

# YATANARPON TELEPORT COMPANY LTD.,

YATANARPON  
CERTIFICATION  
AUTHORITY

## USER MANUAL FOR SECURE E-MAIL MICROSOFT OUTLOOK (2007)

Yatanarpon Teleport Company Ltd.,  
Hlaing Universities Campus,  
Hlaing Township, Yangon, Myanmar  
Ph: 951-652233, Fax: 951-652244  
Email: [opetraingca@myanmar.com.mm](mailto:opetraingca@myanmar.com.mm)  
URL: <http://www.yatanarponca.com.mm>

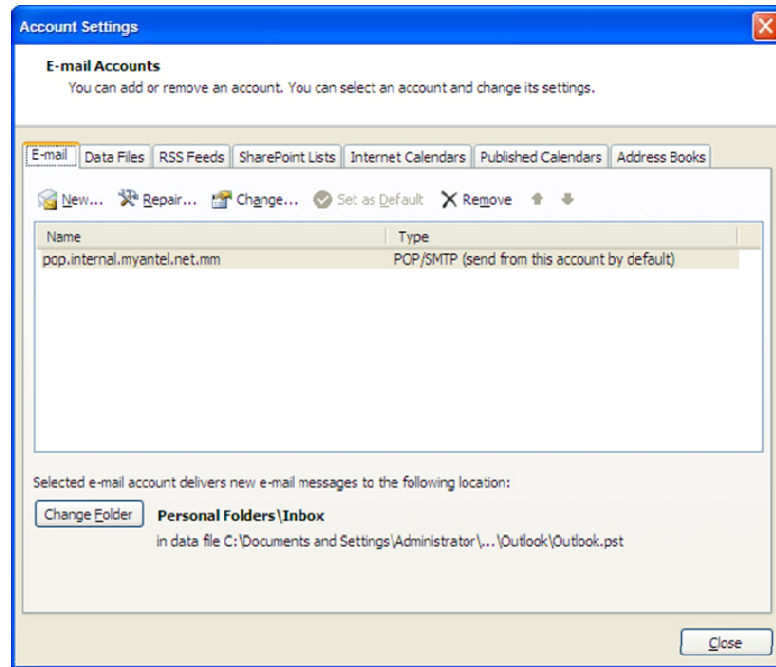
## **Table of Contents**

- 1. Creating E-mail Account in Microsoft Outlook 2007**
- 2. Certificate Installation.**
  - 2.1 Subscriber/ User certificate installation (PFX)**
  - 2.2 CA Certificate Installation**
  - 2.3 Root Certificate Installation**
  - 2.4 Get Digital ID**
    - 2.4.1 Downloading and Importing a Digital ID**
  - 2.5 Importing Digital ID to Contacts**
    - 2.5.1 Importing Digital ID From Trust Center (Default signed messages)**
    - 2.5.2 Importing Digital IDs/ Certificates (proving identity)**
- 3. Certificate Application.**
  - 3.1 Signing Individual E-mail**
  - 3.2 Signing all Outgoing E-mail**
  - 3.3 Encrypting your E-mail**
    - 3.3.1 Encrypting Individual Messages**
    - 3.3.2 Encrypting all Outgoing email**
- 4. Things to know...**
  - 4.1 How to protect your digital IDs**
  - 4.2 What to do if a Digital ID is Lost or stolen**
  - 4.3 Sharing Certificates with others**

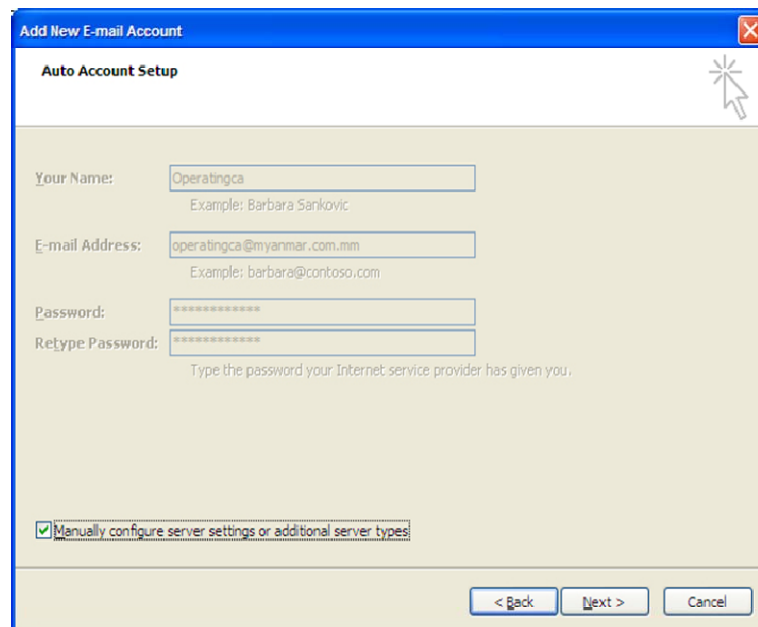
## 1. Creating E-mail Account in Microsoft Outlook

To configure email account setting in Microsoft Outlook:

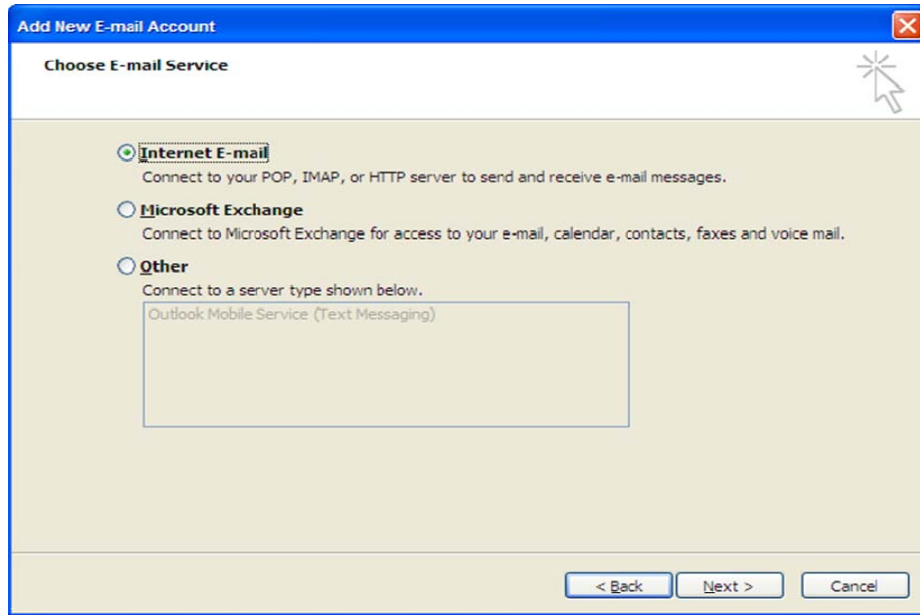
1. Go to Menu bar and select the **Tools** then scroll down to **Email Account** button.
2. Click the **New** button under the **E-mail** tab.



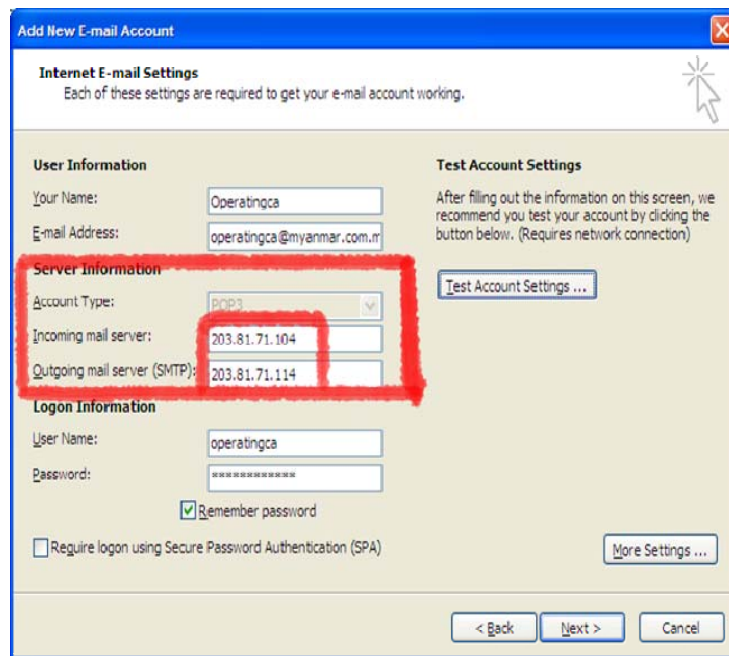
3. You will see Auto Account setup status window and Mark **Manually configure server settings or additional server types**, from left bottom.
4. Click **Next** button.



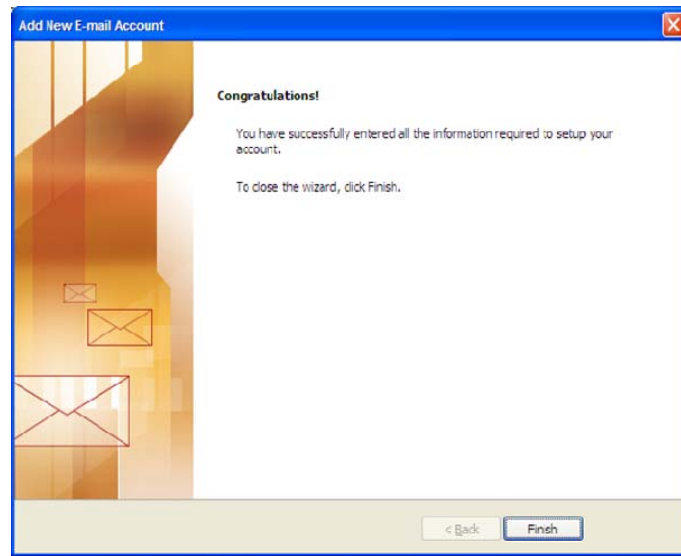
5. Check Internet E-mail tab from Choose E-mail Service status window from Add New E-mail Account.
6. After choosing E-mail service click **Next** button.



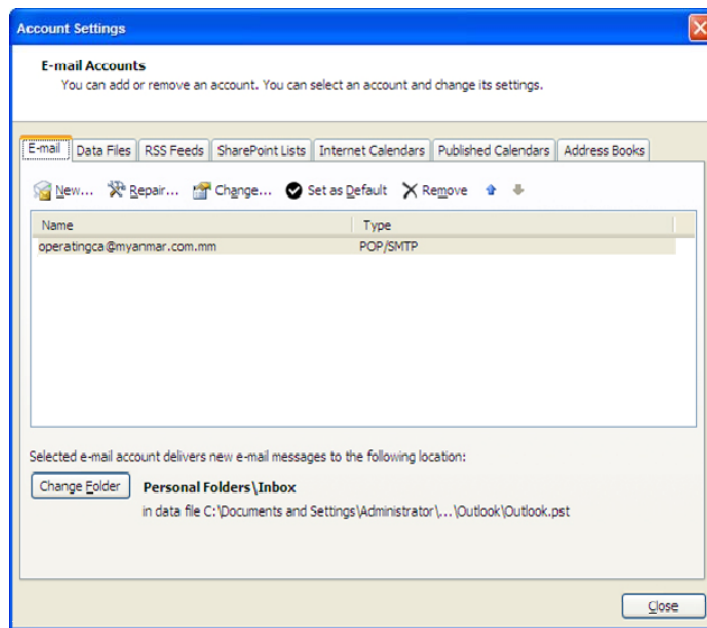
7. Type user name and password now you need to type mail server numbers. These numbers can be change (Red mark) then Click Next button.



8. Click **Next** button. Then you will see Finished Wizard and Click **Finish**.



9. After configuring your email account setting you will see the following dialog and click **Close** button.



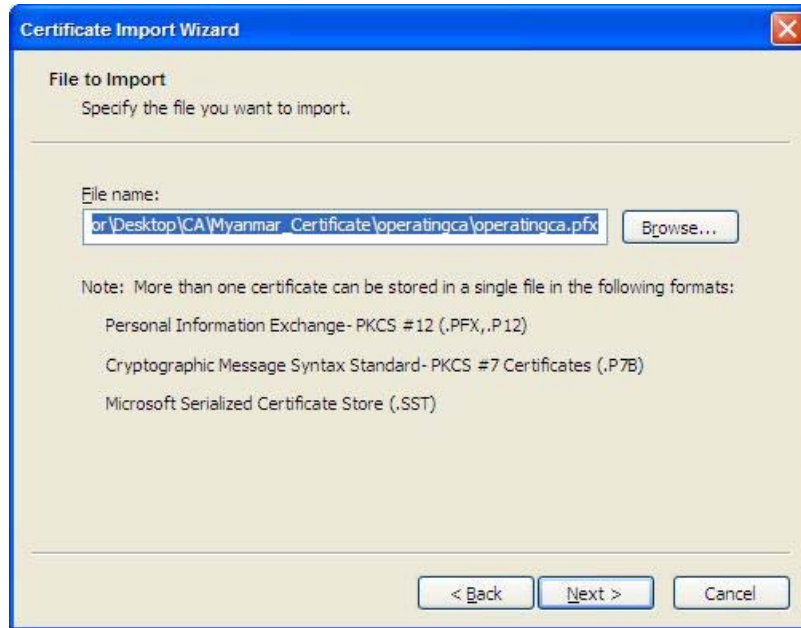
## **2. Certificate Installation.**

To use digital ID in your system, you need to install 3 certificate files as follow;

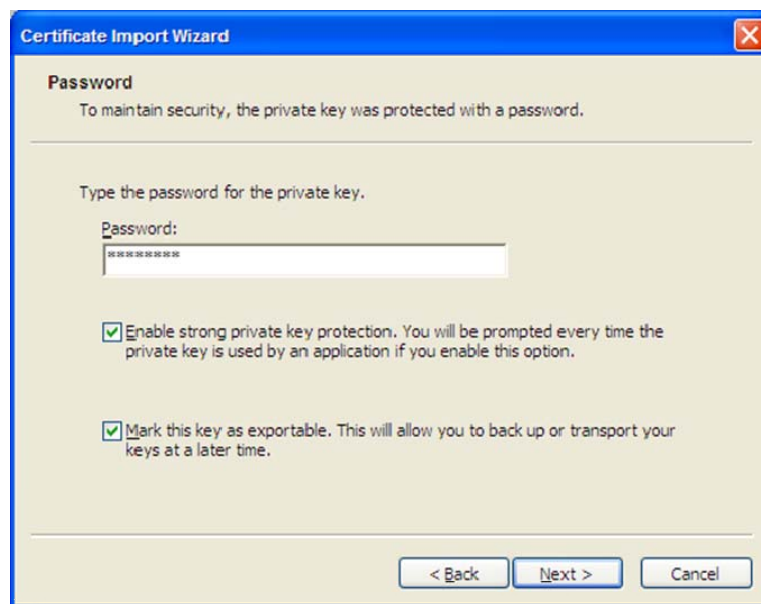
1. Subscriber/User Certificate Installation (.PFX) File
2. Certification Authority (.CER) File
3. Root Certification Authority (.CER) File as provided by the CA.

## 2.1 Subscriber/ User certificate installation

1. Click your certificate (.pfx) file.
2. You will see Certificate Import Wizard window and click **Next** button.
3. Specify the file you want to import by click **Browse** button and choose your file, click **Next** button.



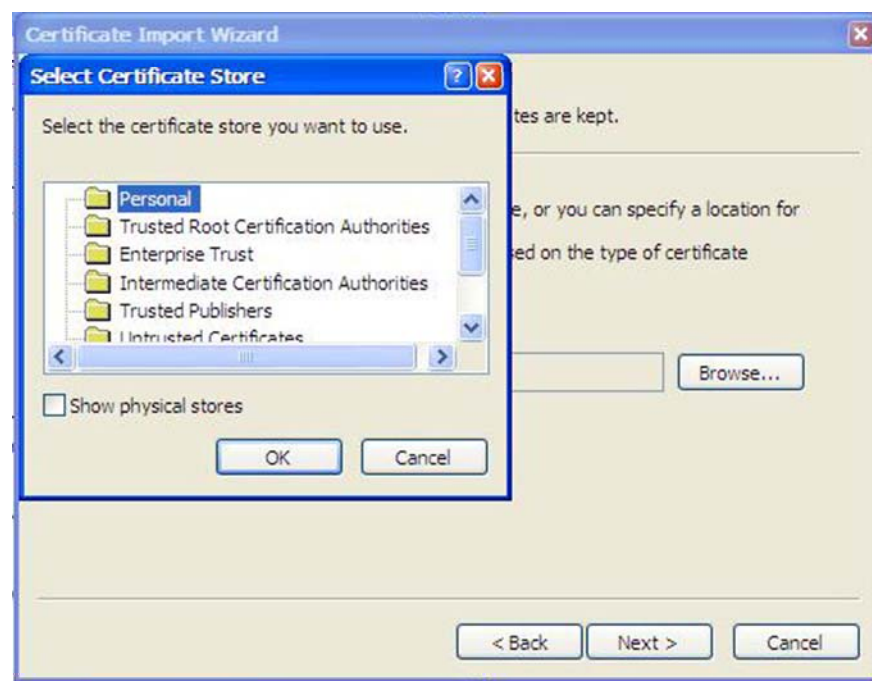
4. To maintain security, the private key was protected with a password. Type the password for the private key.
5. Mark all **Check** boxes and click **Next** button.



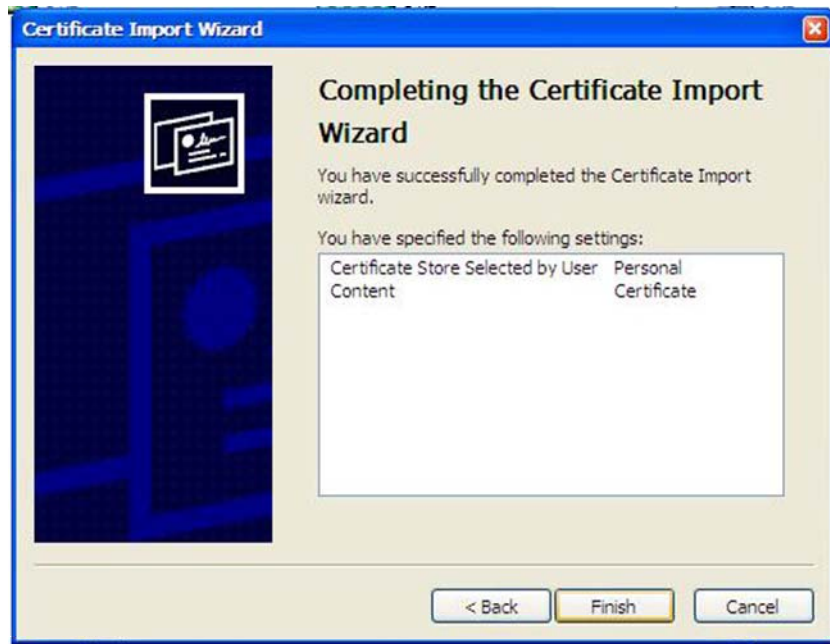
6. Select **Place all Certificate in the following store** button & click **Browse** button.



7. Select the **Personal** Folder and click **OK** button and then click **Next** button in **Certificate Import Wizard** window.



8. If you have successfully completed the Certificate Import Wizard, click **Finish** button.

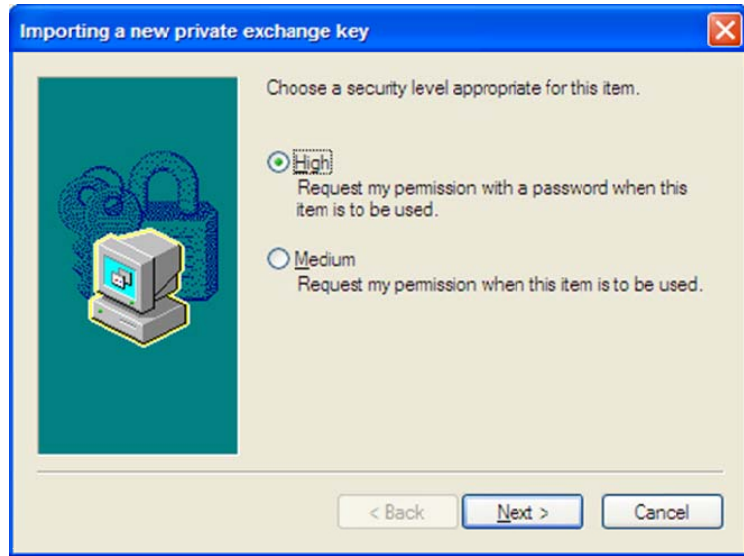


9. After completing the certificate Import Wizard, you need to import a new private exchange key. You can set security level (High or Medium). Click **Set Security Level** from importing a new private exchange key dialog.





10. Select **High** check box. (**If you want to set High security level**) and then click **Next** button.



11. Then **Importing a new private exchange key** wizard dialog will appear. Type Password and Confirm: Password then click **Finish**.



12. Click **OK** button from the Certificate Import Wizard dialog. You are about to Finish the Certificate installation.

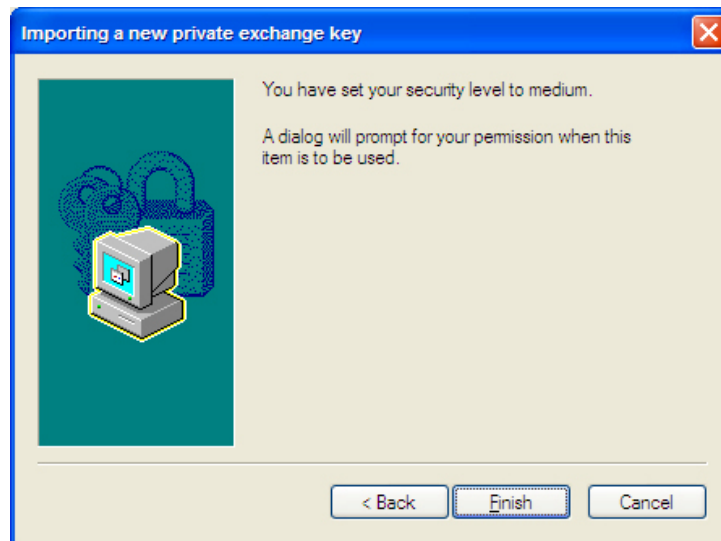


**You can set Medium security level too:-**

10. Select the **Medium** button and Click **Next** button.  
(If you want to set Medium security level)



11. To complete the wizard click **Finish** button.



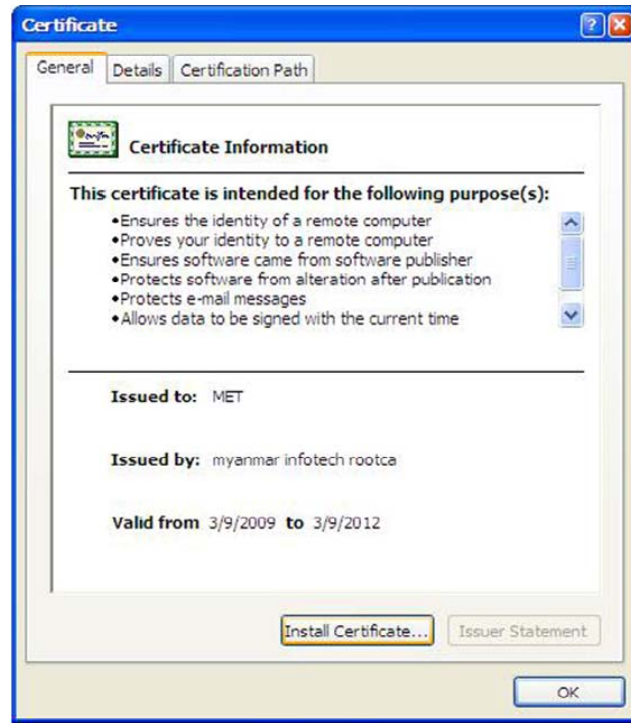
12. Click **OK** button and you Finish Certificate installation.



## 2.2 CA certificate Installation (.CER)

Second step is to install CA certificate (MET.cer) file.

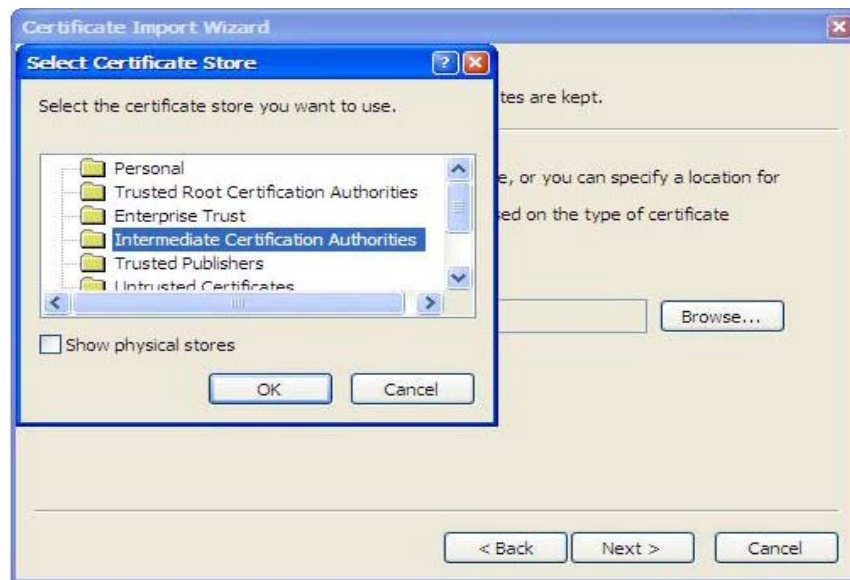
1. Click require (MET.cer) file.
2. Click **Install Certificate** button.



3. Select **Place all Certificate in the following store** button from **Certificate Import Wizard** and then click **Browse** button.



4. Select the **Intermediate Certification Authorities** text and click **OK** button and then click **Next** button in **Certificate Store** status window.



5. And you will see again Certificate Store status window, Click **Next** button, then Import wizard is complete click **Finish** button.



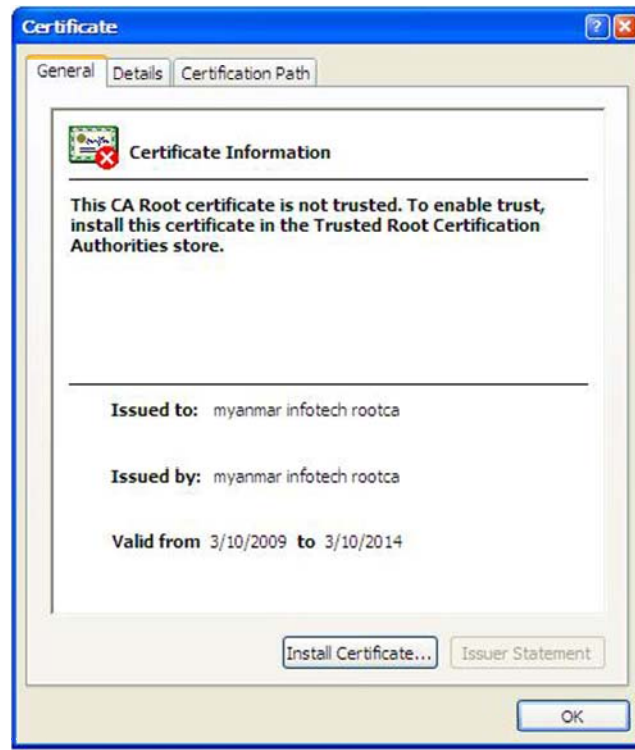
6. Click **OK** button and then your installation is completed.



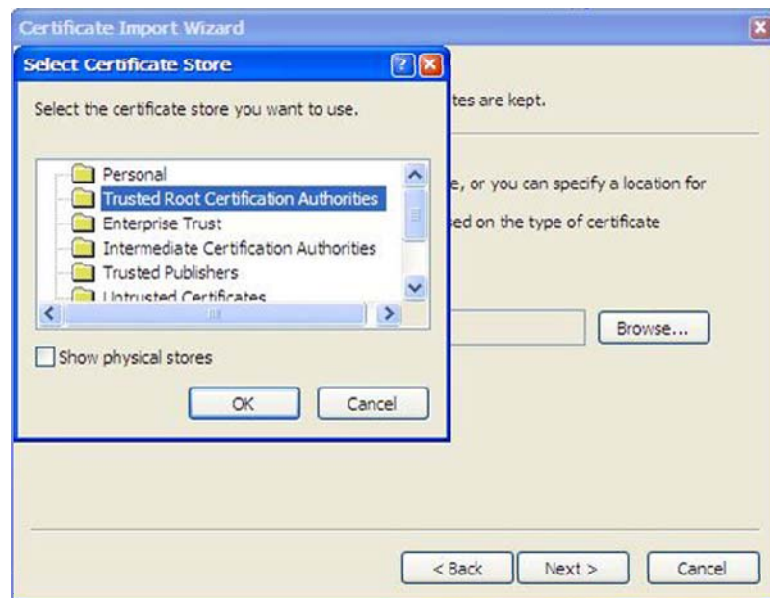
### 2.3 Root certificate Installation (.Cer) File

Third step is to install Root CA certificate (.cer) file.

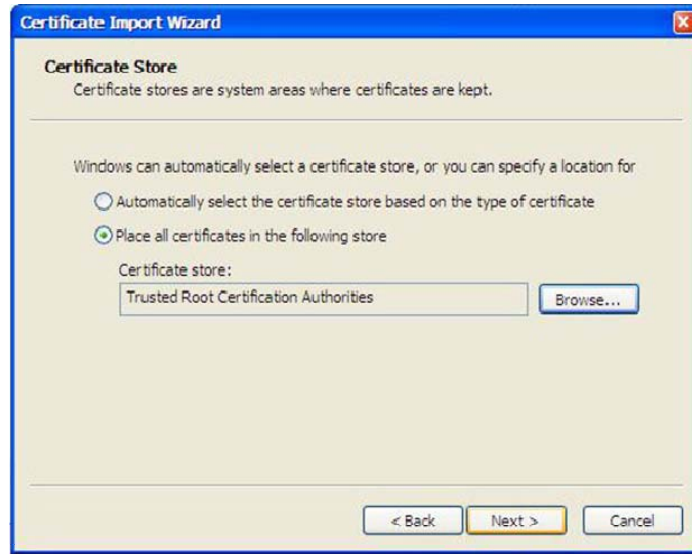
1. Click require (Myanmar Info Tech Rootca .cer) file.
2. Click **Install Certificate** button and click **Next** button.



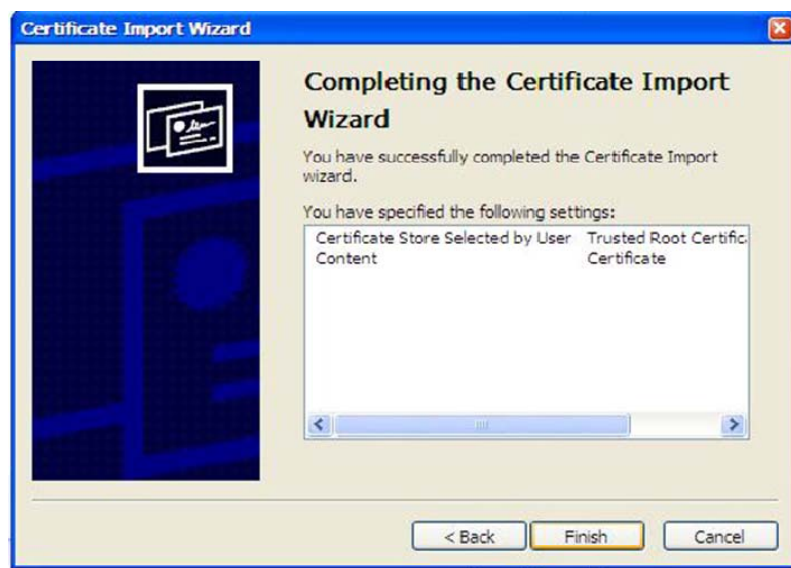
3. Select **Place all Certificate in the following store** button and click **Browse** button. After seeing the Select Certificate Store, choose **Trusted Root Certification Authorities** Folder



4. And you will see again Certificate Store status window, click **Next** button.



5. The Certificate Import wizard is completed by clicking **Finish** button.



6. Click **OK** button and then your Installation is complete.





## 2.4 Get Digital ID


### 2.4.1 Downloading and Import a Digital ID

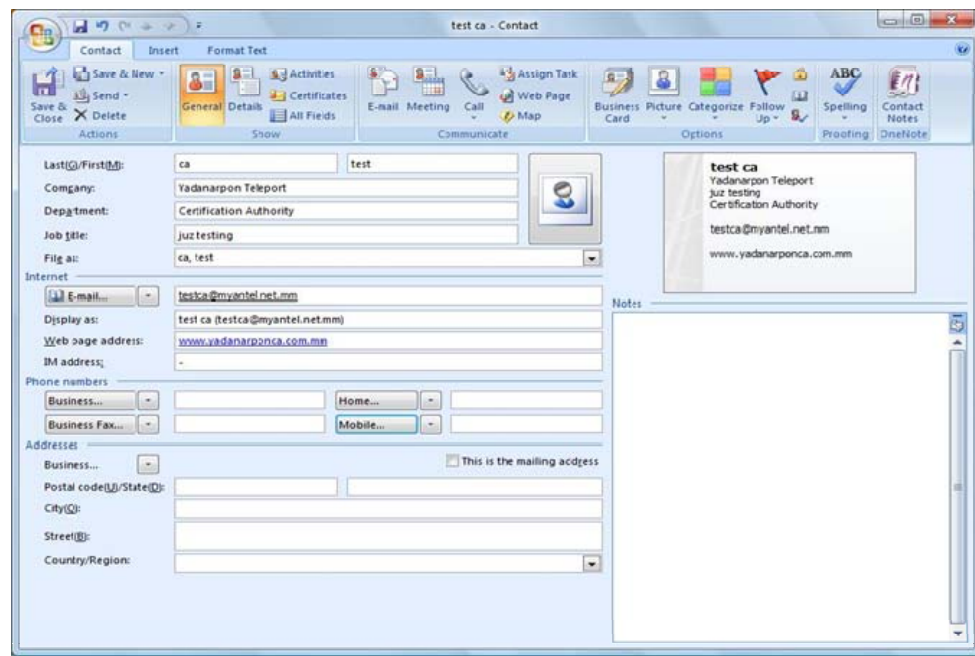
You can also search public directory for someone's Digital ID, download the ID, and import it to your address book. To search for someone's Digital ID in public directory:

1. Visit <http://www.yatanarponca.com.mm> and follow the instructions to search for, select and download a Digital ID.
2. When the browser asks to choose the format for downloading, select "someone's Digital ID" for Microsoft IE (4.0 or later) / Outlook Express/Window Live Mail (Vista) / Microsoft Outlook (2003/2007).
3. Click the Download button and save the certificate to a file on your PC.

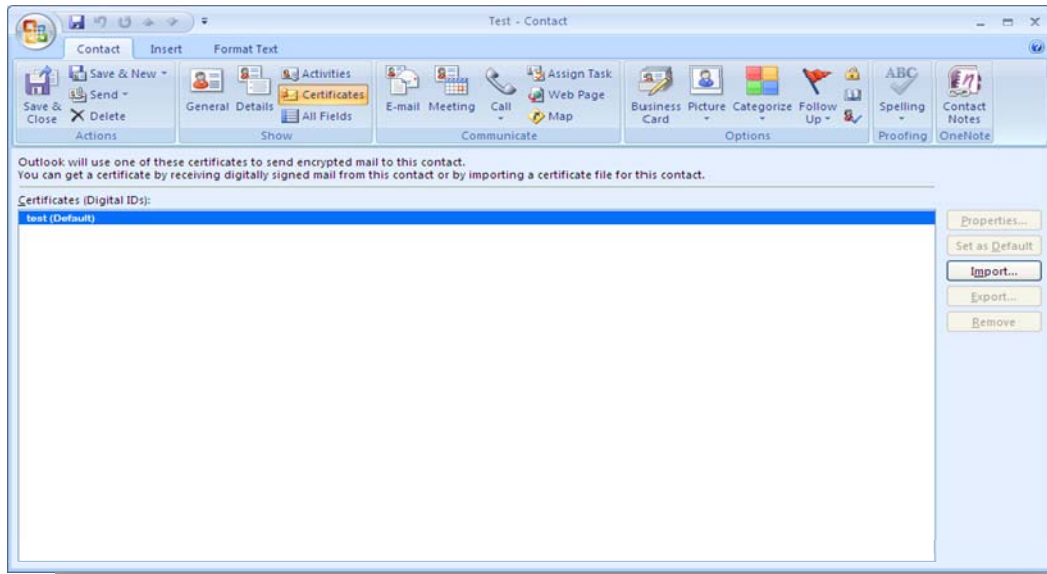
### 2.5 Import Digital ID to Contacts

To import a downloaded Digital ID into your address book:

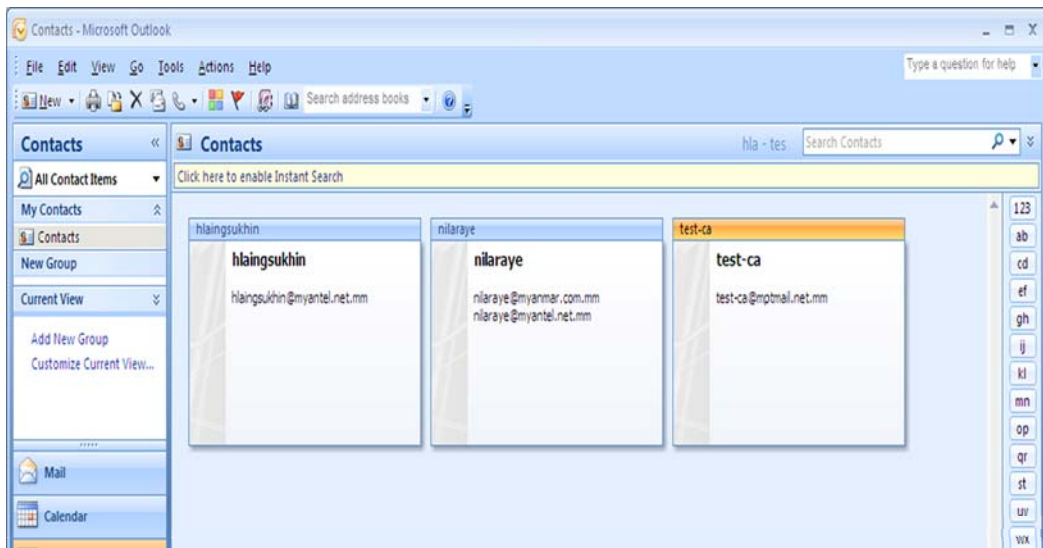
1. Open Microsoft Outlook and in the Menu bar, click **Go** button and scroll down to **Contacts** button.
2. Select **New**, type the required data in the text boxes.
3. After filling the required information click the **Certificate** button 




4. Click on the **Import** button and choose your file in your computer. Locate the Digital ID you just downloaded and click **Open** button. Click on **Save and Close** button.



If it is an existing contact, double click on your contact's name from the Contacts list.



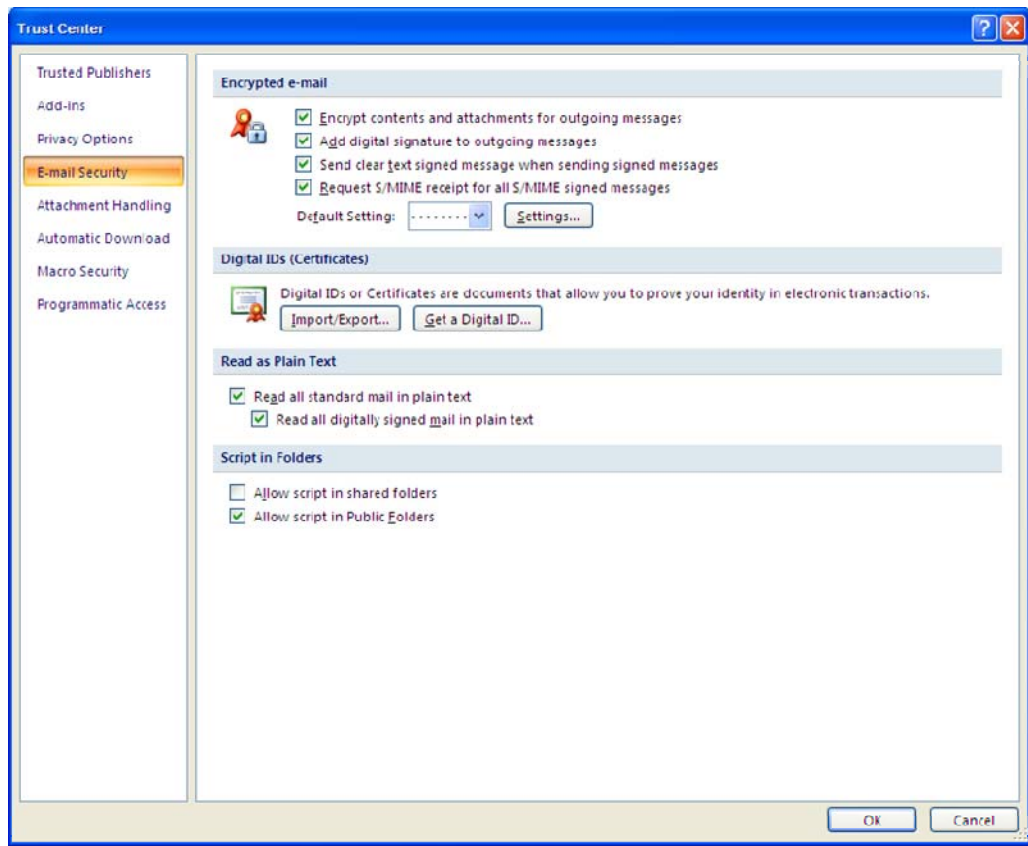
5. Click the **Certificate** button  and choose your file from the folder.
6. Locate the Digital ID you just downloaded and click **Open** button. Click on **Save & Close** button.

### 2.5.1 Import Digital ID from Trust Center (Default Signing Messages)

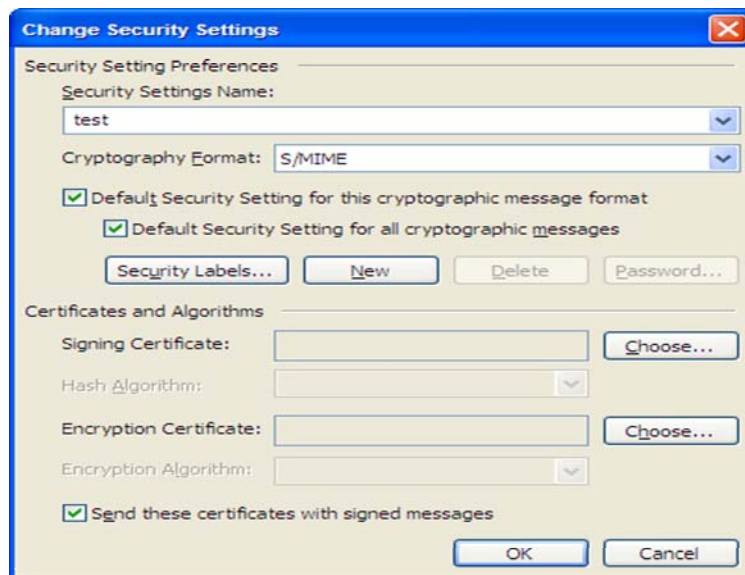
When you finish your email setting you need to import Digital ID from Trust center;

1. Go to Menu bar click **Tools** Menu and scroll down to **Trust Center** tab.
2. And choose **E-mail Security** tab and mark all check box under Encrypted e-mail.
3. Click **Settings** button.

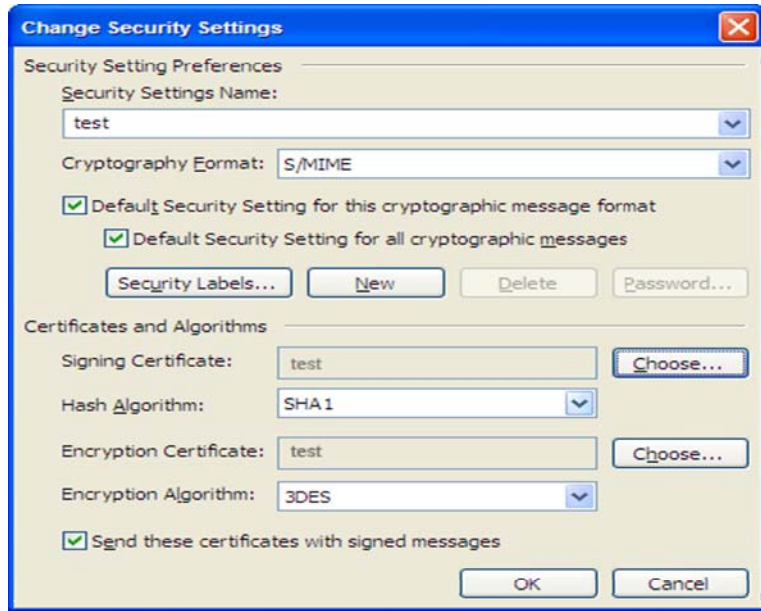




4. If you see **Change Security Settings** wizard, then type display name in **Security Settings Name:**. Mark both **Default Security Setting for this cryptographic message format** and **Default Security Setting for all cryptographic messages**.
5. Click **Choose** button from Signing Certificate:



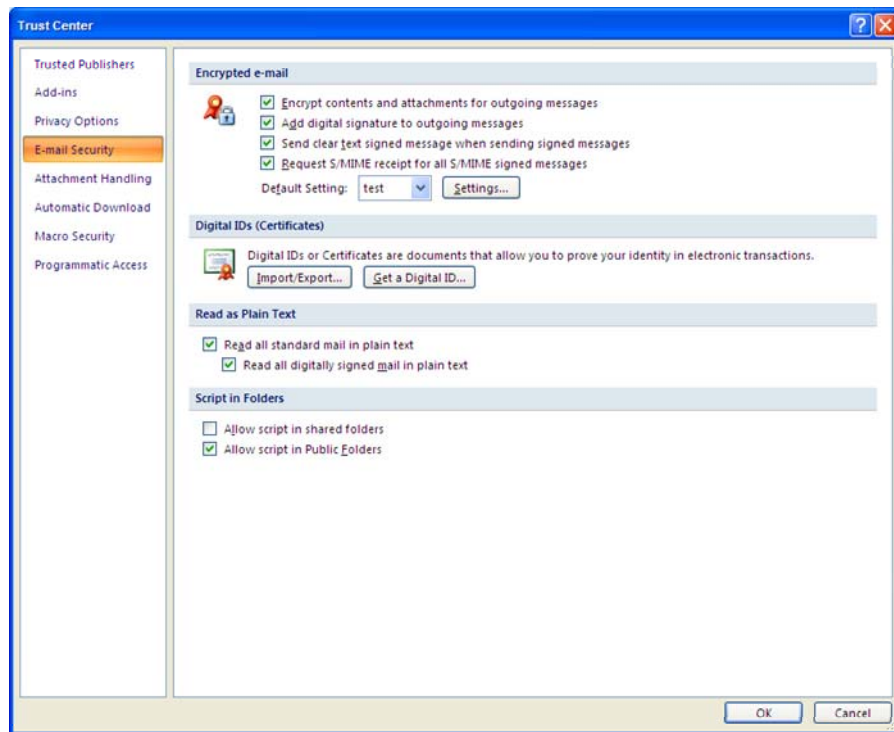
6. When you finished, click **OK** button.



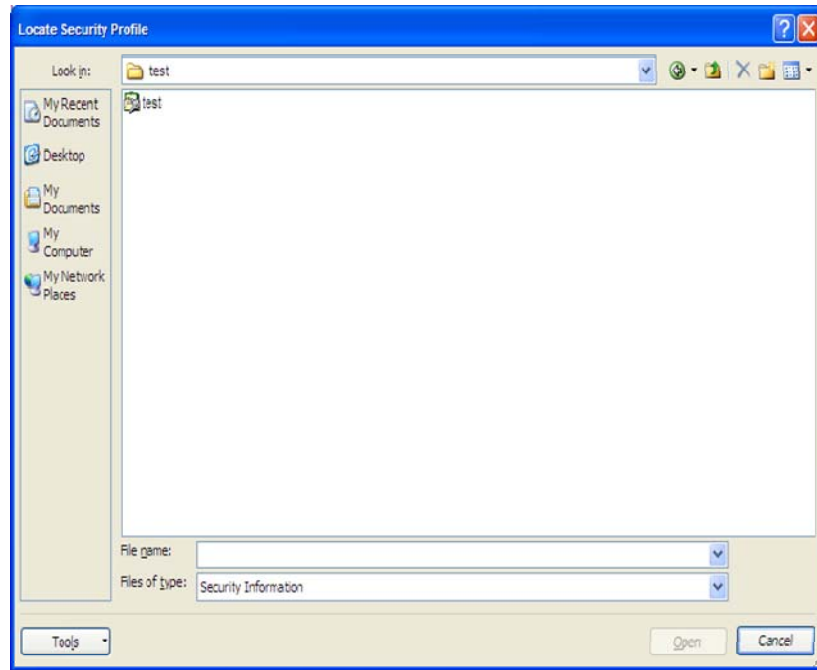
## 2.5.2 Import Digital IDs/ Certificates (Proving Identity)

Digital IDs or Certificates are documents that allow you to prove your identity in electronic transactions:

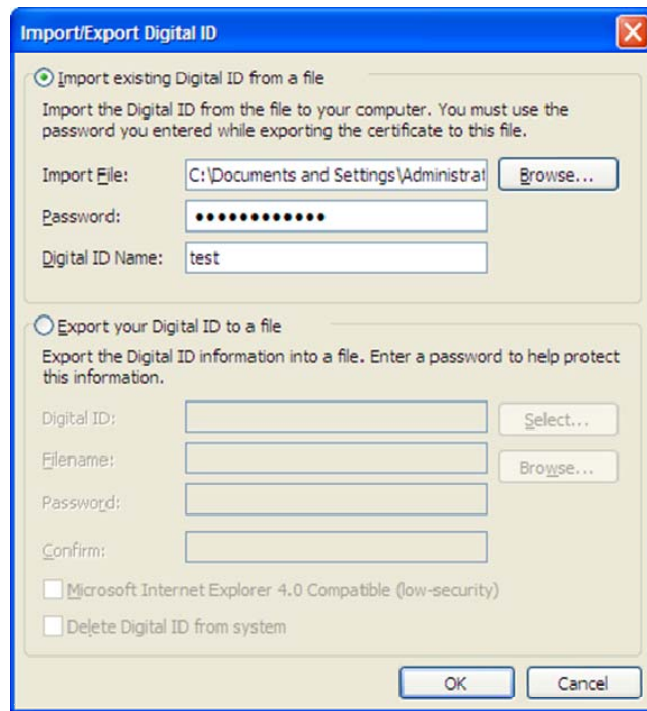
1. Click **Import/Export** button from **Digital IDs (Certificates)** under the E-mail Security tab.



2. Click **Browse** button from **Import existing Digital ID from a file** and choose our certificate security information file from your locate file.



3. Type certificate password in **Password:** text box and type digital ID name in **Digital ID Name:** text box. Check again your password and digital ID then click **OK** button.



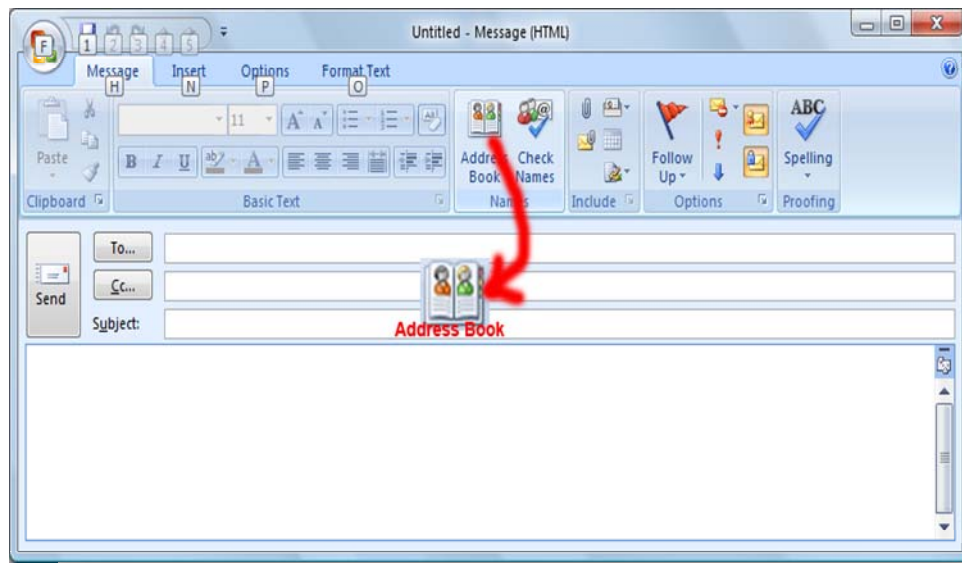
4. If you see again Trust Center status. Please click **OK** button.


### 3. Certificate Application

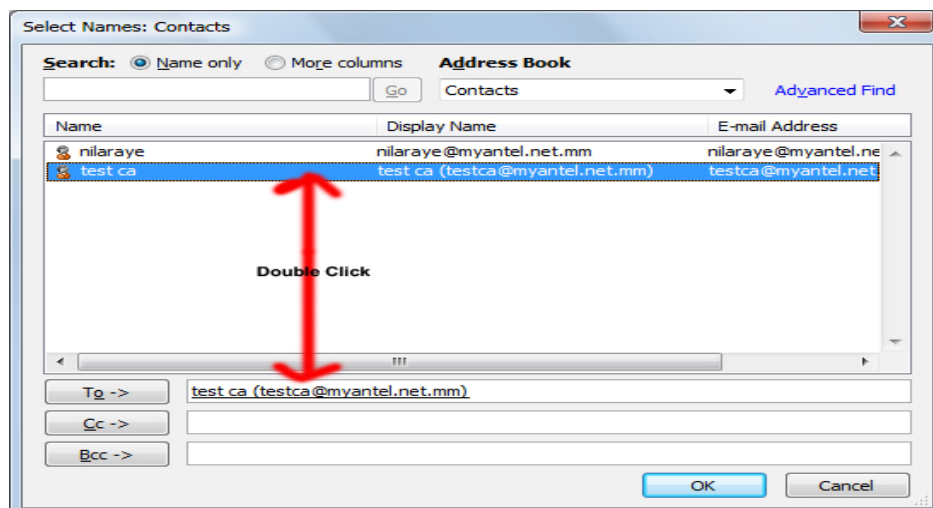
#### 3.1 Signing Individual E-Mail


You can automatically sign all your outgoing E-mail using your Digital ID installed in your browser or E-mail application. Signed E-mail allows an E-mail recipient to verify your identity. To Sign an outgoing message:

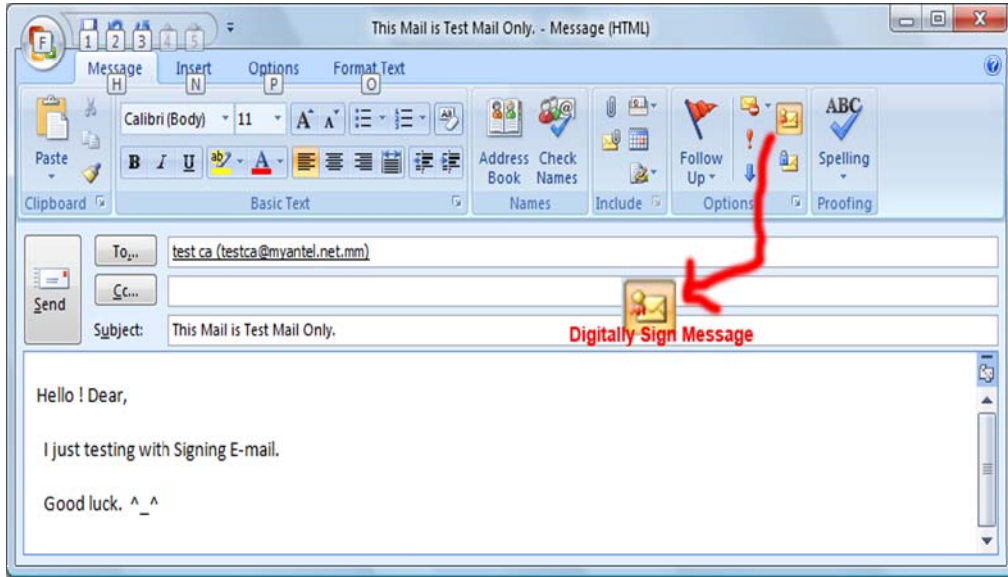
1. Click **New** button from Standard menu.



2. Add recipient's email address from **Address Book**  button. And select contact (eg. tectca@myantel.net.mm) you want to send, then double click that you select and click **OK** button.



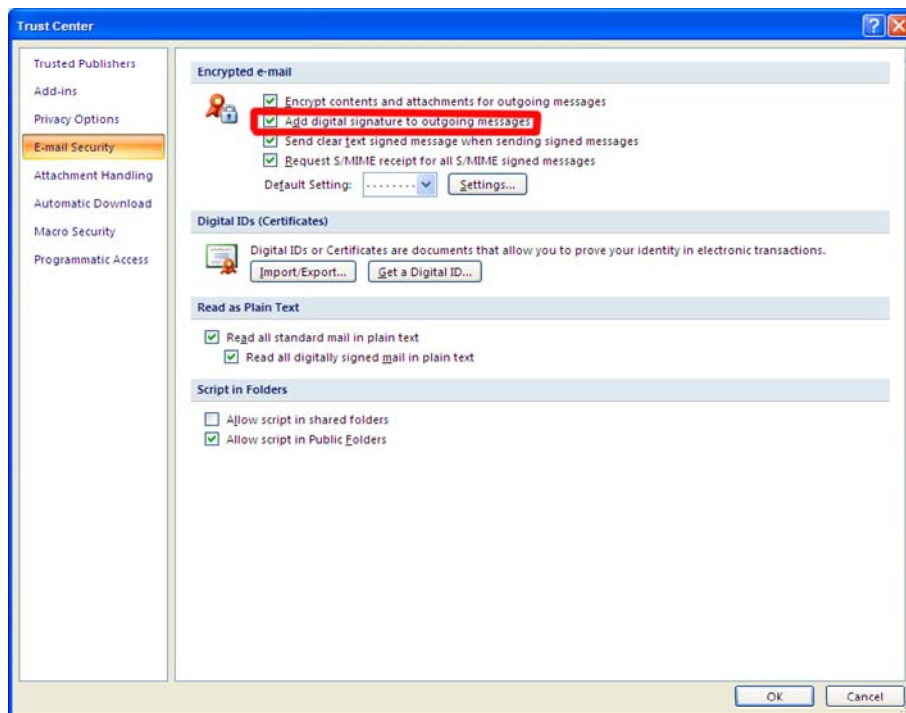
3. In the New Message window display again click on the Digital **Sign** message  button. The signed icon is displayed in the upper right corner of the address pane indicates that the message is signed.



### 3.2 Signing All Outgoing E-Mail.

To Sign an outgoing message automatically:

1. Select the Tool menu and scroll to Trust Center.
2. Select the E-mail Security tab and Mark to **Add digital signature to outgoing messages**.
3. If you do not check this box, all outgoing message will not include sign symbol.  
(To Get Digital ID, see 2.5)




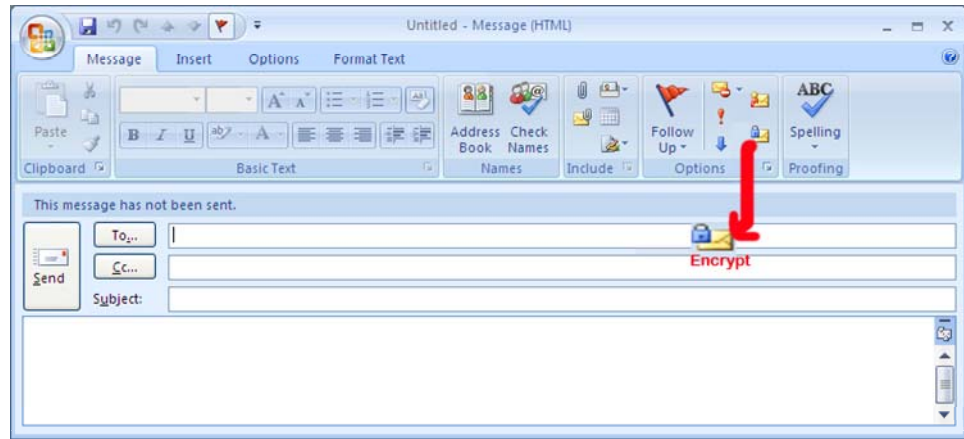
### 3.3 Encrypting your E-mail

You can encrypt individual message or configure your e-mail security option to automatically encrypt all me-mail messages to recipients who Digital IDs are store in your address book.

#### 3.3.1 Encrypting Individual Messages

To encrypt an outgoing message:

1. In the message window click on the **Encrypt Message**  button.

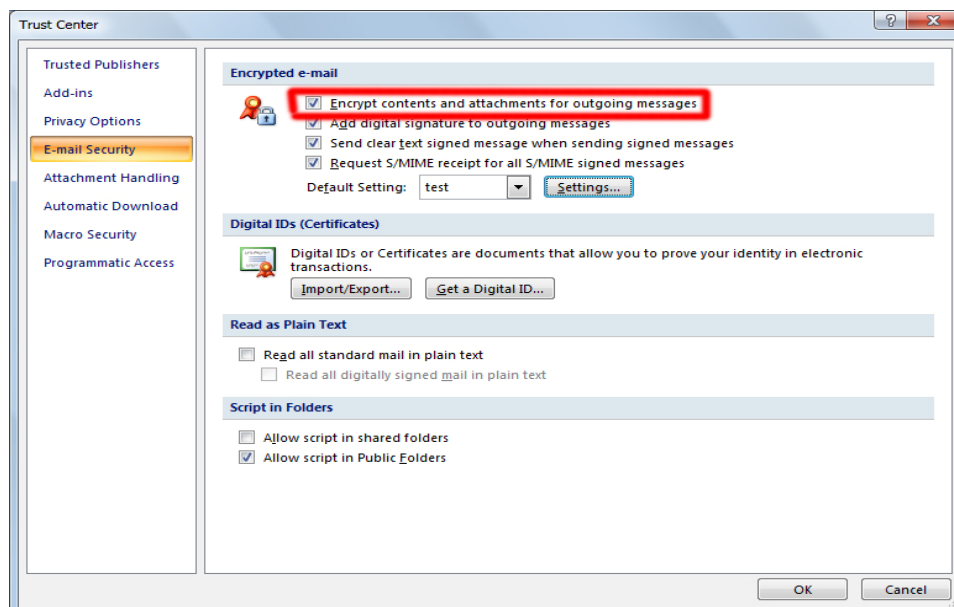


2. If you do not have recipient's Digital ID, you can't send encrypted message.
3. Add the recipient's Digital ID in your Contact and import recipient's certificate in your **Contacts**. (See – 2.4)

#### 3.3.2 Encrypting All Outgoing E-Mail

You can automatically encrypt all your outgoing email:

1. Select the **Tool** button from Menu bar and scroll to **Trust Center** tab.
2. Select the **E-mail Security** tab and mark the **Encrypt contents and attachments for outgoing message**.
3. If you mark this message, all your outgoing email will be encrypted.





## **4. Things to know...**

### **4.1 How to protect your Digital IDs**

When private keys are stored on hardware tokens, smart cards, and other hardware devices that are password- or PIN- protected, are sure to use a strong password or PIN. Never divulge your password to others. You should not write your password down, but if you must, store it in a secure location. Keep your password strong by following these rules:

1. Use eight or more characters
2. Mix uppercase and lowercase letters with numbers and special characters
3. Choose a password that is difficult to guess or hack, but that you can remember without having to write it down
4. Do not use a correctly spelled word in any language, as these are subject to “dictionary attacks” that can crack these password in minutes
5. Change your password on a regular basis. Contact your system administrator for guidelines on choosing a strong password.

To protect private keys stored in P12 (Portable format for storing/transporting a user’s private keys and certificates)/PFX (Personal Information Exchange) files, use a strong password and set your password timeout options appropriately. If using a P12 file to store private keys that you use for signing, set your password timeout option so that your password is always required (this is the default behavior). If using your P12 file to store private keys that are used to decrypt documents, ensure that there is a backup copy of your private key or P12 file so that you can continue to open encrypted documents should you lose your keys.

### **4.2 What to do if a digital ID is Lost or Stolen...**

If your digital ID was issued by a Certification Authority, immediately notify the certificate authority and request the revocation of your certificate. You should also stop using your private key.

### **4.3 Sharing Certificates with others**

Your digital ID includes a certificate that others require to validate your digital signature and to encrypt documents for you. If you know that others will need your certificate, you can send it in advance to avoid delays when exchanging secure documents. Businesses that use certificates to identify participants in signing and secure workflows often store certificates on a directory server that participants can search to expand their list of trusted identities. If you use a third-party security method, you usually don’t need to share your certificate with others. Third-party providers may validate identities using other methods, or these validation methods may be integrated with Acrobat. See the documentation for the third-party provider.

When you receive a certificate from someone, their name is add to your list of trusted identities as a contact. Contacts are usually associated with one or more certificates and can be edited, removed, or unassociated with another certificate. If you trust a contact, you can set your trust setting to trust all digital signatures and certified documents created with their certificate. You can also import certificates from a certificate store, such as the windows certificate store. A certificate store may contain numerous certificates issued by different certification authorities.