

Using PGP TrustCenter's Digital Certificates with Microsoft Outlook Express v4 and v5

To use any of the security features in Outlook Express, you must first configure the program to use your digital ID (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 Express

After you have your private key (digital ID) installed, you need to configure Outlook Express to use the certificate by following these steps:

1. On the Tools menu, click Accounts.
2. Click the Mail tab, click the mail account in which you want to use a digital ID, and then click Properties.
3. On the Security tab, click the "Use a digital ID when sending secure messages from <e-mail address>" check box to select it, and then click Digital ID.
4. Click the appropriate certificate, click OK, click OK, and then click Close.
5. On the Tools menu, click Options.
6. On the Security tab, click Advanced Settings.
7. Click the option to "Include my certificate with signed messages". This allows the recipients of your messages to easily verify your message with your public key.
8. If you want to specify an encryption algorithm other than RC4 40-bit, click the appropriate option.
9. Click OK.
10. If you want to automatically digitally sign all outgoing messages, click the "Add digital signature to all outgoing messages" check box to select it.
11. If you want to automatically encrypt all outgoing messages, click the "Encrypt contents and attachments for all outgoing messages" check box to select it.
12. Click OK, and then click OK again.

Digitally Signing a Message

To digitally sign a message, you can use either of the following methods:

- Have Outlook Express automatically sign all messages each time you compose, reply to, or forward a message (see step 7 in the section titled "Configuring Outlook Express").
- Click the Digitally Sign Message button. This button displays an envelope with a red ribbon. You can also click Digitally Sign on the Tools menu.

When a message is digitally signed, a red ribbon appears to the right of the Subject line. When you click send, Outlook Express signs the message using your private key and sends the message.

If you do not have your private key installed on your computer, Outlook Express displays the following message:

**The message could not be sent.
You cannot send digitally signed messages because you do not have any certificates. (OK)**

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.

You can include your public key with the message (see step 4 in the section titled "Configuring Outlook Express") or you can send your certificate files as an attachment. 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.

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 7 in the section entitled "Configuring Outlook Express". Digital Signatures are done with your private keys, and therefore others cannot use your public key to send messages with your digital signature.

If you do not have the sender's certificate (public key) imported into your address book, Outlook Express displays the following security warning message:

The certificate used to sign this message is either not listed in your Address Book or marked as not trusted by you.

Continue to open this message?

If you have the sender's public key imported into your address book and the certificate is marked as Not Trusted By Me, Outlook Express displays the following security warning message:

You do not trust the certificate used to sign this message.

Continue to open this message?

Adding a Certificate to the Address Book

To be able to verify a sender's digital signature or to send encrypted mail, you must obtain the other person's certificate (public key) and import it into your address book.

There are two ways to obtain a public key:

- Look up the other person's public key by visiting PGP TrustCenter's Web site, searching for the correct person under the Certificate Services section within the Resource Center, and installing the certificate.
- You receive a digitally signed message that includes the sender's certificate (public key).

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

1. Click the message to select it.
2. On the File menu, click Properties, and then click the Security tab.
3. Click "Add the certificate to the address book."
4. Click OK

The default trust relationship for new certificates is Not Trust. To use the certificate, change the trust relationship by following these steps:

1. On the Tools menu, click Address Book.
2. Click the person's entry to select it, and then click Properties.
3. Click the Certificates tab.
4. Click the certificate, and then click Properties.
5. On the General tab, click Trusted By Me in the Trusted box.
6. Click OK, click OK, and then click Close on the File menu to close the Address Book.

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 Express automatically encrypt all messages each time you compose, reply to, or forward a message (see step 8 in the section titled "Configuring Security Features in Outlook Express").

Another way is to click the Encrypt Message button on the toolbar. This button displays an envelope with a padlock. You can also click Encrypt on the Tools menu.

When a message is encrypted, a round gray icon with a white padlock appears to the right of the Subject line. When you click send, Outlook Express 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 many of the recipients (including yourself, the sender), Outlook Express displays the following security warning message:

You do not have a certificate. If you send this message, it will be sent properly, but you will not be able to read it in your sent items folder. Send anyway? (Yes/No)

If you try to read a message when you do not have the private key for one of the recipients (including yourself, the sender), Outlook Express displays the following message:

Your certificate is not listed among those that can decrypt this message. You cannot read it.

When you click OK, Outlook Express displays one of the following messages:

This message failed to display correctly in the Preview Pane.

- or -

One or more of the messages could not be opened.

If you do not have the recipient's public key in your address book, Outlook Express displays the following message:

You do not have valid certificates in the Address Book for the following recipients:

<list of recipients>

You must resolve the certificate problems listed above before you can send this message (Try Again).

Additional Notes

Each time you view a message that has been altered since it was sent, you receive a warning notification. The option to not notify you again applies to the current message only.

Some mail servers rewrite messages before sending them out. These messages are displayed as altered when received; it does not mean that someone has maliciously altered the message. If you receive many altered messages, check with your mail administrator to see if your mail server is causing the problem.