

## Using PGP TrustCenter's Digital Certificates with Microsoft Outlook 2003

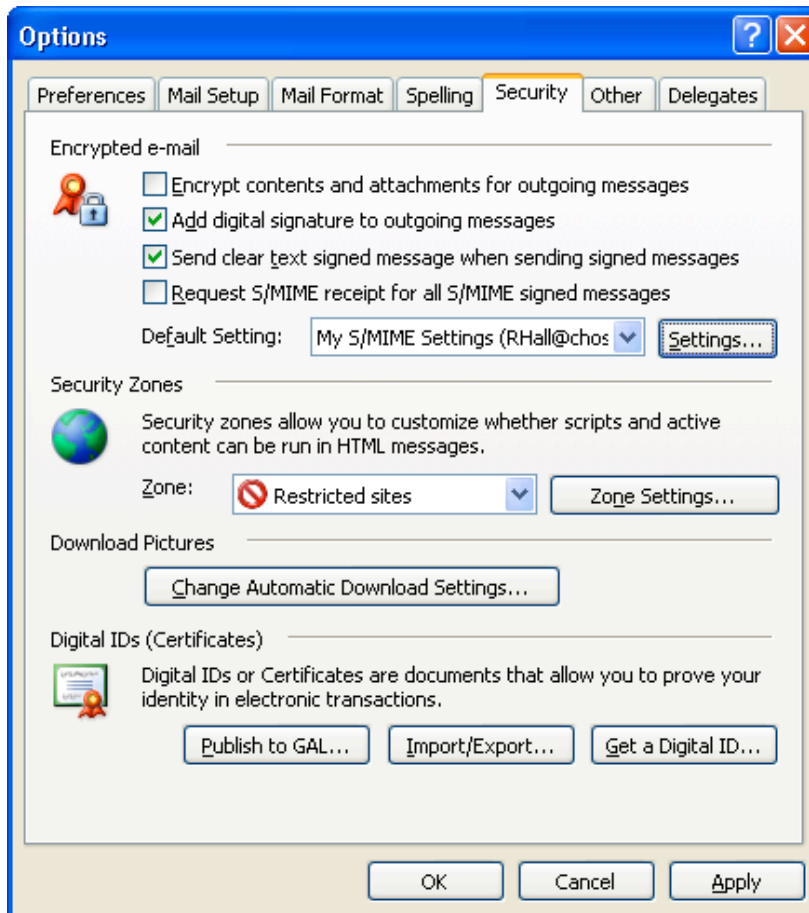
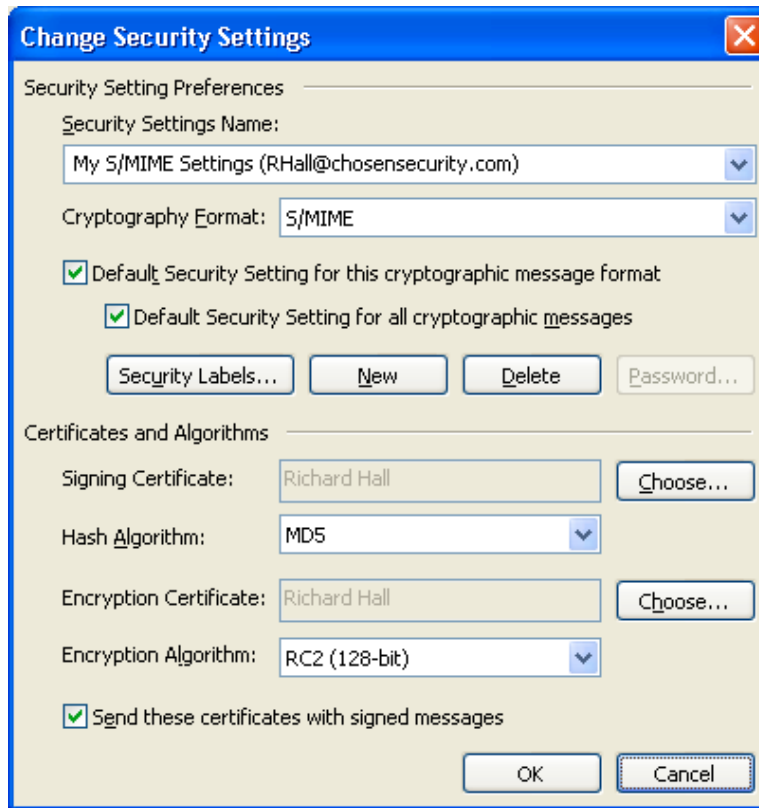
---

To use any of the security features in Outlook, you must first configure the program to use your digital certificate. If you do not already have a digital certificate, please visit PGP TrustCenter's website at <http://www.pgptrustcenter.com/digital-certificate-solutions> to obtain a "TC Personal ID" or "TC Business ID".

### Configuring Outlook 2003

After you have your digital certificate with private keys installed, you need to configure Outlook to use the certificate by following these steps:

1. Click Tools, and then click Options.
2. Click on the Security tab and click Settings.
3. Outlook populates the Change Security Settings dialog box with default information.  
**Note:** If a user has more than one digital certificate in the local computer store, you must specify which digital certificate you want Outlook to use. To specify the certificate, under Certificates and Algorithms, click both Choose buttons.
4. Click the option to "Send these certificates with signed messages". This allows the recipients of your messages to easily verify your message with your public key.
5. Click OK to close the Security Settings options.
6. If you would like to automatically encrypt all outgoing messages, click the option to "Encrypt contents and attachments for outgoing messages".
7. If you would like to automatically sign all outgoing messages, click the option to "Add digital signature to outgoing messages".
8. Choose the option to "Send clear text signed message when sending signed messages".
9. Click OK to Close the Options dialog.

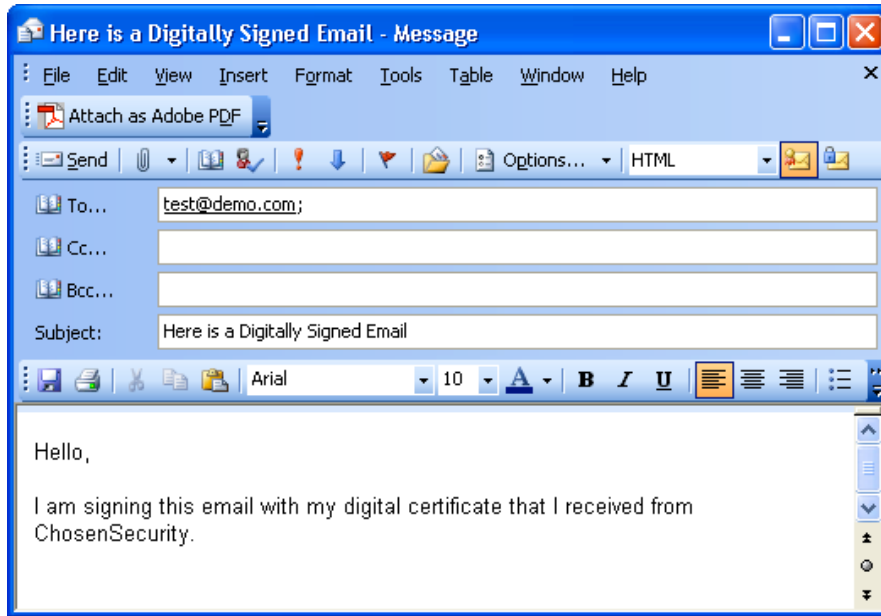


## Digitally Signing an Email

To digitally sign an email, you can use either of the following methods:

- Have Outlook 2003 automatically sign all messages each time you compose, reply to, or forward a message (see step 7 in the section titled "Configuring Outlook 2003").
- Click the Digitally Sign Message button. This button is displayed as an envelope with a red ribbon.

When you click send, Outlook signs the message using your private key and sends the message.

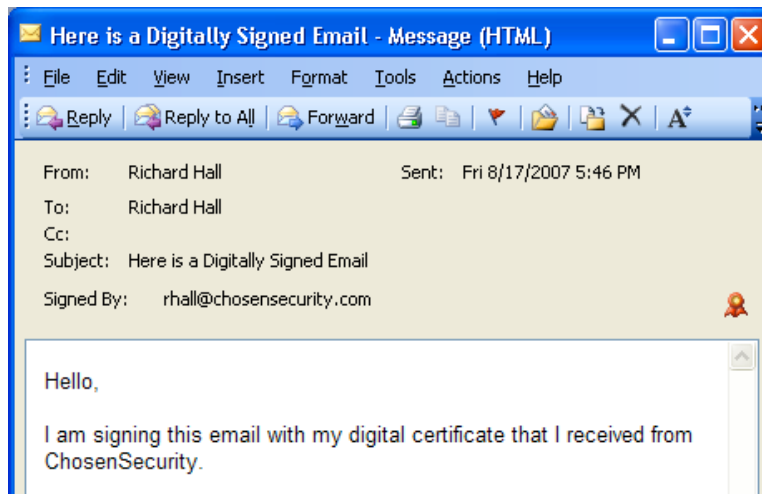


The recipient must have your public key to verify that the digital signature on your message is trustworthy. Others cannot use your public key to send messages with your digital signature.

If the recipient's e-mail client is not S/MIME aware, the public key certificate appears as a file attachment with a .p7s extension. If the e-mail client is S/MIME aware, there is no visible enclosure.

## Receiving Digitally Signed Emails

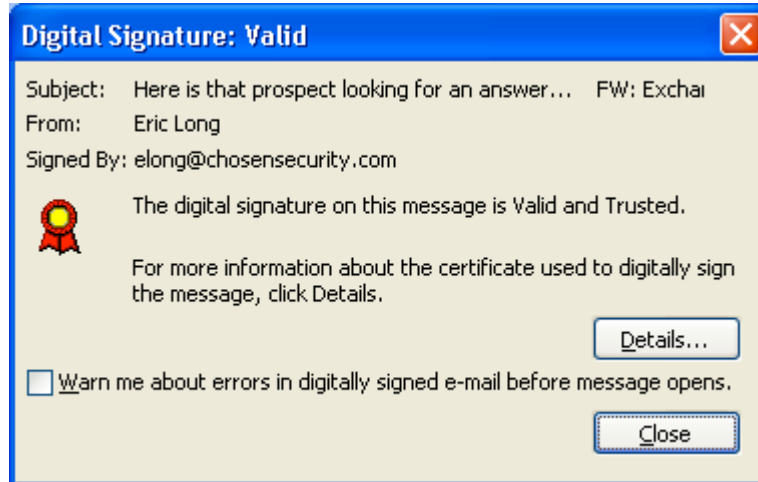
When you receive a digitally signed email, there will be a "Signed by" field below the Subject line. The email will also have a red certificate on the email to show that it has a valid signature.



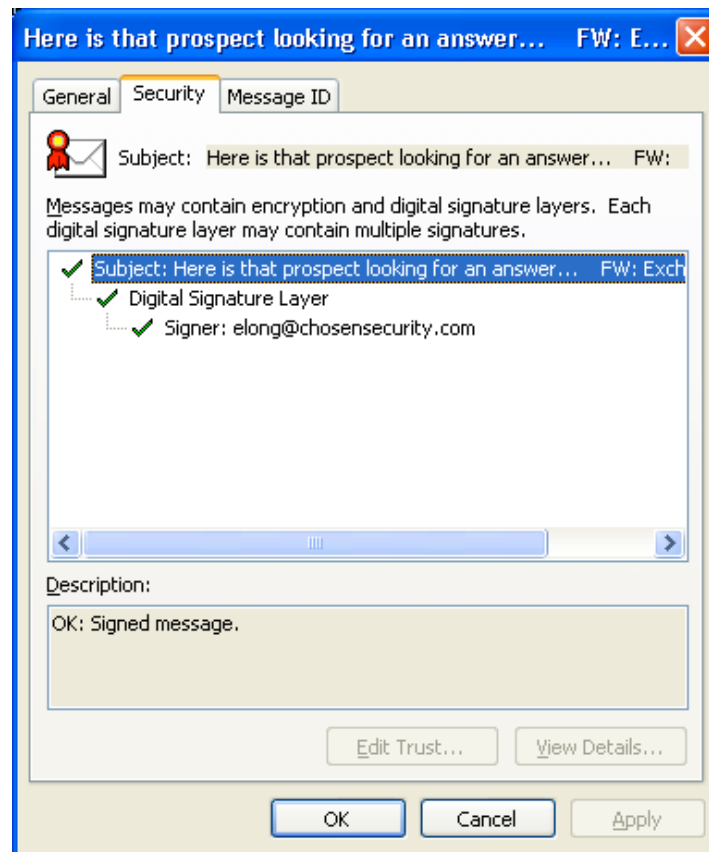
## Verifying a Digitally Signed Message

The recipient must have your public key to verify that the digital signature on your message is trustworthy. This will not be an issue if you have included the certificate with your message as was instructed in step 4 in the section entitled "Configuring Outlook 2003". Digital Signatures are done with your private keys, and therefore others cannot use your public key to send messages with your digital signature.

A digitally signed email can be verified by clicking on the red certificate icon within the message.

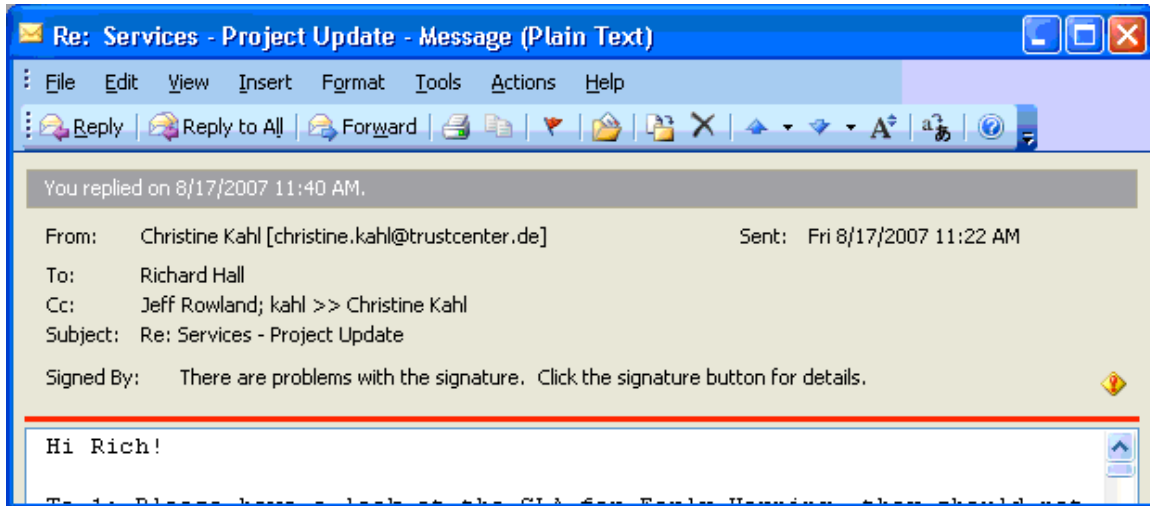


Another way to verify the signature of an email is to open the email and click on Properties from the File menu. Clicking on the Security tab will display the digital signature validity information.

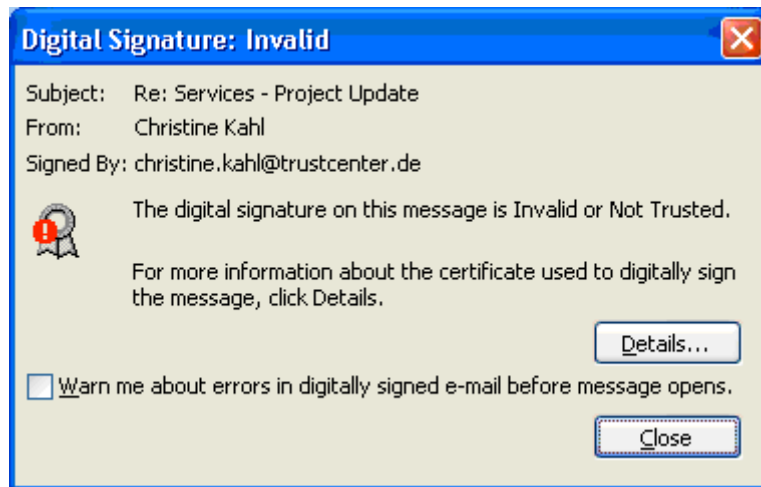


## Receiving Invalid or Un-trusted Signed Emails

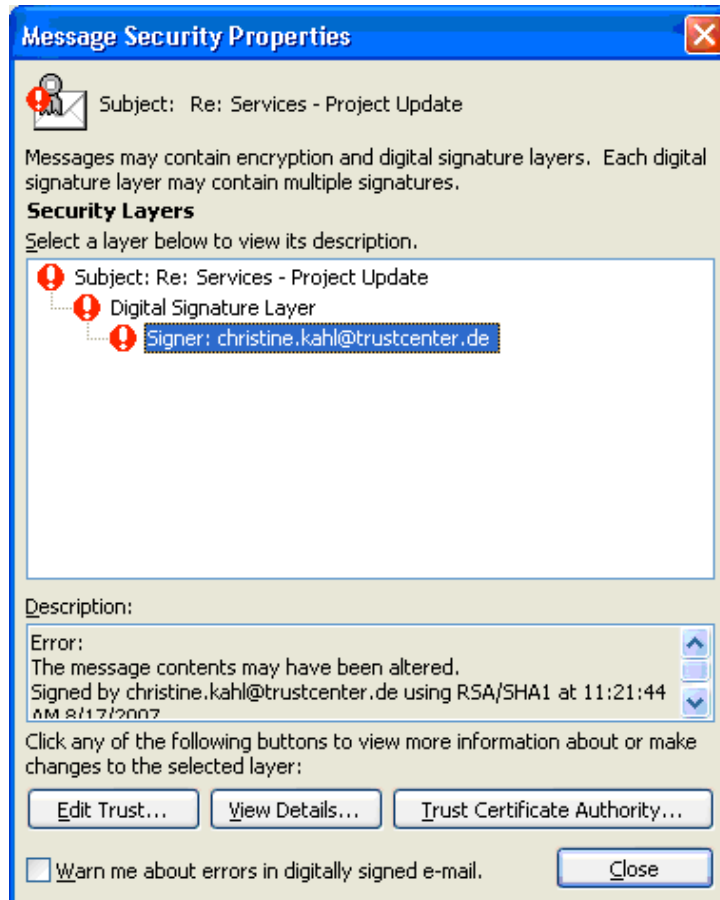
If a digitally signed email is not signed by a trusted certificate, or the certificate is invalid, the message will warn with a message displaying "There are problems with the signature. Click the signature button for details".



Clicking on the warning icon (yellow diamond with a red exclamation mark) will show that the signature is invalid or not trusted.



Clicking on the details button will allow you to see the details of the message as well as the corresponding certificate that was used to sign the email. If you are confident that this email sender and their certificate should be trusted, you can add edit the trust levels accordingly.



## Adding a Certificate to the Address Book

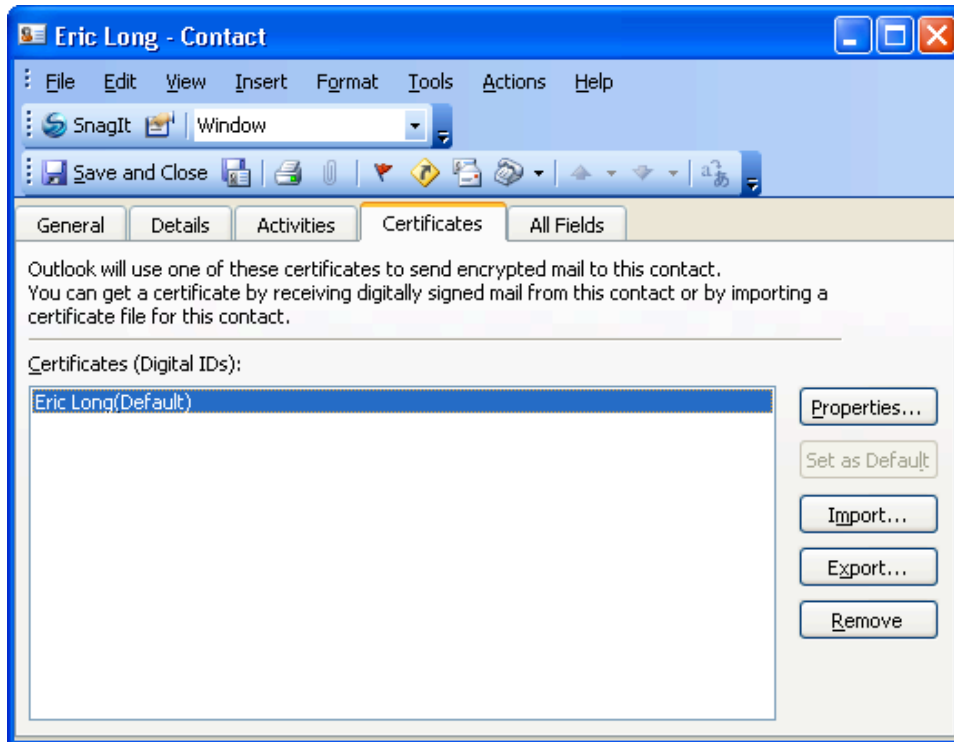
In order to send encrypted mail, you must obtain the other person's certificate (public key) and import it into your address book.

Here are two ways to obtain a person's public key:

- If the intended recipient also has a certificate that was issued by PGP TrustCenter, you can look up the other person's public key by visiting PGP TrustCenter's Web site, searching for the correct person under "Certificate Services", and installing the certificate. This lookup service is available at the following URL: <http://www.pgptrustcenter.com/certificate-services>.
- You receive a digitally signed message that includes the sender's certificate (public key).

To manually add a person's certificate to your address book from a signed message you receive (method 2), follow these steps:

1. Open the message.
2. Right-click on the recipient's name, and choose "Add to Outlook contacts".
3. Any associated certificates will be automatically saved. Click on the "Certificates" tab to verify the presence of a digital certificate.
4. Click "Save and Close".



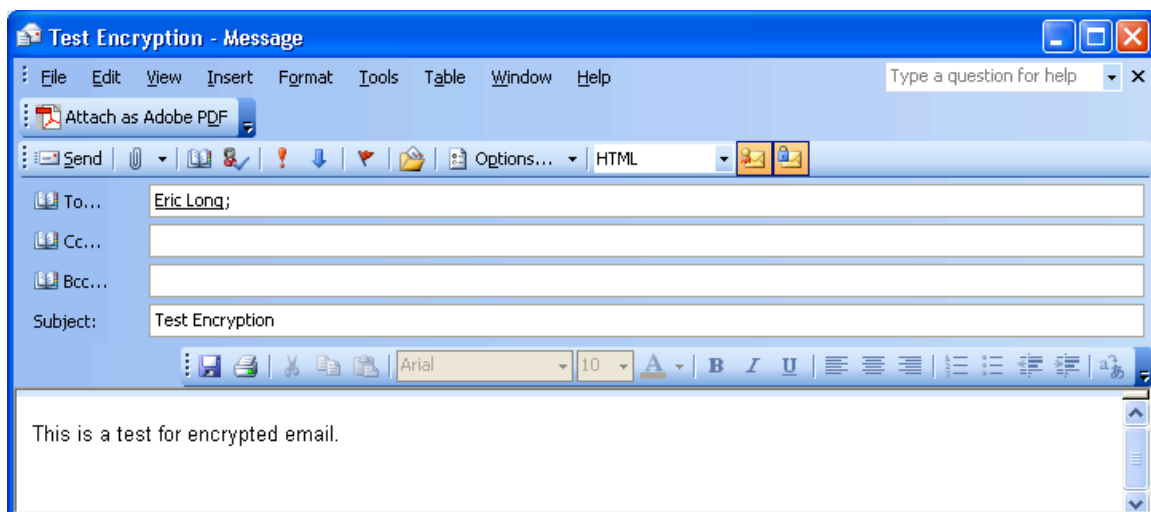
## Encrypting a Message

To encrypt a message so that only the recipient can decrypt the message, you need the recipient's certificate (public key) in your address book and the trust relationship set to Trusted By Me. See the section titled "Adding a Certificate to the Address Book" for information about these items.

One way to encrypt a message is to have Outlook automatically encrypt all messages each time you compose, reply to, or forward a message (see step 14 in the section titled "Configuring Outlook").

Another way is to click the Encrypt Message button on the toolbar. This button displays an envelope with a blue padlock icon.

When you click send, Outlook encrypts the message using a secret key, encrypts that key with the recipient's public key, and sends the message.

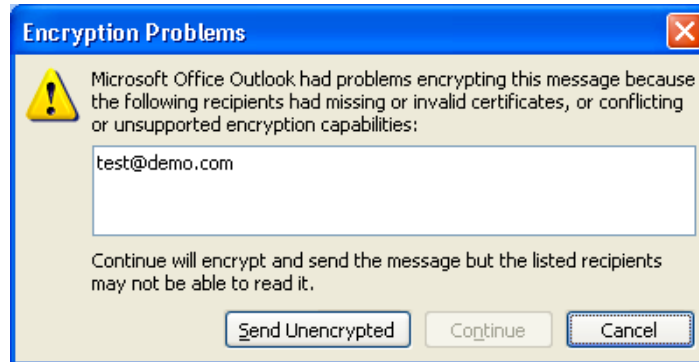


## Errors Received When Sending Encrypted Messages

If you send an encrypted message and you do not have the public key for one or more of the recipients, Outlook displays the following security warning message:

Microsoft Office Outlook had problems encrypting this message because the following recipients had missing or invalid certificates, or conflicting or unsupported encryption capabilities:  
<list of recipients>

Continue will encrypt and send the message but the listed recipients may not be able to read it.



## Receiving Encrypted Emails

When a received message is encrypted, a blue padlock appears on the email. Encrypted emails are not displayed within Outlook's Reading Pane, and must be fully opened in order to read the encrypted contents. An encrypted email may be verified by clicking on the padlock. For more encryption details, highlight the "Encryption Layer" property.

