Using Entrust certificates with Microsoft Office and Windows
Using your Entrust certificate with Microsoft Office applications

This chapter describes how to use your certificate with Microsoft Office applications, such as Microsoft Word, Excel, PowerPoint, and Outlook.

This guide assumes you already have an Entrust certificate. For instructions on obtaining a certificate from Entrust Managed Services PKI, see one of the following guides available from the Resources tab on www.entrust.com/managed_services based on your role. If you are an:

- administrator, see the Entrust Managed Services PKI Administrator Guide
- end-user, see one of the following based on your organization’s deployment:
  - Getting an Entrust certificate using Entrust Authority Administration Services
  - Getting an Entrust certificate using Entrust Entelligence Security Provider

This chapter includes:

- “Signing and sending messages using Microsoft Word, Excel, or PowerPoint” on page 4
- “Sending secure messages Using Microsoft Outlook” on page 6
- “Configuring Outlook to use a single certificate (if you have multiple certificates available)” on page 10
- “Removing message encryption in Outlook (Security Provider for Outlook users only)” on page 13
Signing and sending messages using Microsoft Word, Excel, or PowerPoint

This topic describes how to use your Entrust certificate to sign and send messages using Microsoft Word, Excel, or PowerPoint.

This topic includes:

- “Signing a document created using Word, Excel, or PowerPoint” on page 4
- “Sending a secure message from Word, Excel, or PowerPoint” on page 5

Signing a document created using Word, Excel, or PowerPoint

Once you have an Entrust certificate, you can use it to sign documents created using Word, Excel, and PowerPoint.

Complete the following procedure to sign a Microsoft Office document.

**To sign a Microsoft Office document**

1. Based on your version of Microsoft Office, complete one of the following procedures:

<table>
<thead>
<tr>
<th>Microsoft Office version</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Microsoft Office 2002 and 2003</strong></td>
<td>1. Select <em>Tools &gt; Options</em>.</td>
</tr>
<tr>
<td></td>
<td>2. Click the <em>Security</em> tab and click <em>Digital Signatures</em>.</td>
</tr>
<tr>
<td></td>
<td>The <em>Digital Signatures</em> dialog box appears.</td>
</tr>
<tr>
<td></td>
<td>3. Click <em>Add</em>.</td>
</tr>
<tr>
<td></td>
<td>4. Select a certificate from the list presented.</td>
</tr>
<tr>
<td></td>
<td>5. Enter your password, if prompted.</td>
</tr>
<tr>
<td><strong>Microsoft Office 2007</strong></td>
<td>1. Click the Microsoft Office button in the top-left of the page.</td>
</tr>
<tr>
<td></td>
<td>2. Select <em>Prepare</em>.</td>
</tr>
<tr>
<td></td>
<td>3. In the menu presented, select <em>Add Digital Signature</em>.</td>
</tr>
<tr>
<td></td>
<td>4. On the <em>Sign</em> dialog box, click <em>Sign</em> to add your signature.</td>
</tr>
<tr>
<td></td>
<td>5. Enter your password, if prompted.</td>
</tr>
</tbody>
</table>
If you change a signed document, all digital signatures become invalid or are removed.

Sending a secure message from Word, Excel, or PowerPoint

Windows applications typically have an option available from the menu bar for sending a document as an e-mail attachment. You can use your digital ID to send secure message attachments.

Depending on the version of Office you use, do one of the following in Microsoft Word, PowerPoint, or Excel.

To secure a message from Word, Excel, or PowerPoint
1. Open the Windows program, such as Word, Excel, or PowerPoint.
2. Based on your Microsoft Office version, complete one of the following:

<table>
<thead>
<tr>
<th>Microsoft Office version</th>
<th>Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Office 2002 and 2003</td>
<td>1 Select File &gt; Send To &gt; Mail Recipient (as Attachment). A message window appears.</td>
</tr>
</tbody>
</table>
| Microsoft Office 2007             | 1 Click the Microsoft Office button in the top-left of the page.  
                                         2 Select Send.  
                                         3 Select E-mail. A message window appears. |
|                                   | 3 Add recipient addresses and message text.                                 |
|                                   | 4 Click the Encrypt and/or Sign icons.                                     |
|                                   | 5 Send the message.                                                       |

Other applications have a similar send option.
Sending secure messages Using Microsoft Outlook

In Microsoft Outlook, you can secure a single email message, or configure Outlook so that all messages you send are automatically encrypted and/or signed.

If you have Security Provider for Outlook installed, you can also send and receive secure messages while offline through the certificate caching feature.

This topic includes the following:

- “Securing a single email message in Microsoft Outlook” on page 6
- “Configuring Microsoft Outlook to send all messages securely” on page 7
- “Sending and receiving secure email in offline mode (Security Provider users only)” on page 8

Securing a single email message in Microsoft Outlook

You can use your Entrust certificate to secure sensitive email using Microsoft Outlook’s built-in feature.

Note: If Security Provider for Outlook is installed, Encrypt and Sign icons appear on the New, Reply, Reply to All, Forward, Drafts, and Outbox message windows in Outlook.

Complete the following procedure to secure a single message in Microsoft Outlook.

To secure a single email message in Microsoft Outlook

1 Encrypt and/or sign your email using one of the following methods:
If you... | Do this...
---|---
If you... | Do this...

do not have Security Provider for Outlook installed and want to use Microsoft Outlook’s built-in encryption and signing feature  | 1. Compose your message in Outlook.  
2. From your message window menu bar, click Options. Alternatively, from the toolbar, select View > Options.  
3. From the Message Options dialog box, click Security Settings.  
4. From the Security Properties dialog box, select one or both of the following based on your requirements:  
   • Encrypt message contents and attachments  
   • Add digital signature to this message  
5. Click OK.

have Security Provider for Outlook installed | 1. Compose your message in Outlook.  
2. From your message window menu bar, click Encrypt to encrypt the message and Sign to add your digital ID.

---

**Configuring Microsoft Outlook to send all messages securely**

If you want all messages you sent to be automatically encrypted and/or signed, configure Microsoft Outlook according to the procedure below.

**To configure Microsoft Outlook to send all messages securely**

1. Open Microsoft Outlook.  
2. Select Tools > Options and click the Security tab. 
   The page under the Security tab appears.
3 Under **Encrypted e-mail**, select one or both of the following options:
- Encrypt contents and attachments for outgoing messages
- Add digital signatures to outgoing messages
4 Click **OK**.

**Sending and receiving secure email in offline mode (Security Provider users only)**

Certificate caching is a feature of Security Provider for Outlook.
Security Provider for Outlook works behind the scenes to help create a local cache of certificates belonging to your e-mail recipients like this:

- When you receive an encrypted message, Security Provider for Outlook validates that sender’s certificates, and stores them on your computer.
- When you send a message to a distribution list, Security Provider for Outlook stores each of the recipients’ certificates locally.

With this cache, you can compose secure messages for your regular recipients while working offline.

When you go back online after a period of offline use, synchronize your recipient cache in Outlook by selecting Tools > Send/Receive > Synchronize Certificate Cache. A progress dialog box appears. This operation also removes expired certificates in the cache.

When you send a message, Security Provider for Outlook does the following:

1. It looks in your local cache for a valid certificate for each recipient.

2. If a valid certificate is not found, Security Provider for Outlook checks in the remote directory assigned to you as part of Entrust Managed Services PKI.

3. If more than one valid certificate for a recipient exists, the Select Certificate dialog box appears. You must select the certificate to use.

4. Security Provider for Outlook checks that the e-mail address in the recipient's certificate matches the e-mail address of the recipient in the message. If they do not match, the E-mail Mismatch Address Warning dialog box appears. You can view the certificate. You can choose to send the message despite the mismatch; however, the recipient may not be able to decrypt the message.

5. When Security Provider for Outlook cannot locate a recipient's certificate, the Cannot Find Certificates dialog box appears. You have two choices:
   - Select Remove the recipients and send the message to remove all recipients whose certificates cannot be found. The message is sent encrypted to remaining recipients.
   - Select Send the message unencrypted to all recipients to send the message to all recipients unsecured.
Configuring Outlook to use a single certificate (if you have multiple certificates available)

If you have more than one encryption or signing certificate, you can configure Outlook so that all secure messages you send use specific certificates and algorithms.

To configure Microsoft Outlook messages for specific certificates and algorithms

1. Open Microsoft Outlook.
2. Select Tools > Options and click the Security tab. The page under the Security tab appears.
3 From the **Encrypted e-mail** section, click **Settings**.

The **Change Security Settings** dialog box appears.
4 Click **New** on the dialog box. All fields clear.
5 Give your new security profile a name.
6 Choose both a signing and encryption certificate.
7 If your configuration allows it, you can choose a different signing and encryption algorithm from the drop-down lists.
8 To make this profile your default, select **Default Security Settings for this Secure Message Format**.
9 Click **OK**.
Removing message encryption in Outlook
(Security Provider for Outlook users only)

To make messages easier to read and available for searching, you can permanently decrypt Microsoft Outlook messages.

**Note:** This feature is only available if you installed Security Provider for Outlook.

To decrypt Microsoft Outlook messages permanently

1. In Outlook, select an encrypted message, but do not open it.
2. Select **Actions > Unsecure Selected Message**.
   A progress dialog box appears. You may see warnings that you are about to remove a digital signature.
   This action also removes any message signature.
Using your Entrust certificate with Windows

This chapter describes how to use your Entrust certificate with Windows. This chapter includes the following topics:

- “Securing files in folders” on page 16
- “Sending a secure message from a folder” on page 20
Securing files in folders

Once you have an Entrust certificate, you can encrypt, digitally sign, or encrypt and sign any file. Only you can read a file you encrypt.

To encrypt and/or sign a document

1. Navigate to the folder containing the file or files you want to secure.
2. Right-click the file(s).
   A menu appears.

---

![Menu Options](image)

- **Open**
  - New
  - Print
  - Save As...

- **Convert to Adobe PDF**
- **Convert to Adobe PDF and EMail**
- **Combine in Adobe Acrobat...**

- **Entrust Encrypt File...**
- **Entrust Digitally Sign File...**
- **Entrust Encrypt and Digitally Sign File...**

- **IZArc**

- **Scan for Viruses...**
  - Open With
  - TextPad

- **Send To**

- **Cut**
- **Copy**

- **Create Shortcut**
- **Delete**
- **Rename**

- **Properties**
Choose one of the following options:

- Encrypt File
- Digitally Sign File
- Encrypt and Digitally Sign File

A wizard specific to the option you selected opens listing the files you selected.

Click Next.

Depending on which wizard you opened, a page appears that lets you choose signing and/or encryption certificates, and signing (hashing) and/or encryption algorithms.
5 Select **Next** to accept the default settings, unless you have a clear need to change a certificate or algorithm.

6 If you installed Security Provider, you are asked to enter your Entrust security store password. This is the password you provided when you enrolled for, or updated, your certificate through Security Provider. (This password page may not appear if you entered your password recently as part of another security operation.)

A completion page appears listing your secured files.
7 Make sure the **Delete the original files on finish** option is selected so that your original, unsecure files are deleted.

8 Click **Finish**.
Sending a secure message from a folder

Windows folders typically have an option available from the context menu for sending a file as an e-mail attachment. You can use your certificate to send secure messages, if your e-mail client supports this operation.

To send a secure message from a folder

1. Navigate to the folder containing the file(s) you want to send.
2. Right-click the file(s).
   A menu appears.

<table>
<thead>
<tr>
<th>Open</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
</tr>
<tr>
<td>Print</td>
</tr>
<tr>
<td>Save As...</td>
</tr>
<tr>
<td>Convert to Adobe PDF</td>
</tr>
<tr>
<td>Convert to Adobe PDF and EMail</td>
</tr>
<tr>
<td>Combine in Adobe Acrobat...</td>
</tr>
<tr>
<td>Entrust Encrypt File...</td>
</tr>
<tr>
<td>Entrust Digitally Sign File...</td>
</tr>
<tr>
<td>Entrust Encrypt and Digitally Sign File...</td>
</tr>
<tr>
<td>IZArc</td>
</tr>
<tr>
<td>Scan for Viruses...</td>
</tr>
<tr>
<td>Open With</td>
</tr>
<tr>
<td>TextPad</td>
</tr>
<tr>
<td>Send To</td>
</tr>
<tr>
<td>Cut</td>
</tr>
<tr>
<td>Copy</td>
</tr>
<tr>
<td>Create Shortcut</td>
</tr>
<tr>
<td>Delete</td>
</tr>
<tr>
<td>Rename</td>
</tr>
<tr>
<td>Properties</td>
</tr>
</tbody>
</table>
3 Select **Send To > Mail Recipient**.
   
   An email message window appears.

![Emailing: Sys_prefs.pdf - Message (Plain Text)](image)

   The message is ready to be sent with the following file or link attachments:

   `Sys prefs.pdf`

   Note: To protect against computer viruses, e-mail programs may prevent sending or receiving certain types of file attachments. Check your e-mail security settings to determine how attachments are handled.

4 Add recipient addresses and message text.
5 Click the **Encrypt** and/or **Sign** icons.
6 Send the message.