



Digi-Sign Certification Services Limited

Subscriber Operation Manual

Important Notice

All rights reserved. Unless otherwise stated, this operation manual contains proprietary information and materials subject to copyright belonging to Digi-Sign Certification Services Limited. Except as provided herein, no part of this operation manual may be copied or otherwise incorporated into or stored in any retrieval system, publication or other work in any form including hard copies, electronic or otherwise.

ID-Cert is a trademark of Digi-Sign Certification Services Limited.

Except otherwise stated, the product names mentioned in this operation manual are used for identification purposes only and may be trademarks or registered trademarks of their respective owners. Digi-Sign disclaims any and all rights in those product names or marks.

Copyright © 2014 Digi-Sign Certification Services Limited

Disclaimer

Digi-Sign expressly disclaims any representations, warranties or undertakings in relation to the accuracy, completeness, quality or adequacy of the contents of this operation manual (“the contents”), including but not limited to fitness for any particular purposes. You shall use this operation manual solely at your own risk. Digi-Sign accepts no responsibility and liability for any loss occasioned as a result of reliance placed on any part of the contents. Digi-Sign Certification Services Limited shall in no event be liable for any direct, indirect, incidental, consequential or special damages, losses or expenses arising from or in connection with the contents of this operation manual or any reliance thereon, whether caused by negligence or otherwise.

Table of Content

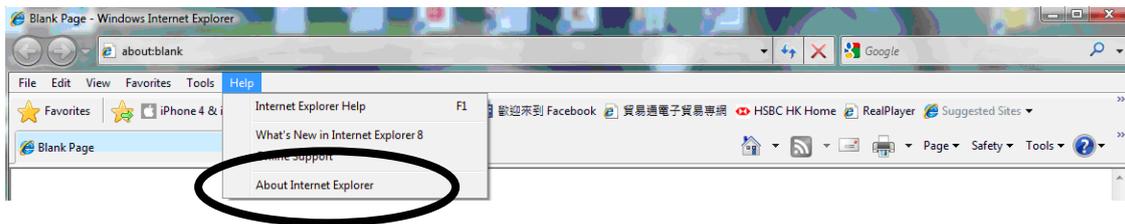
1	Internet Explorer Operation	1
1.1	Internet Explorer Pre-requisite.....	1
1.2	Importing ID-Cert	2
1.3	Install ID-Cert Root CA and Signing CA Certificate.....	10
1.3.1	Installation via ID-Cert Storage Medium	10
1.3.2	Installation via Digi-Sign Web Site	14
1.4	View Your ID-Cert Content	19
1.5	Backup Your ID-Cert	21
1.6	Restore Your ID-Cert	26
1.7	Search for E-mail Recipient.....	27
1.7.1	Searching via Digi-Sign web site.....	27
1.7.2	Searching via ID-Cert Directory with Outlook Express	29
1.8	Verify Name On The Certificate with Outlook Express	35
1.9	40-bit Encryption Security Warning Message	37
1.9.1	Disable 40-bit Encryption Security Warning Message	37
1.10	Use ID-Cert to Sign and Encrypt E-mails with Outlook Express.....	39
2	Thunderbird Operation.....	41
2.1	Importing ID-Cert	41
2.2	Install ID-Cert Root CA and Signing CA Certificate.....	45
2.2.1	Installation via ID-Cert Storage Medium	45
2.3	View Your ID-Cert Content	48
2.4	Backup Your ID-Cert	50
2.5	Restore Your ID-Cert	53
2.6	Search for E-mail Recipient via ID-Cert Directory with Thunderbird	54
2.7	Use ID-Cert to Sign and Encrypt E-mails with Thunderbird	57

1 Internet Explorer Operation

1.1 Internet Explorer Pre-requisite

The ID-Cert installation supports Internet Explorer version 5.5 and above with 128-bit cipher strength. For IE version less than 5.5, the following general guidelines can verify and upgrade Internet Explorer's cipher strength.

1. From the menu bar of Internet Explorer, select <**Help**> and then <**About Internet Explorer**>.

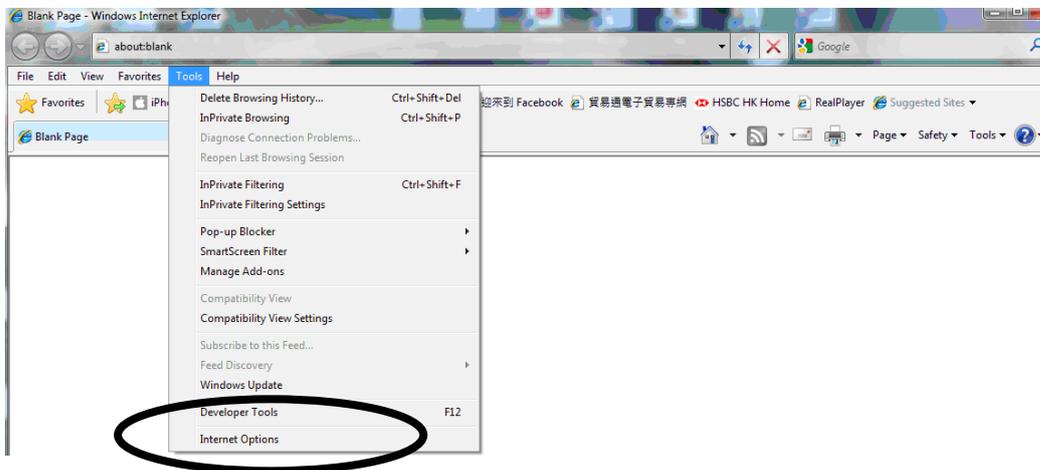


2. If the cipher strength is less than 128-bit, please select the “**Update Information**” hyperlink to obtain the latest IE version updates.

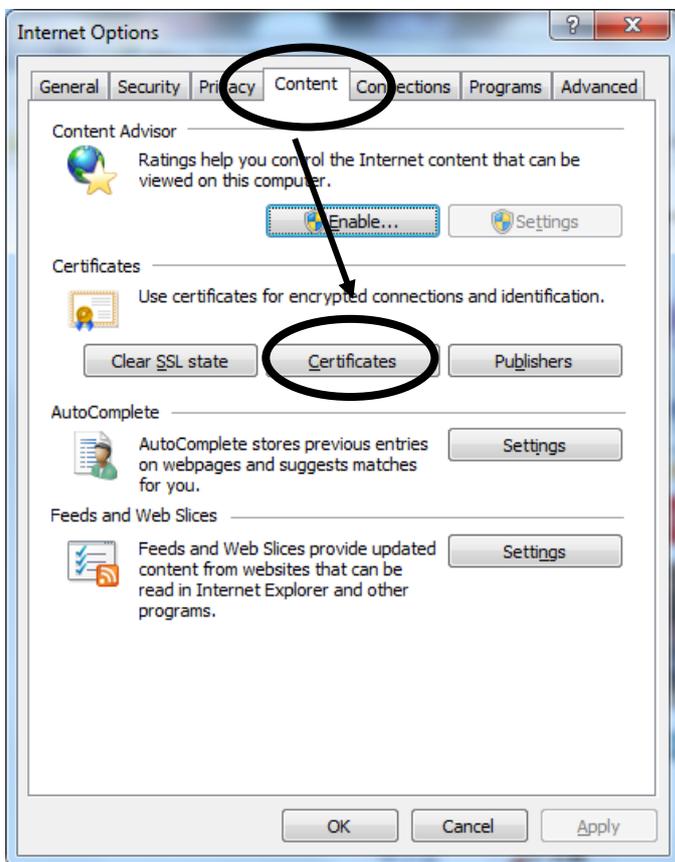


1.2 Importing ID-Cert

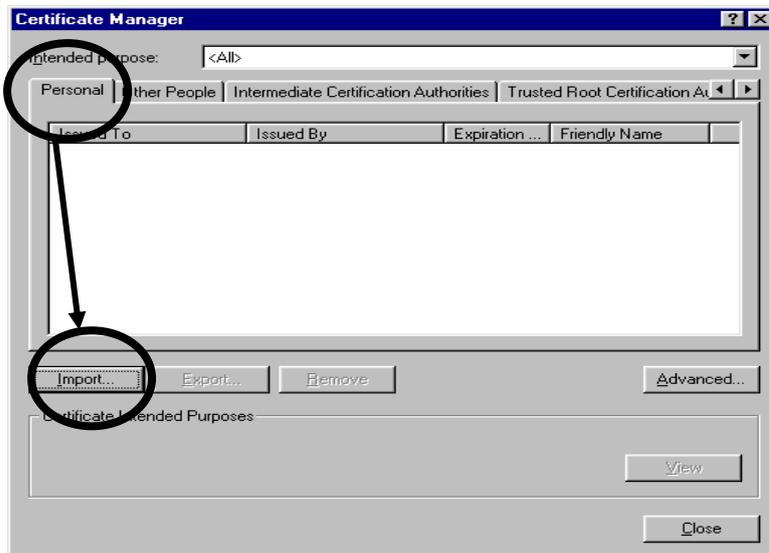
1. From the menu bar of Internet Explorer, select <Tools> and then <Internet Options>.



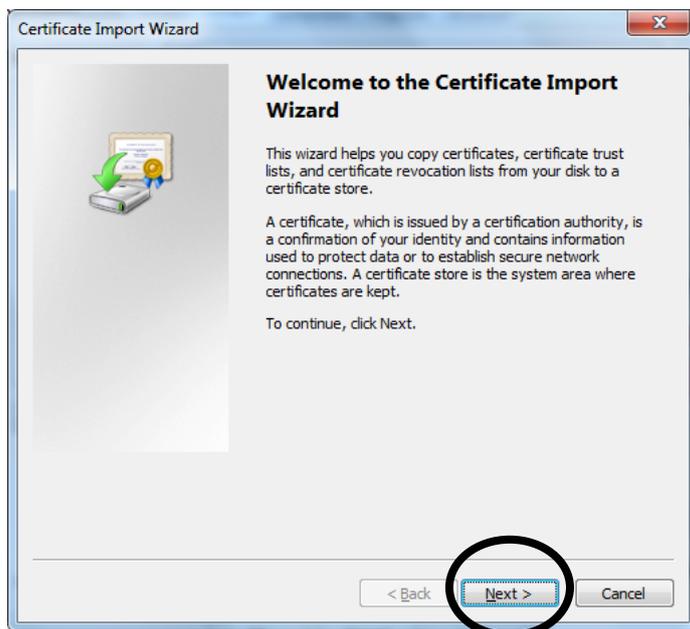
2. In the Internet Options window, select the <Content> tab and click the [Certificates] button.



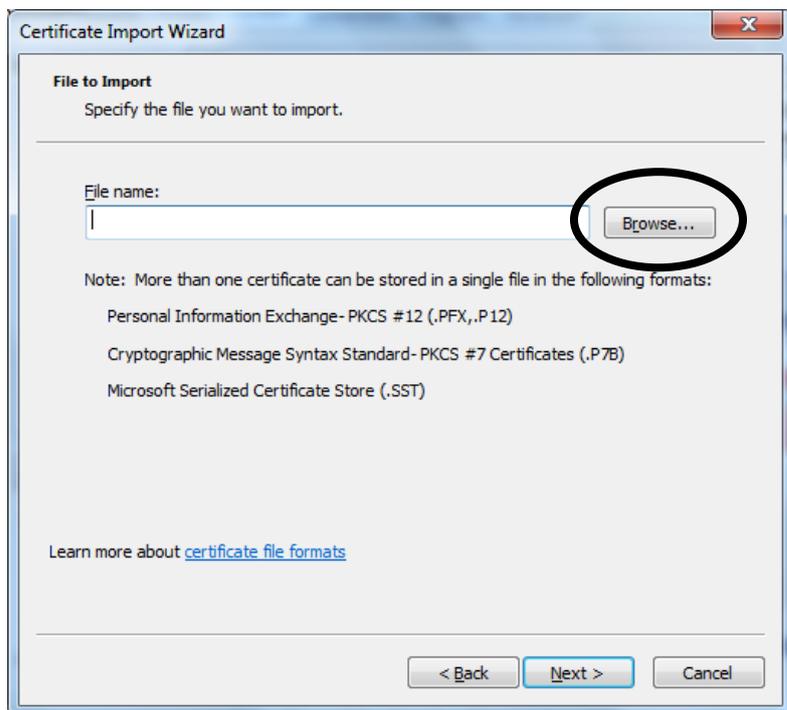
3. Select the <Personal> tab and click the [Import] button. The Certificate Manager Import Wizard will pop up.



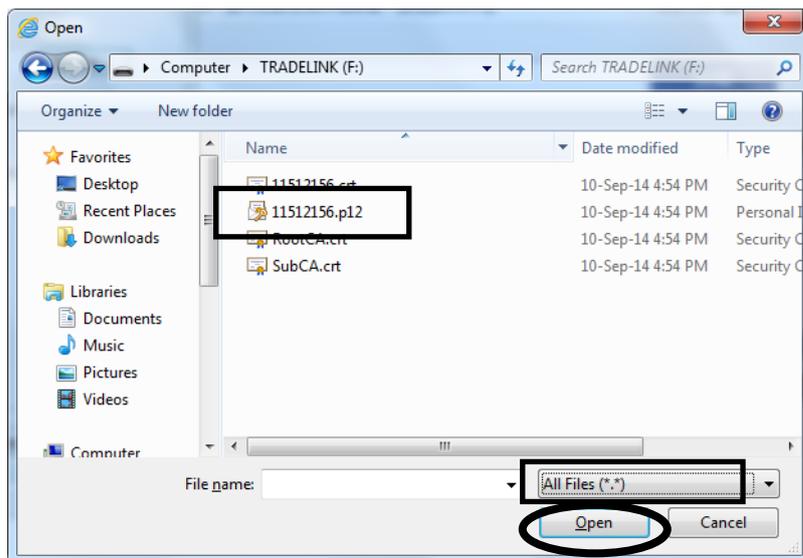
4. Click [Next>] to continue.



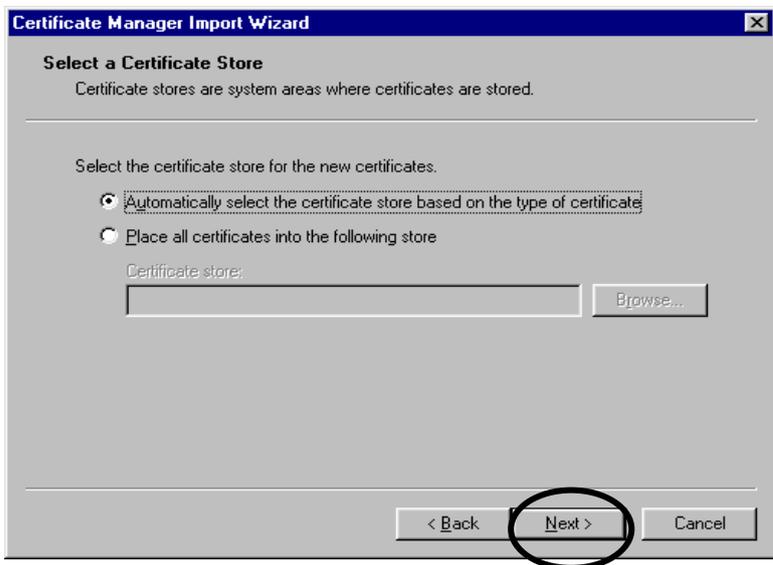
- 5. Insert your signature **ID-Cert storage medium**.
- 6. Click the **[Browse]** button and you can look up your ID-Cert files.



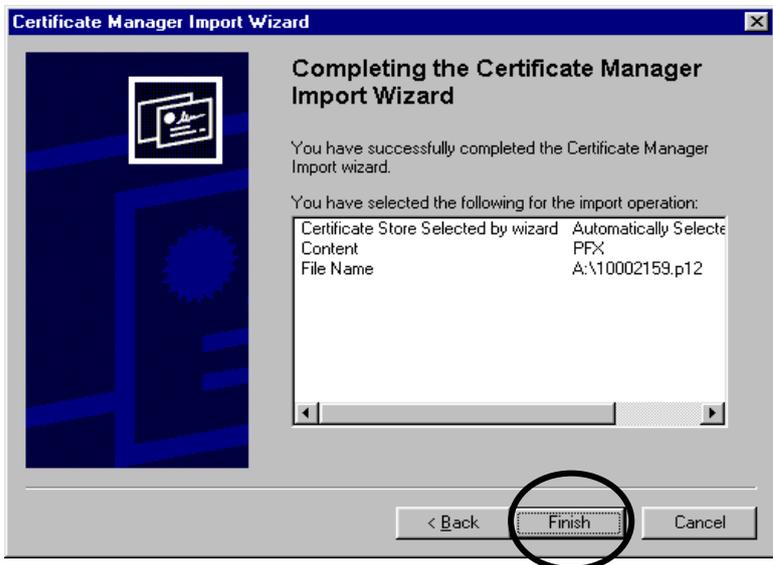
- 7. Select your drive from the “**Look In**” drop box and select “**All files (*.*)**” from the “**Files of Type**” drop box. The ID-Cert file is named as **xxxxxxx.p12** where **xxxxxxx** is your Subscriber Number. Highlight it and click the **[Open]** button.



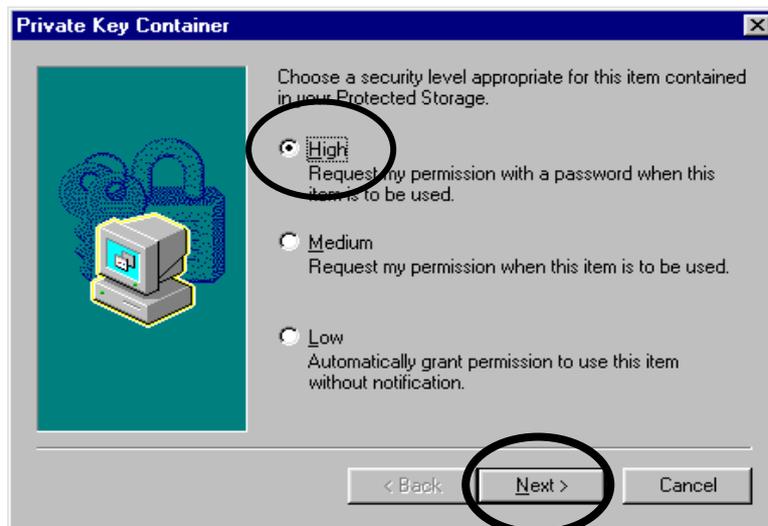
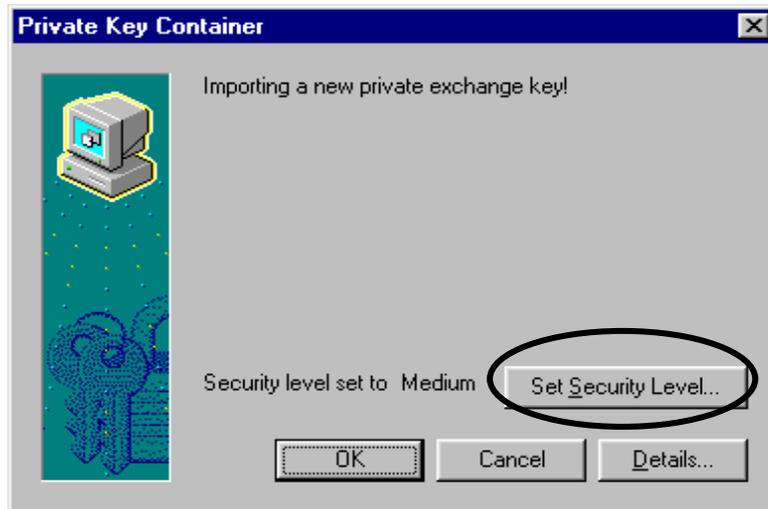
9. Select the way to store your ID-Cert. You can check the box “**Automatically select the certificate store based on the type of certificate**” or “**Place all certificates into the following store**” to specify a directory or storage device to store the certificates. Click [**Next>**] to continue.



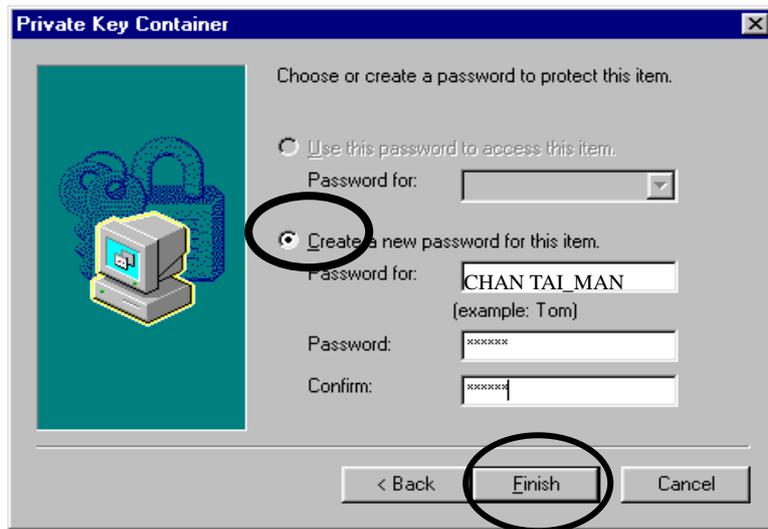
10. You have finished importing your ID-Cert and you can click [**Finish**] now.



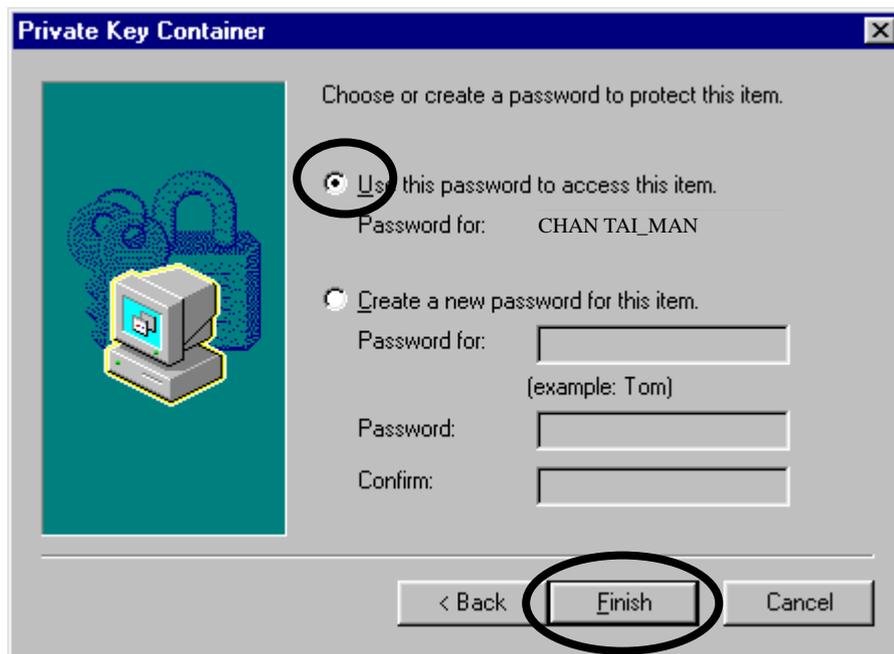
11. The “**Private Key Container**” screen will pop up and you need to set the security level of your ID-Cert. Click [Set Security Level...] and click the [High] radio button. Click [Next>] to continue.



12. You are required to enter a password to protect your ID-Cert. Select “**Create a new password for this item**” and enter a name and a password for your ID-Cert profile.



** Alternatively, if you have specified a profile before, you can select the option “**Use this password to access this item**” and select the previous profile from the drop box.



Click [Finish] button and the next screen will prompt you to enter your new password again.

13. Enter the password again, and click [OK] to continue.



14. You will see on the screen “**The import was successful**” and you can click [OK] to continue.



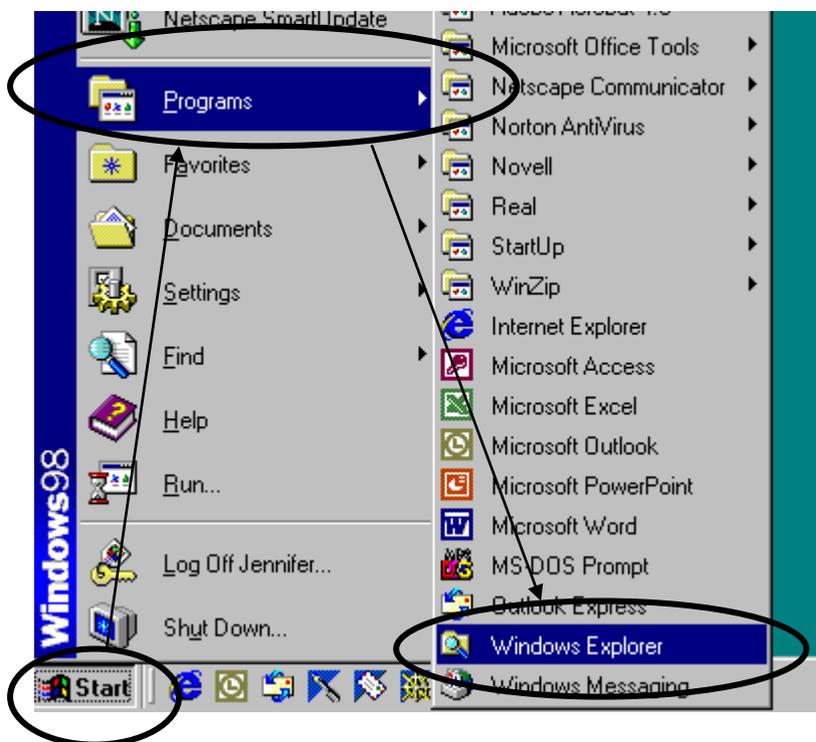
15. Repeat the above steps if you need to import your Encipherment ID-Cert. (Encipherment ID-Cert will allow you to sign and encrypt your e-mail messages.)

1.3 Install ID-Cert Root CA and Signing CA Certificate

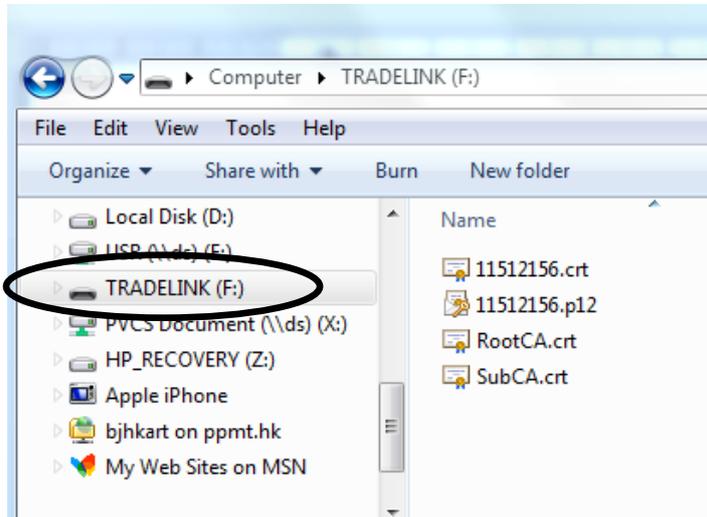
The ID-Cert Root CA and Signing CA Certificates are used to validate certificates issued by Digi-Sign. You can either choose to install the ID-Cert Root CA and Signing CA Certificates from your ID-Cert storage medium or from www.dg-sign.com web site.

1.3.1 Installation via ID-Cert Storage Medium

1. Start up Windows and click [Start] button. Select [Program] and then [Windows Explorer].

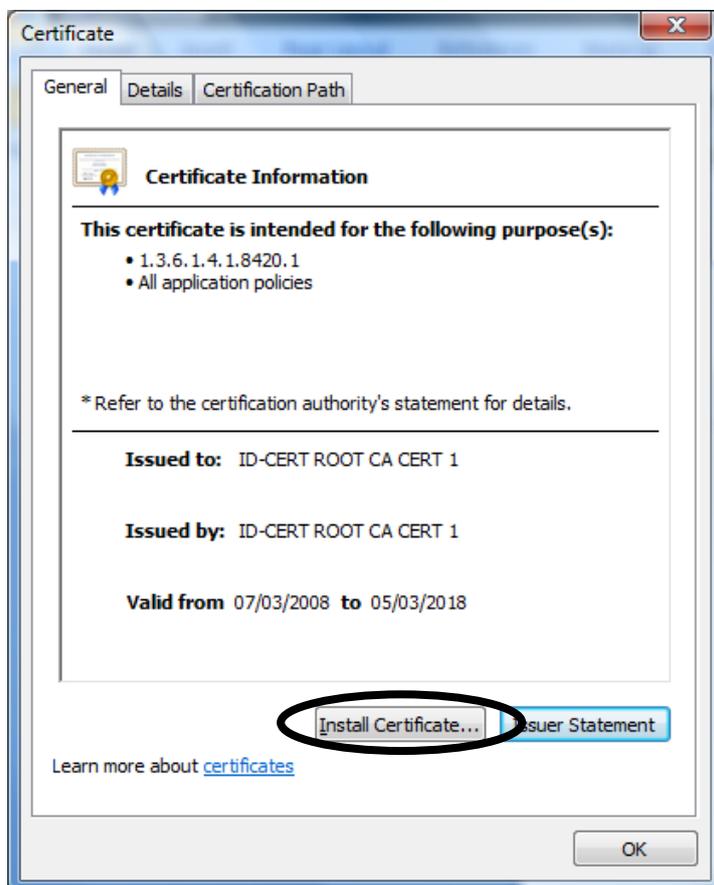


2. Insert your signature **ID-Cert storage medium** into the computer. Select your USB drive e.g. TRADELINK (F:) and you will see the content of your ID-Cert storage medium.



The ID-Cert Root CA Certificate file is named **rootca.crt**. Double-click it to open.

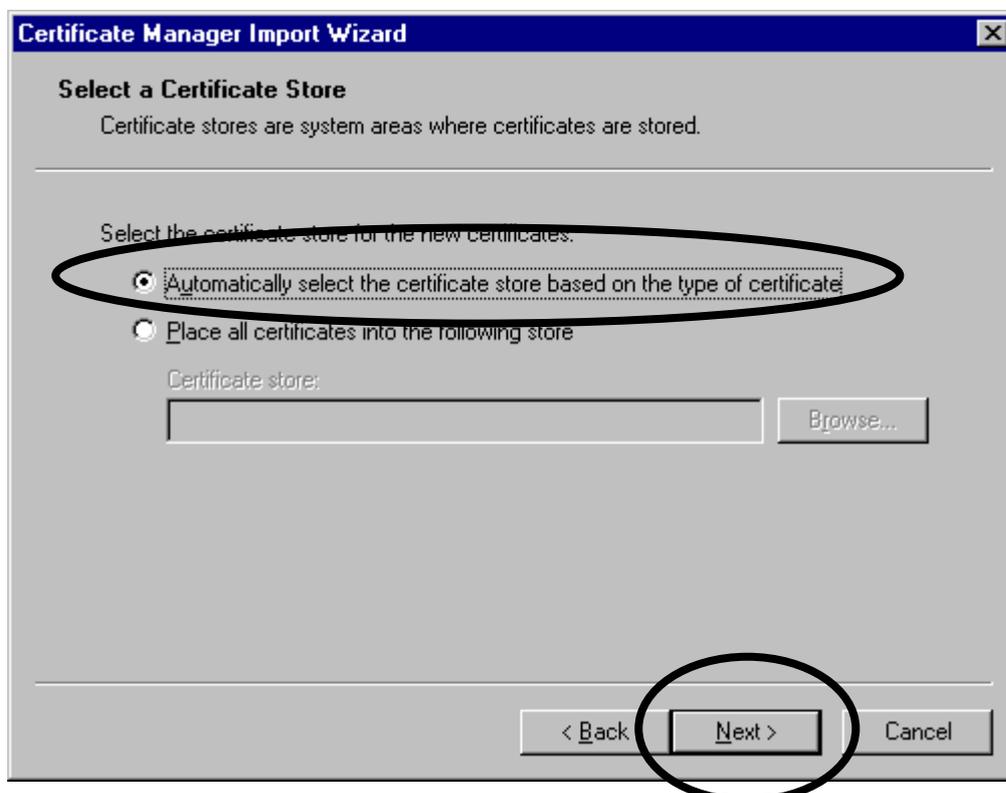
3. Click [**Install Certificate**] button to install the certificate.



4. Click [Next>] to continue.



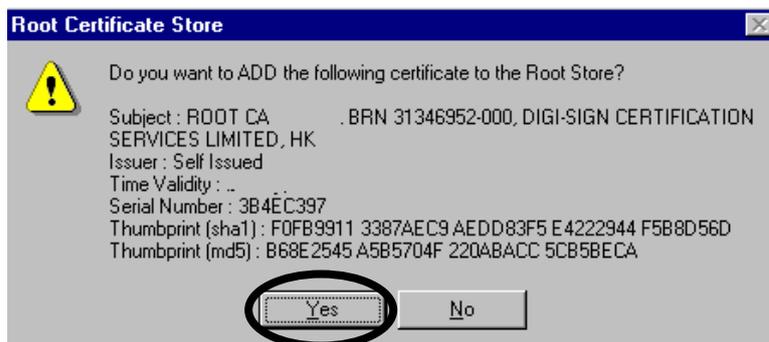
5. You may select <Automatically select the certificate store based on the type of certificate>. Click [Next>] to continue.



6. The Completing screen will pop up and you can click **[Finish]**.



7. The screen will also prompt you to choose if you want to add the ID-Cert Root CA Certificate to the Root Store. Click **[Yes]** to continue.



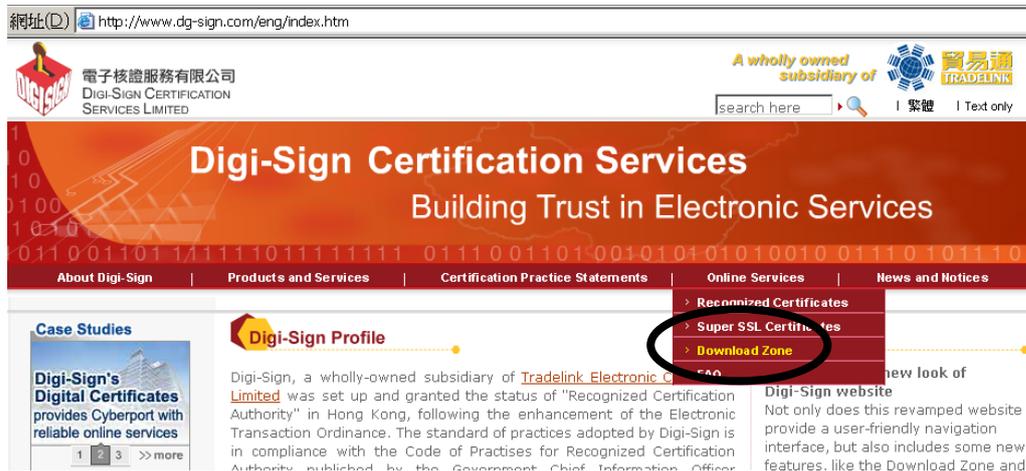
8. The installation of ID-Cert Root CA Certificate is completed successfully. Click **[OK]** to continue.



9. Repeat the above steps to install the “**ID-Cert Signing CA Certificate 1**”. Choose the file named **subca.crt**.

1.3.2 Installation via Digi-Sign Web Site

1. Start up Internet Explorer. In the address bar, enter the Uniform Resource Locator (URL) of Digi-Sign web site: “**www.dg-sign.com**” and press [Enter]. Click the “**Online Services**” and select the “**Download Zone**”.



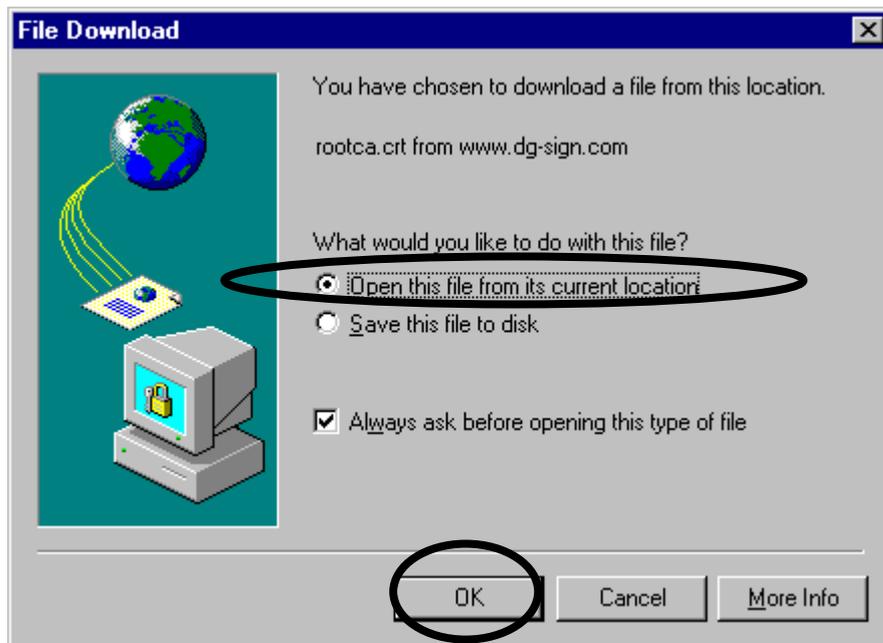
2. Goto the “**Root CA and Signing CA Certificate**” and click  button.

	Recognized Certificates	Super SSL Certificates	Premium Certificate
Certification Practice Statements			
Forms			
Application Forms and Procedures			Nil
Change of Subscriber Information		Nil	Nil
Certificate Revocation Form and Procedures			Nil
Manual			
Subscriber Operation Manual	<input checked="" type="checkbox"/>	Nil	Nil
Change Password Utility User Manual	<input checked="" type="checkbox"/>	Nil	Nil
Certificate Signing Request Generation Guide	Nil		Nil
Installation Guide	Nil		Nil
Utilities and Drivers			
Change Password Utility		Nil	Nil
Windows 98 Drivers for USB Flash Drive		Nil	Nil
CA Certificate and Certificate Revocation List			
Root CA and Signing CA Certificate	 (circled in black)	Nil	Nil
Certificate Revocation List		Nil	Nil

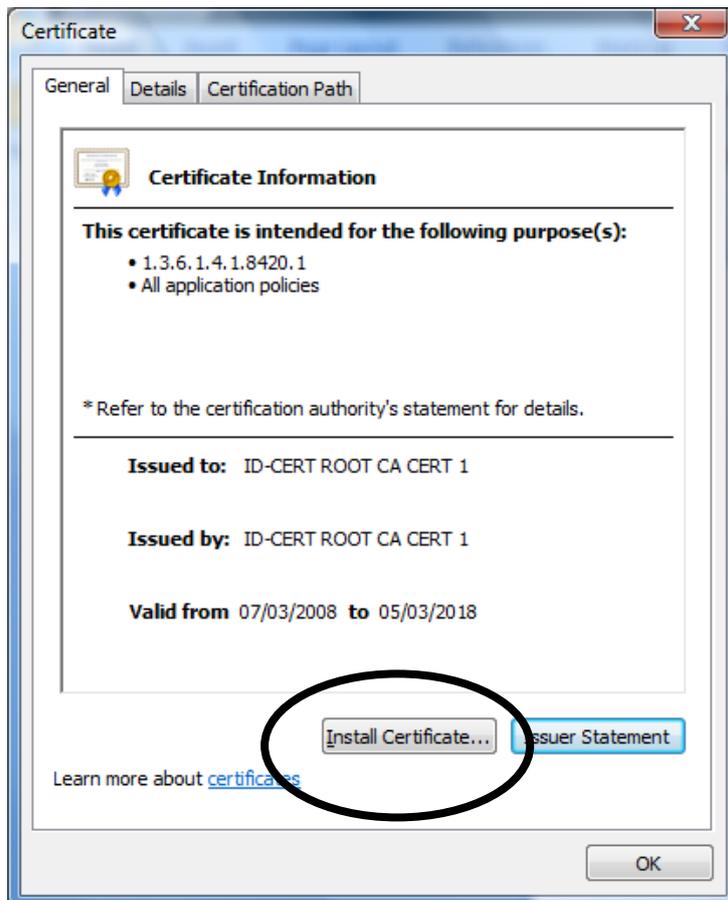
3. Select the Root CA and Signing CA certificate 1.



4. Choose <Open this file from its current location> and then click [OK].



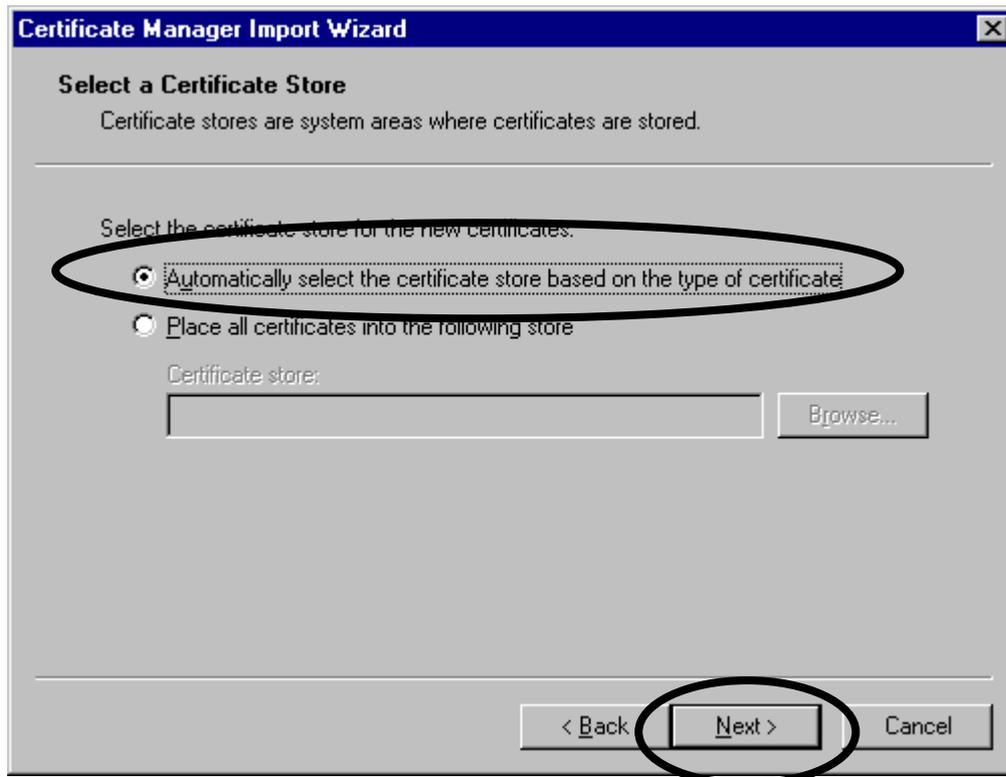
5. Click [**Install Certificate**] button to install the certificate.



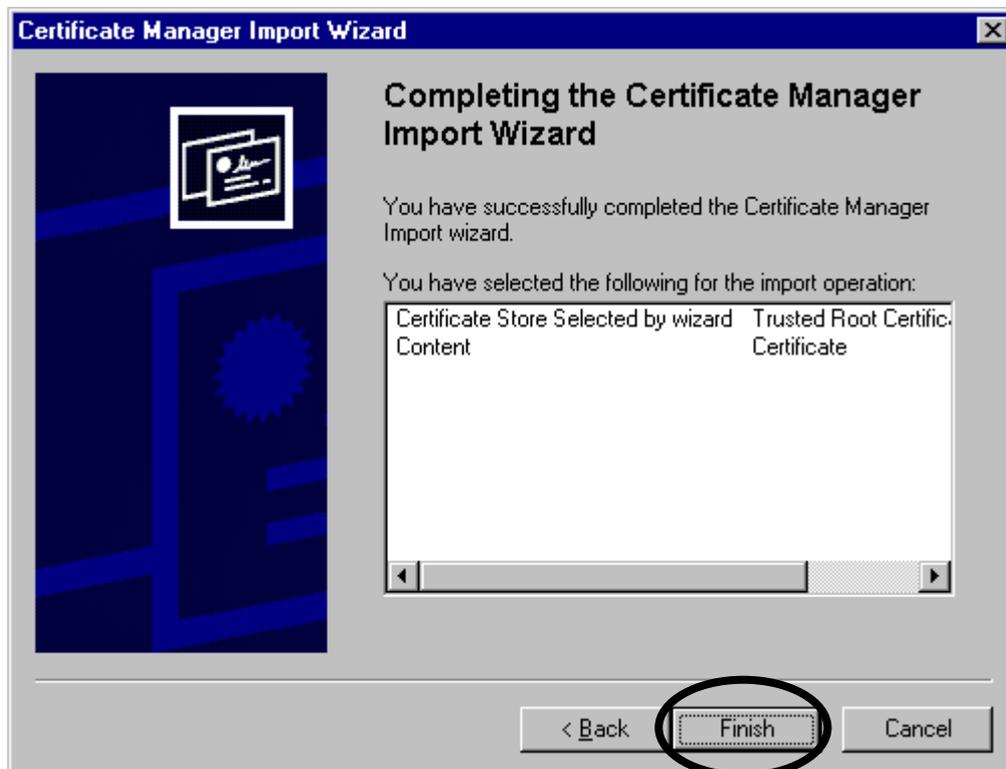
6. Click [**Next>**] to continue.



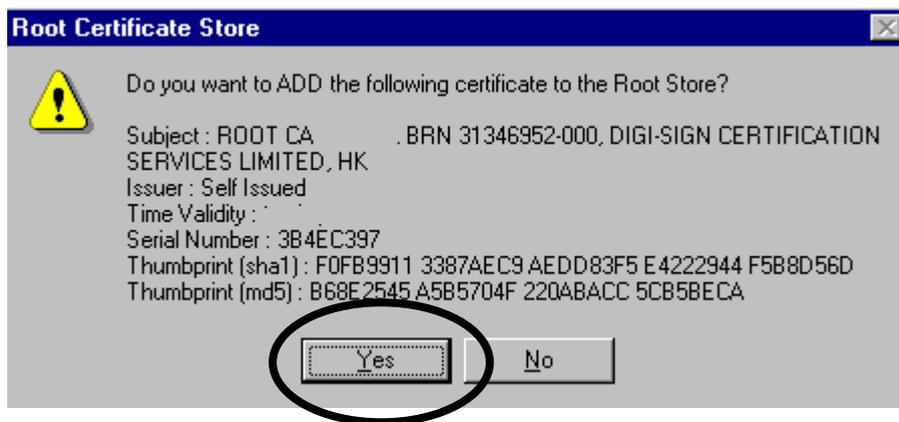
7. You may select <Automatically select the certificate store based on the type of certificates>. Click [Next>] to continue.



8. The Completing screen will pop up and you can click [Finish] to continue.



9. The screen will prompt you to choose if you want to add the ID-Cert Root CA Certificate to the Root Store. Click [**Yes**] to continue.



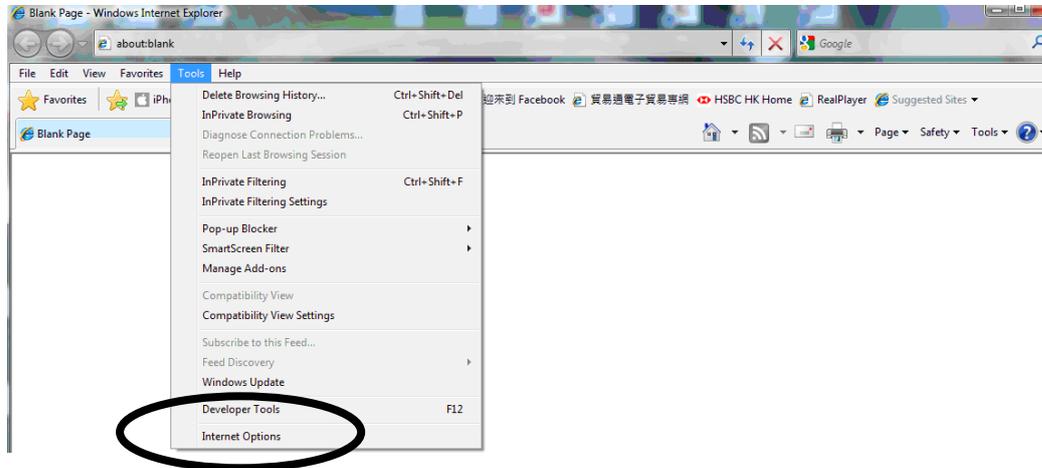
10. The installation of ID-Cert Root CA Certificate is completed successfully. Click [**OK**] to continue.



11. Repeat the above steps to install the “**ID-Cert Signing CA Certificate 1**”. At step three, select the file “**Click here**” hyperlink of “**ID-Cert Signing CA certificate 1**”.

1.4 View Your ID-Cert Content

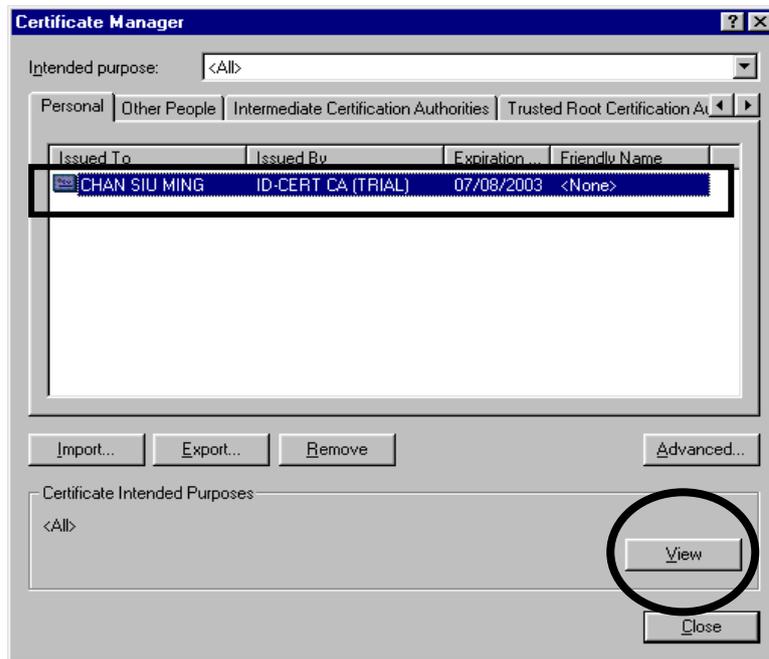
1. From the menu bar of Internet Explorer, select <Tools> and then <Internet Options>.



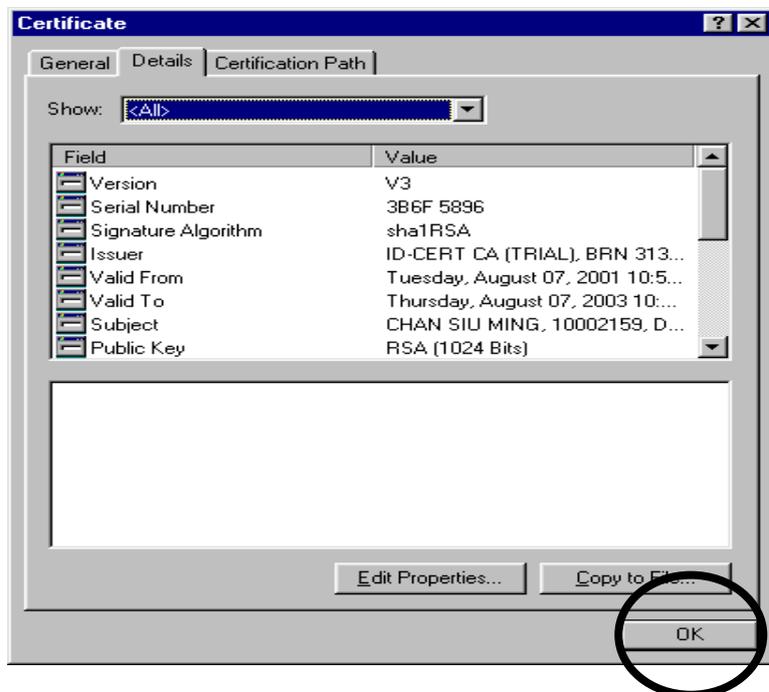
2. In the Internet Options window, select the “Content” tab and click the [Certificates] button.



3. Select the ID-Cert to be viewed and click the [View] button.



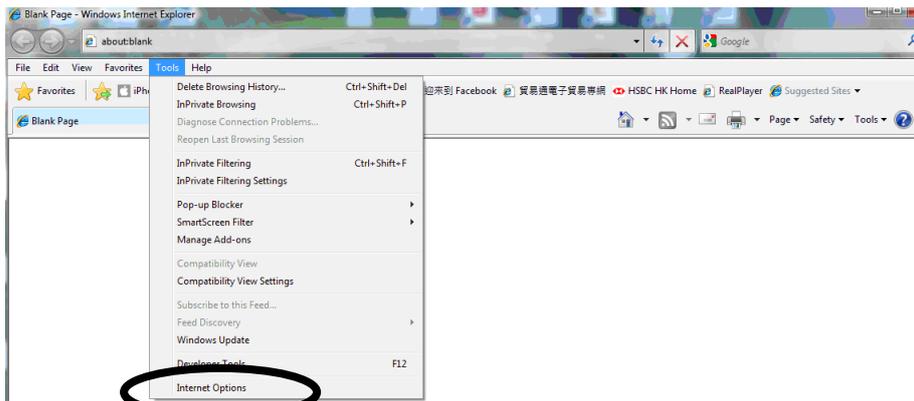
4. Your ID-Cert will be displayed in a new window. Select the “Details” tab to view the contents. You can click [OK] to close the window.



1.5 Backup Your ID-Cert

For ID-Cert Class 8 & Class 9, the private key cannot be export.

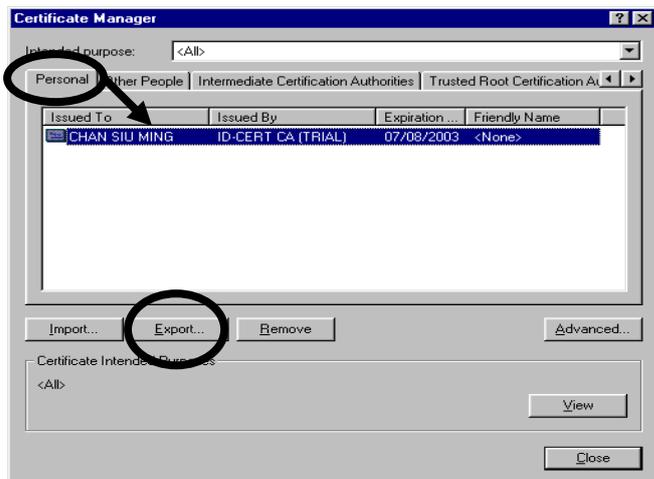
1. Insert a blank ID-Cert storage medium into your computer.
2. From the menu bar of Internet Explorer, select <Tools> and then <Internet Options>.



3. On the Internet Options window, select the “Content” tab and click the [Certificates] button.



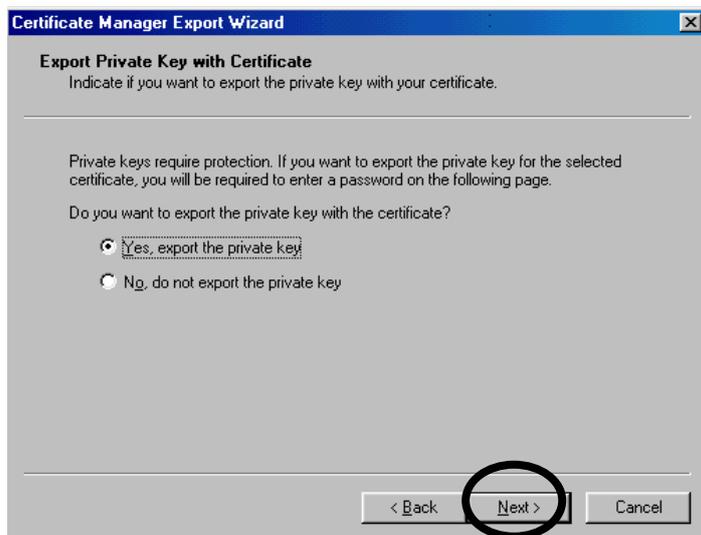
4. Select the “**Personal**” tab, highlight the certificate name and click the [**Export**] button. The Certificate Manager Export Wizard will pop up.



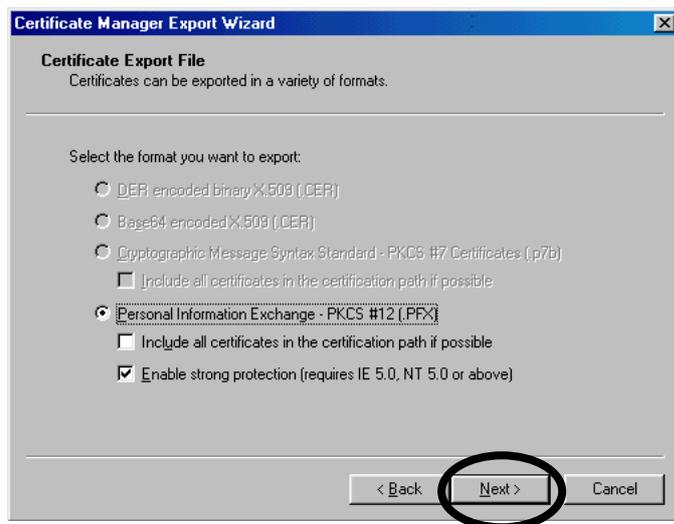
5. Click [**Next>**] to continue.



6. Click [**Next>**] to continue.



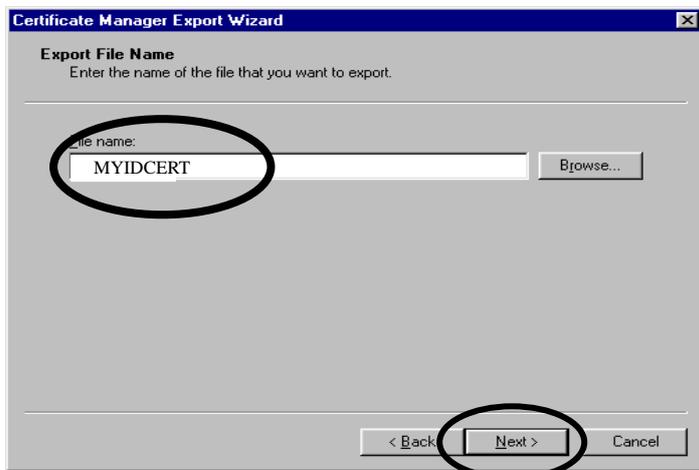
7. Click [**Next>**] to continue.



8. You are required to enter the previous password used to store the private key. Click [**Next>**] to continue. (Please refer to “1.2 Importing ID-Cert” on page 8)



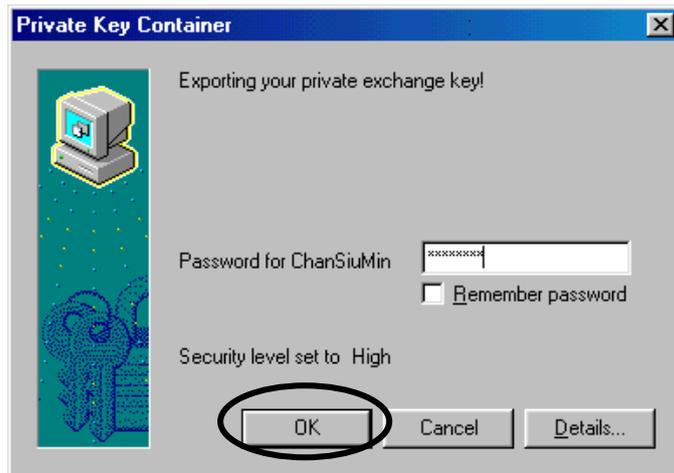
- 9. Enter the location of your drive and the file name you are going to use for export:
e.g. **D:\MYIDCERT** ← your floppy drive is **D:** and the file name is **MYIDCERT**
Click [**Next>**] to continue.



- 10. The finishing screen will pop up and then you can click the [**Finish**] button.



11. Enter the password, and click [OK] to continue.



12. You will see the screen “**The export was completed successfully**” and you can click [OK].



13. After exporting your ID-Cert, keep the ID-Cert storage medium in safe custody.

14. Use a separate ID-Cert storage medium and repeat the above steps to backup other ID-Certs.

1.6 Restore Your ID-Cert

1. Insert your ID-Cert backup storage medium.
2. Follow the procedures in “**1.2 Importing ID-Cert**”. The file name required now should be the one you specified in the backup section and you need to enter the new password that you have assigned in the section “**1.5 Backup your ID-Cert**”.

1.7 Search for E-mail Recipient

1.7.1 Searching via Digi-Sign web site

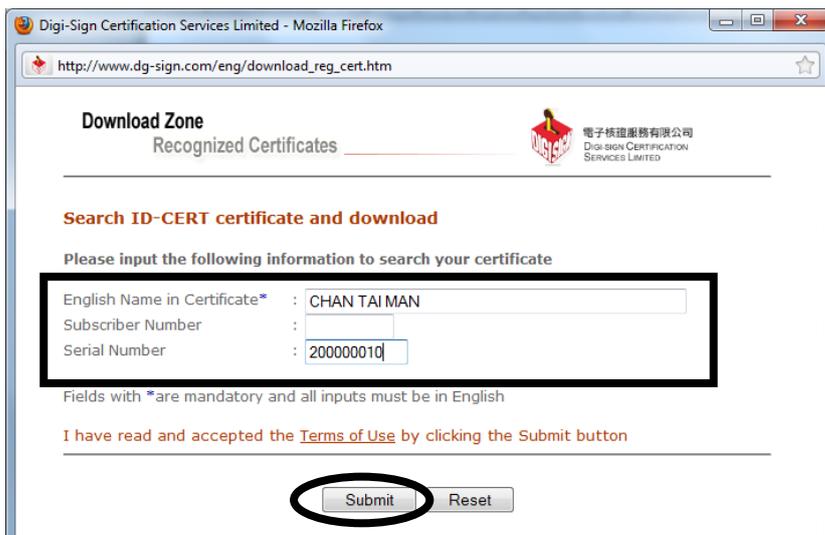
1. Start up Internet Explorer. In the address bar, enter the Uniform Resource Locator (URL) of Digi-Sign web site: “**www.dg-sign.com**” and press [Enter]. Click the “**Online Services**” and select the “**Download Zone**”.



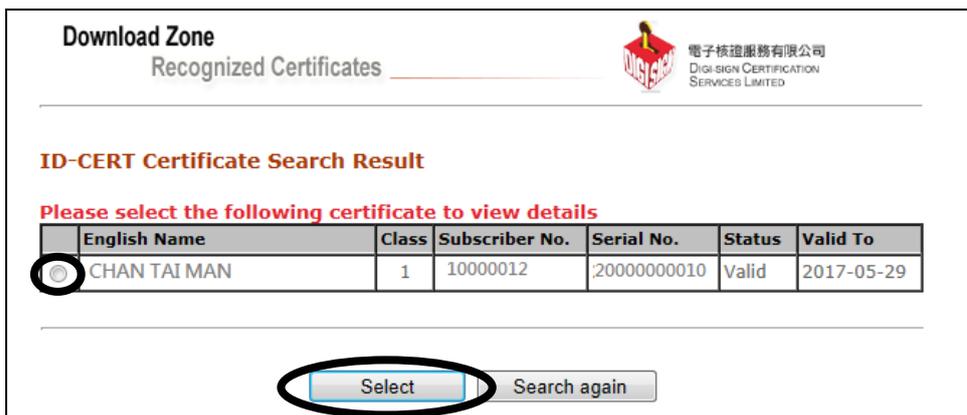
2. Goto the “**ID-CERT Certificate**” and click  button.

	Recognized Certificates	Super SSL Certificates	Premium Certificate
Certification Practice Statements			
Forms			
Application Forms and Procedures			Nil
Change of Subscriber Information		Nil	Nil
Certificate Revocation Form and Procedures			Nil
Manual			
Subscriber Operation Manual		Nil	Nil
Change Password Utility User Manual		Nil	Nil
Certificate Signing Request Generation Guide	Nil		Nil
Installation Guide	Nil		Nil
Certificate			
ID-CERT Certificate		Nil	Nil
Utilities and Drivers			
Change Password Utility		Nil	Nil
Windows 98 Drivers for USB Flash Drive		Nil	Nil

3. Input the following information to search your certificate.



4. ID-CERT certificate search result will be displayed.

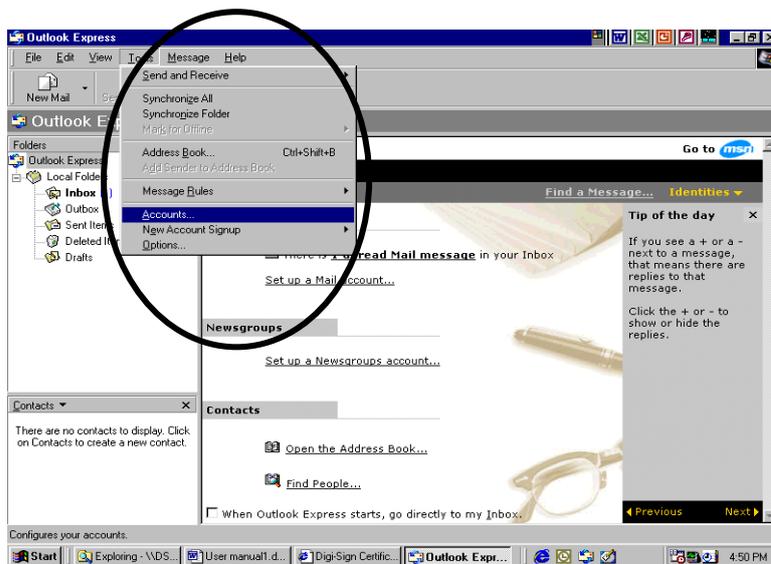


5. Click your certificate to download the cert.

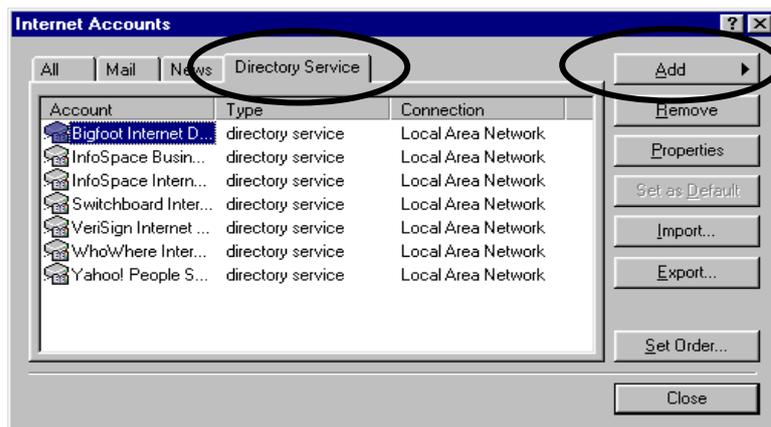


1.7.2 Searching via ID-Cert Directory with Outlook Express

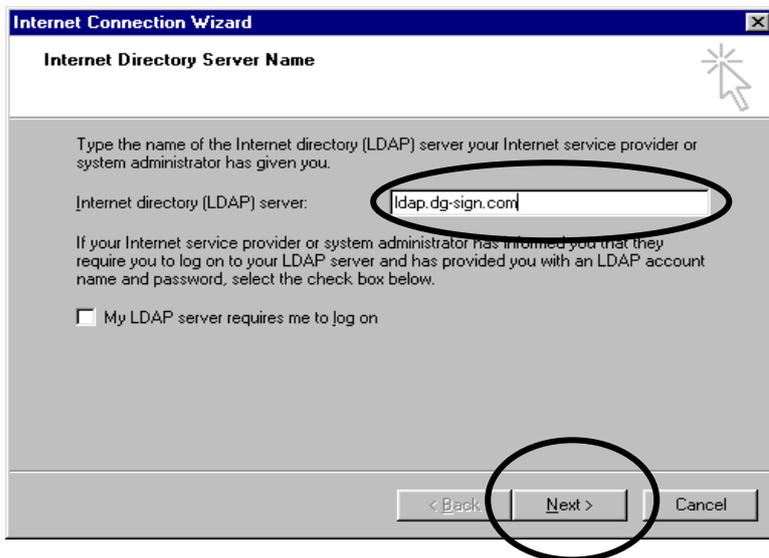
1. Start up Outlook Express.
2. Select <Tools> and then <Accounts>.



3. Click the [Directory Services] tab. Click [Add] button and select “Directory Services”.

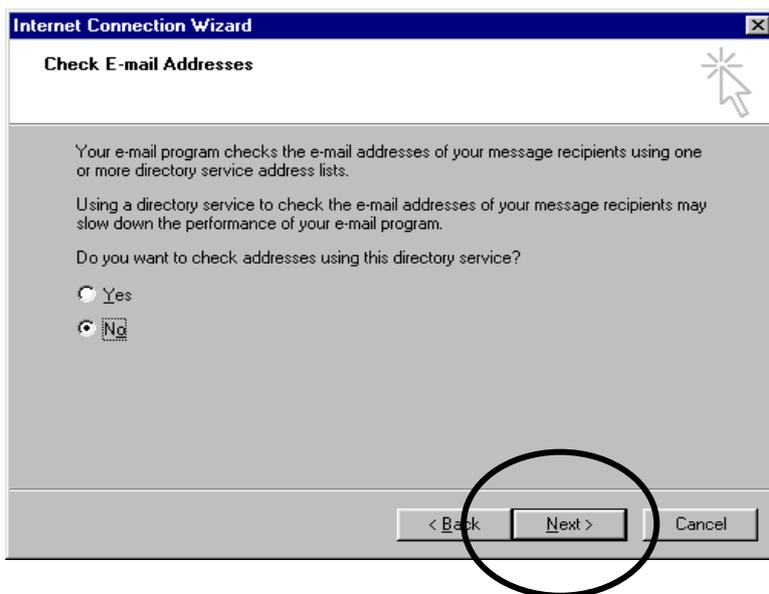


- An “**Internet Connection Wizard**” window will pop up. Enter the Digi-Sign Internet directory “**ldap.dg-sign.com**” in the space provided and click the [**Next**] button.

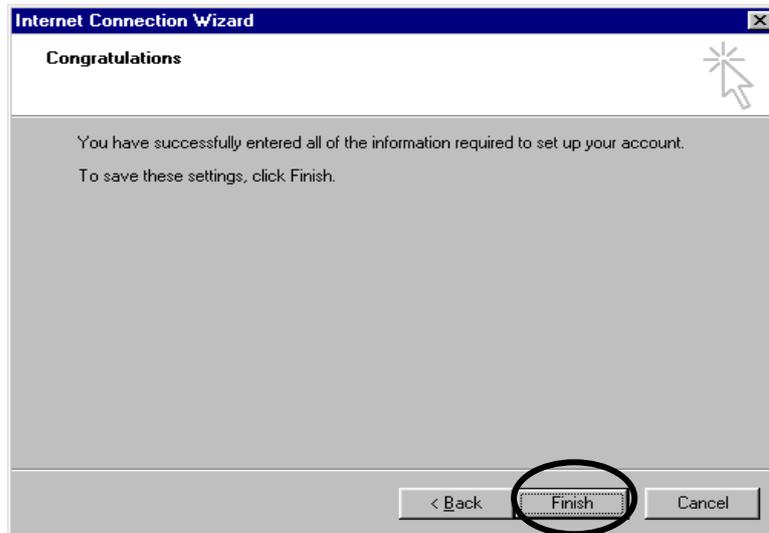


No need to check the box of “**My LDAP server requires me to log on**” since Digi-Sign Internet Directory does not require so.

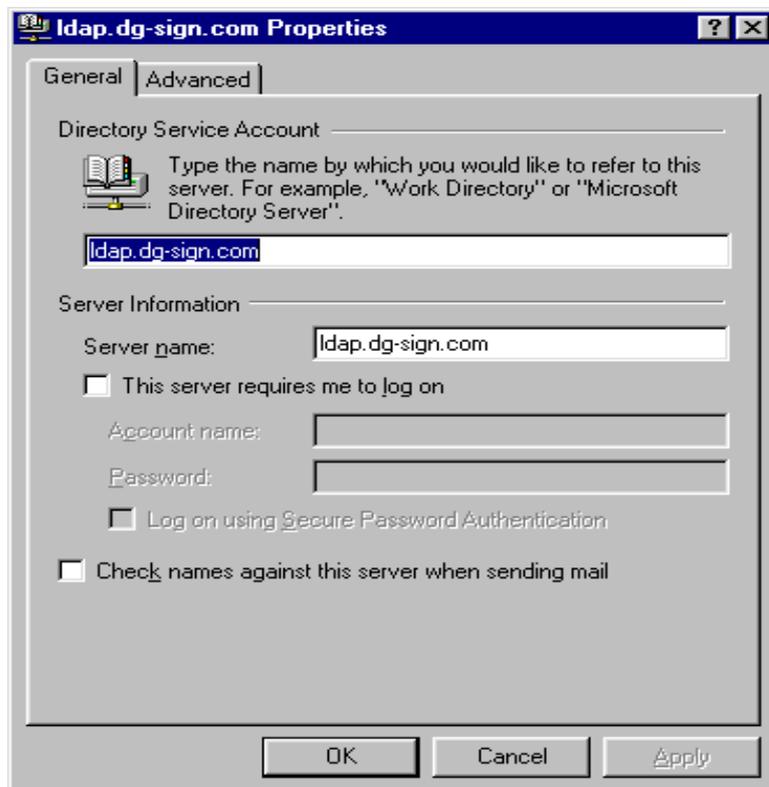
- The next window is “**Check E-mail Addresses**”, the default selection is “**No**” and you can click [**Next >**] to continue.



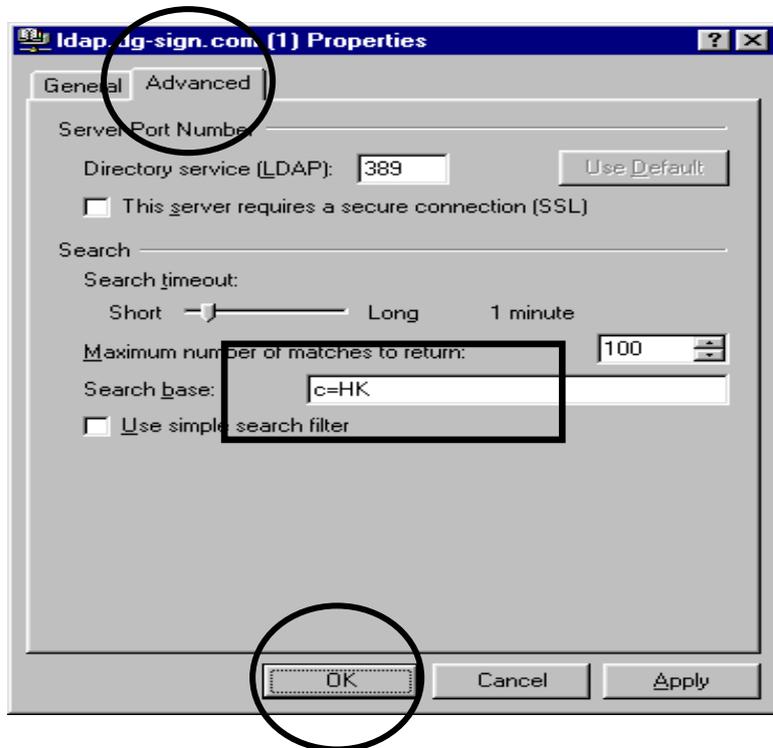
- The finishing screen will pop up and you can click [**Finish**].



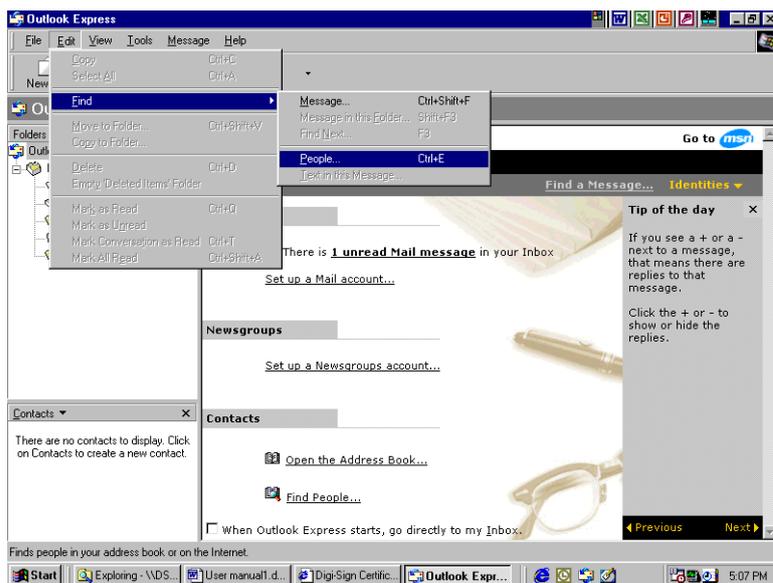
- You are diverted to the Directory Service screen again. Double click the selection of “ldap.dg-sign.com” or highlight the selection and click the [**Properties**] button to give the entry a user-friendly name, e.g. “**Digi-Sign**” or simply leave it as “ldap.dg-sign.com”.



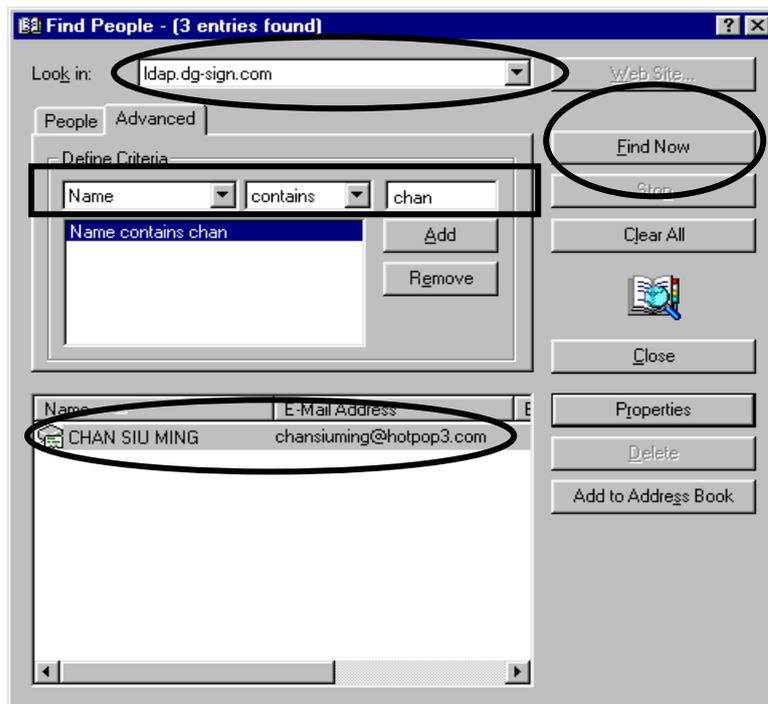
8. Select the “**Advanced**” tab and enter “**c=HK**” as Search Base. Click [OK] button and you are back to the Internet Accounts windows. Close this window now and you can start to search your e-mail recipient in the ID-Cert Directory.



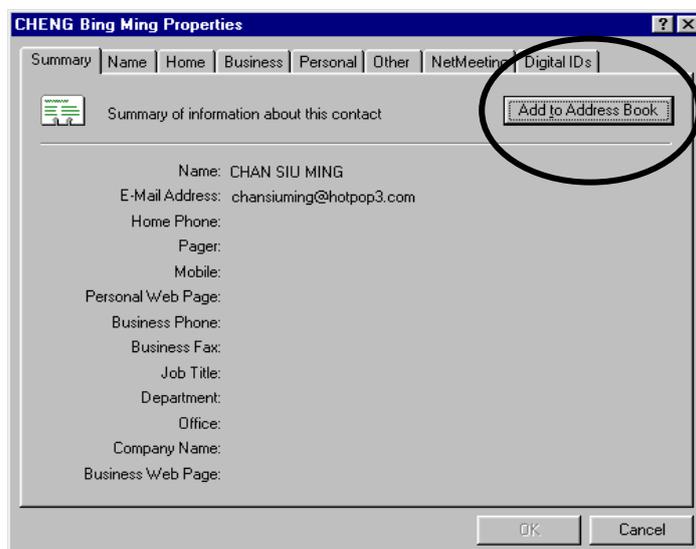
9. Return to the main menu of Outlook Express. Select <Edit> <Find> <People> from the menu bar.



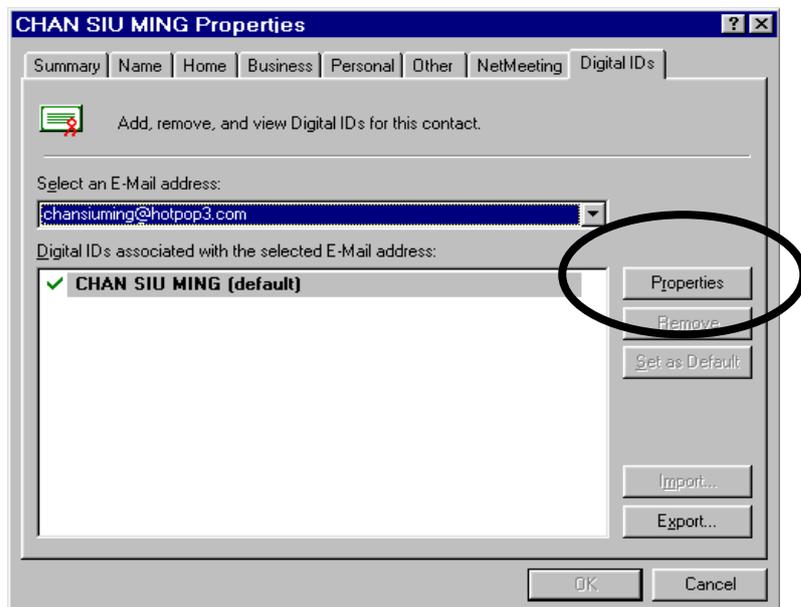
10. A “**Find People**” window will pop up. Enter the searching criteria in the space and make sure you have selected the correct “**Internet Directory Server Name**” in your “**Look in**” directory. Click the button [**Find now**] to search for your e-mail recipient. You may select the “**Advanced**” tab and use the advanced search function if you want to search in various modes, e.g. to search by part of the name / e-mail address.



11. Once you have located your e-mail recipient, double-click the e-mail recipient name and click the [**Add to address book**] button.



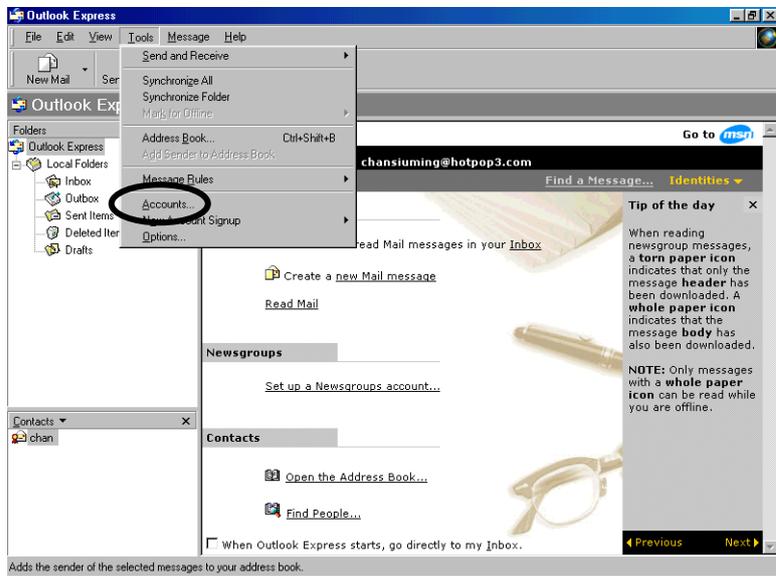
12. You may also view his / her digital certificates by selecting the “**Digital IDs**” tab. Highlight the digital certificate and click [**Properties**] button.



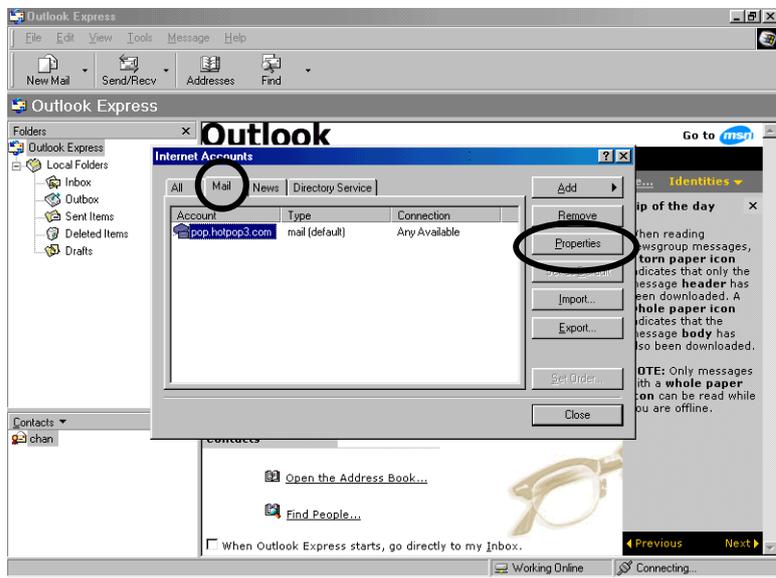
13. Close all windows if you have finished.

1.8 Verify Name On The Certificate with Outlook Express

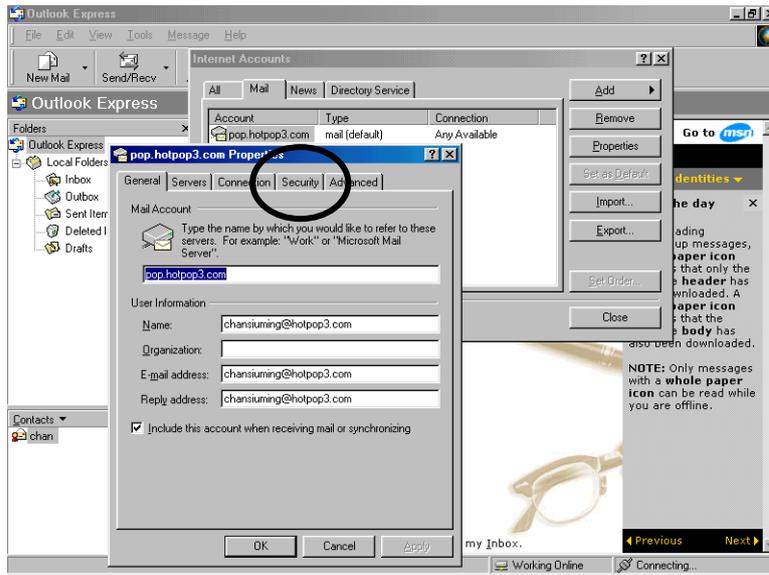
1. From the menu bar of Outlook Express, select <Tools> and then <Accounts>.



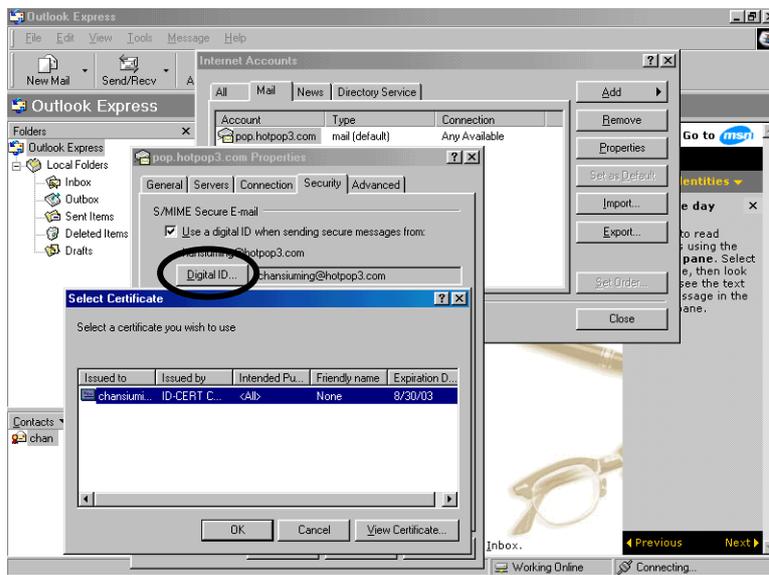
2. On the Internet Accounts window, select the <Mail> tab and click the [Properties] button.



3. On the Properties window, select the “Security” tab.

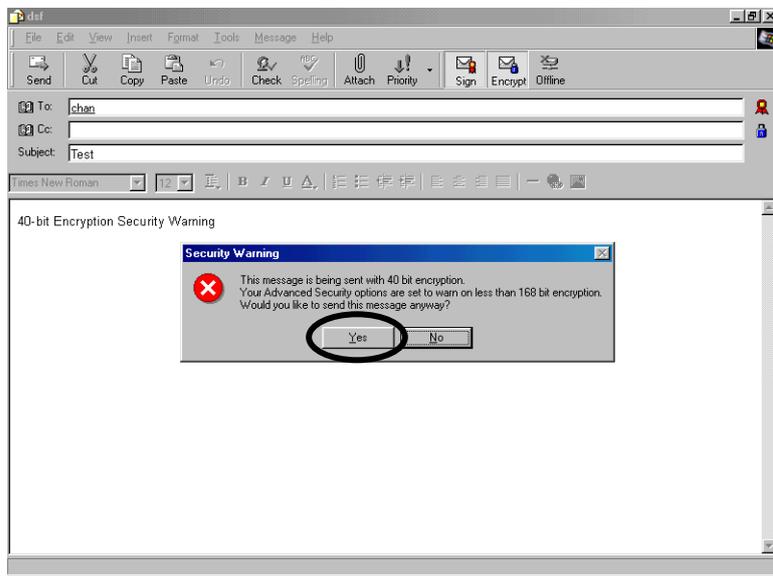


4. On the “Security” tab, click the [Digital ID] button to view your name on the certificate.



1.9 40-bit Encryption Security Warning Message

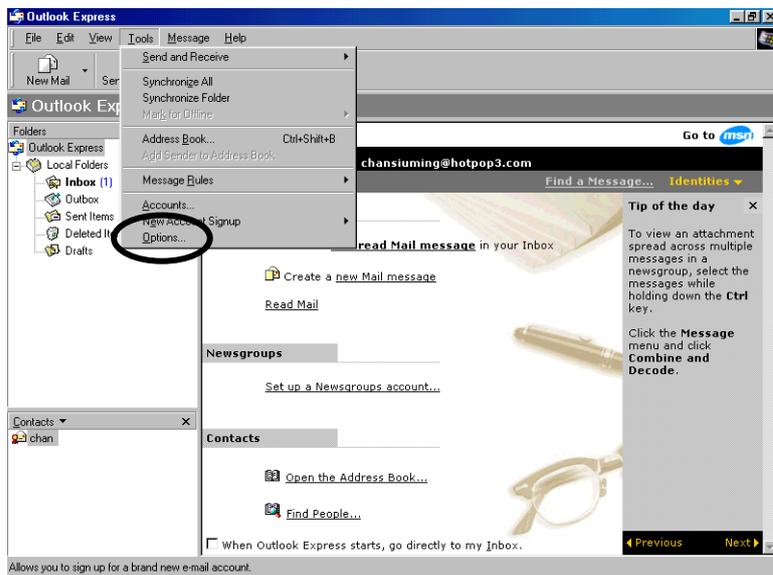
Please note that while sending e-mail messages with Outlook Express, it is normal for the following security-warning message to be displayed. You can select “Yes” to ignore the message and still send out the e-mail message accordingly.



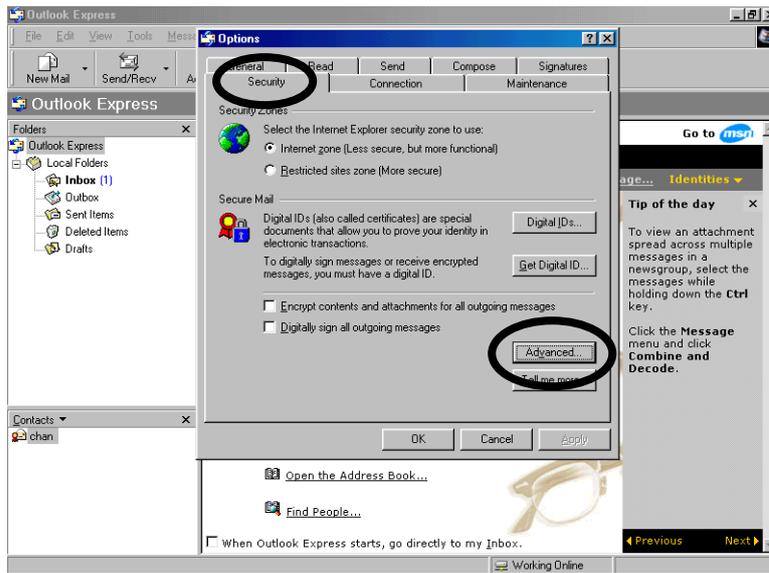
Alternatively you can disable the security warning message feature by selecting 40-bit encryption level.

1.9.1 Disable 40-bit Encryption Security Warning Message

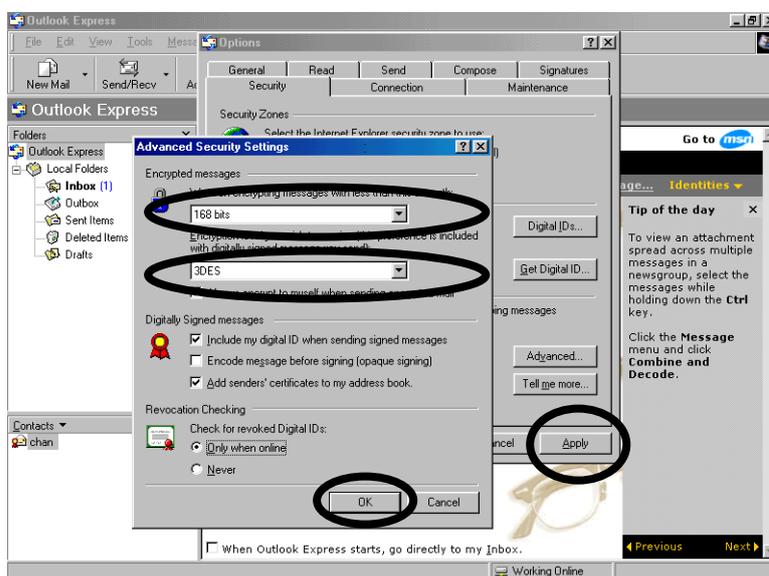
1. On the Outlook Express window, select <Tools> and then <Options>.



2. On the Options window, select the “Security” tab and click the [Advanced] button.



3. On the Advanced Security Settings window, click on the “168 bits” down arrow and select “40 bit”. Click on the “3DES” down arrow and select “RC2 (40-bit)”. Click [OK] button and then [Apply] button.



1.10 Use ID-Cert to Sign and Encrypt E-mails with Outlook Express

You should follow the previous steps to locate your mail recipient (*Please refer to “1.7 Search for E-mail Recipient via ID-Cert Directory with Outlook Express”*) before sending a signed and encrypted e-mail.

1. Start up Outlook Express.
2. Select <File> <New> <Mail> or click the [New Mail] button on the menu bar.



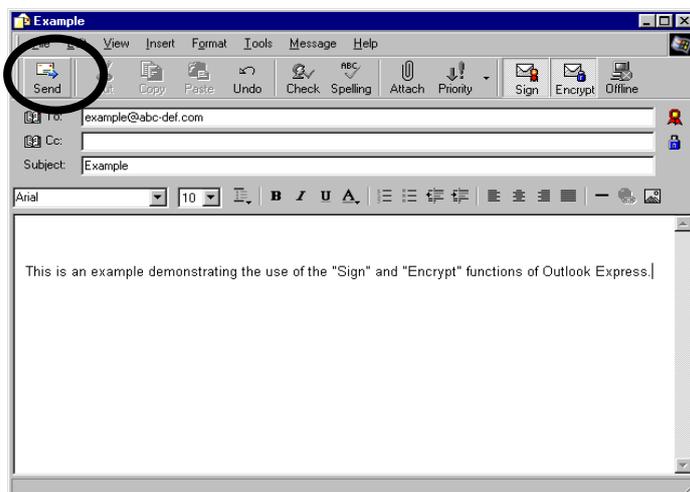
3. Select your e-mail recipient by clicking the [To:] button and select from the list.



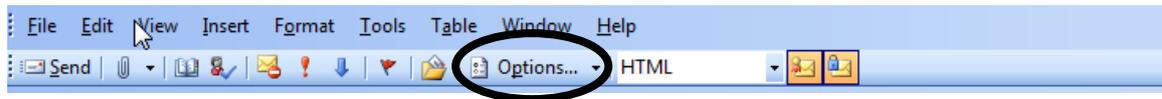
4. Click the [Sign] and [Encrypt] button to secure your e-mail.



5. Enter the subject and body of your e-mail and click the [Send] button to send.



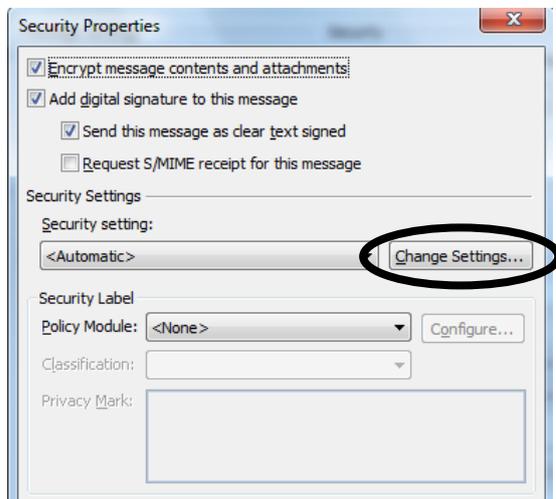
For ID-Cert Class 8 and Class 9, click the [Options].



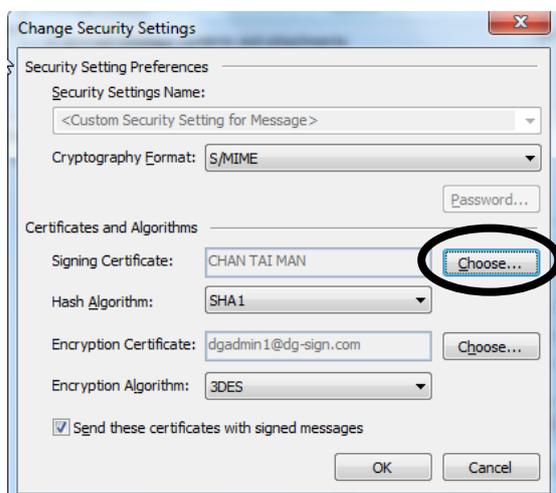
Select the [Security Settings] to select the certificate



Click the [Change Settings] in Security Properties.



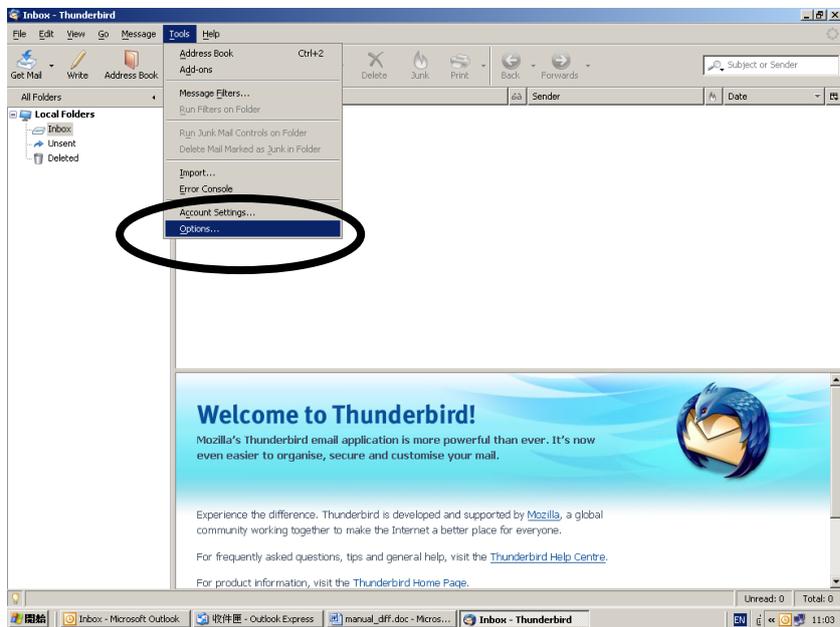
Click [Choose] to select the certificates



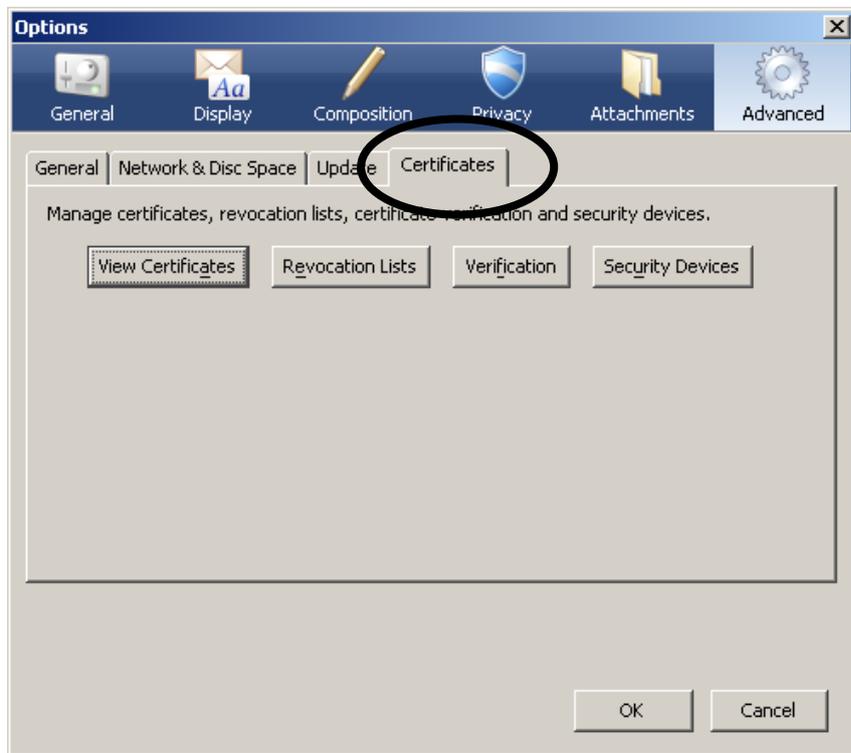
2 Thunderbird Operation

2.1 Importing ID-Cert

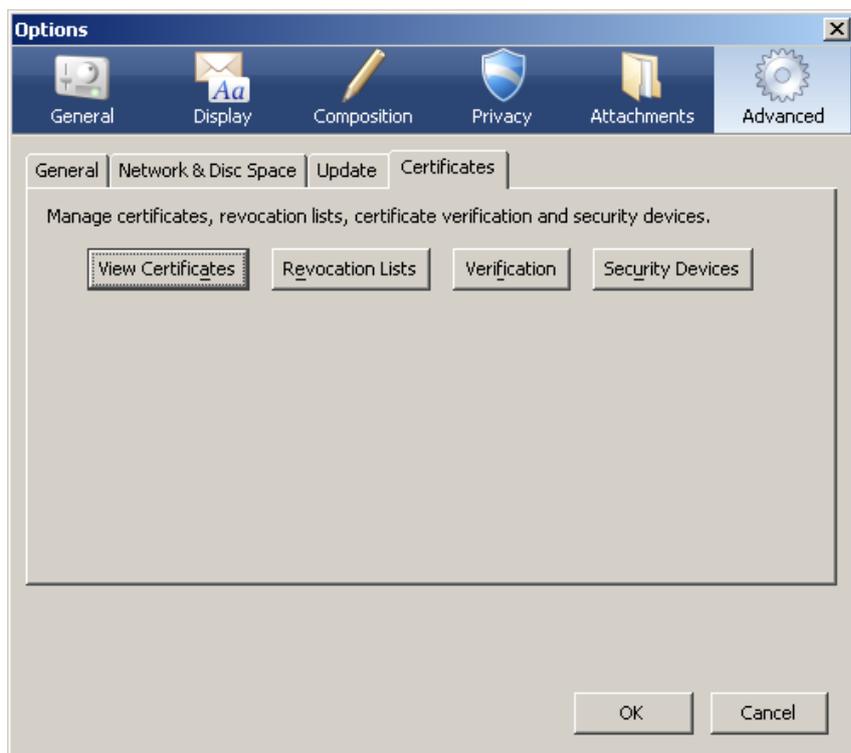
1. From the menu bar of Thunderbird, select <Tools> and then <Options>.



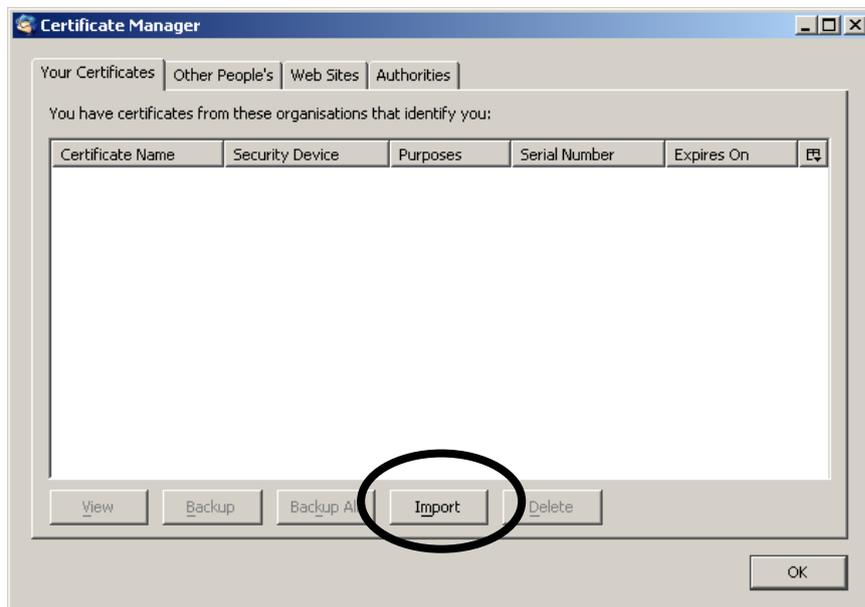
2. In the Options window, click the <Advanced> button and select the <Certificates> tab.



3. Click the [View Certificates] button. The Certificate Manager Import wizard will pop up.

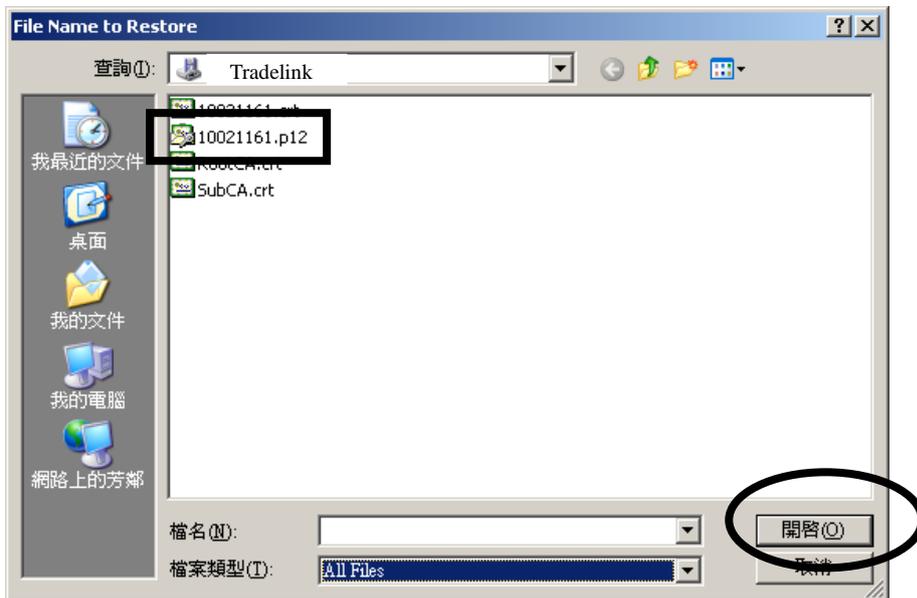


4. Select the <Your Certificates> tab and click [Import] button to continue.

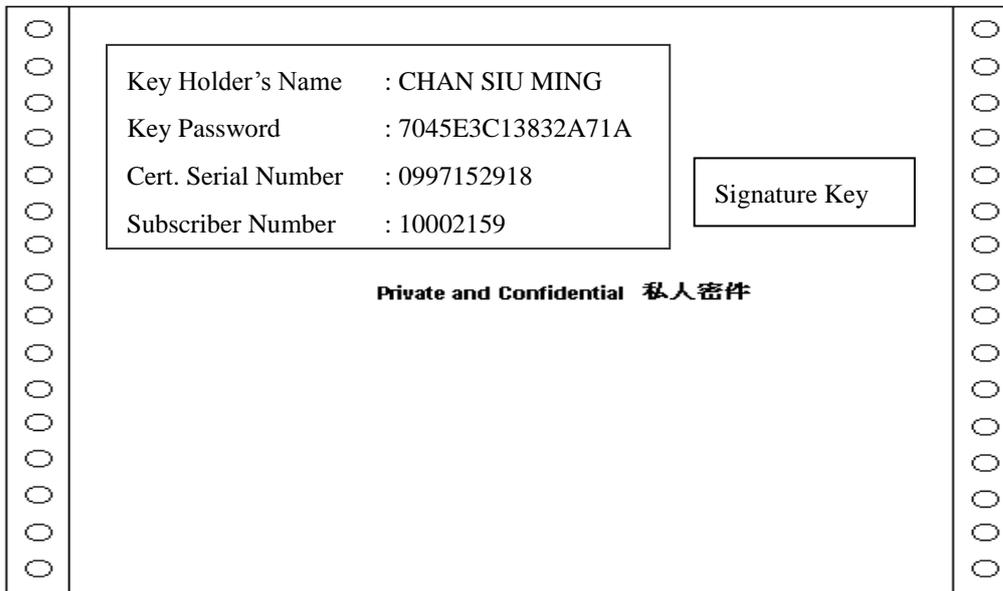


5. Insert your signature ID-Cert storage medium into the computer.

6. Select your drive from the “Look In” drop box and select “All files (*.*)” from the “Files of Type” drop box. The ID-Cert file is named as xxxxxxxx.p12 where xxxxxxxx is your Subscriber Number. Highlight it and click the [Open] button.



7. Input the password into the <Password Entry Dialogue> and click [OK]



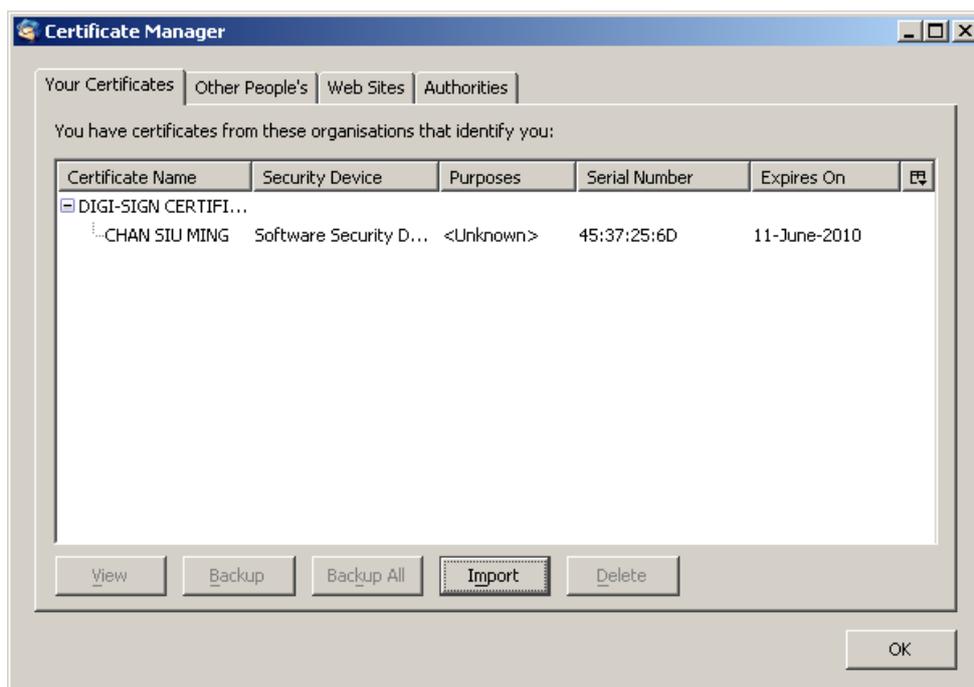
* If the password envelope is not intact when you receive it, please do not use the password and report immediately to the Services Hotline.

** Make sure that the Serial Number in the password envelope is identical to that of the ID-Cert storage medium.

After entering your password, the successful message will pop up. Click [OK] to finish.



8. You have finished importing your ID-Cert and you can view your certificate under <Your Certificates> page.



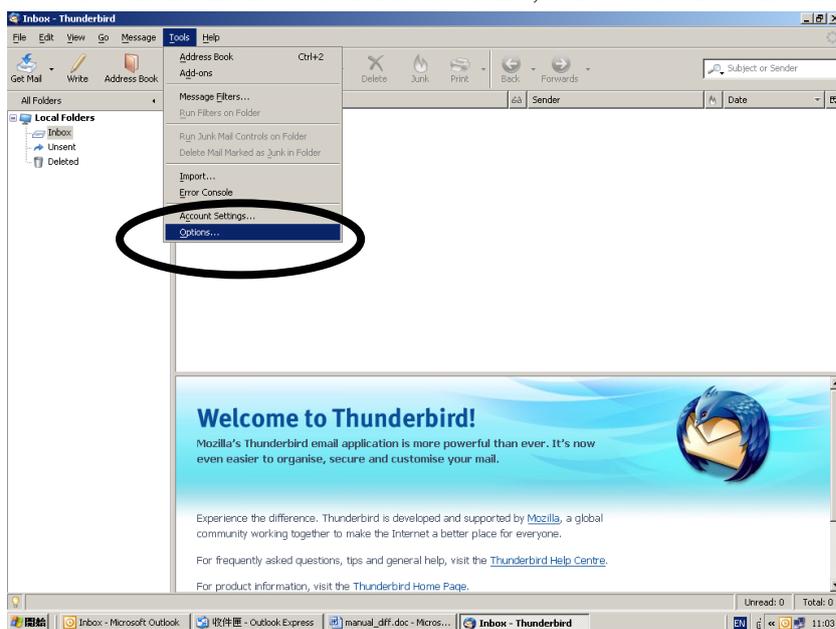
9. Repeat the above steps if you need to import your Encipherment ID-Cert. (Encipherment ID-Cert will allow you to sign and encrypt your e-mail message.)

2.2 Install ID-Cert Root CA and Signing CA Certificate

The ID-Cert Root CA and Signing CA Certificates are used to validate certificates issued by Digi-Sign. You can install the ID-Cert Root CA and Signing CA Certificates from your ID-Cert storage medium.

2.2.1 Installation via ID-Cert Storage Medium

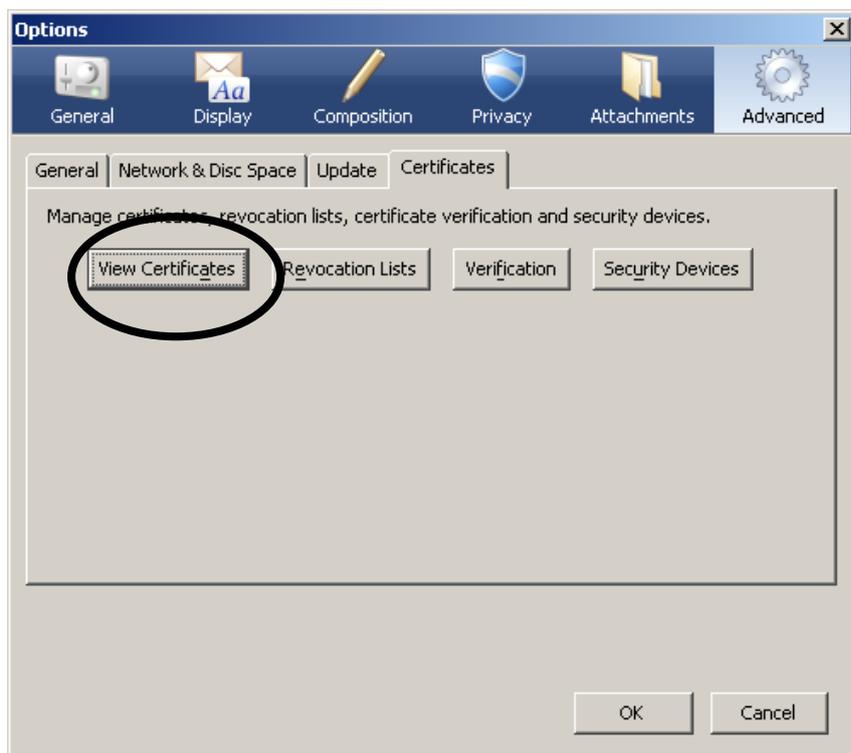
1. From the menu bar of Thunderbird, select <Tools> and then <Options>.



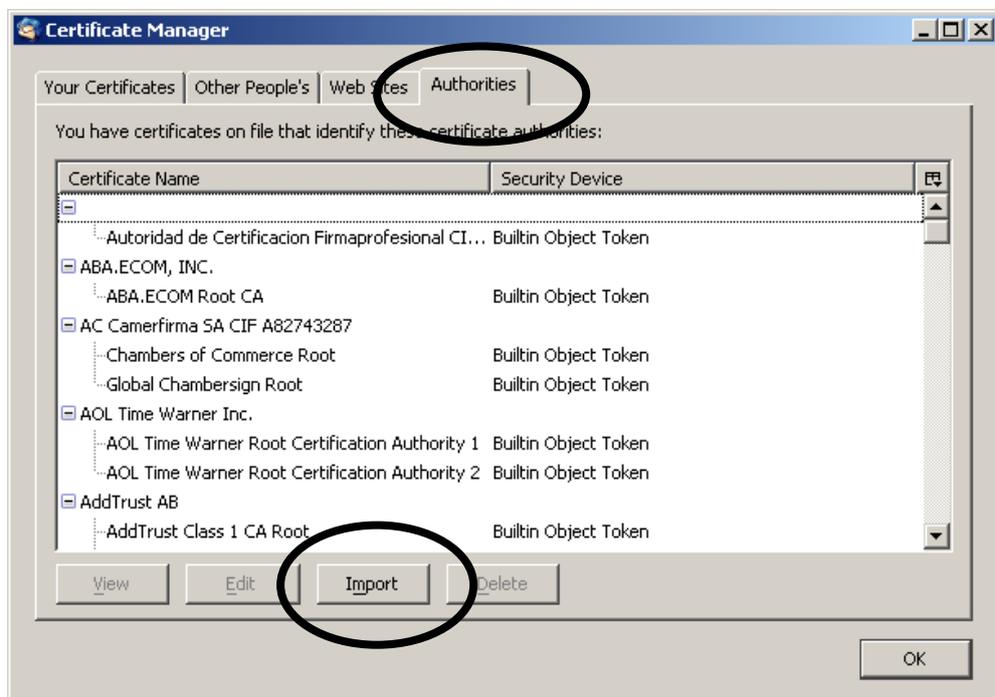
2. In the Options window, click the <Advanced> button and select the <Certificates> tab.



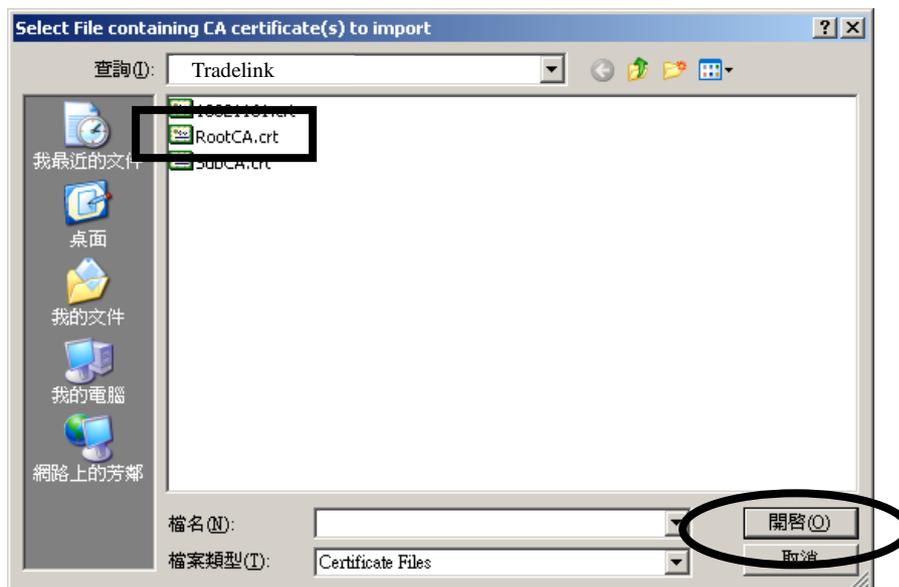
3. Click the [View Certificates] button. The Certificate Manager Import wizard will pop up.



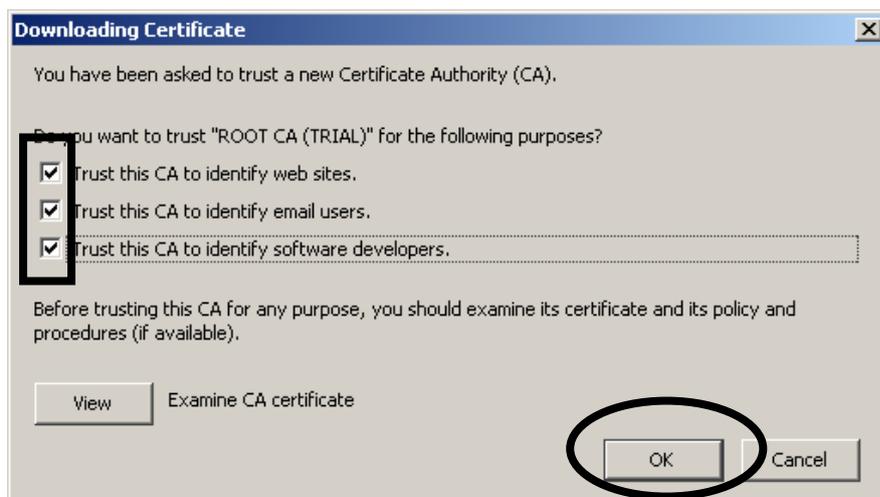
4. Select the <Your Certificates> tab and click [Import] button to continue.



- Select your drive from the “Look In” drop box. Highlight RootCA.crt file and click the [Open] button.



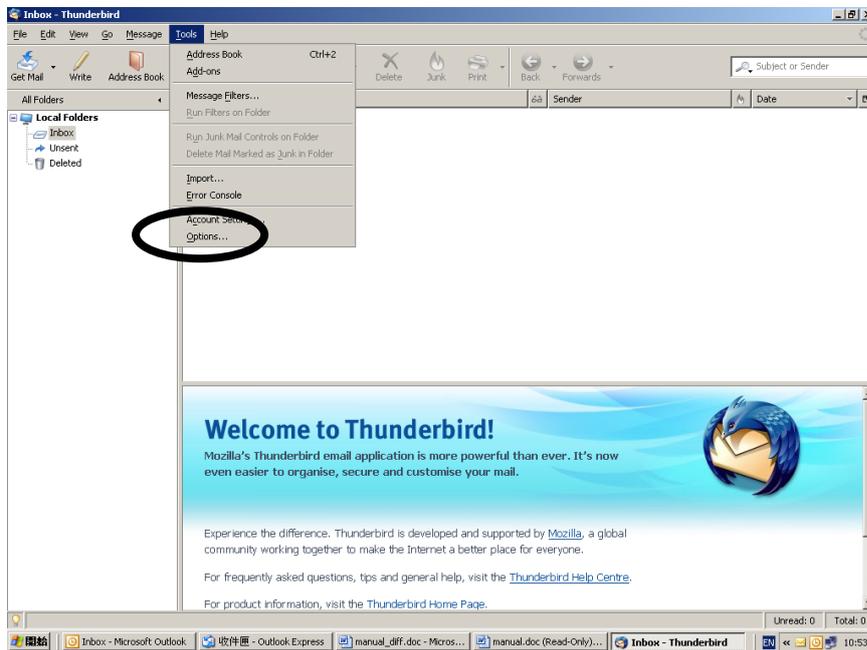
- Check the box to set the trust option and click [OK] to finish.



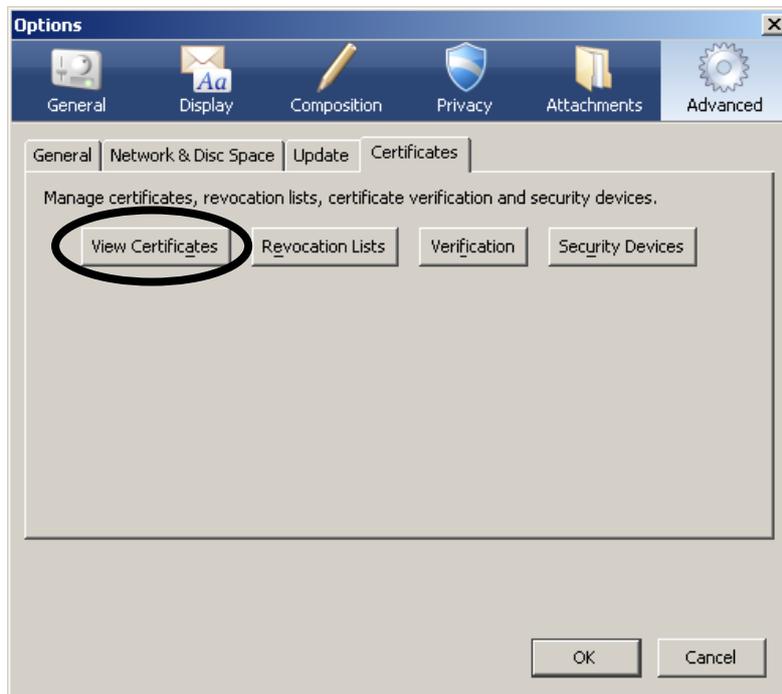
- Repeat the above step to install the “ID-Cert Signing CA certificate 1”. Choose the file named “subca.crt”.

2.3 View Your ID-Cert Content

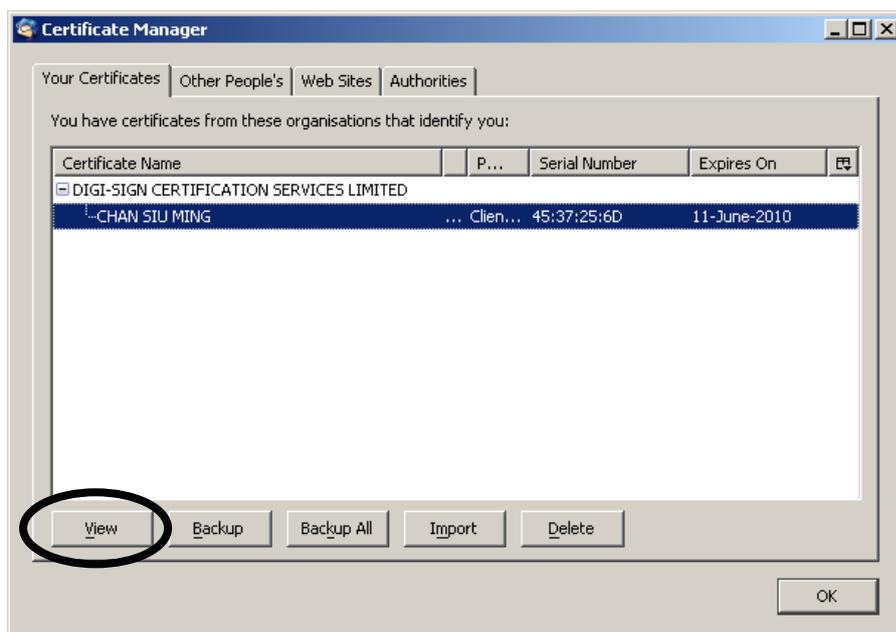
- 1 From the menu bar of Thunderbird, select <Tools> and then <Options>.



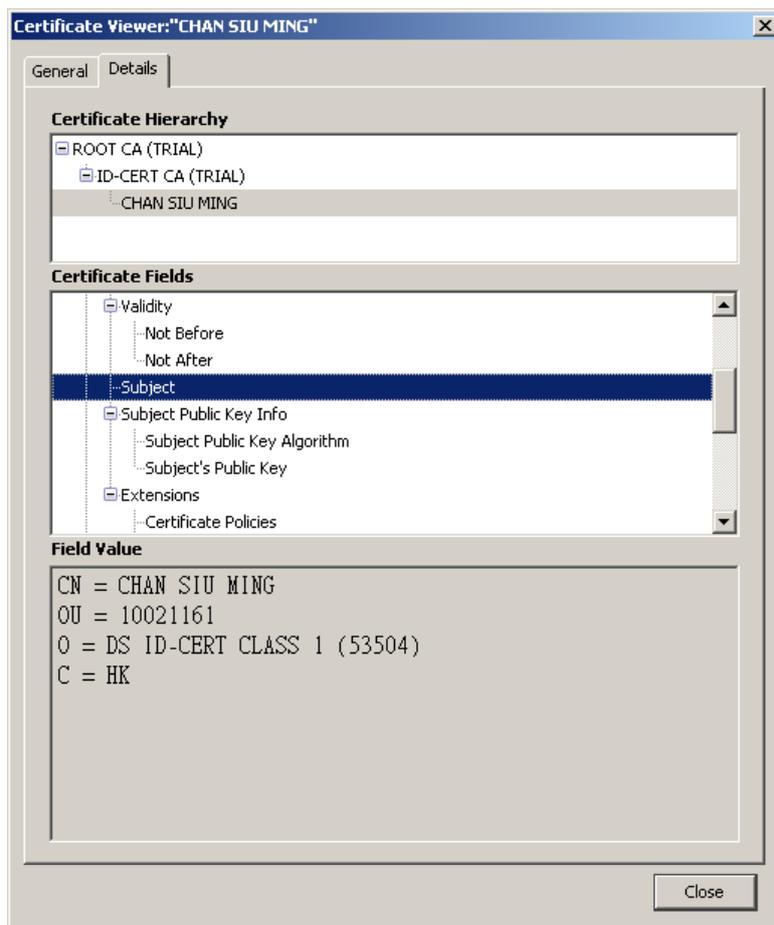
- 2 In the Options window, select the <Certificates> tab and click [View Certificates] button.



3 Select the ID-Cert to be viewed and click the [View] button.

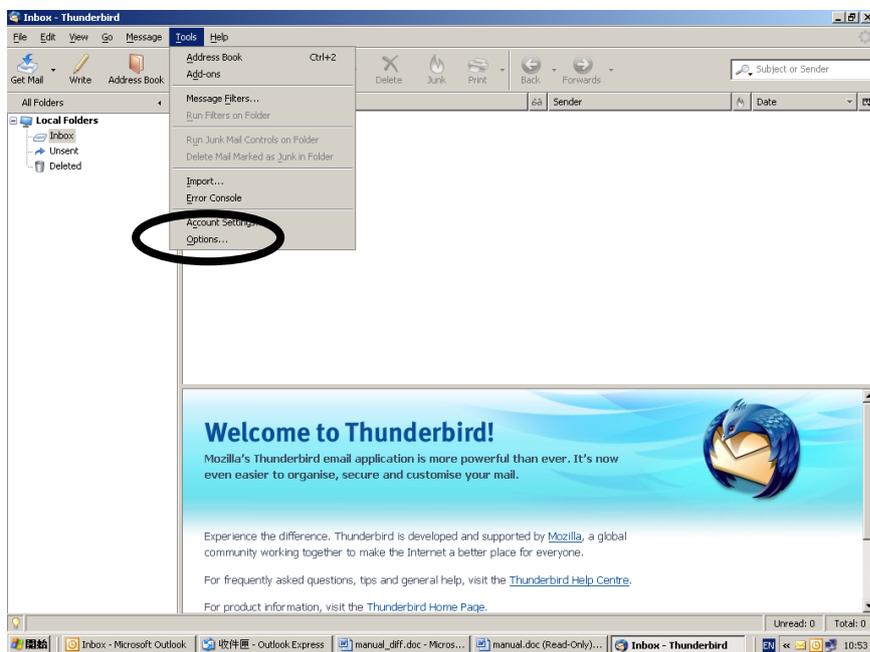


4 Your ID-Cert will be displayed in a new window. Select the “Details” tab to view the contents. You can click [Close] to close the window after viewing.

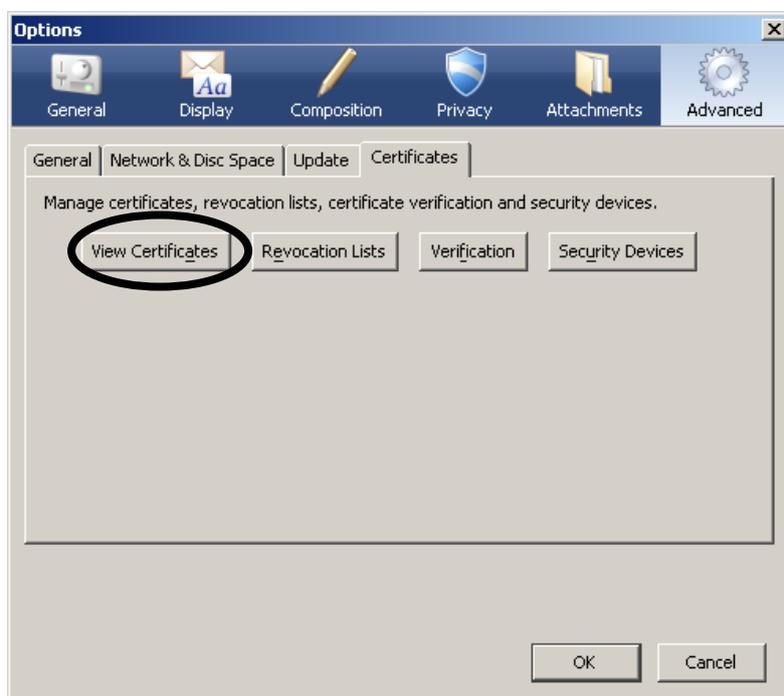


2.4 Backup Your ID-Cert

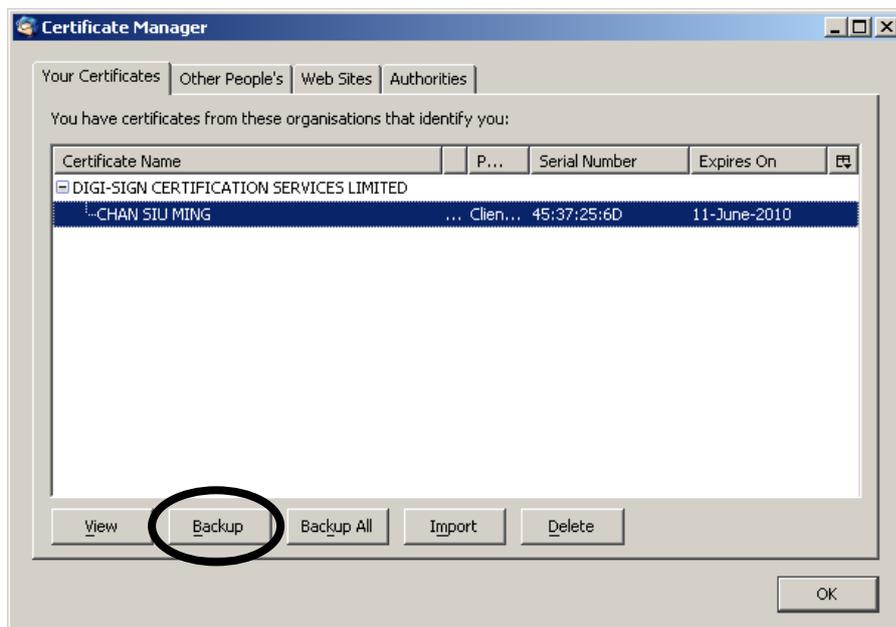
- 1 Insert a blank ID-Cert storage medium into your computer.
- 2 From the menu bar of Thunderbird, select <Tools> and then <Options>.



- 3 In the Options window, select the <Certificates> tab and click [View Certificates] button.



- 4 Select the “Your Certificates” tab, highlight the certificate name and click [Backup] button.



- 5 Input the file name for the private key and click [Save] button.



- 6 You are required to enter the new password used to protect the private key. Click [OK] to finish.



- 7 You will see the screen "Successfully backed up your security certificate(s) and private key(s)" and you can click [OK].



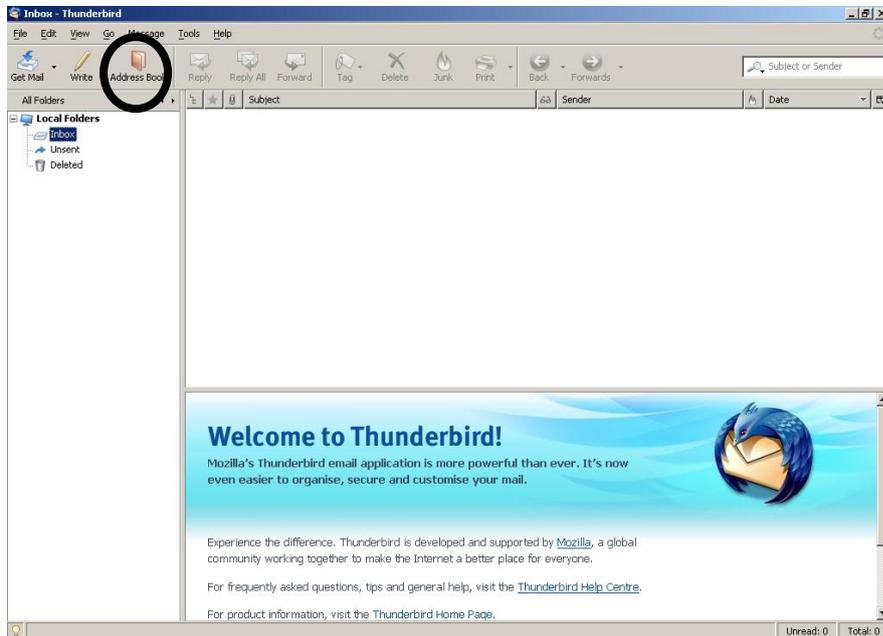
- 8 After exporting your ID-Cert, keep the private key in safe custody.

2.5 Restore Your ID-Cert

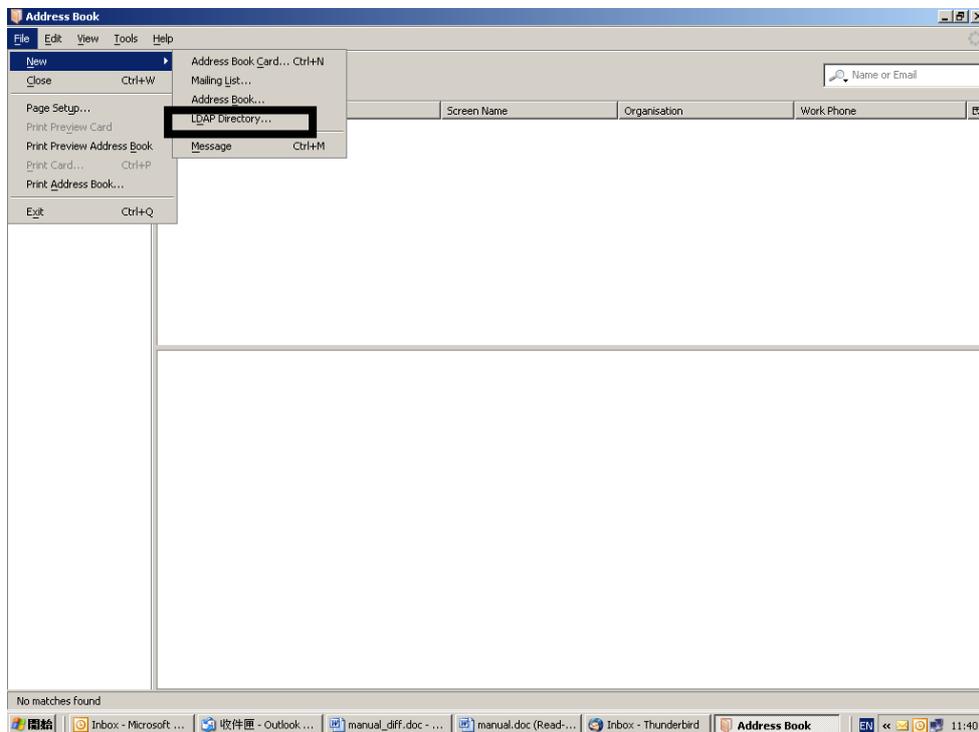
- 1 Inset your ID-Cert backup storage medium.
- 2 Follow the procedures in “**2.1 Importing ID-Cert**”. The file name required now should be the one you specified in the backup section and you need to enter the new password that you have assigned in the section “**2.4 Backup your ID-Cert**”.

2.6 Search for E-mail Recipient via ID-Cert Directory with Thunderbird

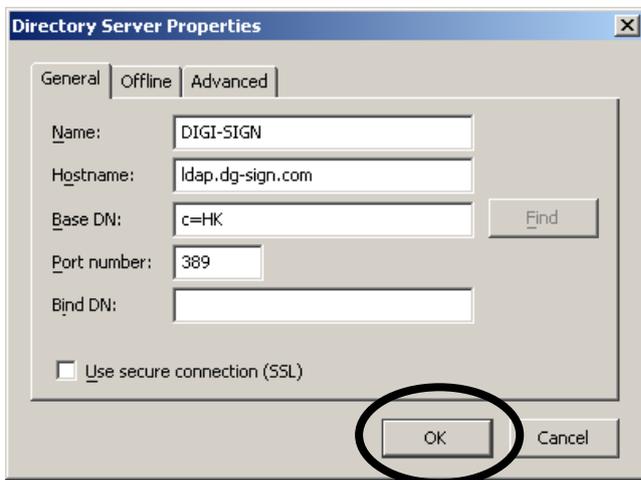
- 1 Startup Thunderbird
- 2 Click [Address Book]



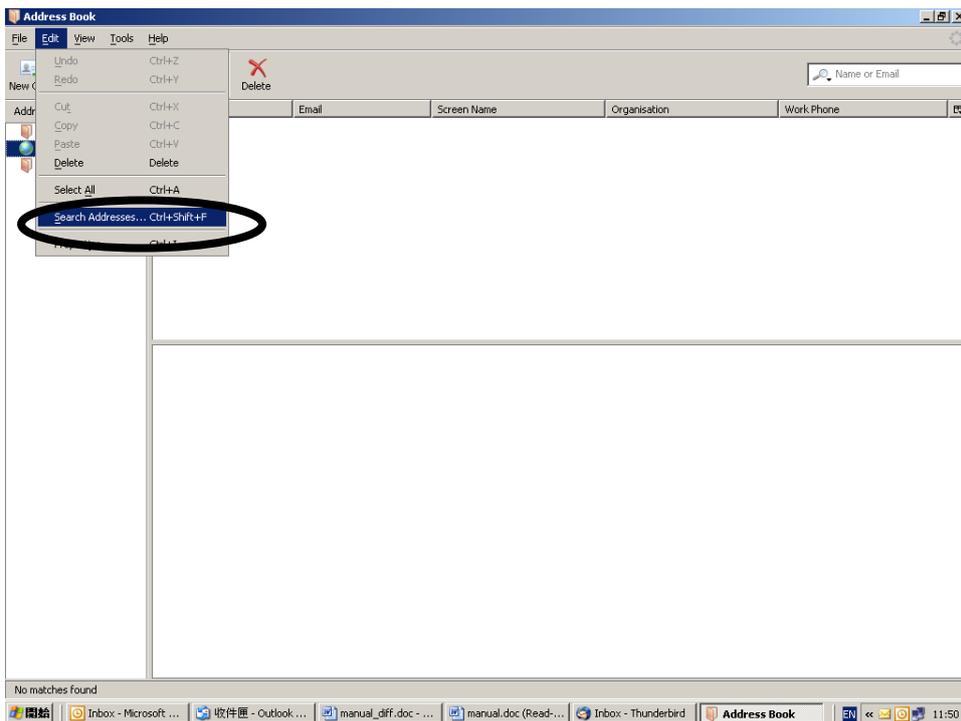
- 3 Click the <File> from the menu bar, select <New> and then <LDAP directory>.



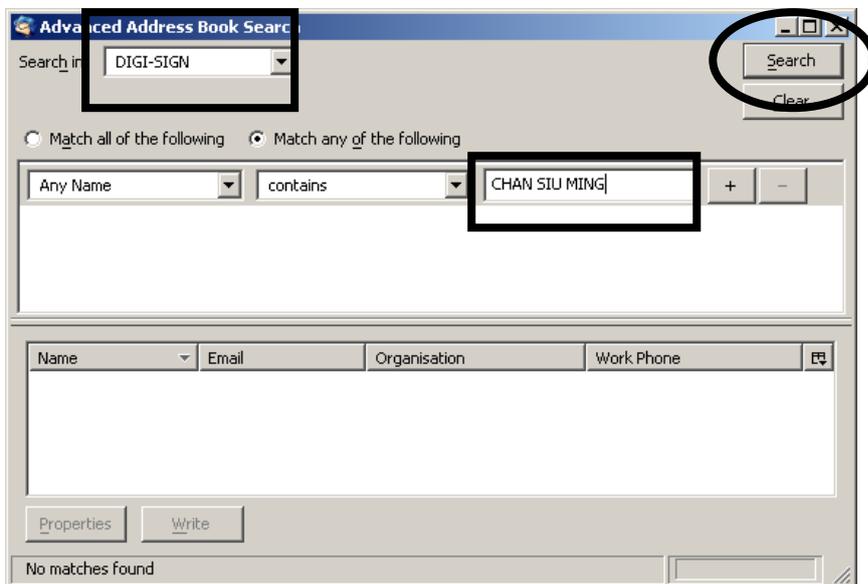
- 4 A “Directory Server Properties” window will pop up. Enter the following details
 - Name = DIGI-SIGN
 - Host Name = **ldap.dg-sign.com**
 - Base DN = c=HK
 click the [OK] button.



- 5 Select the <Edit> from the menu bar and <Search Addresses>.

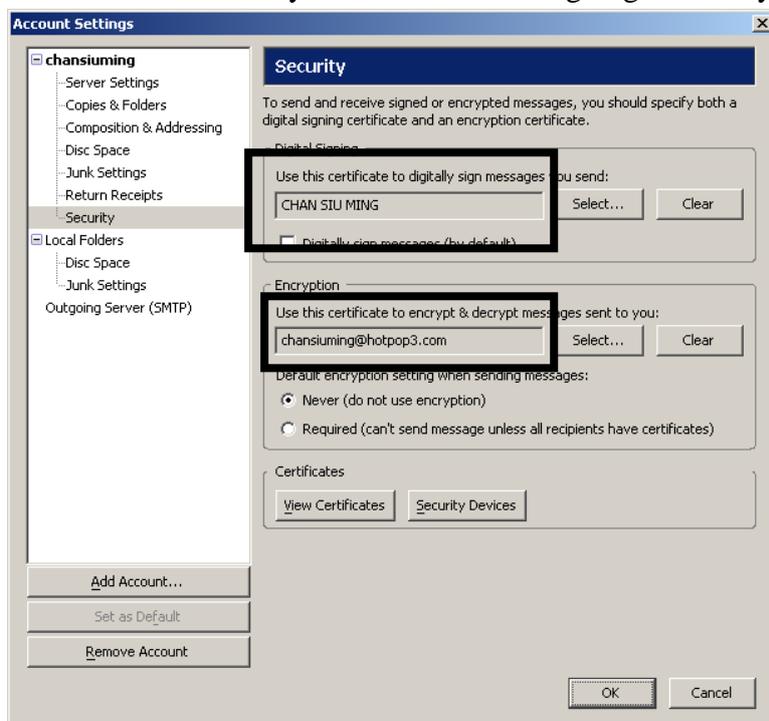


- 6 An “Advanced Address Book Search” window will pop up. Select the directory from <Search in> and enter the searching criteria in the space. Click [Search] to start the search.



2.7 Use ID-Cert to Sign and Encrypt E-mails with Thunderbird

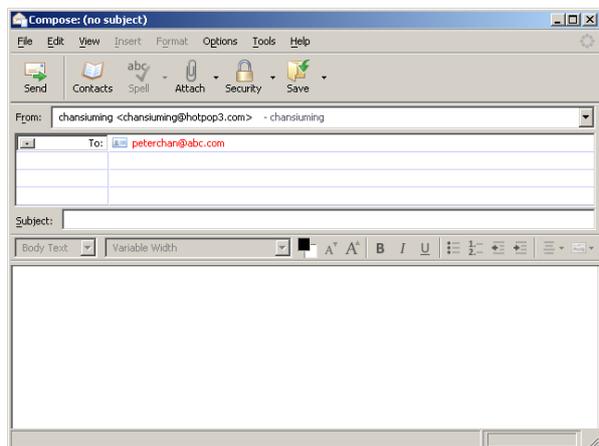
- 1 Startup Thunderbird
- 2 Select the <Tools> from the menu bar and then select <Account Settings> to select the certificate which you want to use for signing and encryption.



- 3 Click [Write] on the menu bar.



- 4 Select your e-mail recipient



- 5 Click the [Security] button and select <Encrypt the message> and <Digitally Sign the Message> and click the [Send] button to send.

