IdenTrust
part of HID Global

Using a Digital Certificate in Microsoft® Outlook 2010 or Later to Digitally Sign and Encrypt Emails

If you have a digital certificate, you can use it to digitally sign and encrypt emails. IdenTrust digital certificates that can be used for this application include:

- DoD ECA certificates
- IdenTrust TrustID® certificates
- IdenTrust Global Common (IGC) certificates
- GSA ACES certificates (which can *only* be used to digitally sign emails)

When you are using Microsoft Outlook 2010 or later as your email client, you will need to first configure Outlook to use your digital certificate. This document includes instructions on how to:

- Install a digital certificate into Microsoft Outlook.
- Use a digital certificate once installed to digitally sign and encrypt email.

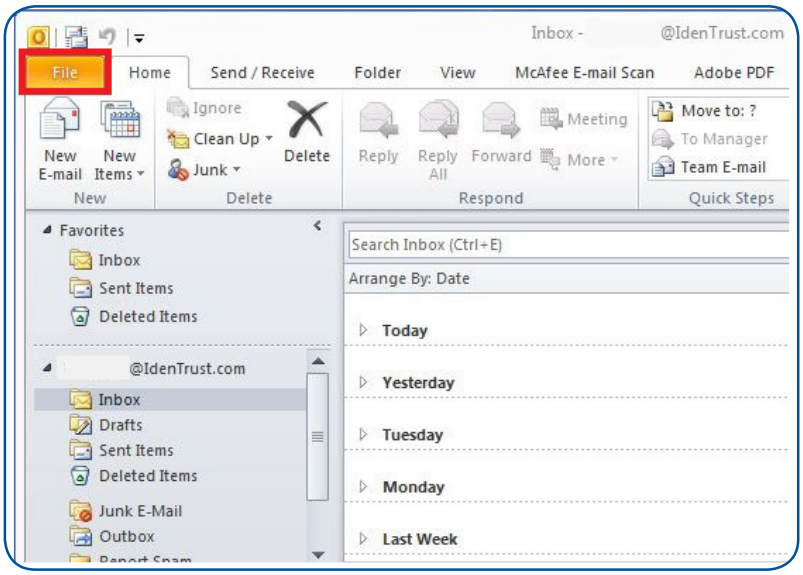
These instructions assume that:

- The certificate is already installed into Windows (Internet Explorer) on the same computer.
- You have Outlook 2010 or later; the certificate installation process differs slightly for Outlook 2003 and Outlook 2007.

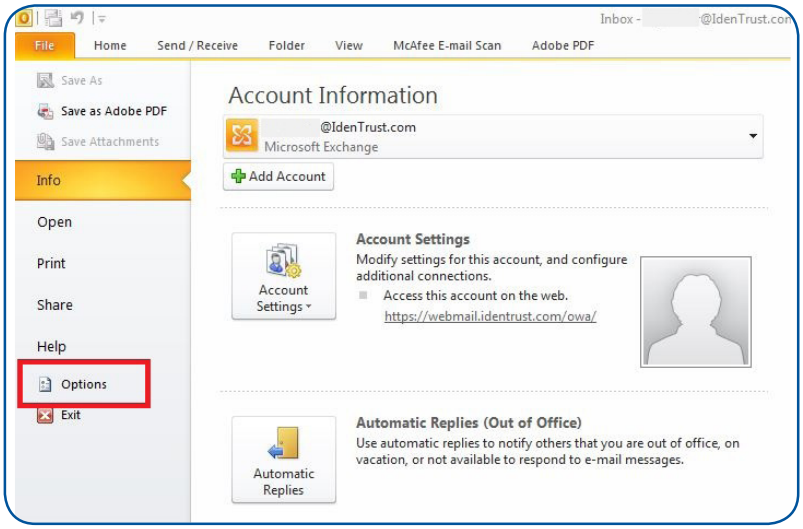
Now let's get started!

1. First you must have your digital certificate installed on your computer.
2. Once you have your digital certificate installed, you should open Outlook.

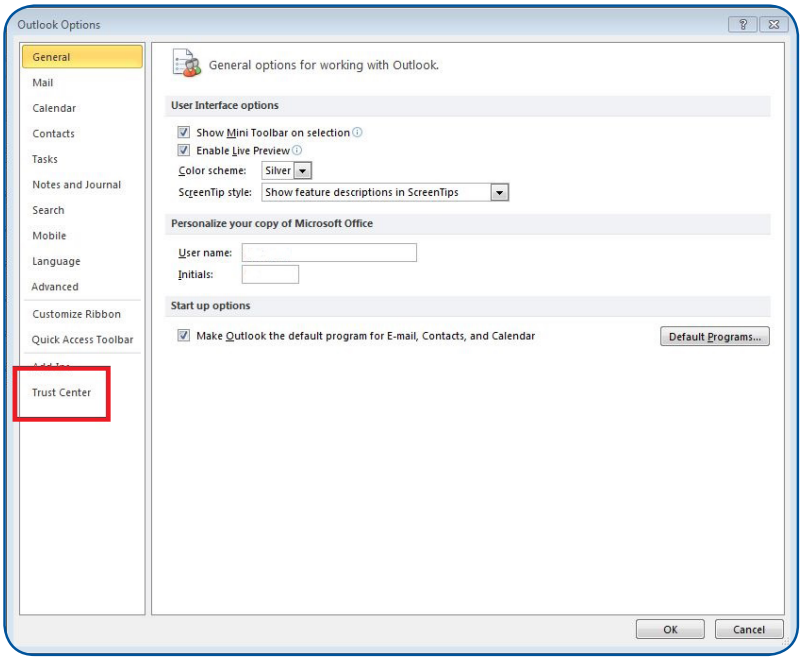
3. Once Outlook is opened, click on the **"File"** tab in the top left corner of the page.



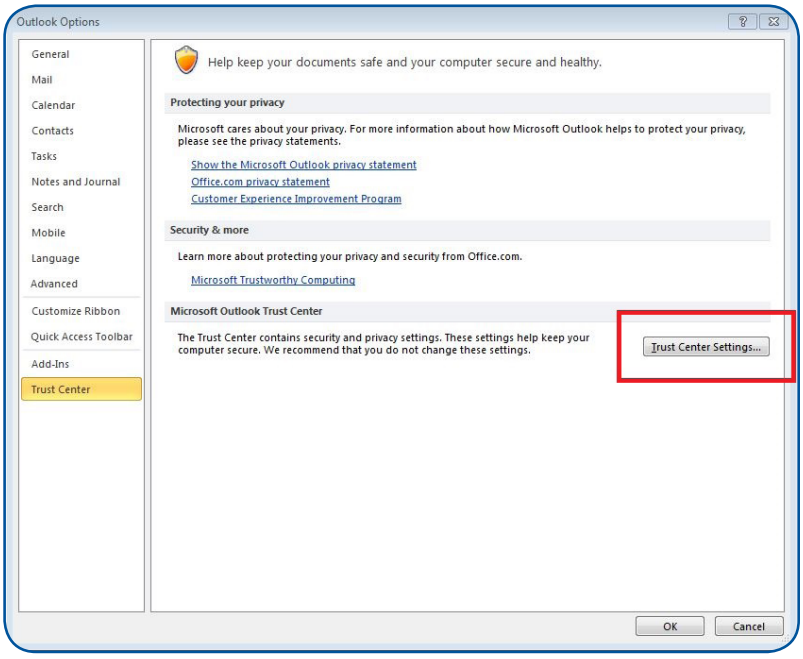
4. On the left-hand set of options, click on the **"Options"** button.



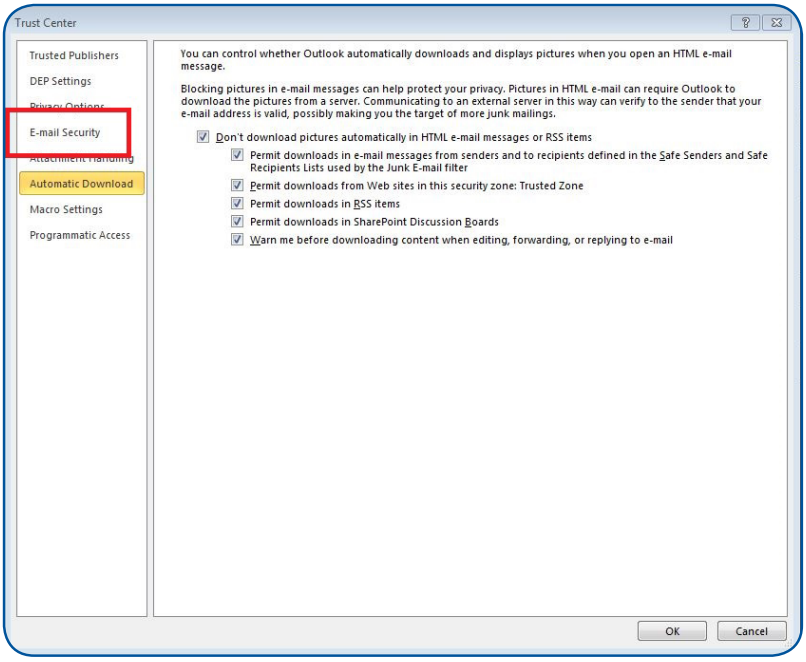
5. A window entitled **“Outlook Options”** will appear. On the left-hand pane, click on the **“Trust Center”** button at the bottom of the list.



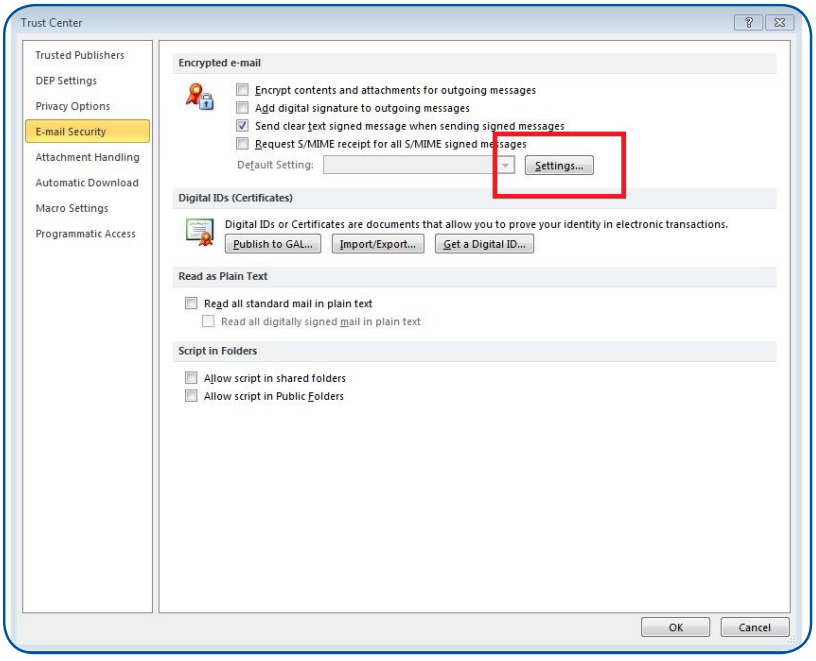
6. The right side of the window will change. Click on the **“Trust Center Settings”** button on the right-hand side.



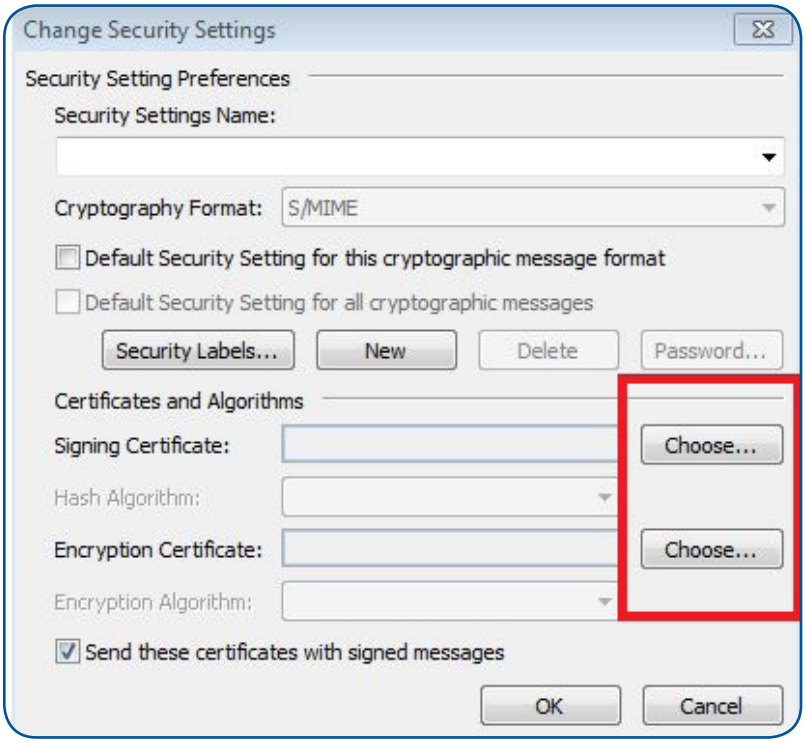
7. A window named **“Trust Center”** will appear. On the left-hand side, you will see selectable options. Click on the **“Email Security”** option on the left-hand pane.



8. Upon clicking on the **“Email Security”** button in the left-hand pane, you will see a drop down field next to **“Default Setting”**. Click on the **“Settings”** button next to this field.

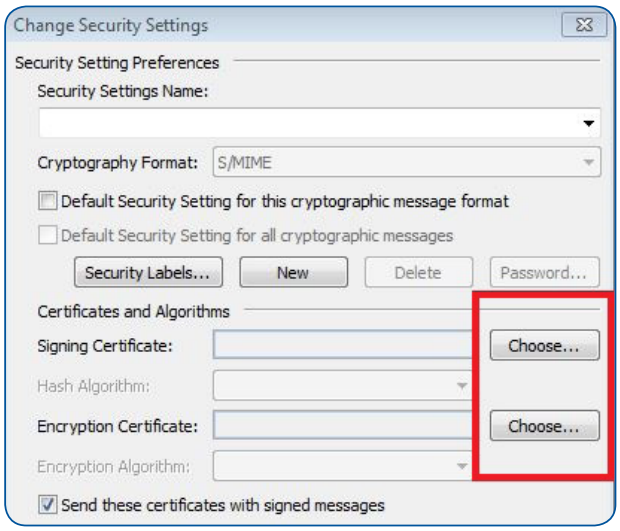


9. A new window will appear named **"Change Security Settings"**. In this window, you will see two **"Choose"** buttons on the right-hand side under the **"Certificates and Algorithms"** section.

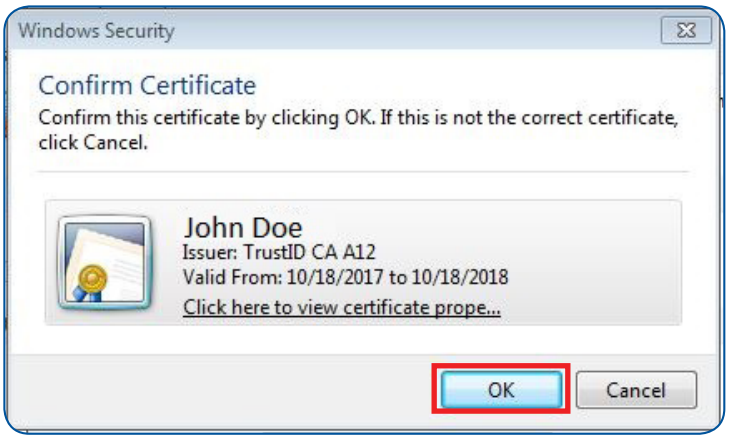


- Choose **"Signing Certificate"**. First you will choose the **"Signing Certificate"**. This is the certificate that you will use to digitally sign emails that you send out. The email in the certificate that you have installed on your computer must match the email address that you are using to sign. This certificate must also be valid.

    1. In the **"Certificates and Algorithms"** section of the **"Change Security Settings"** window, you should see the heading **"Signing Certificate"**. Click on the **"Choose"** button directly to the right of this heading.



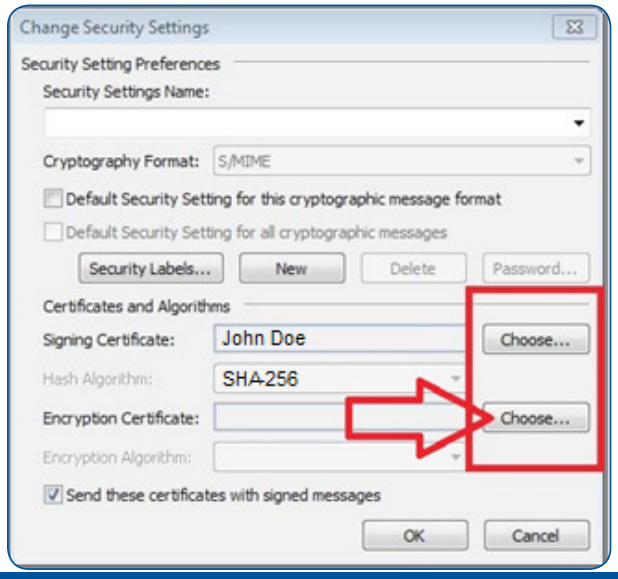
2. The **"Windows Security"** window will appear and ask you to **"Confirm Certificate"**. Click **"OK"** to continue.



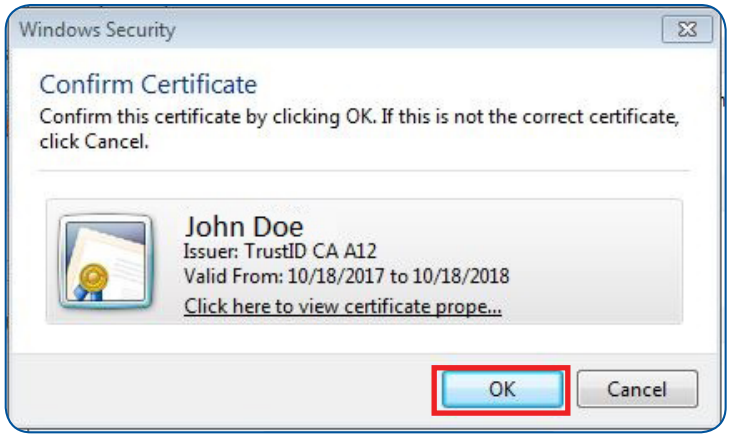
Please note that if you have more than one (1) digital certificate, you will be asked to choose the **"Digital Certificate"** you would like to sign with from a list of certificates installed on your computer. If you are unsure which certificate to choose, you can always highlight a certificate and click on the **"View Certificate"** button to see the details for that certificate. Simply choose the certificate you wish to use and follow the same instructions as provided above.

- Next you will choose the **"Encryption Certificate"**. This is the certificate that other users will use when attempting to encrypt an email to you. In typical use, you will use the same digital certificate for both signing and encryption. (The exception is for Secure Email S/MIME certificates which are only able to digitally sign emails.) You can still decrypt an email with an expired certificate.

1. In the **"Certificates and Algorithms"** section of the **"Change Security Settings"** window, you should see the heading **"Encryption Certificate"**. Click on the **"Choose"** button directly to the right of this heading.

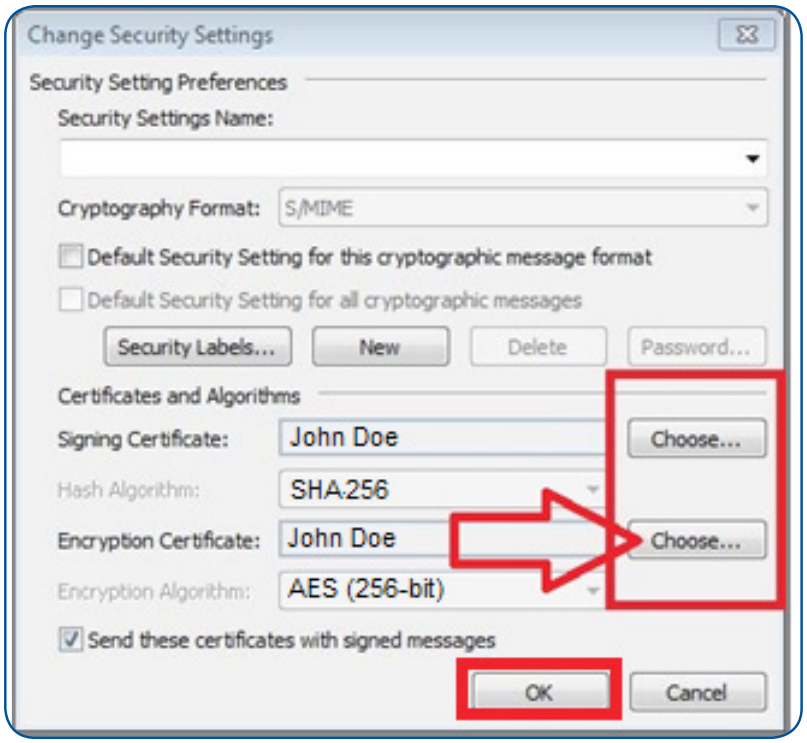


2. The **"Windows Security"** window will appear and ask you to **"Confirm Certificate"**. Click **"OK"** to continue.



Please note that if you have more than one (1) digital certificate, you will be asked to choose the **"Digital Certificate"** you would like to sign with from a list of certificates installed on your computer. If you are unsure which certificate to choose, you can always highlight a certificate and click on the **"View Certificate"** button to see the details for that certificate. Simply choose the certificate you wish to use and follow the same instructions as provided above.

10. When you return to the **"Change Security Settings"** window, you should see that the certificate you have chosen has appeared greyed out in the **"Encryption Certificate"** field. When you have finished selecting your **"Digital Certificate"**, you can press the **"OK"** button at the bottom.



11. There are additional optional configurations available. When you return to the **"Trust Center"** window, you can further configure Outlook 2010 with the way that it uses your **"Digital Certificate"**.

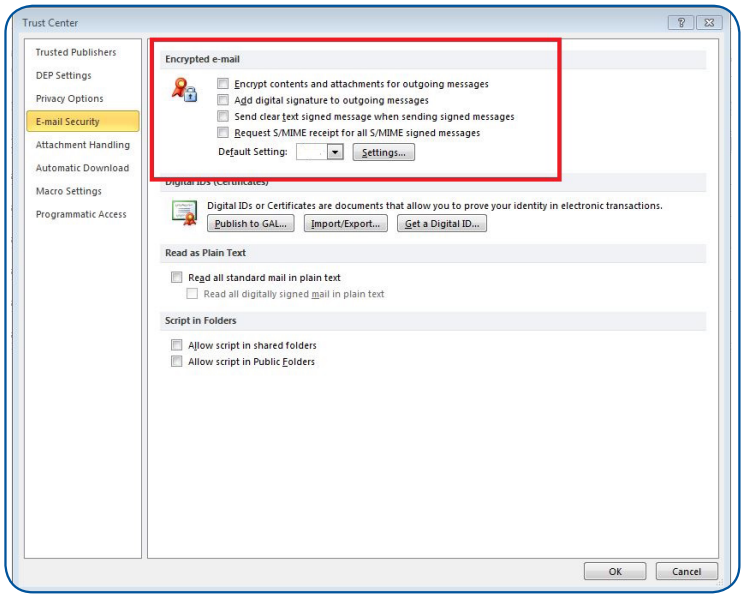
    Under the **"Encrypted e-mail"** heading, you should see four (4) check boxes. These check boxes add various features when using Outlook 2010 or later and digital certificates.

    1. **Encrypt contents and attachments for outgoing messages.** This will try to encrypt every outgoing message. In order to encrypt to a user, you must have a copy of their public key/certificate in your address book.

    2. **Add digital signature to outgoing messages.** This will digitally sign every outgoing message using your digital certificate.

    3. **Send clear text signed message when sending signed message.** This sends a digitally signed message to a recipient who does not use S/MIME.

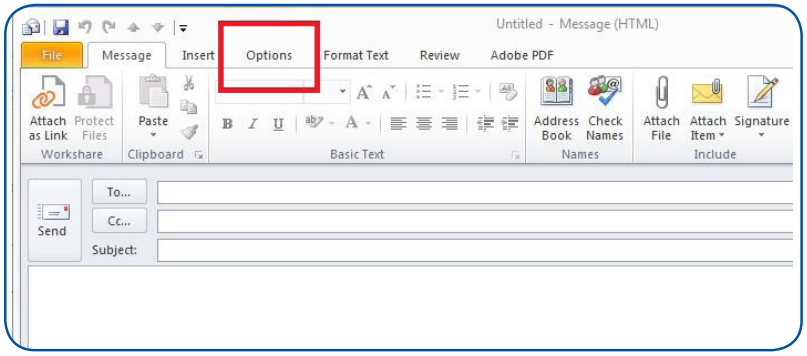
    4. **Request S/MIME receipt for all S/MIME signed messages.** This will request confirmation that a message was received unaltered. Outlook will automatically do this.



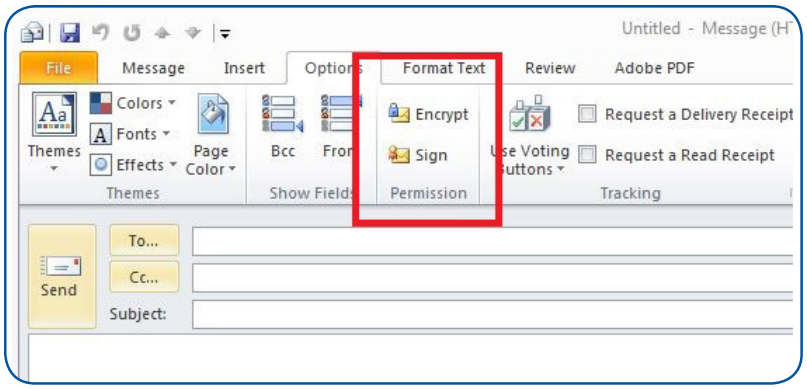
Digitally Sign and Encrypt E-Mail

Once you have followed this guide and selected a certificate for both the **"Signing Certificate"** and the **"Encryption Certificate"** headings, you will be able to use them while composing an email.

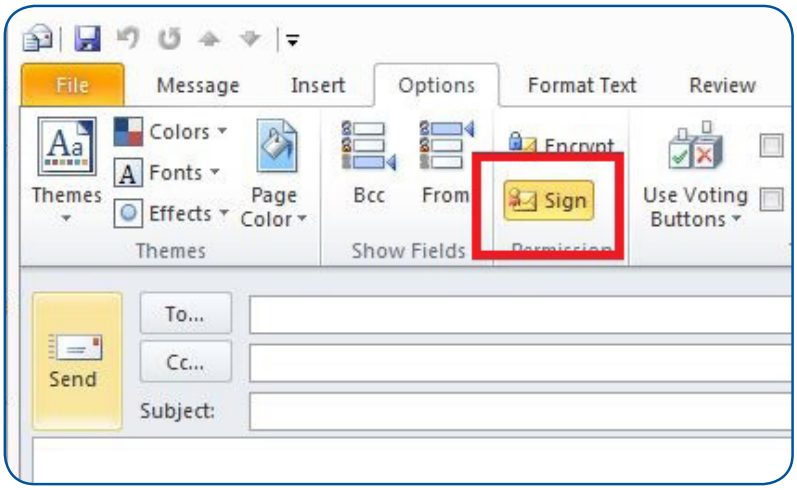
1. When you have an email open, click on the **"Options"** tab at the top of the email.



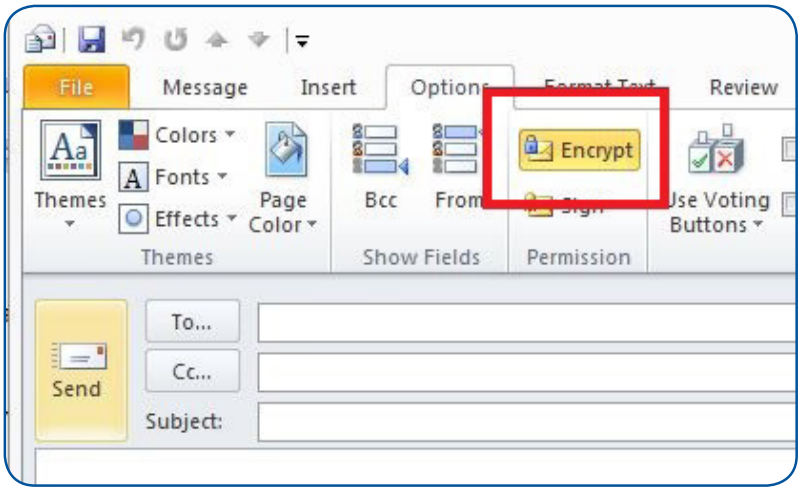
2. In the **"Permission"** section, directly below the top tabs, you should see two (2) buttons named **"Encrypt"** and **"Sign"**.



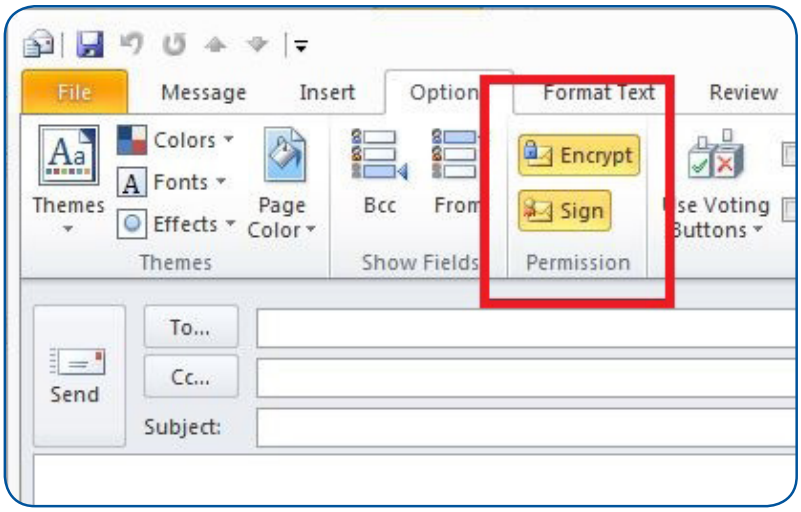
3. Click on the **"Sign"** button to depress it to digitally sign this email.



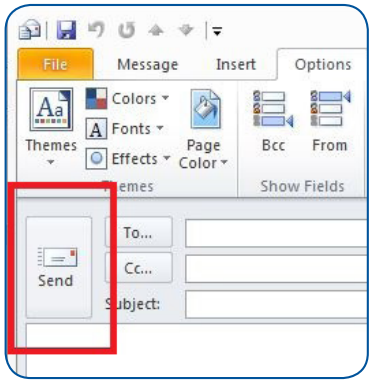
4. Click on the **"Encrypt"** button to depress it to encrypt this email. (Please note you must have the recipient's public key in order to encrypt an email.)



5. Click on both buttons, **"Sign"** and **"Encrypt"**, to digitally sign and encrypt the message.



6. After you have finished typing the new email or preparing a reply or forward, press the **"Send"** button.



2017-12-07-identrust-sign-encrypt-emails-outlook-en