

# YATANARPON TELEPORT COMPANY LTD.,

YATANARPON  
CERTIFICATION  
AUTHORITY

## USER MANUAL FOR SECURE E-MAIL MICROSOFT OUTLOOK (2003)

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>

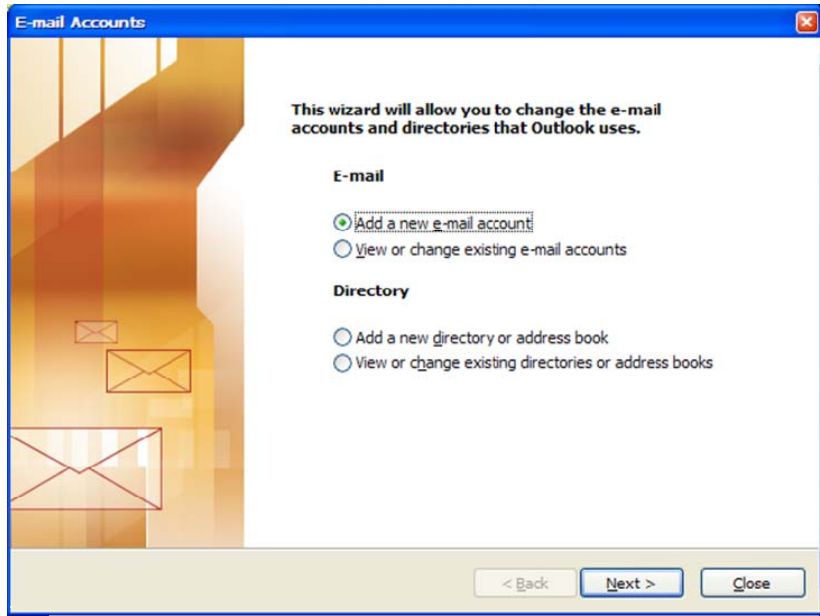
## **Table of Contents**

- 1. Creating E-mail Account in Microsoft Outlook 2003**
- 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 Import a Digital ID**
  - 2.5 Import 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**

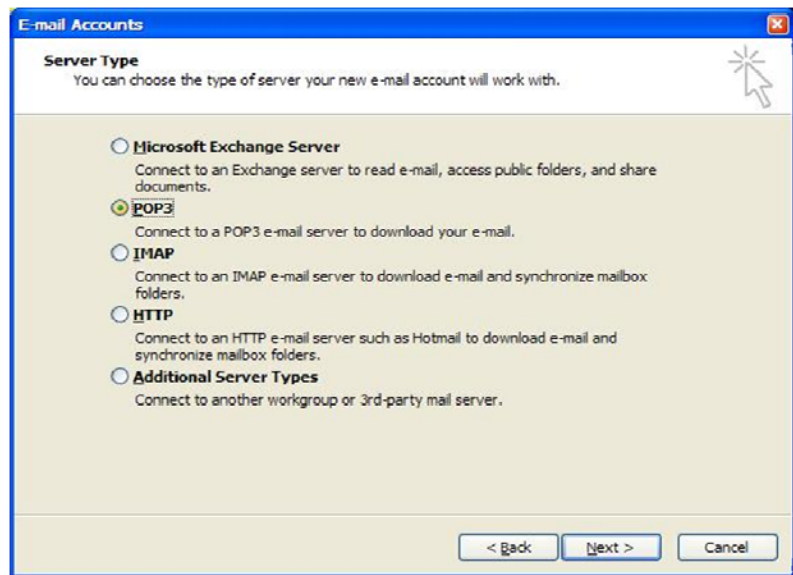
1. **Creating E-mail Account in Microsoft Outlook 2003**

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. Choose **Add a new e-mail account** and click **Next** button.



3. Choose **POP3** server type and click **Next** button.



- In E-Mail dialog box fill the **User Information** and **logon Information** in appropriate boxes. In **logon Information**, please fill the user name from the email address and the password which you use for your email address.
- In **Server Information**, type the mail server numbers. These numbers (marked with red color) can be changed according to the domain name. Then, click **Next** button.

**E-mail Accounts**

**Internet E-mail Settings (POP3)**  
Each of these settings are required to get your e-mail account working.

**User Information**  
Your Name:   
E-mail Address:

**Server Information**  
Incoming mail server (POP3):   
Outgoing mail server (SMTP):

**Logon Information**  
User Name:   
Password:   
 Remember password  
 Log on using Secure Password Authentication (SPA)

**Test Settings**  
After filling out the information on this screen, we recommend you test your account by clicking the button below. (Requires network connection)

< Back   Next >   Cancel

- You will see the following dialog box and Click **Finish**.

**Add New E-mail Account**

**Congratulations!**

You have successfully entered all the information required to setup your account.  
To close the wizard, click Finish.

< Back   Finish

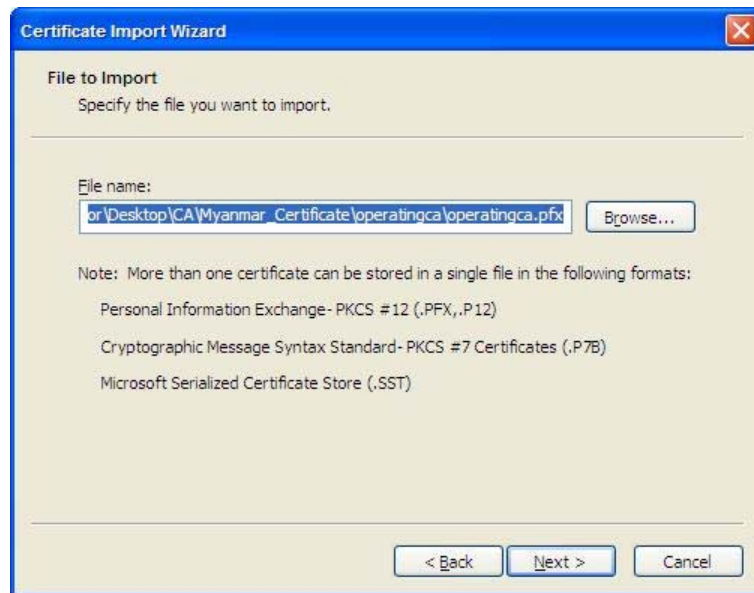
## 2. Certificate Installation.

To use digital ID in your system, you need to install 3 certificate files provided by Yatanarpon CA . They are,

1. **Subscriber / User Certificate Installation (.PFX) File**
2. **Certification Authority (.CER) File and**
3. **Root Certification Authority (.CER) File**

### 2.1 Subscriber/ User Certificate Installation

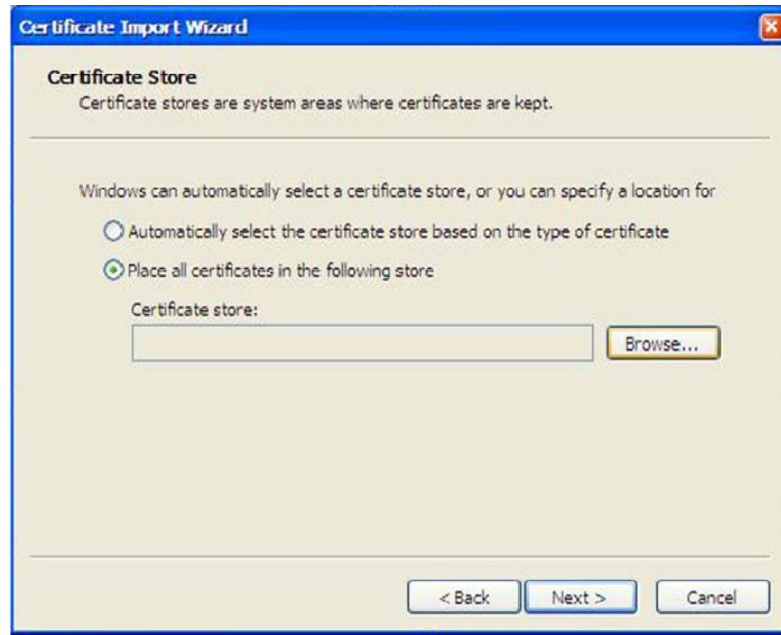
1. Click your Certificate (.pfx) file.
2. You will see Certificate Import Wizard and click **Next** button.
3. Specify the file you want to import by clicking **Browse** button and choose your file, then click **Next** button.



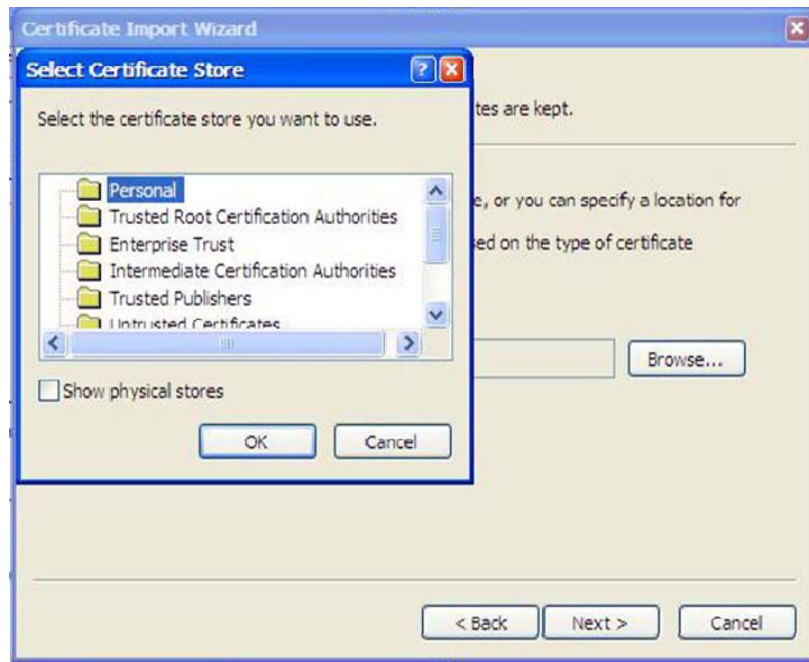
4. For the security, the private key is protected with a password.  
Type the password for the private key. Mark all **Check** boxes and click **Next** button.



5. Select **Place all Certificates in the following store** and click **Browse** button then click **Next**.



6. Select the **Personal** Folder and click **OK**. Then click **Next** button in **Certificate Import Wizard** dialog.



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



8. After completing the Certificate Import Wizard, you need to import a new private exchange key. You can set security level (High or Medium).



9. Click Set **Security Level** button and tick **High** check box. (If you want to set **High security level**) and then click Next button.



10. Importing a new private exchange key dialog will appear. Type password and Confirm: password and then click Finish button.



11. Click **OK** button from the Certificate Import Wizard dialog. You are about to finish the Certificate Installation.



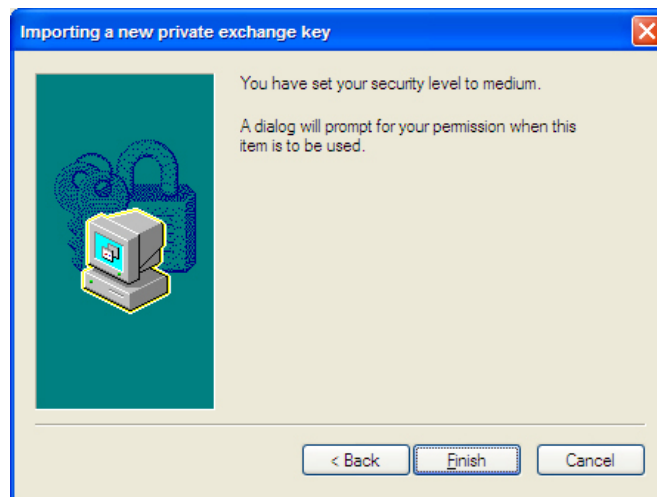


**You can set Medium security level too:-**

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



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



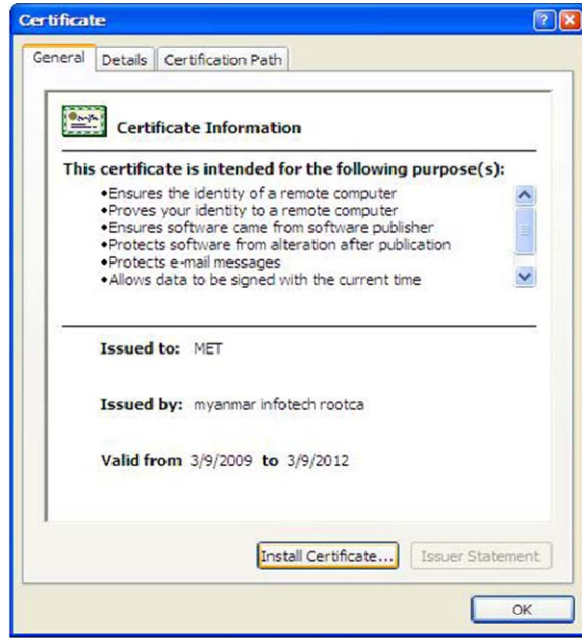
11. Click **OK** button and you Finish Certificate installation.



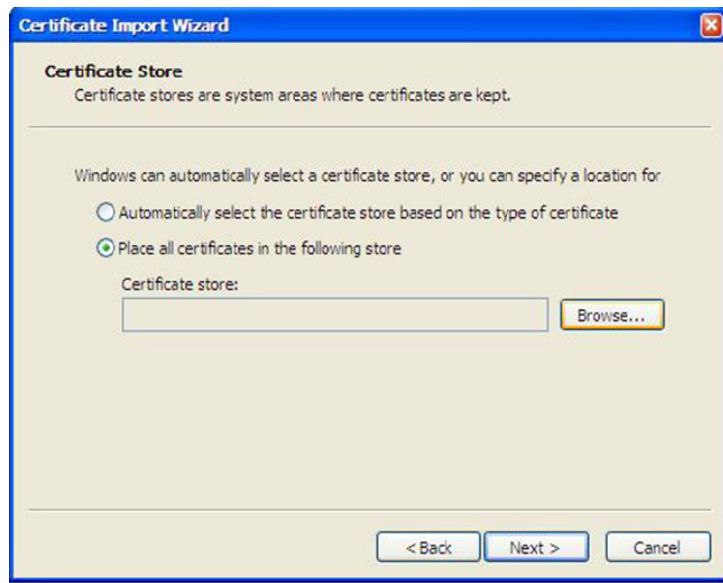
## 2.1 CA certificate Installation (.CER)

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

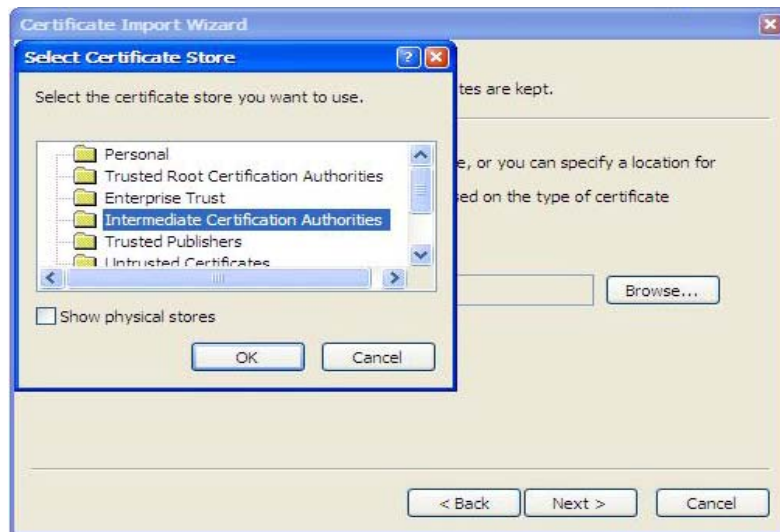
1. Click require (MET.cer) file.
2. Click **Install Certificate** button.



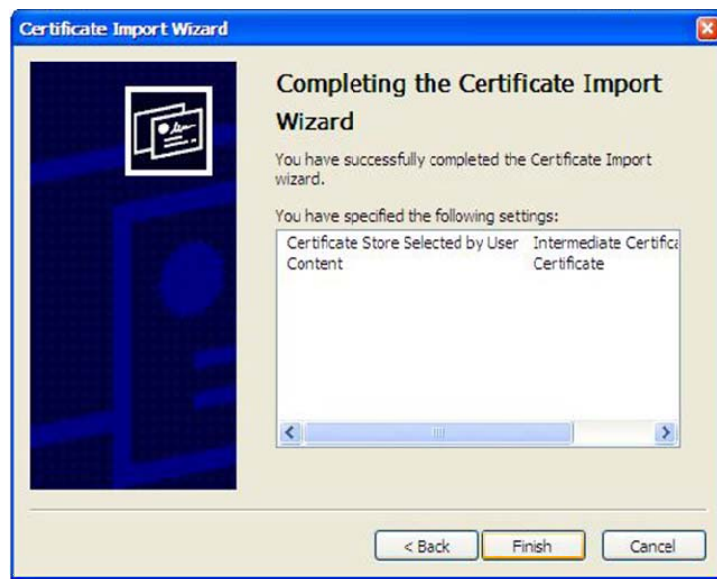
3. Select **Place all Certificate in the following store** button from the Certificate Import Wizard window , click **Browse** button and then Click **Next** button.



4. Select the **Intermediate Certification Authorities** and click **OK** button click **Next** button in **Certificate Import Wizard** status window.



5. The certificate Import Wizard is completed and Click **Finish** button.



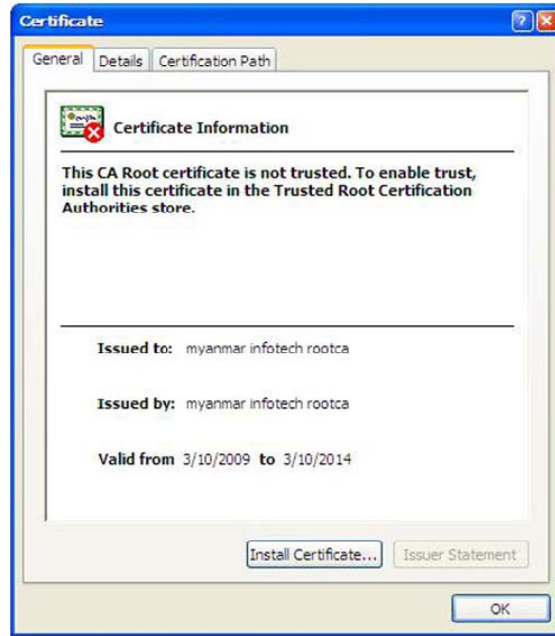
6. The Import was successful and Click **OK** button.



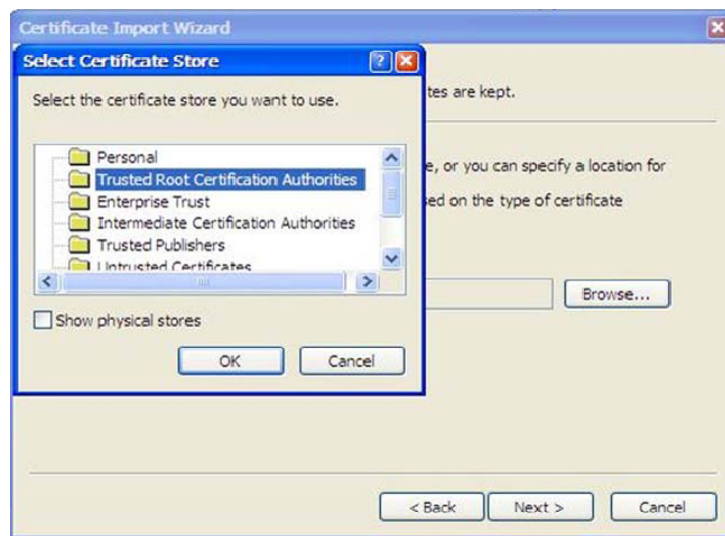
## 2.2 Root Certificate Installation (.Cer) File

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

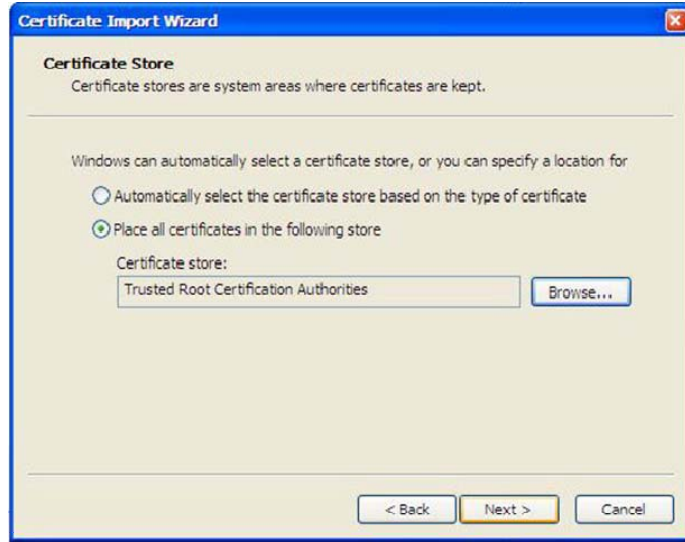
1. Click require (Myanmar InfoTech Rootca .cer) file.
2. Click **Install Certificate** button and click **Next** button.



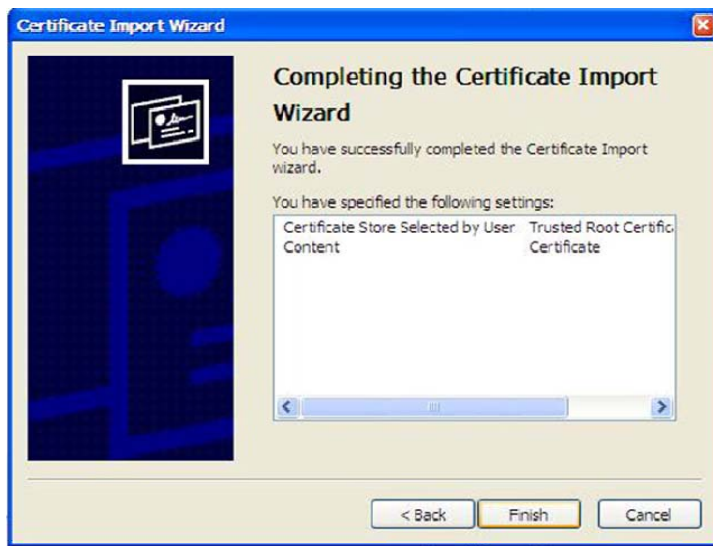
3. Select **Place all Certificate in the following store** button from the Certificate Import Wizard dialog and click **Browse** button. You will see the Select Certificate Store Dialog and choose **Trusted Root Certification Authorities** and Click Next >.



4. After selecting **Trusted Root Certification Authorities** tab from Select Certificate Store dialog you will see again Certificate Import Wizard window as follow and click **Next** button



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



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



## 2.3 Get Digital ID

### 2.3.1 Downloading and Importing a Digital ID

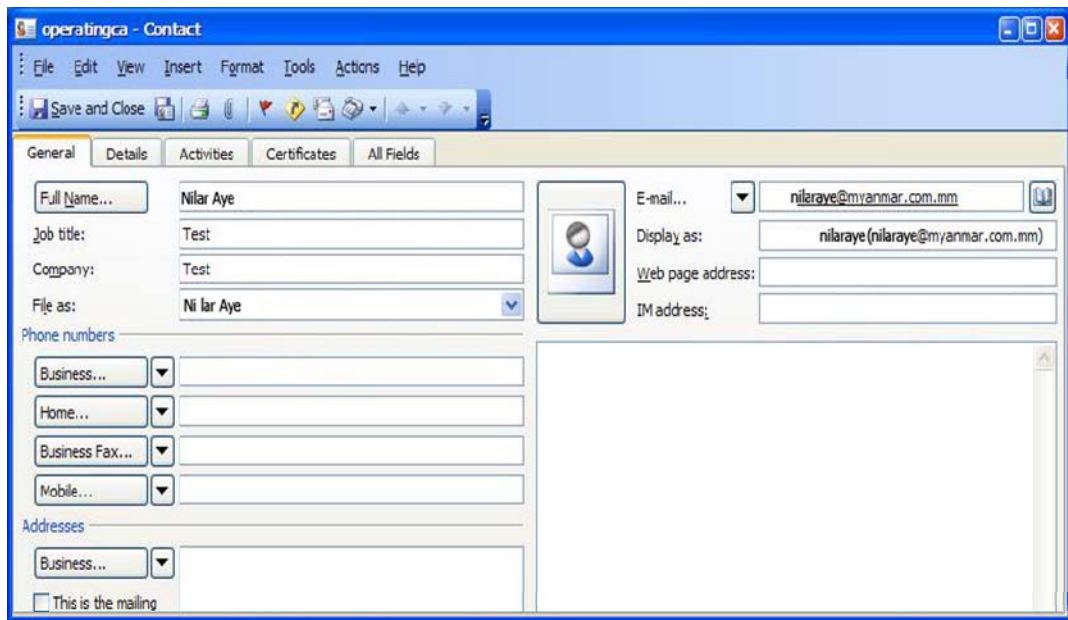
You can also search public directory for someone's Digital ID, download the ID, and import it to your address book. To search for someone's Digital ID in public directory:

1. Visit <http://www.yadanarponca.com.mm> or <http://www.yandarponca.com.mm/repositry> 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 / Microsoft Outlook (2003/2007).
3. Click the Download button and save the certificate to a file on your PC.

## 2.4 Import Digital ID to Contacts

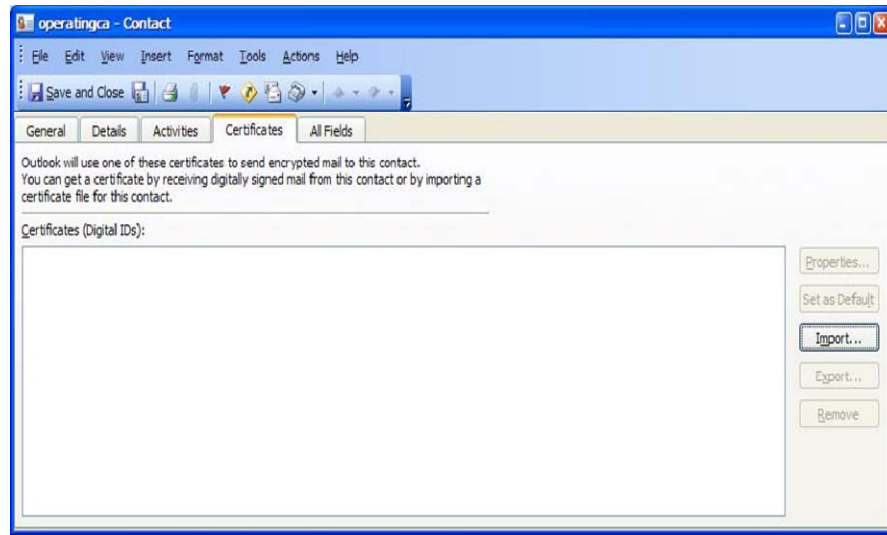
To import a downloaded Digital ID into your address book:

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 require information click the **Certificate** tab.





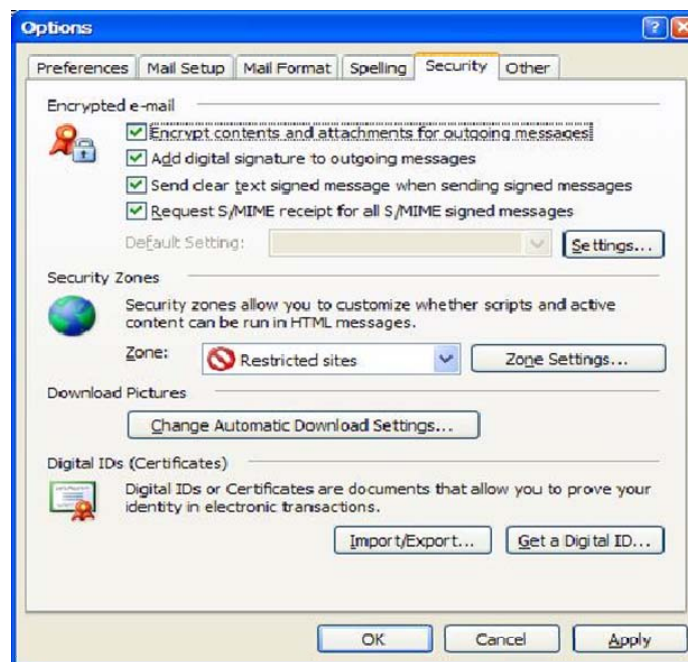
4. Click on the **Import** button and choose your file from your computer.
5. Locate the Digital ID you just downloaded and click **Open** button. Then Click on **Save and Close** button.

## Two types of Importing Digital ID

### 2.4.1 Importing Your Digital ID From Trust Center( Default Signing Messages)

When you finish configuring your email setting, you need to import your Digital ID to security option;

1. Go to Menu bar click **Tools** Menu and scroll down to **Options** tab.
2. And choose **Security** tab and mark all check box under Encrypted e-mail, (All outgoing messages will be include signed & encrypted message) { see- under 3. Certificate Application. }
3. Click **Settings** button.

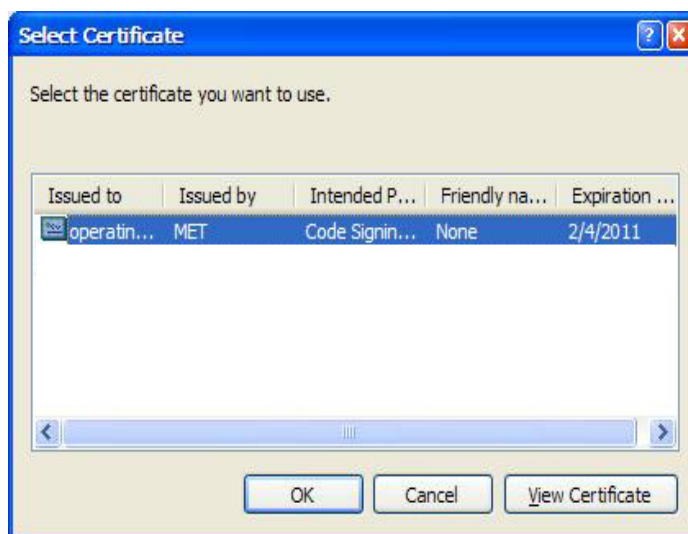


After Clicking **Settings** from **Option** dialog,

1. You will see **Change Security Settings** wizard as follow, then type display name in **Security Settings Name:** .
2. Mark both **Default Security Setting for this cryptographic message format** and **Default Security Setting for all cryptographic messages.**
3. Click **Choose** button from Signing Certificate:



4. Choose your file and click **OK** button.



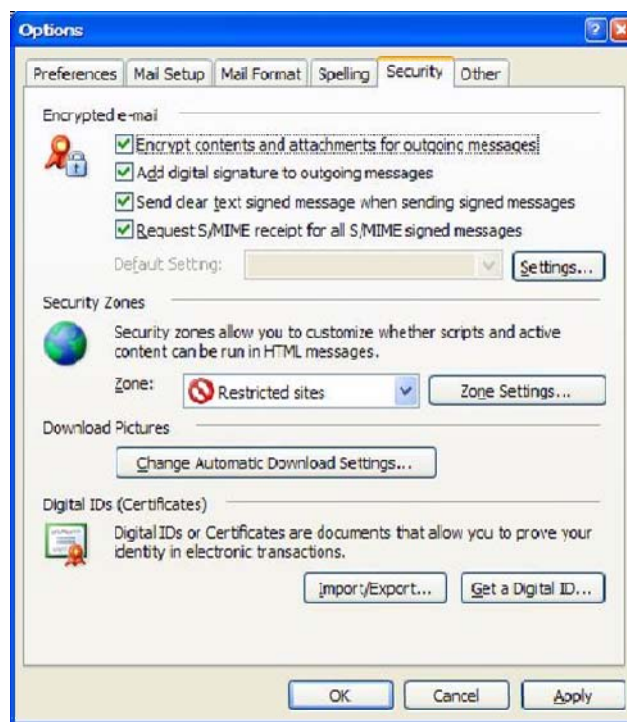


5. When you finished filling **Change Security Settings**, click **OK**.

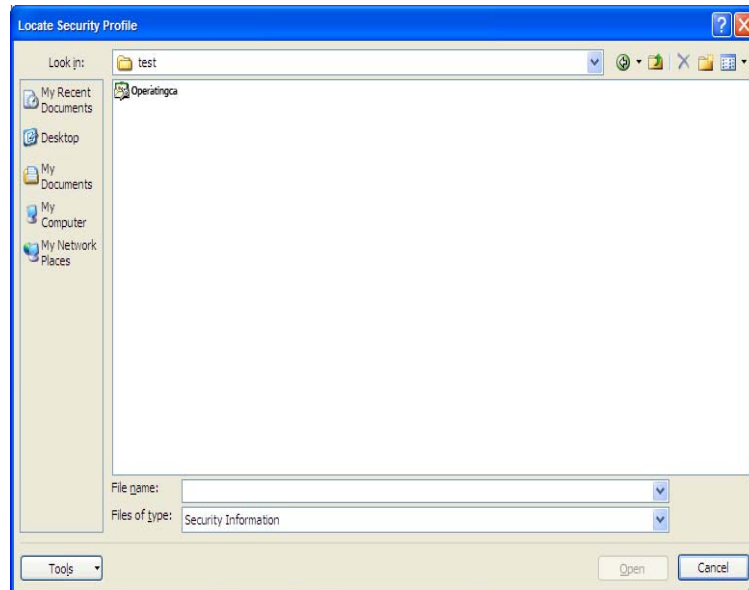


#### 2.4.2 Importing Digital IDs/ Certificates (Proving Identity)

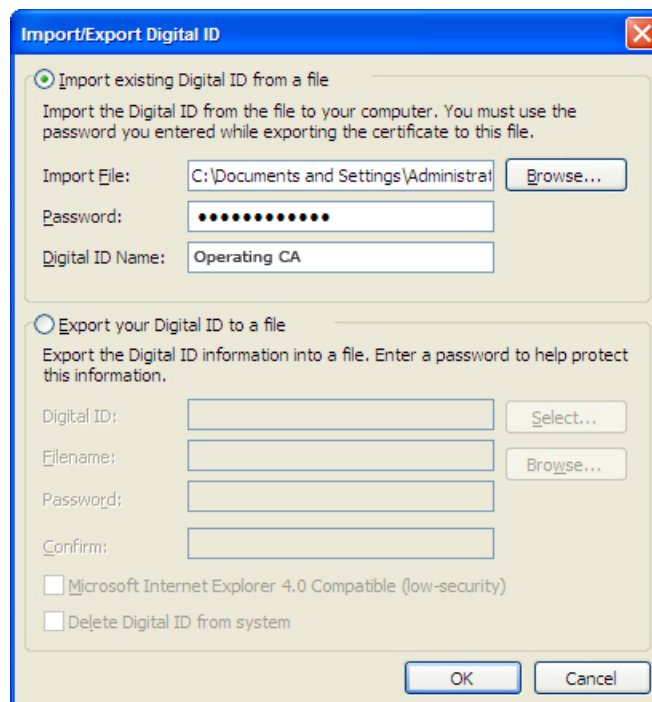
1. Go to Menu bar click **Tools** Menu and scroll down to **Options** tab.
2. And choose **Security** tab and mark all check box under Encrypted e-mail, (All outgoing messages will be include signed & encrypted message) {see- under 3. Certificate Application.}
3. Click **Import/Export** button from **Digital IDs (Certificates)** under **Security** tab.



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



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



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

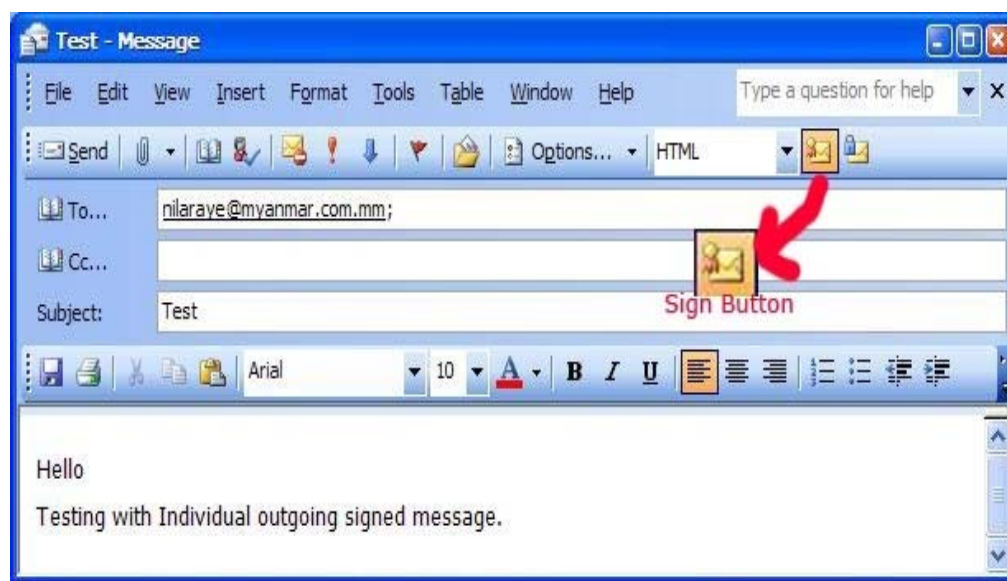
### 3. Certificate Application

#### 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. Click on the Digital **Sign** message  button.

The signed icon will be displayed in the upper right corner of the address pane. It indicates that the message has signed.

#### 3.2 Signing All Outgoing E-Mail.

To Sign an outgoing message automatically, you already mark Add digital signature to outgoing messages check box.



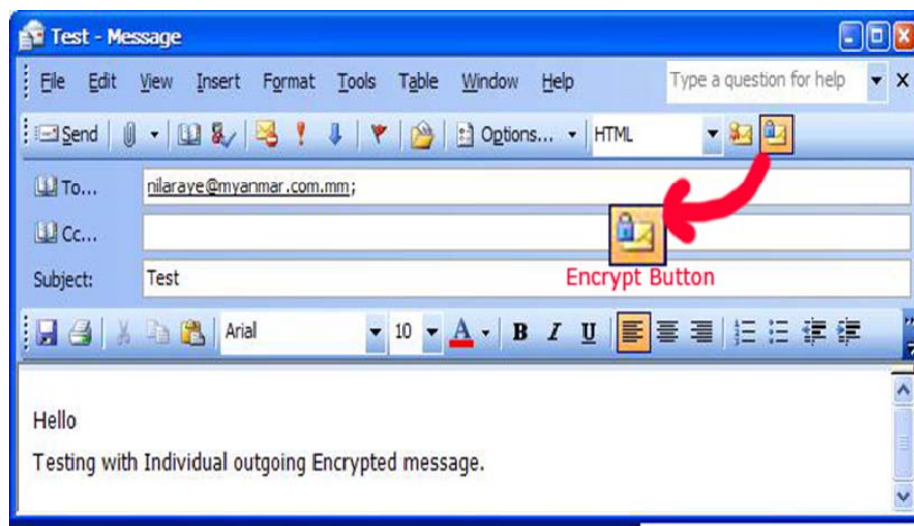
1. Select the **Tools** menu and scroll to **Options** tab.
2. Select the **Security** tab and Mark to “**Add digital signature to outgoing messages.**”
3. If you do not check this box, all outgoing message will not include sign symbol.


### 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.

#### 3.3.2 Encrypting All Outgoing E-Mail

You can automatically encrypt all your outgoing email, You already mark Encrypt contents and attachment for outgoing messages check box.

1. Select the **Tool** button from Menu bar and scroll to **Options** tab.
2. Select the **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.  
{see image -3.1}

## 4. Things to know...

### 4.3 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, be 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.

#### **4.4 What to do if a digital ID is lost or stolen**

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

#### **4.5 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 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 your 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.