

Using PGP TrustCenter's Digital Certificates with Microsoft Outlook 2007

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 2007

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

1. On the **Tools** menu, click **Trust Center**, and then click **E-mail Security**.
2. Under **Encrypted e-mail**, click **Settings**.

Note: If you have a digital ID, the settings to use the digital ID are automatically configured for you. If you want to use a different digital ID, specify the digital ID by following the remaining steps in this procedure.

3. At the bottom of the **Security Setting Preferences** section, click **New**.
4. In the **Security Settings Name** box, enter a name.
5. In the **Cryptography Format** list, click **S/MIME**. Depending on your certificate type, you can choose Exchange Security instead.
6. Next to the **Signing Certificate** box, click **Choose**, and then select a certificate that is valid for digital signing.

Note: To learn if the certificate is intended for digital signing and encryption, on the **Select Certificate** dialog box, click **View Certificate**. An appropriate certificate for cryptographic messaging (such as digital signing) might say, for example, "Protects e-mail messages."

7. Next to the **Encryption Certificate** box, click **Choose**, and then select a certificate that is valid for encryption.
8. Select the **Send these certificates with signed messages** check box unless you will be sending and receiving signed messages only within your organization.

Note: The settings that you choose become the default whenever you send cryptographic messages. If you do not want these settings to be used by default for all your cryptographic messages, clear the **Default Security Setting** for all cryptographic messages check box.


Digitally Signing Emails

By digitally signing a message, you apply your signature to the message. The digital signature includes your certificate and public key. This information proves to the recipient that you signed the contents of the message and not an imposter, and that the contents have not been altered in transit.

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

1. **Digitally sign on a per message basis**
2. **Digitally sign all messages**

1. Digitally signing on a per message basis

1. In the message, on the **Message** tab, in the **Options** group, click the **Digitally Sign Message** button .
2. Compose your message and send it.

2. Digitally sign all messages

1. On the **Tools** menu, click **Trust Center**, and then click **E-mail Security**.
2. Under **Encrypted e-mail**, select the **Add digital signature to outgoing messages** check box.
3. If available, you can select one of the following options:

If you want recipients who don't have S/MIME security to be able to read the message, select the **Send clear text signed message when sending signed messages** check box. This check box is selected by default.

To verify that your digital signature is being validated by recipients and to request confirmation that the message was received unaltered, as well as notification telling you who opened the message and when it was opened, select the **Request S/MIME receipt for all S/MIME signed messages** check box. When you send a message with an S/MIME return receipt request, this verification information is returned as a message sent to your Inbox.

4. To change additional settings, such as choosing a specific certificate to use, click **Settings**.

Encrypting Emails


Encrypting an e-mail message in Microsoft Office Outlook 2007 protects the privacy of the message by converting it from readable plaintext into ciphered (scrambled) text. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message.

In order to send encrypted messages over the Internet, you need to exchange certificates with the recipient. You can do this in a number of ways:

- Send a digitally signed message. The recipient adds your e-mail name to Contacts and in doing so, also adds your certificate.
- Send an e-mail message with your .cer file attached. The recipient can import the .cer file into your contact card.
- Create a contact card with your .cer file, and send the contact card.
- Publish your certificate to an LDAP directory or another directory that is available to the other person.
- Post the certificate on a share that is available to the other person.
- If your system administrator has set up security for your network using Microsoft Exchange, it is not necessary to swap certificates.

To setup Encryption with email, follow the steps below:

1. Encrypt a single message

1. In the message, on the **Message** tab, in the **Options** group, click the **Encrypt Message Contents and Attachments** button .
2. Compose your message and send it.

2. Encrypt all messages

1. On the **Tools** menu, click **Trust Center**, and then click **E-mail Security**.
2. Under **Encrypted e-mail**, select the **Encrypt contents and attachments for outgoing messages** check box.
3. To change additional settings, such as choosing a specific certificate to use, click **Settings**.
4. Click **OK** twice.

Adding a Recipient's Certificate to your Contacts

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 a message that has been digitally signed.
2. Right-click the name in the **From** box, and then click **Add to Outlook Contacts** on the shortcut menu.
3. If you already have an entry for this person, in the **Duplicate Contact Detected** dialog box, select **Update information of selected Contact**. A backup copy will be saved in Deleted Items Folder.

The certificate is now stored with your contact entry for this recipient. You can now send encrypted e-mail messages to this person.

To view the certificate for a contact, double-click the person's name, and then click the **Certificates** tab.

Digitally Signing Outlook 2007 Macro Projects

To digitally sign macro projects, follow the steps below:

1. Open the file that contains the macro project you want to sign.
2. On the **Tools** menu, point to **Macro**, and then click **Visual Basic Editor**.
3. In the Visual Basic Project Explorer, select the project you want to sign.
4. On the **Tools** menu, click **Digital Signature**.
5. Do one of the following:
 - If you haven't previously selected a digital certificate or want to use another one, click **Choose**, select the certificate, and then click **OK** twice.
 - To use the current certificate, click **OK**.

Notes:

Sign macros only after your solution has been tested and is ready for distribution, because whenever code in a signed macro project is changed in any way, its digital signature is removed. However, if you have the valid digital certificate that was previously used to sign the project on your computer, the macro project is automatically re-signed when you save it.

If you want to prevent users of your solution from accidentally changing your macro project and invalidating your signature, lock the macro project before you sign it. Your digital signature says only that you guarantee that the project has not been tampered with since you signed it. Your digital signature does not prove that you wrote the project. Therefore, locking your macro project doesn't prevent another user from replacing the digital signature with another signature. Corporate administrators can re-sign templates and add-ins so that they can control exactly what users can run on their computers.

If you create an add-in that adds code to a macro project, your code should determine if the project is digitally signed and should notify the users of the consequences of changing a signed project before they continue.

When you digitally sign macros, it is important to obtain a timestamp so that other users can verify your signature even after the certificate used for the signature has expired. If you sign macros without a timestamp, the signature remains valid only for the validity period of your certificate.