about the authenticity of your cert. Whether you always add a cert to your outbound mails depends on whether the e-mail is for business or personal. It will be infrequent when you use a cert for personal e-mails. The cert added for business e-mails may not even identify you as the sender but is instead one that was assigned to your company. You never divulged WHY you *think* you need to encrypt your e-mails.

Post replies to the newsgroup. Share with others.
For e-mail: Remove "NIX" and add "#VN" to Subject.
