

InCommon®



InCommon Certificate Manager

Email and Client Certificate End User Guide

InCommon
c/o Internet2
1000 Oakbrook Drive, Suite 300
Ann Arbor MI, 48104

Introduction

This step by step guide will explain how to enroll for and download your email or client certificate.

Step 1 - Enrollment and Collection of Your Email and Client Certificate

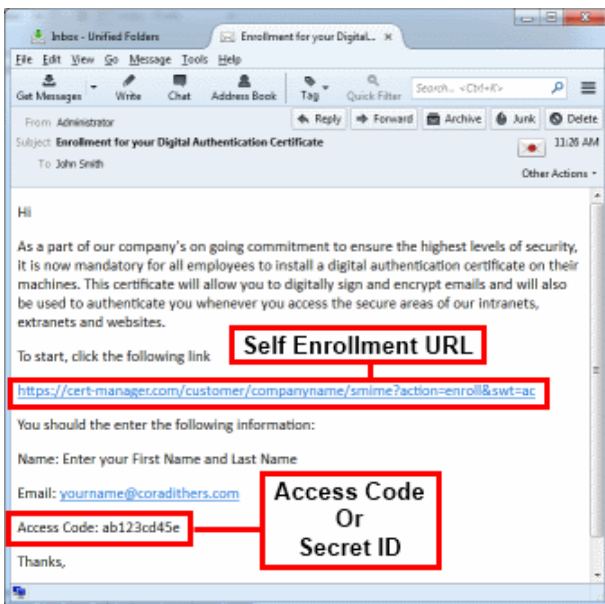
Firstly, your administrator should have sent you a provisioning email. The exact procedure to follow will depend on the type of email you have received:

Enrollment Mails (2 Options):

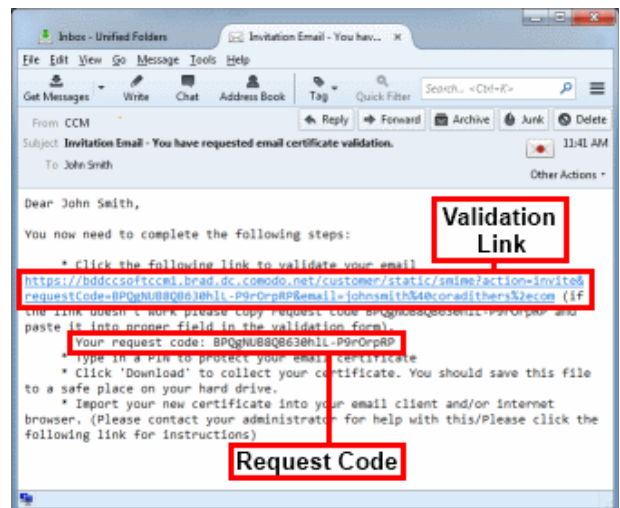
- [Click here if your email contains an Access Code](#)
- OR
- [Click here if your email contains a Secret ID](#)

Invitation Mail

- [Click here if your email contains a Request Code and a Validation Link](#)



Enrollment Type Email



Invitation Email

Enrollment by Access Code

- Click the URL in the email to visit the certificate enrollment page.

Certificate Manager

S/MIME Certificate Enroll

Access Code: * ●●●●●●


First Name: * John

Middle Name:

Last Name: * Smith

Email: * johnsmith@coradithers.com

Certificate Type: * High Persona Validated Cert

Self Enrollment Passphrase: * ●●●●●● 

Re-type Self Enrollment Passphrase: * ●●●●●●

1
Comodo ePKI Certificate Manager Agreement – EV Enabled
THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE
READ THE
AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND
CONDITIONS.

IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS
CAREFULLY BEFORE APPLYING
FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE
MANAGER ACCOUNT OR THE
CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR,
ACCESSING, OR
PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR
ACCESSING CERTIFICATE
MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I
ACCEPT" BELOW, YOU
ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND
THAT YOU
UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS
PRESENTED HEREIN.

PRINT

 I accept the terms and conditions.**Scroll to bottom of the agreement to activate check box.*

ENROLL

CANCEL

- Copy and paste the **Access code** from your enrollment email.
- Type your full name in the **Name** Field.
- Type your internal corporate **E-mail** address in the 'E-Mail' field.
- Enter your password phrase. This phrase is needed to revoke the certificate should the situation arise.

- In addition to the standard fields in the enrollment form, additional custom fields such as 'Telephone No.' 'Employee Code' may also be displayed depending on how the administrator has configured it.
- Read the *License Agreement* and check the box alongside the 'I accept terms and conditions'.

Note: If you decline the agreement you will not be able to continue the enrollment process.

- Click the '**Submit**' button.

Important! The application for the certificate must be made from the machine that certificate will be installed on (i.e. your office machine.)

After you click the '**Submit**' button, you will see a confirmation dialog...

Certificate Manager

Confirmation

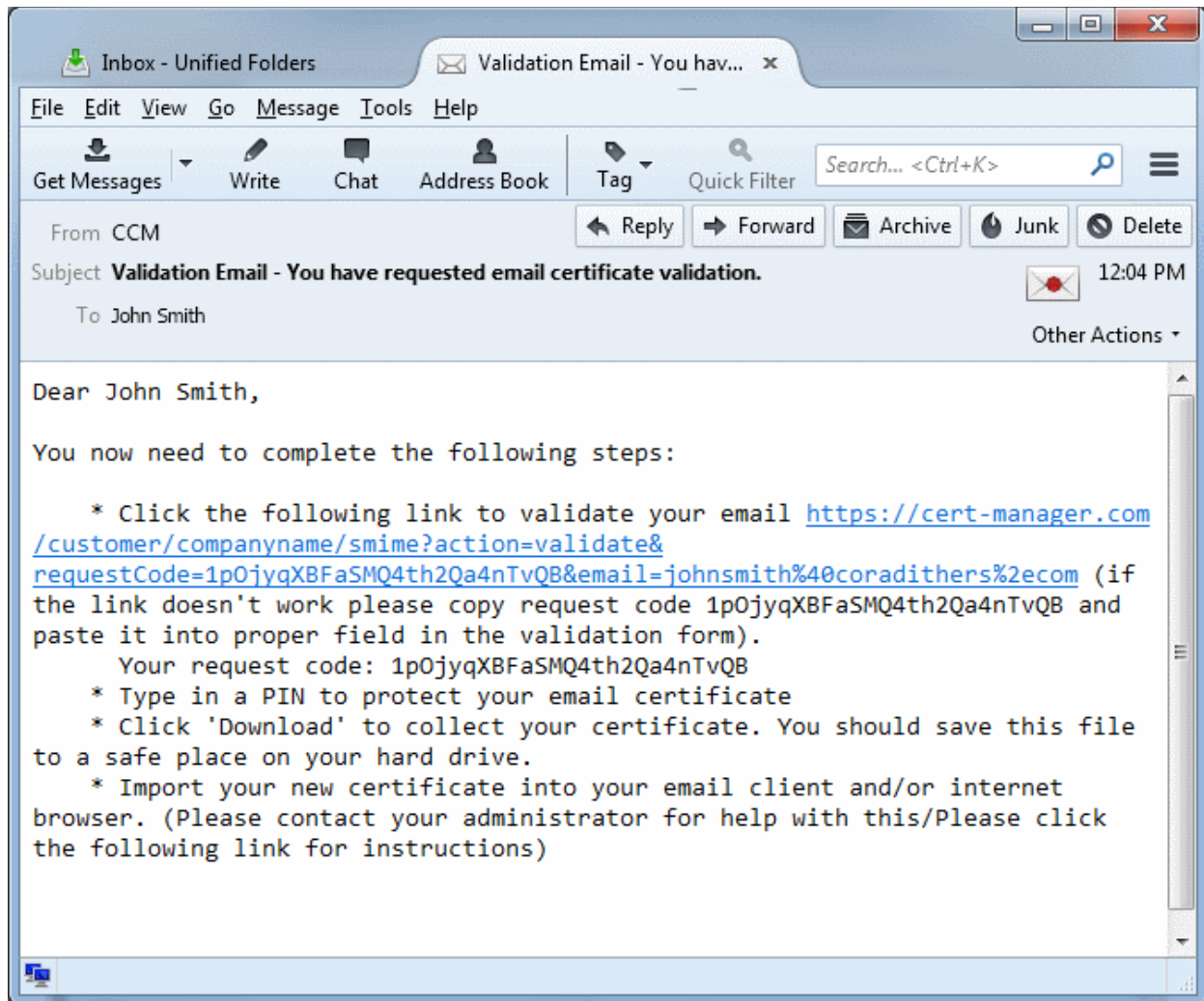
You have requested a S/MIME Certificate with the follow details:

Email: **johnsmith@coradithers.com,**
Name: **John Smith.**

We have sent you an email containing an enrollment link in order to complete the rest of the enrollment process.

[BACK](#)

... and you will receive an email containing a link for validation, a request validation code and instructions for downloading and collecting the certificate. An example is shown below.



Validation email

The precise content may differ to the example shown

- You will be taken to the validation form upon clicking the link in the email.

Certificate Manager

Account Validation

Code: *

Email: *

Certificate Type: *

PIN: ⓘ

Re-type PIN:

Select address fields to remove from the certificate.

Address as it will appear in certificate		Remove
Address1:	<input type="text" value="Mount Road"/>	<input type="checkbox"/>
Address2:	<input type="text"/>	<input type="checkbox"/>
Address3:	<input type="text"/>	<input type="checkbox"/>
City:	<input type="text" value="Riverdale"/>	<input type="checkbox"/>
State or province:	<input type="text" value="Alabama"/>	<input type="checkbox"/>
Postal Code:	<input type="text" value="123456"/>	<input type="checkbox"/>
Employee ID: *	<input type="text"/>	

- The **Code** and **E-mail** fields will be auto-populated.
- Type the PIN in the '**PIN**' fields to protect your certificate. You will be asked for this PIN when you import the certificate into the certificate store of your Internet browser and/or mail client.
- If you wish to have the certificate without the address details, select the appropriate '**Remove**' check boxes.
- Click the '**Submit**' button to complete the validation process.

Once the validation process is completed, a download dialog will be displayed for you download and save the certificate.

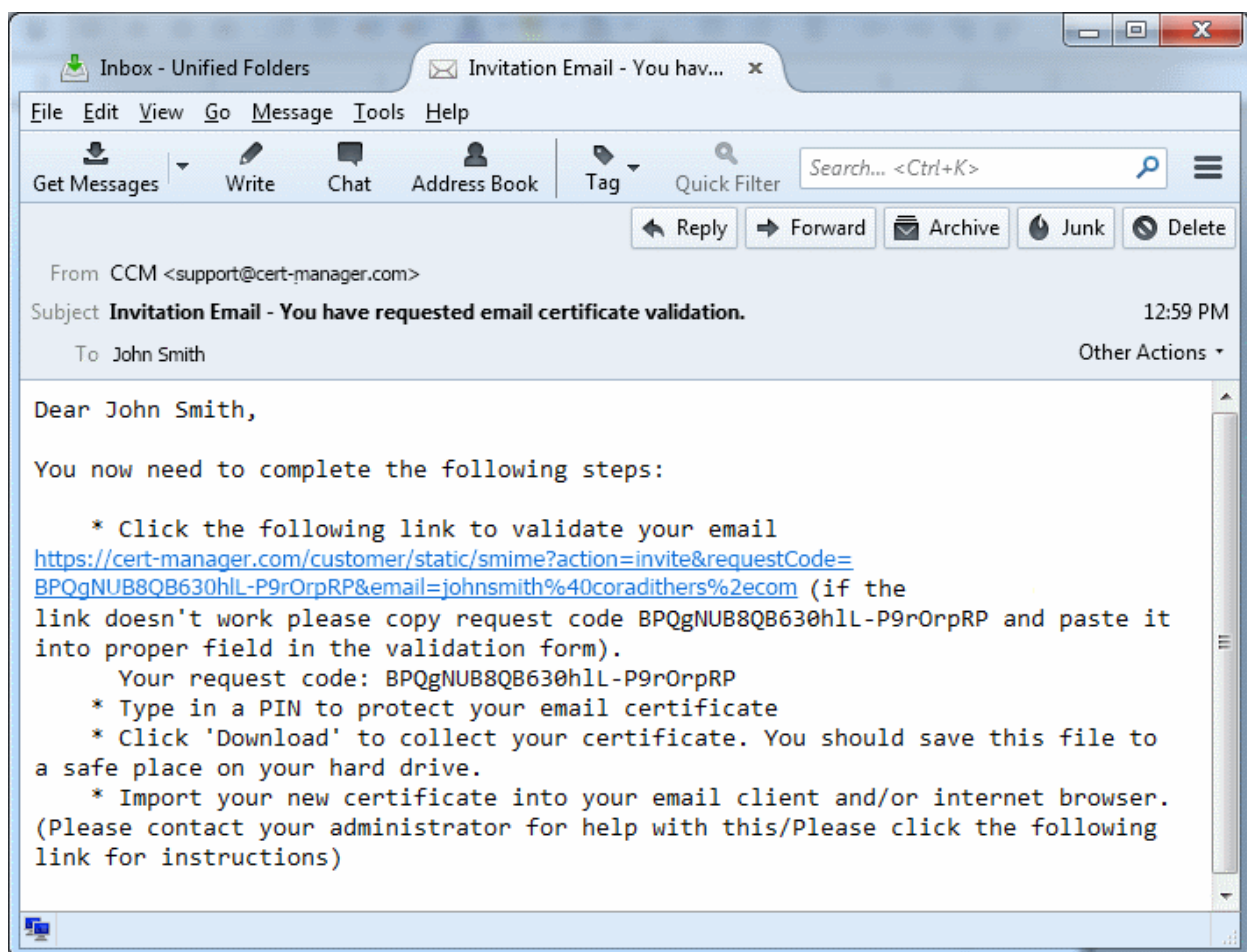
Next: [Collecting your certificate](#)

- Enter your password phrase in the '**Annual Renewal Pass-phrase**' fields. This phrase is needed to revoke or renew the certificate.
- Enter the password in the '**Password**' fields. This will protect access to your Digital ID.
- In addition to the standard fields in the enrollment form, additional custom fields such as 'Telephone No.' 'Employee Code' may also be displayed depending on how the administrator has configured it.
- The address details that are selected in the check boxes under '**Remove**' will not appear in your certificate.
- Read the License Agreement and check the box alongside the 'I accept terms and conditions'.
- Click the '**Enroll**' button.
- A download dialog will be displayed for you to download and save the certificate.
- [Click here](#) to find out more about certificate collection.

Next: [Collecting your certificate](#)

Enrollment by Invitation from Administrator

The invitation mail contains a link for validation, a request validation code and instructions for downloading and collecting the certificate. An example is shown below.



Invitation email - The precise content may differ to the example shown

- You will be taken to the 'User Registration' form upon clicking the link in the email.

Certificate Manager

User Registration

Code: *

Email: *

Certificate Type:

PIN: ⓘ

Re-type PIN:

Self Enrollment Passphrase: * ⓘ

Re-type Self Enrollment Passphrase: *

Select address fields to remove from the certificate.

Address as it will appear in certificate	Remove
Address1: <input type="text" value="100, Raleigh Street"/>	<input type="checkbox"/>
Address2: <input type="text"/>	<input type="checkbox"/>
Address3: <input type="text"/>	<input type="checkbox"/>
City: <input type="text" value="Riverdale"/>	<input type="checkbox"/>
State or province: <input type="text" value="Alabama"/>	<input type="checkbox"/>
Postal Code: <input type="text" value="123456"/>	<input type="checkbox"/>
Employee ID: * <input type="text"/>	

1
 Comodo ePKI Certificate Manager Agreement – EV Enabled
 THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE
 READ THE
 AGREEMENT CAREFULLY BEFORE ACCEPTING THE TERMS AND
 CONDITIONS.

IMPORTANT—PLEASE READ THESE TERMS AND CONDITIONS
 CAREFULLY BEFORE APPLYING
 FOR, ACCEPTING, OR USING YOUR COMODO EPKI CERTIFICATE
 MANAGER ACCOUNT OR THE
 CERTIFICATE MANAGER SOFTWARE. BY USING, APPLYING FOR,
 ACCESSING, OR
 PURCHASING A CERTIFICATE MANAGER ACCOUNT OR USING OR
 ACCESSING CERTIFICATE
 MANAGER OR BY ACCEPTING THIS AGREEMENT BY CLICKING ON "I
 ACCEPT" BELOW, YOU
 ACKNOWLEDGE THAT YOU HAVE READ THIS LICENSE AGREEMENT AND
 THAT YOU
 UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS
 PRESENTED HEREIN.

PRINT

I accept the terms and conditions.*
 Scroll to bottom of the agreement to activate check box.

SUBMIT

CANCEL

- The Code and E-mail fields will be auto-populated.
- Type the PIN in the 'PIN' and Re-type PIN fields to protect your certificate. You will be asked for this PIN when you import the certificate into the certificate store of your Internet browser and/or mail client.

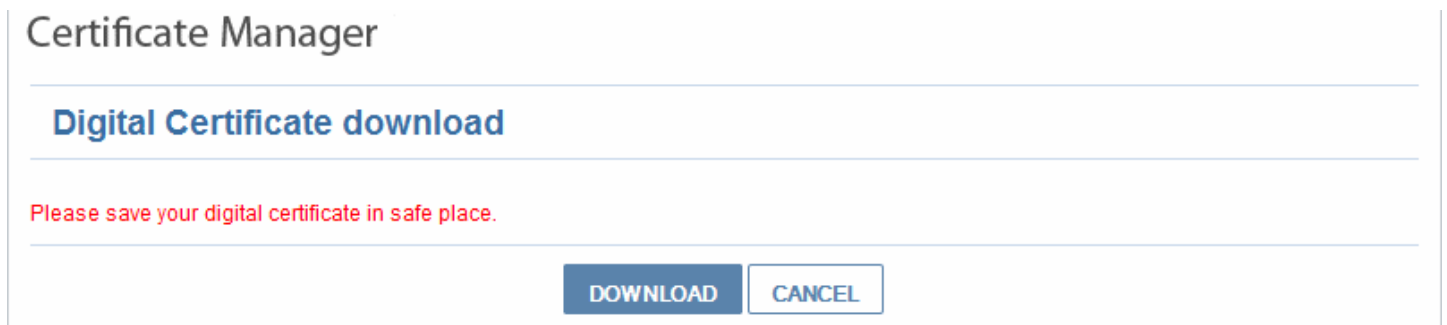
- Type the Pass-Phrase and Re-type Pass-Phrase fields for your client certificate. This phrase is needed to revoke the certificate should the situation arise.
- If you wish to have the certificate without the selected address details, select the appropriate 'Remove' check boxes.
- Click the 'Submit' button to complete the validation process.

Once the registration process is completed, a download dialog will be displayed for you download and save the certificate.

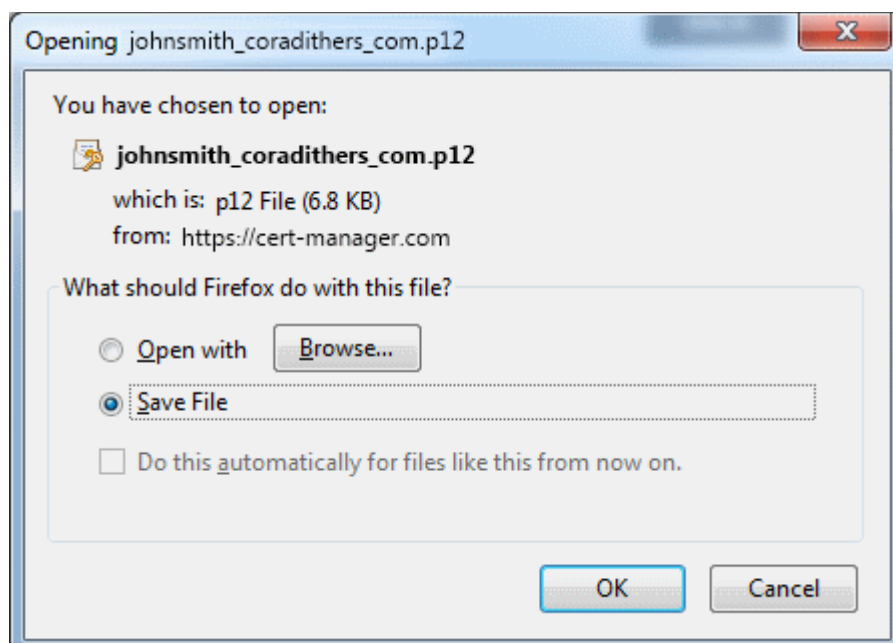
Next: [Collecting your certificate.](#)

Certificate Collection

To collect your certificate click the certificate download URL stated in the certificate collection email. A download dialog will be displayed enabling the applicant to download and save the certificate once the validation is complete.



The applicant can collect the certificate by clicking the '**Download**' button and save the file in a safe location in his/her computer.



InCommon Certificate Services Manager will deliver the certificate in PKCS#12 file format (.p12 file). The pass-code specified in the PIN fields is used to protect access to this .p12 file. You will be asked for this PIN when you import the certificate into the certificate store of your Internet browser and/or mail client.

The second (and final) stage of the procedure is to import your digital certificate into the certificate storage of your Internet browser and/or mail client. The exact process for completing this task is dependent on which browser and/or mail client you use. See the following section '[Importing Your Certificate into Your Browser or/and Email Client – Step 2](#)' for more details.

Step 2 - Importing Your Certificate into Your Browser or/and Email Client

Once [Step 1](#) has been successfully completed, you need to import your certificate into your web browser or/and email client. Select you type of application from the list below to view step-by-step guidance on this process:

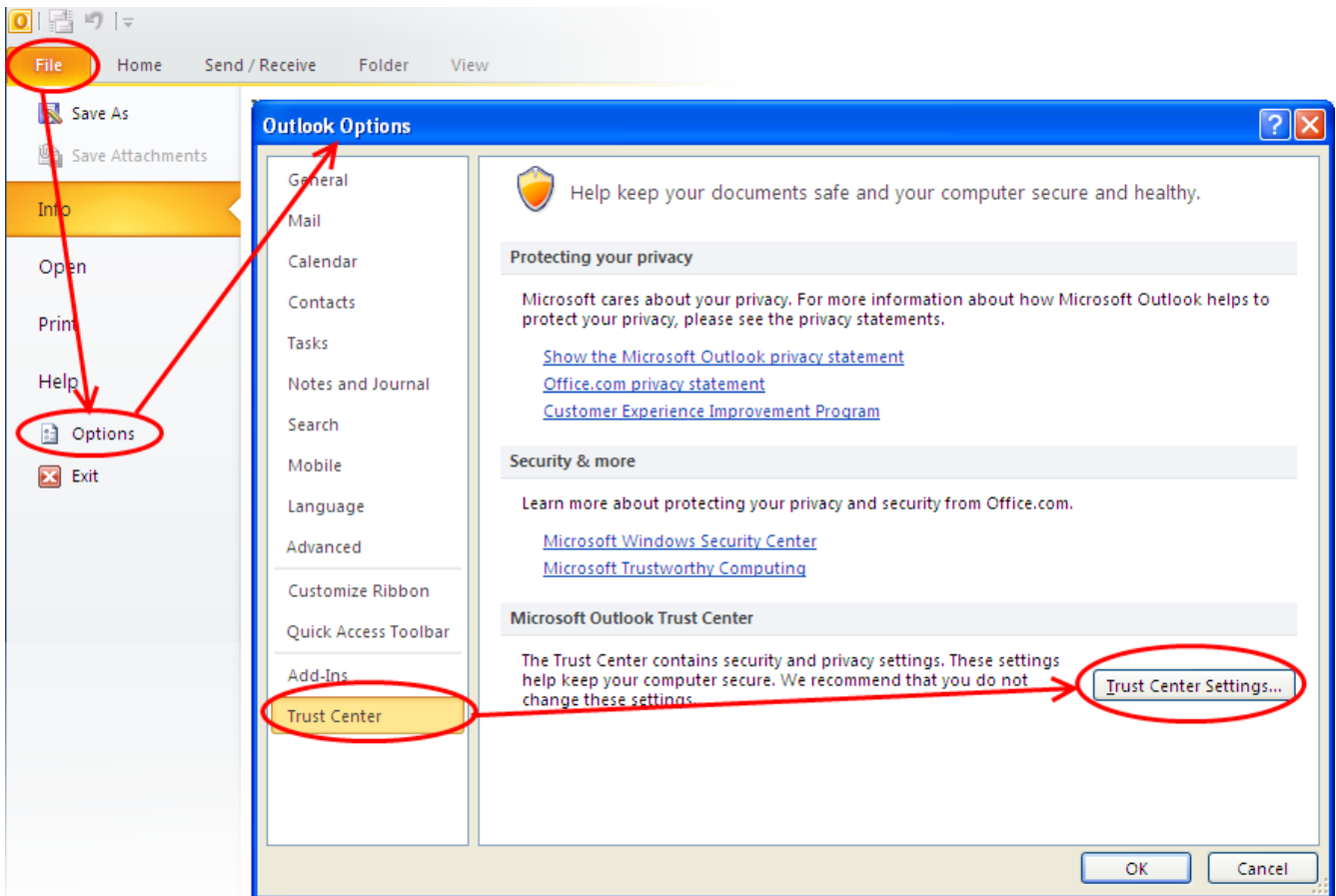
Email Clients	Browsers	Mobile Devices
<ul style="list-style-type: none"> • Outlook 2010 / 2013 • Outlook 2003 • Windows Live Mail • Mozilla Thunderbird • Mac OS X Mail/Apple Mail • Eudora • Bat! • Outlook Express 5 & 6 • Mozilla SeaMonkey 	<ul style="list-style-type: none"> • Internet Explorer • Comodo Dragon • Comodo IceDragon • Firefox • Opera • Safari (Windows) • Safari (Mac) • Chrome (Windows) • Chrome (Mac) 	<ul style="list-style-type: none"> • iPhone/iPad • Android Device – Native • Android – Djigzo App

Importing your Certificate into Outlook 2010/2013

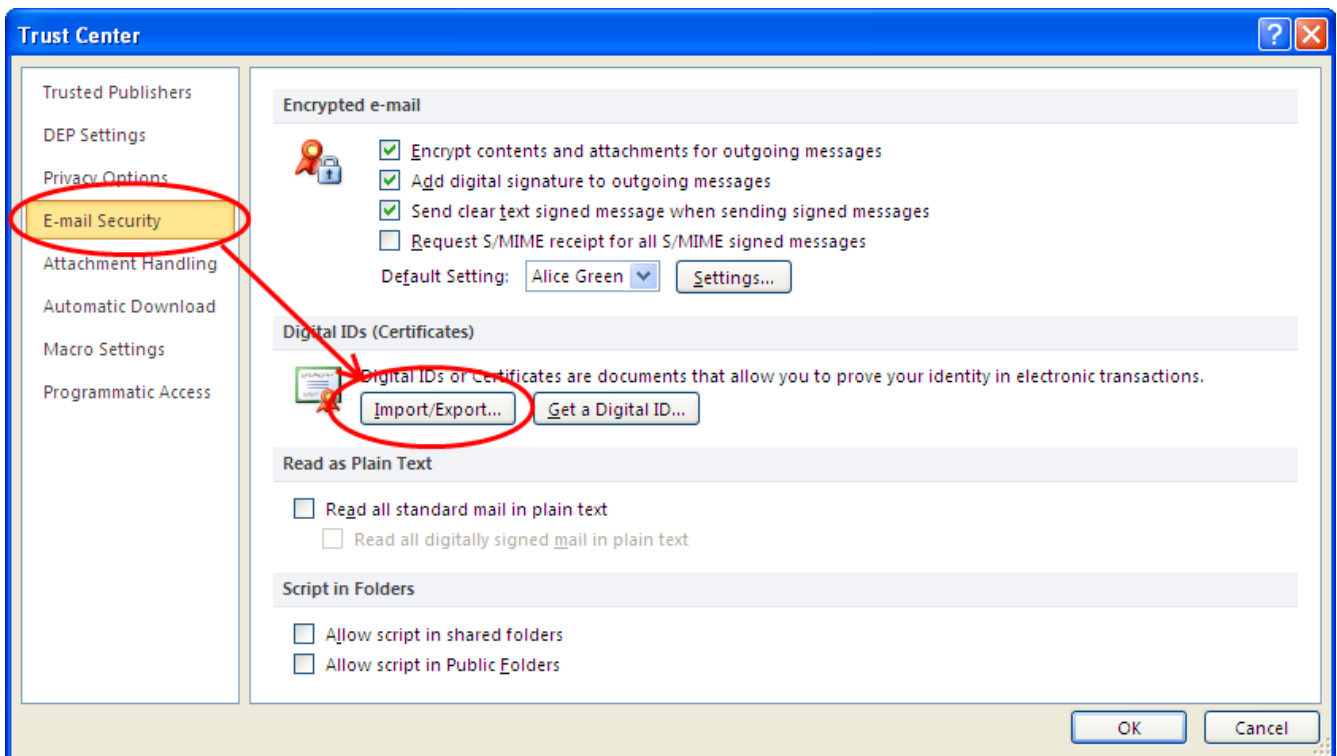
- If you have originally downloaded the certificate on the same computer as your Outlook installation then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import' the certificate into Outlook installation by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section 'Enrollment and Collection of your Certificate' first.

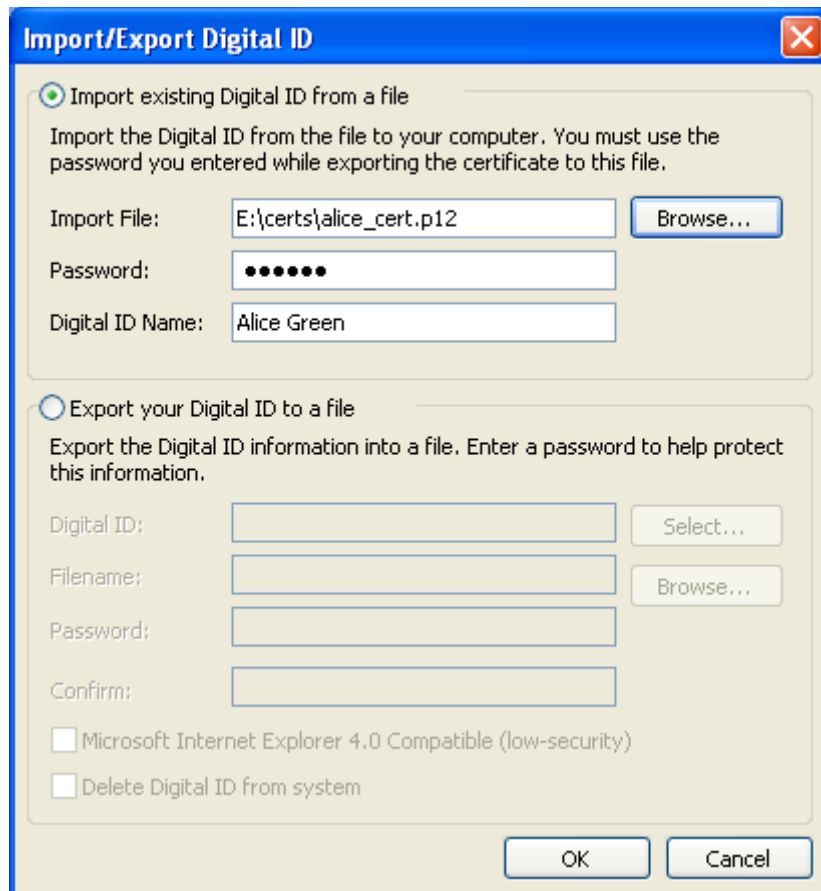
1. Open Outlook 2010, then click '**File**' > '**Options**'.
2. In the **Outlook Options** screen, click '**Trustcenter**' > '**Trustcenter Settings**'



3. In the **Trust Center** screen, select '**E-mail Security**' then click the '**Import/Export**' button..



In the Import/Export Digital ID interface, navigate to the location of your PKCS12 certificate file and click '**Open**'. Enter the password that was used while exporting the certificate and provide a Digital ID name.



Import/Export Digital ID

Import existing Digital ID from a file

Import the Digital ID from the file to your computer. You must use the password you entered while exporting the certificate to this file.

Import File:

Password:

Digital ID Name:

Export your Digital ID to a file

Export the Digital ID information into a file. Enter a password to help protect this information.

Digital ID:

Filename:

Password:

Confirm:

Microsoft Internet Explorer 4.0 Compatible (low-security)

Delete Digital ID from system

4. Click '**OK**'.



Importing a new private exchange key

An application is creating a Protected item.



CryptoAPI Private Key

Security level set to Medium

5. Select the security level for storing the Private Key in your system and click **OK**.

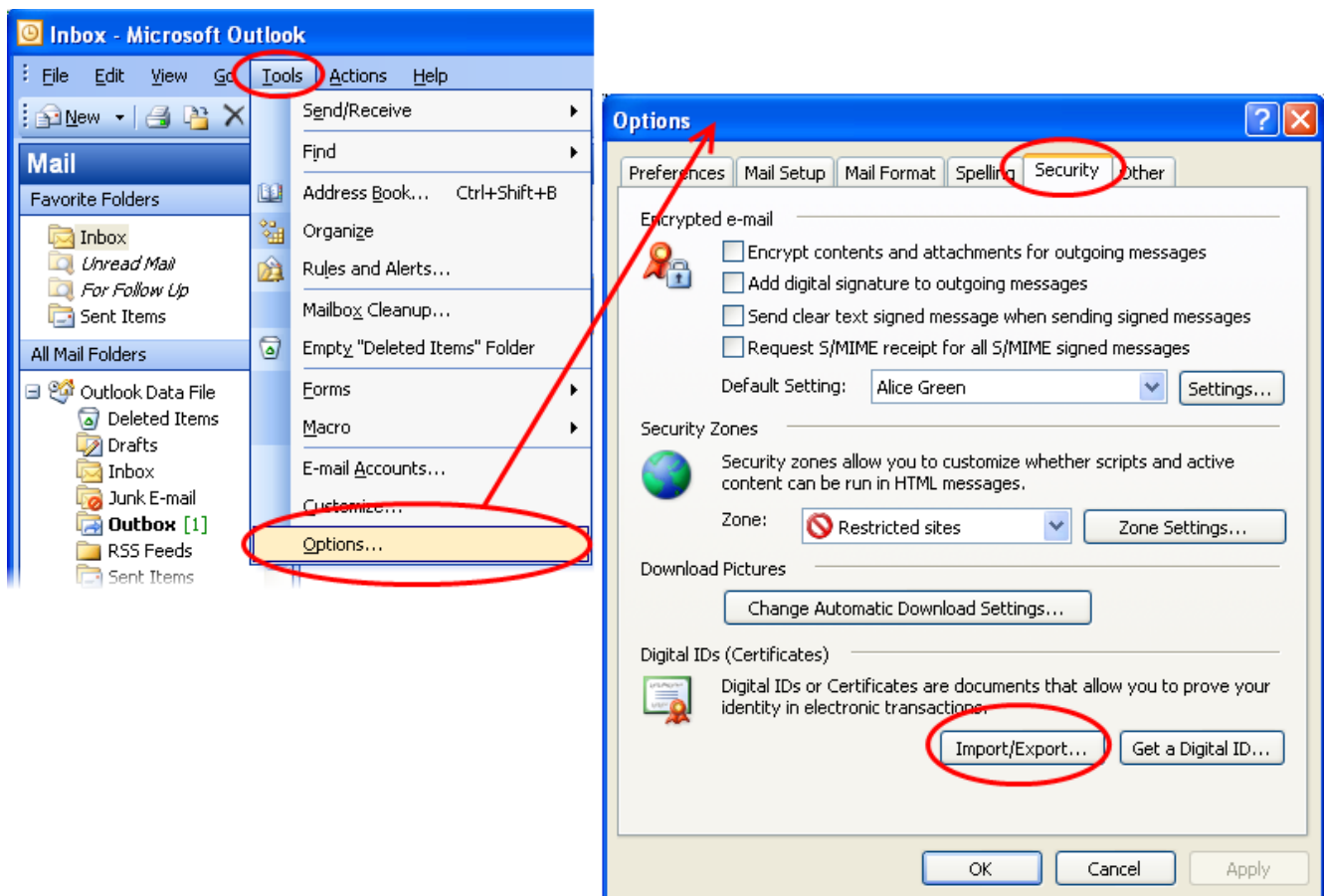
That's it. You have successfully imported your digital certificate into Outlook 2010 / 2013.

Importing Your Certificate into Outlook 2003

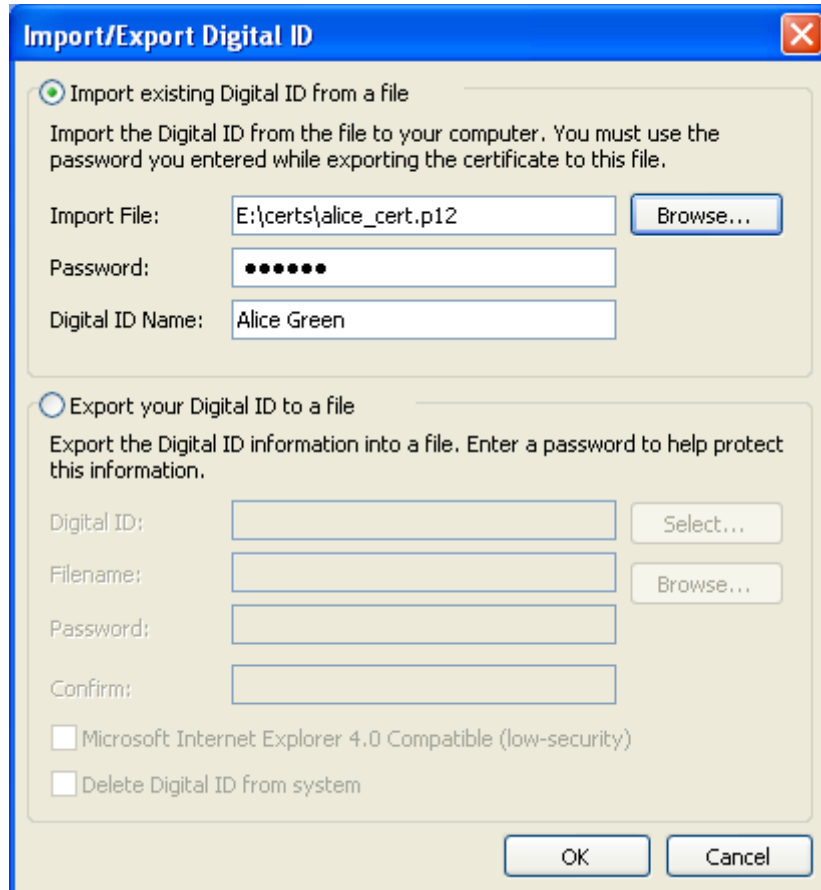
- If you have originally downloaded the certificate on the same computer as your Outlook installation then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Outlook installation by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

1. Open Outlook 2003, then click '**Tools**' > '**Options...**'.
2. In the **Options** screen, click '**Security**' > '**Import/Export...**'



3. In the Import/Export Digital ID interface, navigate to the location of your PKCS12 certificate file and click '**Open**'. Enter the password that was used while exporting the certificate and provide a Digital ID name.



4. Click 'OK'.



5. Select the security level for storing the Private Key in your system and click **OK**.


6. Click '**Apply**' and then '**OK**' in the Options screen.

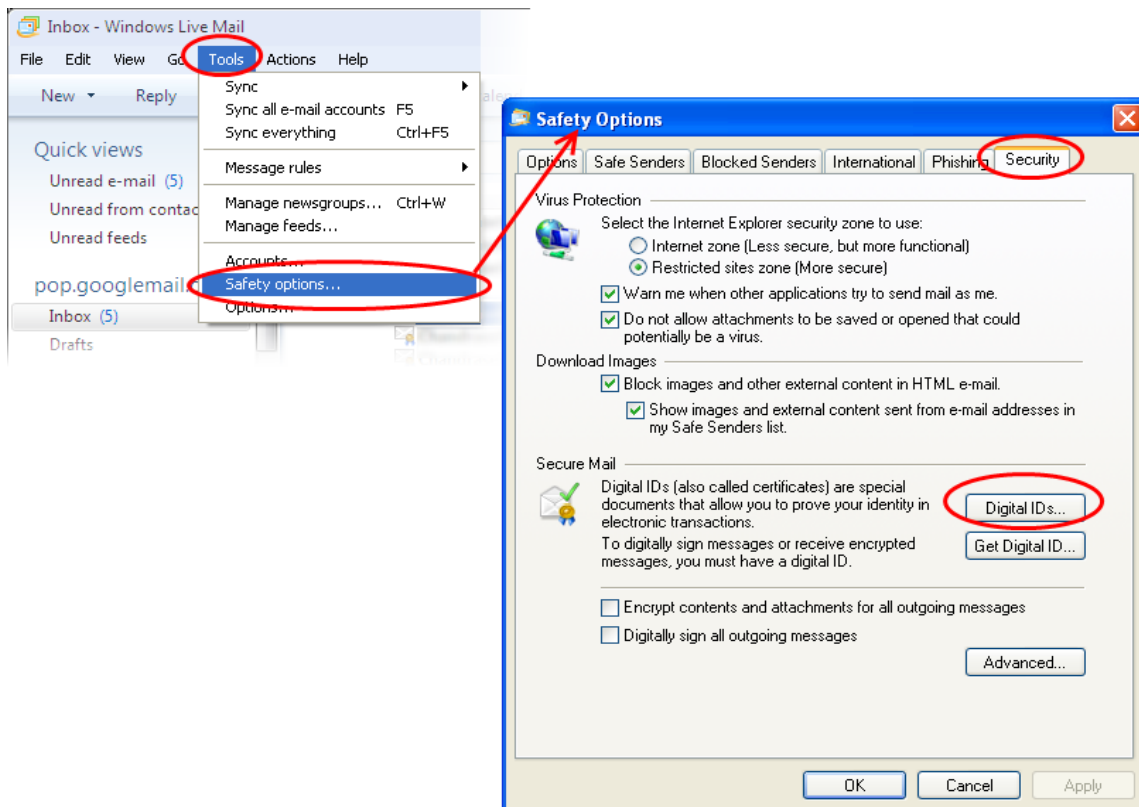
That's it. You have successfully imported your digital certificate into Outlook 2003.

Importing Your Certificate into Windows Live Mail

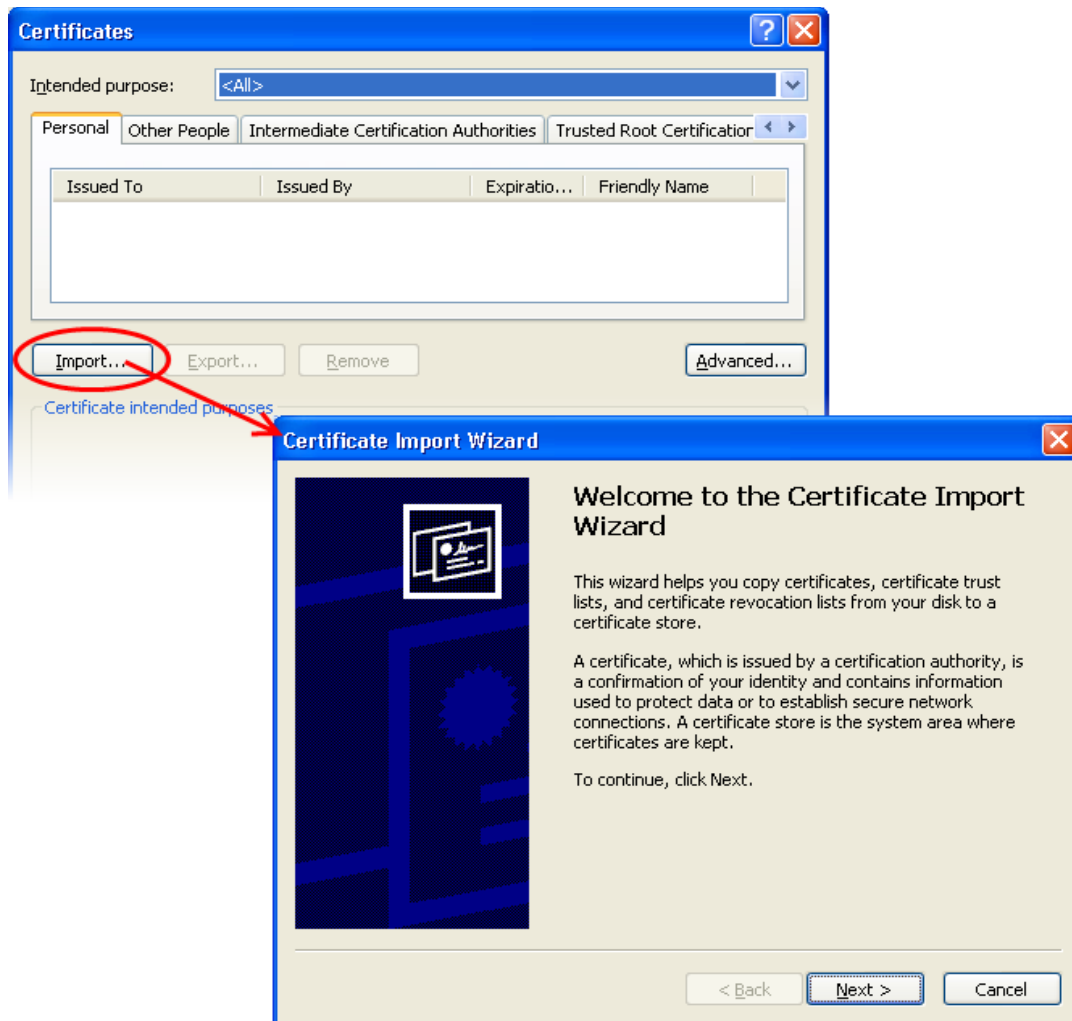
- If you have originally downloaded the certificate on the same computer as your Windows Live Mail installation then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Outlook installation by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

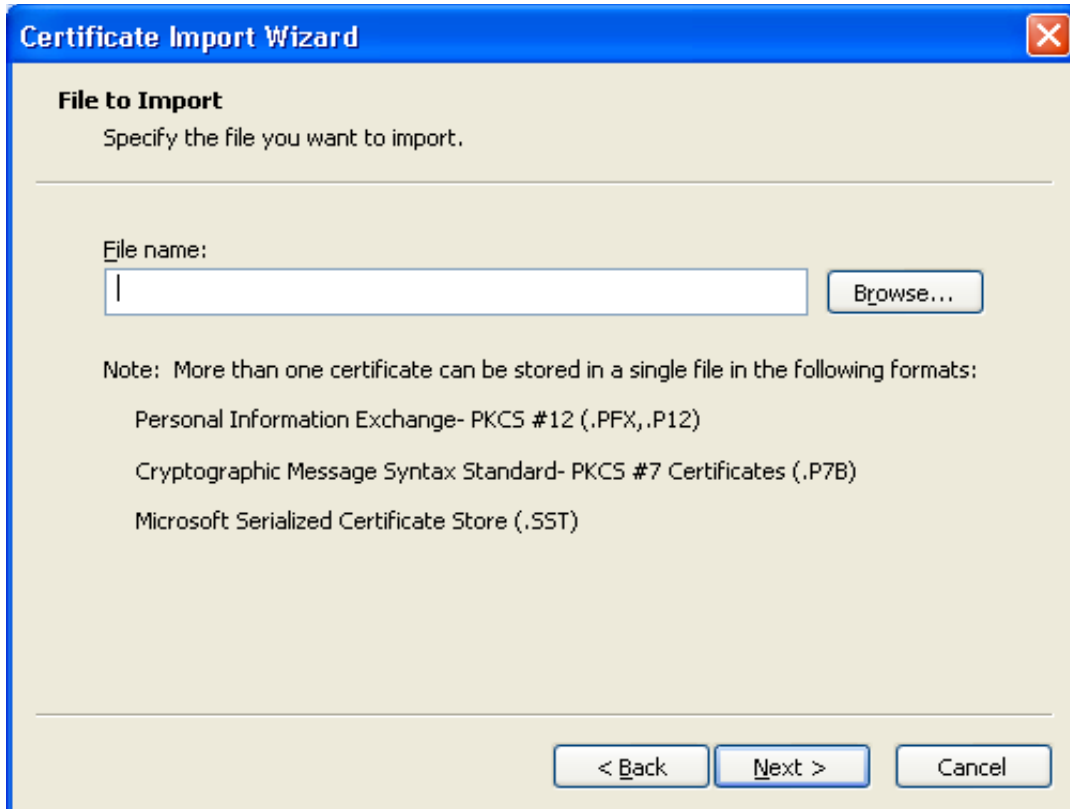
1. Open Windows Live Mail and click '**Tools**' > '**Safety Options...**'. (If the menu bar is not displayed, click on the Menu icon  in the tool bar and choose **Show menu bar** from the drop-down.)
2. Select the '**Security**' tab and then click the '**Digital IDs**' button.



3. In the Certificates interface, make sure the '**Personal**' tab is selected, click '**Import**' and then click '**Next**'.



4. Click '**Browse**' in the next step and navigate to the location of your PKCS12 certificate file.



Certificate Import Wizard

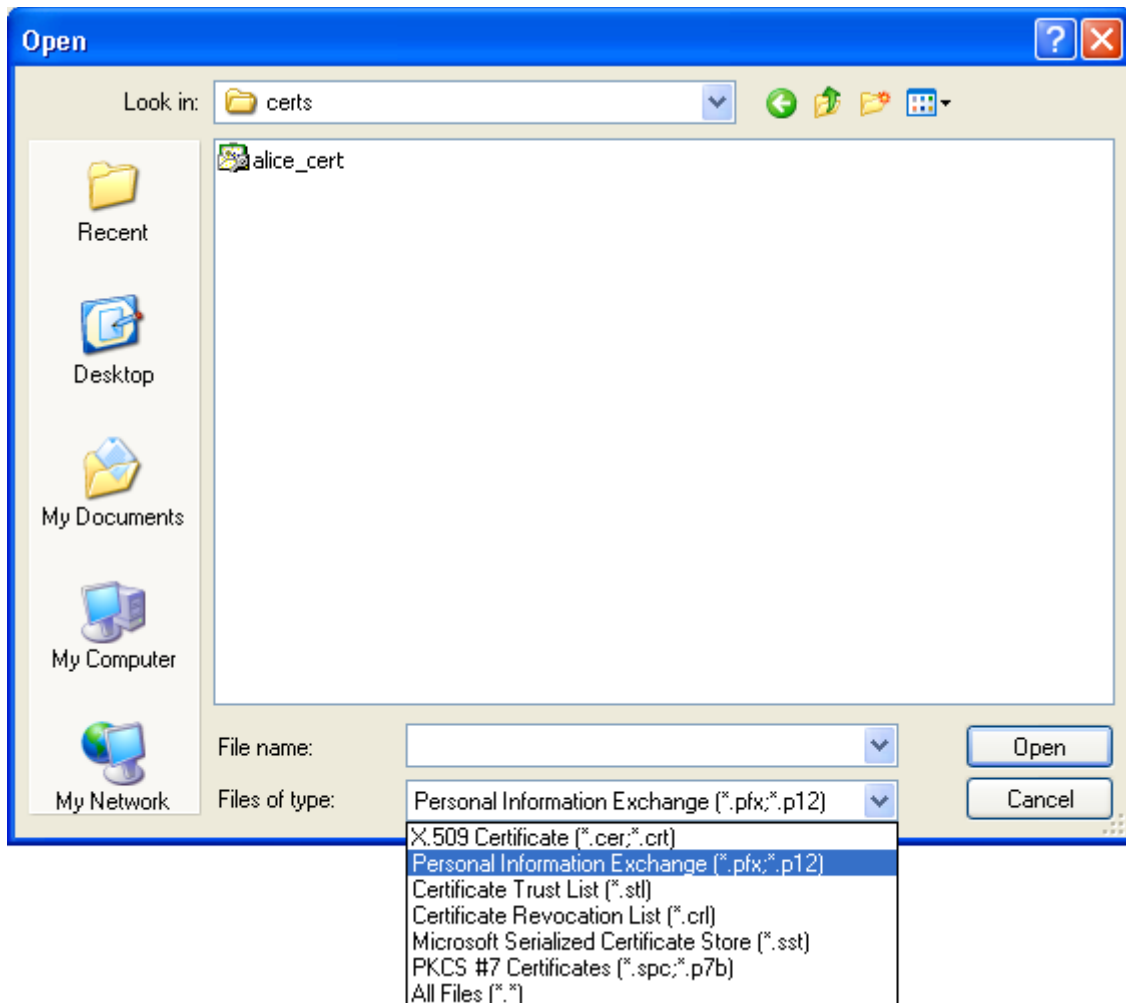
File to Import
Specify the file you want to import.

File name:

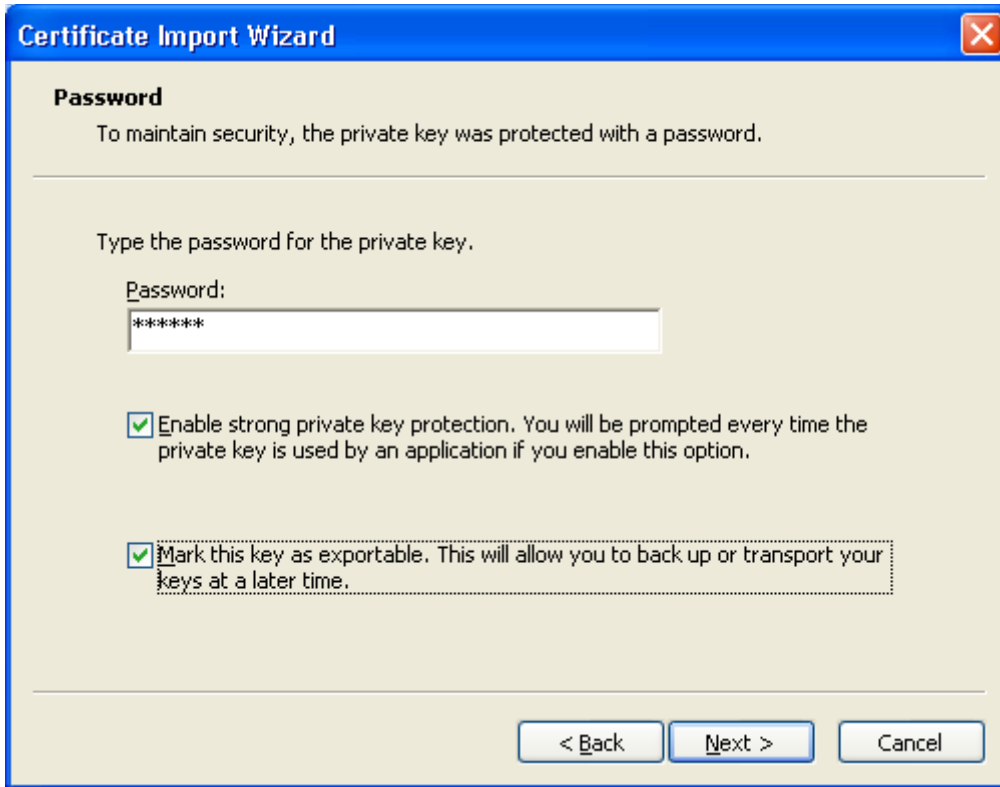
Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

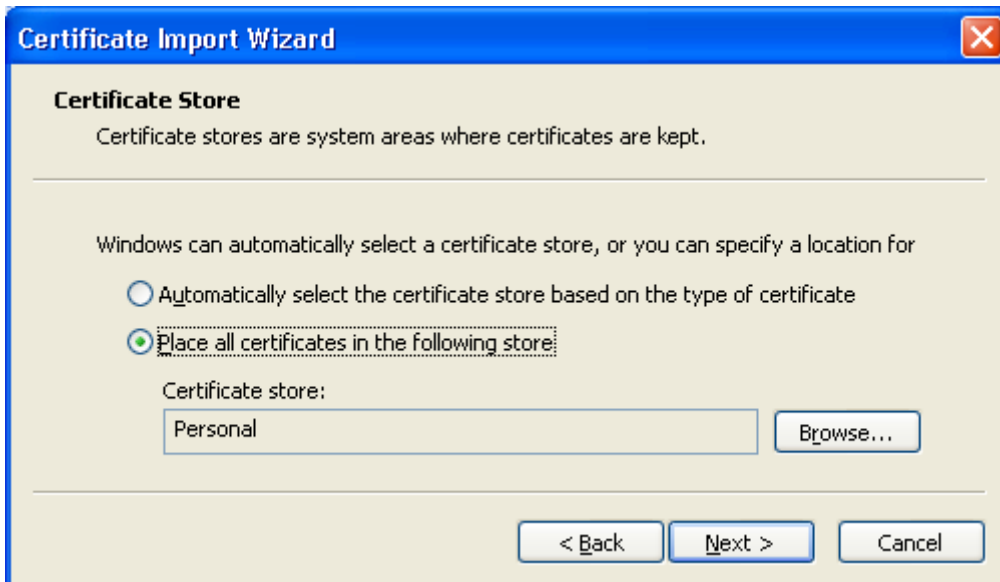
5. Now you need to change type of the file, select '**Personal Information Exchange (.p12)**' from the drop down box, locate your certificate file (.p12) and click '**Open**' (see below).



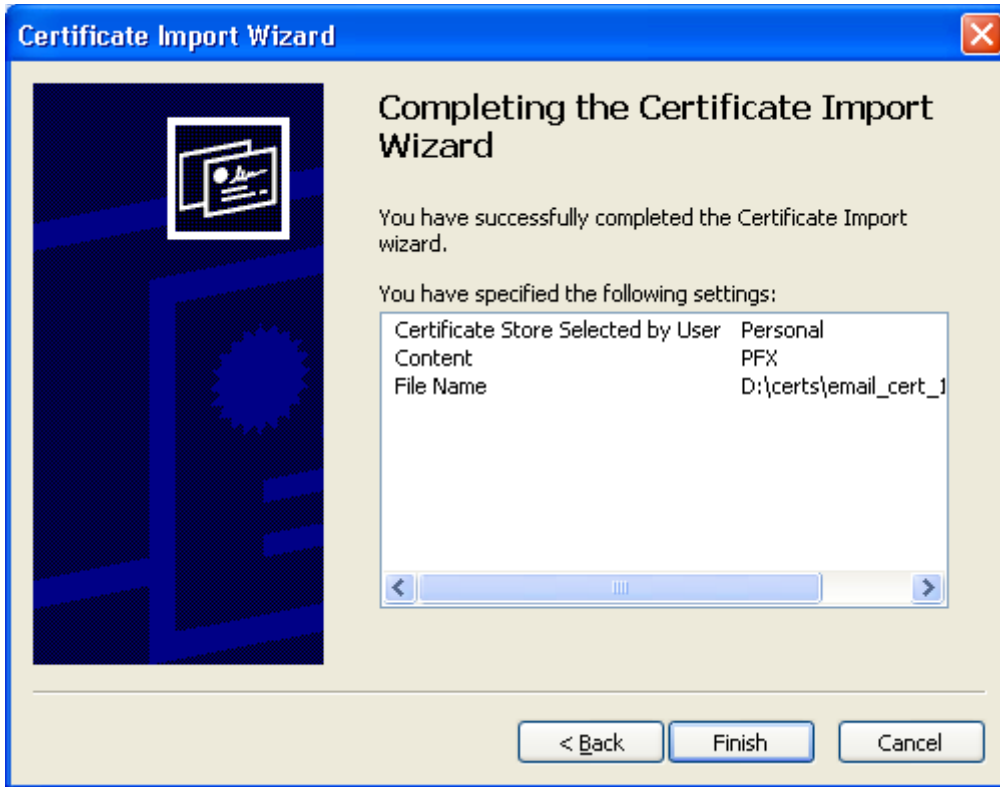
6. Click **Next**. To complete the installation process, you are required to enter the PIN (password) you set up for the certificate during the enrollment process. If you have forgotten your password, contact your system administrator who will be able to reset it for you.



- 7. Click **Next**. You will be prompted to choose the certificate store for your certificate. Unless your administrator has specified otherwise, you should leave this at the default **Place all certificates in the following store** option.



- 8. Click **'Next'**.



9. The last step: completing the **Certificate Import Wizard**.
10. Click **Finish** to complete the process. The certificate will be imported.
11. Select the security level for storing the Private Key in your system and click **OK**.



That's it. You have successfully imported your digital certificate into your Windows Live Mail.

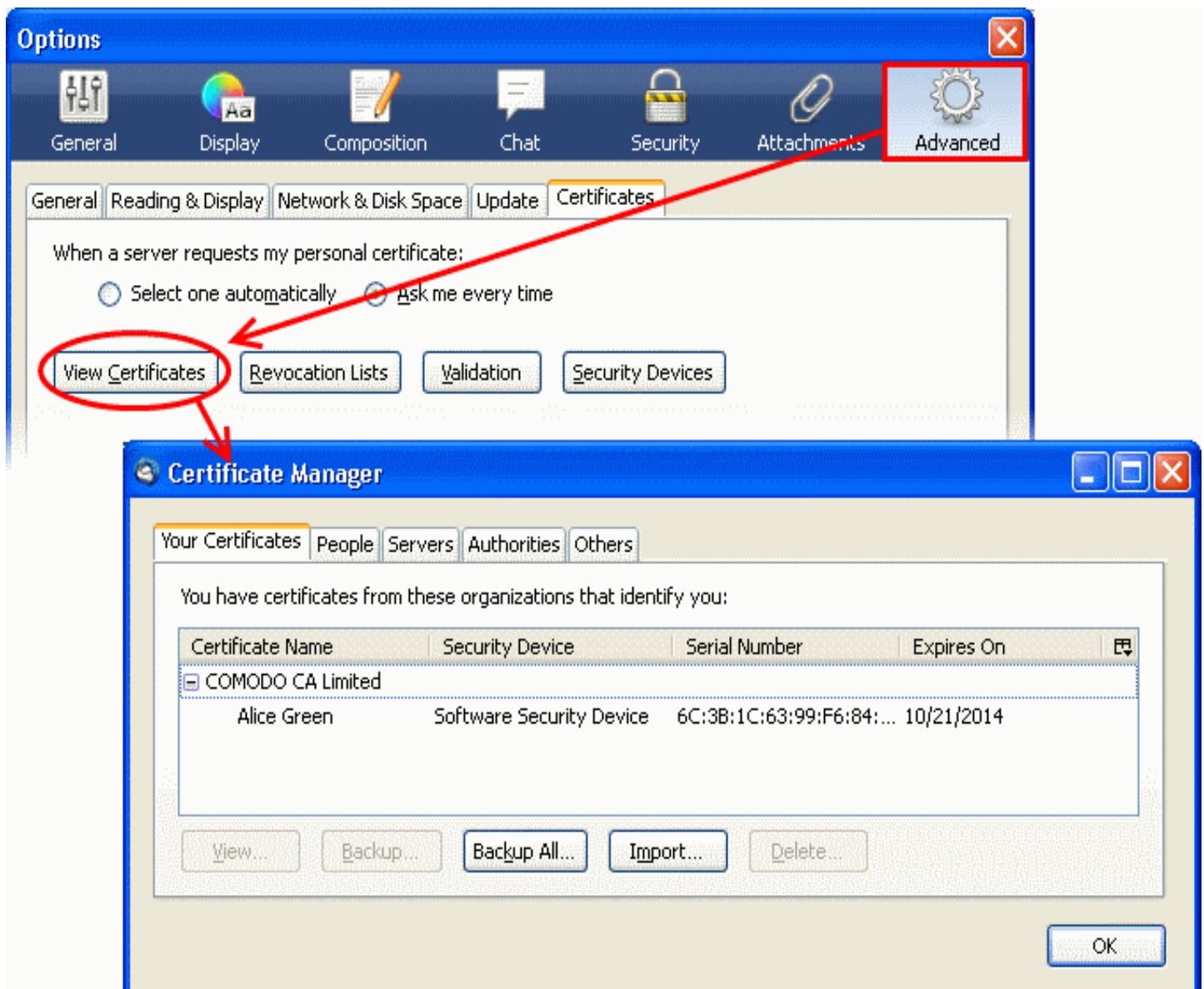
Importing Your Certificate into Mozilla Thunderbird

- If you have originally downloaded the certificate through Mozilla Thunderbird on the same computer then it should have been already installed.

- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Thunderbird installation by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

1. Open Thunderbird and then click '**Tools**' > '**Options**' > '**Advanced**'.
2. Click the '**Certificates**' tab
 - Optional - select **Ask me every time** under **When a server requests my personal certificate**.
 - Doing this alerts you to the fact that a server has requested identity confirmation and enables you to select your Client Certificate.
3. Click the '**View Certificates**' button.
4. In the certificate manager interface, make sure the '**Your Certificates**' tab is selected and click '**Import**'.



5. Navigate to the location of your PKCS12 certificate file and enter any necessary passwords. Once complete the certificate will appear and you will be able to digitally sign and encrypt e-mails.
6. Click '**OK**' to Thunderbird.

That's it. You have successfully imported your digital certificate into Mozilla Thunderbird.

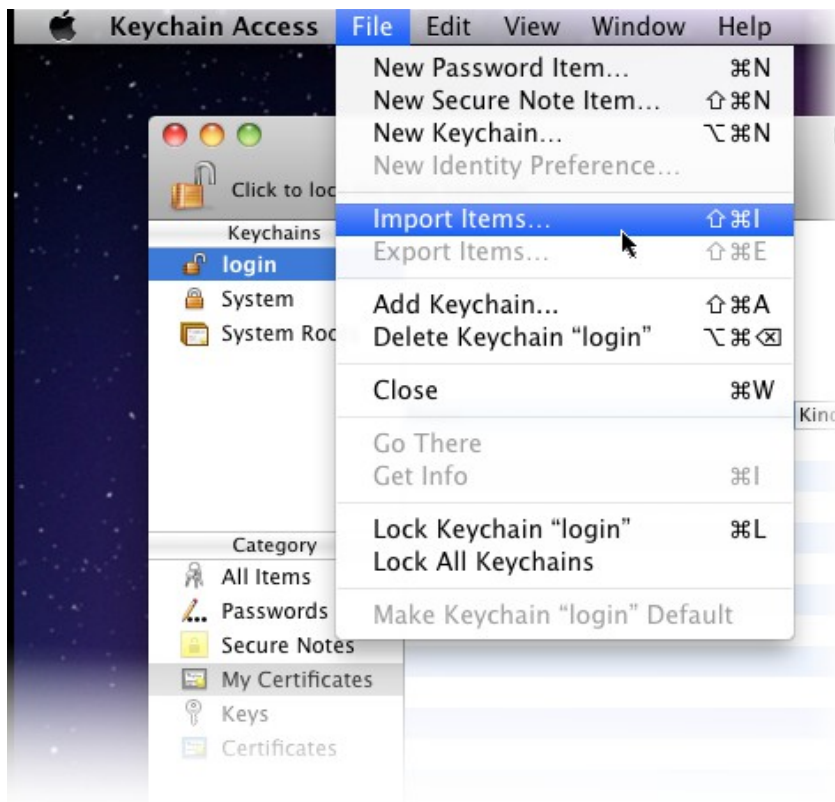
Importing Your Certificate into Mac OS X Mail / Apple Mail

- If you have originally downloaded the certificate through the Mac Mail/Apple Mail installation on the Mac OS computer then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Mac Mail/Apple Mail installation by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

Apple Mac OS uses the Keychain Access Utility to manage digital certificates.

1. Click '**Applications**' > '**Utilities**' > '**Keychain Access**'
2. Select '**Login**' from left side and click '**File**' > '**Import Items...**'

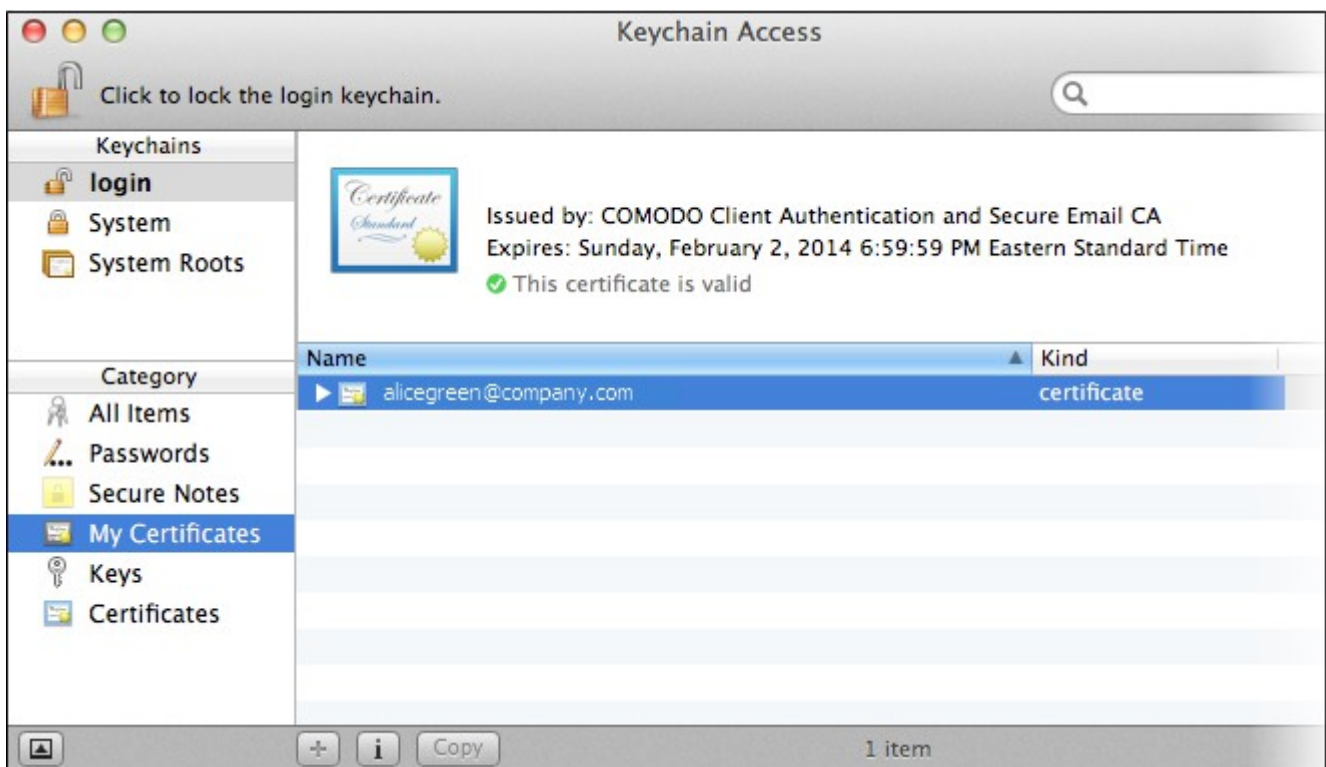


3. Navigate to the location of your PKCS12 certificate file and click 'Open'.



4. Enter the key pair's password and click 'OK'. Note: If prompted whether to trust certificates issued by your CA automatically, select Always Trust option to trust and install your certificate.

The certificate will be installed and can be viewed by clicking **Category > My Certificates** in the Keychain Access interface.



Once installed the certificate will be available for digitally signing and encrypting your emails through Mac Mail and Apple Mail and for authenticating yourself to the websites that require certificate authentication.

Importing Your Certificate into Eudora (PC)

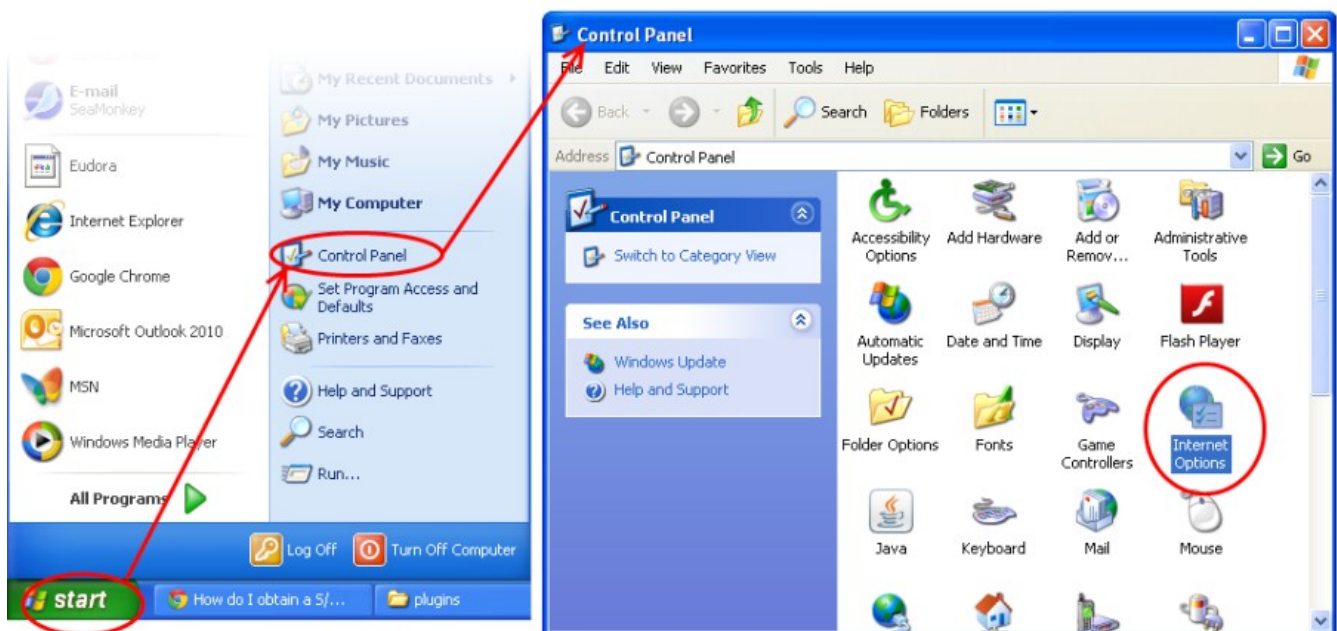
- If you have originally downloaded the certificate through the Eudora on the same computer then it should have been already installed.

- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Eudora installation by following the steps given below.

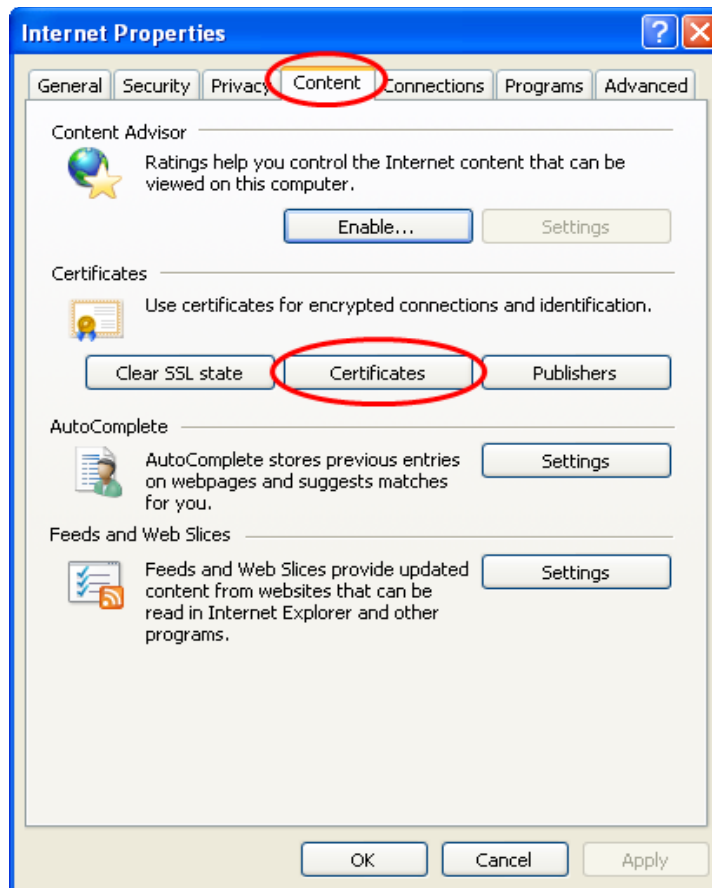
Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

The Eudora mail client itself does not manage digital certificates but uses the Windows certificate store instead.

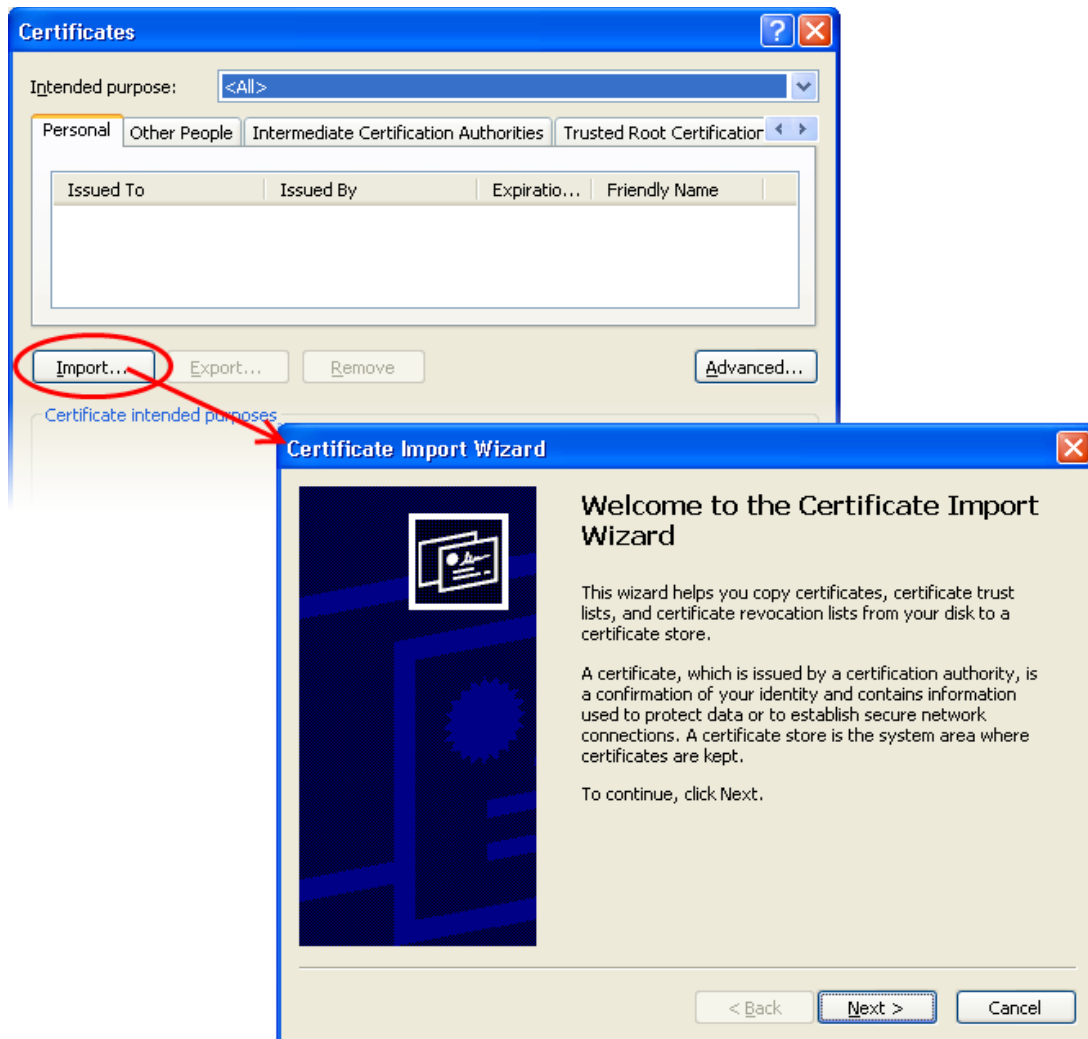
1. Click **Start > Control Panel > Internet Options**



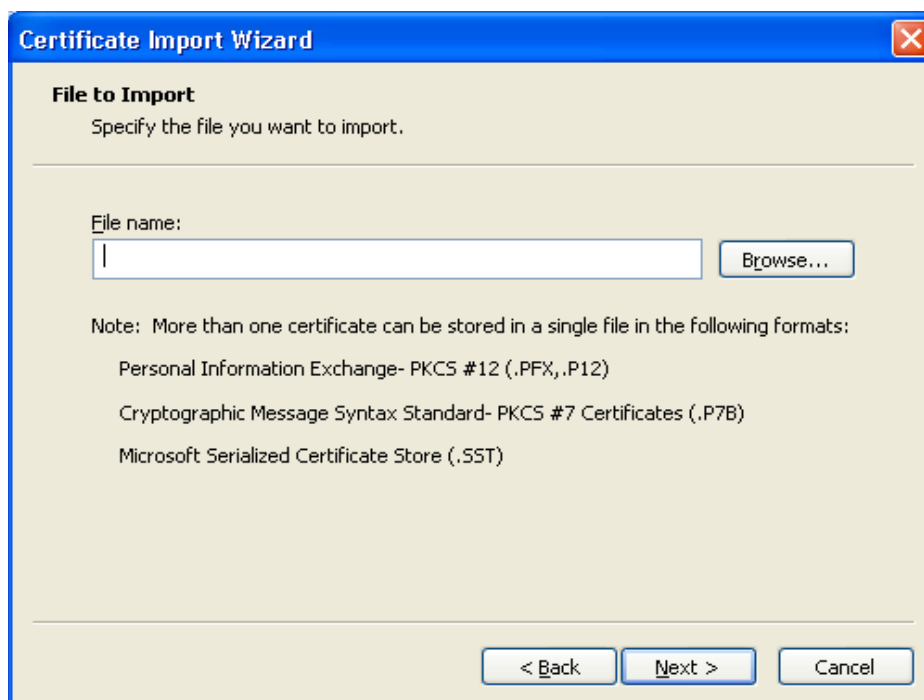
2. Select the '**Content**' tab and then click the '**Certificates**' button.



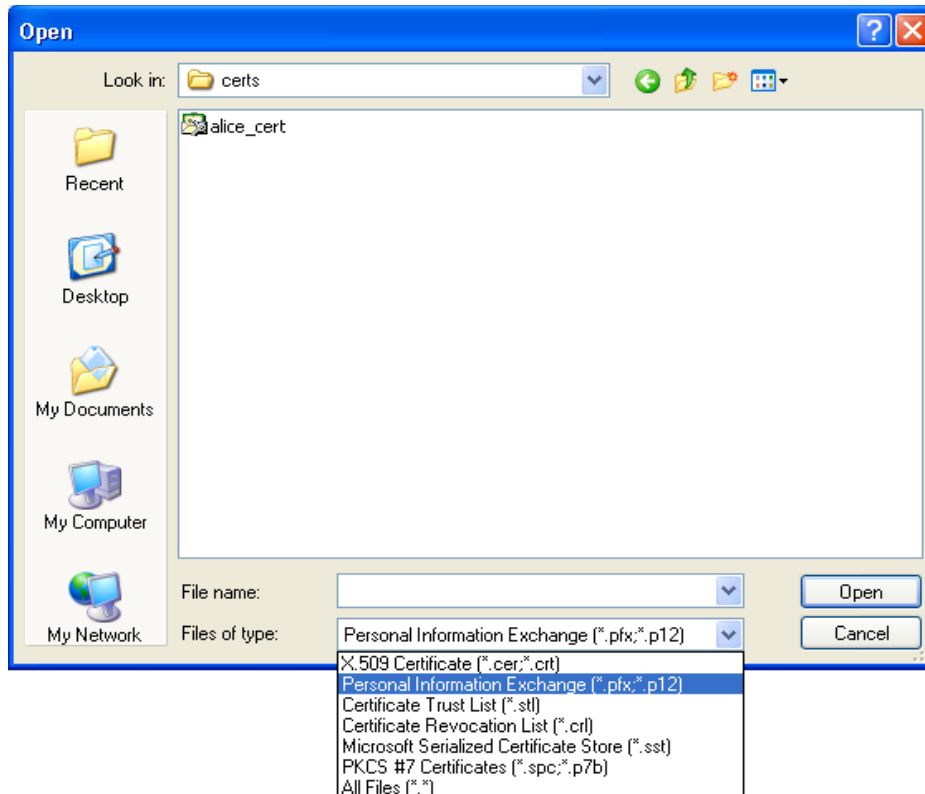
3. In the 'Certificates interface', make sure the '**Personal**' tab is selected, click '**Import**' and then click '**Next**'.



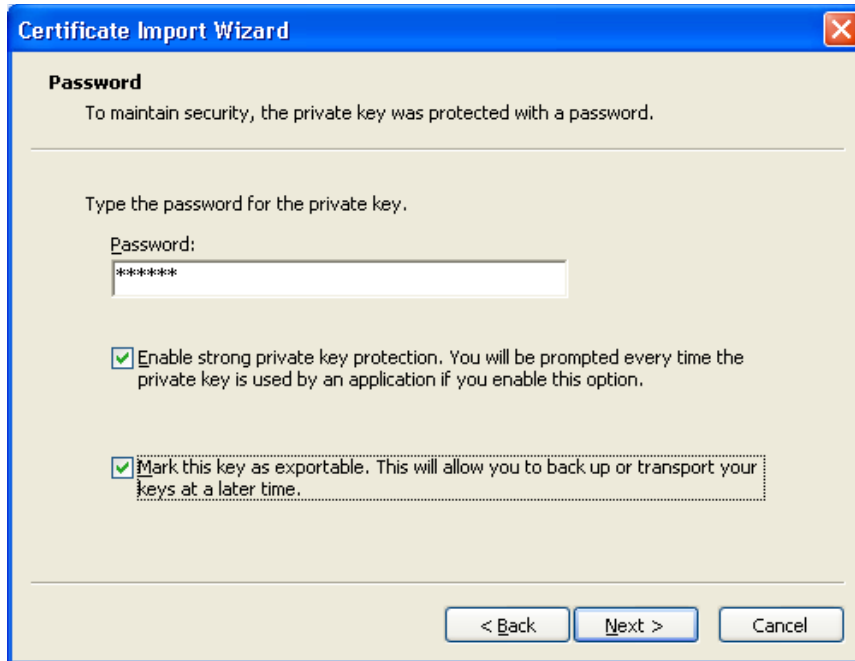
4. Click '**Browse**' in the next step and navigate to the location of your PKCS12 certificate file.



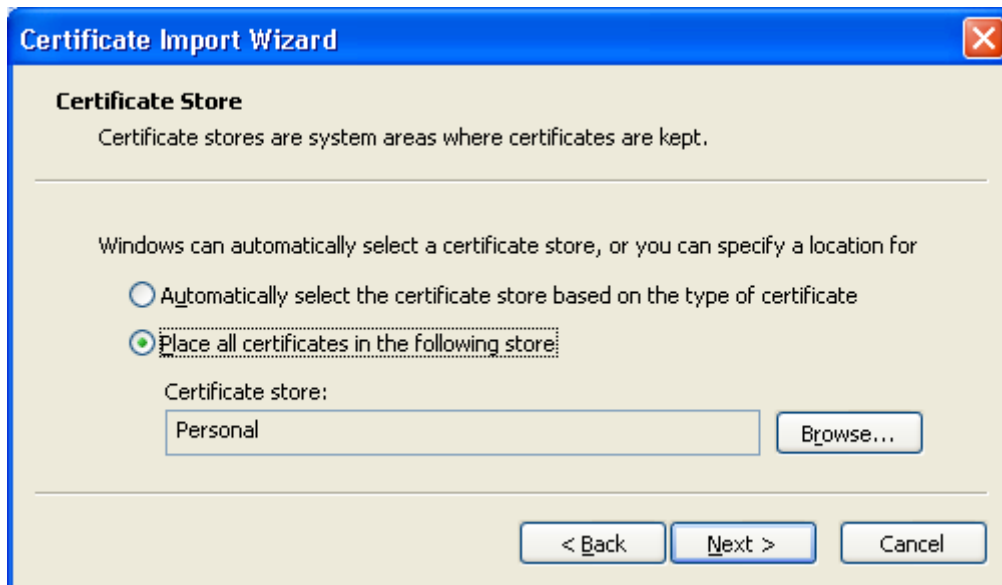
5. Now you need to change type of the file, select '**Personal Information Exchange (.p12)**' from the drop down box, locate your certificate file (.p12) and click '**Open**' (see below).



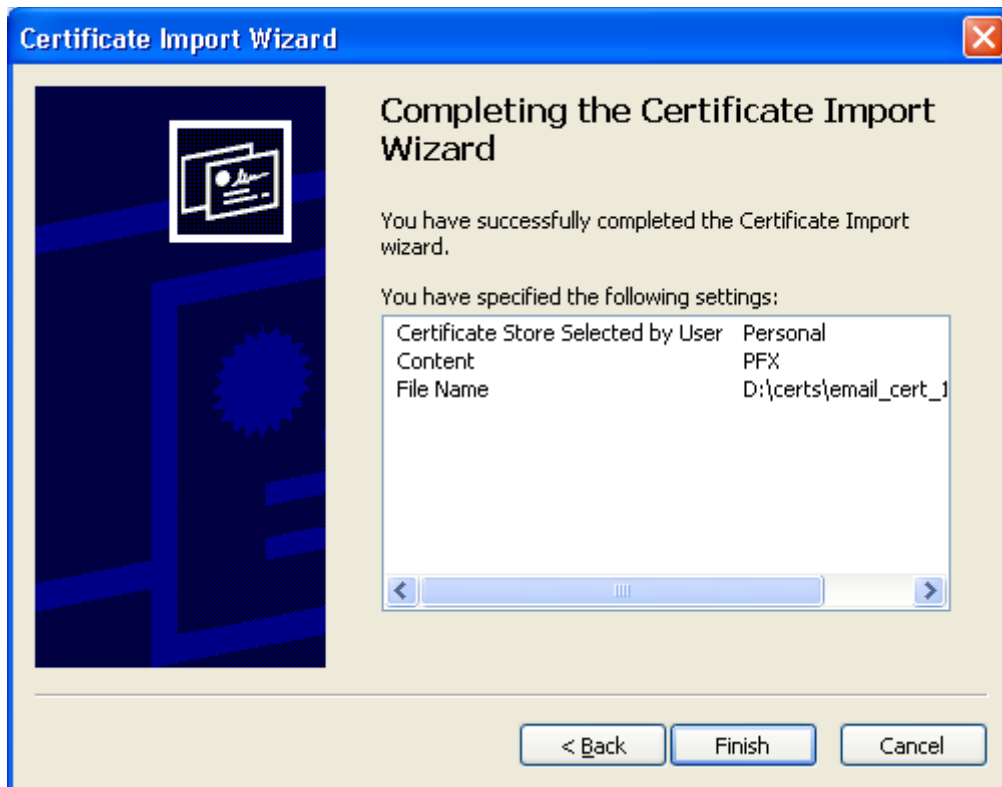
6. Click **Next**. To complete the installation process, you are required to enter the PIN (password) you set up for the certificate during the enrollment process. If you have forgotten your password, contact your system administrator who will be able to reset it for you.



- 7. Click **Next**. You will be prompted to choose the certificate store for your certificate. Unless your administrator has specified otherwise, you should leave this at the default **Place all certificates in the following store** option.



- 8. Click 'Next' to proceed to the the last step - completing the **Certificate Import Wizard**.



9. Review your settings and click **Finish** to import your certificate.

10. Select the security level for storing your private key and click **OK**.



That's it. You have successfully imported your digital certificate into Windows. You can now sign and encrypt mails in Eudora using this certificate.

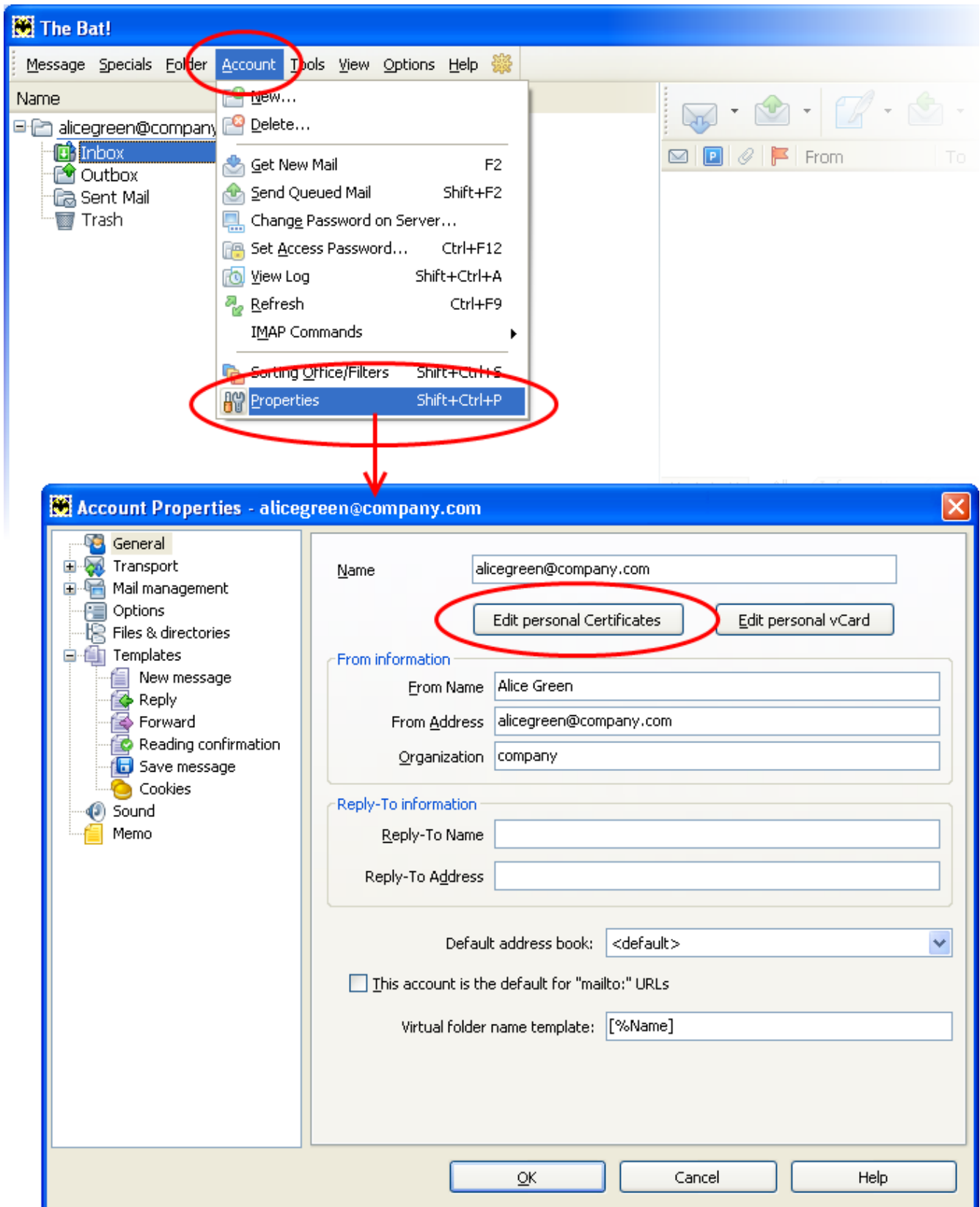
Importing Your Certificate into The Bat!

- If you have originally downloaded the certificate through Bat!, then it should have been already installed on the same computer

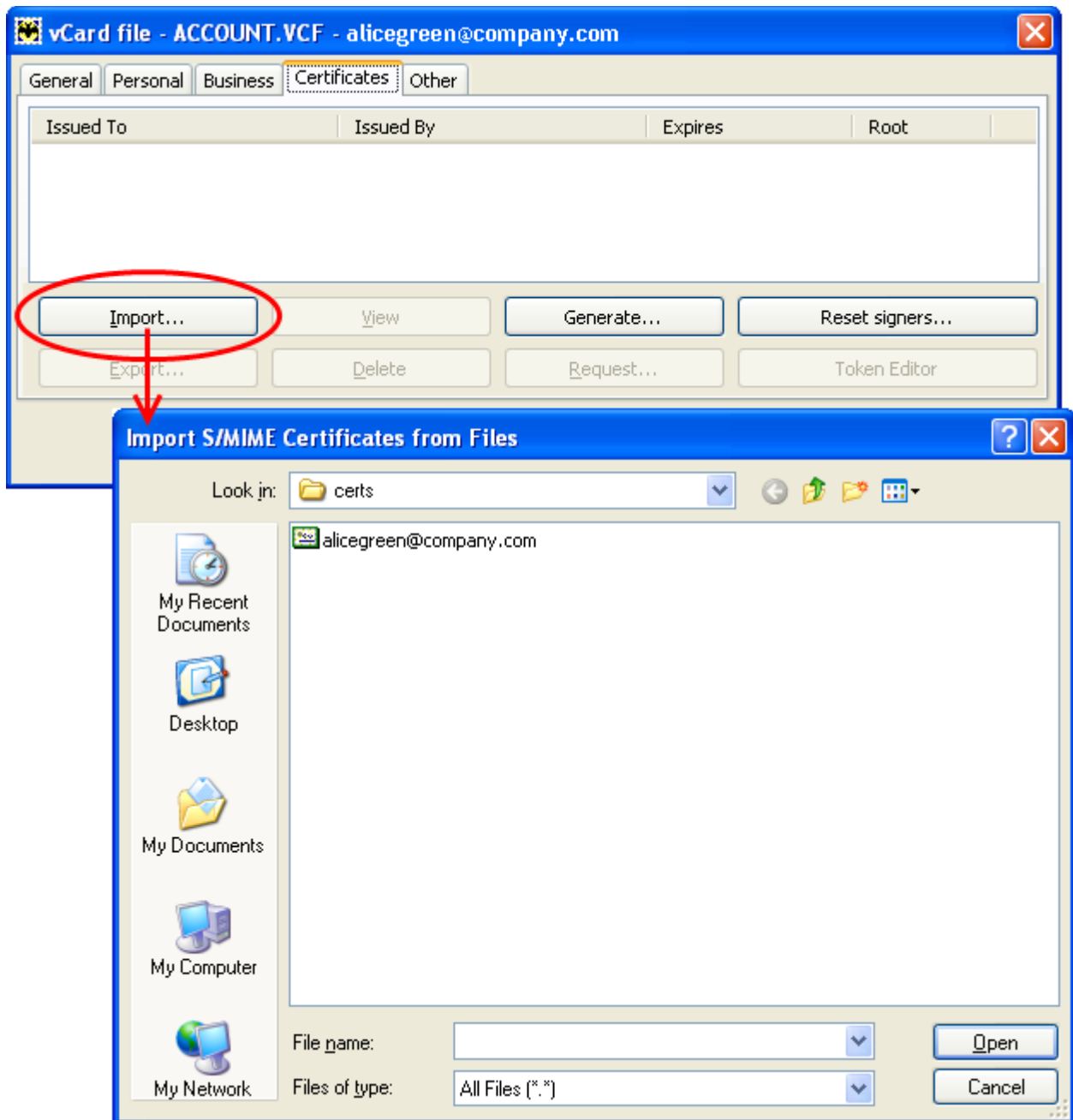
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Bat! installation by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

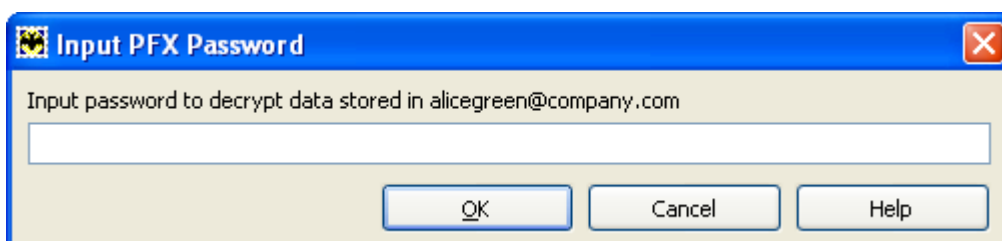
1. Open The Bat!, then click '**Account**' > '**Properties**'.
2. In the **Account Properties** screen, select **General** from the left hand nav and click the '**Edit personal Certificates**' button:



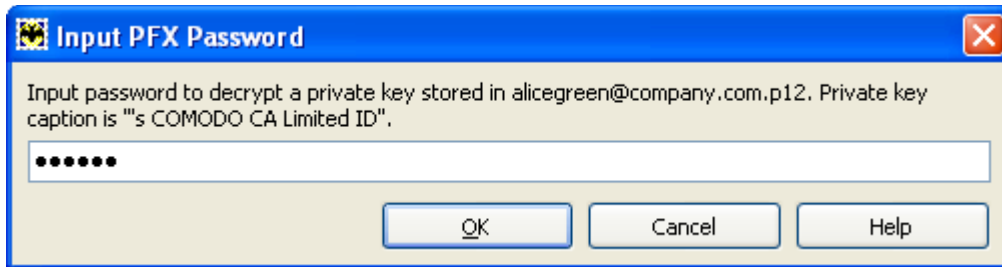
3. In the **ACCOUNT.VCF** screen, make sure the '**Certificates**' tab is selected and then click '**Import**':



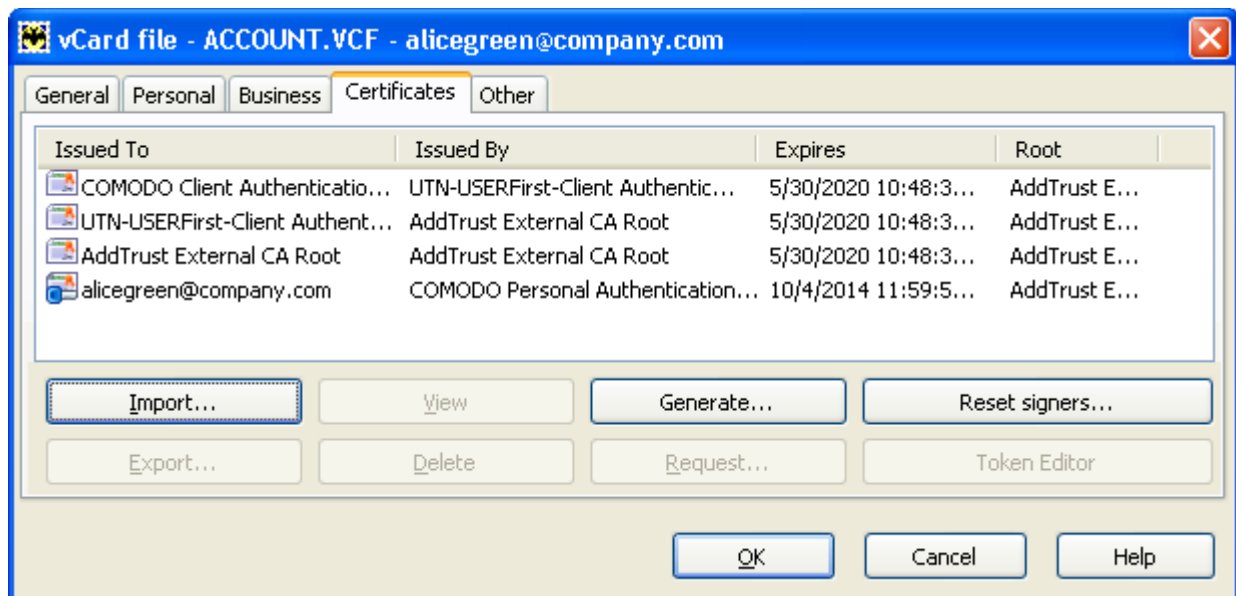
4. Navigate to the location of your InCommon Client Certificate file in .p12 format.
5. If this is the first time you have tried to import a certificate, then The Bat! will ask you to set a password for the certificate store. It will then request you enter this password every time you access the store (including this first time). You should choose a secure password that features both alphabetic and numeric characters. Please make a note of this password for future reference.



- To complete the import and the installation process, you are required to enter the PIN (password) that you set up while exporting/backup of the certificate.



- Click **OK** to finish the process. The certificate will be imported into The Bat! Certificate store and can be used for digitally signing emails.



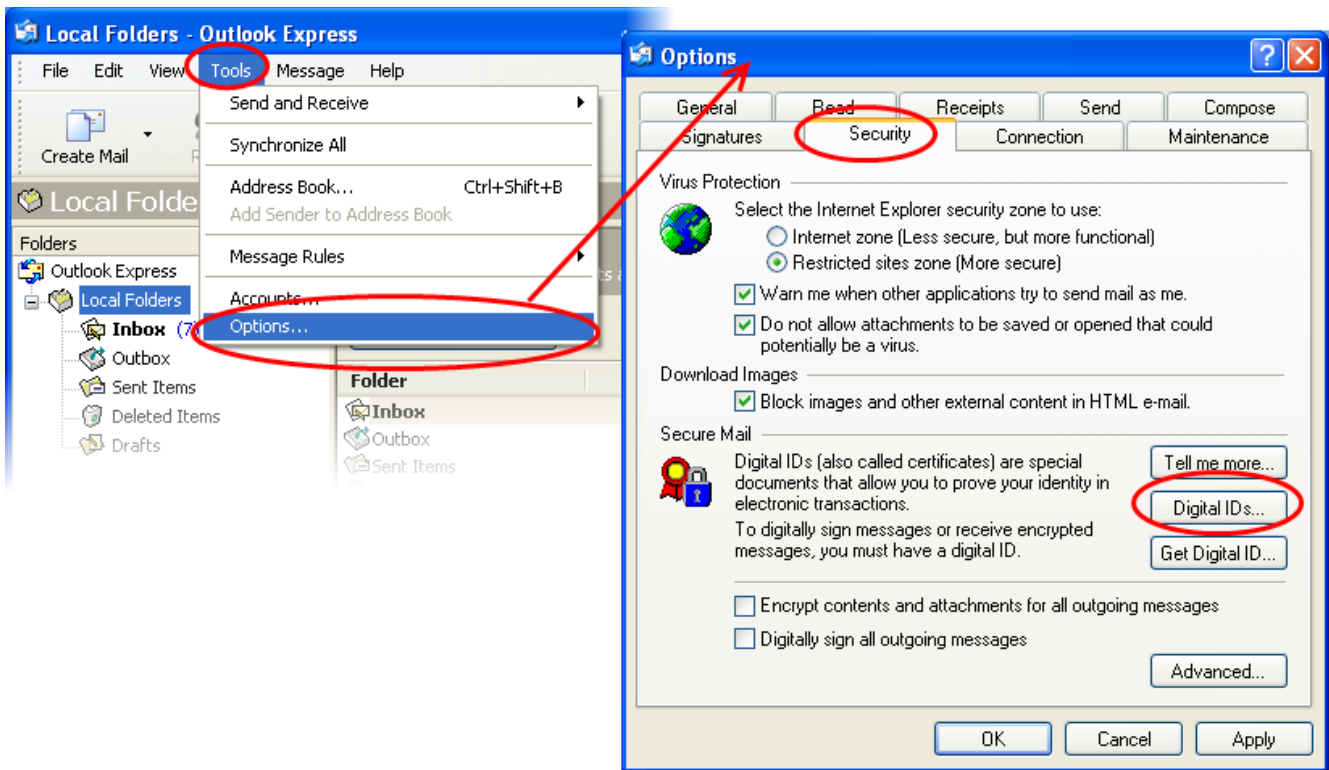
That's it. You have successfully imported your digital certificate into Windows. You can now sign and encrypt mails in Bat! using this certificate.

Importing Your Certificate into Outlook Express 5 & 6

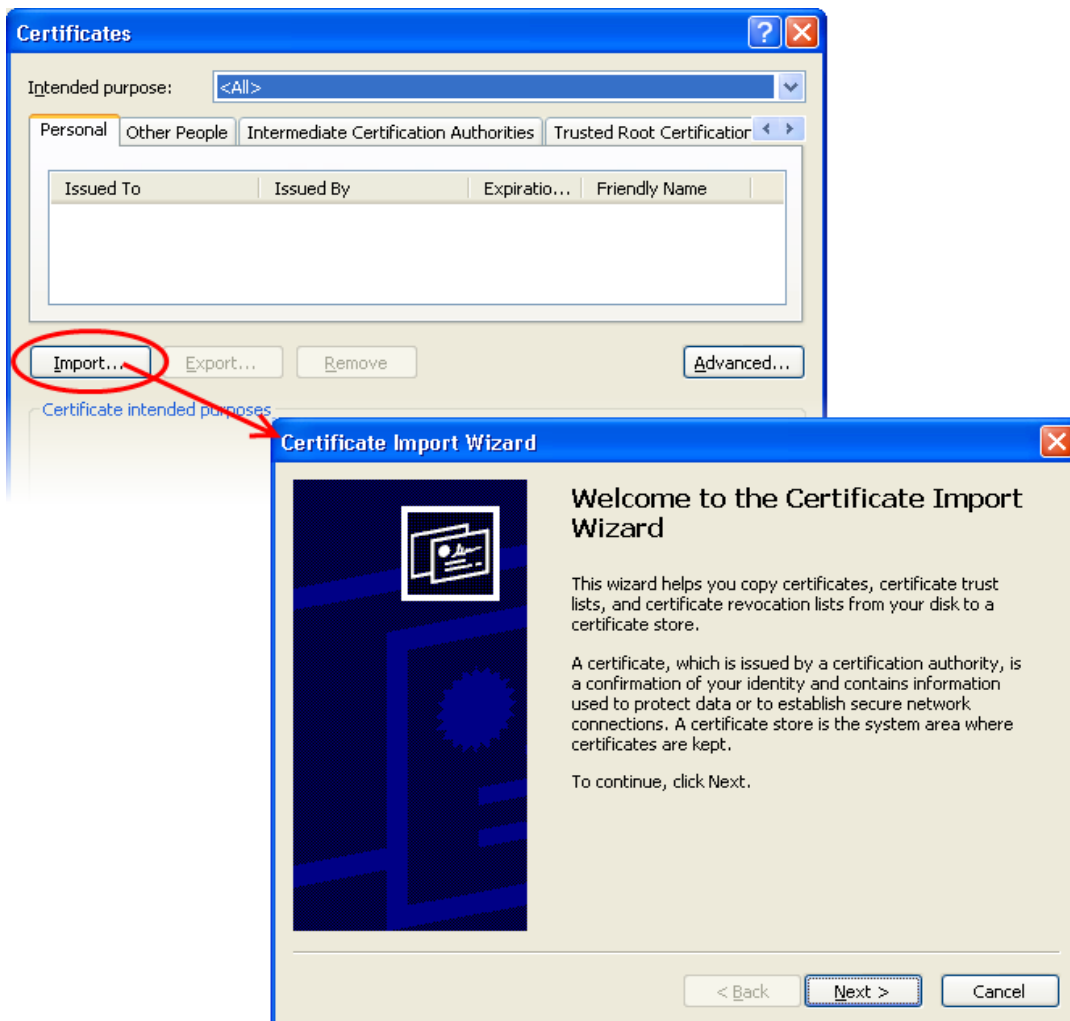
- If you have originally downloaded the certificate through Outlook Express, then it should have been already installed on the same computer
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import' the certificate into Outlook Express installation by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

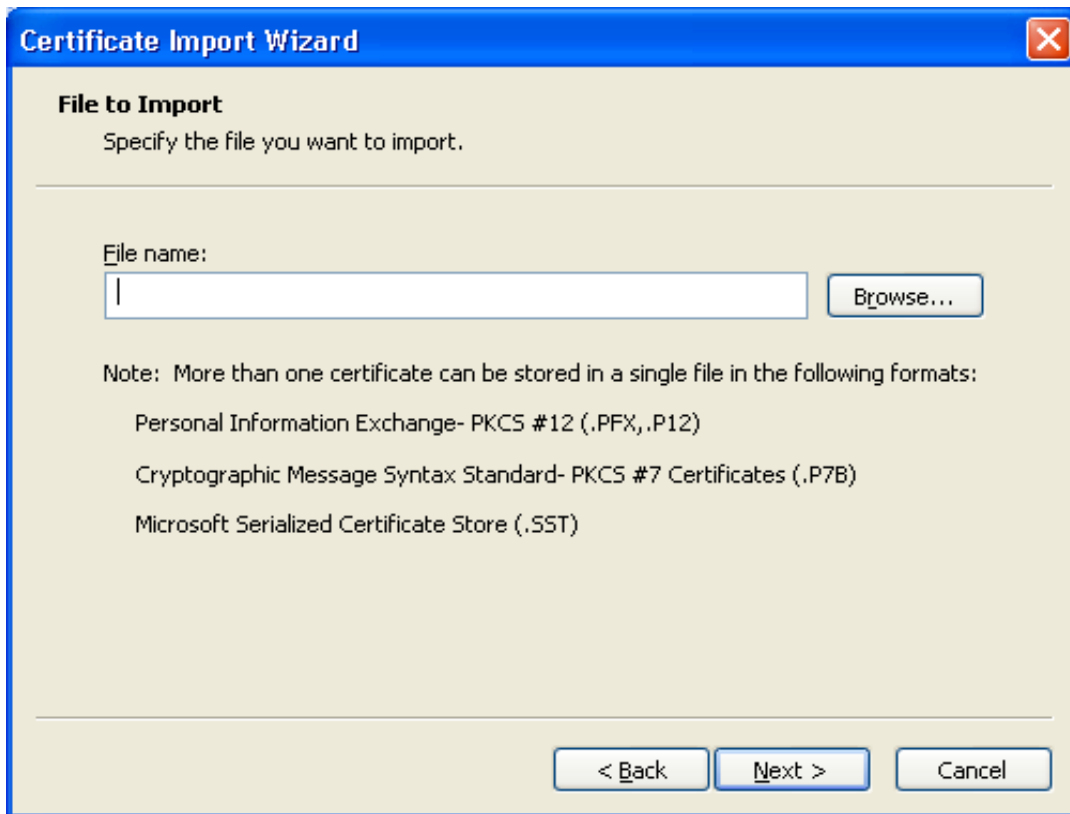
- Open Outlook Express and click '**Tools**' > '**Options**'.
- Select the '**Security**' tab and then click the '**Digital IDs**' button.



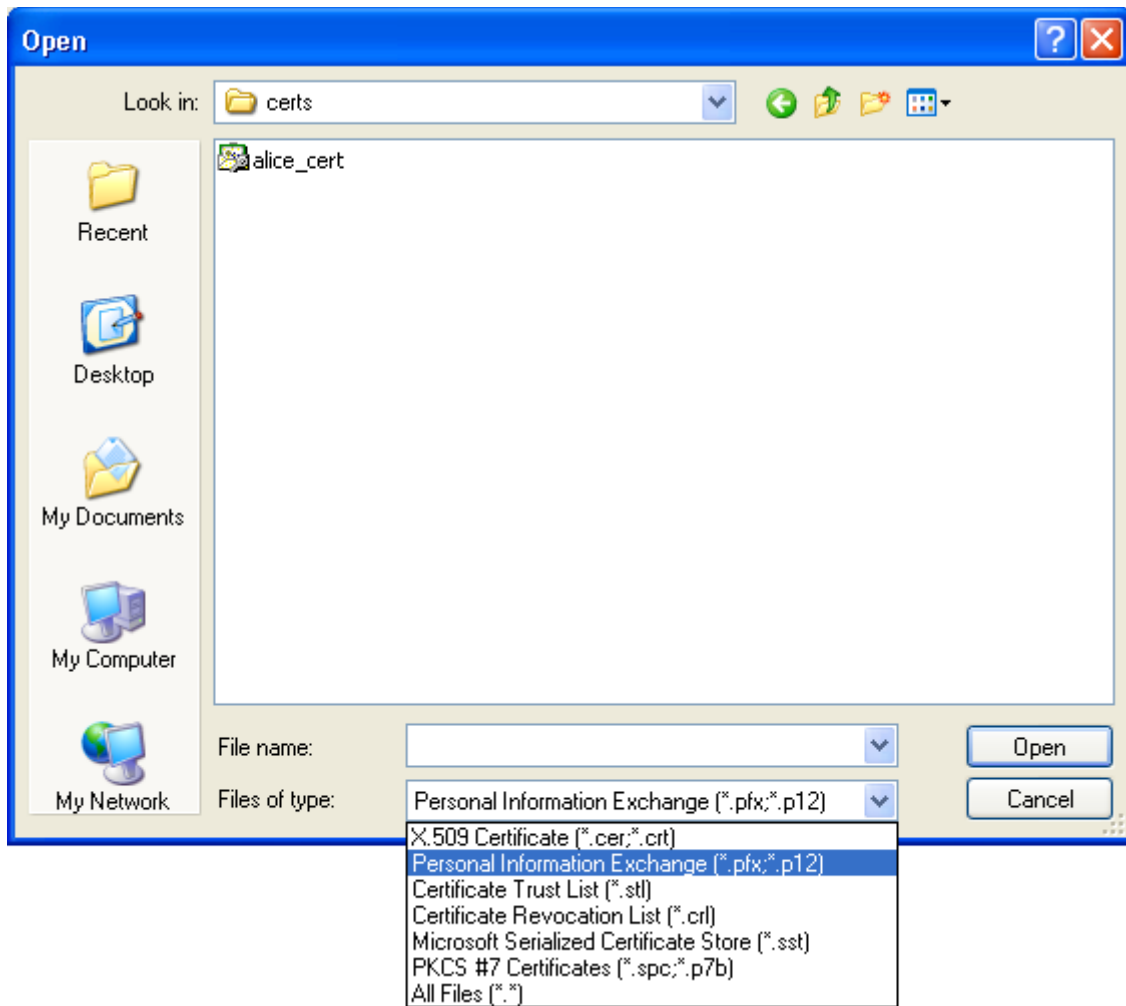
3. In the Certificates interface, make sure the 'Personal' tab is selected, click 'Import' and then click 'Next'.



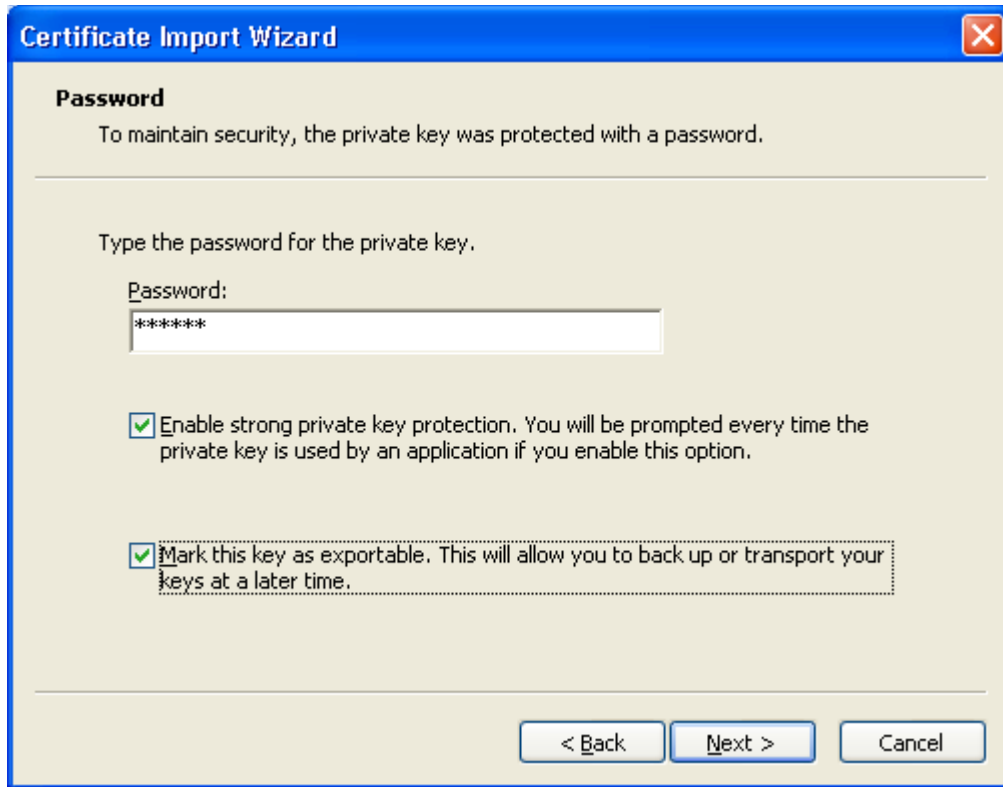
4. Click '**Browse**' in the next step and navigate to the location of your PKCS12 certificate file.



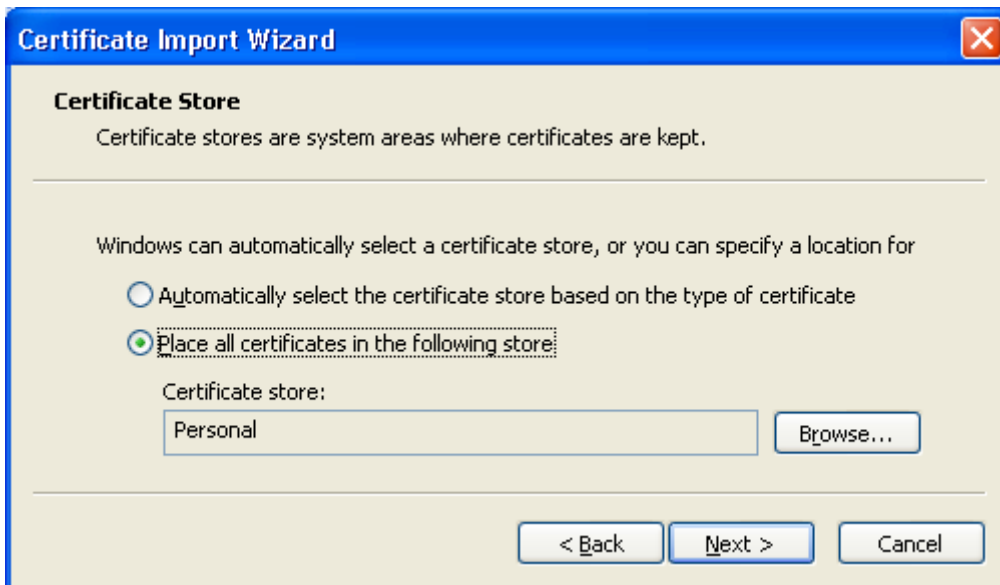
5. Now you need to change type of the file, select '**Personal Information Exchange (.p12)**' from the drop down box, locate your certificate file (.p12) and click '**Open**' (see below).



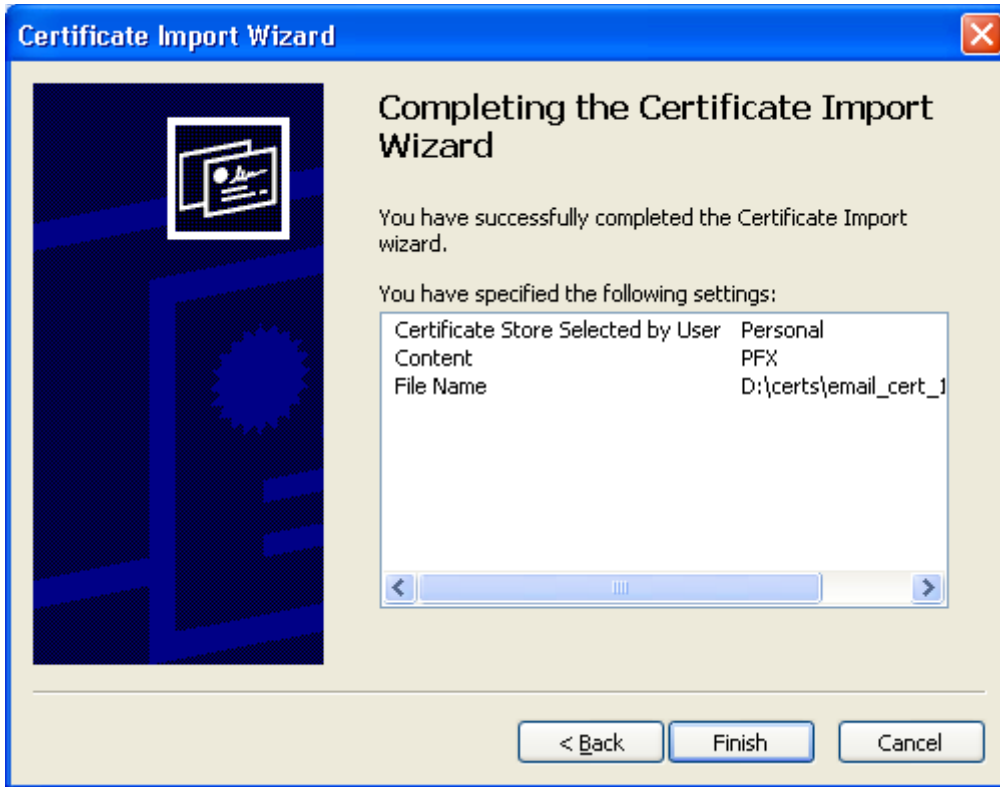
6. Click **Next**. To complete the installation process, you are required to enter the PIN (password) you set up for the certificate during the enrollment process. If you have forgotten your password, contact your system administrator who will be able to reset it for you.



- 7. Click **Next**. You will be prompted to choose the certificate store for your certificate. Unless your administrator has specified otherwise, you should leave this at the default **Place all certificates in the following store** option.



- 8. Click 'Next'.
- 9. The last step: completing the **Certificate Import Wizard**.



10. Click **Finish** to complete the process. The certificate will be imported.

11. Select the security level for storing the Private Key in your system and click **OK**.



That's it. You have successfully imported your digital certificate into Outlook Express.

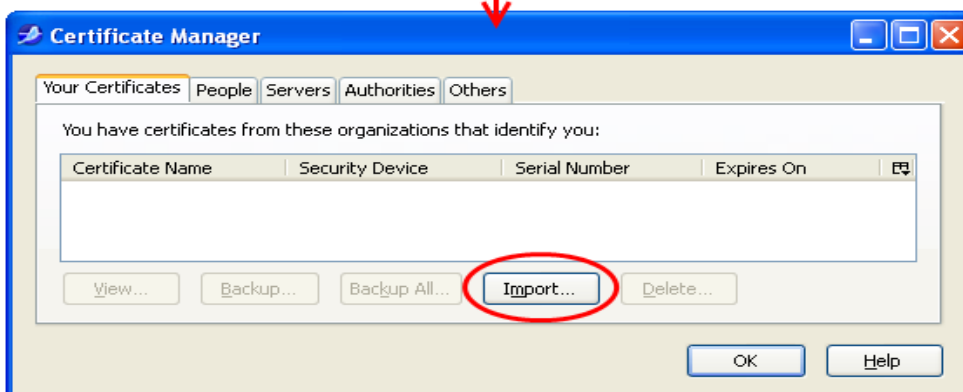
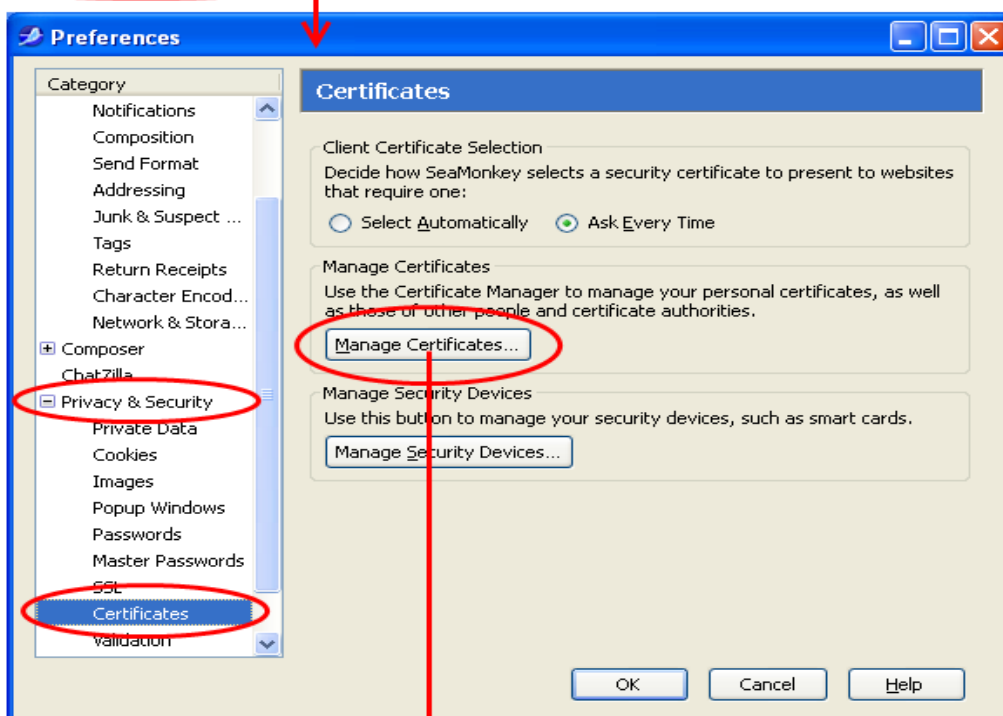
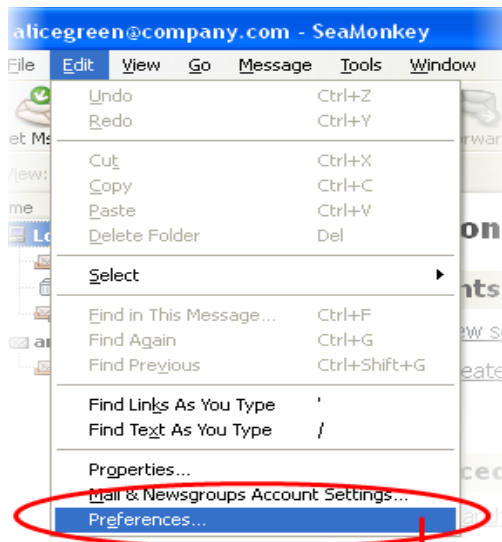
Importing Your Certificate into Mozilla SeaMonkey Email Client

- If you have originally downloaded the certificate through Mozilla SeaMonkey then it should have been already installed.

- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into SeaMonkey installation by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

1. Open SeaMonkey and then click '**Edit**' > '**Preferences**'.
2. In the **Preferences** screen, select '**Privacy & Security**' > '**Certificate**' and then click the '**Manage Certificates...**' button.



3. In the certificate manager interface, make sure the **'Your Certificates'** tab is selected and click **'Import'**.
4. Navigate to the location of the PKCS12 certificate file in which your certificate is stored and enter any necessary passwords. Your certificate will be imported and you will be able to use it to digitally sign and encrypt e-mails.
5. Click **OK** in the **Certificate Manager** dialog to return to the **Preferences** screen.

- Optional - select **Ask me every time** under **When a server requests my personal certificate**.

Doing this alerts you to the fact that a server has requested identity confirmation and enables you to select your InCommon Client Certificate.

6. Click **OK** in the **Preferences** interface to return to SeaMonkey.

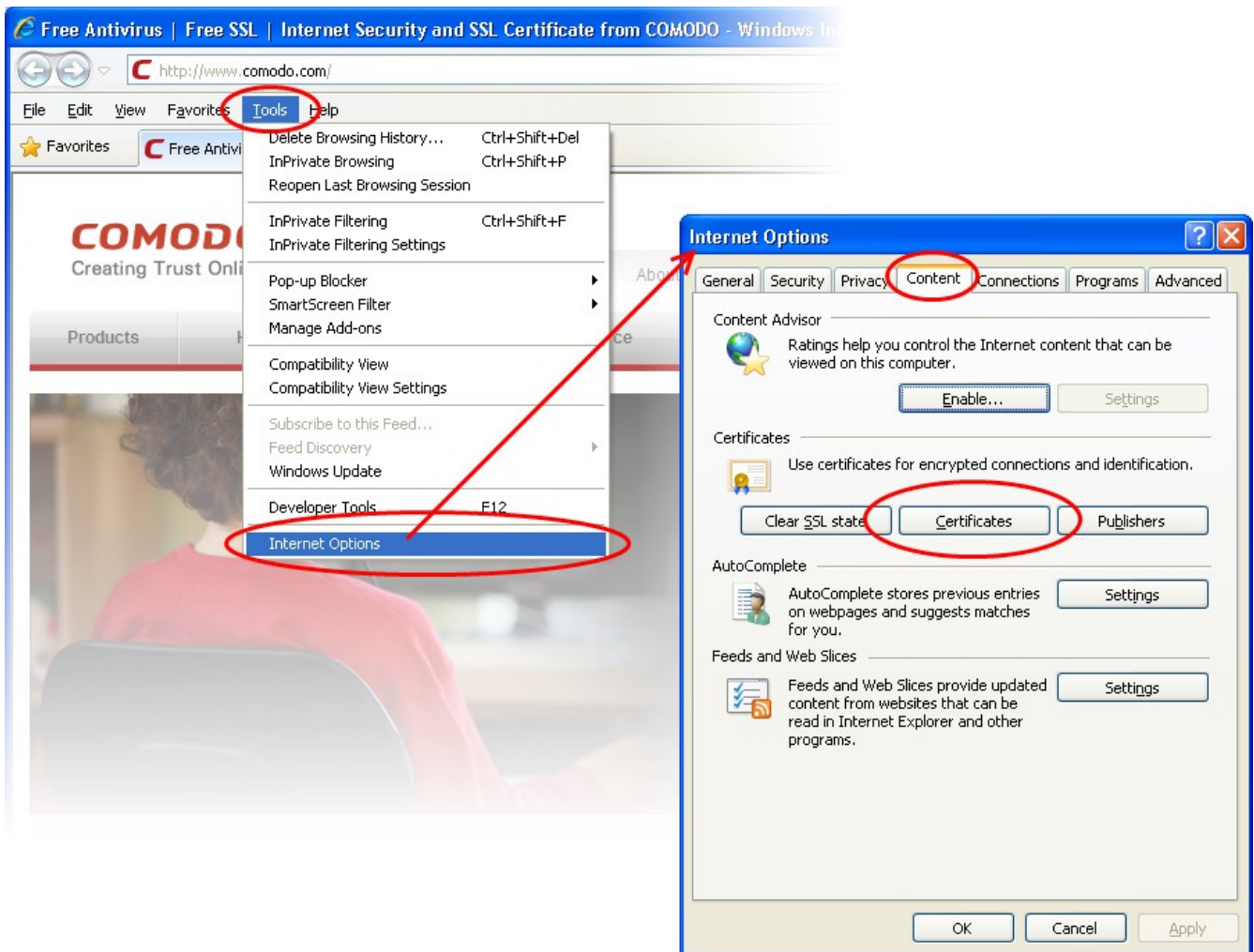
That's it. You have successfully imported your digital certificate into Mozilla SeaMonkey.

Importing Your Certificate into Internet Explorer

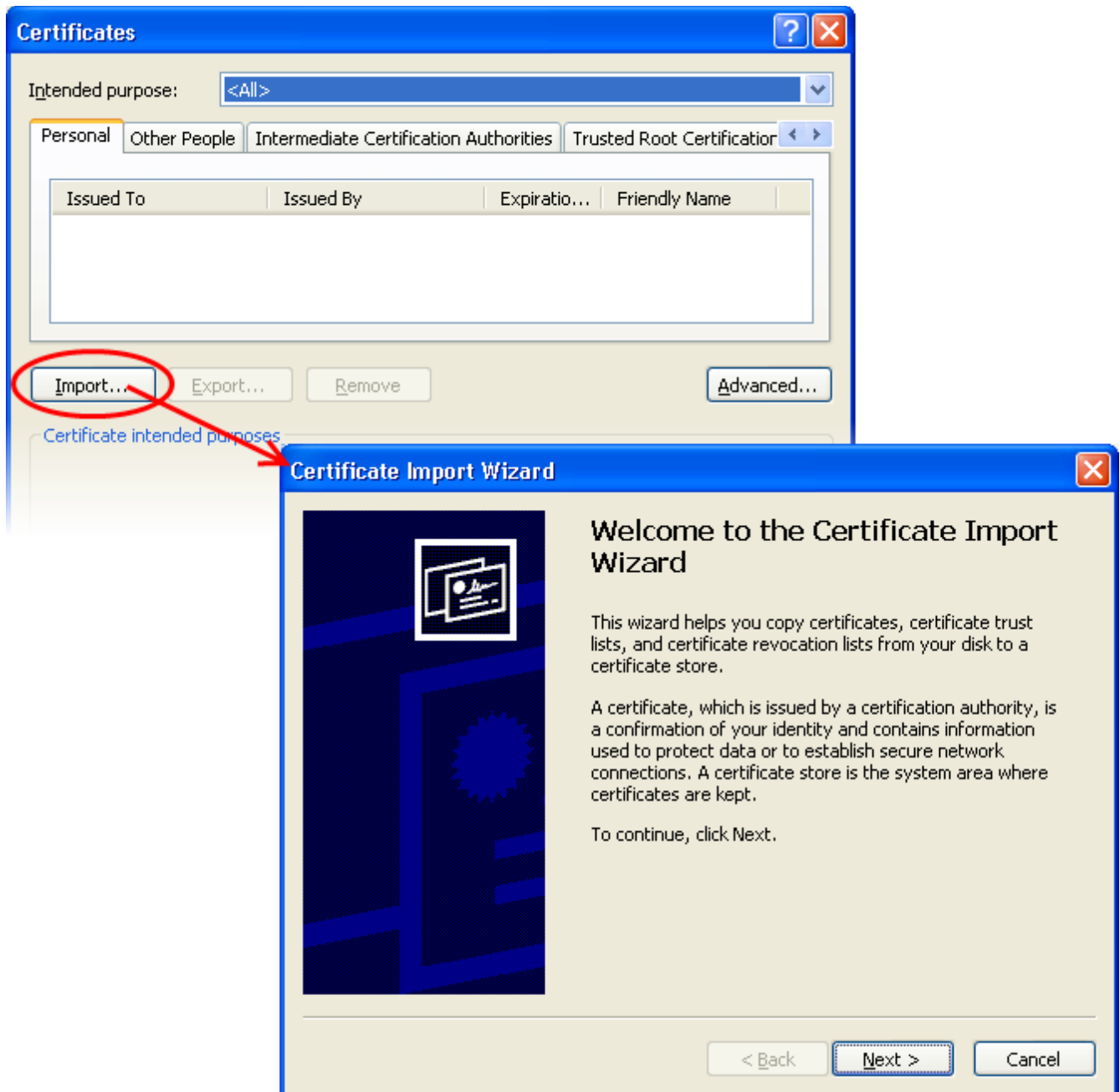
- If you have originally downloaded the certificate through Internet Explorer then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into your computer by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

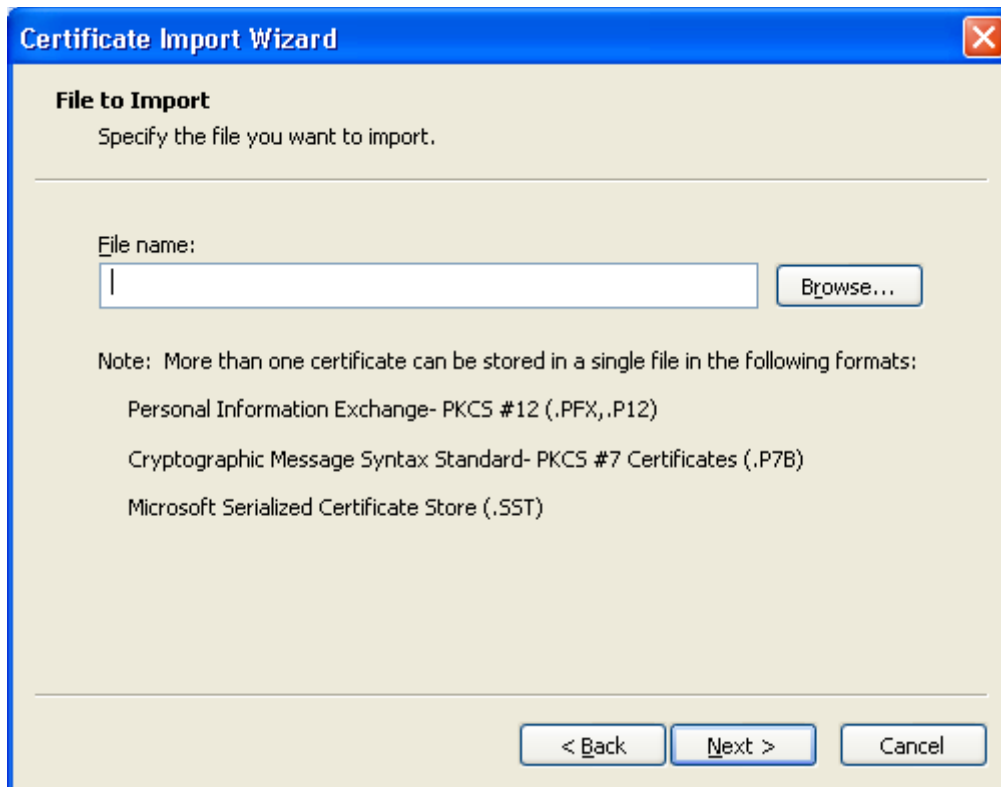
1. Open Internet Explorer and click '**Tools**' > '**Internet Options**'.
2. Select the '**Content**' tab and then click the '**Certificates**' button.



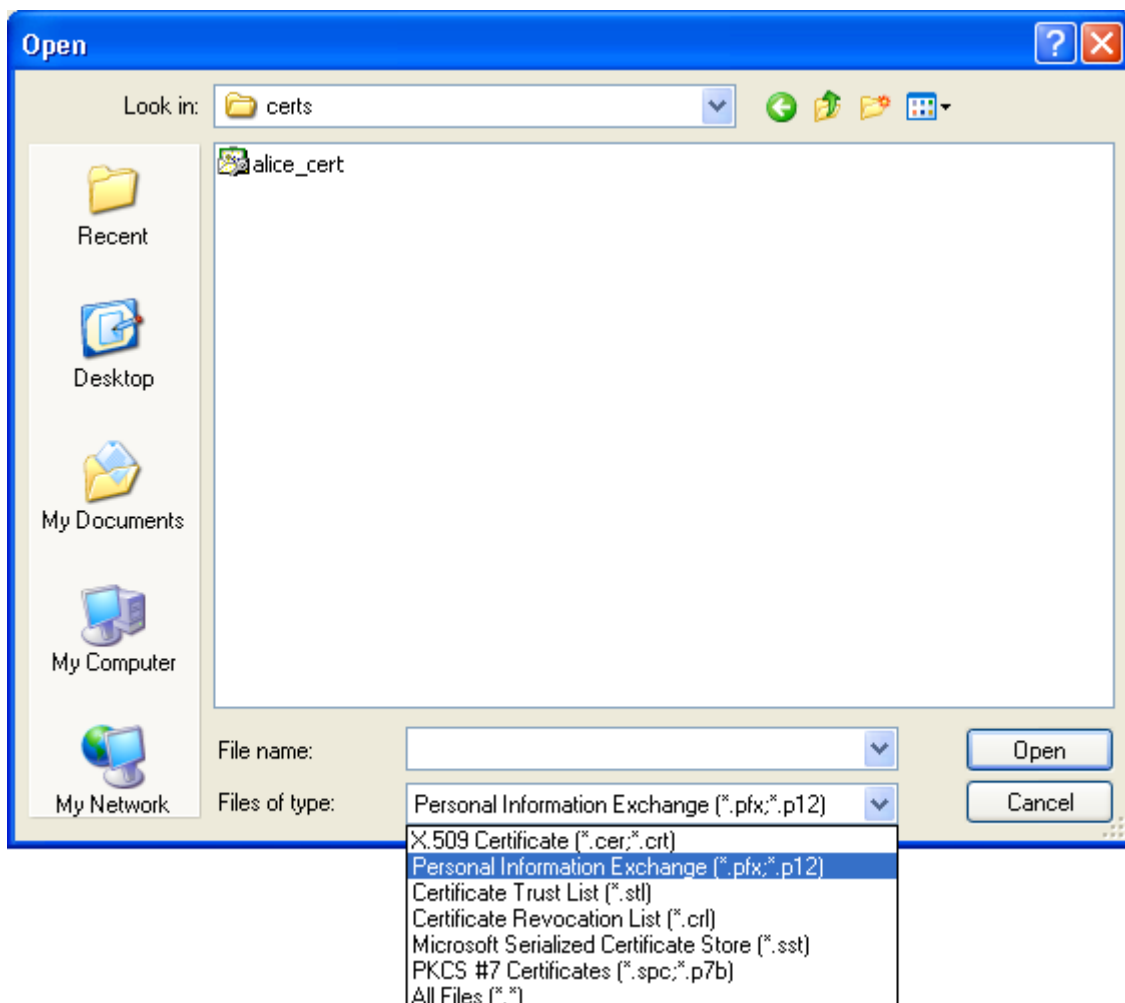
3. In the Certificates interface, make sure the '**Personal**' tab is selected, click '**Import**' and then click '**Next**'.



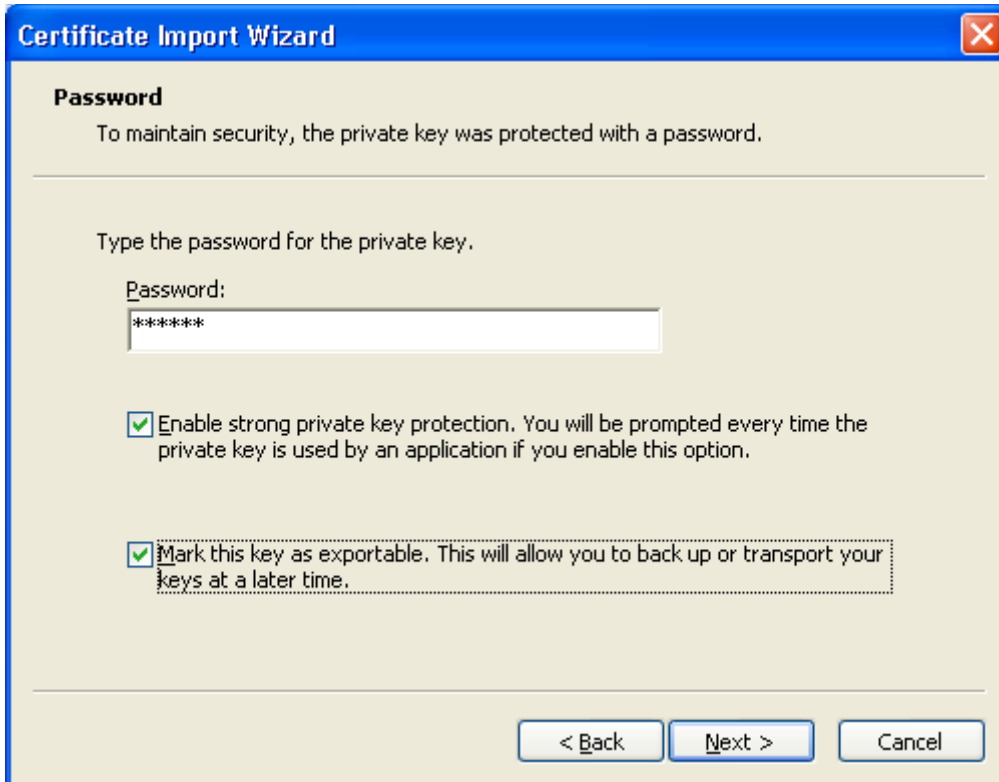
4. Click '**Browse**' in the next step and navigate to the location of your PKCS12 certificate file.



5. Locate your certificate file (.p12) and click **'Open'**:



6. After locating your certificate file, click **Next**. To complete the installation process, you are required to enter the PIN (password) you set up for the certificate during the enrollment process. If you have forgotten your password, contact your system administrator who will be able to reset it for you.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

< Back Next > Cancel

7. Click **Next**. You will be prompted to choose the certificate store for your certificate. Unless your administrator has specified otherwise, you should leave this at the default **Place all certificates in the following store** option.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

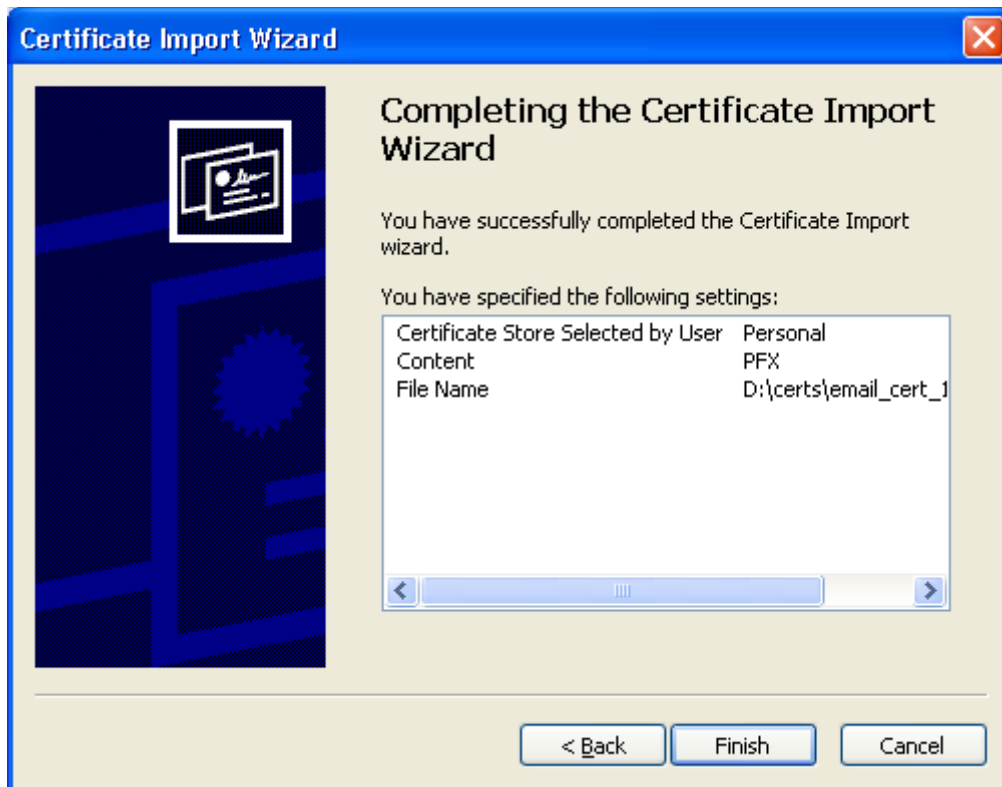
Automatically select the certificate store based on the type of certificate

Place all certificates in the following store:

Certificate store:
Personal Browse...

< Back Next > Cancel

8. Click **Next** to proceed to the review and confirm stage:



9. Click **Finish** to complete the process. The certificate will be imported.

10. Select the security level for storing the Private Key in your system and click **OK**.



That's it. You have successfully imported your digital certificate into Internet Explorer.

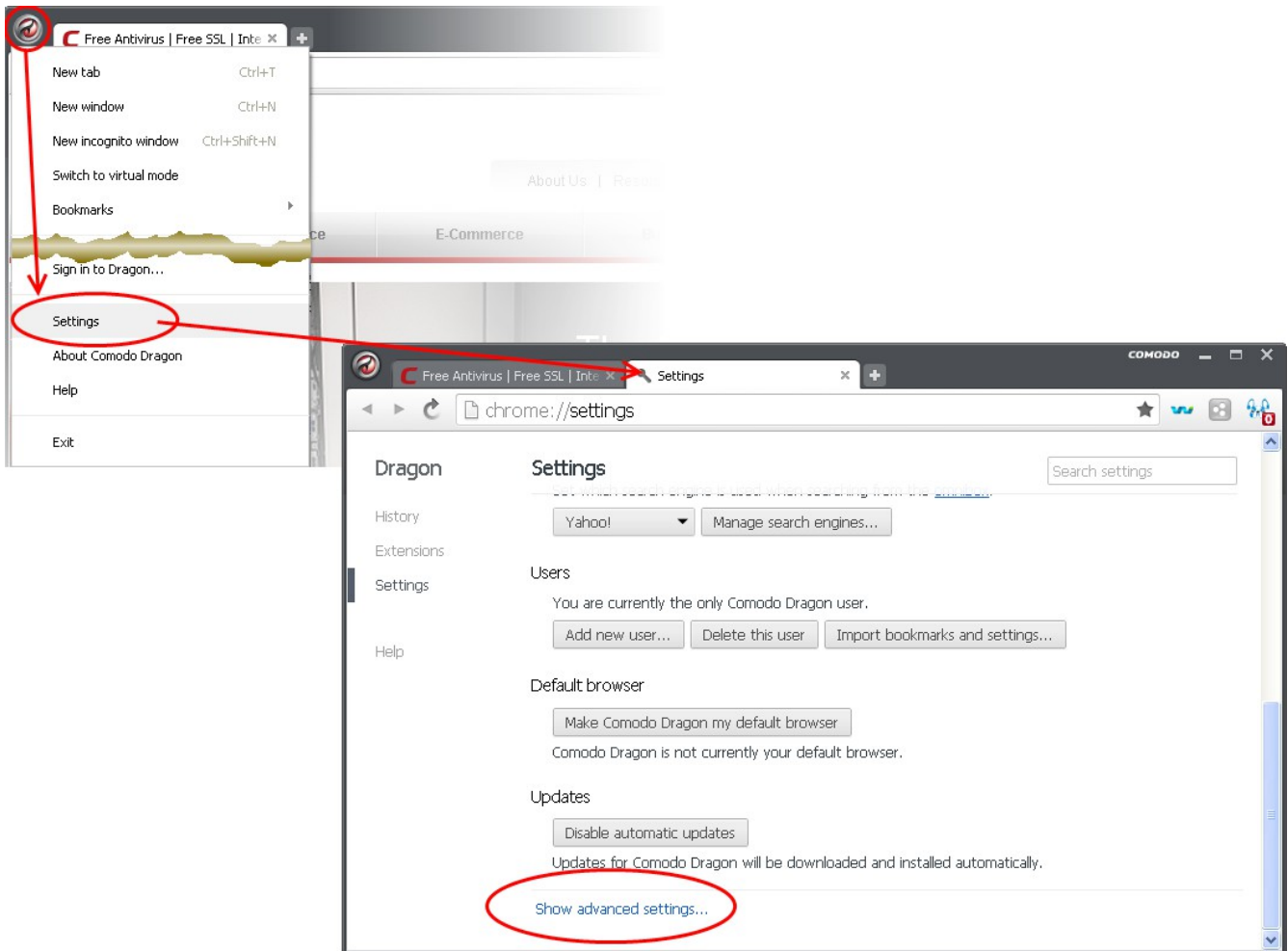
Importing Your Certificate into Comodo Dragon

- If you have originally downloaded the certificate through Comodo Dragon then it should have been already installed.

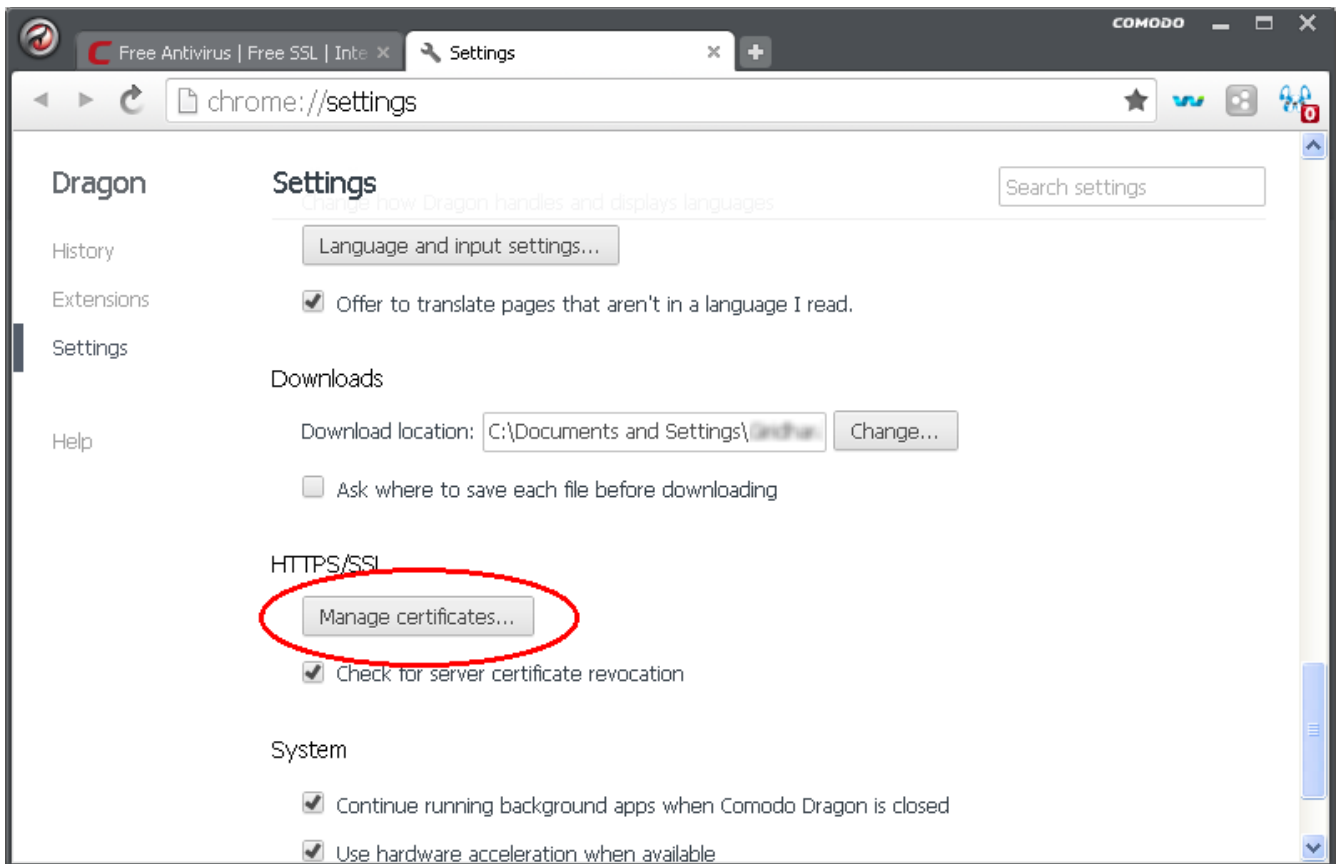
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into your computer by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

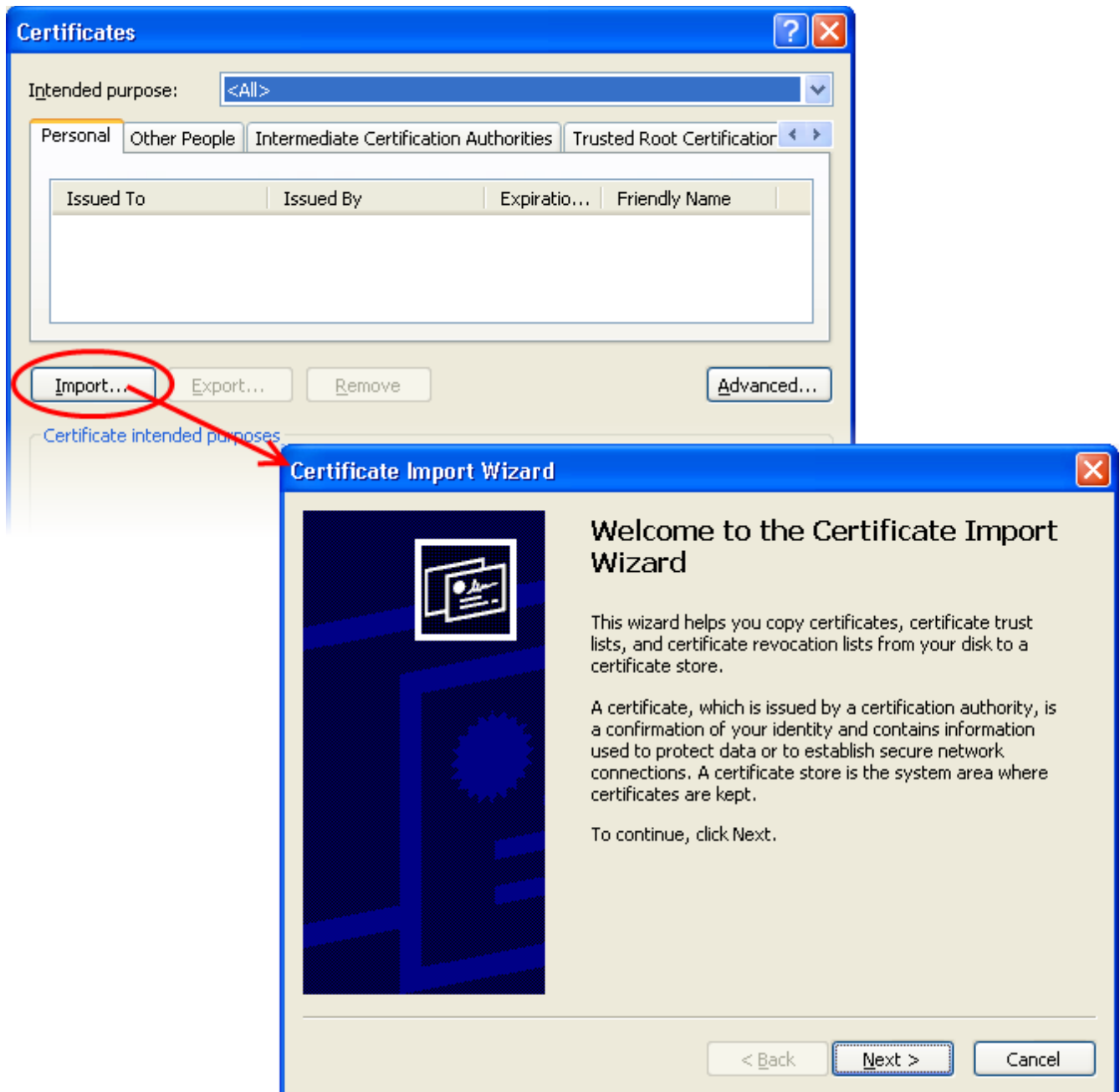
1. Open Comodo Dragon then click '**Comodo Dragon icon**' > '**Settings**'.
2. Scroll down the **Settings** page in the new tab and click the **Show Advanced Settings** link.



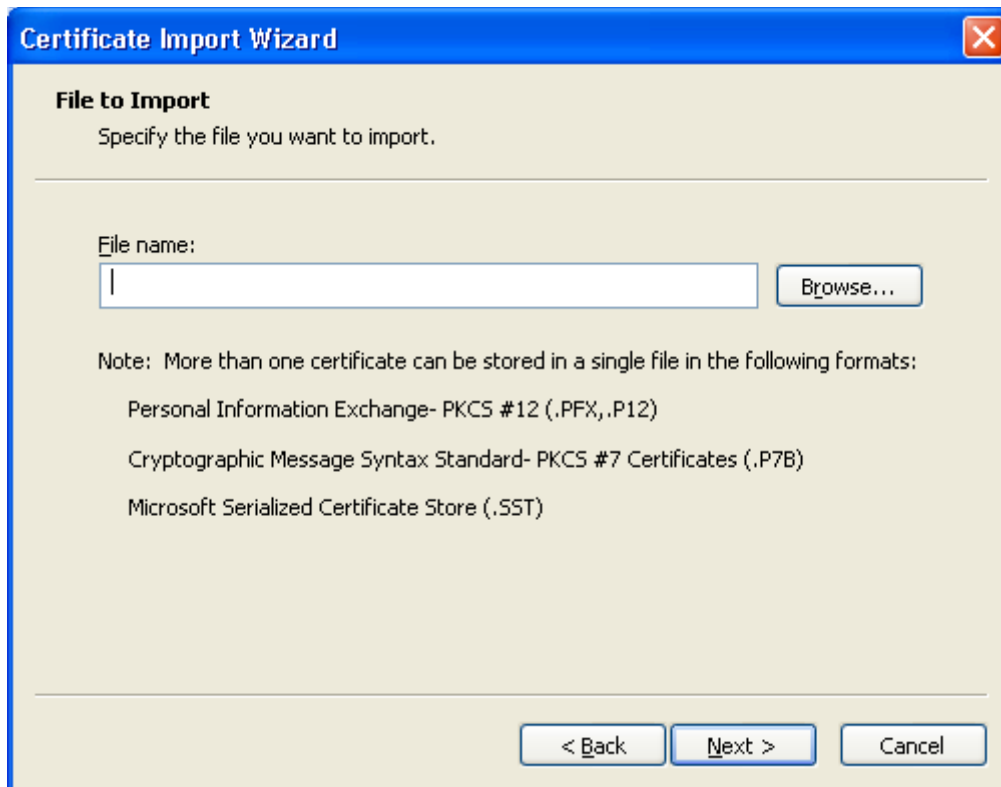
3. Scroll down the page and click the **Manage Certificates** button under **HTTPS/SSL**.



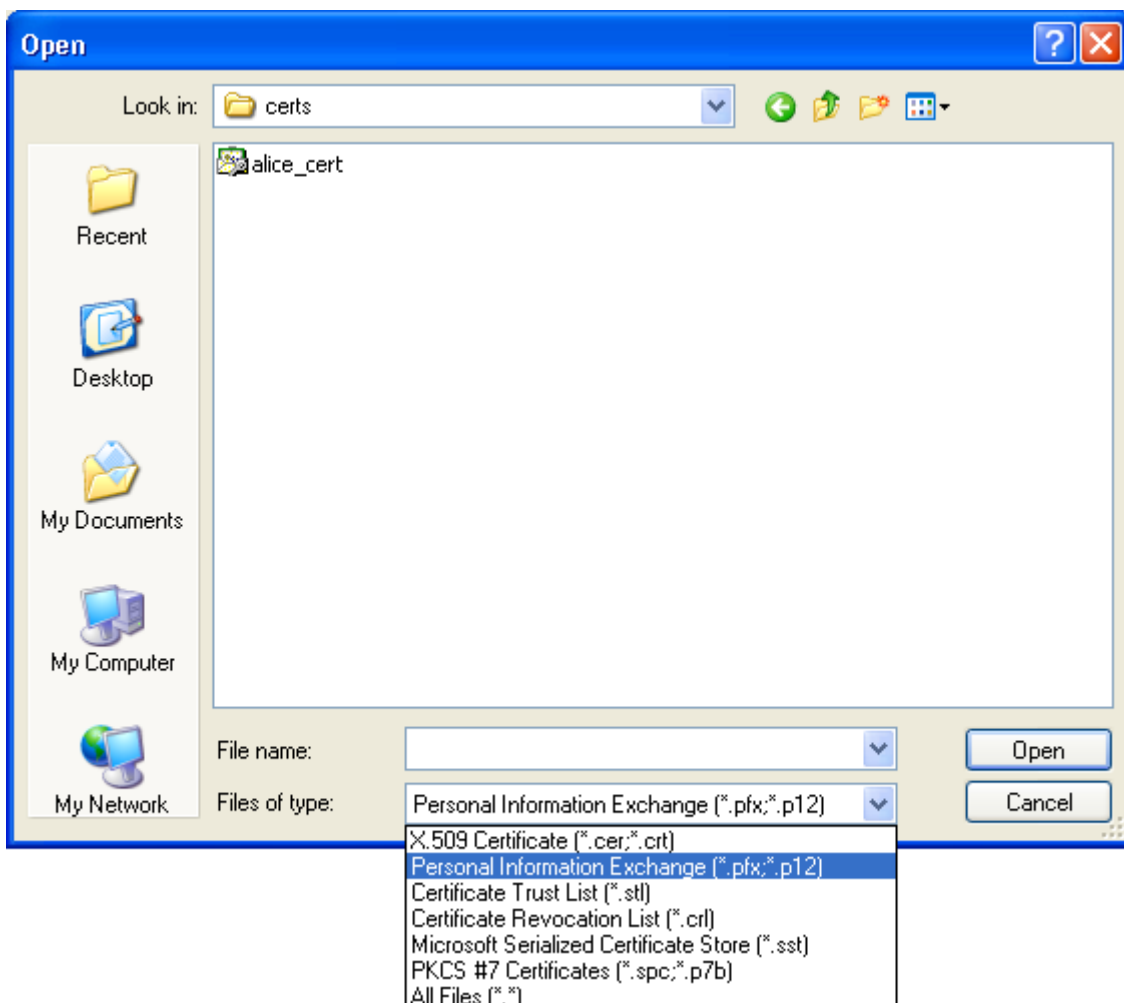
4. In the Certificates interface, make sure the **'Personal'** tab is selected, click **'Import'** and then click **'Next'**.



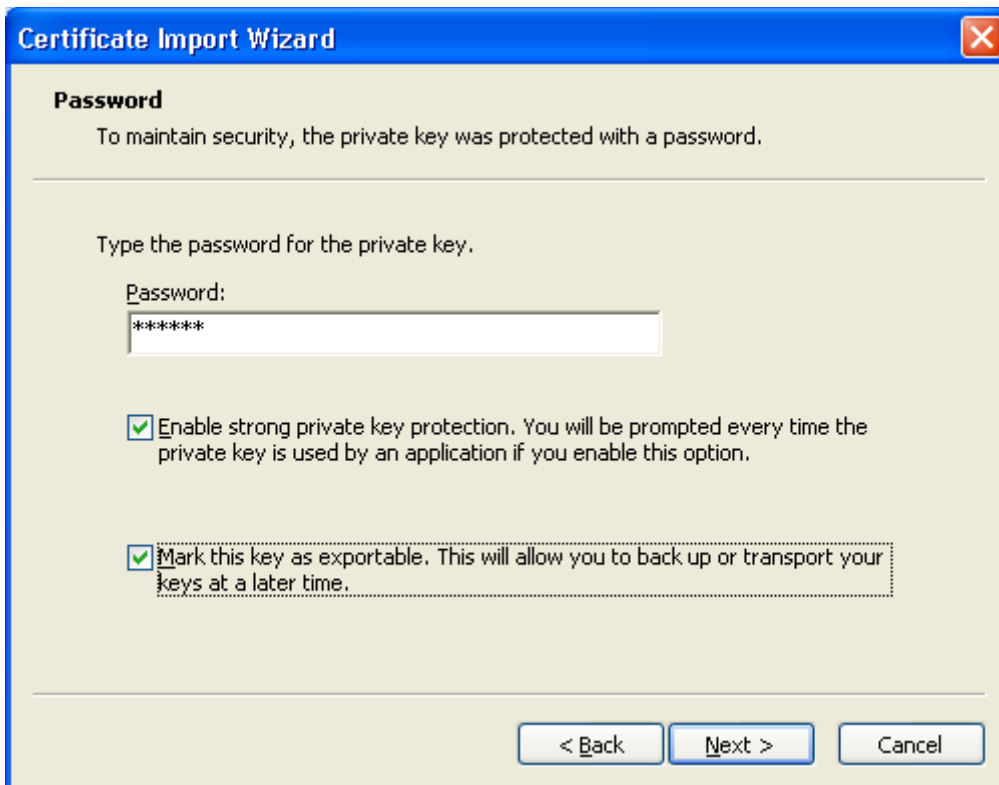
5. Click '**Browse**' in the next step and navigate to the location of your PKCS12 certificate file.



6. Locate your certificate file (.p12) and click **'Open'**:



- To complete the installation process, you are required to enter the PIN (password) you set up for the certificate during the enrollment process. If you have forgotten your password, contact your system administrator who will be able to reset it for you.



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

< Back Next > Cancel

- Next you will be prompted to choose which certificate store for your certificate. Unless your administrator has specified otherwise, you should leave this at the default **Place all certificates in the following store** option.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for

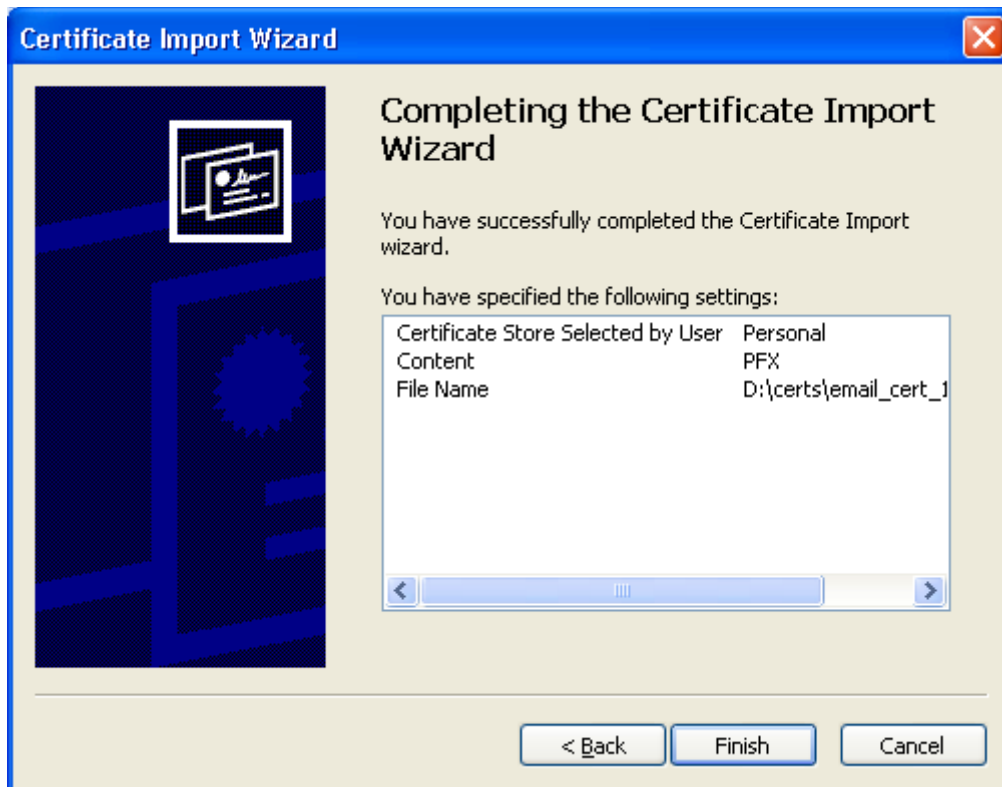
Automatically select the certificate store based on the type of certificate

Place all certificates in the following store:

Certificate store:
Personal Browse...

< Back Next > Cancel

- Click '**Next**' to proceed to the review and confirm stage:



10. Click **Finish** to complete the process. The certificate will be imported.

11. Select the security level for storing the Private Key in your system and click **OK**.



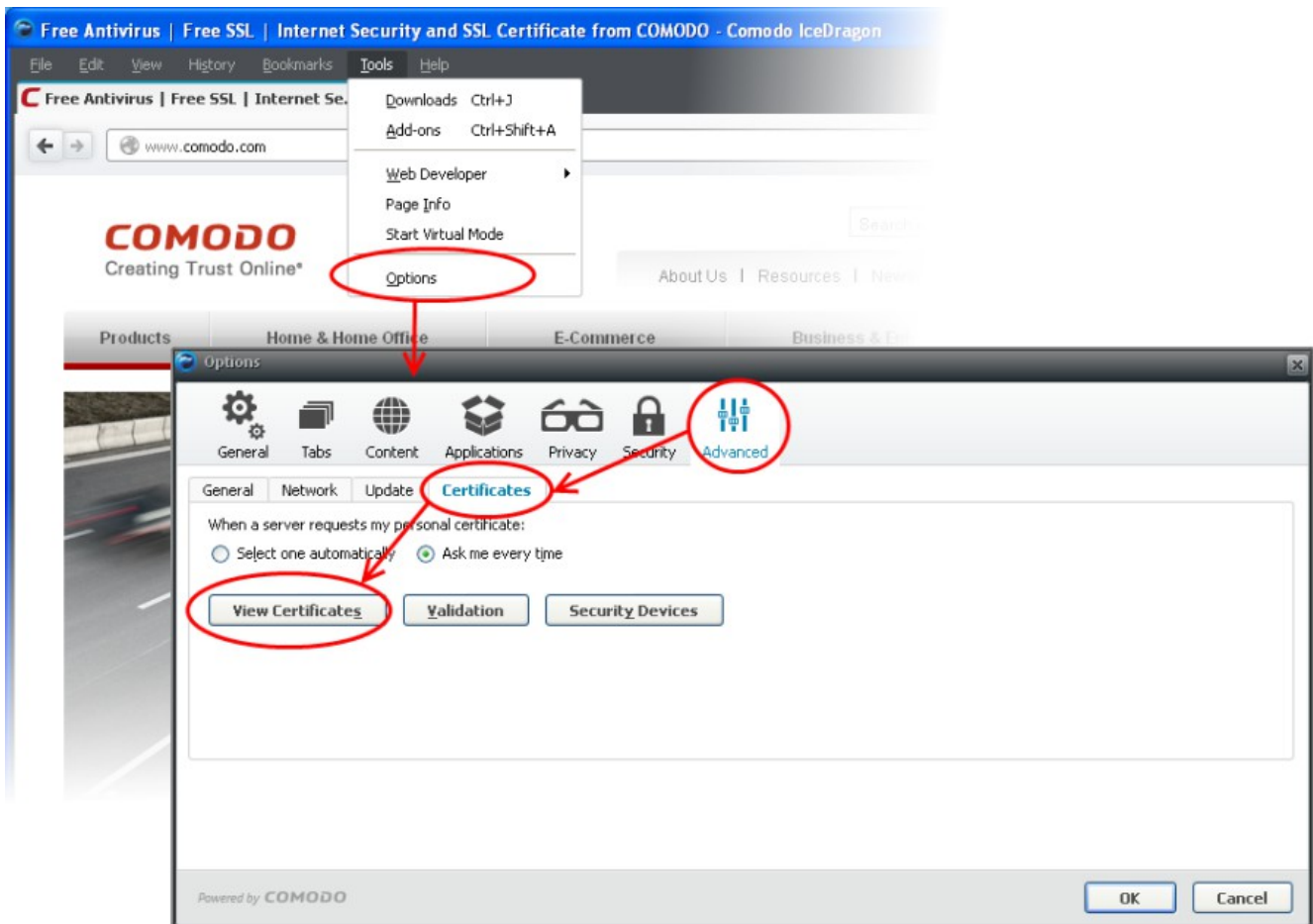
That's it. You have successfully imported your digital certificate into Comodo Dragon.

Importing Your Certificate into Comodo IceDragon

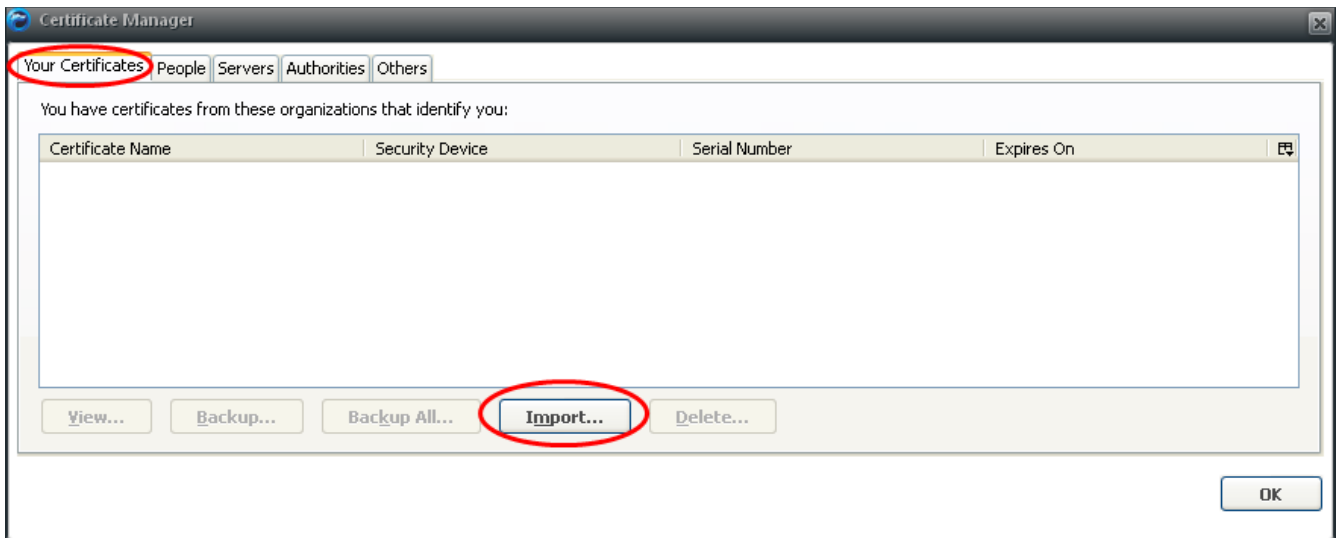
- If you have originally downloaded the certificate through Comodo IceDragon then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import' the certificate into your computer by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

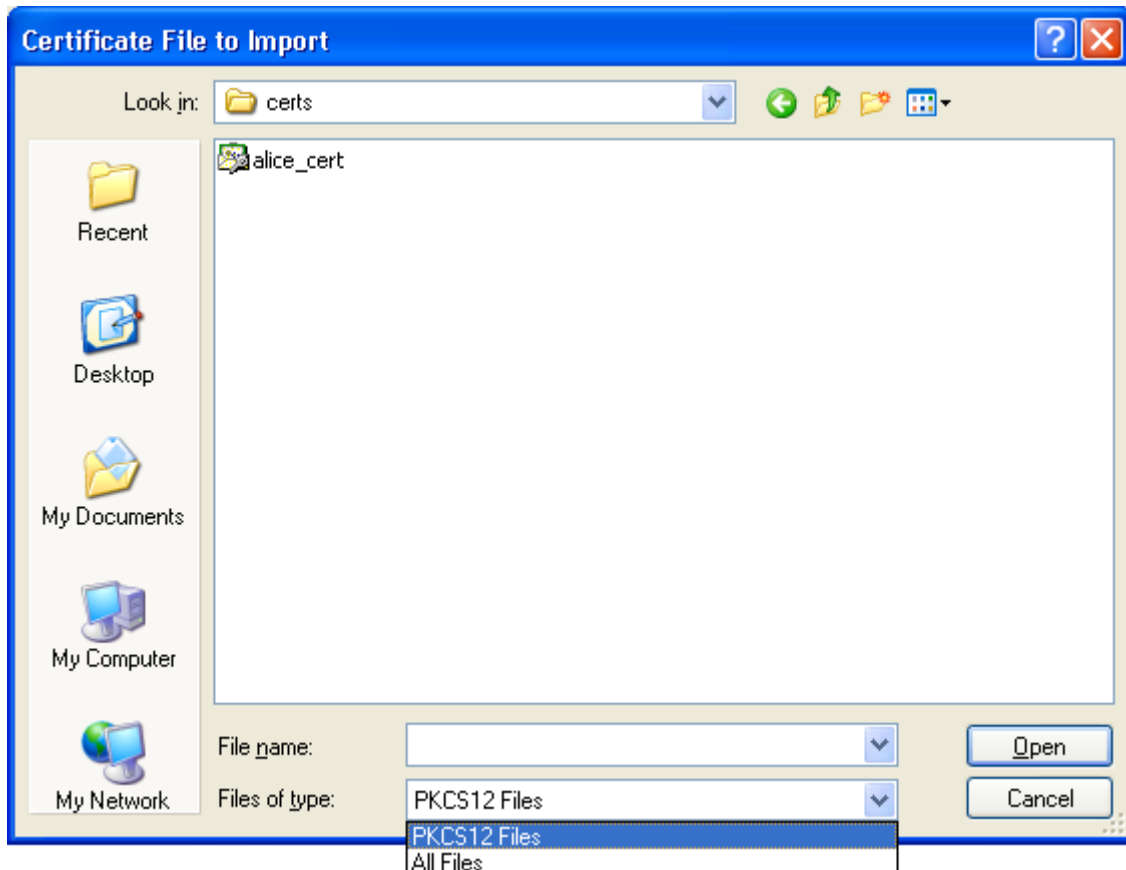
1. Open Comodo IceDragon then click '**Tools**' > '**Options**' > '**Advanced**'.
2. Select the '**Certificates**' tab
 - Optional - Leave enabled 'Ask me every time' under 'When a server requests my personal certificate'.
 - Doing so alerts you to the fact that a server has requested identity confirmation and enables you to select your InCommon Client Certificate.



3. Click the '**View Certificates**' button
4. In the certificate manager interface, make sure the '**Your certificates**' tab is selected and click '**Import**'.



5. Navigate to the location of your PKCS12 certificate file, select your InCommon Client Certificate and click '**Open**'.



6. To complete the import process, you are required to enter the password you set up while exporting or backing up your certificate. Enter the password and click **OK**.



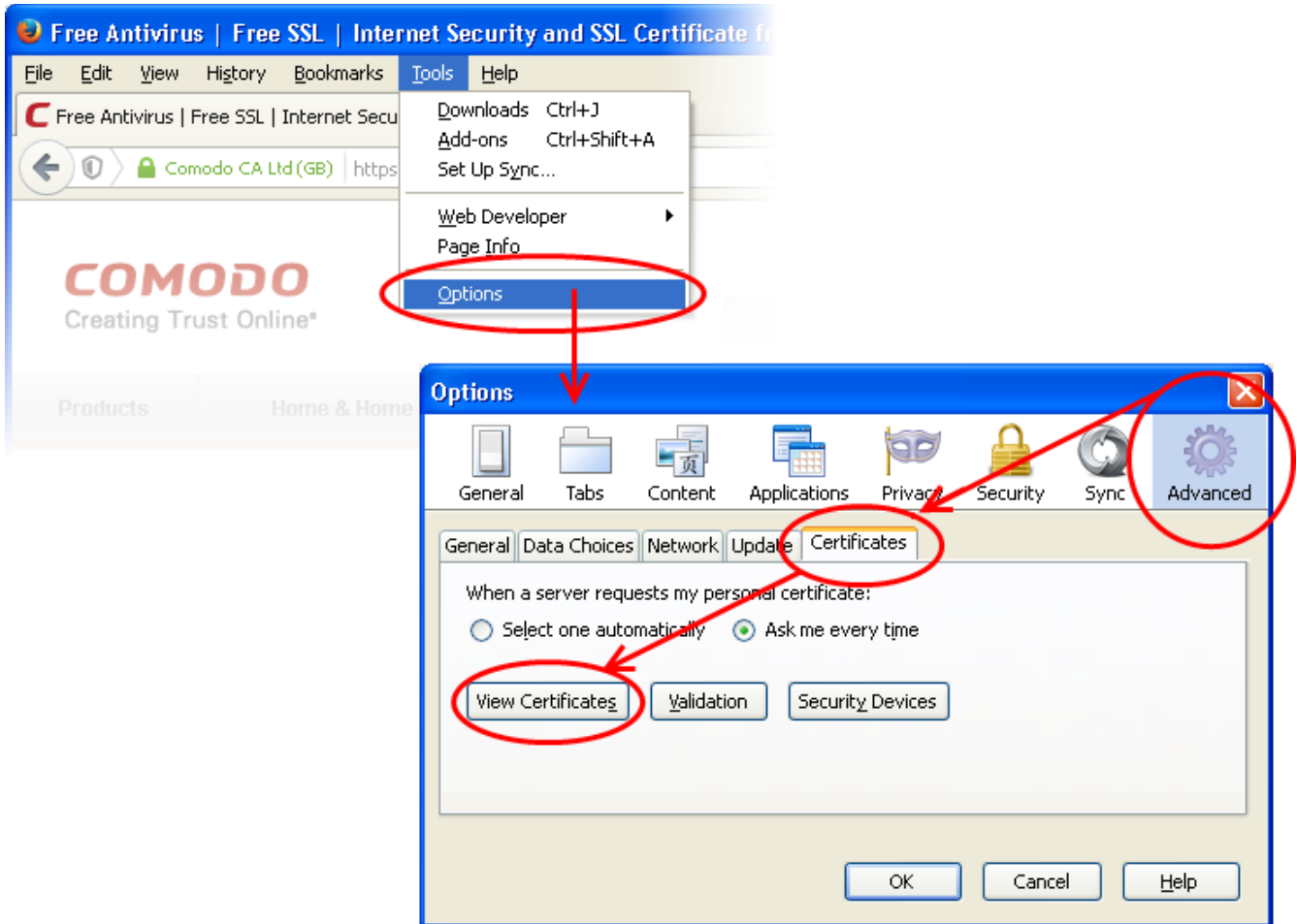
That's it. You have successfully imported your Digital Certificate into Comodo IceDragon.

Importing Your Certificate into Mozilla Firefox

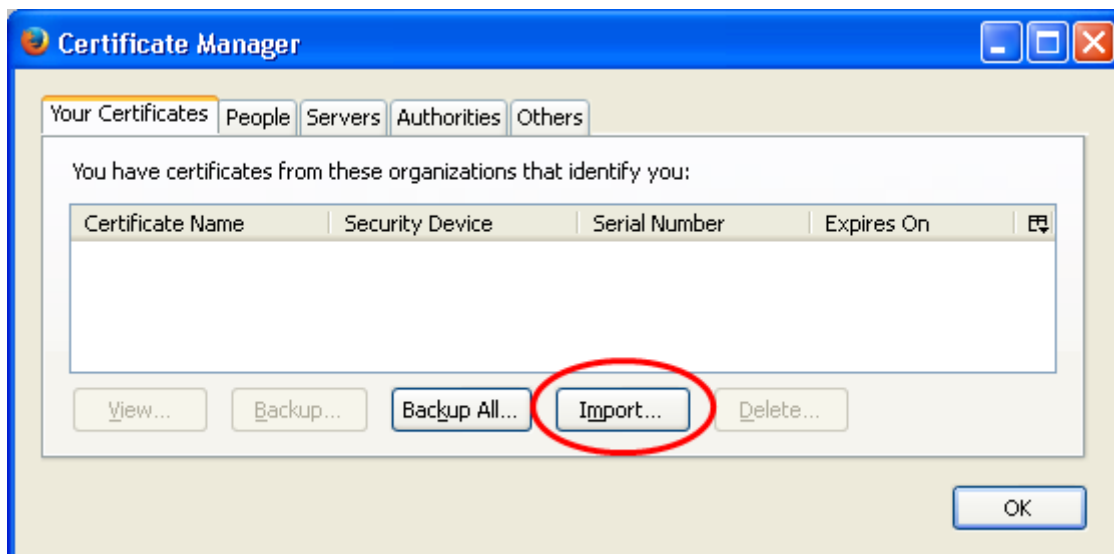
- If you have originally downloaded the certificate through Mozilla Firefox then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Mozilla Firefox by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

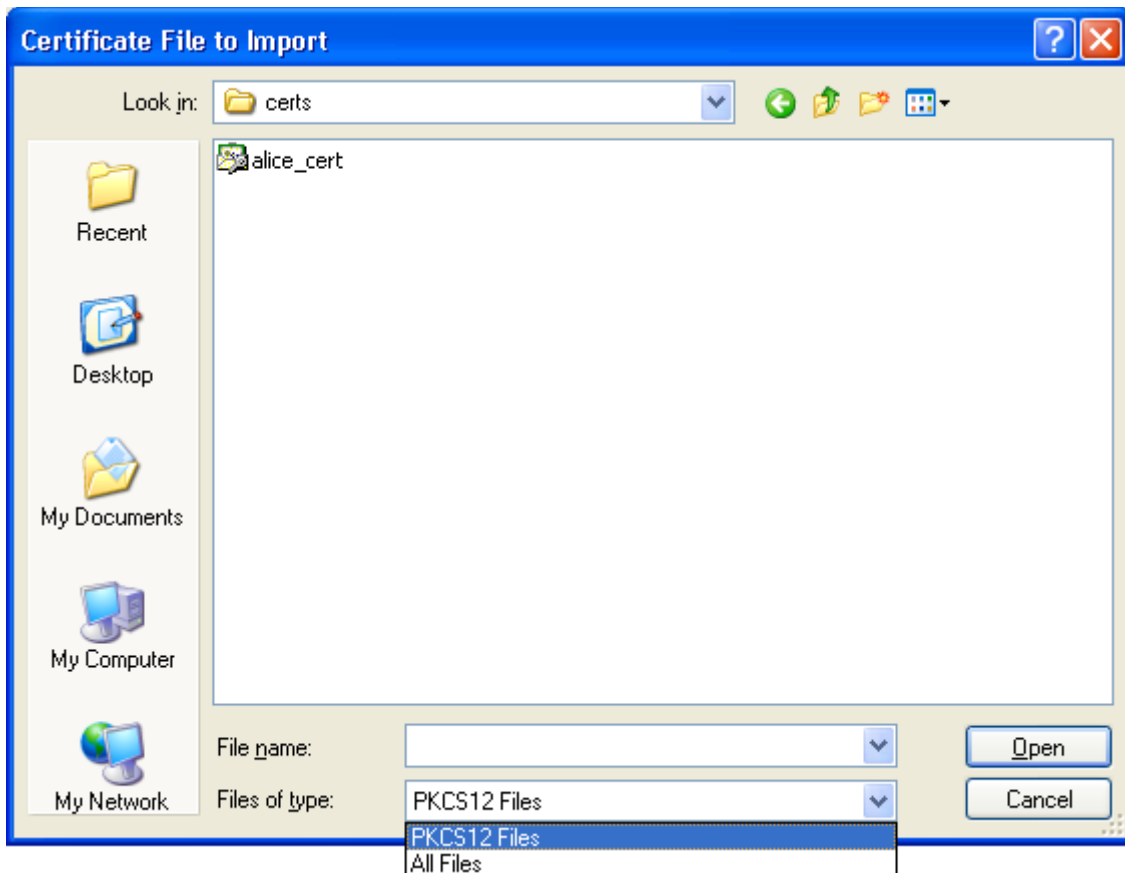
1. Open Firefox then click '**Tools**' > '**Options**' > '**Advanced**'.
2. Select the '**Certificates**' tab
 - Optional - Leave enabled '**Ask me every time**' under '**When a server requests my personal certificate**'.
 - Doing so alerts you to the fact that a server has requested identity confirmation and enables you to select your InCommon Client Certificate.



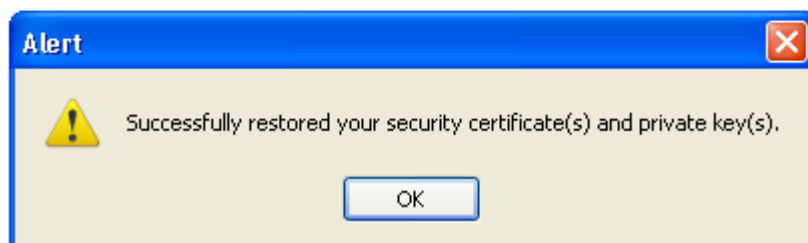
3. Click the **'View Certificates'** button.
4. In the certificate manager interface, make sure the **'Your Certificates'** tab is selected and click **'Import'**.



5. Navigate to the location of your PKCS12 certificate file, select your InCommon Client Certificate and click **'Open'**.



6. To complete the import process, you are required to enter the password you set up while exporting or backing up your certificate. Enter the password and click **OK**.



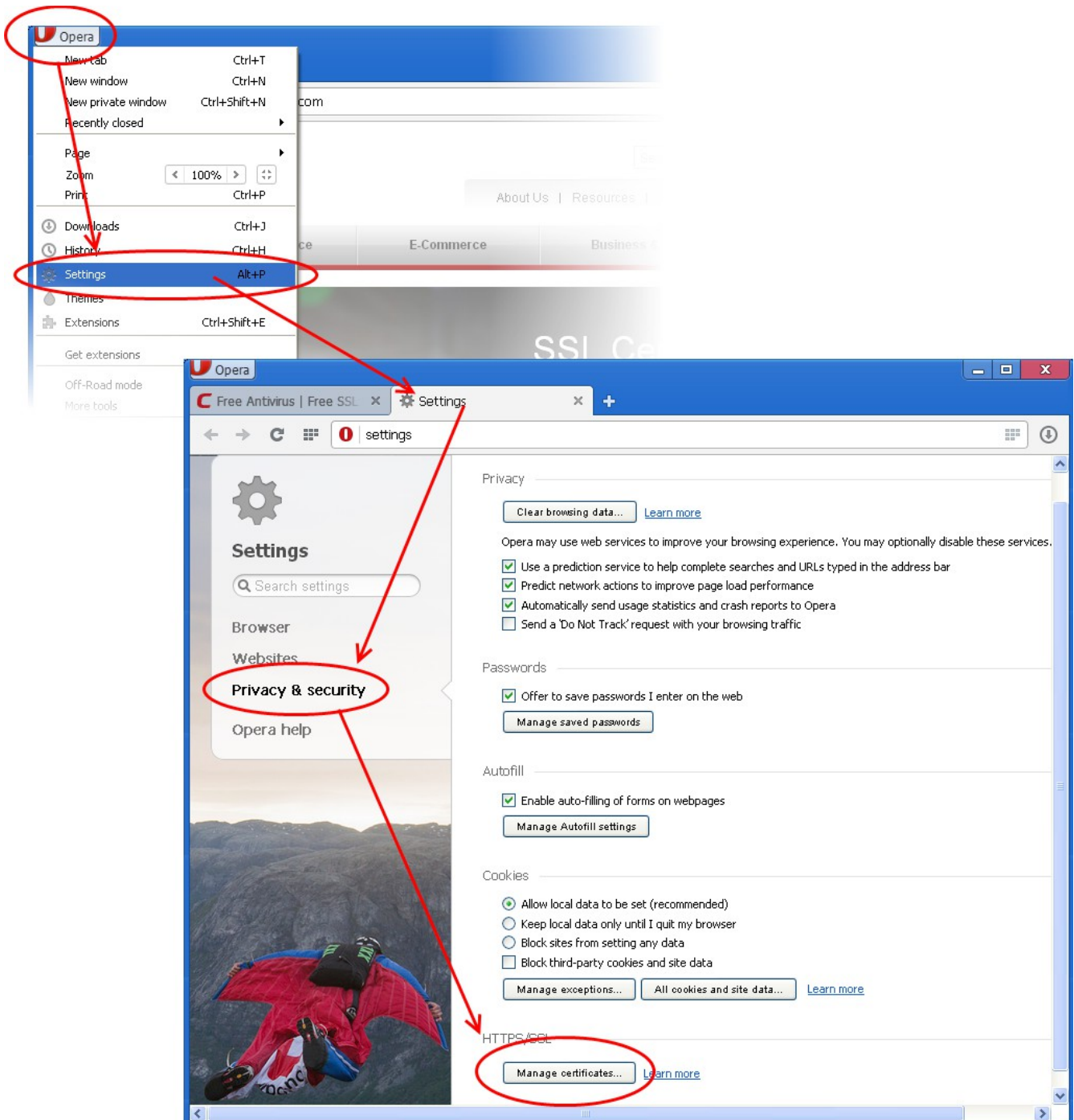
That's it. You have successfully imported your digital certificate into Mozilla Firefox.

Importing your Certificate into Opera

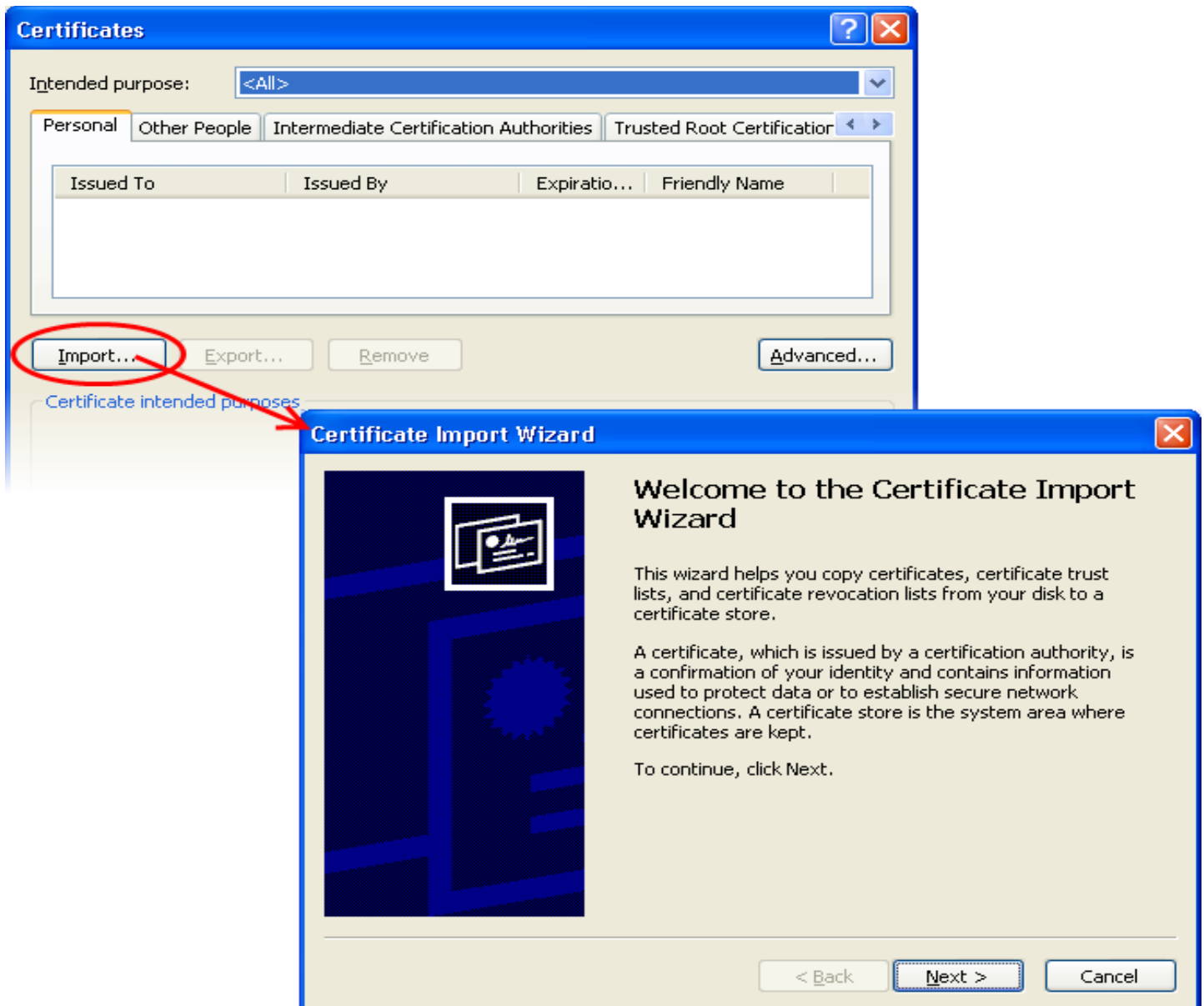
- If you have originally downloaded the certificate through Opera then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Opera by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

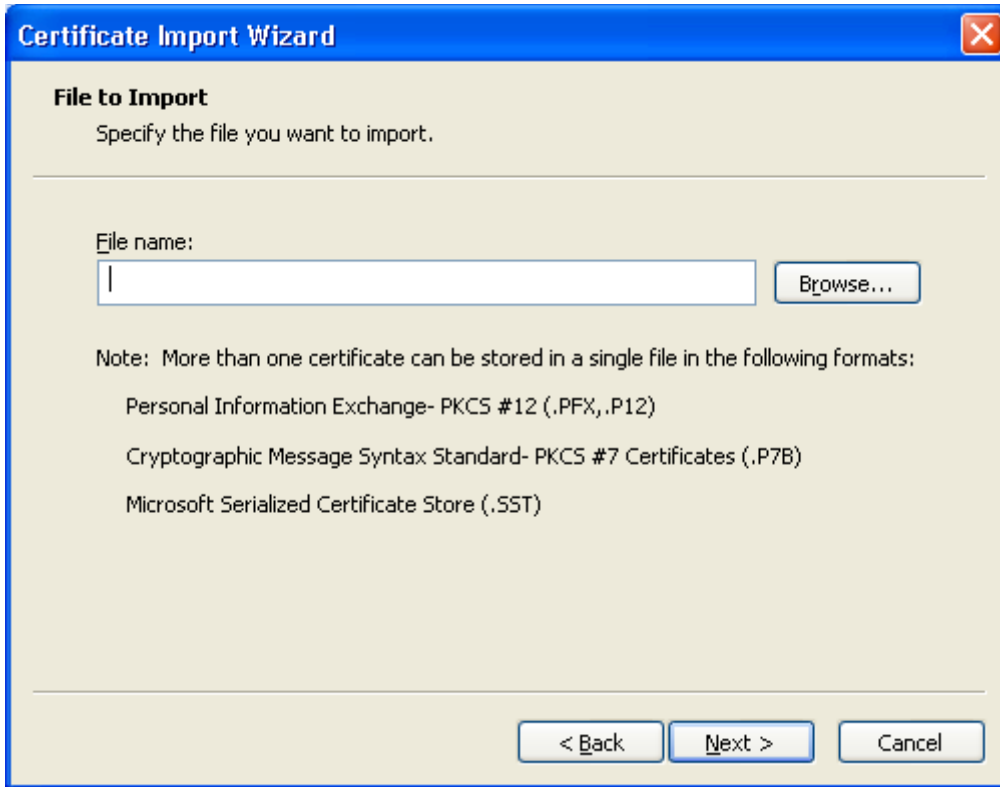
1. Open Opera then click '**Opera icon**' > '**Settings**' .
2. In the Settings tab, click 'Privacy & Security' > 'Manage Certificates'.



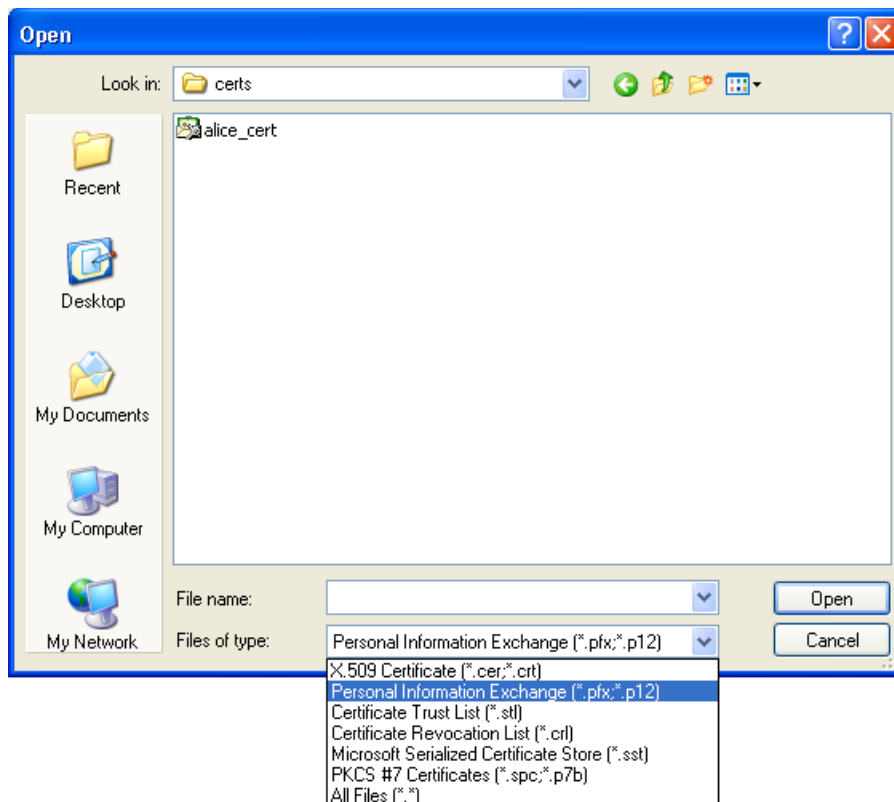
3. In the Certificates interface, make sure the '**Personal**' tab is selected, click '**Import**' and then click '**Next**'.

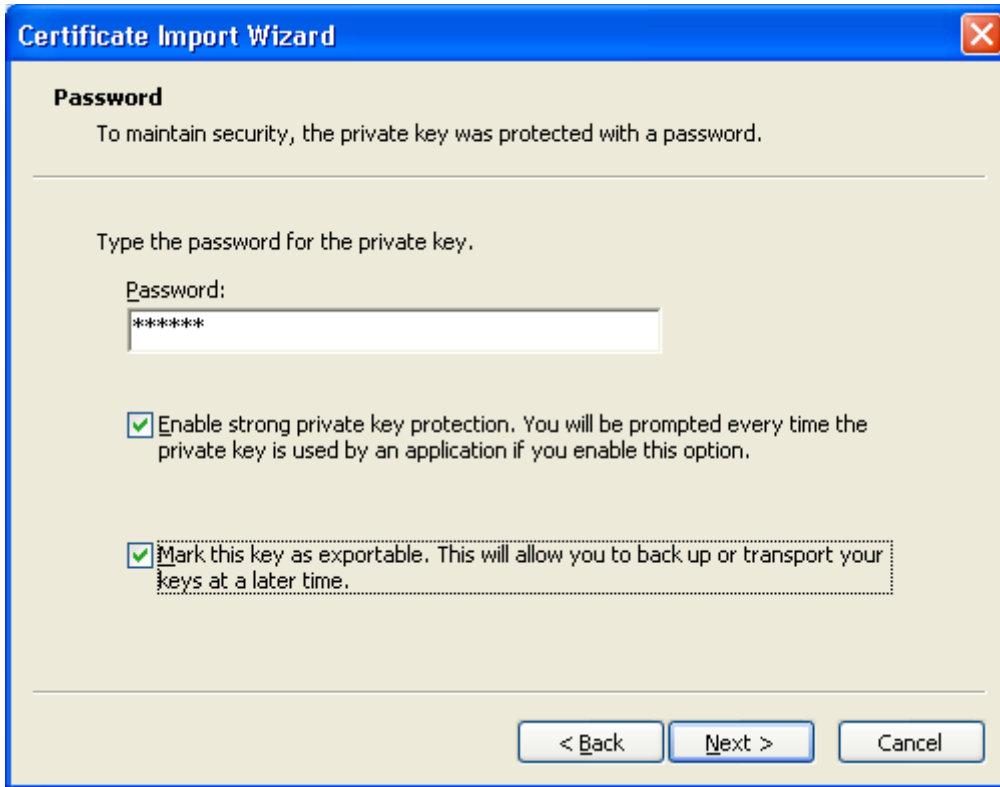


4. Click '**Browse**' in the next step and navigate to the location of your PKCS12 certificate file.



- 5. After locating your certificate file, click **Next**. To complete the installation process, you are required to enter the PIN (password) you set up for the certificate during the enrollment process. If you have forgotten your password, contact your system administrator who will be able to reset it for you.

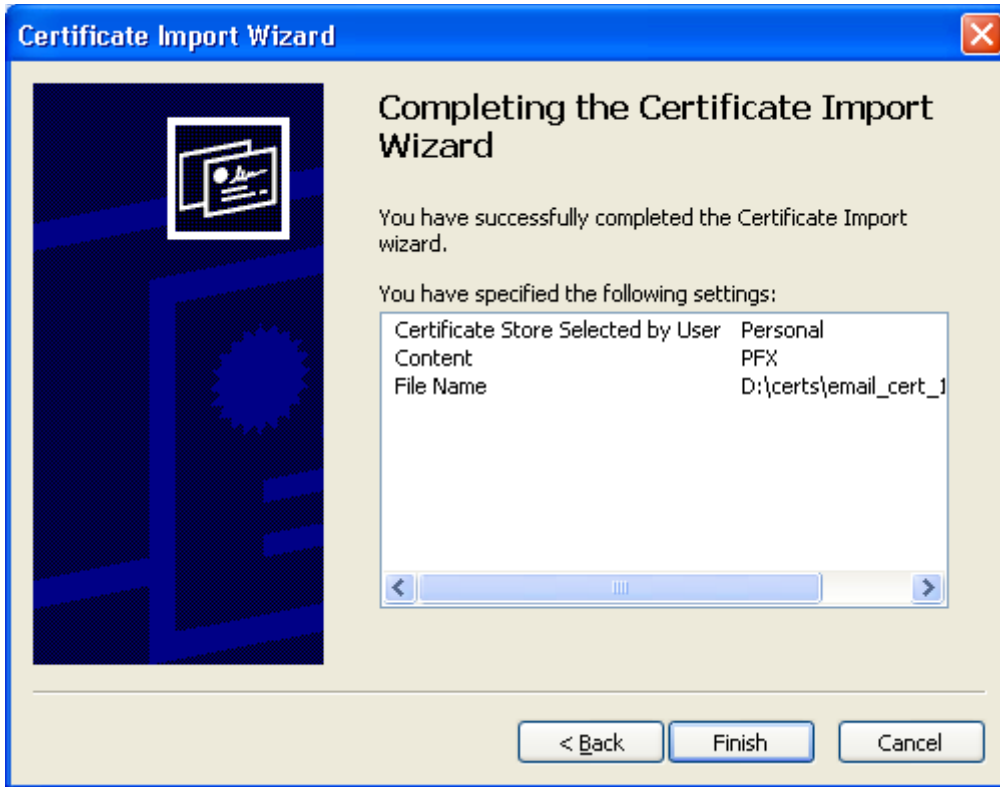




- 6. Click Next. You will be prompted to choose the certificate store for your certificate. Unless your administrator has specified otherwise, you should leave this at the default **Place all certificates in the following store** option



- 7. Click **'Next'** to proceed to the review and confirm stage:



8. Click **Finish** to complete the process. The certificate will be imported.
9. Select the security level for storing the Private Key in your system and click **OK**.



That's it. You have successfully imported your digital certificate into Opera.

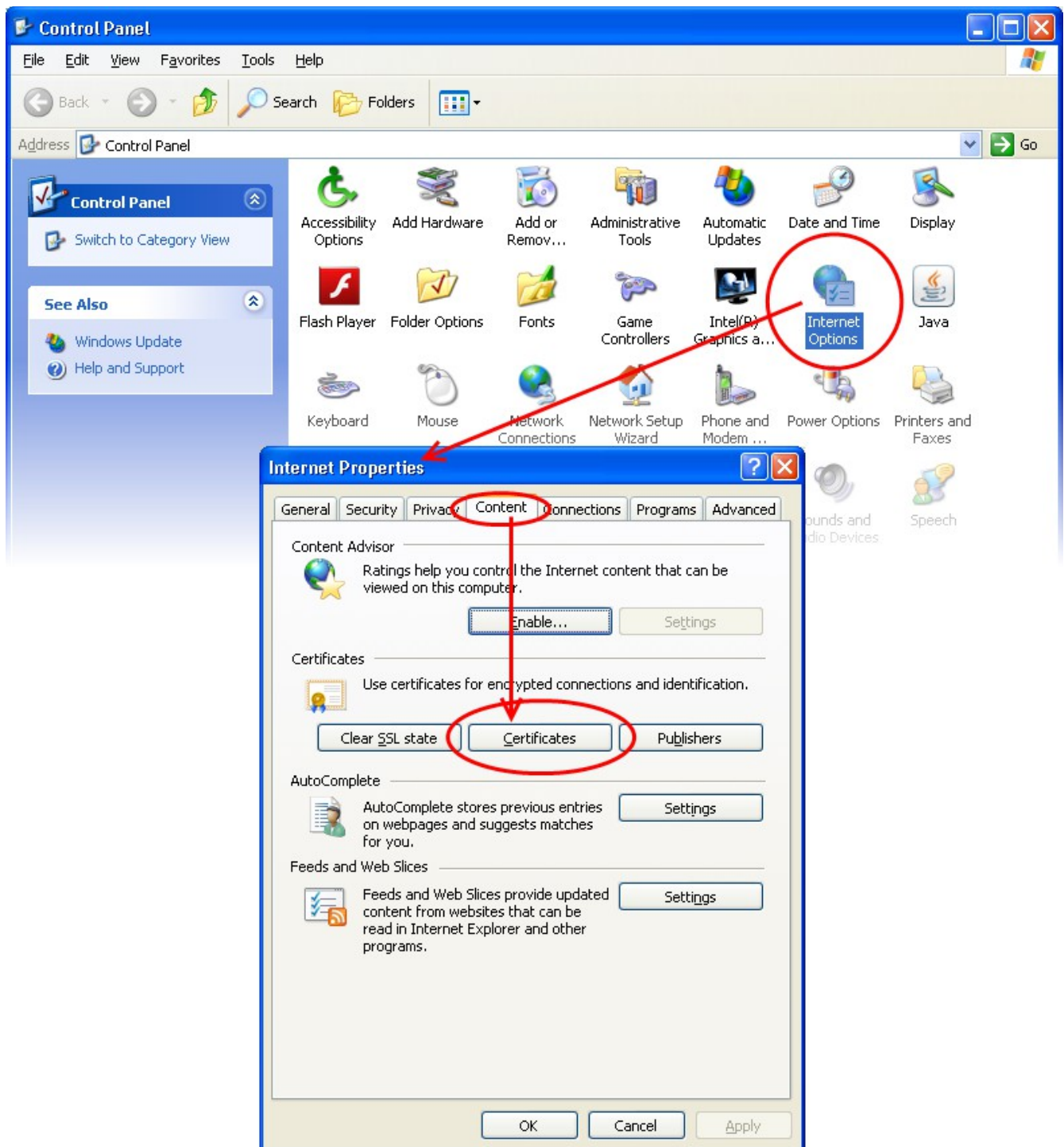
Importing your Certificate into Safari on Windows

- If you have originally downloaded the certificate through Safari then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Safari by following the steps given below.

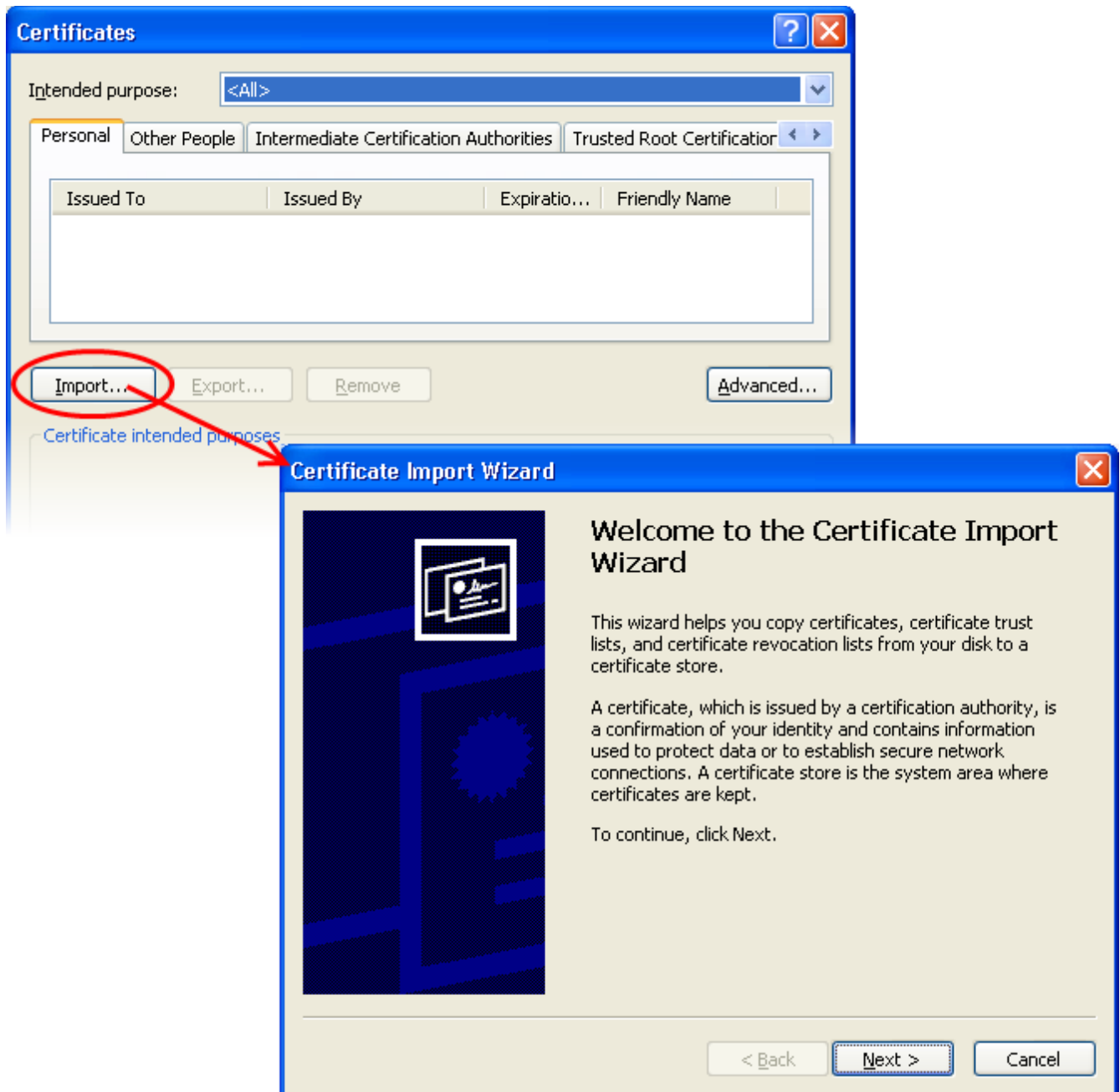
Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

Safari uses the Windows OS certificate store for encryption and authentication.

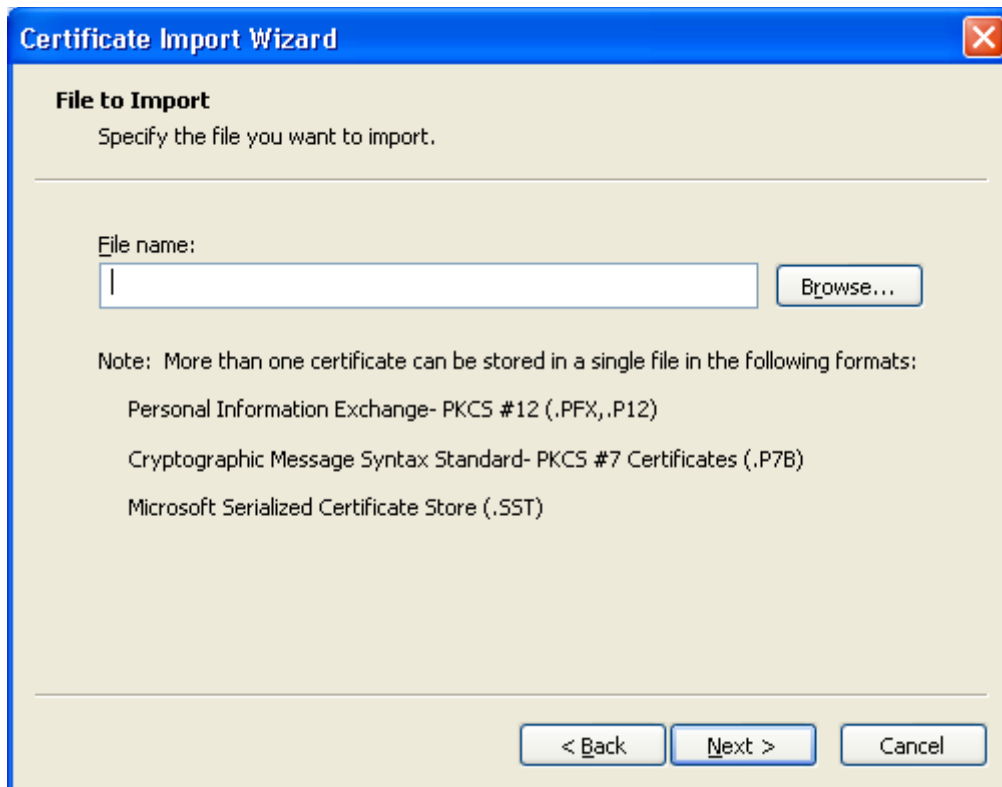
1. Click **Start Menu > Control Panel > Internet Options**.
2. In the **Internet Properties** screen select the '**Content**' tab and then click the '**Certificates**' button.



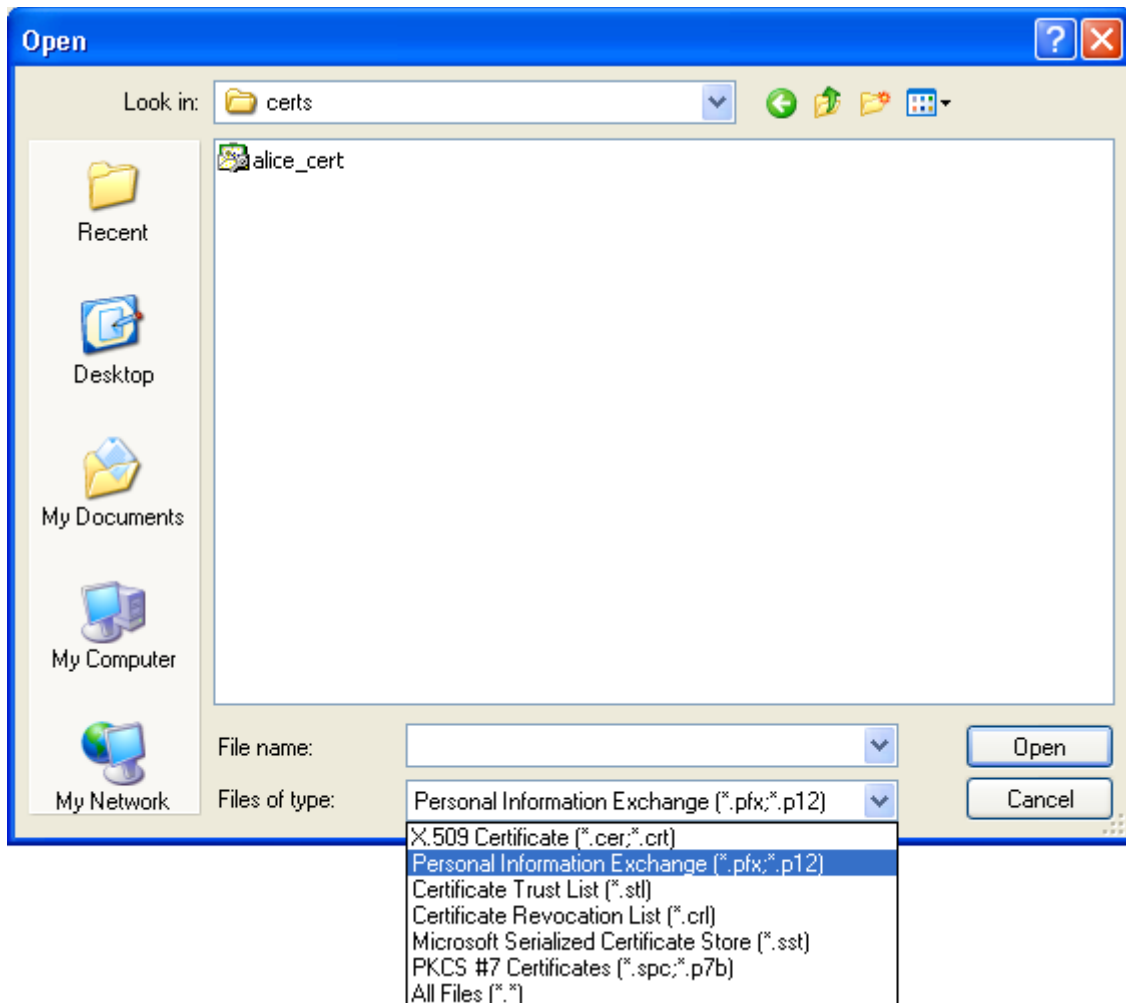
3. In the **Certificates** interface, make sure the '**Personal**' tab is selected, click '**Import**' and then click '**Next**'.



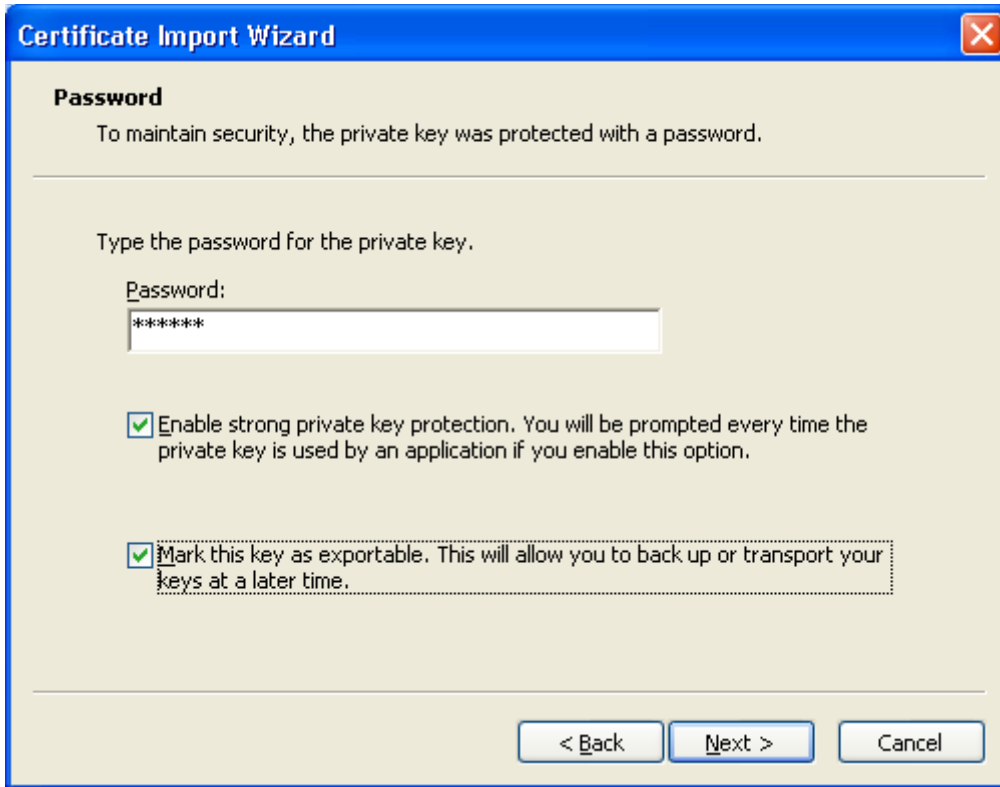
4. Click '**Browse**' in the next step and navigate to the location of your PKCS12 certificate file.



5. Now you need to change type of the file, select '**Personal Information Exchange (.p12)**' from the drop down box, locate your certificate file (.p12) and click '**Open**' (see below).



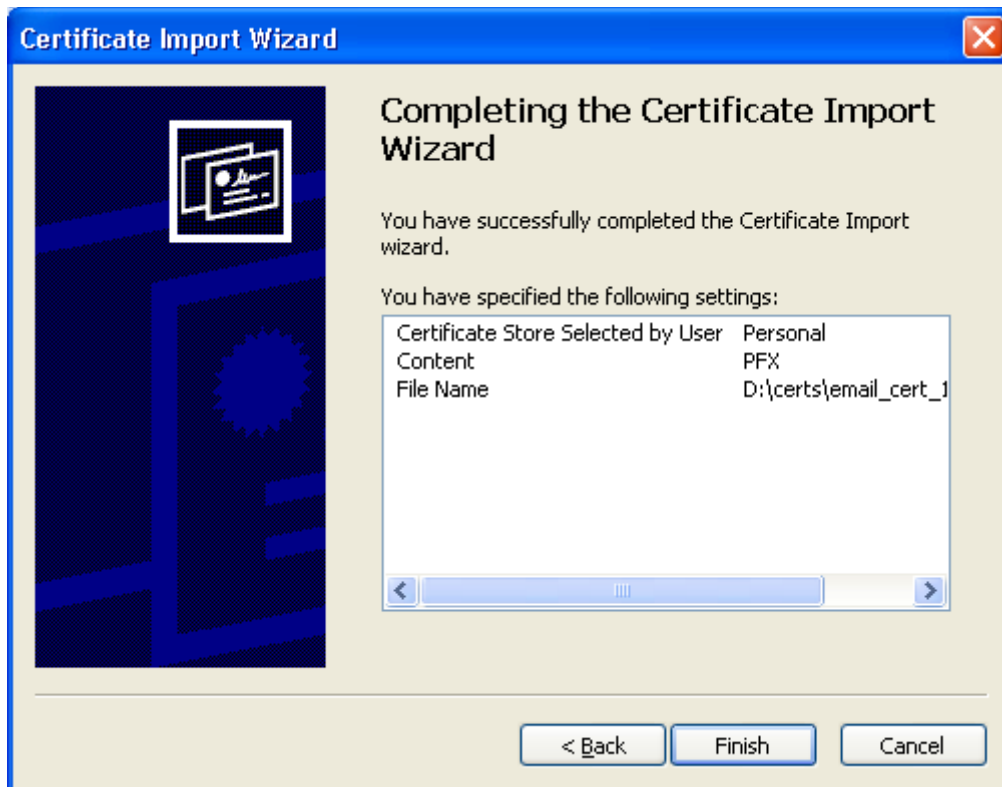
6. After locating your certificate file, click **Next**. To complete the installation process, you are required to enter the PIN (password) you set up for the certificate during the enrollment process. If you have forgotten your password, contact your system administrator who will be able to reset it for you.



- 7. Next you will be prompted to choose the certificate store for your certificate. Unless your administrator has specified otherwise, you should leave this at the default **Place all certificates in the following store** option.



- 8. Click '**Next**' to proceed to the review and confirm stage:



9. Click **Finish** to complete the process. The certificate will be imported.

10. Select the security level for storing the Private Key in your system and click **OK**.



That's it. You have successfully imported your digital certificate into Safari.

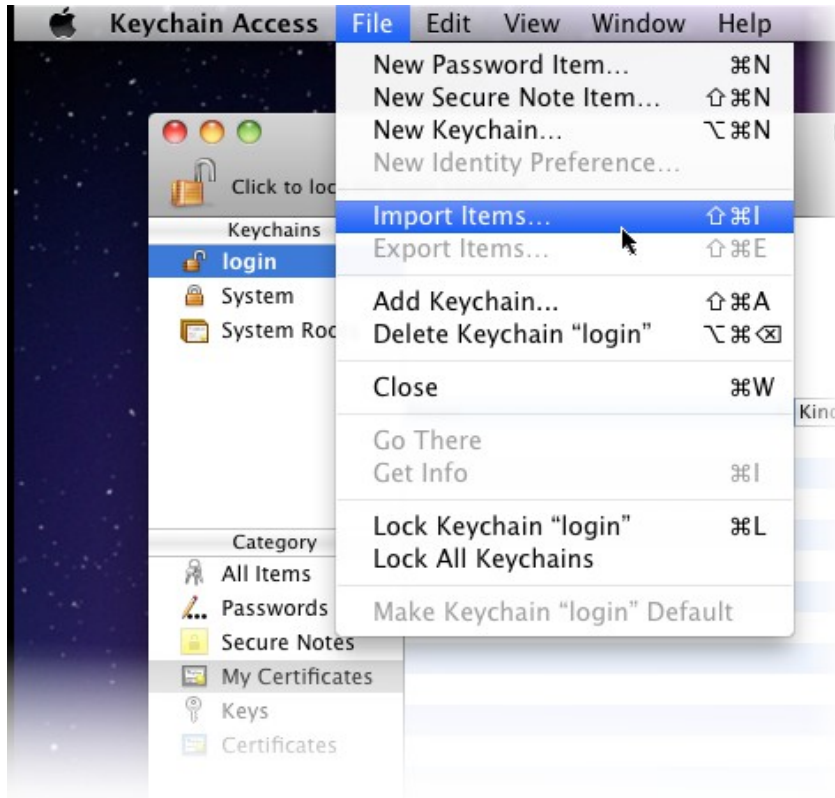
Importing Your Certificate into Safari on Mac OS X

- If you have originally downloaded the certificate through Safari then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import' the certificate into Safari by following the steps given below.

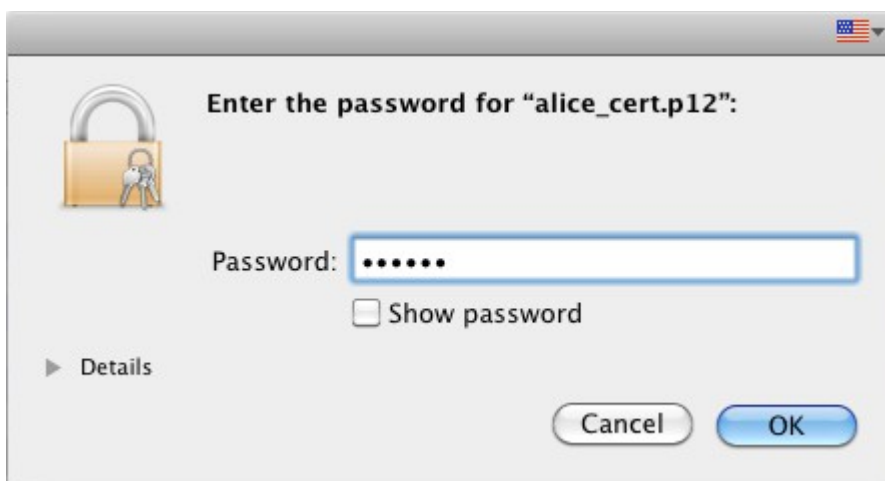
Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

Safari uses the Keychain Access utility built into Mac OS to manage digital certificates.

1. Click '**Applications**' > '**Utilities**' > '**Keychain Access**'
2. Under '**Keychains**' on the left, select '**Login**' then '**File**' > '**Import Items...**'

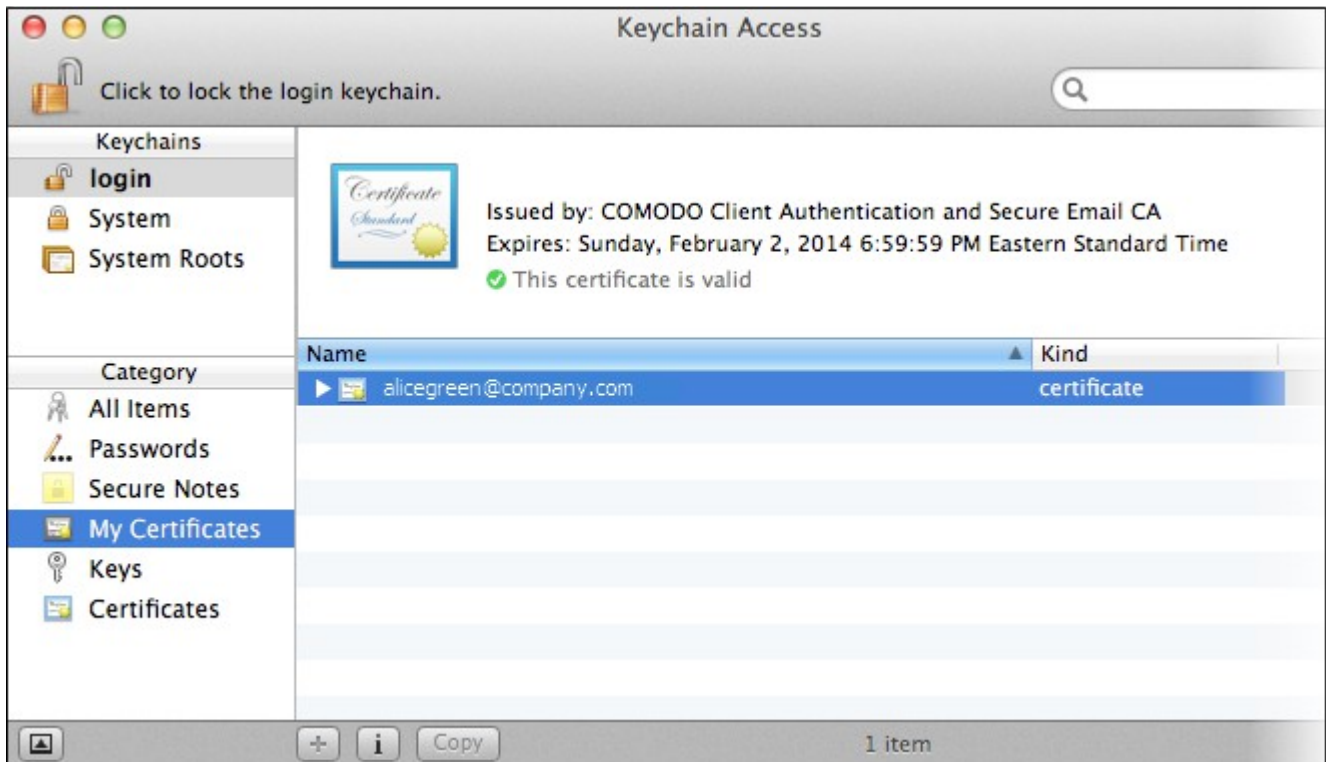


3. Navigate to the location of your saved certificate file and click '**Open**'.



4. Enter the key pair's password and click '**OK**'. **Note:** If prompted whether to trust certificates issued by your CA automatically, select the **Always Trust** option to trust and install your certificate.

The certificate will be installed and can be viewed by clicking **Category** > **My Certificates** in the Keychain Access utility.



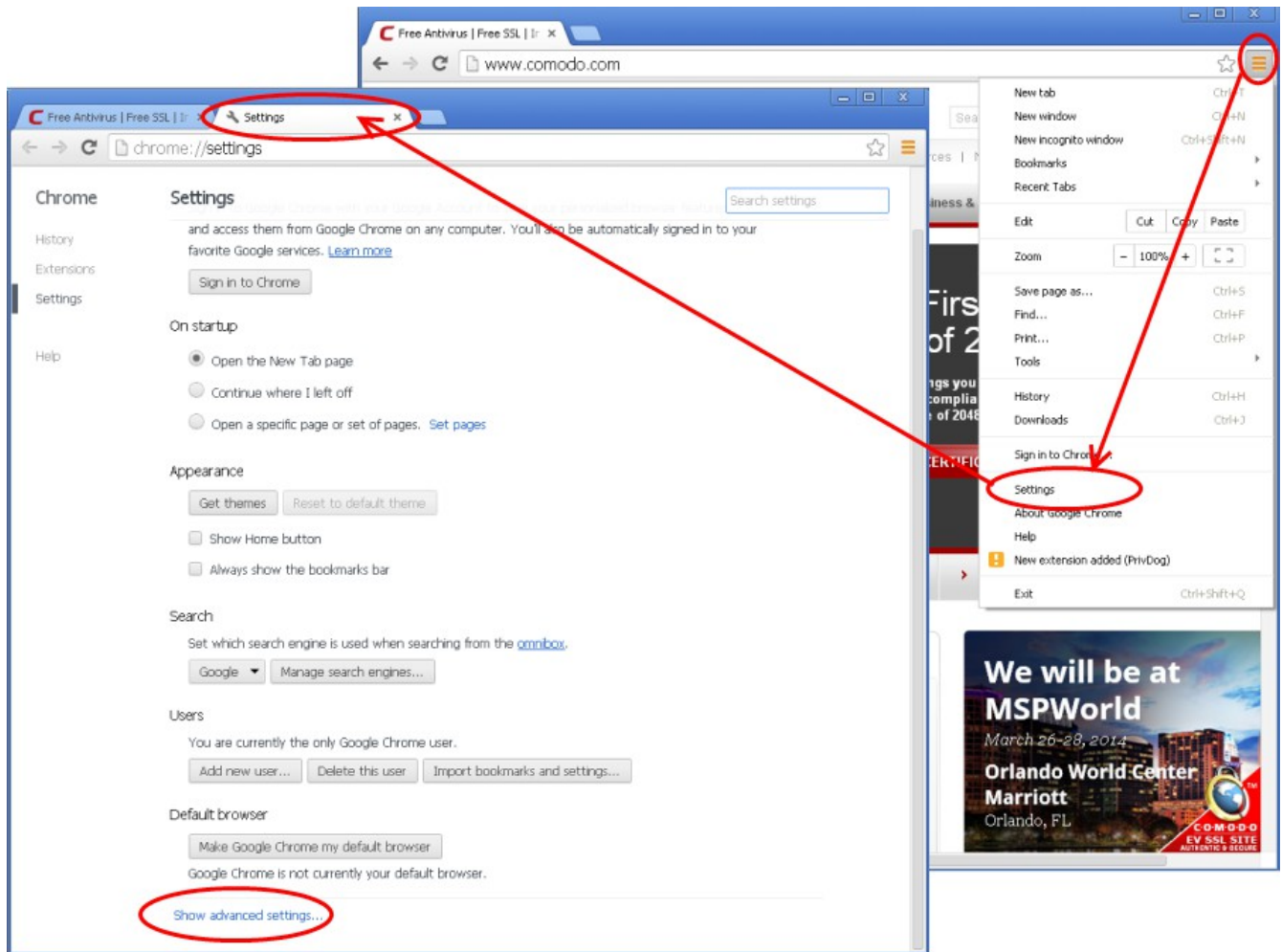
That's it. You have successfully imported your digital certificate into Safari.

Importing Your Certificate into Google Chrome on Windows

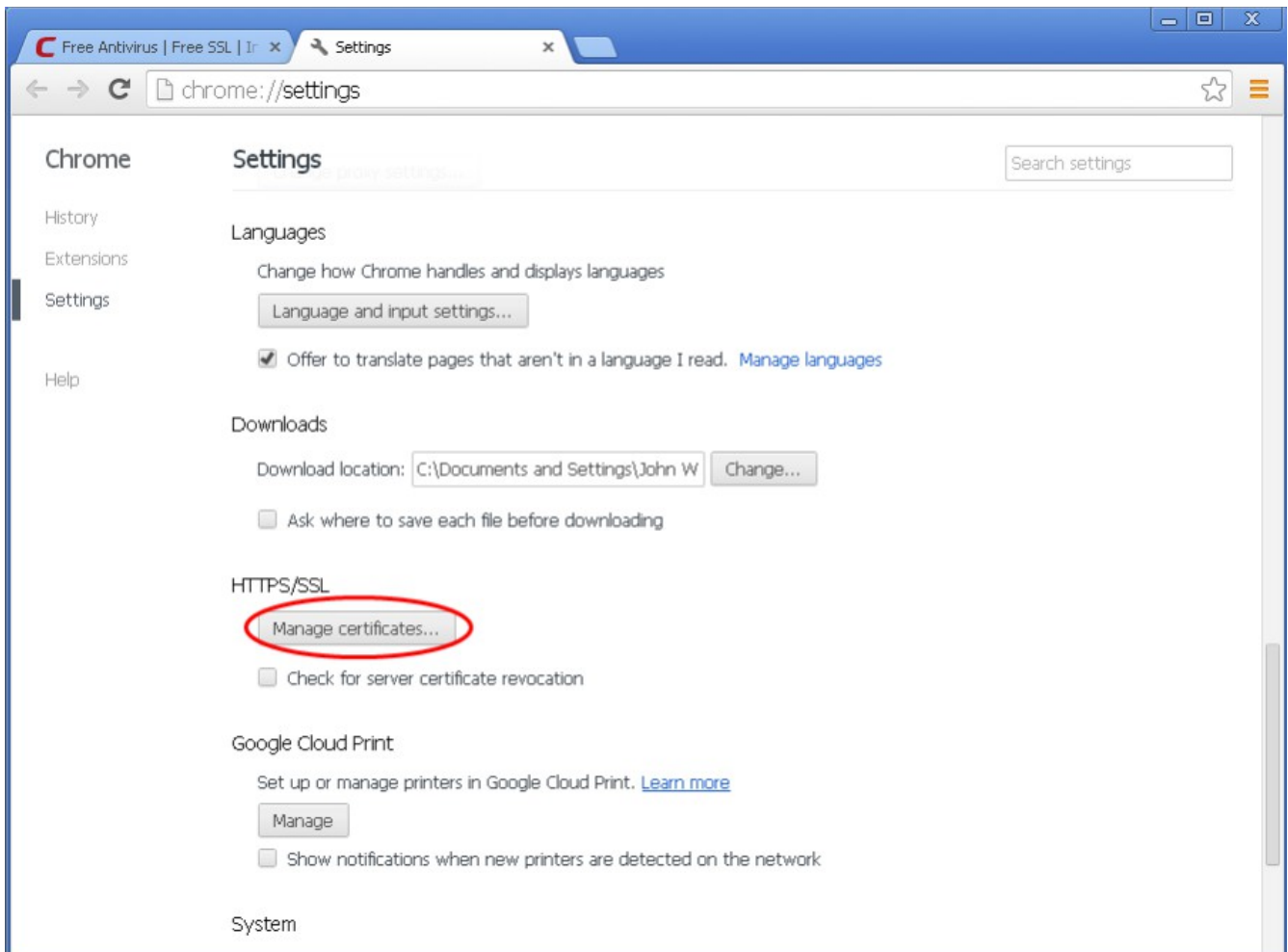
- If you have originally downloaded the certificate through Chrome then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Chrome by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

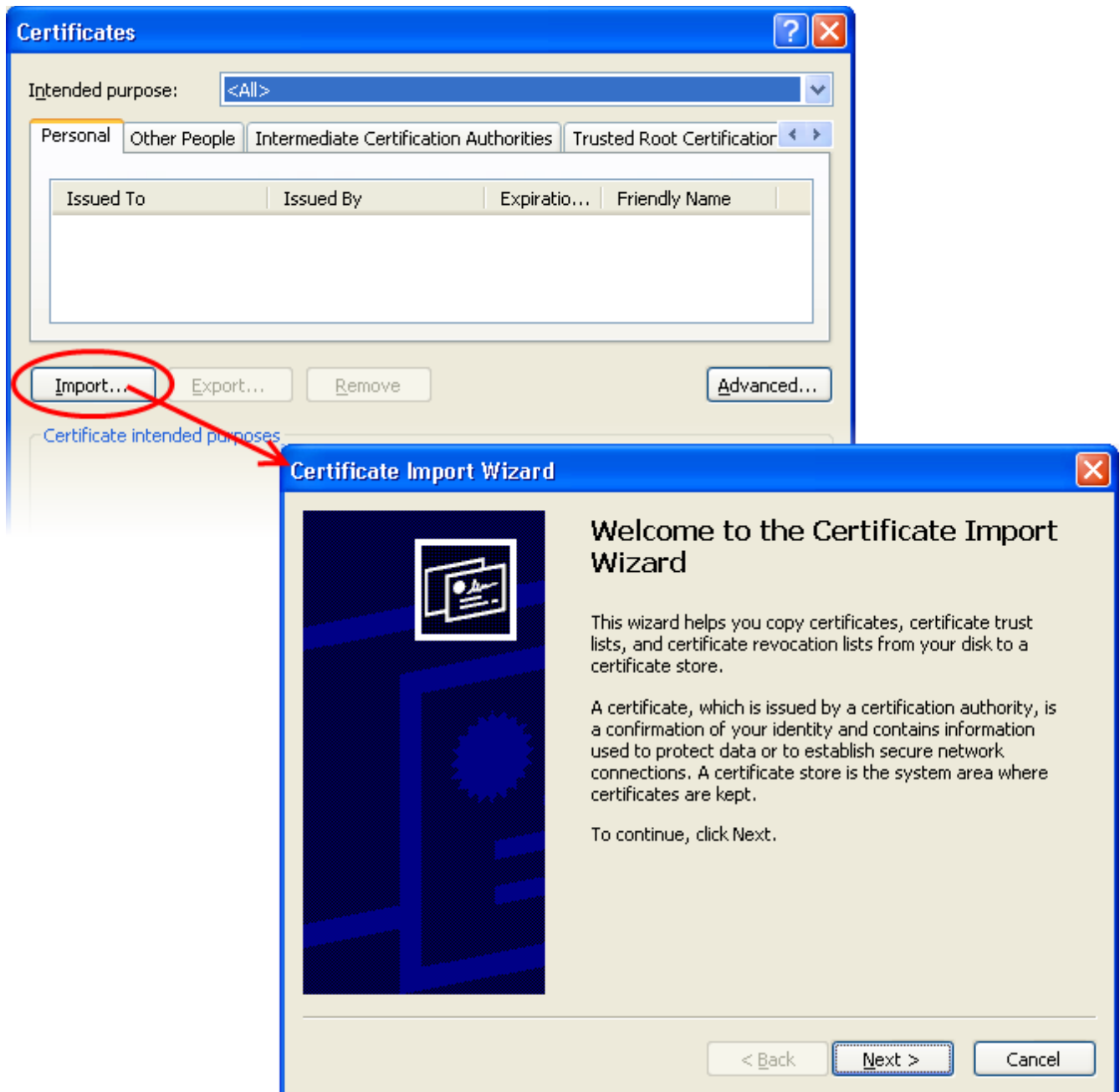
1. Open Google Chrome, then click '**Menu icon**' > '**Settings**'.
2. Scroll down and click the **Show Advanced Settings** link.



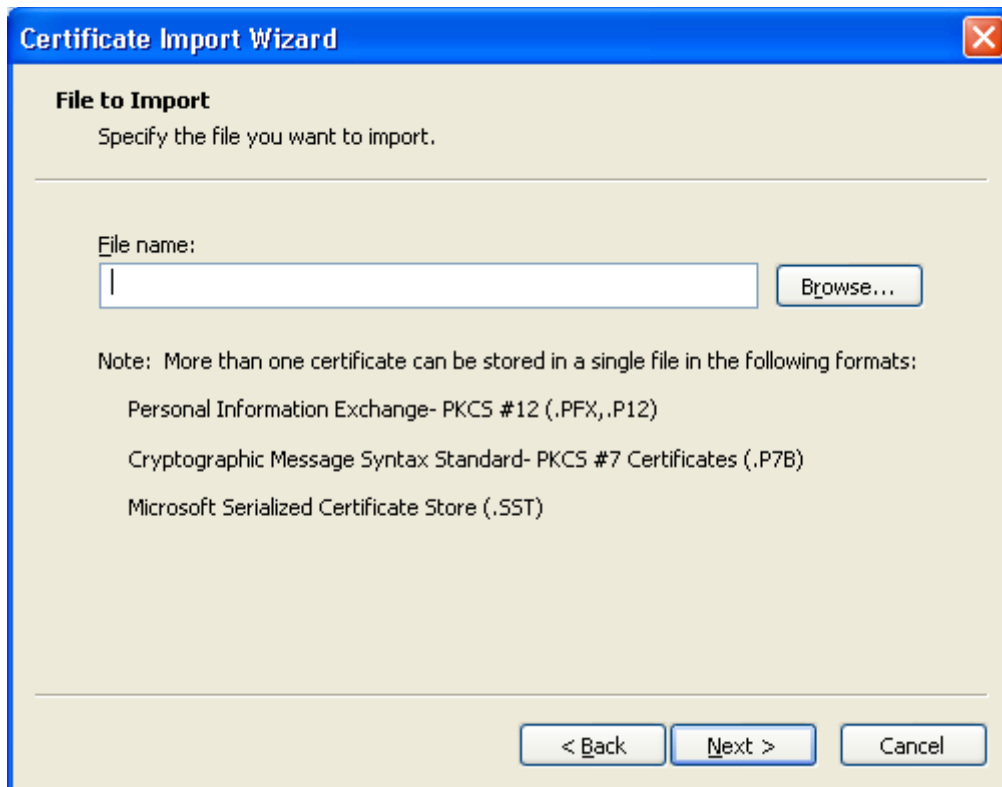
3. Scroll down again and click the **Manage Certificates** button under **HTTPS/SSL**.



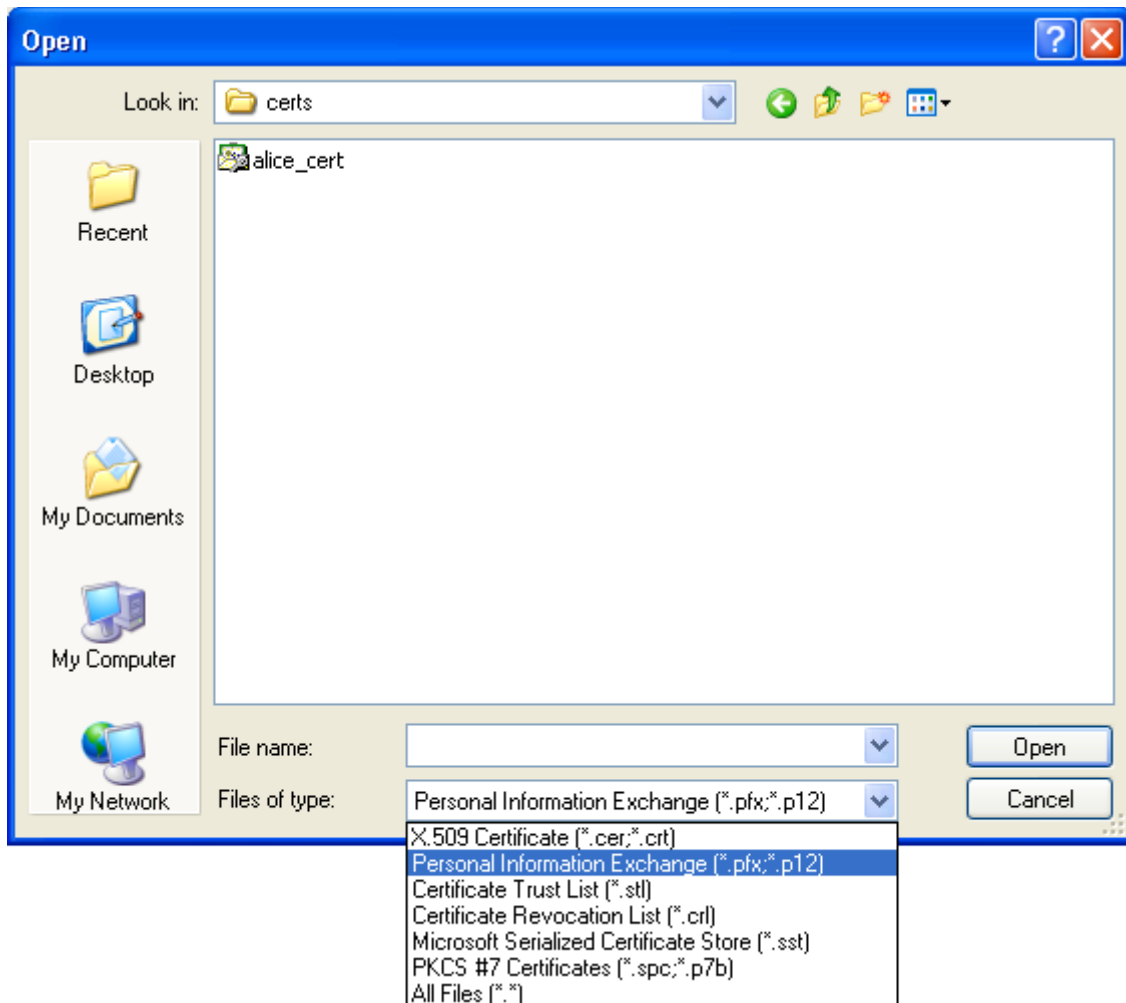
4. In the Certificates interface, make sure the **'Personal'** tab is selected, click **'Import'** and then click **'Next'**.



5. Click '**Browse**' in the next step and navigate to the location of your PKCS12 certificate file.

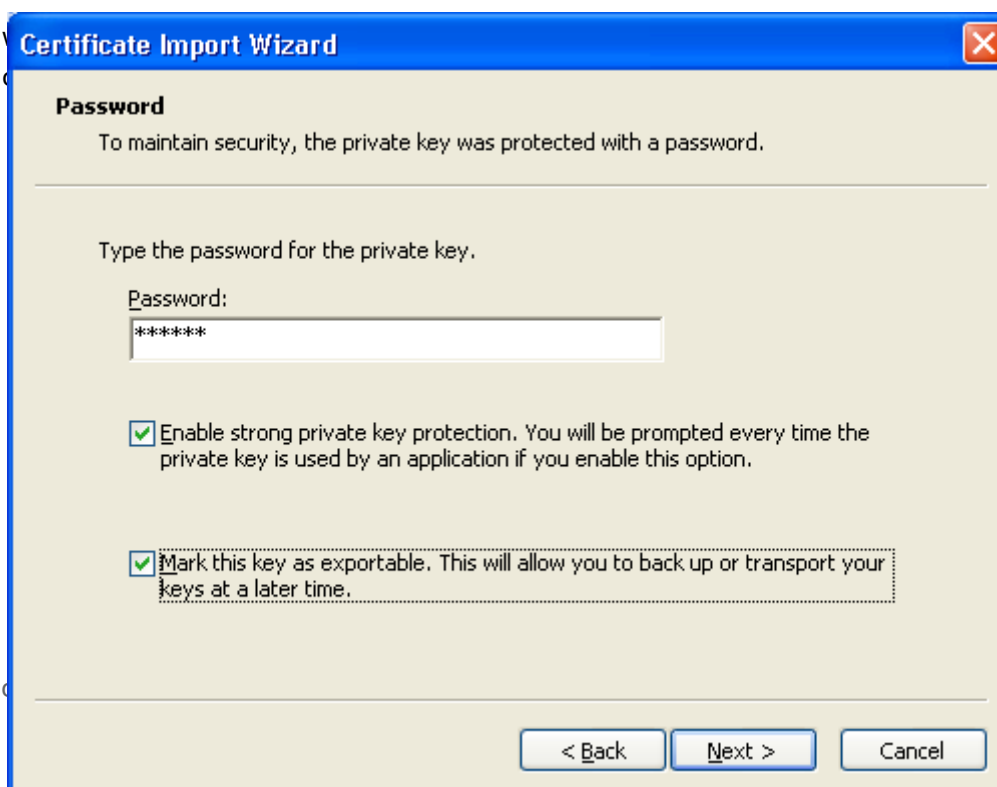


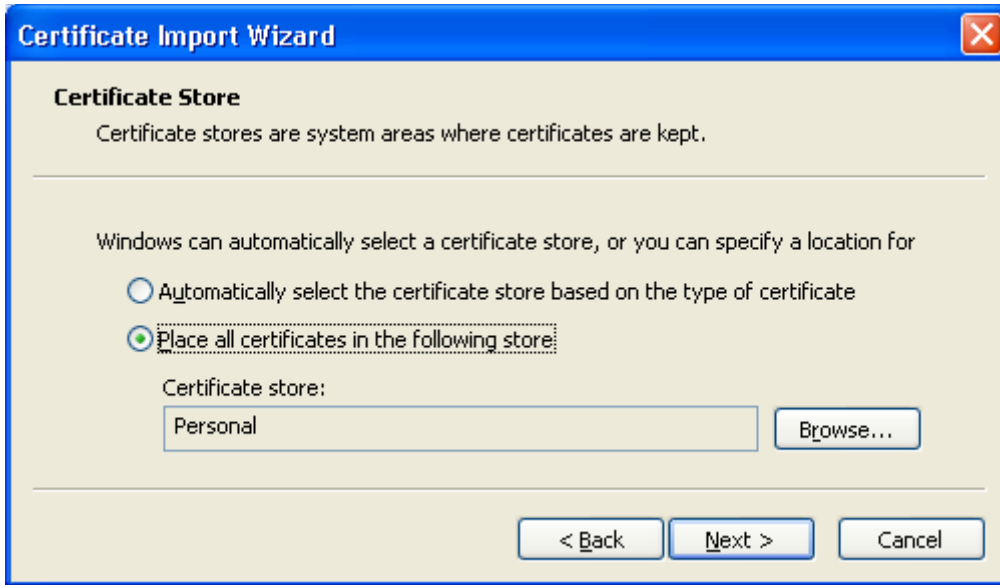
6. Locate your certificate file (.p12) and click '**Open**':



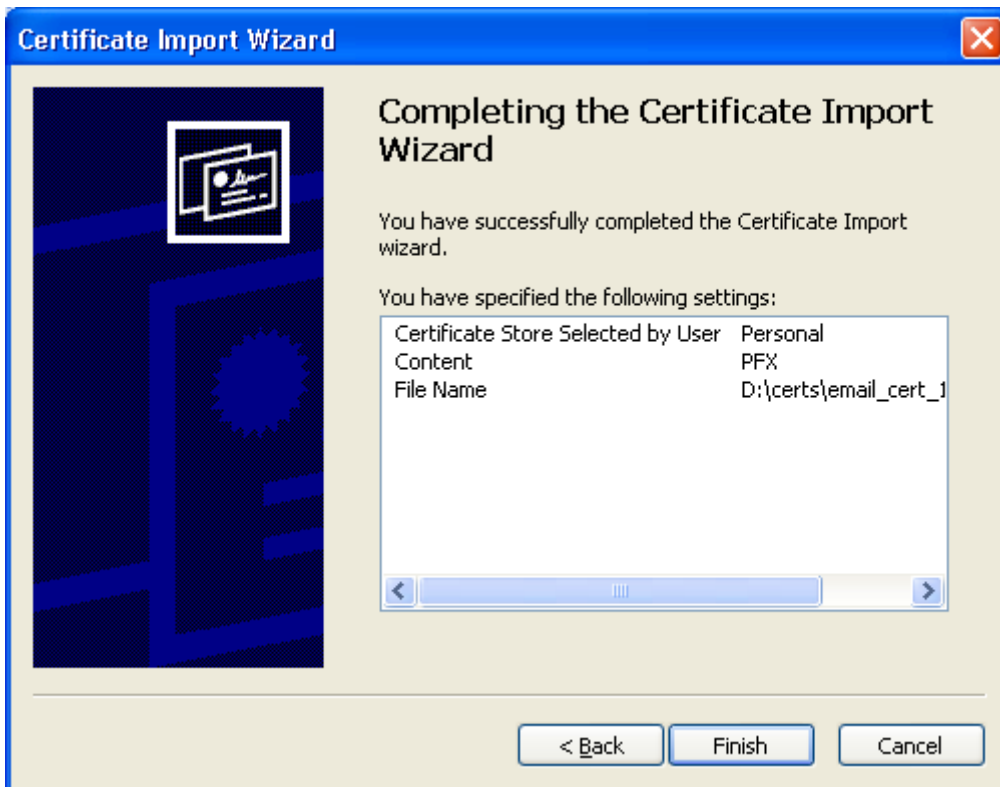
- To complete the installation process, you are required to enter the PIN (password) you set up for the certificate during the enrollment process. If you have forgotten your password, contact your system administrator who will be able to reset it for you.

- Next you will be prompted for the password you specified when the administrator has selected the **Exportable** store option.





9. Click 'Next' to proceed to the review and confirm stage:



10. Click **Finish** to complete the process. The certificate will be imported.

11. Select the security level for storing the Private Key in your system and click **OK**.



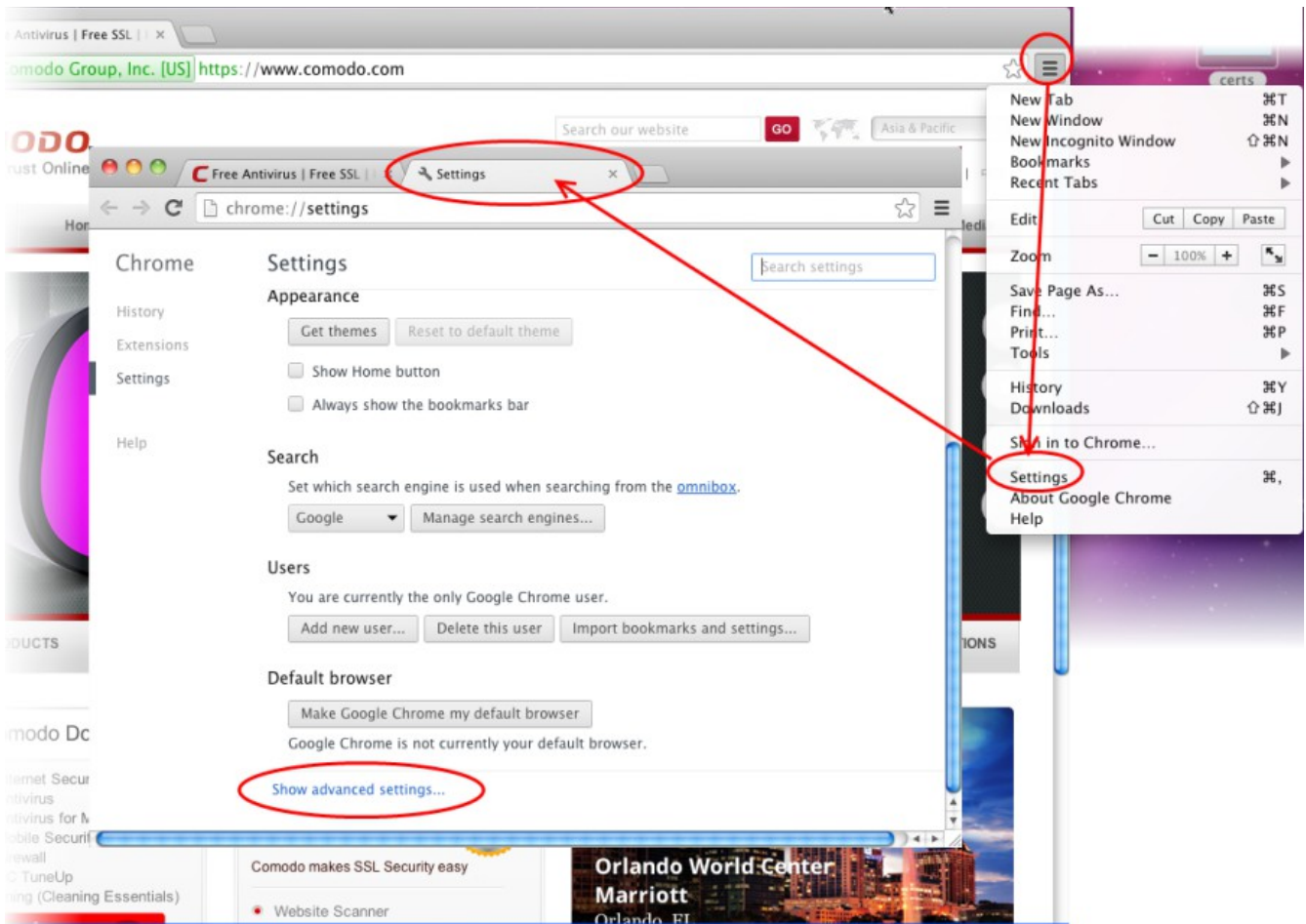
That's it. You have successfully imported your digital certificate into Google Chrome.

Importing Your Certificate into Google Chrome on Mac OS X

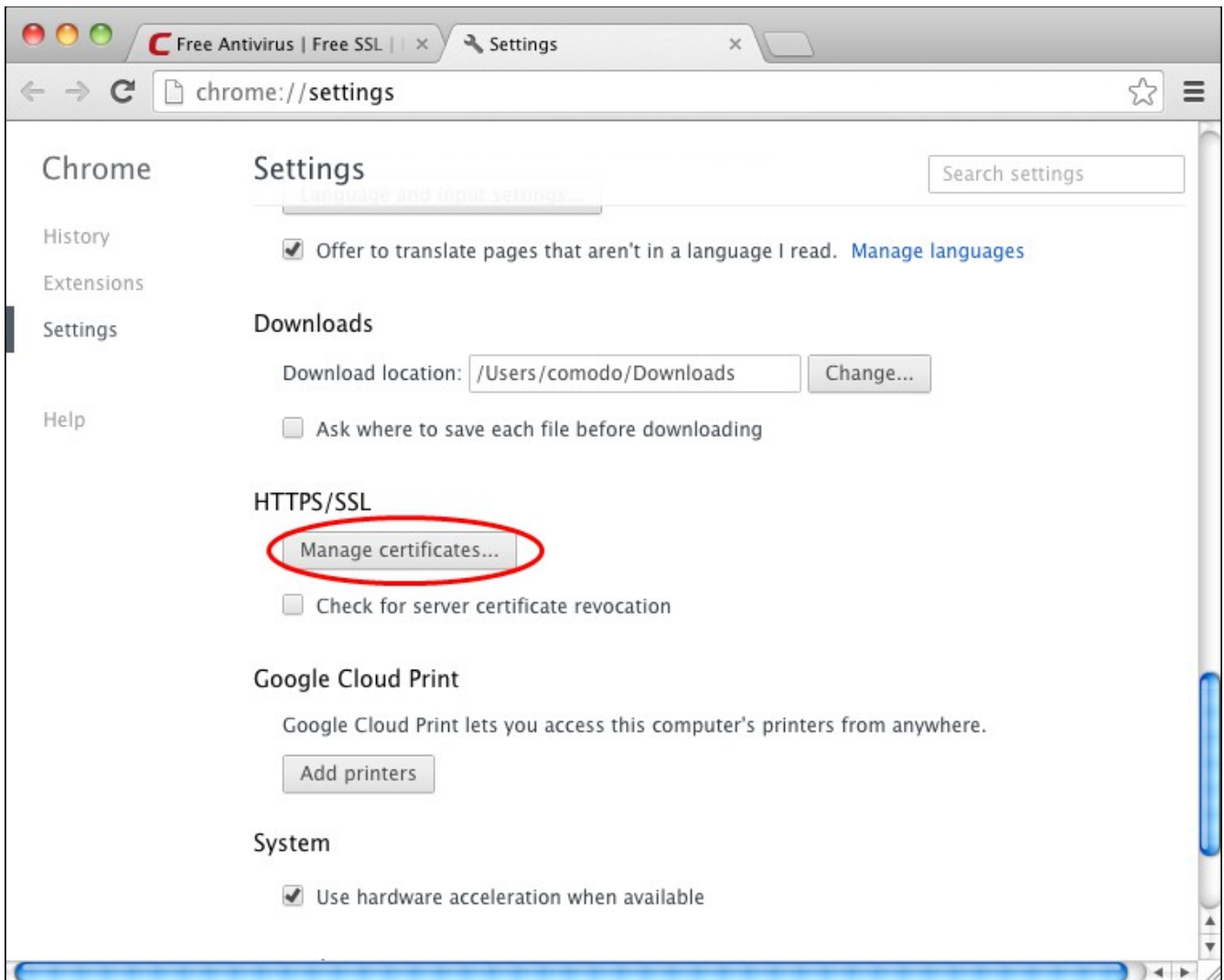
- If you have originally downloaded the certificate through Chrome then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into Chrome by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

1. Open Google Chrome, then click '**Menu icon**' followed by '**Settings**'.
2. Scroll down and click the **Show Advanced Settings** link.

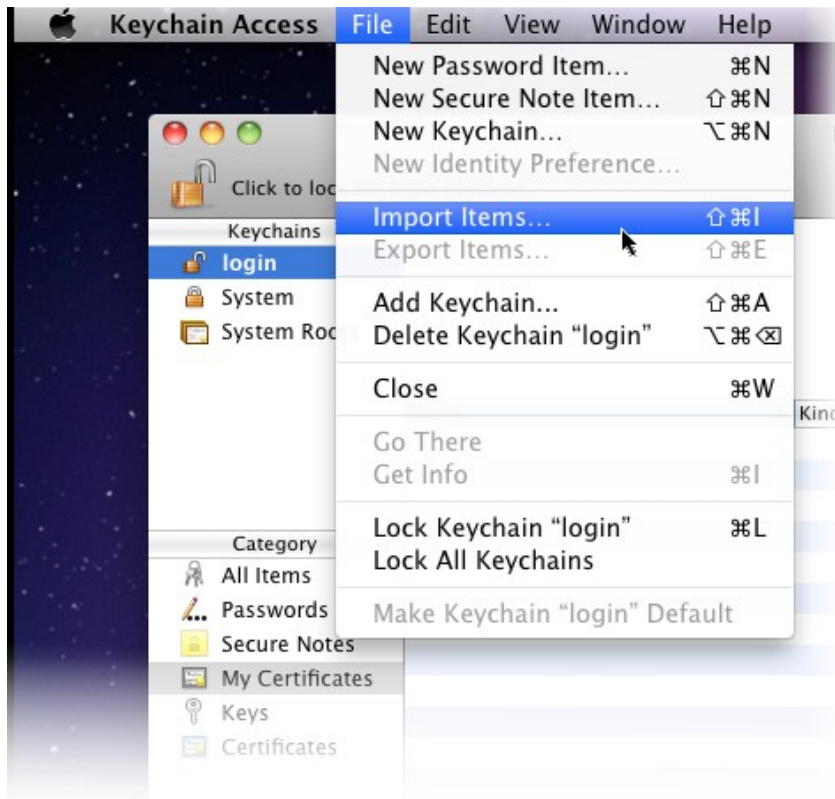


3. Scroll down again and click the **Manage Certificates** button under **HTTPS/SSL**.

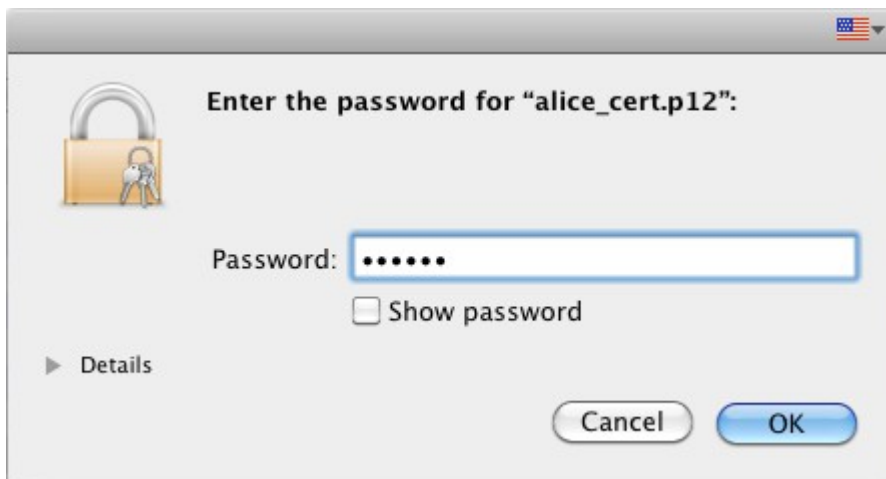


The Keychain Access utility will open. Chrome uses the Keychain Access utility built into MAC OS manage digital certificates.

4. Under '**Keychains**' on the left, select '**Login**' then '**File**' > '**Import Items...**'

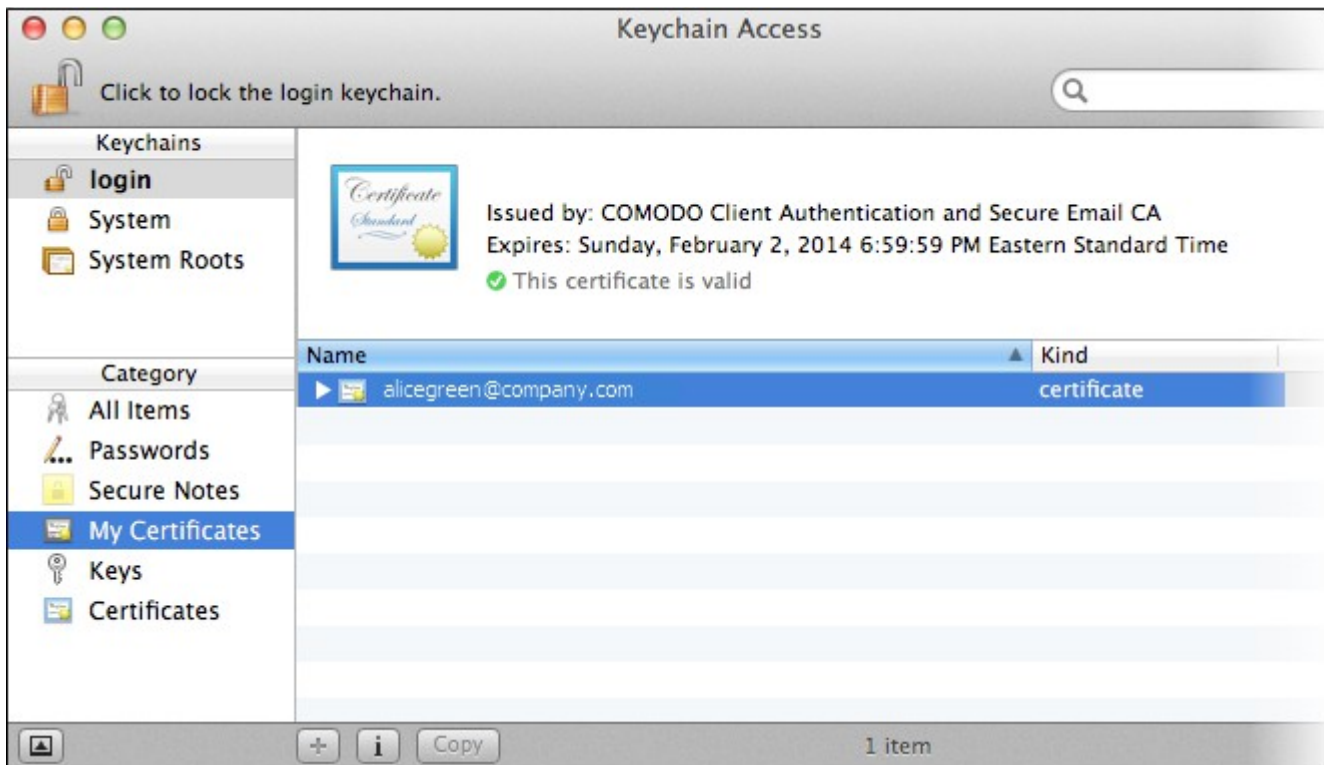


- 5. Navigate to the location of your saved certificate file and click 'Open'.



- 6. Enter the key pair's password and click 'OK'. **Note:** If prompted whether to trust certificates issued by your CA automatically, select the **Always Trust** option to trust and install your certificate.

The certificate will be installed and can be viewed by clicking **Category > My Certificates** in the Keychain Access utility.



That's it. You have successfully imported your digital certificate into Google Chrome

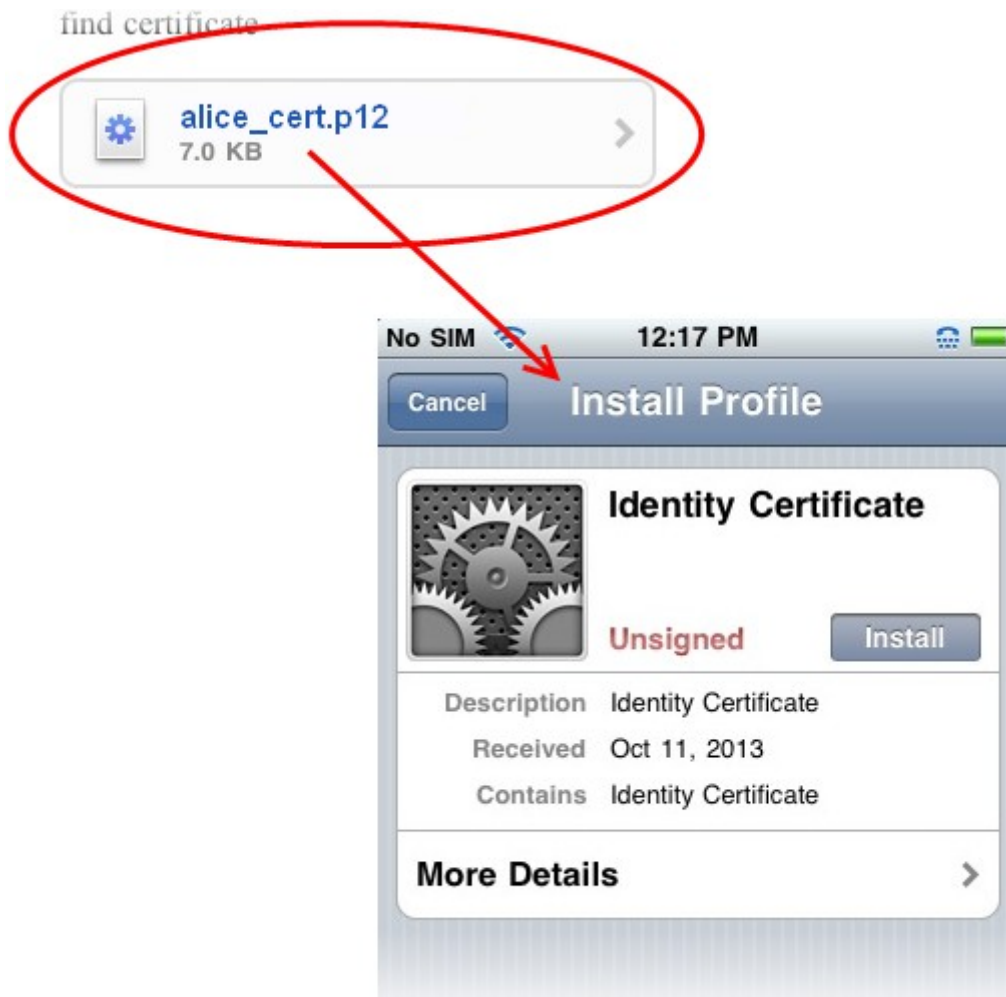
Importing Your Certificate into iOS Devices

This document explains how you can import your InCommon Client Certificate into iOS devices such as the iPhone and iPad.

- If you have originally downloaded the certificate from the iOS device, then it should have been already installed.
- If your certificate is not already installed on the device you are using, then please export it from the machine on which it resides. You then need to transfer it to this device (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into the iOS device by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

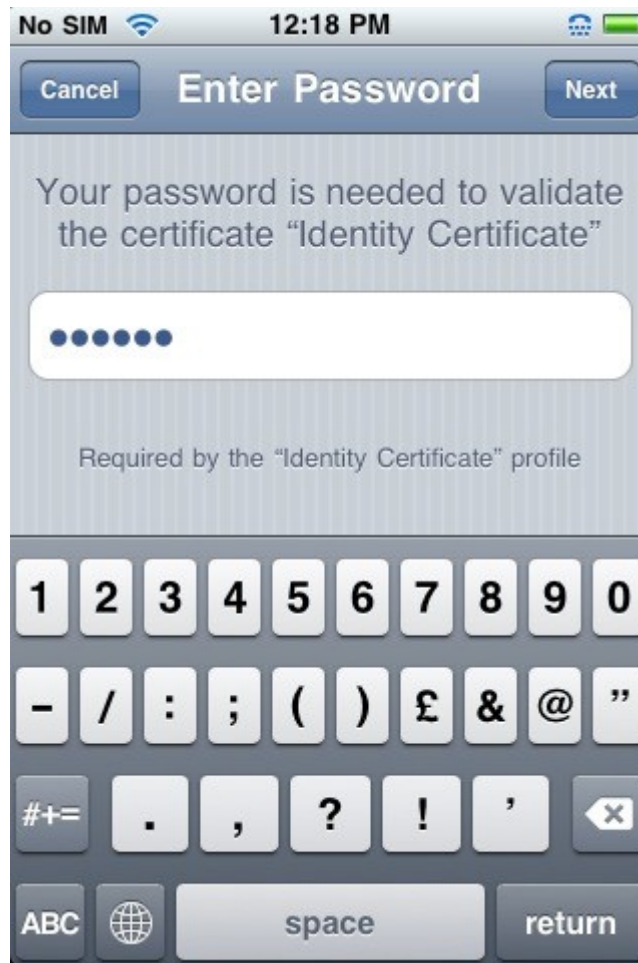
1. Locate and open the .p12 file that contains the certificate you wish to import.



Tap the **Install** button to begin the certificate import wizard.

2. Select **Install Now** then enter the password you set up for the certificate when it was exported.





3. After your password is accepted, iOS will automatically import your certificate. You should see a confirmation dialog similar the one shown below.



4. Tap **Done** to exit the wizard.

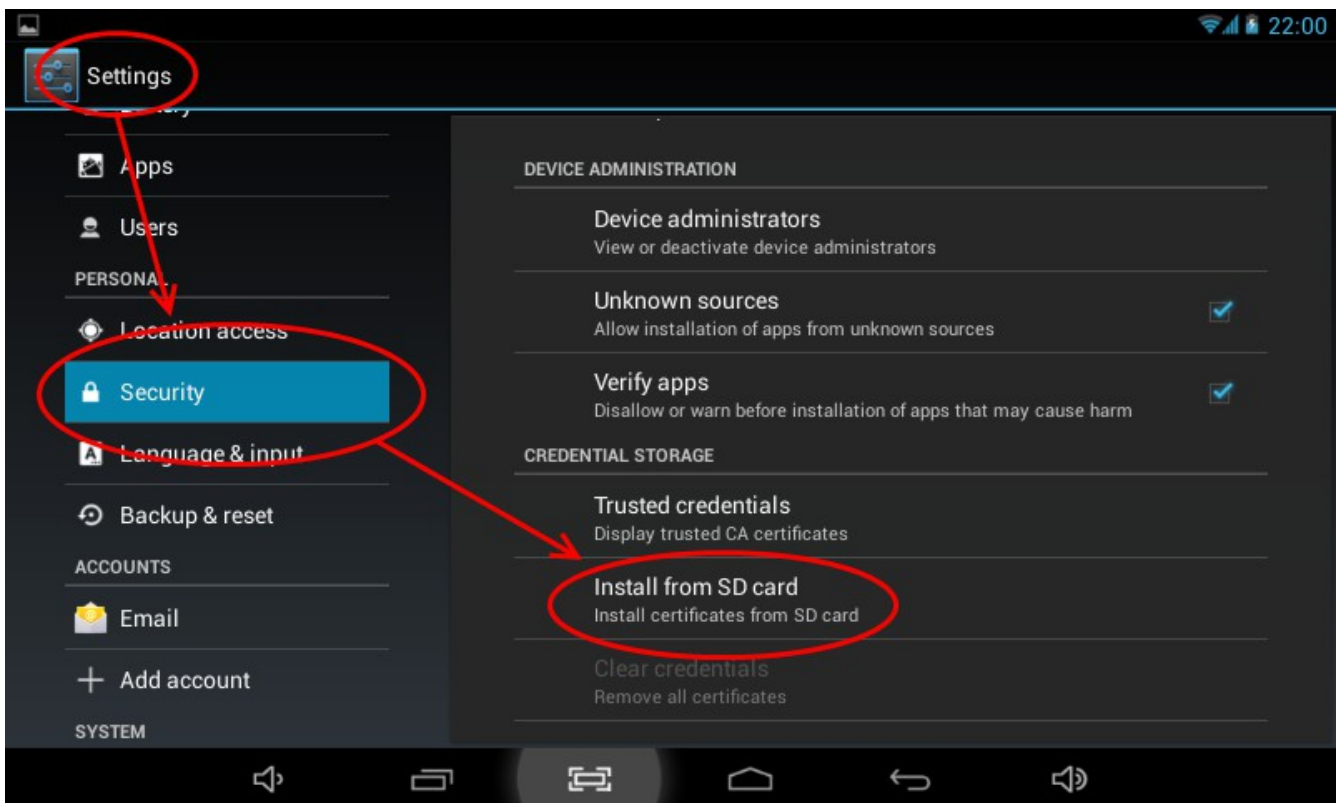
Your certificate is now installed on the iOS device. This certificate can be used to digitally sign and encrypt your emails and/or authenticate your identity.

Importing Your Certificate into Android Devices

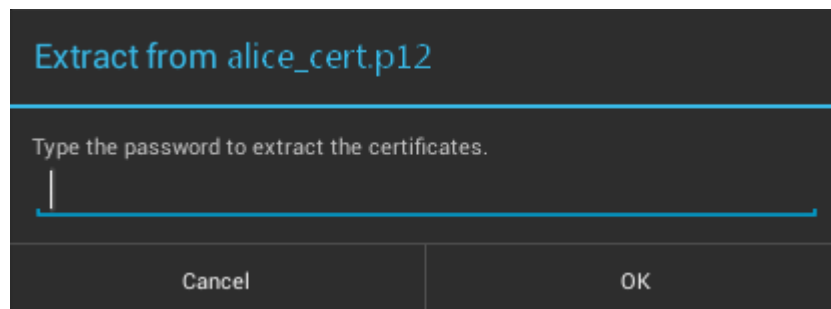
- If you have originally downloaded the certificate from the Android device, then it should have been already installed.
- If your certificate is not already installed on the device you are using, then please export it from the machine on which it resides. You then need to transfer it to this device (email it to yourself or save the certificate file to USB then copy over). You can then import the certificate into the device by following the steps given below.

Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '[Enrollment and Collection of your Certificate](#)' first.

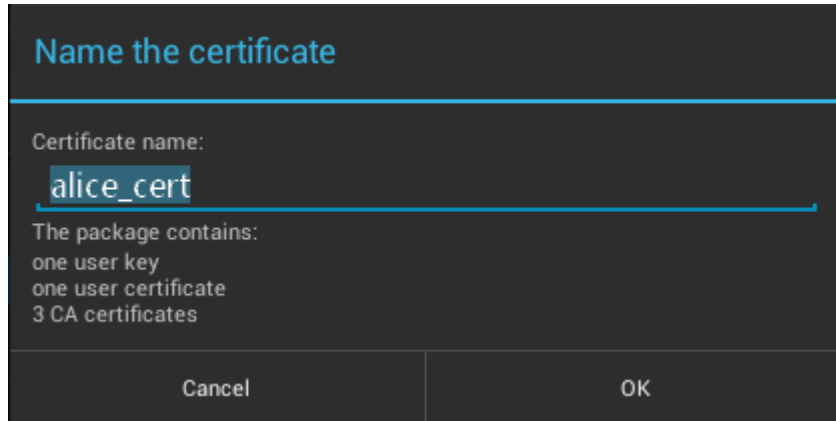
1. Tap **Settings > Security**. Under '**Credential Storage**' select '**Install from SD card**'.



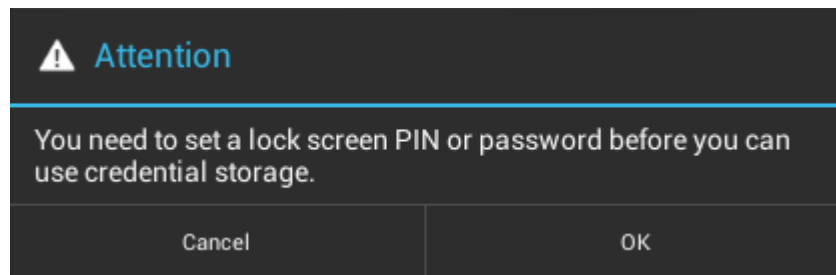
2. Enter the password you set up for the certificate when it was exported and click 'OK'.



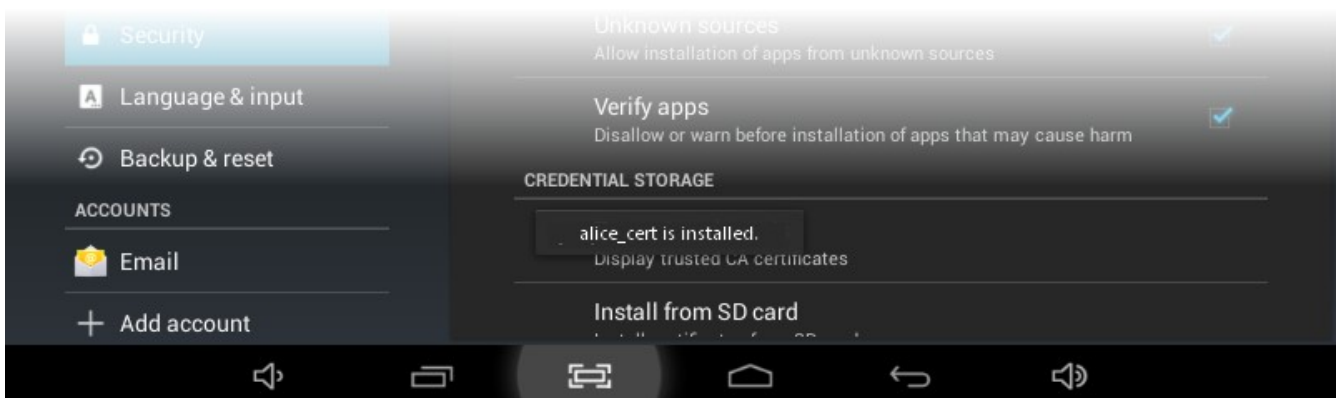
3. In the '**Name the certificate**' screen, enter a friendly name to identify the certificate and tap **OK**.



- If you have not yet set a passcode or pattern to lock your home screen then you will be prompted to do so before proceeding. This is required before you can install your certificate and will be requested in future to access the Android certificate store (Settings > Trusted Credentials). If you have already set a screen passcode this step will be skipped and the certificate will be installed.

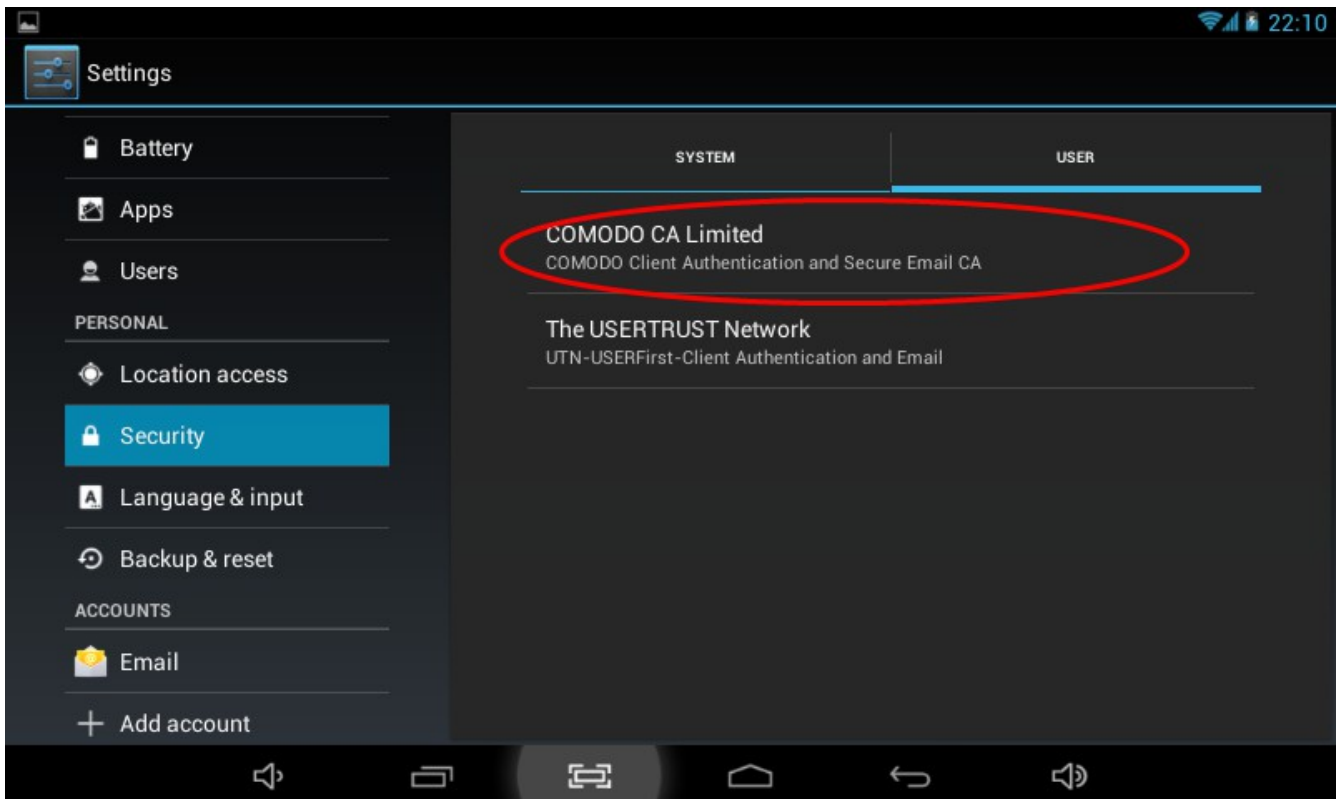


- Click **OK**. The Certificate will be installed.



You can confirm the certificate installation by viewing the User Certificates under Trusted Credentials.

- Open the Settings panel and tap **Security > Trusted Credentials**
- Tap the **User** tab. You will see the list of user authentication certificates installed on your Android device.



Your certificate is now installed on the Android device. This certificate can be used to digitally sign and encrypt your emails and/or authenticate your identity.

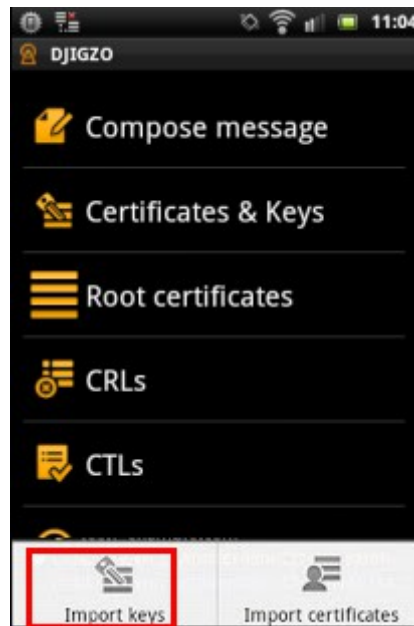
Importing your certificate into Android Djigzo

If you have originally downloaded your certificate to your desktop or laptop then you first need to export it from the computer. When doing this, please make sure you export the private key and include all certificates in the certificate path if possible. You must also specify a strong password to protect the certificate file.

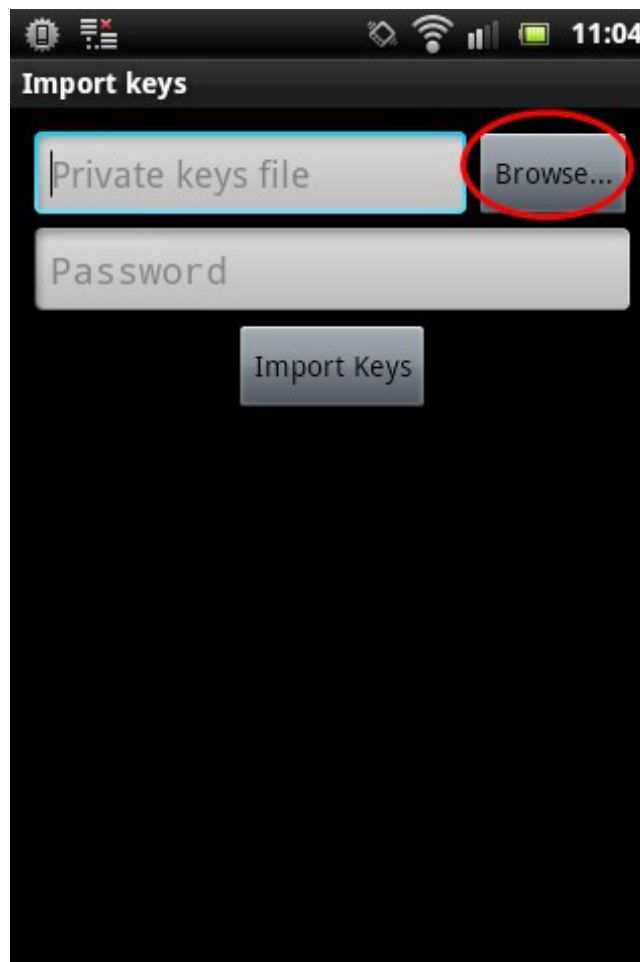
Once exported you can email the certificate file to your Android device or transfer it in some other manner (for example, copy to a USB drive or upload then download from online storage).

Before importing your certificate into Djigzo, make sure that you have configured your mail account with an existing Android email client such as Google Mail app, K9 or the default mail client.

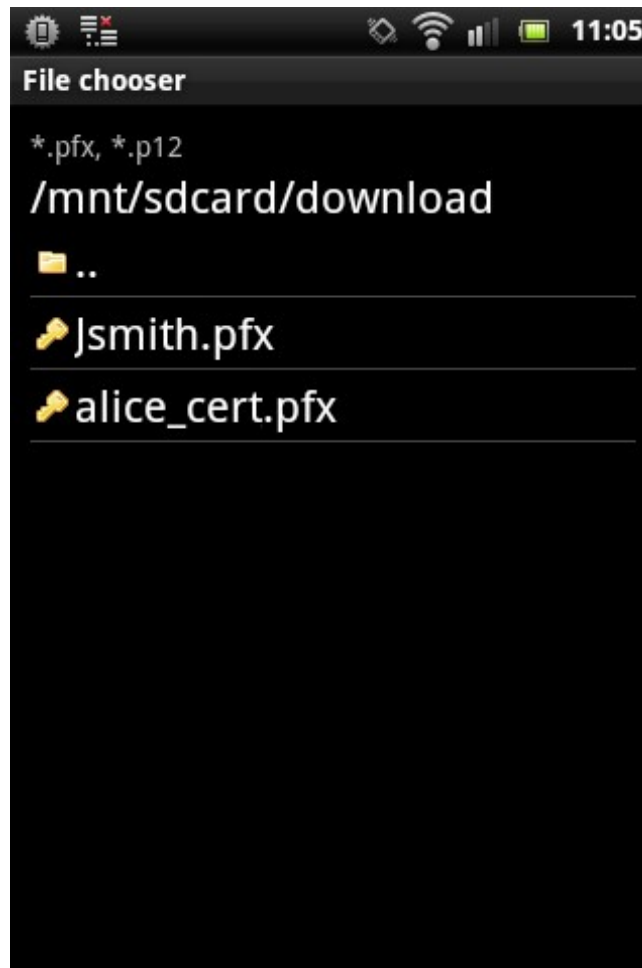
1. Open Djigzo app and tap menu button in the device.
2. Tap **'Import Keys'**.



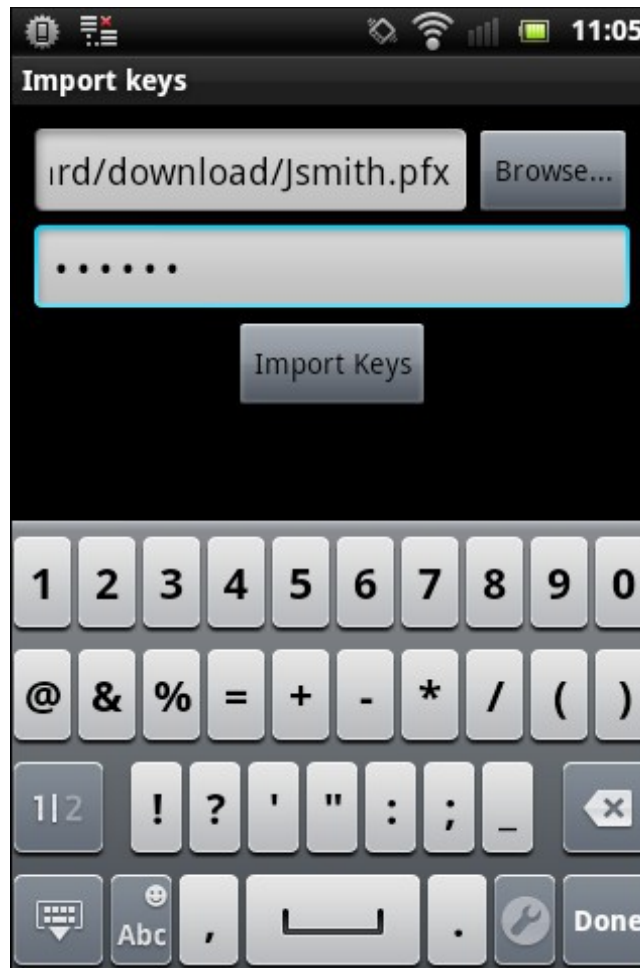
3. Tap '**Browse**' and navigate to the location where the certificates are stored.



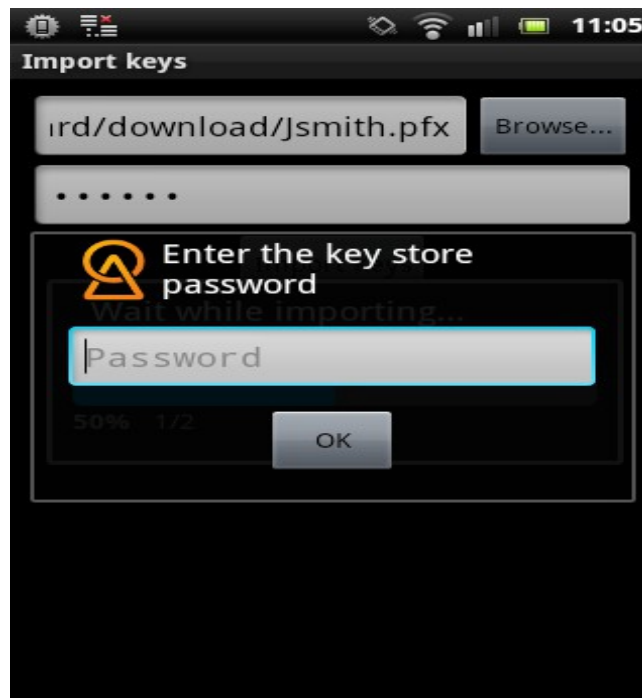
4. Tap on the certificate that you want to import.



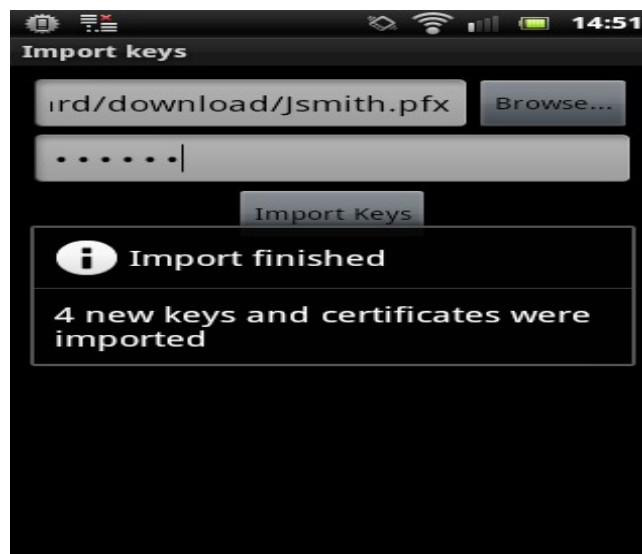
5. Enter the password you set up for the certificate when it was exported and tap '**Import Keys**'.



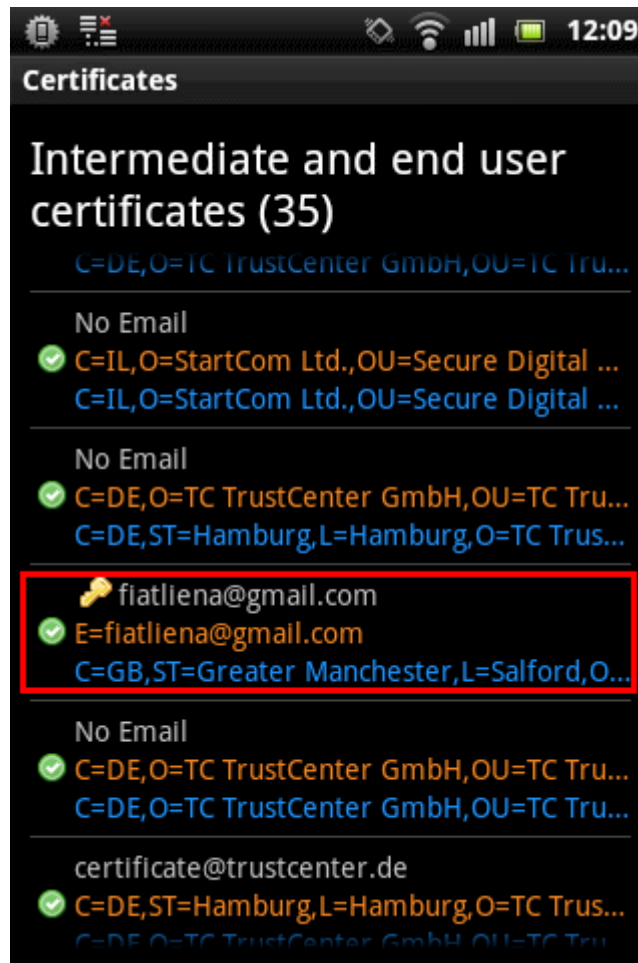
6. Next, you have to enter the password for the key store that was set during the first certificate import. **Note:** This key store password is different from the password used for importing certificates.



The certificate will be imported and the following message will be displayed.



The imported certificate can be viewed in the **Certificate & Keys** screen.



Now the certificate can be used for signing and encrypting messages for the account that you have configured in the device.