



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

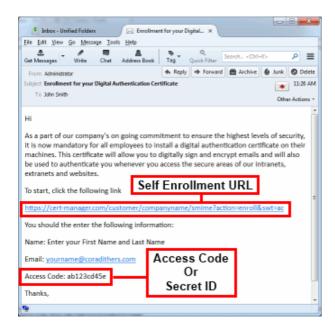
Firstly, your administrator should have sent you a provisioning email. The exact procedure to follow will depend on the type of email you have received:

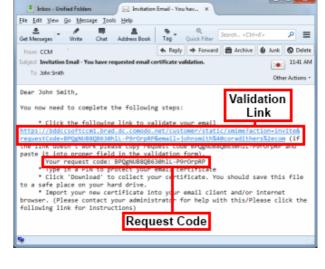
Enrollment Mails (2 Options):

Invitation Mail

- <u>Click here if your email contains an Access Code</u>
- Click here if your email contains a Request Code and a Validation Link

- OR
- Click here if your email contains a Secret ID





Invitation Email

Enrollment Type Email

Enrollment by Access Code

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



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: *	•••••	i
Re-type Self Enrollment Passphrase: *	•••••	
	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	•

- 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.
ВАСК

... 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.



					• X
📩 Inbox - Unified Folders 🛛 🖂 Validation Email - You hav 🗙					
<u>File Edit View Go M</u> essage <u>T</u> ools <u>H</u> elp		_			
Get Messages Write Chat Address Book	► Tag ►	Quick Filter	Search <ctrl< th=""><th>!+K></th><th>₽≡</th></ctrl<>	!+K>	₽≡
From CCM	🐟 Reply	➡ Forward	Archive	🌢 Junk	O Delete
Subject Validation Email - You have requested email ce	ertificate va	lidation.			12:04 PM
To John Smith					_
				Othe	er Actions 🔹
Dear John Smith,					^
<pre>Other Actions - Dear John Smith, You now need to complete the following steps: * Click the following link to validate your email <u>https://cert-manager.com</u> /customer/companyname/smime?action=validate& requestCode=1p0jyqXBFaSMQ4th2Qa4nTvQB&email=johnsmith%40coradithers%2ecom (if the link doesn't work please copy request code 1p0jyqXBFaSMQ4th2Qa4nTvQB and paste it into proper field in the validation form). Your request code: 1p0jyqXBFaSMQ4th2Qa4nTvQB * Type in a PIN to protect your email certificate * Click 'Download' to collect your certificate. You should save this file to a safe place on your hard drive. * Import your new certificate into your email client and/or internet browser. (Please contact your administrator for help with this/Please click the following link for instructions)</pre>					
聖					
Valid	lation om				

Validation emailThe 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: *	1p0jyqXBFaSMQ4th2Qa4nTvQB]
Email: *	johnsmith@coradithers.com]
Certificate Type: *	High Persona Validated Cert]
PIN:		i
Re-type PIN:]
Select address fields to remove f	rom the certificate.	
	Address as it will appear in certificate	Remove
Address1:	Mount Road	
Address2:		
Address3:		
City:	Riverdale	
State or province:	Alabama	
Postal Code:	123456	
Employee ID: *		
	VALIDATE CANCEL	

- 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



Enrollment by Secret ID Certificate Manager Digital Certificate Download **Enter your Digital ID information** Fill in all required fields Email Address: * johnsmith@coradithers.com Secret identifier: * ab123cde45f Certificate Type: * -High Persona Validated Cert Annual Renewal Self Enrollment Passphrase The Annual Renewal Self Enrollment Passphrase is a unique phrase that protects you against unauthorized action on your Digital ID. Do not share it with anyone. Do not lose it. You will need it when you want to revoke or renew your Digital ID. Annual Renewal Self Enrollment Passphrase: Confirm Annual Renewal Self Enrollment Passphrase: Password: This value will be used as password to protect access to your Digital ID. Password: Confirm Password: Select address fields to remove from the certificate. Address as it will appear in certificate Remove 100, Raleigh Street Address1: Address2: Address3: Riverdale City: Alabama State or province: 123456 Postal Code: Comodo ePKI Certificate Manager Agreement – EV Enabled THIS AGREEMENT CONTAINS A BINDING ARBITRATION CLAUSE. PLEASE READ THE THAT YOU UNDERSTAND IT, THAT YOU AGREE TO AND ACCEPT THE TERMS AS + PRINT I accept the terms and conditions.* Scroll to bottom of the agreement to activate check box ENROLL CANCEL

- Enter the Secret ID from your enrollment email in the 'Secret Identifier' field.
- Type your internal corporate E-mail address in the 'E-Mail Address' field.



- 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.
- <u>Click here</u> 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.

	- 0 <u>X</u>
Inbox - Unified Folders	
<u>F</u> ile <u>E</u> dit <u>V</u> iew <u>G</u> o <u>M</u> essage <u>T</u> ools <u>H</u> elp	
Get Messages Write Chat Address Book Tag Quick Filter Search < Ctrl+K>	∈ ۹
← Reply → Forward 🔂 Archive 🌢 Ju	ink 🔕 Delete
From CCM <support@cert-manager.com></support@cert-manager.com>	
Subject Invitation Email - You have requested email certificate validation.	12:59 PM
To John Smith	Other Actions 🔹
Dear John Smith,	^
You now need to complete the following steps: * Click the following link to validate your email https://cert-manager.com/customer/static/smime?action=invite&requestCode= BPOgNUB8QB630hlL-P9rOrpRP&email=johnsmith%40coradithers%2ecom (if the link doesn't work please copy request code BPOgNUB8QB630hlL-P9rOrpRP and pa into proper field in the validation form). Your request code: BPOgNUB8QB630hlL-P9rOrpRP * Type in a PIN to protect your email certificate * Click 'Download' to collect your certificate. You should save this fi a safe place on your hard drive. * Import your new certificate into your email client and/or internet br (Please contact your administrator for help with this/Please click the foll link for instructions)	≡ ile to rowser.
22	ai

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.



ser Registration		
Code: *	BPQgNUB8QB630hIL-P9rOrpRP	7
Email: *	johnsmith@coradithers.com	Ĩ
Certificate Type:	High Persona Validated Cert]
PIN:		0
Re-type PIN:		Ĩ
Self Enrollment Passphrase: *		0
Re-type Self Enrollment Passphrase: *		Ĩ
elect address fields to remove fi	rom the certificate.	-
	Address as it will appear in certificate	Remo
Address1:	100, Raleigh Street	
Address2:		
Address3:		
City:	Riverdale	
State or province:	Alabama	
Postal Code:	123456	
Employee ID: *		
	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 PRINT	-

- 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.

Certificate Manager	
Digital Certificate download	
Please save your digital certificate in safe place.	
	DOWNLOAD CANCEL

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

Opening johnsmith_coradithers_com.p12
You have chosen to open:
johnsmith_coradithers_com.p12
which is: p12 File (6.8 KB)
from: https://cert-manager.com
What should Firefox do with this file?
Open with Browse
Save File
Do this <u>a</u> utomatically for files like this from now on.
OK Cancel





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 <u>Step 1</u> 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
Outlook 2010 / 2013	Internet Explorer	• <u>iPhone/iPad</u>
Outlook 2003	<u>Comodo Dragon</u>	Android Device – Native
Windows Live Mail	<u>Comodo IceDragon</u>	
Mozilla Thunderbird	• <u>Firefox</u>	<u>Android – Djigzo App</u>
Mac OS X Mail/Apple Mail	• <u>Opera</u>	
• <u>Eudora</u>	• <u>Safari (Windows)</u>	
• <u>Bat!</u>	• <u>Safari (Mac)</u>	
Outlook Express 5 & 6	<u>Chrome (Windows)</u>	
Mozilla SeaMonkey	<u>Chrome (Mac)</u>	

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'



0 3 9 -

Certificate Manager

File Home Send /	/ Receive Folder Vie	w
Save As	Outlook Options	
凹 Save Attachments	General Mail	Help keep your documents safe and your computer secure and healthy.
Open	Calendar	Protecting your privacy
Print	Contacts	Microsoft cares about your privacy. For more information about how Microsoft Outlook helps to protect your privacy, please see the privacy statements.
	Tasks	Show the Microsoft Outlook privacy statement
Help	Notes and Journal	Office.com privacy statement
Options	Search	Customer Experience Improvement Program
Exit	Mobile	Security & more
_	Language	Learn more about protecting your privacy and security from Office.com.
	Advanced	Microsoft Windows Security Center Microsoft Trustworthy Computing
	Customize Ribbon	
	Quick Access Toolbar	Microsoft Outlook Trust Center
	Add-Ins	The Trust Center contains security and privacy settings. These settings help keep your computer secure. We recommend that you do not Trust Center Settings
	Trust Center	change these settings.
		OK Cancel

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 Di	gital ID		×
💿 Import existing [Digital ID from a file		
	D from the file to your computer. You mu ered while exporting the certificate to this		
Import File:	E:\certs\alice_cert.p12	Browse	
Password:	•••••		
Digital ID Name:	Alice Green		
Export your Digit Export the Digital 1 this information.	tal ID to a file ID information into a file. Enter a passwor	d to help protect	
Digital ID;		Select	
Filename:		Browse	
Password:			
Confirm:			
Microsoft Inter	net Explorer 4.0 Compatible (low-security))	
Delete Digital II	O from system		
	ОК	Cancel	

4. Click 'OK'.

Importing a n	ew private exchange key
	An application is creating a Protected item.
	CryptoAPI Private Key
	Security level set to Medium Set Security Level
	OK Cancel Details

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.

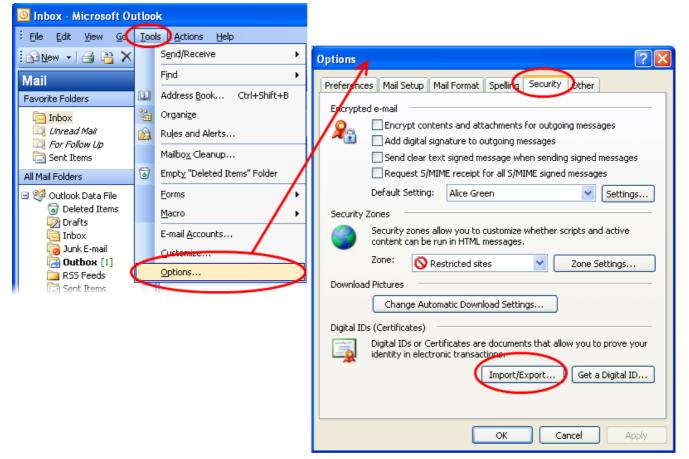


Importing Your Certificate into Outlook 2003

- 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 '<u>Enrollment and Collection of your Certificate</u>' 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.

' |



Import/Export Di	gital ID	×
	Digital ID from a file ID from the file to your computer. You mus ared while exporting the certificate to this	
Import File:	E:\certs\alice_cert.p12	Browse
Password:	•••••	
Digital ID Name:	Alice Green	
Export your Digit Export the Digital I this information.	D information into a file. Enter a password	l to help protect
	D'Ill'Offiduor into a nie, Enter a passwort	10 neip protect
Digital ID:		Select
Filename:		Browse
Password:		
Confirm:		
Microsoft Intern	net Explorer 4.0 Compatible (low-security)	
🔄 Delete Digital II) from system	
	ОК	Cancel

4. Click 'OK'.

Importing a new private exchange key				
	An application is creating a Protected item.			
A	CryptoAPI Private Key			
	Security level set to Medium Set Security Level OK Cancel Details			

- 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.

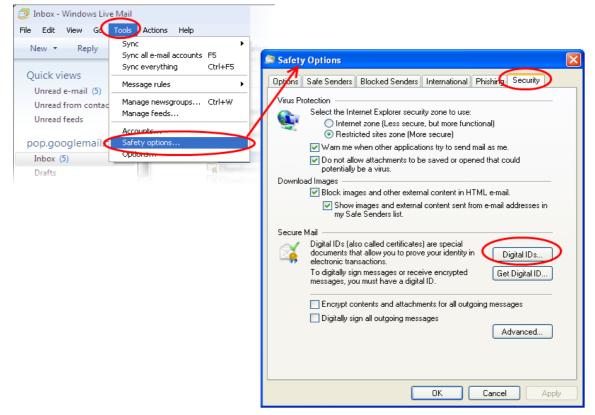


Importing Your Certificate into Windows Live Mail

- 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 '<u>Enrollment and Collection of your Certificate</u>' first.

- Open Windows Live Mail and click 'Tools' > 'Safety Options...'. (If the menu bar is not displayed, click on the Menus 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'.



Certificates	? 🗙
Intended purpose: <a>All> Personal Other People Intermediate Certification Authorities	Trusted Root Certification
Issued To Issued By Expiration	o Friendly Name
Import Export Remove	Advanced
Certificate Import Wizard	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next.
	< <u>B</u> ack Next > Cancel

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



File to Import Specify the file you want to import. Eile name: I Browse 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)
Ejle name: Image: Browse 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)
Browse 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)
Browse 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)
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)
Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (SST)
Microsoft Denalized Certificate Store (JDT)
< <u>B</u> ack <u>N</u> ext > Cancel

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).



Open				? 🗙
Look in:	🚞 certs	O Ø	P [
📁 Recent	🔊 alice_cert			
Desktop				
My Documents				
My Computer				
	File name:		*	Open
My Network	Files of type:	Personal Information Exchange (*.pfx;*.p12)	~	Cancel
		X.509 Certificate (*.cer;*.crt) Personal Information Exchange (*.pfx;*.p12) Certificate Trust List (*.stl) Certificate Revocation List (*.crl) Microsoft Serialized Certificate Store (*.sst) PKCS #7 Certificates (*.spc;*.p7b) All Files (*.*)		

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.



Certificate Import Wizard	×
Password To maintain security, the private key was protected with a password.	
Type the password for the private key. <u>Password:</u>	
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.	
< <u>B</u> ack <u>N</u> ext > 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
< <u>B</u> ack <u>N</u> ext > Cancel

8. Click 'Next'.



Certificate Import Wizard		
	Completing the Certif Wizard You have successfully completed the wizard. You have specified the following sett Certificate Store Selected by User Content File Name	Certificate Import
	< <u>B</u> ack Fi	nish Cancel

- 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.

Importing a new private exchange key				
	An application is creating a Protected item.			
	CryptoAPI Private Key			
	Security level set to Medium Set <u>Security Level</u>			
	OK Cancel <u>D</u> etails			

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 '<u>Enrollment and Collection of your Certificate</u>' 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'.

Options							
신			<u>_</u>	9	0	۲ ن ن	
General	Display	Composition	Chat	Security	Attachments	Advanced	
General Reading	g & Display Nel	work & Disk Space	Update Cert	ificates			
When a serve	r requests my p	ersonal certificate					
		:ally 🕑 <u>A</u> sk me					
	\checkmark						
View <u>C</u> ertifica	ates	ation Lists Va	lidation <u>S</u> e	curity Devices			
			Mose statute and a statute				
9	Certificate M	lanager					
(Y	our Certificates	People Servers	Authorities Ot	hers			
		ficates from these	THE CONTRACTOR IN CONTRACTOR IN CONTRACTOR	010000011-1			
	Certificate Na		ecurity Device		Number	Expires On	E.
			scuricy Device	Jeriai	Number	Expires Of	Lŧ
	Alice Gre	een Sol	tware Security	Device 6C:3B:	1C:63:99:F6:84:	. 10/21/2014	
	View	Backup	Backup All	Import	Delete		
							ОК



- 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.

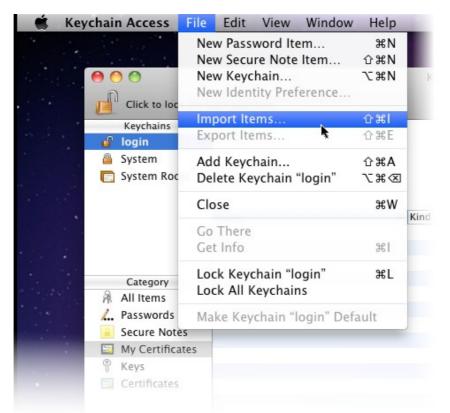
Importing Your Certificate into Mac OS X Mail / Apple Mail

- If you have originally downloaded the certificate through the Mac Mail/Apple Mail installation on the Mas 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 '<u>Enrollment and Collection of your Certificate</u>' 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'.



		-
	Enter the password for "alice_cert.p12":	
	Password: ••••••	
▶ Details		
	Cancel OK	

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.

00	Keycha	in Access	
Click to lock the	login keychain.	Q	
Keychains login System System Roots		Client Authentication and Secure Email CA oruary 2, 2014 6:59:59 PM Eastern Standard Time valid	
Category All Items Passwords Secure Notes My Certificates Keys Certificates	Name Image: Second s	Kind certificate	
	+ i Copy	1 item	

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.

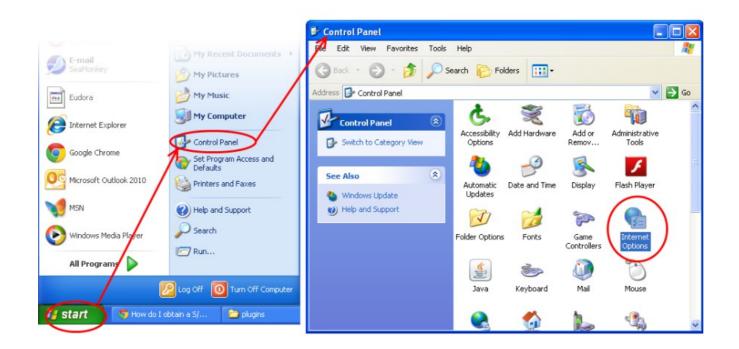


If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import' the certificate into Eudora 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 '<u>Enrollment and Collection of your Certificate</u>' 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.



Internet Properties
General Security Privac Content Connections Programs Advanced
Content Advisor Ratings help you control the Internet content that can be viewed on this computer.
Enable Settings
Certificates Use certificates for encrypted connections and identification.
Clear SSL state Certificates Publishers
AutoComplete
AutoComplete stores previous entries Settings on webpages and suggests matches for you.
Feeds and Web Slices
Feeds and Web Slices provide updated Settings content from websites that can be read in Internet Explorer and other programs.
OK Cancel Apply

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



ertificates	? 🔀
Intended purpose: <a>All>	
Personal Other People Intermediate Certification A	uthorities Trusted Root Certification
Issued To Issued By	Expiratio Friendly Name
Import Export Remove	Advanced
Certificate Import	Wizard
	Welcome to the Certificate Import Wizard This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store. A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept. To continue, click Next.
	< Back Next > Cancel

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

Certificate Import Wizard	\mathbf{X}
File to Import Specify the file you want to import.	
<u>File name:</u>	
Browse	
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)	
< <u>B</u> ack <u>N</u> ext > Cancel	



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).

Open						? 🔀
Look in:	🚞 certs		. 3 🖉	1 🖻	 -	
D Recent	🔊 alice_cert					
Desktop						
My Documents						
My Computer						
	File name:			~	(Open
My Network	Files of type:	Personal Information Exchange (*.pfx;*.p12)	*	(Cancel
		X.509 Certificate (*.cer;*.crt) Personal Information Exchange (Certificate Trust List (*.stl) Certificate Revocation List (*.crl) Microsoft Serialized Certificate St PKCS #7 Certificates (*.spc;*.p7l All Files (*.*)	ore (*.sst)			

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.



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.	
< <u>B</u> ack <u>N</u> ext > 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.

Ce	ertificate Import Wizard	\mathbf{X}
	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 O Automatically select the certificate store based on the type of certificate	
	• Place all certificates in the following store	
	Certificate store:	
	Personal Browse	
-		
	< <u>B</u> ack <u>N</u> ext > Cancel	

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



Certificate Import Wizard			×
	Completing the Certif Wizard You have successfully completed the wizard. You have specified the following sett Certificate Store Selected by User Content File Name	Certificate Import	
	< <u>B</u> ack Fi	inish Cancel	

- 9. Review your settings and click **Finish** to import your certificate.
- 10. Select the security level for storing your private key and click **OK**.

Importing a n	iew private exchange key 🛛 🔀
	An application is creating a Protected item.
A	CryptoAPI Private Key
	Security level set to Medium Set <u>Security Level</u>
	OK Cancel <u>D</u> etails

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 '<u>Enrollment and Collection of your Certificate</u>' 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:



The Bat!	
Message Specials Folder Account Tho	ols <u>V</u> iew Options Help 🎆
ires Set <u>A</u> cces iros View Log [™] <u>R</u> efresh IMAP Con	Mail F2 eued Mail Shift+F2 Password on Server ss Password Ctrl+F12 Shift+Ctrl+A Ctrl+F9 mmands ►
Account Properties - alicege General Transport Mail management Options Files & directories Templates New message Reply Forward Reading confirmation Save message Cookies Sound Memo	Warre alicegreen@company.com Edit personal Certificates Edit personal vCard From information Erom Address Prom Address alicegreen@company.com Organization company Reply-To information Reply-To Name Reply-To Name enderse Default address book: <default> Organization is the default for "mailto:" URLs Virtual folder name template:</default>
	OK Cancel Help

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



🖥 vCard file	e - ACCOUNT.	VCF - alicegree	n@company.co	m		
General Pers	sonal Business	Certificates Othe	er			
Issued To		Issued By		Expires	Root	
Impo	ort	⊻iew	Gen	erate	Reset signer:	5
Expo	rt	<u>D</u> elete	Rec	uest	Token Edito	ır 🔤
	port S/MIME	Certificates from	n Files			? 🗙
	Look jn:	🗀 certs		~	G 🏚 📂 🖽•	
	Lookyn	alicegreen@con				
	3	ancegreen accon	npany.com			
	My Recent Documents					
	Desktop					
· · · · · ·	My Documents					
	My Computer					
		File <u>n</u> ame:	A # 57 (X X)		*	<u>Open</u>
	My Network	Files of <u>type</u> :	All Files (*.*)		~	Cancel

- 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.

😹 Input PFX Password	X
Input password to decrypt data stored in alicegree	n@company.com Cancel Help



6. 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.

M Input PFX Password	
Input password to decrypt a private key stored in alicegreen@company.com.p12. Privat caption is '''s COMODO CA Limited ID''.	e key
•••••	
<u>OK</u> Cancel H	Help

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

🕷 vCard file - ACCOUNT.VCF -	alicegreen@compan	y.com			×
General Personal Business Certif	icates Other				
Issued To	Issued By	Expires		Root	
COMODO Client Authenticatio	UTN-USERFirst-Client Aut	hentic 5/30/202	20 10:48:3	AddTrust E	
UTN-USERFirst-Client Authent	AddTrust External CA Ro	ot 5/30/202	20 10:48:3	AddTrust E	
AddTrust External CA Root					
alicegreen@company.com	COMODO Personal Authe	ntication 10/4/201	4 11:59:5	AddTrust E	
Turnet		Concernation		- t - i	
Import	View	Generate	Rese	et signers	
Export	Delete	Request	To	ken Editor	
		ОК	Cancel	Неір	
			Cancer		

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.

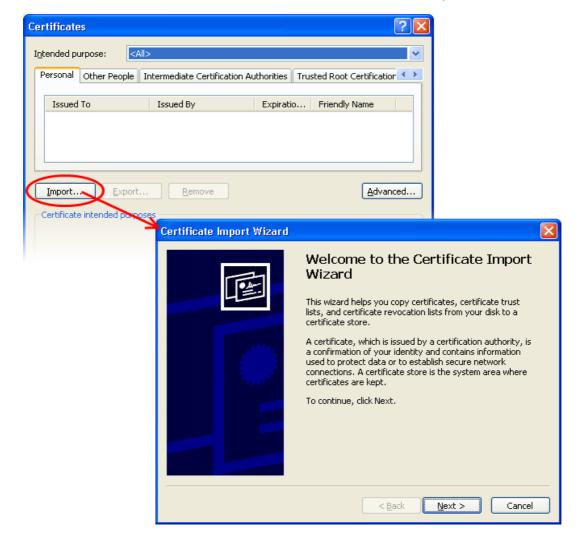
Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '<u>Enrollment and Collection of your Certificate</u>' first.

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



🗐 Local Folders -	Outlook Express	
File Edit View	Tools Message Help	Options ? 🔀
:	Send and Receive	General Bead Receipts Send Compose
Create Mail F	Synchronize All	Signatures Security Connection Maintenance
© Local Folde	Address Book Ctrl+Shift+B Add Sender to Address Book	Virus Protection
Folders	Add Sender to Address Book	Internet zone (Less secure, but more functional)
Outlook Express	Message Rules	 Restricted sites zone (More secure)
🛓 🧐 Local Folders	Accounter	Warn me when other applications try to send mail as me.
- 🙀 Inbox (7	Options	Do not allow attachments to be saved or opened that could potentially be a virus.
	Folder	Download Images
Calebra The	A	Block images and other external content in HTML e-mail.
💮 💮 Deleted Ite	ms Outbox	Secure Mail
Draits میں	Sent Items	Digital IDs (also called certificates) are special documents that allow you to prove your identity in electronic transactions. Tell me more To digitally sign messages or receive encrypted messages, you must have a digital ID. Get Digital ID
		Encrypt contents and attachments for all outgoing messages
		Digitally sign all outgoing messages
		Advanced
		OK Cancel Apply

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	$\mathbf{ imes}$
File to Import	
Specify the file you want to import.	
<u>File name:</u>	
Browse	
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)	
	_
< <u>B</u> ack <u>N</u> ext > Cancel	

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).



Open				? 🗙
Look in:	🚞 certs	v 🕑 🔊	P [
📁 Recent	🔊 alice_cert			
Desktop				
My Documents				
My Computer				
	File name:		*	Open
My Network	Files of type:	Personal Information Exchange (*.pfx;*.p12)	~	Cancel
		X.509 Certificate (*.cer;*.crt) Personal Information Exchange (*.pfx;*.p12) Certificate Trust List (*.stl) Certificate Revocation List (*.crl) Microsoft Serialized Certificate Store (*.sst) PKCS #7 Certificates (*.spc;*.p7b) All Files (*.*)		

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.



Certificate Import Wizard
Password To maintain security, the private key was protected with a password.
Type the password for the private key. <u>P</u> assword:

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.
< <u>B</u> ack <u>N</u> ext > 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	
\bigcirc Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Personal Browse	
	_
< <u>B</u> ack <u>N</u> ext > Cancel	

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



Certificate Import Wizard		
	Completing the Certif Wizard You have successfully completed the wizard. You have specified the following sett Certificate Store Selected by User Content File Name	: Certificate Import
	< <u>B</u> ack Fi	nish Cancel

- 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**.

Importing a n	ew private exchange key	×
	An application is creating a Protected item.	
	CryptoAPI Private Key	
<u>B</u>	Security level set to Medium Set Security Level	7
	OK Cancel <u>D</u> etails	

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.

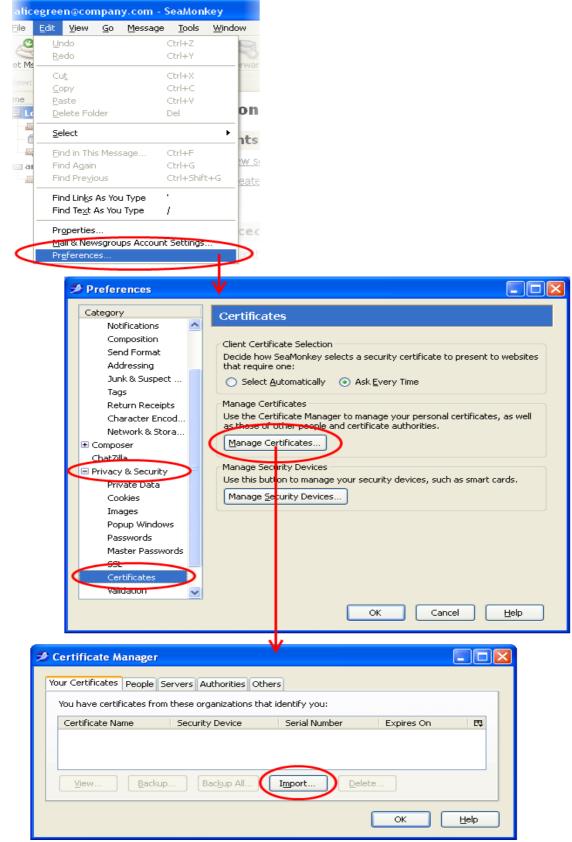


If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email it to yourself or save the certificate file to USB then copy over). You can then import' the certificate into SeaMonkey 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 '<u>Enrollment and Collection of your Certificate</u>' first.

- 1. Open SeaMonkey and then click 'Edit' > 'Preferences'.
- 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 '<u>Enrollment and Collection of your Certificate</u>' first.

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



🖉 Free Antivirus Free SSI	Internet Security and S	SL Certificate	from COMODO - Wind		
C http://www.co	omodo.com/				
File Edit View Favorite					
😤 Favorites 🗲 Free Antivi	Delete Browsing History InPrivate Browsing Reopen Last Browsing Session	Ctrl+Shift+Del Ctrl+Shift+P			
СОМОД	InPrivate Filtering InPrivate Filtering Settings	Ctrl+Shift+F	Internet Op	ptions	? 🛛
Creating Trust Onli	Pop-up Blocker SmartScreen Filter Manage Add-ons) }	Abor General Se Content A		
Flouido	Compatibility View Compatibility View Settings			Ratings help you control the Internet cont viewed on this computer.	settings
T Cass	Subscribe to this Feed Feed Discovery Windows Update		Certificate	es Use certificates for encrypted connection:	s and identification.
	Developer Tools Internet Options	E12		lear <u>S</u> SL state	Publishers
lan		1		AutoComplete stores previous entries on webpages and suggests matches for you.	Settings
			Feeds and	d Web Slices Feeds and Web Slices provide updated content from websites that can be read in Internet Explorer and other programs.	Setti <u>n</u> gs
				ОК Са	ancel Apply

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



Certificates			?	X	
Intended purpose:	>			*	
Personal Other People	Intermediate Certification A	Authorities Tru	sted Root Certificatior 🛃	>	
Issued To	Issued By	Expiratio	Friendly Name		
Import Export	. <u>R</u> emove		Advanced		
Certificate intended parage	Certificate Import		Nizard his wizard helps you copy sts, and certificate revoc ertificate store.	/ certifi ation lis ed by a ntity ar establ	sts from your disk to a a certification authority, is ad contains information ish secure network
			< <u>B</u> ack		Next > Cancel

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)
< <u>B</u> ack <u>N</u> ext > Cancel

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

Open				? 🛛
Look in:	🚞 certs	💌 😋 🌶	Þ	
D Recent	🔊 alice_cert			
Desktop				
My Documents				
My Computer				
	File name:		~	Open
My Network	Files of type:	Personal Information Exchange (*.pfx;*.p12)	~	Cancel
		X.509 Certificate (*.cer;*.crt) Personal Information Exchange (*.pfx;*.p12) Certificate Trust List (*.stl) Certificate Revocation List (*.crl) Microsoft Serialized Certificate Store (*.sst) PKCS #7 Certificates (*.spc;*.p7b) All Files (*.*)		



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. 	
< <u>B</u> ack <u>N</u> ext > 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	
\bigcirc Automatically select the certificate store based on the type of certificate	
Place all certificates in the following store	
Certificate store:	
Personal Browse	
< <u>B</u> ack <u>N</u> ext > Cancel	

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



Certificate Import Wizard			×
	Completing the Certif Wizard You have successfully completed the wizard. You have specified the following sett Certificate Store Selected by User Content File Name	Certificate Import	
	< <u>B</u> ack Fi	inish Cancel	

- 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**.

Importing a n	ew private exchange key 🛛 🔀
	An application is creating a Protected item.
	CryptoAPI Private Key
	Security level set to Medium Set <u>Security Level</u>
	OK Cancel <u>D</u> etails

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

Importing Your Certificate into Comodo Dragon

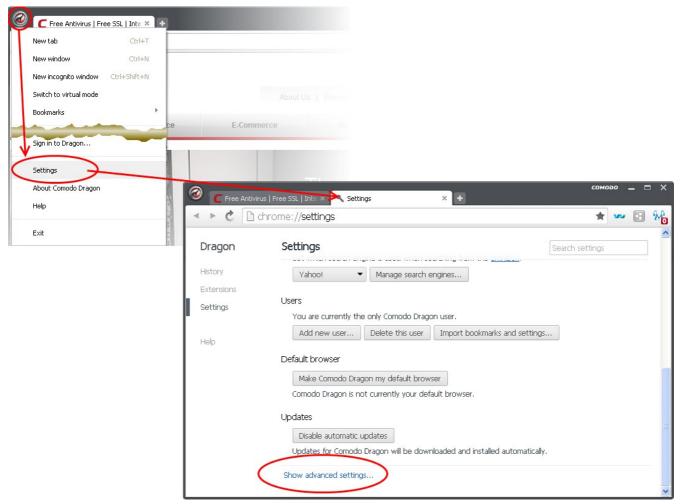
• If you have originally downloaded the certificate through Comodo Dragon then it should have been already installed.



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 '<u>Enrollment and Collection of your Certificate</u>' 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.



Tree /	Antivirus Free SSL Inte × 🔦 Settings 🛛 × 🛨	сомо	DO .	- □	×
⊲ ≻ Ĉ	🗅 chrome:// settings	*	w		8e
Dragon	Settings Charles now Dragon handles and displays languages	Search settings			^
History	Language and input settings				
Extensions	Offer to translate pages that aren't in a language I read.				
Settings	Downloads				
Help	Download location: C:\Documents and Settings\ Change				
	Ask where to save each file before downloading				
	HTTPS/SSI Manage certificates				
	Check for server certificate revocation				
	System				Ξ
	🕑 Continue running background apps when Comodo Dragon is closed				
	🗹 Use hardware acceleration when available				~

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



Certificates			?	×	
Intended purpose:	>			~	
Personal Other People	Intermediate Certification	Authorities Tru	sted Root Certification <	>	
Issued To	Issued By	Expiratio	Friendly Name		
Import Export.	<u>R</u> emove		Advanced		
Certificate intended parts	Certificate Impor		Nelcome to the Nizard This wizard helps you copy of sts, and certificate revocat certificate store. A certificate, which is issued a confirmation of your ident ised to protect data or to e connections. A certificate st certificates are kept. To continue, click Next.	certific ion lis I by a ity an	cates, certificate trust its from your disk to a certification authority, is id contains information ish secure network
			< <u>B</u> ack		Next > Cancel

5. 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.
Eile 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)
< <u>B</u> ack <u>N</u> ext > Cancel

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

Open				? 🗙
Look in:	🚞 certs	💌 😋 🌶	Þ	•
D Recent	🔊 alice_cert			
Desktop				
My Documents				
My Computer				
	File name:		~	Open
My Network	Files of type:	Personal Information Exchange (*.pfx;*.p12)	*	Cancel
		X.509 Certificate (*.cer;*.crt) Personal Information Exchange (*.pfx;*.p12) Certificate Trust List (*.stl) Certificate Revocation List (*.crl) Microsoft Serialized Certificate Store (*.sst) PKCS #7 Certificates (*.spc;*.p7b) All Files (*.*)		



7. 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	$\mathbf{\times}$
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.	
< <u>B</u> ack <u>N</u> ext > Cancel	

8. 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	
< <u>B</u> ack <u>N</u> ext > Cancel	

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



Certificate Import Wizard		
	Completing the Certif Wizard You have successfully completed the wizard. You have specified the following sett Certificate Store Selected by User Content File Name	Certificate Import
	< <u>B</u> ack Fi	nish Cancel

- 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.

Importing a n	ew private exchange key	×
	An application is creating a Protected item.	
A	CryptoAPI Private Key	
	Security level set to Medium Set <u>Security Level</u>	
	OK Cancel <u>D</u> etails	

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 '<u>Enrollment and Collection of your Certificate</u>' 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.

🗣 Free Antivirus Free SSL Internet S	Security and SSL Certificat	e from COMODO - Como	do IceDragon	
<u>Fi</u> le <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks	Tools Help			
Free Antivirus Free SSL Internet Se. 🛞 www.comodo.com	Downloads Ctrl+J Add-ons Ctrl+Shift+A			
сомодо	Web Developer Page Info Start Virtual Mode			
Creating Trust Online*	Options me Office E-C	About Us I R	esources 1 News	
Options	Y	_	_	×
General Tabs	Content Applications Prive)	
Select one automa View Certificate	<u> </u>	ecurity Devices		
Powered by COMODO				OK Cancel

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



0	Certificate Manager				×				
	Your Certificates People Servers Authorities Others								
	You have certificates from these organizations that identify you:								
	Certificate Name	Security Device	Serial Number	Expires On	EŞ				
	Yiew	Backup All	Delete						
					OK				

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

Certificate File	to Import					? 🔀
Look jn:	🚞 certs		*	3 🕫	• 🖽 🥙	
Content Conten	🔊 alice_cert					
Desktop						
My Documents						
My Computer						
	File <u>n</u> ame:				~	<u>O</u> pen
My Network	Files of <u>type</u> :	PKCS12 Files			*	Cancel
		PKCS12 Files All Files				

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**.



	🔁 Password Entry Dialog 🛛 🕅 🕅
	Please enter the password that was used to encrypt this certificate backup.
	Password: •••••
	OK Cancel
	lert
J AI	
1	Successfully restored your security certificate(s) and private key(s)
	ΟΚ

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 '<u>Enrollment and Collection of your Certificate</u>' 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.



😺 Free Antivirus Free SSL Inter	met Security and SSL Certificate fr
<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks	Tools Help
Free Antivirus Free SSL Internet Secu	<u>A</u> dd-ons Ctrl+Shift+A
	Web Developer Page Info
COMODO Creating Trust Online®	Options
	Options V
	General Tabs Content Applications Private Security Synce Advanced General Data Choices Network Update Certificates When a server requests my personal certificate: Select one automatically Ask me every time View Certificates View Certificates View Certificates Validation Security Devices
	OK Cancel <u>H</u> elp

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

e	Certificate Manager	
	Your Certificates People Servers Authorities Others You have certificates from these organizations that identify you:	
	Certificate Name Security Device Serial Number Expires On	Ę
	View Backup Backup All Import Delete	ОК
	L	

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



Certificate File	to Import							? 🔀
Look jn:	🗀 certs		(~ (3 🤌	Þ	···· •	
CO Recent	👰 alice_cert							
Desktop								
My Documents								
My Computer								
	File <u>n</u> ame:					~	(<u>O</u> pen
My Network	Files of <u>type</u> :	PKCS12 Files				~	(Cancel
		PKCS12 Files All Files						.::

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**.

	Password Entry Dialog	
	Please enter the password that was used to encrypt this certificate backup.	
	Password:	
	V	
Aler	t	×
4	Successfully restored your security certificate(s) and private key	(s).
	ок	

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.

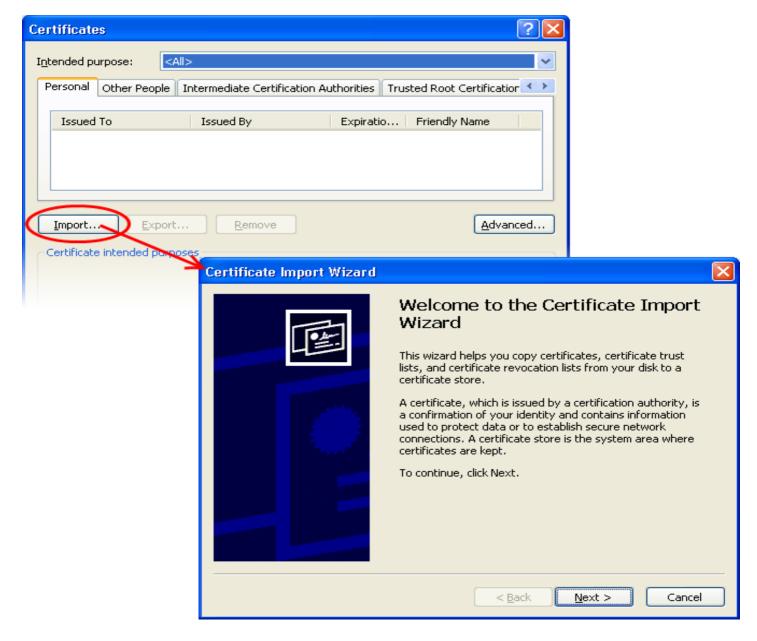
Note: This document assumes you have already enrolled for and downloaded your certificate. If this is not the case then please read the section '<u>Enrollment and Collection of your Certificate</u>' first.

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

	U Opera				
\checkmark	Newtab	Ctrl+T			
	New window	Ctrl+N			
	New private window	w Ctrl+Shift+N	com		
	Recently closed	•			
	Page	•			
	Zoom	< 100% > (;)			
	Print	Ctrl+P		About Us Resources	
	③ Downloads	Ctrl+J			
	() History	Ctrl+H	ce E-Comme	erce Business 1	
0	🌸 Settings	Alt+P			
	1 Themes				
	Extensions	Ctrl+Shift+E			
	Get extensions			SSI Ce	
		U Opera	1		- • ×
	Off-Road mode More tools	C Free Antivirus	Free SSL × 🕏 Setting	15 × +	
		← → G	III O settings		
			/	Privacy	^
		200		Clear browsing data	
		Setting	is /	Opera may use web services to improve your browsing experience. You may optionally disa	able these services.
				Use a prediction service to help complete searches and URLs typed in the address bar	
		Q Search	settings	Predict network actions to improve page load performance	
		Browser		Automatically send usage statistics and crash reports to Opera Send a 'Do Not Track' request with your browsing traffic	
			V.		
		Websites		Passwords	
		Privacy 8	& security	Offer to save passwords I enter on the web	
		On one has		Manage saved passwords	
		Opera he	ib di		
				Autofill	
				Enable auto-filling of forms on webpages	
				Manage Autofill settings	
		Carlo and and a		manage Autonn settings	
			the state of the	Cookies	
		and the second	Contraction of the line		
		A States		 Allow local data to be set (recommended) Keep local data only until I quit my browser 	
		Contraction of the second	7 3	Block sites from setting any data	
		50 120		Block third-party cookies and site data	
		Helfert .	Course of the second	Manage exceptions All cookies and site data Learn more	
		and the second			
		No.	110000 M	HTTPS/SGL	
				Manage certificates Ligarn more	
		200	and the second	Manage certificates Laarn more	
		<			

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.	
Eile 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)	
< <u>B</u> ack <u>N</u> ext > Cancel	

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.

Open							? 🛛
Look in:	🚞 certs		*	0	1 🖻	•	
📁 Recent	🔊 alice_cert						
Desktop							
My Documents							
My Computer							
	File name:				~]	Open
My Network	Files of type:	Personal Information Exchange	je (*.pf	x;*.p12)	~		Cancel
		X.509 Certificate (*.cer,*.crt) Personal Information Exchang Certificate Trust List (*.stl) Certificate Revocation List (*.rt Microsoft Serialized Certificate PKCS #7 Certificates (*.spc)*. All Files (*.*)	orl) Store				



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.	
< <u>B</u> ack <u>N</u> ext > Cancel	

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

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 O Automatically select the certificate store based on the type of certificate	
• Place all certificates in the following store	
Certificate store:	
Personal Browse	
	_
< <u>Back</u> <u>Next</u> Cancel	

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



Certificate Import Wizard		
	Completing the Certif Wizard You have successfully completed the wizard.	Certificate Import
	You have specified the following sett Certificate Store Selected by User Content File Name	-
	< <u>B</u> ack Fi	nish Cancel

- 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.

Importing a n	ew private exchange key	<
	An application is creating a Protected item.	
	CryptoAPI Private Key	
	Security level set to Medium Set <u>Security Level</u>	
	OK Cancel <u>D</u> etails	

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

Importing your Certificate into Safari on Windows

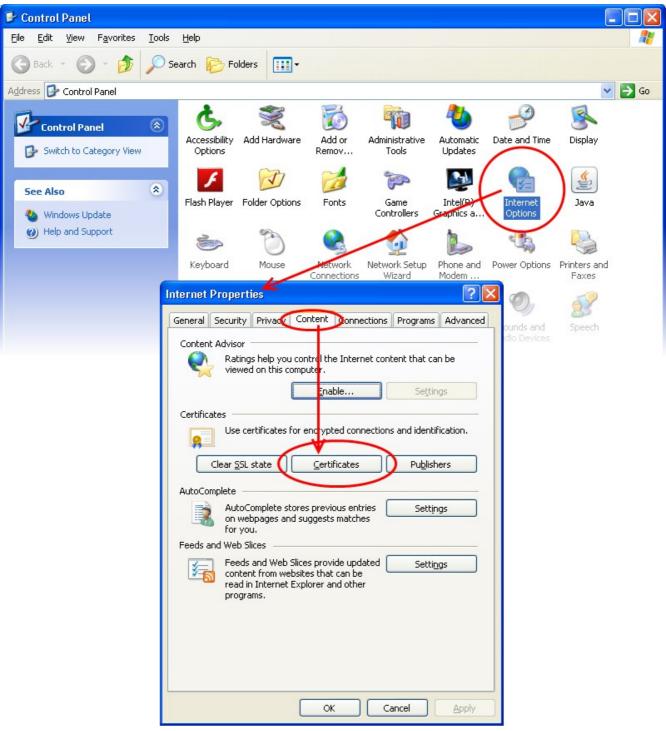
- If you have originally downloaded the certificate through Safari then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email 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 '<u>Enrollment and Collection of your Certificate</u>' 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'.



Certificates				?×	
Intended purpose:				~	
Personal Other People In	termediate Certification Aut	horities Tru:	sted Root Certification	< >	
Issued To	Issued By	Expiratio	Friendly Name		
Export	Remove		Advance	:d	
	Certificate Import V		Vizard his wizard helps you co sts, and certificate revo ertificate store. certificate, which is iss confirmation of your id sed to protect data or	py certification list	a certification authority, is nd contains information

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



Certificate Import Wizard	X
File to Import Specify the file you want to import.	
Eile 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)	
< <u>B</u> ack <u>N</u> ext > Cancel	

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).



Open				? 🔀
Look in:	🚞 certs	💌 🖸 🌶	🕫 📂	•
D Recent	🔊 alice_cert			
Desktop				
My Documents				
My Computer				
	File name:		*	Open
My Network	Files of type:	Personal Information Exchange (*.pfx;*.p12)	~	Cancel
		X.509 Certificate (*.cer;*.crt) Personal Information Exchange (*.pfx;*.p12) Certificate Trust List (*.stl) Certificate Revocation List (*.crl) Microsoft Serialized Certificate Store (*.sst) PKCS #7 Certificates (*.spc;*.p7b) All Files (* *)		

 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.	
< <u>B</u> ack <u>N</u> ext > Cancel	

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.

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 O Automatically select the certificate store based on the type of certificate O Place all certificates in the following store			
Certificate store:			
Personal Browse			
	_		
< <u>Back</u> <u>N</u> ext > Cancel			

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



Certificate Import Wizard		
	Completing the Certif Wizard You have successfully completed the wizard. You have specified the following sett Certificate Store Selected by User Content File Name	Certificate Import
	< <u>B</u> ack Fi	inish Cancel

- 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.

Importing a n	iew private exchange key 🛛 🔀
	An application is creating a Protected item.
	CryptoAPI Private Key
	Security level set to Medium Set <u>Security Level</u>
	OK Cancel <u>D</u> etails

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

Importing Your Certificate into Safari on Mac OS X

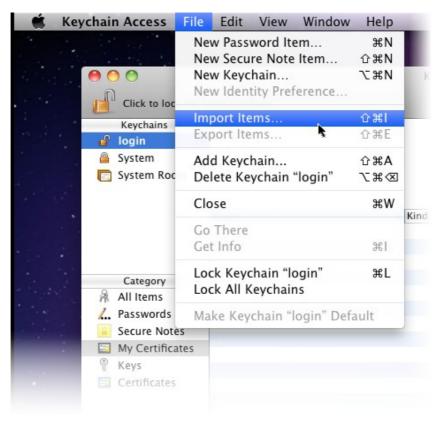
- If you have originally downloaded the certificate through Safari then it should have been already installed.
- If your certificate is not already installed on the computer you are using, then please export it from the machine on which it resides. You then need to transfer it to this computer (email 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 '<u>Enrollment and Collection of your Certificate</u>' 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'.

		-
	Enter the password for "alice_cert.p12":	
	Password: •••••	
	Show password	
▶ Details		
	Cancel OK	

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.

00	Keychain	Access
Click to lock the	login keychain.	٩
Keychains login System System Roots		lient Authentication and Secure Email CA ary 2, 2014 6:59:59 PM Eastern Standard Time lid
Category All Items Passwords Secure Notes	Name Name Image: state stat	▲ Kind certificate
 My Certificates Keys Certificates 		
	+ i Copy	1 item

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

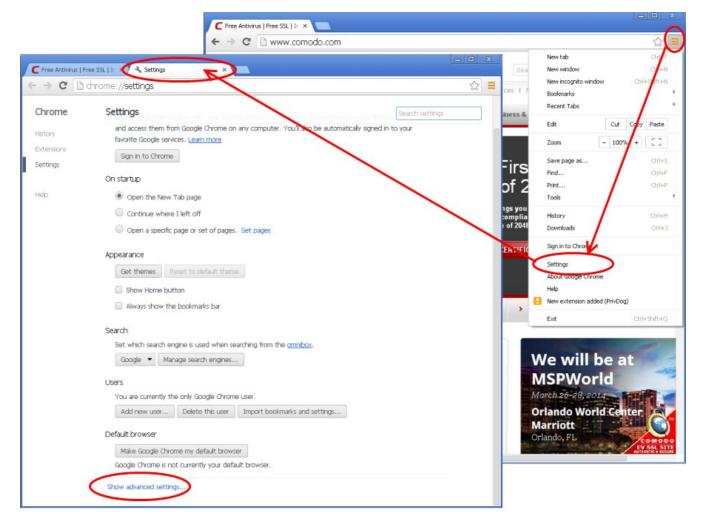
Importing Your Certificate into Google Chrome on Windows

- 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 '<u>Enrollment and Collection of your Certificate</u>' 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.



C Free Antivirus Free	SSL Ir × Settings ×		x
← → C □ d	rome://settings	5	=
	Settings Search settings Languages Change how Chrome handles and displays languages Language and input settings Image and input settings Image offer to translate pages that aren't in a language I read. Manage languages Downloads Download location: C:\Documents and Settings\John W Change Ask where to save each file before downloading HTTPS/SSL Image certificates Check for server certificate revocation Google Cloud Print Google Cloud Print		
	Set up or manage printers in Google Cloud Print. <u>Learn more</u> Manage Show notifications when new printers are detected on the network		
	System		

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



Certificates				?×	
Intended purpose:				~	
Personal Other People In	ermediate Certification Auth	horities Trus	ited Root Certification	< >	
Issued To	Issued By	Expiratio	Friendly Name		
Export	Remove		Advance	:d	
	Certificate Import W	TI Iis Ce A us Ce	Vizard his wizard helps you cop ts, and certificate revo ertificate store. certificate, which is issi confirmation of your id sed to protect data or t	py certifi cation li: ued by a entity ar to establ e store i:	a certification authority, is nd contains information

5. 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.	
Eile 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)	
< <u>B</u> ack <u>N</u> ext > Cancel	

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



Open				? 🔀
Look in:	🚞 certs	💌 😋 🌶	🔊 🥙	Ŧ
📁 Recent	🔊 alice_cert			
Desktop				
My Documents				
My Computer				
	File name:		~	Open
My Network	Files of type:	Personal Information Exchange (*.pfx;*.p12)	~	Cancel
		X.509 Certificate (*.cer;*.crt) Personal Information Exchange (*.pfx;*.p12) Certificate Trust List (*.stl) Certificate Revocation List (*.crl) Microsoft Serialized Certificate Store (*.sst) PKCS #7 Certificates (*.spc;*.p7b) All Files (*.*)		

7. 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.

8. Next you specified						
Specified (Password To maintain security, the private key was protected with a password.	store option.				
	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.					
InCommon Certific	< <u>B</u> ack <u>N</u> ext > Cancel	76				



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	
< <u>B</u> ack <u>N</u> ext > Cancel	

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

Certificate Import Wizard		X			
	Completing the Certificate Import Wizard You have successfully completed the Certificate Import wizard. You have specified the following settings:				
	Certificate Store Selected by User Content File Name				
	< <u>B</u> ack F	inish Cancel			

- 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**.



Importing a n	ew private exchange key 🛛 🛛 🔀
	An application is creating a Protected item.
	CryptoAPI Private Key
	Security level set to Medium Set <u>S</u> ecurity Level OK Cancel <u>D</u> etails

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 '<u>Enrollment and Collection of your Certificate</u>' first.

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



	Search our website GO Search Our website GO Search Our website GO Search Our website I Asia & Pacific	New Tab
Hor $\leftrightarrow \mathcal{C}$	hrome://settings	ii Edit Cut Copy Past
Chrome	Settings	Zoom - 100% +
Minterry	Appearance	Save Page As
History	Get themes Reset to default theme	Find a Print a
Extensions	Show Home button	Tools
Settings	Always show the bookmarks bar	History 3 Downloads û 3
Help		SM in to Chrome
	Search Set which search engine is used when searching from the <u>omnibox</u> . Google Manage search engines	Settings About Google Chrome Help
	Users	
	You are currently the only Google Chrome user.	
	Add new user Delete this user Import bookmarks and settings	NS
	Default browser	
	Make Google Chrome my default browser	
Dc	Google Chrome is not currently your default browser.	
for N	Show advanced settings	5
Jp	Comodo makes SSL Security easy Orlando World Center	
eaning Essentials)	Marriott	

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



\varTheta 🔿 🔿 🧲 Free Antivirus Free SSL × 🔍 Settings 🛛 ×					
♦ ⇒ C	hrome://settings	☆ =			
Chrome	Search settings				
History Extensions	Offer to translate pages that aren't in a language I read. Manage languages				
Settings	Downloads				
	Download location: /Users/comodo/Downloads Change				
Help	Ask where to save each file before downloading				
	HTTPS/SSL Manage certificates Check for server certificate revocation				
	Google Cloud Print				
	Google Cloud Print lets you access this computer's printers from anywhere.				
	Add printers				
	System				
	Use hardware acceleration when available	*			
C					

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...'



Keychain Access	File	Edit	View	Window	Help	
			word Ite re Note	em Item	光N 企業N	I
Click to loc			hain tity Pref	erence	₹₩N	1
Keychains	lm	port Ite	ems		企業I	-
login	Ex	port Ite	ms	4	ΰжE	
🔒 System	Ad	d Keyc	hain		ŵжА	
📄 System Roc	De	lete Ke	ychain '	"login"	₹¥⊗	
	Clo	ose			жW	Kind
	Go	There				KINC
1	Ge	t Info			¥1	
Category			chain "lo Ceychair	-	жL	
2. Passwords	Ma	ke Key	chain "l	ogin" Defa	ault	
🧧 Secure Note	2S					
🔄 My Certifica	tes					
Reys Keys Key						
📴 Certificates						

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

		-
	Enter the password for "alice_cert.p12":	
	Password: •••••	
	Show password	
▶ Details		
	Cancel	ОК

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.



00	Keychain Access					
Click to lock th	e login keychain.	Q				
Keychains login System System Roots	Expires: S					
Category	Name	Kind	I,			
All Items All	alicegreen@company	certificate certificate				
My Certificates						
% Keys Gertificates						
	÷ i Copy	1 item				

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 '<u>Enrollment and Collection of your Certificate</u>' first.

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



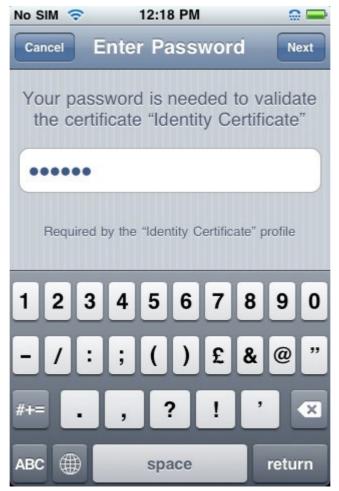


Tap the **Install** button to begin the certificate import wizard.

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.

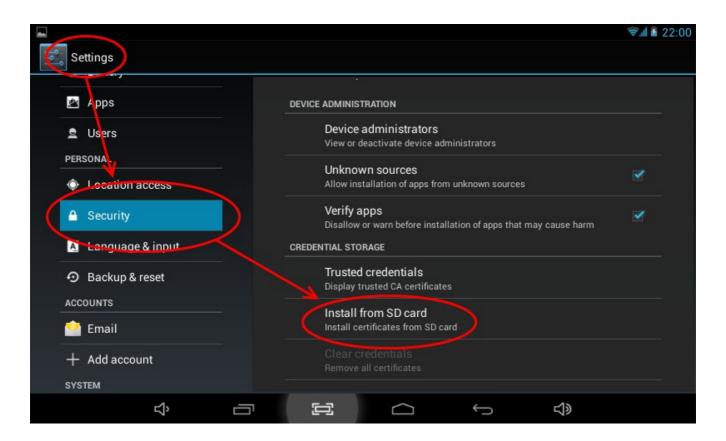


Importing Your Certificate into Android Devices

- 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 '<u>Enrollment and Collection of your Certificate</u>' 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'.

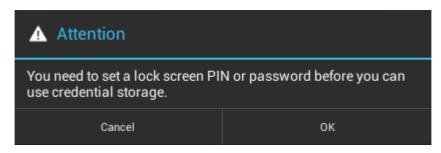
Extract from alice_cert.p12			
Type the password to extract the certificates.			
Cancel	ок		

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



Name the certificate	
Certificate name: alice_cert	
The package contains: one user key one user certificate 3 CA certificates	
Cancel	ок

4. 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.



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

📕 Language & input	Verify apps 🥪
• Backup & reset	Disallow or warn before installation of apps that may cause harm
•	CREDENTIAL STORAGE
ACCOUNTS	alice cert is installed.
🔮 Email	Display trusted CA certificates
+ Add account	Install from SD card

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.



					(P)	1 22:10		
Settings								
Battery			SYSTEM		USER			
🕿 Apps		COMODO	CA Limited			-		
单 Users			ent Authentication a	nd Secure Email CA				
PERSONAL		The USER ⁻	TRUST Network					
Location access	UTN-USERFirst-Client Authentication and Email							
Security								
A. Language & input								
D Backup & reset								
ACCOUNTS								
Semail								
+ Add account								
り つ	ā	IJ		¢	山 》			

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

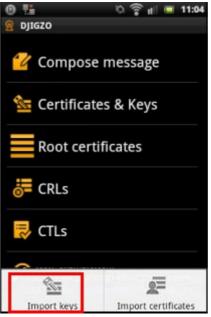
If you have originally downloaded your certificate to your desktop or laptop then you first need to export it from the computer. When doing this, please make sure you export the private key and include all certificates in the certificate path if possible. You must also specify a strong password to protect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

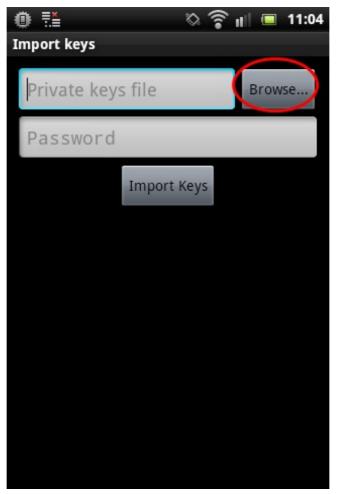
Before importing your certificate into Djigzo , make sure that you have configured your mail account with an existing Android email client such as Google Mail app, K9 or the default mail client.

- 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.





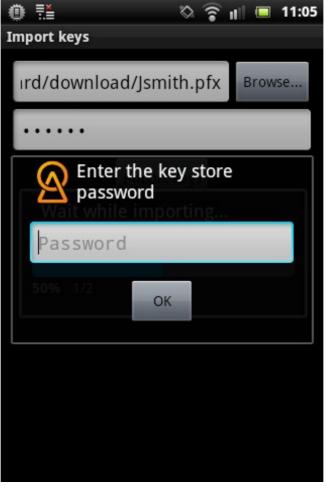
5. Enter the password you set up for the certificate when it was exported and tap 'Import Keys'.



0					\diamond		ntil 🛛	1	1:05
Imp	ort k	eys							
ir	ırd/download/Jsmith.pfx Browse								
·	•••••								
			I	mpor	t Key	s			
1	2	3	4	5	6	7	8	9	0
@	&	%	=	+	•	*	1	()
112 ! ? ' " : ; _ 💌									
I		⊕ bc	,	_	_				one

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.