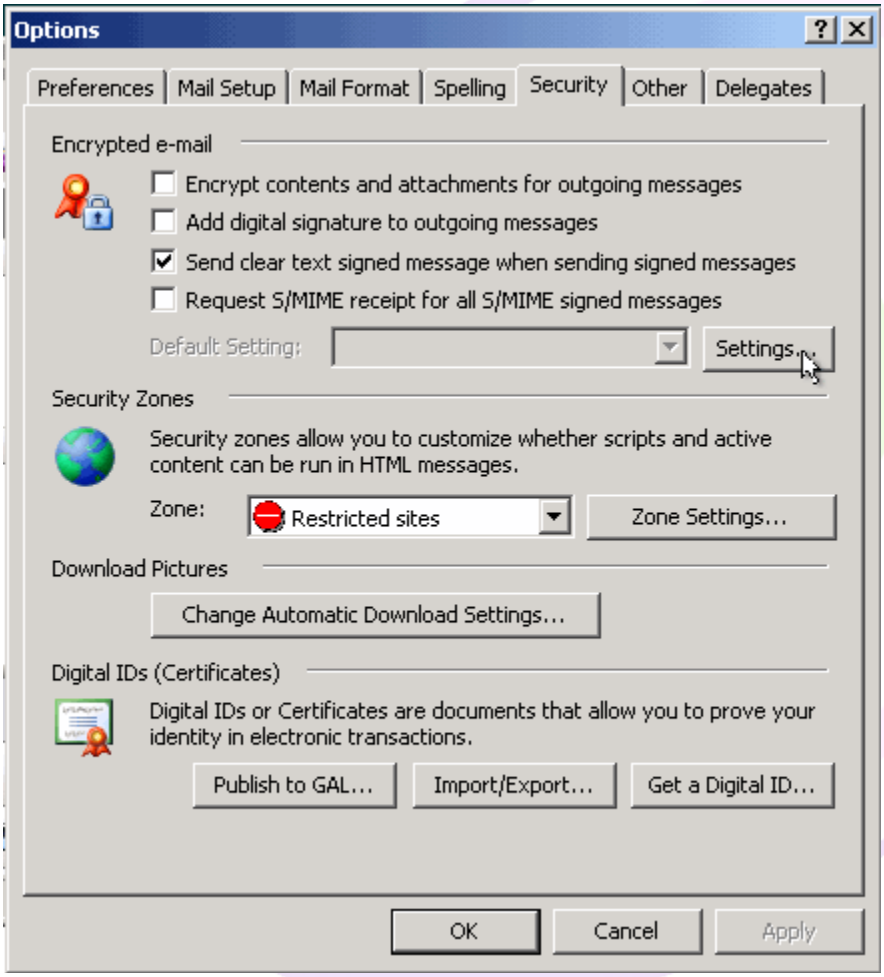
I. Configuring Digital signature certificate in Microsoft Outlook 2003:

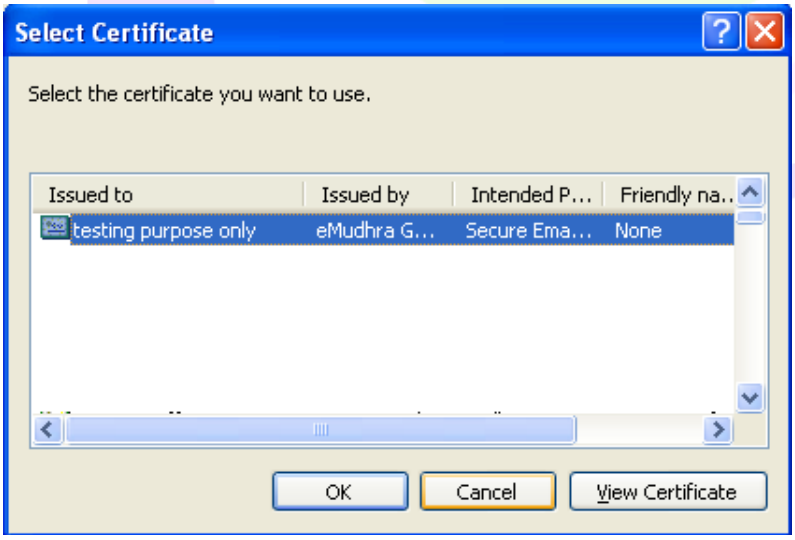
In order to configure Outlook 2003 to use the new message security settings please follow these steps:

1. Open Outlook.
2. Go to Tools > Options > Security tab.
3. In the Encrypted E-Mail section press the Settings button



4. In the Security Settings Name drop-down list make sure you see a "My S/MIME Settings (your e-mail)" title appears.

5. In the Cryptography Format make sure S/MIME is selected.
6. In the Certificates and Algorithms section, under Signing Certificate make sure that the Digital Certificate you've previously obtained is listed. If not, press Choose and browse to the required certificate.



Note: The obtained certificate should be listed automatically, and in most cases you will not need to modify any setting.

1. In the Encryption Certificate section, under Encryption Certificate make sure that the Digital Certificate you're previously obtained is listed. If not, press Choose and browse to the required certificate. Note: The obtained certificate should be listed automatically, and in most cases you will not need to modify any setting.
2. To make sure you always send your Public Key with any message you send or reply to, select the "Send these certificates with signed messages" check-box.
3. Click Ok twice.

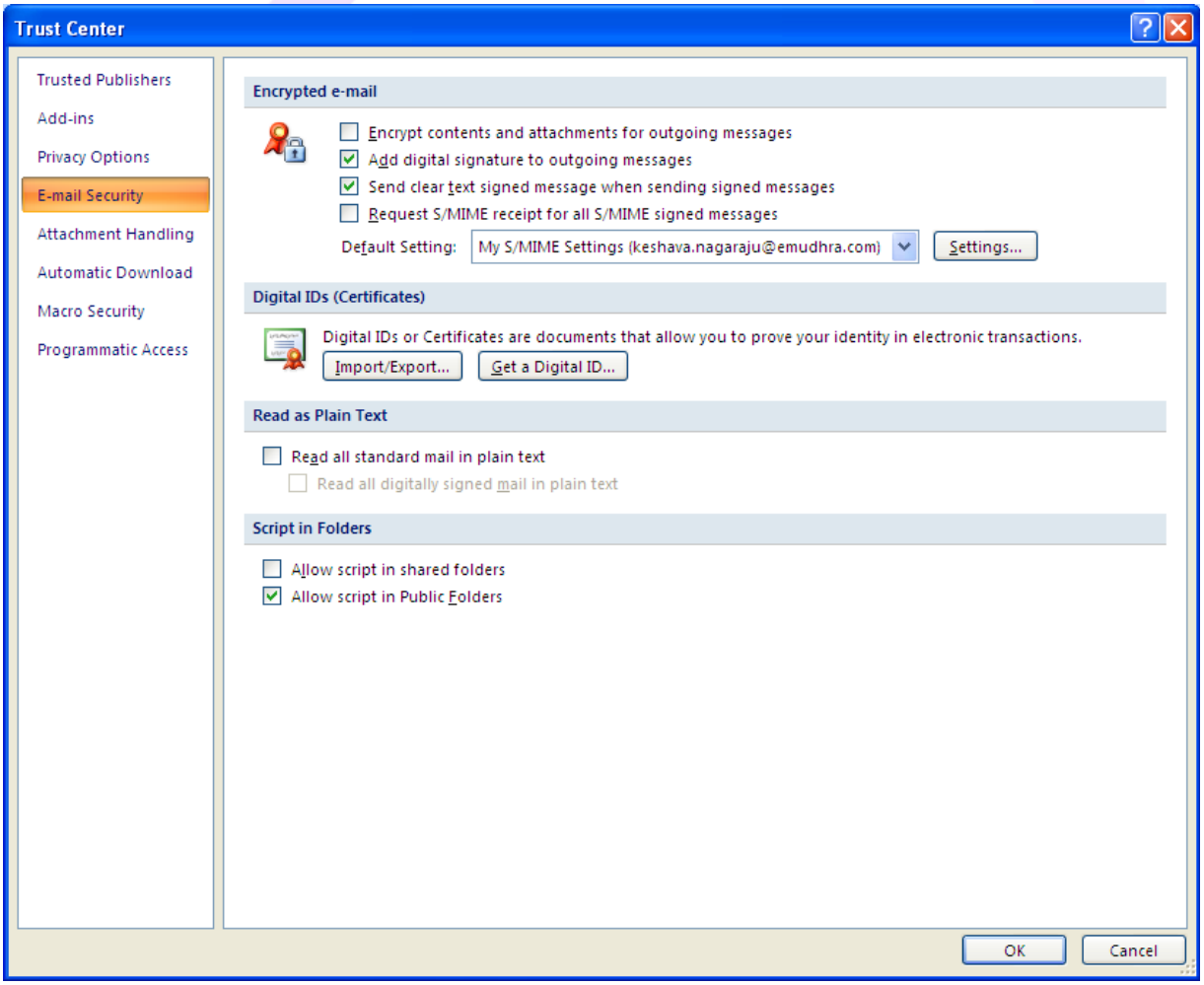
Using Message Digital Signature

In order to use the Message Digital Signature feature you do not need to perform any special action. Just type your message as you would in any regular message, press the "Add a Digital Signature to this message" icon, then press the Send button.

II. Configuring Digital signature certificate in Microsoft Outlook 2007:

- Operating System: **Windows XP, Windows Vista, Windows 7**
- Application: **Outlook 2007**

1. Make sure that you have imported your certificates into the Windows Certificate store.
2. Open Outlook.
3. From the **Tools** menu, select **Trust Center** and click the **E-mail Security** section.

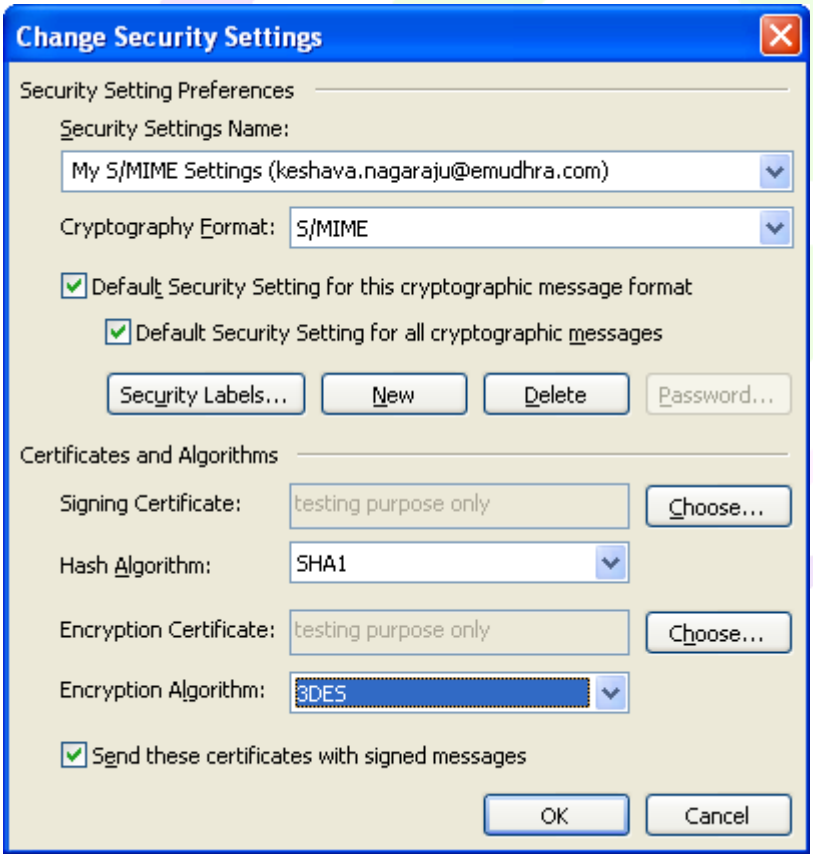


4. Select the following options:
   - **Add Digital Signature to Outgoing Messages.** This option includes your signing certificate on all outgoing messages.
   - **Send clear text signed messages when sending signed messages.** This ensures that recipients can read your signed messages. It is especially important if your recipient is using a Web or mobile email client.

5. For encryption, ITS recommends that you do not select the option to "Encrypt contents and attachments for outgoing messages." ITS recommends that you manually choose encryption for individual messages rather than setting it by default

Note: You can send an encrypted message only if you have the recipient's public key.

6. Click the **Settings** button. Outlook displays options for your signing and public encryption certificates under **Certificates and Algorithms**. Outlook includes your public signing certificate in the messages sent so that other users may send you encrypted messages.



7. Click the **Choose** button to the right of **Signing Certificate**, select your certificate from the list, and click OK.
8. Click the **Choose** button to the right of **Encryption Certificate,** select your certificate from the list, and click OK.

9. Click **OK** again.

10. Send an email to yourself as a test. Delivered messages display the signing icon, encryption icon, or both, depending on the options you selected.

Note : If you are using Windows Vista or Windows 7, recipients of your emails may not be able to read your encrypted messages if they are using an older email client. To fix this problem, follow the steps below:

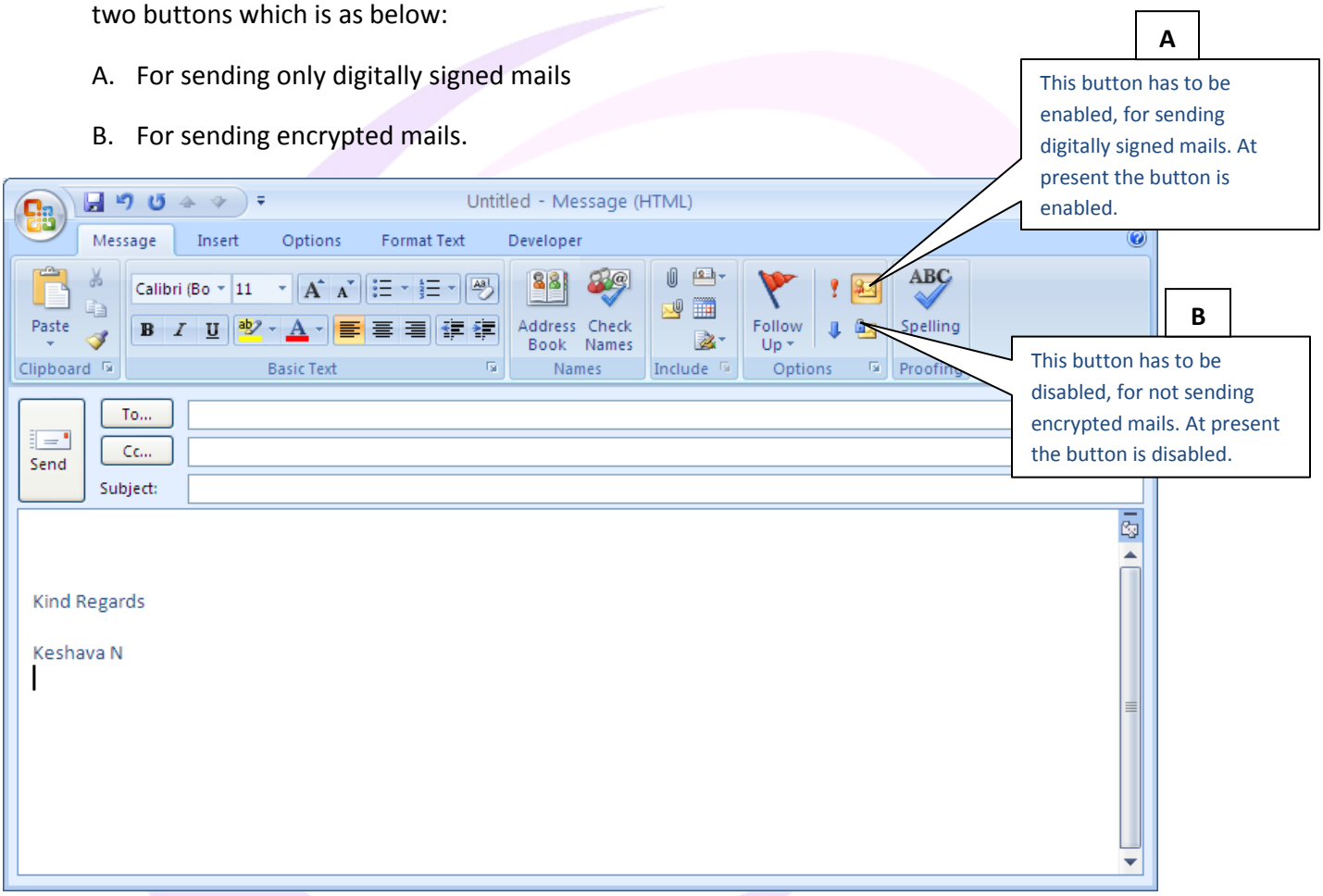
1. From the **Tools** menu, select **Trust Center** and click the **E-mail Security** section.
2. Under the **Encrypted e-mail** header, click **Setting** button.
3. Under **Certificates and Algorithms** section, from the **Encryption Algorithm** drop-down menu, select **3DES**.
4. Click **OK**
5. Click **OK**

To send digitally signed and encrypted mails in Outlook 2007 & 2010:

1. Open Microsoft outlook and login to your mail account.
2. Click on New mail, and on right side top of the new mail window, you will be able to view two buttons which is as below:

   A. For sending only digitally signed mails

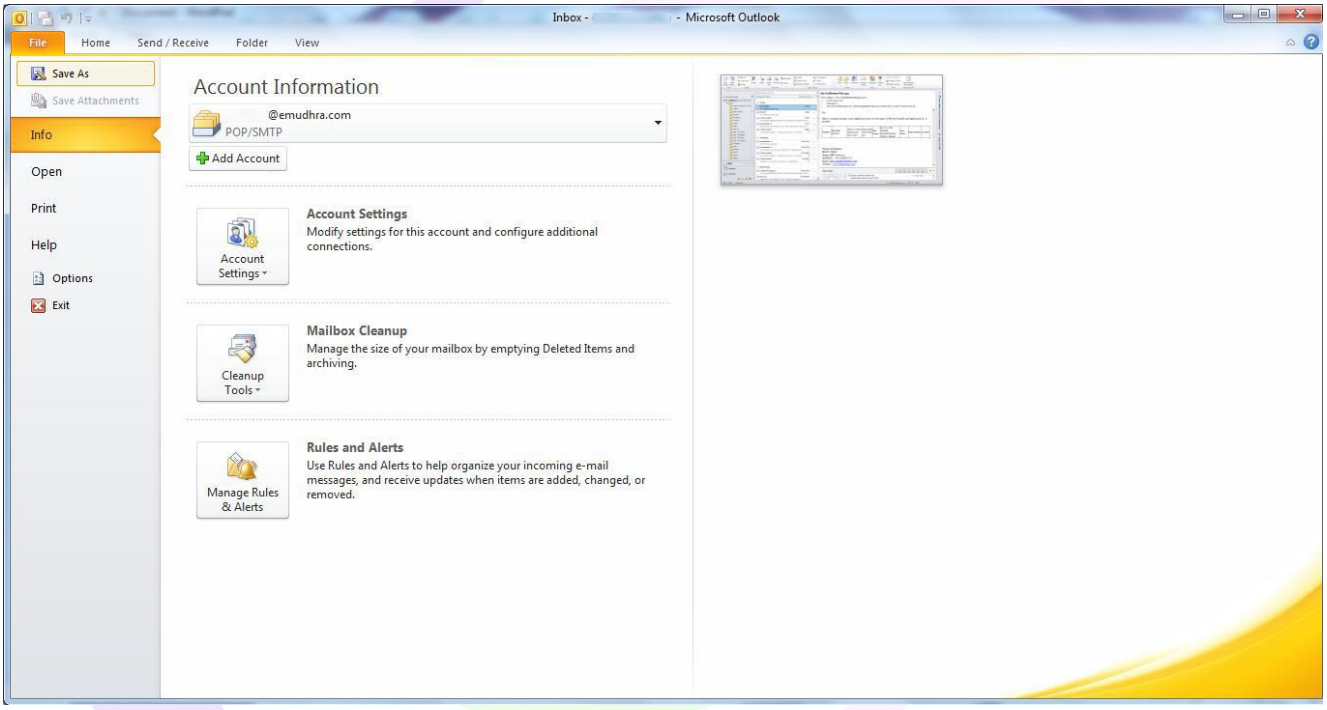
   B. For sending encrypted mails.



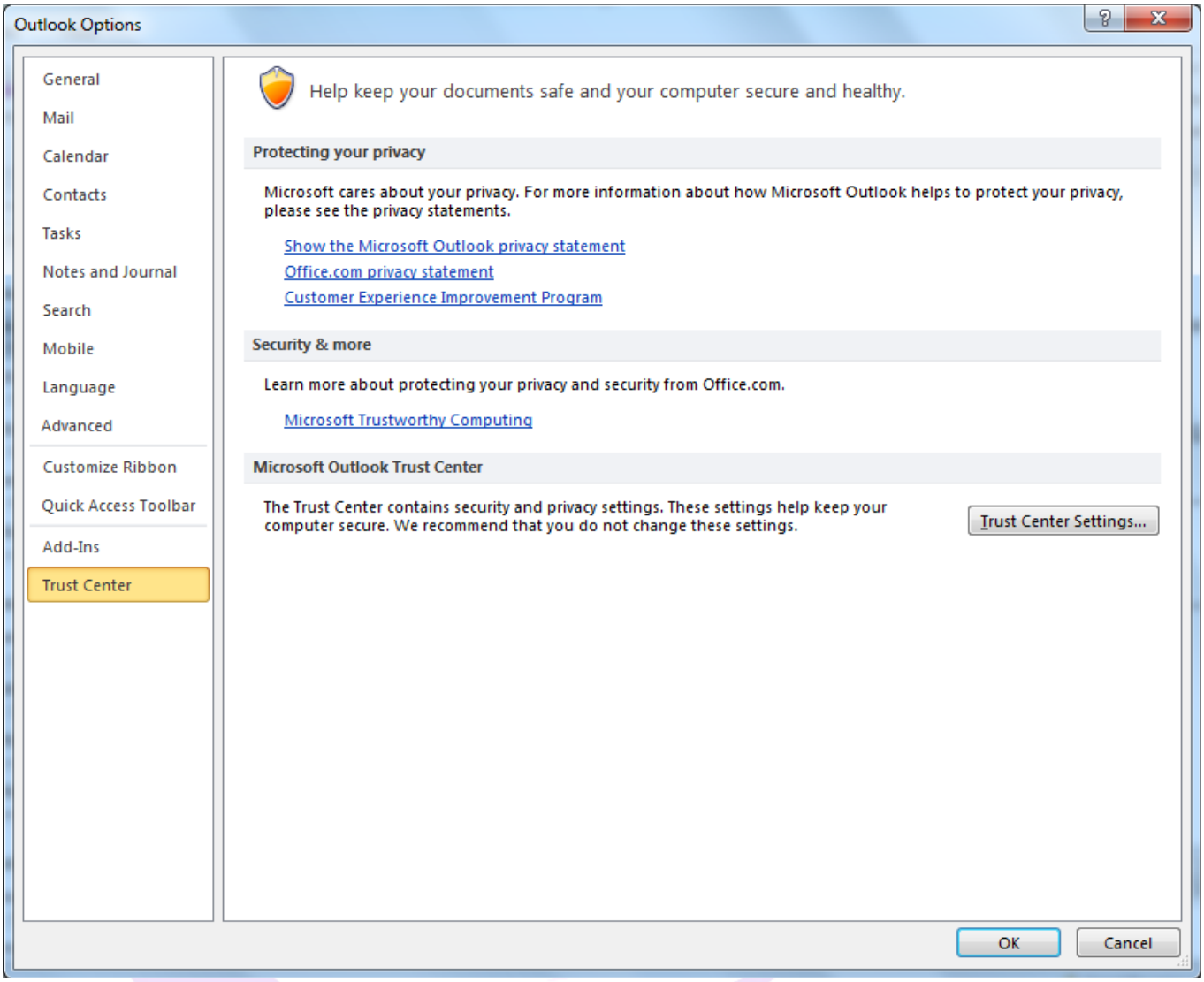
3. If you want to send only digitally signed mails, Enable button “A” as shown in the above screen shot.
4. If you want to digitally sign and encrypt the mail, both the Buttons “A and B” has to be enabled.

III. Configuring Digital signature certificate in Microsoft Outlook 2010:

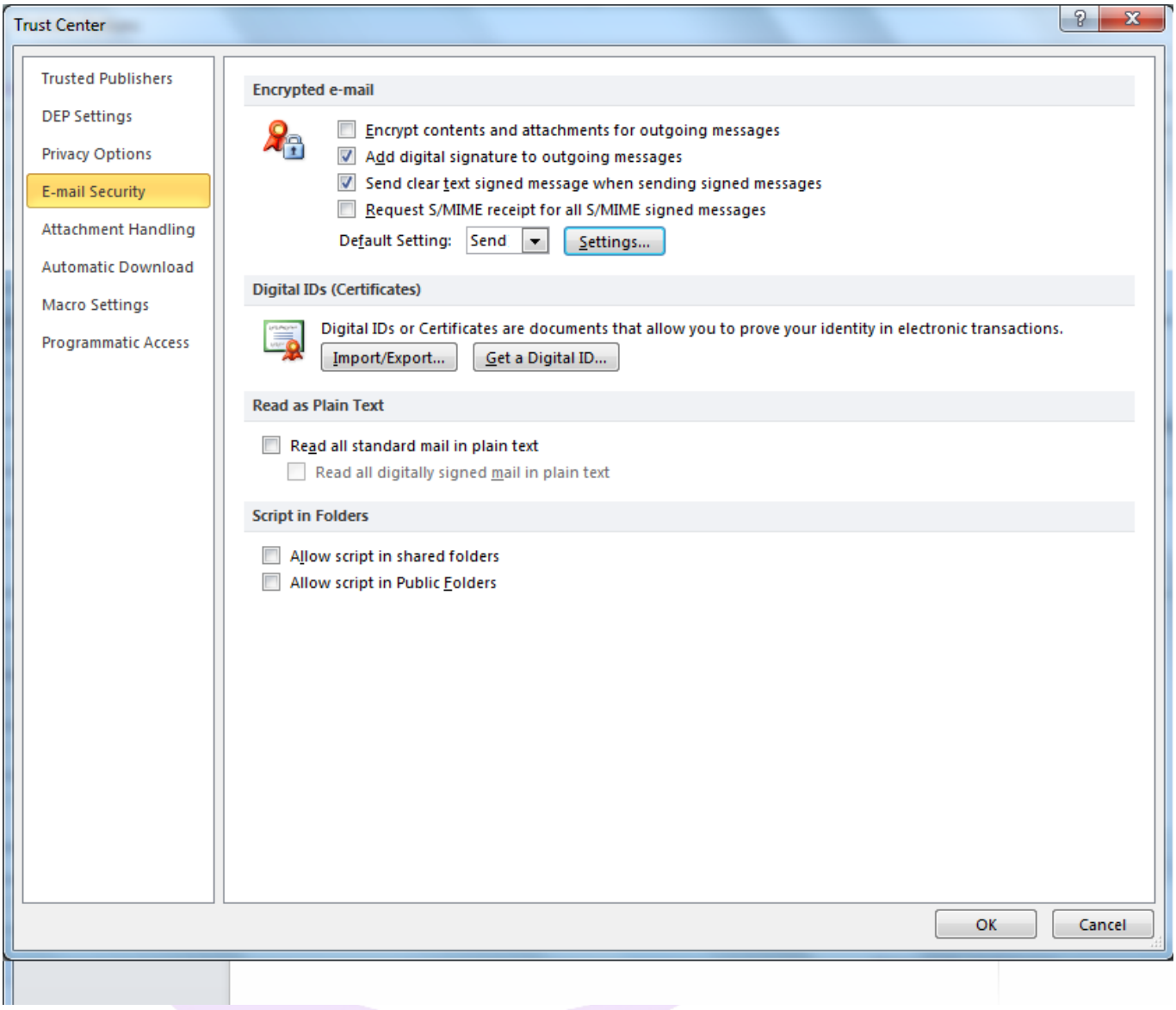
1. Make sure that you have imported your certificates into the Windows Certificate store i.e. root certificates.
2. Open Outlook.
3. Go to File and click on options



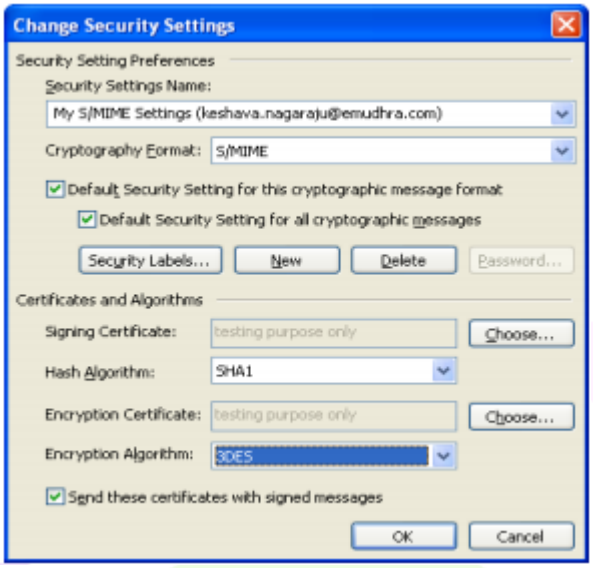
4. Select Trust Center and click on trust center settings button.



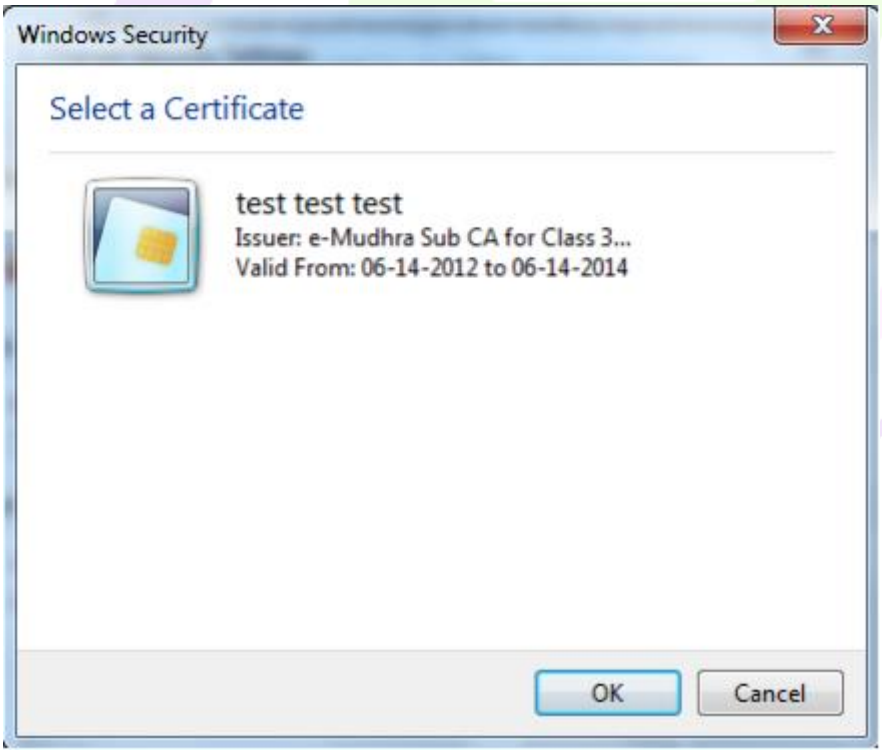
5. Select e-Mail Security and click on **Settings** button.



6. Click the Settings button. Outlook displays options for your signing and public encryption certificates under Certificates and Algorithms. Outlook includes your public signing certificate when it sends your signing certificate so that other users may send you encrypted messages.



7. Click the Choose button to the right of Signing Certificate, select your certificate from the list, and click OK.
8. Click the Choose button to the right of Encryption Certificate, select your certificate from the list, and click OK
9. Click **OK** again.



IV. Sending digitally signed mails in MAC OS X:

1. On the Tools menu, click Accounts.

2. Click on the account that you want to send a digitally signed message from, click on Advanced button, and then click on the Security tab.

3. Under Digital Signing, on the Certificate pop-up menu, click the certificate that you want to use.

Note: The Certificate pop-up menu only displays certificates that are valid for digital signing or encryption that you have already added to the keychain for your Mac OS X user account.

Do any of the following:

To	Do this
Make sure that your digitally signed messages can be opened by all recipients, even if they do not have an S/MIME security standard built into many e-mail applications, including Outlook, that enables you to use digital signing and encryption. To use digital signing and encryption, both the sender and recipient must have a mail application that supports the S/MIME standard. mail application and can't verify the certificate	Select the Send digitally signed messages as clear text check box.
Allow your recipients to send encrypted messages to you	Make sure that you have selected your signing and encryption certificates on this screen, and then select the Include my certificates in signed messages check box.

4. Click OK, and then close the Accounts dialog box.

5. In an e-mail message, on the Options tab, click Security, and then click Digitally Sign Message.

6. Finish composing your message, and then click Send.

V. Sending Encrypted mails in MAC OS X:

1. On the **Tools** menu, click on **Accounts**.

2. Click the account that you want to send an encrypted message from, click **Advanced**, and then click on the **Security** tab.

3. Under **Encryption**, on the **Certificate** pop-up menu, click on the certificate that you want to use.

   Note: The Certificate pop-up menu only displays certificates that are valid for digital signing or encryption that you have already added to the keychain for your Mac OS X user account.

4. Click on OK, and then close the Accounts dialog box.

5. In an e-mail message, on the Options tab, click Security, and then click **Encrypt Message**.

6. Finish composing your message, and then click Send.

   Note: When you send an encrypted message, your recipient's certificate is used to encrypt his or her copy of the message. Your certificate is used to encrypt the copy that is saved to your Sent Items or Drafts folder in Outlook.

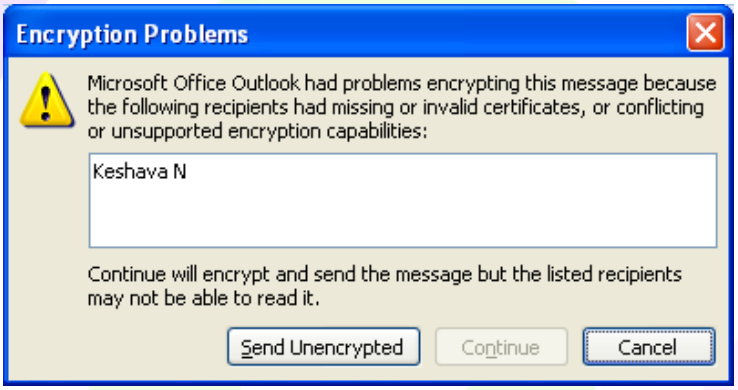
VI. Exceptions in the e-Mail security:

1. **When I'm viewing the digitally mail from Web interface like Microsoft email web interface, Gmail yahoo mail etc... Certificate is not getting verified?**

→ If signed mails are sent from Microsoft outlook client to the recipient and if the recipient accesses the mail from Microsoft web based or any web based login like Gmail etc... He will be authorized view the content of the mail and Digital signature will viewed as an attachment with .p7s extension. This means that these web based login does not have SMIME cryptographic add-on to either validate the certificate or to download the mail as digitally signed.

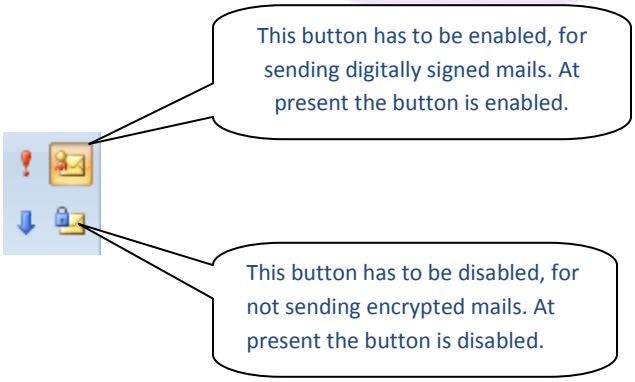
---

2. **Not able to send the encrypted mails? And I'm getting the below error.**



→ When you send an encrypted message, your recipient's certificate is used to encrypt his or her copy of the message. So you need to get the digitally signed mail from the recipient mail to which you can reply to that particular mail by selecting the both digitally signing and encryption options as below:

When you are sending mails on the top right side there will be two buttons, one for digitally signing and one for encrypting mails. Kindly disable the encryption button which is as showed in the below screen shot:



3. Not able to select the certificate when configuring the email security for digitally signing.

→ Kindly check the respective token drivers is installed as per your operating system compatibility. We recommend you to verify the certificate functionality by signing on a word document. Check whether you are able to view the certificate in the admin tool. Please follow the below procedure to view:

A. If you are using the eMudhra Watchdata token in windows system, click on Start → All programs → select eMudhra USB token → click on eMudhra Watchdata token Tool. You should be able to view the certificate.

B. If you are using Aladdin token in windows system, click on start → all programs → eToken → click on eToken PKI Client properties and select advance view → in the left hand side, expand eToken and select User certificate to view your certificate.

C. Click here to download the token drivers for your Operating system.

---

4. Not able to select Hash Algorithm after selecting the certificate in the email security.

→ If the system is connected to the domain network, there will be the group policy which will be updated to all the systems. These policies will not provide you to access/use the complete features in order to operate cryptographic functions. So you need to either check with your system administrator to update the group policy of the system to make use of cryptographic features or to provide complete admin privilege for the system.

→ Also check if any security applications like Spybolt are installed. If so, please uninstall the same and try to send a signed email.

→ Also check if Antivirus application is causing any issue. If so, please uninstall the same and try to send a signed email.

→ Also check if the intended user has admin privileges enabled on the machine at the time of configuring DSC.

---

5. Error message below when mails are read on mobile phones: "The encrypted message can't be displayed because this version of Exchange server doesn't support encrypted S/MIME messages on mobile phones. To view this message, you need to open it on a computer using Outlook."

→ There is no problem with the encrypted mail which you received to your mail box. Mail clients in the mobile phones are not completely enabled with the extended features like which you are having in the Microsoft outlook for Windows OS.

To open the encrypted mail in mobile phones you required the Digital signature certificate and necessary key store to store the certificate in the mobile, so that the mobile mail client can decrypt the message using your DSC. If this feature (Encryption S/MIME) is not available in the mobile mail client, then you will not be able to view the mail content from the mobile mail client which is not compatible for S/MIME encryption. It can only be viewed from your system with Microsoft outlook and also with your certificate.