# YATANARPON TELEPORT COMPANY LTD.,

YATANARPON CERTIFICATION AUTHORITY

# USER MANUAL FOR SECURE E-MAIL WINDOW LIVE MAIL (VISTA)

**Yatanarpon Teleport Company Ltd.,**
**Hlaing Universities Campus,**
**Hlaing Township, Yangon, Myanmar**
**Ph: 951-652233, Fax: 951-652244**
**Email:opetraingca@myanmar.com.mm**
**URL: http://www.yatanarponca.com.mm**

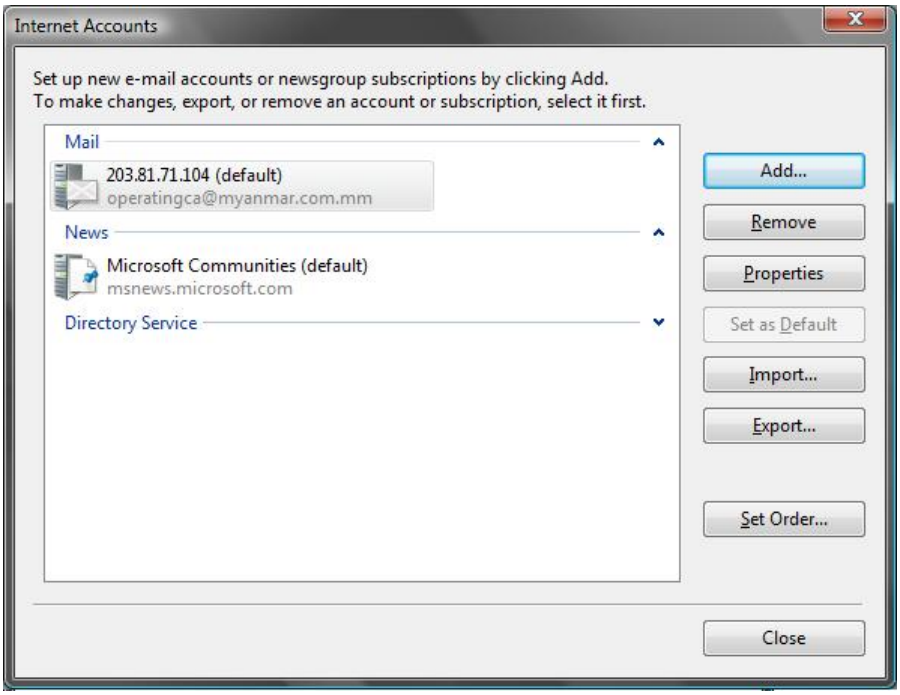
# Table of Contents


1. Creating Email Account in Window live Mail
2. Certificate Installation
   - 2.1 Subscriber/ User Certificate installation
   - 2.2 CA certificate Installation (.CER)
   - 2.3 Root certificate Installation (.cer) File
   - 2.4 How to get Digital ID
     - 2.4.1 Downloading and Importing a Digital ID
   - 2.5 Importing Digital ID to Contacts
3. Certificate Application
   - 3.1 Signing Individual E-Mail
   - 3.2 Signing All Outgoing E-Mail
   - 3.3 Individual Encrypting your E-mail
   - 3.3.1 Encrypting Individual Messages
   - 3.3.2 Encrypting All Outgoing E-Mail
4. Things to Know
   - 4.1 How to protect your digital IDs
   - 4.1 What to do if a digital ID is lost or stolen
   - 4.2 Sharing certificates with others

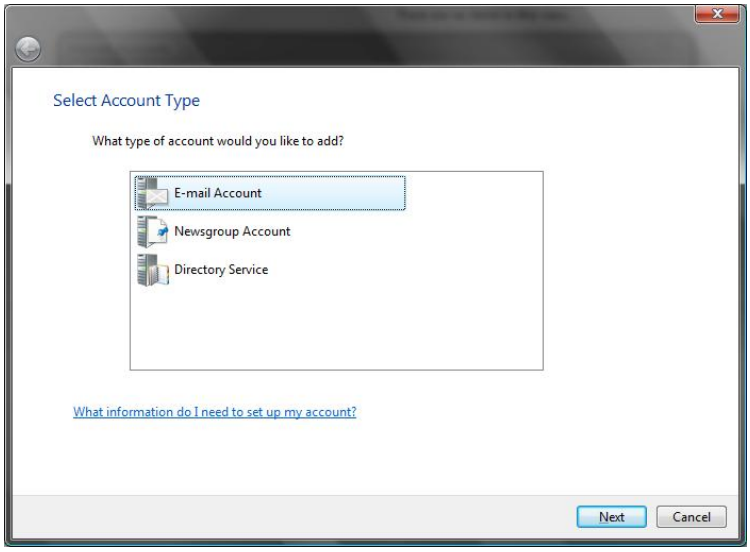
## 1. ***Creating E-mail Account in Window Live Mail***

To create email account setting in Window Live Mail:

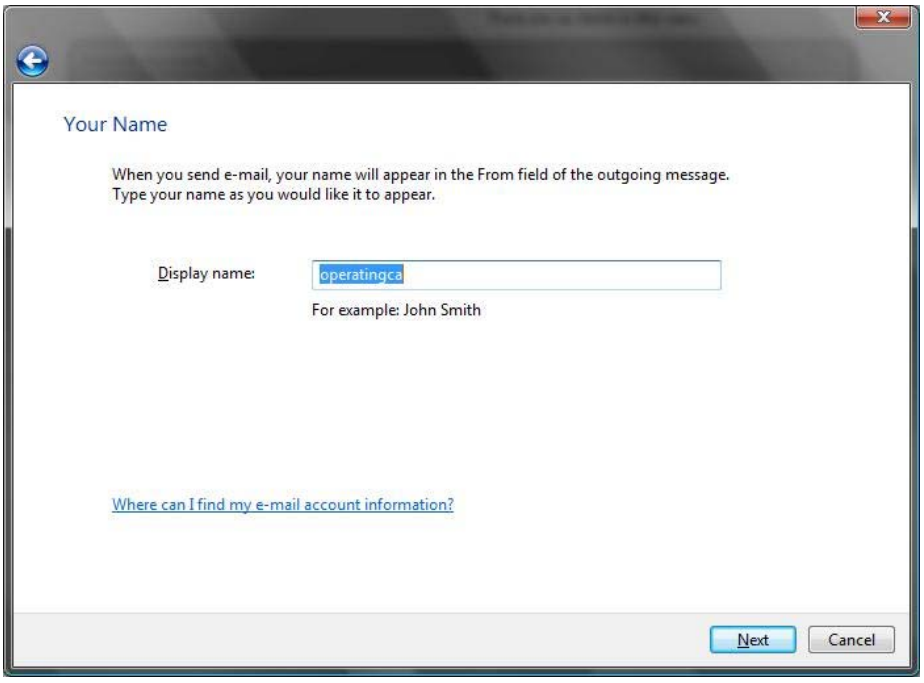
1. Go to **Menu** bar and select **Tools** and scroll down to **Account**.
2. Click **Add** button



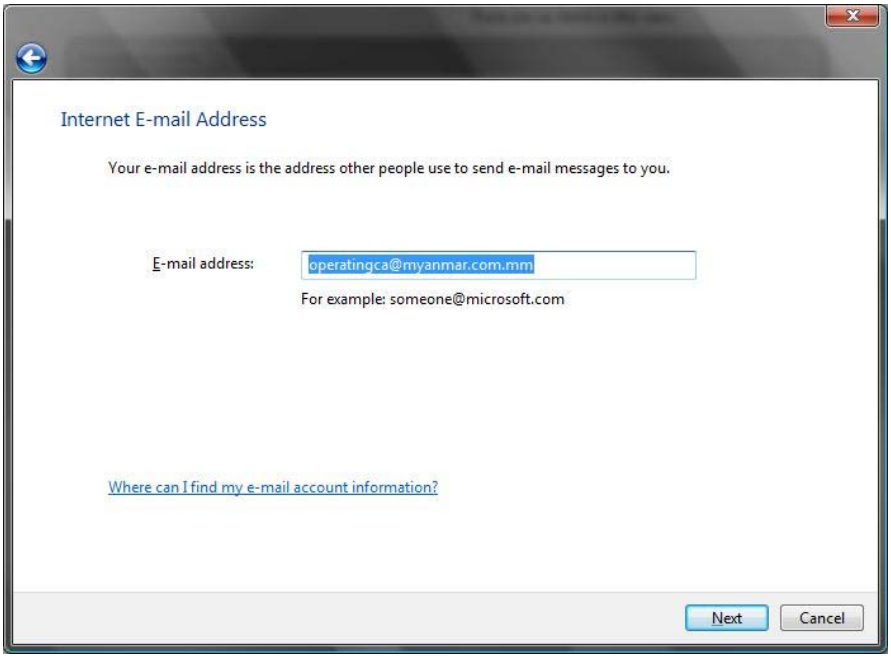

3. You will see **Select Account Type Dialog** and choose **Email Account**.
4. Click **Next** button.



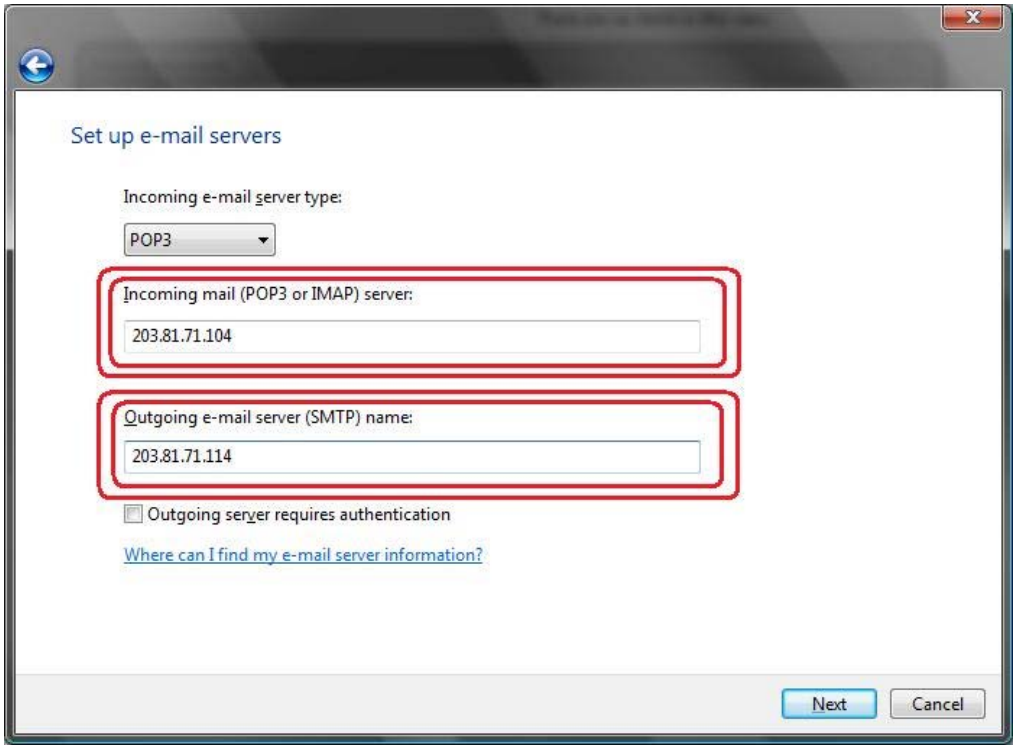
5. Type your name in the following **Display name:** text box.
6. Then click **Next** button.



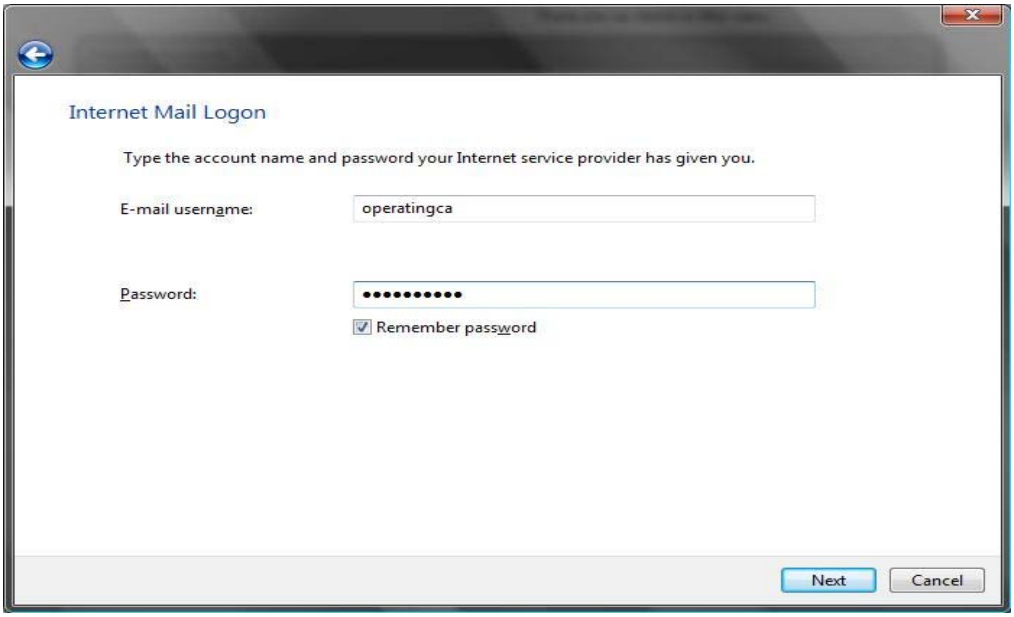

7. Type your Email address in **E-Mail Address :** text box.
8. Click **Next** button.



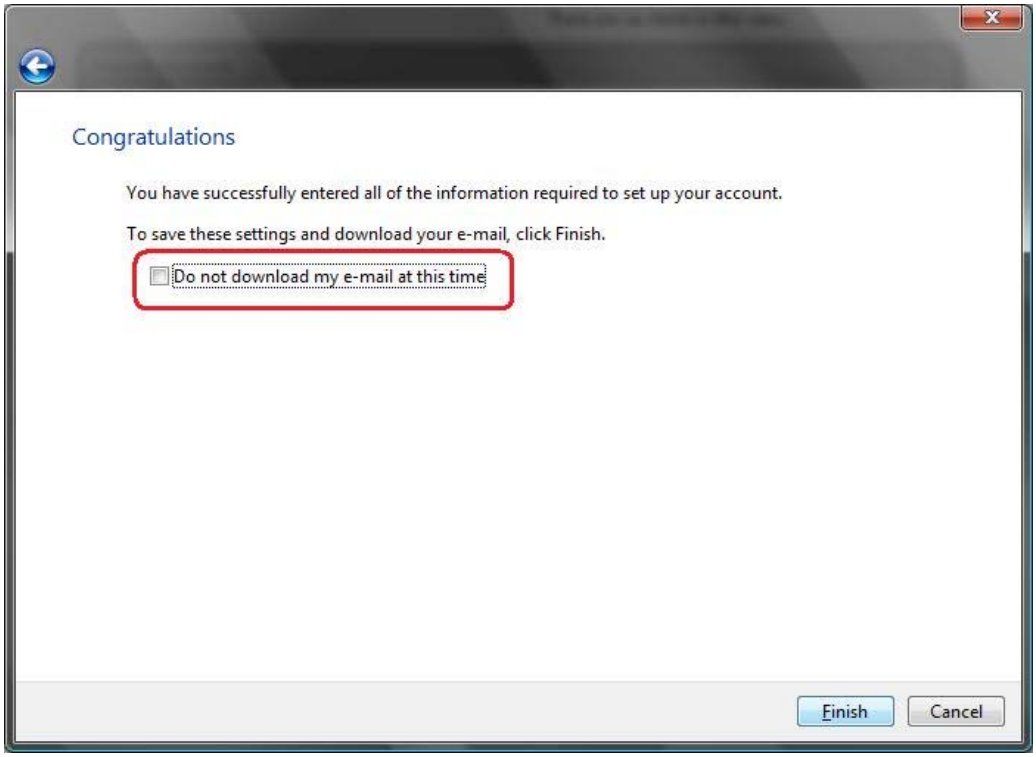
9. Type mail server numbers in Incoming e-mail server type:, Incoming mail (POP3 or IMAP) server and Outgoing E-Mail Server (SMTP) name. The following numbers are mail servers used for myanmar.com.mm.




10. Then you will see Mail logon and fill up your password, then click **Next**.



Finally your account creation is finished. If you don't want to download your mail at this time, mark (**Do not download my email at this time**), and click **Finish** button.




## 2. ***Certificate Installation.***

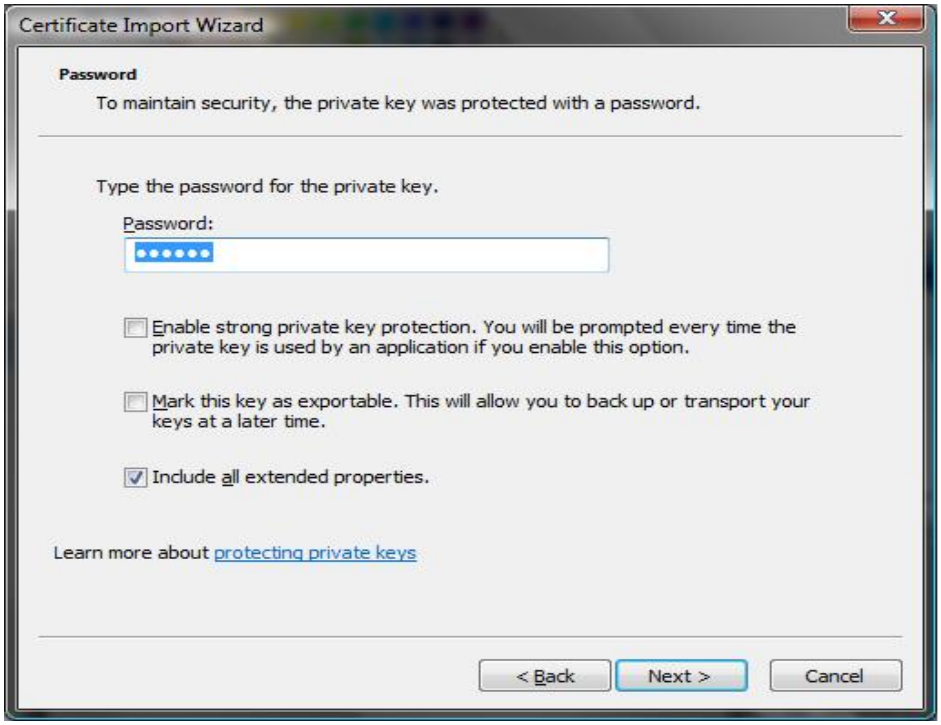
To use digital ID in your system, you need to install 3 certificate files as follow;

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

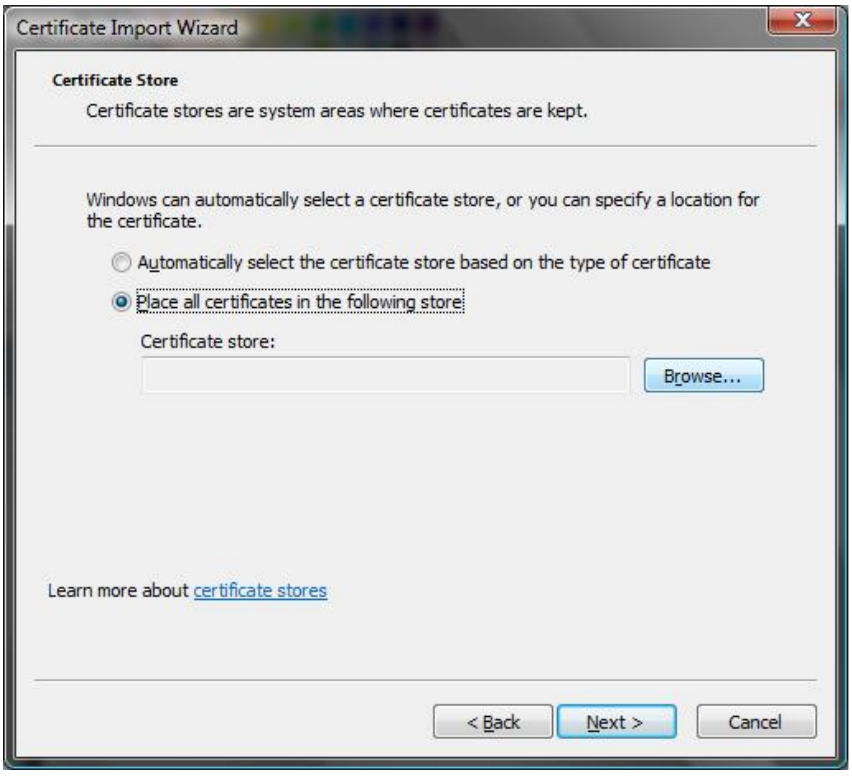
### *2.1 Subscriber/ User Certificate installation*

1. Click your certificate (.**pfx**) file.
2. You will see **Certificate Import Wizard**, click **Next** button.
3. Specify the file you want to import by clicking **Browse** button and choose your file then click **Next** button.
4. To maintain security, the private key was protected by password. Type the password for the private key.

5. You can select all **Check** buttons or can choose one you like and click **Next** button.

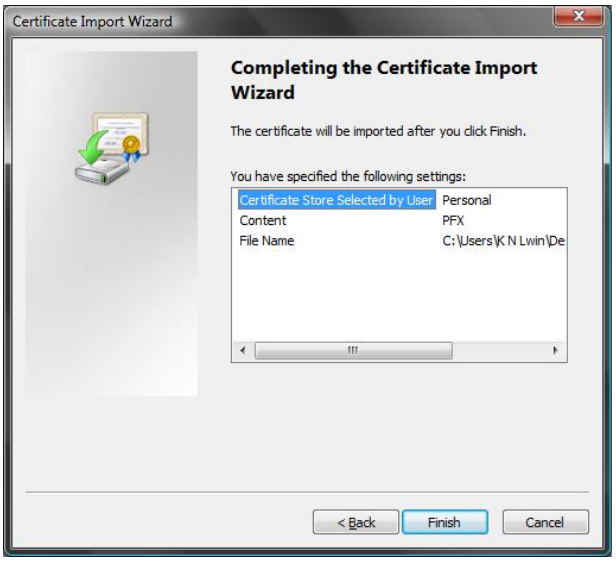



6. Select **Place all Certificate in the following store** & click **Browse** button. You will see the **Select Certificate Store dialog** and choose the **Certificate Store**.



7. Select the **Personal** folder and click **OK** button. Then click **Next** button in **Certificate Store** status window.


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

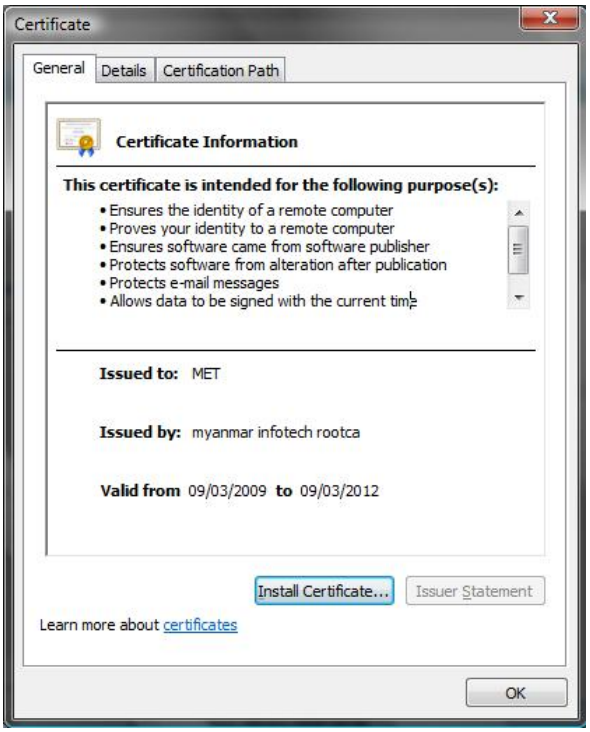



9. Click **OK** button to finish Certificate installation.

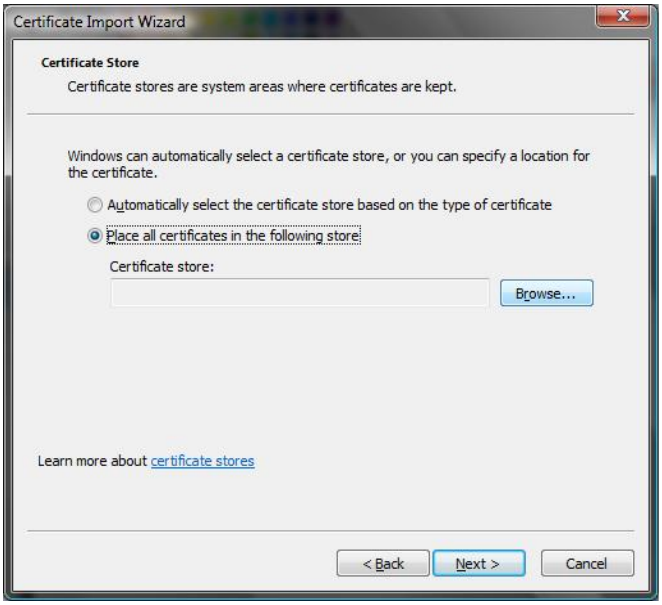
## ***2.2 CA certificate Installation (.CER)***

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

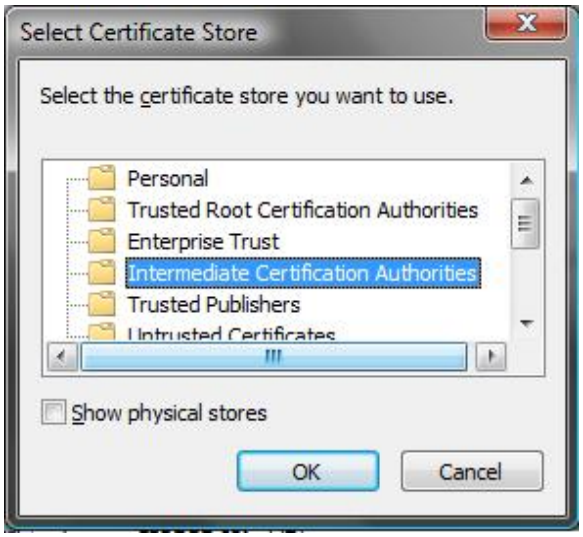
1. Click the required (MET.cer) file.
2. Click Install Certificate button and follow the steps.



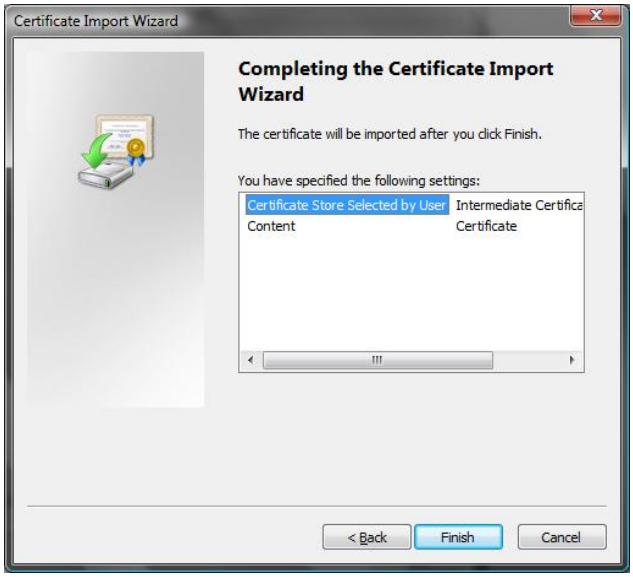

3. Select **Place all Certificate in the following certificate store** and click **Browse** button to select the **certificate store**:..



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




5. You will see again **Certificate Store status window** and follow the steps. Click **Finish** button to complete the **Certificate Import Wizard**.

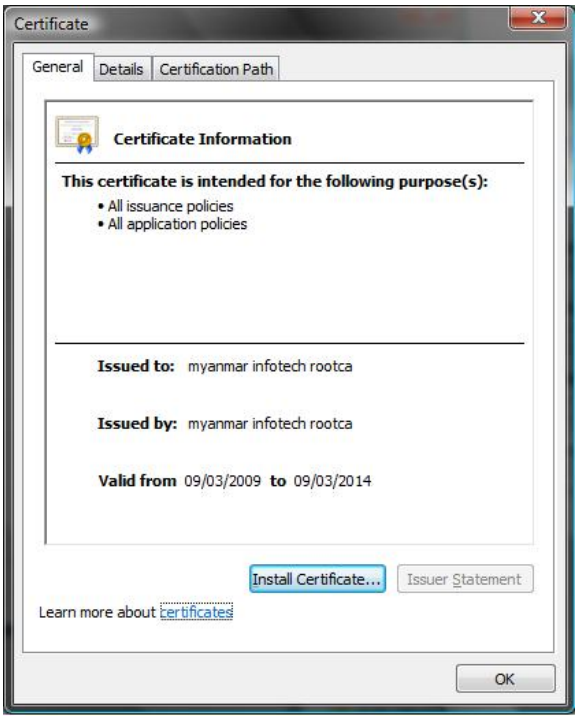



6. When the Certificate Import Wizard is completed, click OK button.

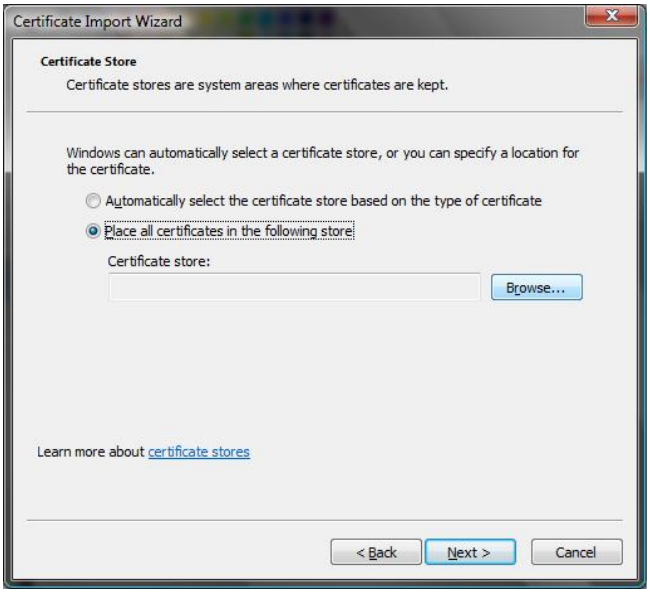
## *2.3 Root certificate Installation (.cer) File*

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

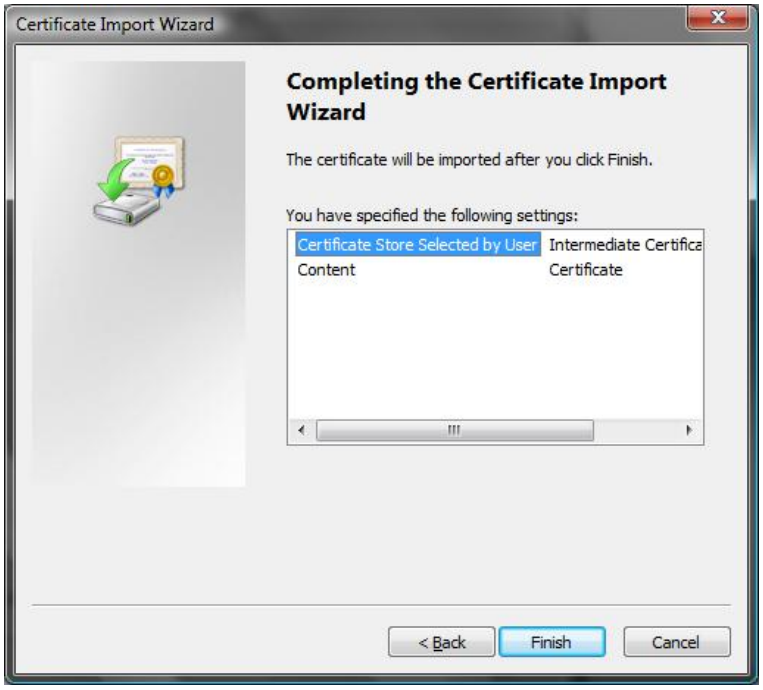
1. Click (Myanmar Infotech Rootca .cer) file.
2. Click **Install Certificate** button and then click **Next** button.




3. Select **Place all Certificate in the following store** and click **Browse** button.
4. Select Trusted Root Certification Authorities folder in **Select Certificate Store**.




5. Click Finish button in **Certificate Import Wizard** dialog.




6. Click OK button and your Installation is completed.

## *2.4 How to get Digital ID….*

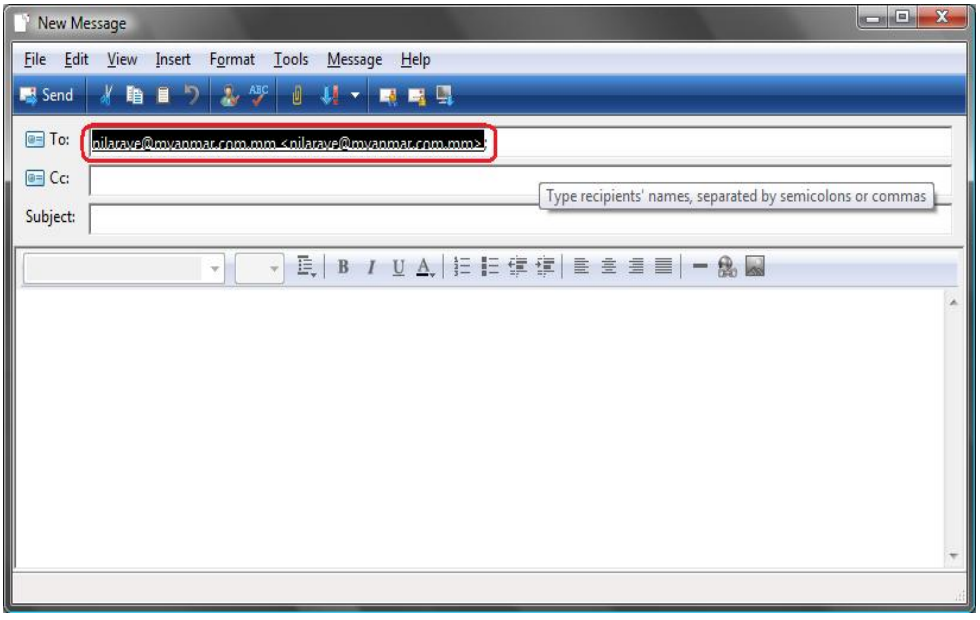
### *2.4.1 Downloading and Importing a Digital ID*

You can also search in the public directory for someone's Digital ID, when you find it, you have to download the ID and import it to your contacts list. If you want to search for someone's Digital ID in public directory please do the following steps:

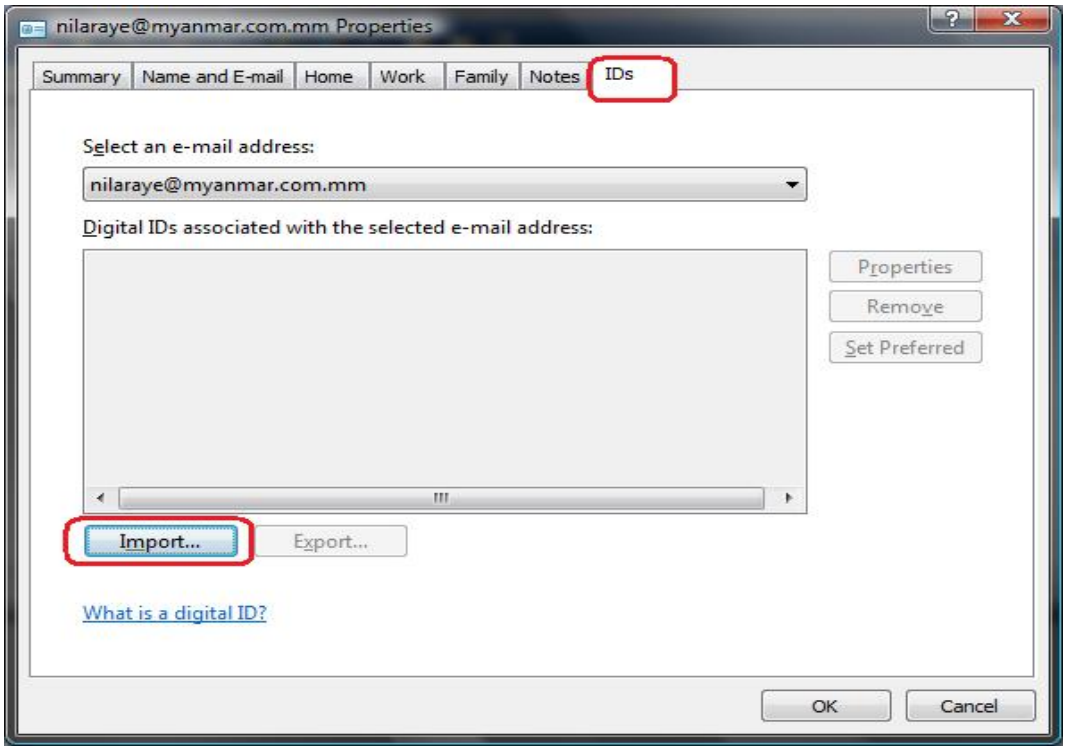
1. Visit http://www.yatanarponca.com.mm or http://www.yantanarponca.com.mm/reposity and follow the instructions to search for, then select and download the Digital ID.
2. When asked to choose the format for downloading select "someone else's Digital ID for Microsoft IE (4.0 or later) / Outlook Express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

## *2.5 Importing Digital ID to Contacts*

To import a downloaded Digital ID into your Contacts:




1. When you send an email to recipient, Double click on recipient email(red mark).
2. Select IDs tab and click Import button.
3. Then choose recipient public key and click OK.




## 3. Certificate Application

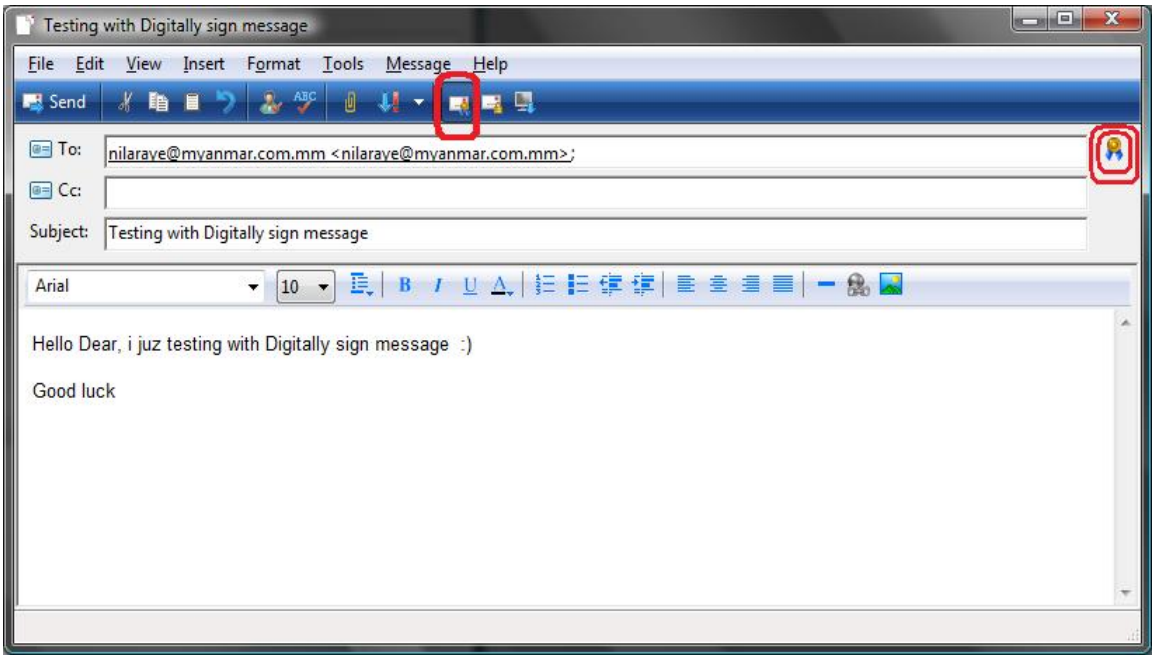
### 3.1 Signing Individual E-Mail

You can automatically sign all your outgoing E-mail by using your Digital ID installed in your browser or E-mail application. Signed E-mail lets the E-mail recipients to verify your identity.

If you want to sign an outgoing message please follow these steps:

1. In the New Message window, click on the Digital Sign message button.

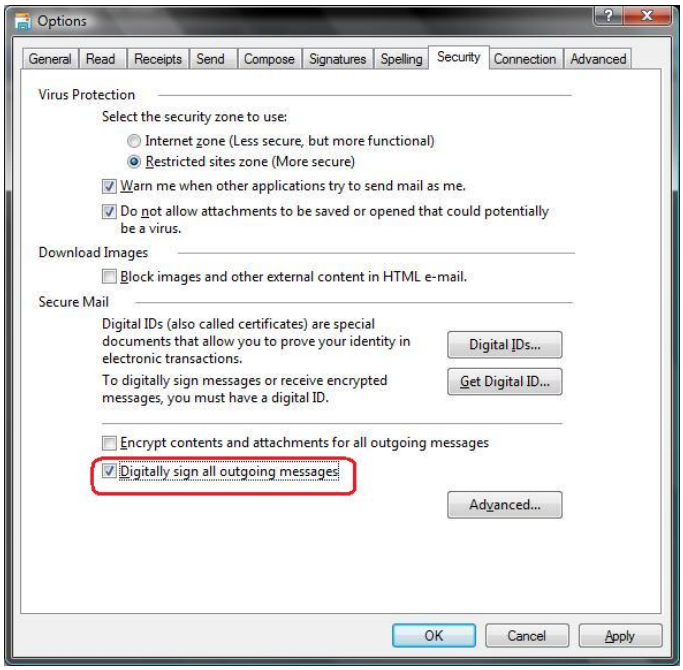
The signed icon will display in the upper right corner of the address pane and it indicates the message is signed or not.




## *3.2 Signing All Outgoing E-Mail*

To Sign all outgoing message automatically:

1. Select the **Tool** menu and scroll to **Option**.
2. Select the Security tab and Mark Digital **sign all outgoing messages**.
3. If you do not check this box, all outgoing message will not include sign symbol.



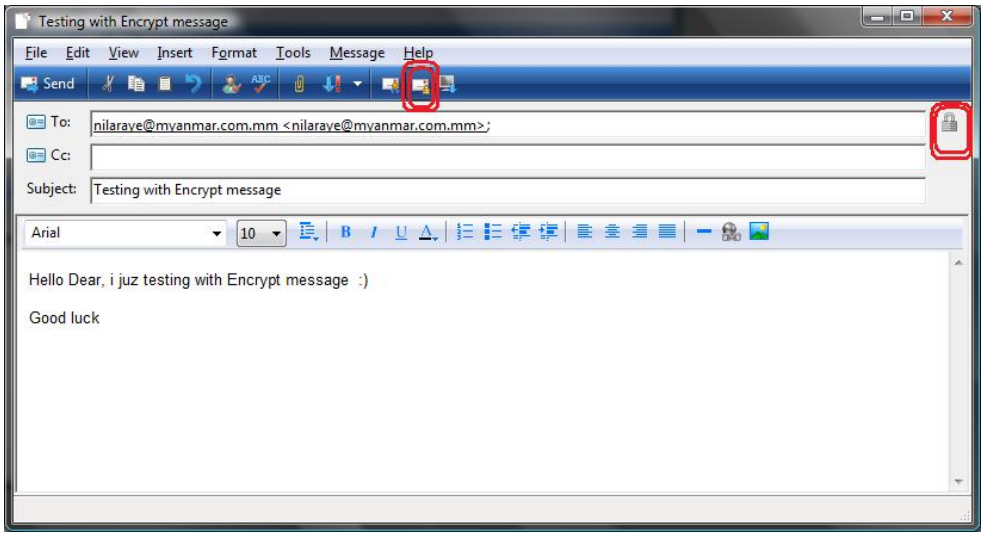
## *3.3 Individual Encrypting your E-mail*

You can also encrypt individual message or configure your e-mail security option to automatically encrypt all E-mail messages to the recipients whose Digital IDs are stored in your contacts list.

### *3.3.1 Encrypting Individual Messages*

To encrypt an outgoing message:

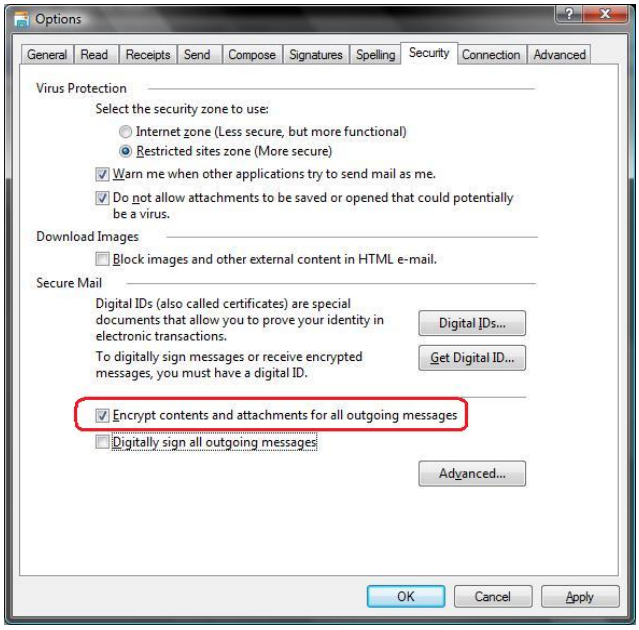
1. In the message window click on the **Encrypt Message button**.
2. If you do not have recipient's Digital ID, you can't send encrypted message.
3. Add the recipient's email address in your **contacts** and import recipient's certificate in your Contacts List**.** (See – 2.5)




### *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 Option tab.
2. Select **Security tab** and mark the **Encrypt** contents and attachments for all outgoing messages.
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 in hardware tokens, smart cards, and other hardware devices which are password- or PIN- protected, be sure to use a strong password or PIN. Never give 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 this 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 certificate 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 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.