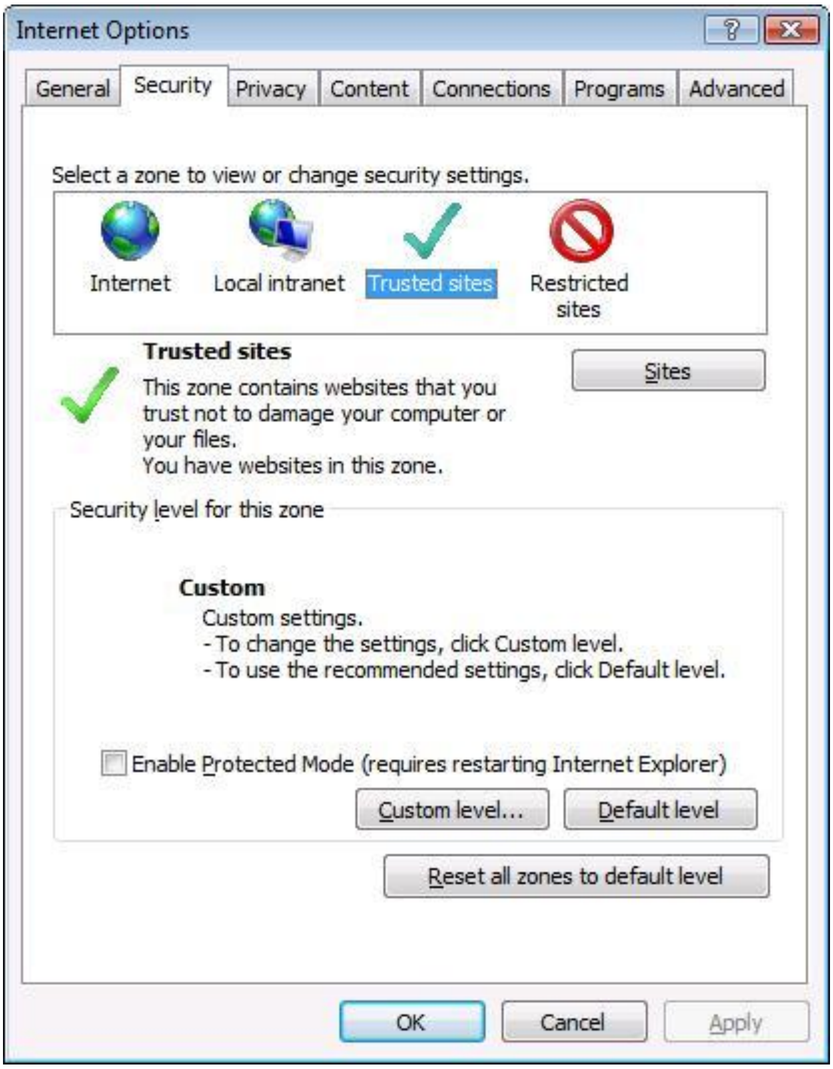
How to order and install Odette certificates

Contents

1. Before you start

Users wishing to buy certificates using Windows Vista or Windows7 should add the Odette CA site to their list of trusted web sites in Internet Explorer.

Go to *Internet Options* > *Security* > *Trusted Sites* and then click *Sites*.



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.
You have websites in this zone.

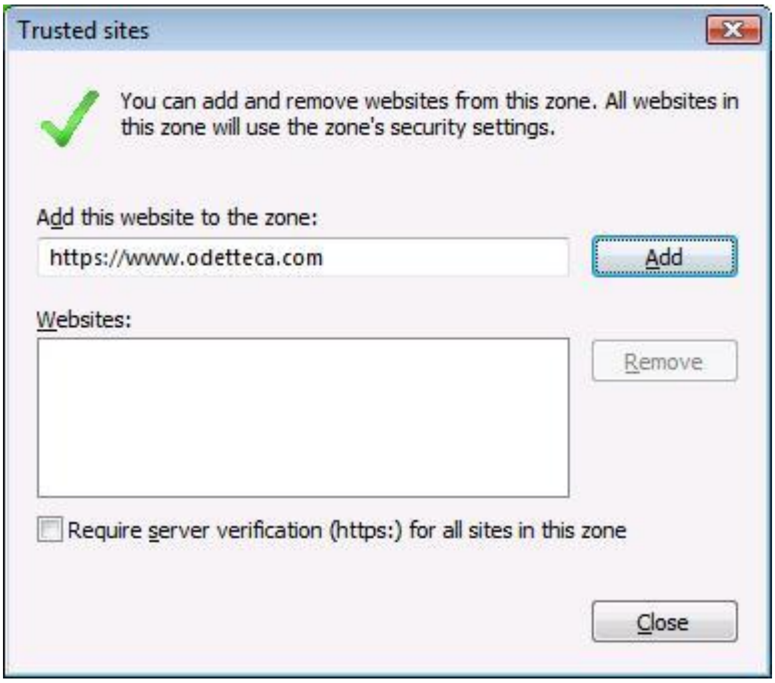
Security level for this zone

Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

□ Enable Protected Mode (requires restarting Internet Explorer)

Type 'https://www.odetteca.com/ ' into the text box and click *Add*.



Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone: https://www.odetteca.com

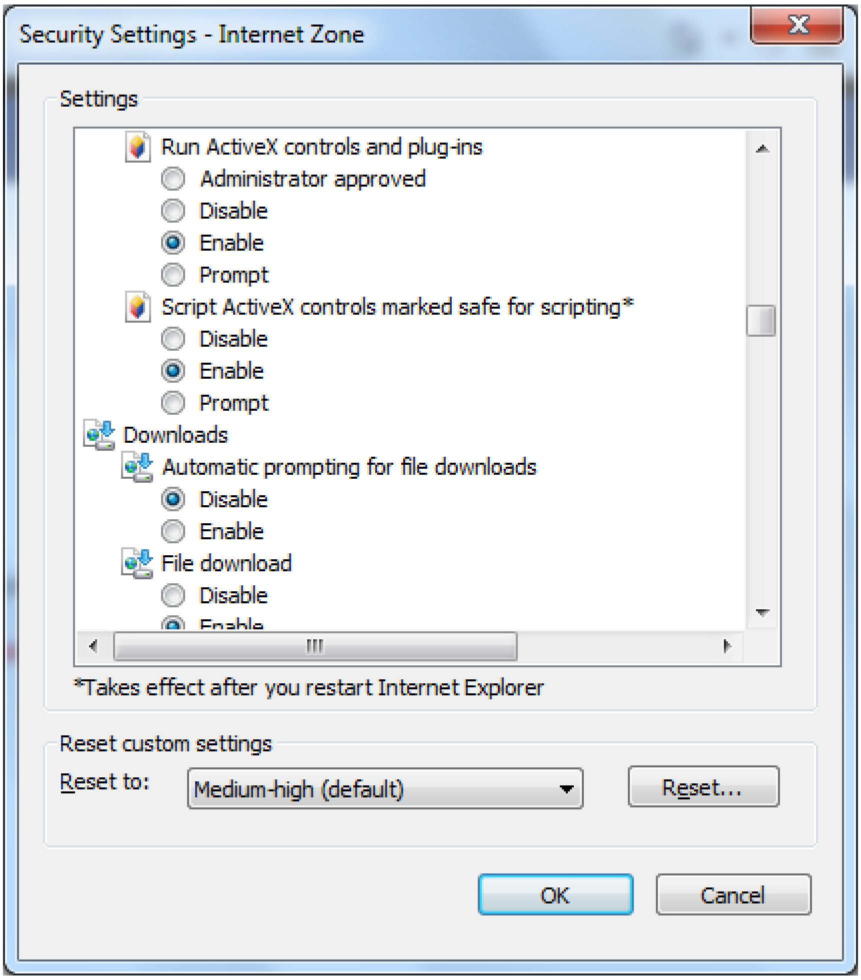
Websites:

□ Require server verification (https:) for all sites in this zone

Click *Close* and then click *OK* on the 'Internet Options' dialogue.

ActiveX
Please verify that your browser allows ActiveX execution.

Go to *Internet Options* > *Security* > *Internet Zone* and click *Custom Level*



Security Settings - Internet Zone

Settings

- Run ActiveX controls and plug-ins
  - ○ Administrator approved
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Script ActiveX controls marked safe for scripting*
  - ○ Disable
  - ● Enable
  - ○ Prompt
- Downloads
  - Automatic prompting for file downloads
    - ● Disable
    - ○ Enable
  - File download
    - ○ Disable
    - ● Enable

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: Medium-high (default)

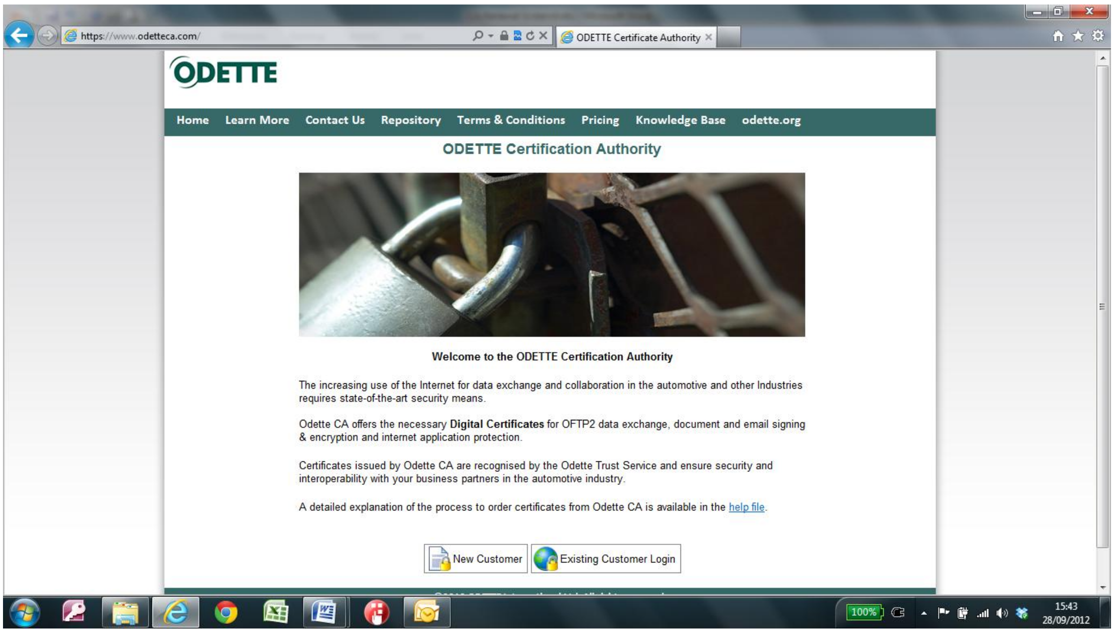
Enable ActiveX controls.

During the certificate order process the browser will run an ActiveX control that creates the private key and the public key on the computer being used.

If the security policy of your company does not allow the running of ActiveX then you will have to create the private key and the certificate signing request (CSR) separately before you start the order process. Please refer to the annexe How to create a certificate signing request (CSR) on a Linux or Windows machine ***with an external tool*** for further instructions.

2. Log on to the Odette CA and start the order process

It is recommended to order the certificate using the computer on which you wish to install it (target computer). If you cannot use the target computer to order the certificate, please also read the Annexes 'How to export a certificate including the private key from one Windows machine to another (Windows keystore)' and 'How to import the certificate on the target computer'.



ODETTE Certification Authority

Welcome to the ODETTE Certification Authority

The increasing use of the Internet for data exchange and collaboration in the automotive and other Industries requires state-of-the-art security means.

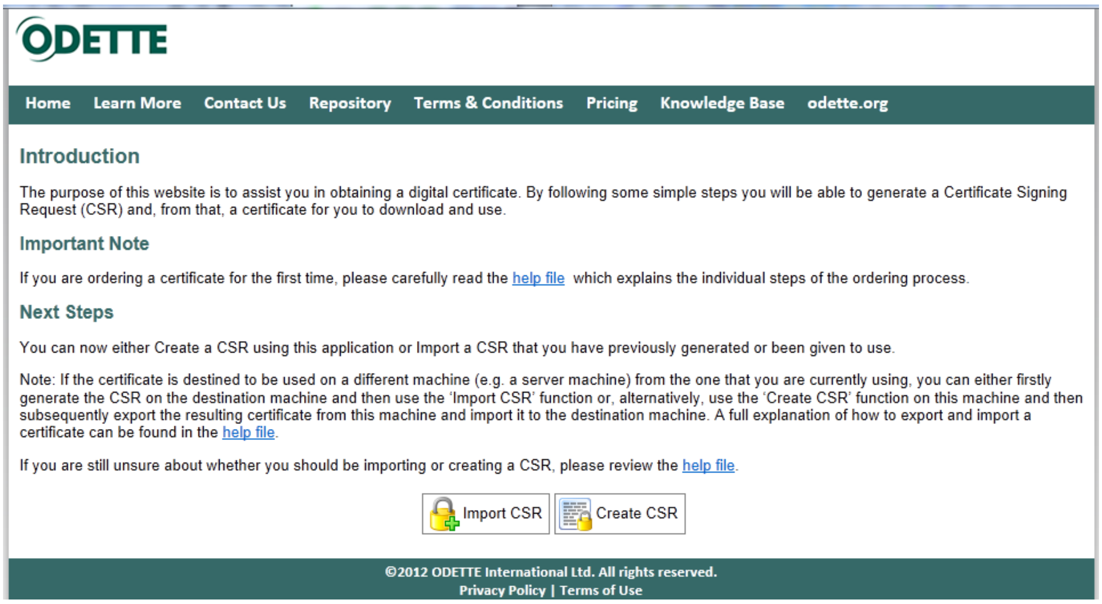
Odette CA offers the necessary **Digital Certificates** for OFTP2 data exchange, document and email signing & encryption and internet application protection.

Certificates issued by Odette CA are recognised by the Odette Trust Service and ensure security and interoperability with your business partners in the automotive industry.

A detailed explanation of the process to order certificates from Odette CA is available in the help file.

If you are ordering a certificate for the first time, click on *New Customer* (your user account will be created during the order process).

If you have bought an Odette certificate previously and want to renew it or order a different one or if you want to download or revoke an existing Odette certificate, click on *Existing Customer Login*.



Introduction

The purpose of this website is to assist you in obtaining a digital certificate. By following some simple steps you will be able to generate a Certificate Signing Request (CSR) and, from that, a certificate for you to download and use.

Important Note

If you are ordering a certificate for the first time, please carefully read the help file which explains the individual steps of the ordering process.

Next Steps

You can now either Create a CSR using this application or Import a CSR that you have previously generated or been given to use.

Note: If the certificate is destined to be used on a different machine (e.g. a server machine) from the one that you are currently using, you can either firstly generate the CSR on the destination machine and then use the 'Import CSR' function or, alternatively, use the 'Create CSR' function on this machine and then subsequently export the resulting certificate from this machine and import it to the destination machine. A full explanation of how to export and import a certificate can be found in the help file.

If you are still unsure about whether you should be importing or creating a CSR, please review the help file.

©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

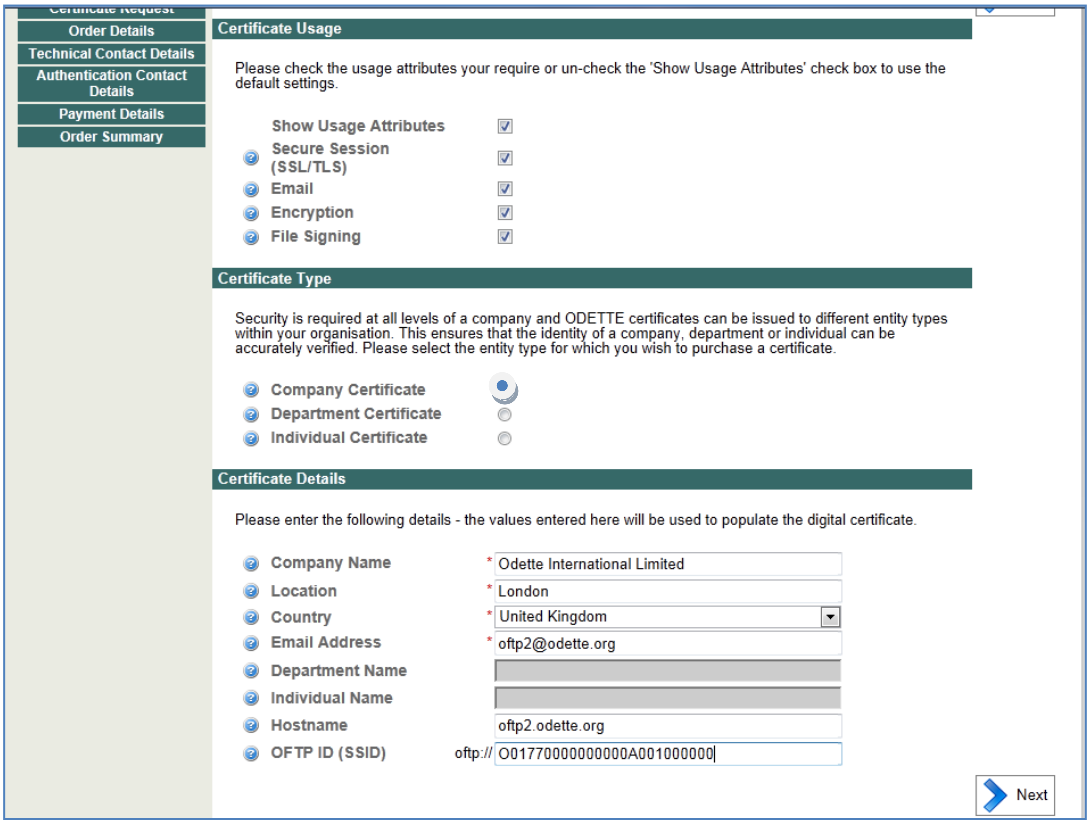
On the Introduction page you need to decide whether to import a previously prepared Certificate Signing Request (CSR) or to create the CSR on-line during the order process.

On-line creation of the CSR can only be done with the **Internet Explorer** browser. In addition, the execution of **ActiveX** code must be enabled.

If your system does not support these requirements, you will need to create the CSR with an external tool (see annexe 5) and then select "*Import CSR*". Continue with chapter 3 in this help file.

Otherwise select "*Create CSR*".

3. *Creating the CSR on-line*



Certificate Usage

Please check the usage attributes your require or un-check the 'Show Usage Attributes' check box to use the default settings.

Show Usage Attributes	☑
Secure Session (SSL/TLS)	☑
Email	☑
Encryption	☑
File Signing	☑

Certificate Type

Security is required at all levels of a company and ODETTE certificates can be issued to different entity types within your organisation. This ensures that the identity of a company, department or individual can be accurately verified. Please select the entity type for which you wish to purchase a certificate.

Company Certificate	●
Department Certificate	○
Individual Certificate	○

Certificate Details

Please enter the following details - the values entered here will be used to populate the digital certificate.

Company Name	* Odette International Limited
Location	* London
Country	* United Kingdom
Email Address	* oftp2@odette.org
Department Name	
Individual Name	
Hostname	oftp2.odette.org
OFTP ID (SSID)	oftp:// O01770000000000A001000000

Certificate Usage
In the above example, the certificate can be used for various purposes. By default, all the listed certificate usage attributes are enabled.

If you want to connect your OFTP2 system to other OFTP2 systems, at least “Secure Session (SSL/TLS)” must be enabled,
Encryption (i.e. file encryption) and File Signing are advanced functions of OFTP2 and can be used in addition to TLS session security. Email (encryption and signing) is an application outside the scope of OFTP2 but is also supported by Odette certificates.

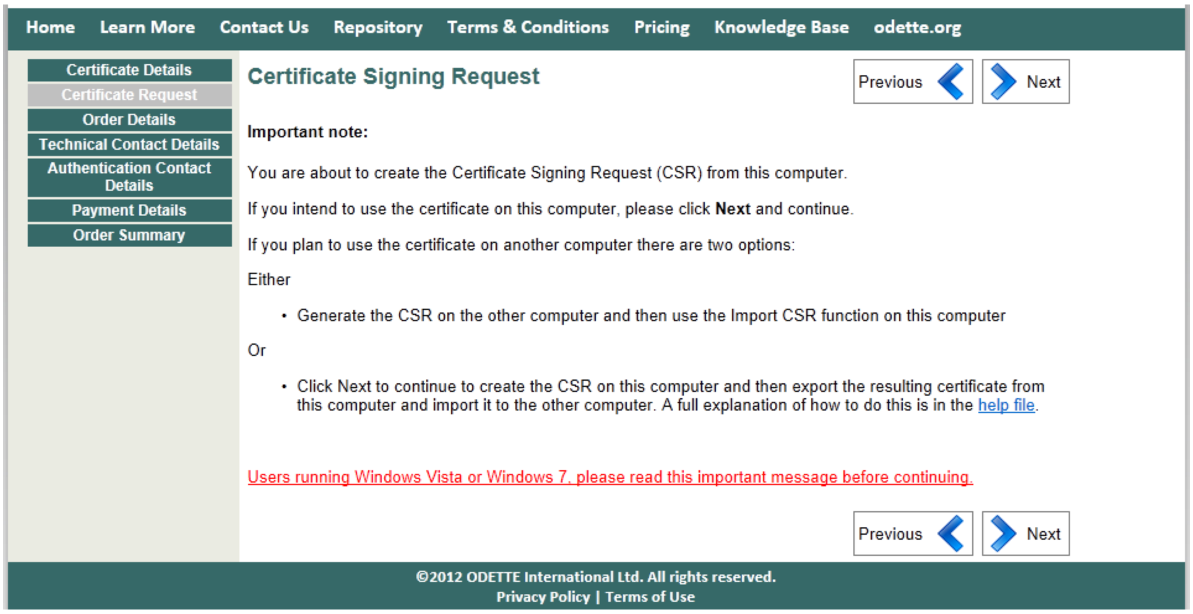
Certificate Type
For use with OFTP2, normally a Company Certificate is selected but it is also possible to order a certificate for use by a specific Department or by an Individual.

Certificate Details
Fields marked with an asterisk (*) are mandatory.

Please note that current implementations of OFTP2 at some companies require the OFTP2 servers of their business partners to use qualified domain names which are registered and resolvable by the domain name system (DNS).
If you are certain that none of your OFTP business partners have this requirement, you can use a static IP address or a virtual host name instead.

For OFTP2, you should also enter your SSID (aka OFTP ID or Odette ID).

Click ‘*Next*’ to continue.



Certificate Signing Request

Important note:

You are about to create the Certificate Signing Request (CSR) from this computer.

If you intend to use the certificate on this computer, please click **Next** and continue.

If you plan to use the certificate on another computer there are two options:

Either

- Generate the CSR on the other computer and then use the Import CSR function on this computer

Or

- Click Next to continue to create the CSR on this computer and then export the resulting certificate from this computer and import it to the other computer. A full explanation of how to do this is in the help file.

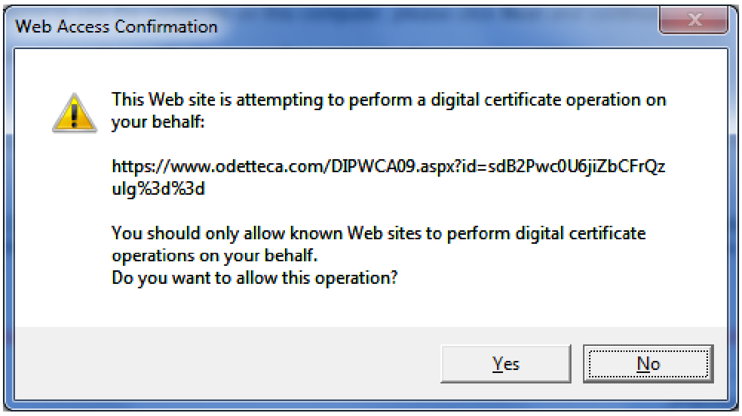
Users running Windows Vista or Windows 7, please read this important message before continuing.

©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

An important message for Windows Vista / Windows 7 users is also given at the start of this document.

Click "*Next*" to continue or "*Previous*" if you want to review/change the certificate details which you entered on the previous page.

Depending on the settings of your browser you may see a message like this:



This Web site is attempting to perform a digital certificate operation on your behalf:

https://www.odetteca.com/DIPWCA09.aspx?id=sdB2Pwc0U6jiZbCFrQzulg%3d%3d

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?

Click "*Yes*" to continue. Subsequently, a private key is generated in your local keystore and a matching CSR is submitted to the Odette CA application.

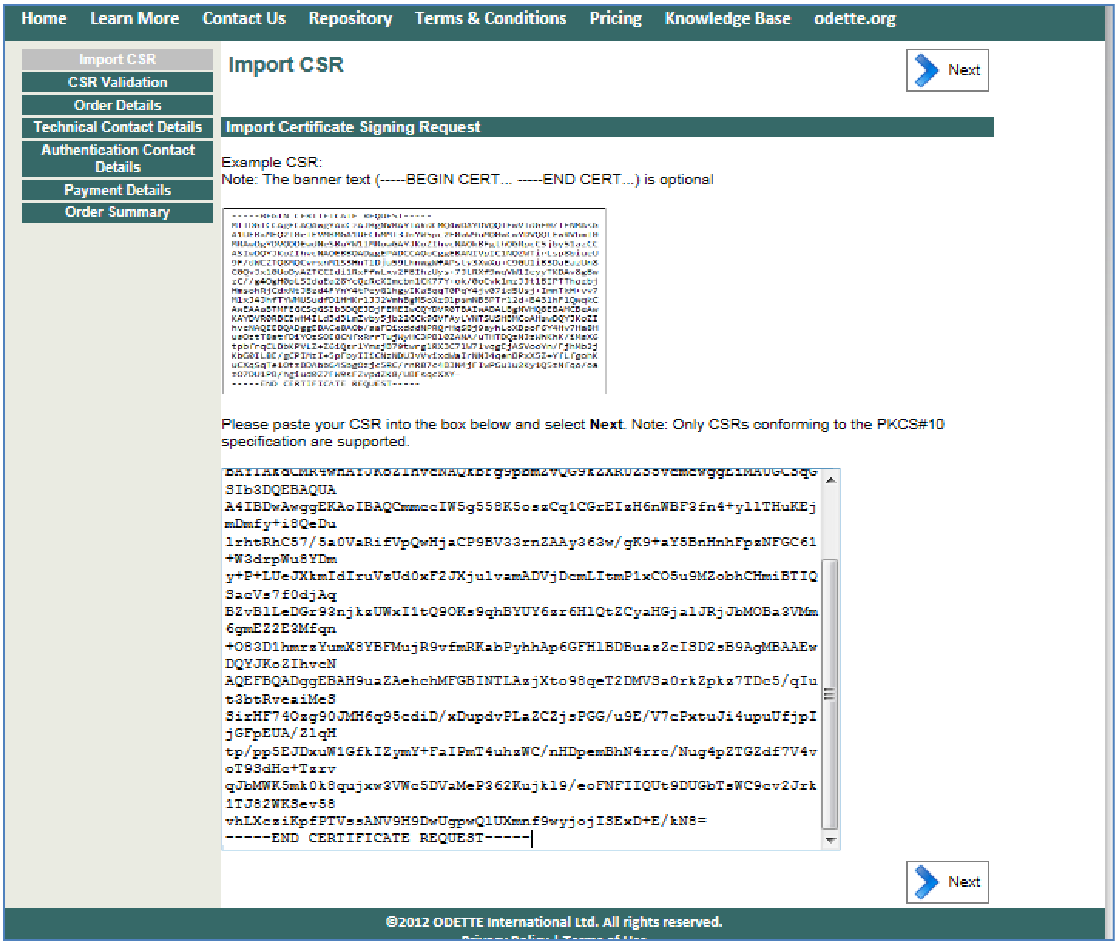
You can check whether the operation was successful by inspecting the Windows keystore.
The Certificate should be listed under Certificate Enrolment Requests of the current user and the symbol should show a key in the upper left corner, indicating that you possess a private key.

See annexe 2 for detailed instructions on how to access the Windows keystore.

Continue at Chapter 5 of this document.

4. *Importing a previously created CSR*

After you have created a key pair and a corresponding CSR with an external programme (refer to annexe 5 for more information) you should open the CSR text file and copy the content into the corresponding space in the Odette CA application.



Import CSR

Import Certificate Signing Request

Example CSR:
Note: The banner text (-----BEGIN CERT... -----END CERT...) is optional

```
-----BEGIN CERTIFICATE REQUEST-----
[illegible]
-----END CERTIFICATE REQUEST-----
```

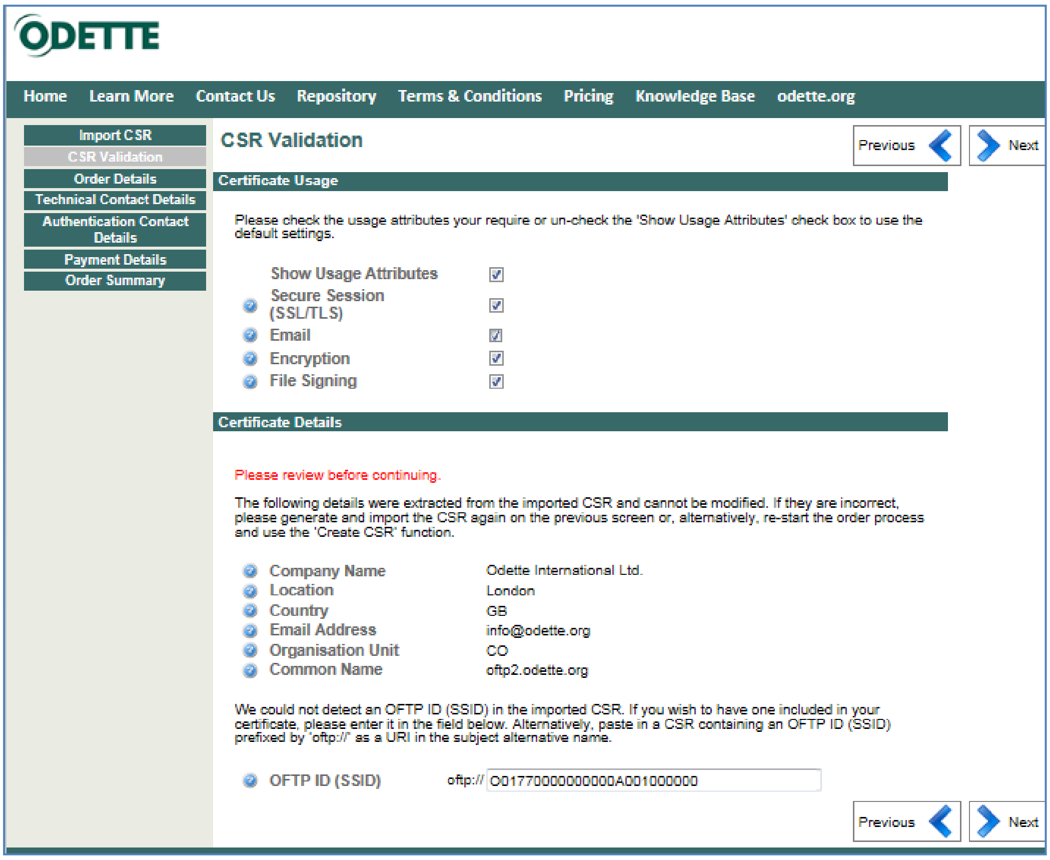
Please paste your CSR into the box below and select **Next**. Note: Only CSRs conforming to the PKCS#10 specification are supported.

```
SIb3DQEBAQUA
A4IBDwAwggEKAoIBAQCmmccIW5g558K5oszCq1CGrEIzH6nWBF3fn4+yl1THuKEj
mDmfy+i8QeDu
1rhtRhC57/5a0VaRifVpQwHjaCP9BV33rnZAAy363w/gK9+aY5BnHnhFpzNFGC61
+W3drpWu8YDm
y+P+LUeJXkmIdIruVzUd0xF2JXjulvamADVjDcmLItmP1xCO5u9MZobhCHmiBTIQ
SacVs7f0djAq
BZvB1LeDGr93njkzUWxI1tQ9OKs9qhBYUY6zr6H1QtZCyaHGja1JRjJbMOBa3VMm
6gmEZ2E3Mfqn
+O83D1hmrzYumX8YBFMujR9vfmRKabPyhhAp6GFH1BDBuazZcISD2sB9AgMBAAEw
DQYJKoZIhvcN
AQEFBQADggEBAH9uaZAehchMFGBINTLAzjXto98qeT2DMVSa0rkZpkz7TDc5/qIu
t3btRveaiMeS
SizHF74Ozg90JMH6q95cdiD/xDupdvPLaZCZjsPGG/u9E/V7cPxtuJi4upuUfjpI
jGFpEUA/Z1qH
tp/pp5EJDxuW1GfkIZymY+FaIPmT4uhzWC/nHDpemBhN4rrc/Nug4pZTGZdf7V4v
oT98dHc+Tzrv
qJbMWK5mk0k8qujxw3VWc5DVaMeP362Kujkl9/eoFNFIIQUt9DUGbTsWC9cv2Jrk
1TJ82WKSev58
vhLXcziKpfPTVssANV9H9DwUgpwQ1UXmnf9wyjojISExD+E/kN8=
-----END CERTIFICATE REQUEST-----
```

©2012 ODETTE International Ltd. All rights reserved.

Click *Next* to continue.

The details of your CSR will be shown. You will also have the opportunity to add the OFTP ID (SSID) since this auxiliary information often cannot be included in a separately created CSR.



CSR Validation

Certificate Usage

Please check the usage attributes your require or un-check the 'Show Usage Attributes' check box to use the default settings.

Show Usage Attributes ☑
Secure Session (SSL/TLS) ☑
Email ☑
Encryption ☑
File Signing ☑

Certificate Details

Please review before continuing.

The following details were extracted from the imported CSR and cannot be modified. If they are incorrect, please generate and import the CSR again on the previous screen or, alternatively, re-start the order process and use the 'Create CSR' function.

Company Name	Odette International Ltd.
Location	London
Country	GB
Email Address	info@odette.org
Organisation Unit	CO
Common Name	oftp2.odette.org

We could not detect an OFTP ID (SSID) in the imported CSR. If you wish to have one included in your certificate, please enter it in the field below. Alternatively, paste in a CSR containing an OFTP ID (SSID) prefixed by 'oftp://' as a URI in the subject alternative name.

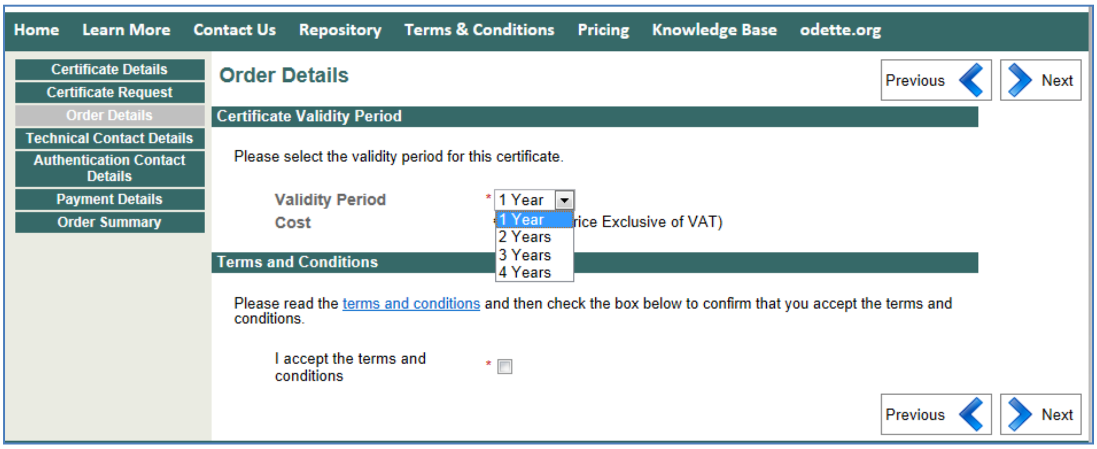
OFTP ID (SSID) oftp:// O0177000000000A001000000

Click *Next* to continue

5. *Purchase Details*

On this page you select the desired validity period of the certificate (1 to 4 years).

Before continuing, you need to accept the terms and conditions of the Odette CA.



Order Details

Certificate Validity Period

Please select the validity period for this certificate.

Validity Period * 1 Year

Cost rice Exclusive of VAT)

Terms and Conditions

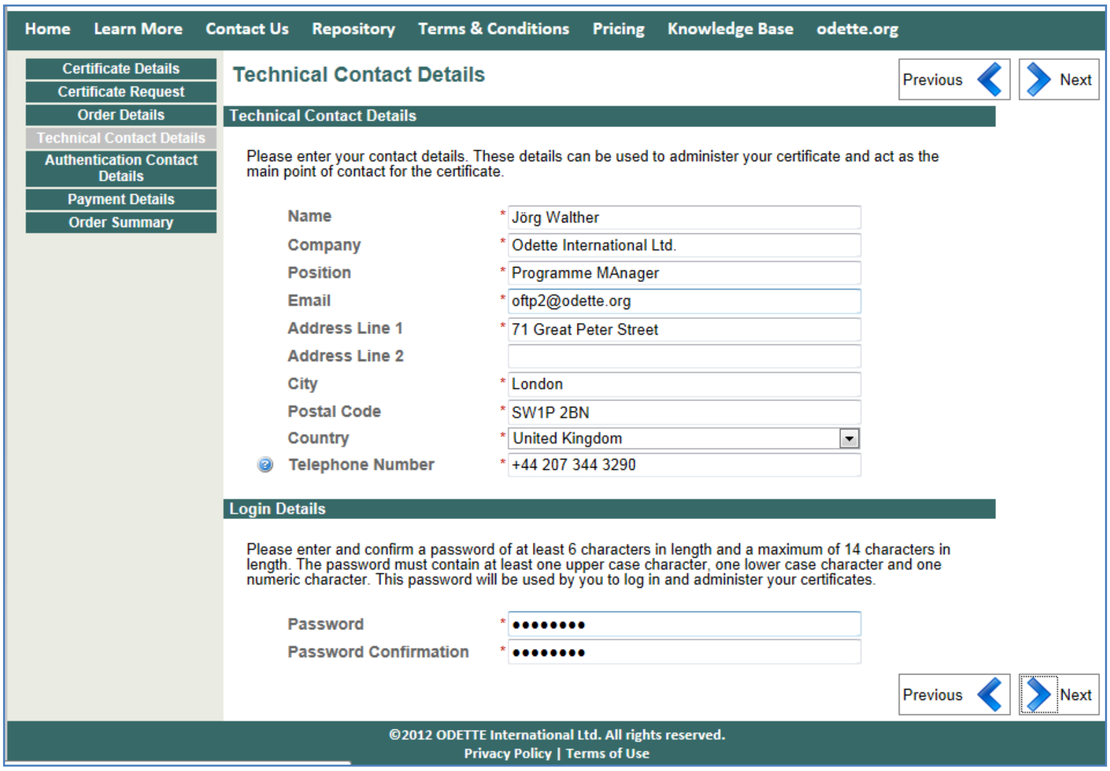
Please read the terms and conditions and then check the box below to confirm that you accept the terms and conditions.

I accept the terms and conditions * □

Click *Next* to continue.

6. Technical Contact

If ordering for the first time, you will need to enter the Technical Contact details and you will also be asked to assign a password to your account.



Technical Contact Details

Technical Contact Details

Please enter your contact details. These details can be used to administer your certificate and act as the main point of contact for the certificate.

Name	* Jörg Walther
Company	* Odette International Ltd.
Position	* Programme MAnager
Email	* oftp2@odette.org
Address Line 1	* 71 Great Peter Street
Address Line 2	
City	* London
Postal Code	* SW1P 2BN
Country	* United Kingdom
Telephone Number	* +44 207 344 3290

Login Details

Please enter and confirm a password of at least 6 characters in length and a maximum of 14 characters in length. The password must contain at least one upper case character, one lower case character and one numeric character. This password will be used by you to log in and administer your certificates.

Password	* ••••••••
Password Confirmation	* ••••••••

©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

Click *Next* to continue.

This data will be used to update your User account in the Odette CA application.

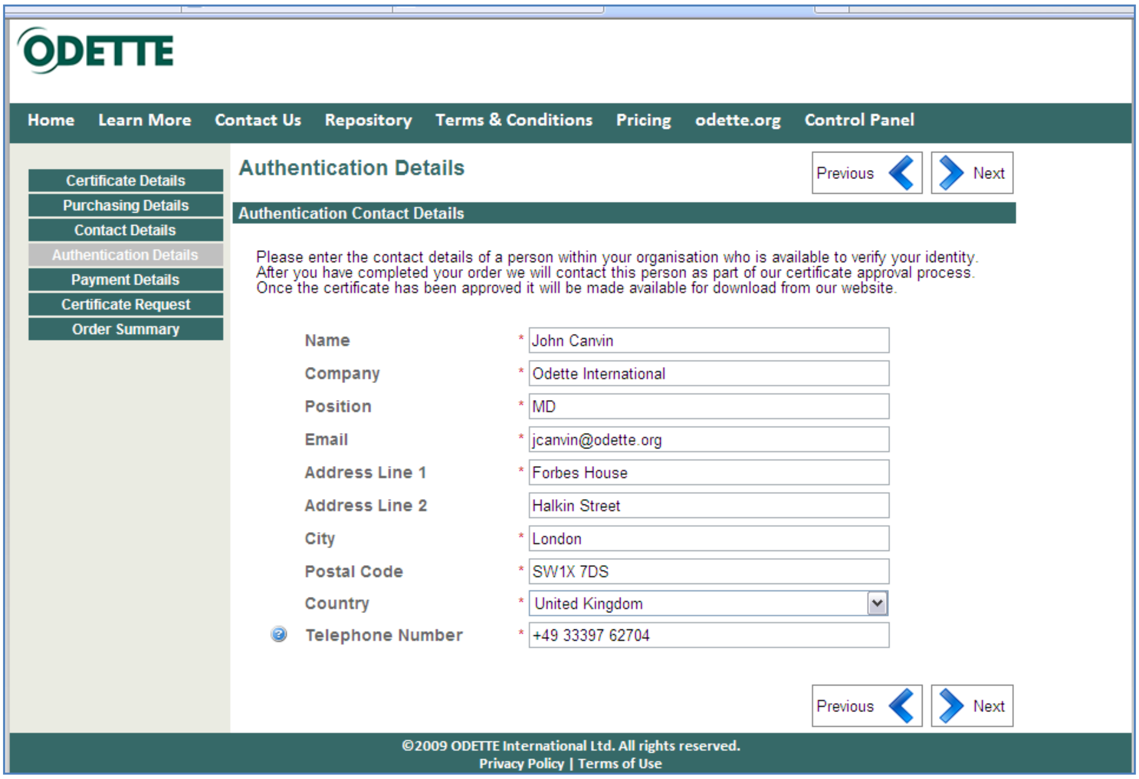
In subsequent certificate orders the Technical Contact details will be pre-populated from your user details. These can be changed, if necessary.

7. Authentication Contact

The Authentication Contact is used to verify your certificate request. He/she will be asked to confirm the data provided by you and that you are authorised to request a certificate on behalf of your company or department. Depending on the structure of your company the Authentication Contact could be the head of your department, the CIO or the managing director.

Please note that the Authentication Contact must:

i. Belong to the organisation for which the certificate is intended
ii. Be in a position to authorise the certificate order
iii. Not be the same as the Technical Contact.



Authentication Details

Authentication Contact Details

Please enter the contact details of a person within your organisation who is available to verify your identity.
After you have completed your order we will contact this person as part of our certificate approval process.
Once the certificate has been approved it will be made available for download from our website.

Name	*	John Canvin
Company	*	Odette International
Position	*	MD
Email	*	jcanvin@odette.org
Address Line 1	*	Forbes House
Address Line 2		Halkin Street
City	*	London
Postal Code	*	SW1X 7DS
Country	*	United Kingdom
Telephone Number	*	+49 33397 62704

©2009 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

Complete the required fields and click *Next* to continue.

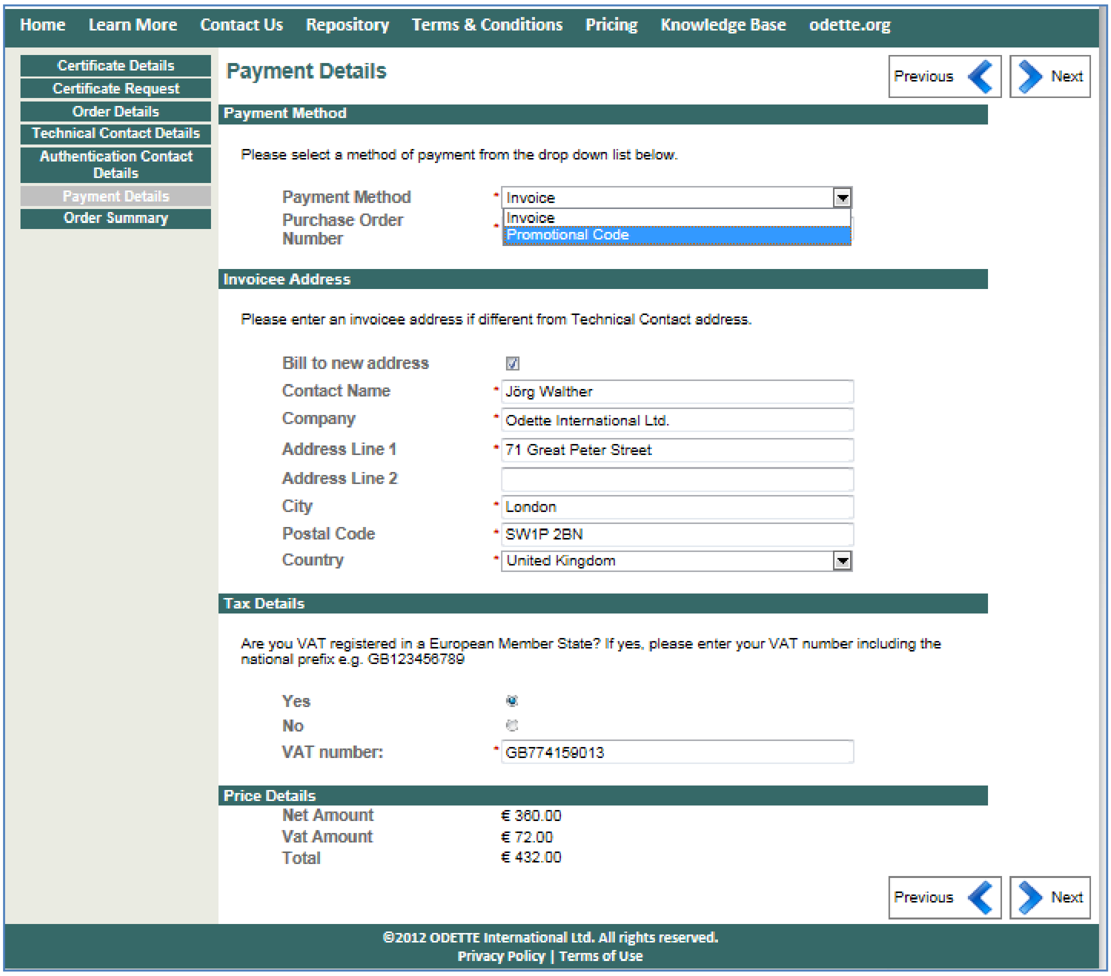
8. Payment details

Payment Method: If you are making a normal purchase of a cerificate you should select ‘Invoice’. If you have a special promotion code from Odette you should select ‘Promotional Code’. You will then be presented with a version of the screen which will allow you to enter your promotion code.

Purchase Order: You can enter any purchase order number you wish to have included as a reference on your invoice.

By default, the invoicing address is the one entered for the Technical Contact. If you wish the invoice to be sent to a different address or a different company, tick the box “Bill to new address” and enter the different address data.

Companies situated in the EU must provide their VAT registration number (including the appropriate country prefix).



Payment Details

Payment Method

Please select a method of payment from the drop down list below.

Payment Method *	Invoice ▾ Invoice Promotional Code
Purchase Order Number *	

Invoicee Address

Please enter an invoicee address if different from Technical Contact address.

Bill to new address	☑
Contact Name *	Jörg Walther
Company *	Odette International Ltd.
Address Line 1 *	71 Great Peter Street
Address Line 2	
City *	London
Postal Code *	SW1P 2BN
Country *	United Kingdom ▾

Tax Details

Are you VAT registered in a European Member State? If yes, please enter your VAT number including the national prefix e.g. GB123456789

Yes	●
No	○
VAT number: *	GB774159013

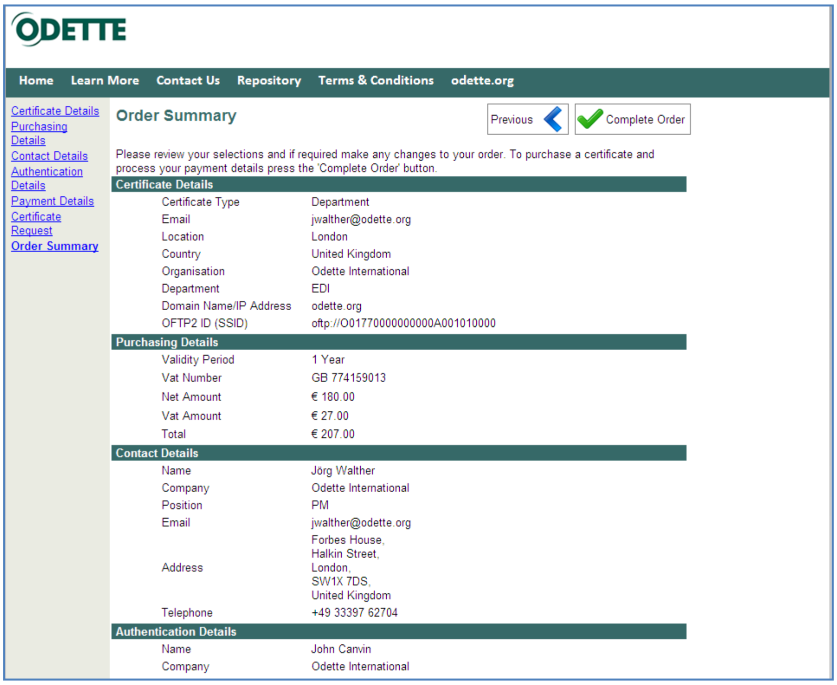
Price Details

Net Amount	€ 360.00
Vat Amount	€ 72.00
Total	€ 432.00

©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

Click *Next* to continue.

9. *Review and complete your certificate order.*

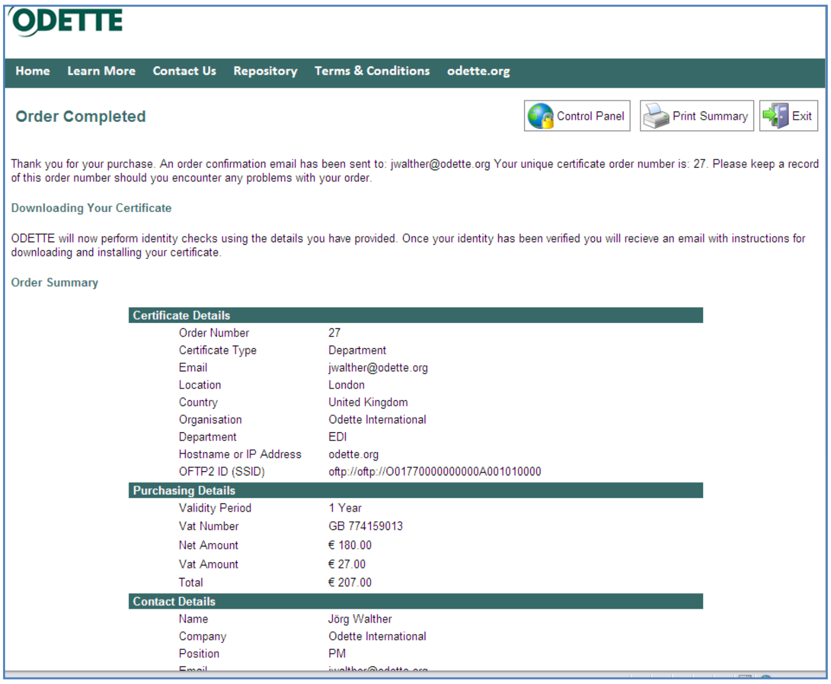


Order Summary

Please review your selections and if required make any changes to your order. To purchase a certificate and process your payment details press the 'Complete Order' button.

Certificate Details	
Certificate Type	Department
Email	jwalther@odette.org
Location	London
Country	United Kingdom
Organisation	Odette International
Department	EDI
Domain Name/IP Address	odette.org
OFTP2 ID (SSID)	oftp://O0177000000000A001010000
Purchasing Details	
Validity Period	1 Year
Vat Number	GB 774159013
Net Amount	€ 180.00
Vat Amount	€ 27.00
Total	€ 207.00
Contact Details	
Name	Jörg Walther
Company	Odette International
Position	PM
Email	jwalther@odette.org
Address	Forbes House, Halkin Street, London, SW1X 7DS, United Kingdom
Telephone	+49 33397 62704
Authentication Details	
Name	John Canvin
Company	Odette International

A summary of your order will be displayed. Check carefully and, if OK, click *Complete Order*.



Order Completed

Thank you for your purchase. An order confirmation email has been sent to: jwalther@odette.org Your unique certificate order number is: 27. Please keep a record of this order number should you encounter any problems with your order.

Downloading Your Certificate

ODETTE will now perform identity checks using the details you have provided. Once your identity has been verified you will recieve an email with instructions for downloading and installing your certificate.

Order Summary

Certificate Details	
Order Number	27
Certificate Type	Department
Email	jwalther@odette.org
Location	London
Country	United Kingdom
Organisation	Odette International
Department	EDI
Hostname or IP Address	odette.org
OFTP2 ID (SSID)	oftp://oftp://O0177000000000A001010000
Purchasing Details	
Validity Period	1 Year
Vat Number	GB 774159013
Net Amount	€ 180.00
Vat Amount	€ 27.00
Total	€ 207.00
Contact Details	
Name	Jörg Walther
Company	Odette International
Position	PM
Email	jwalther@odette.org

10. Order confirmation

You will receive an order confirmation by email.

```
Dear [user name],

Thank you for purchasing a digital certificate from ODETTE.

Your unique certificate order number is: xx. Please keep a record of this number in
case of any problems with your order. To view the status of your certificate order or
purchase further certificates please log into your account control panel using your
email address and password provided during purchase. The account control panel is
available at the following address: http://www.odetteca.com

An invoice has been attached to this email which must be paid within 30 days of the
certificate being issued.

Should you have any queries of problems please email us at odetteca@odette.org

Certificate Details:
********************
. . .
```

The invoice (pdf) for the certificate will be attached to this mail.

11. Validation and approval process

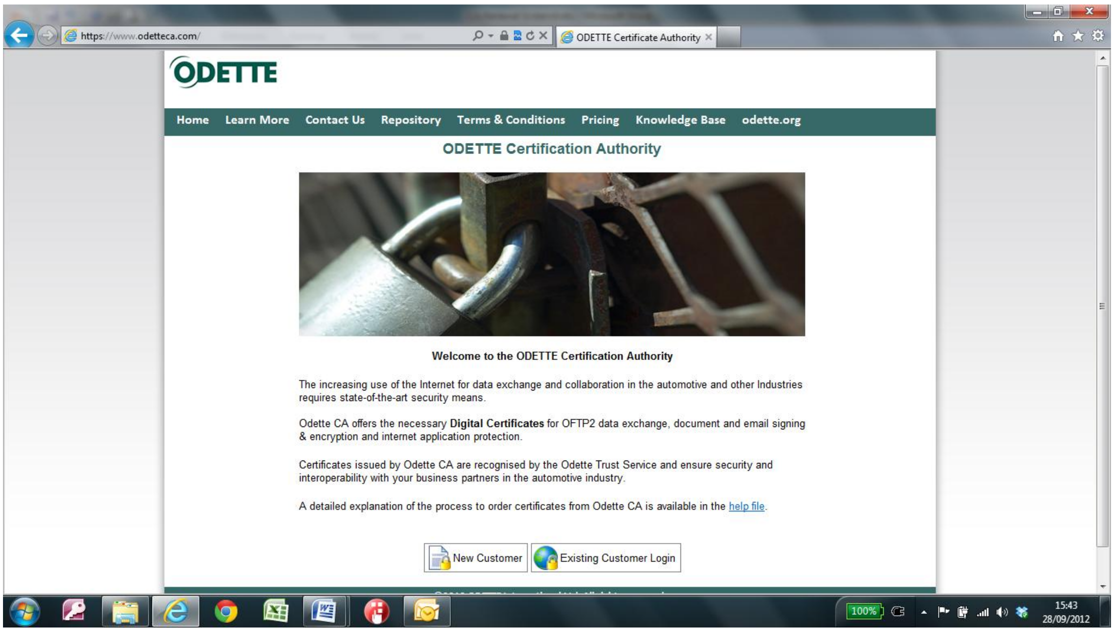
As soon as the order has been made, the Odette CA will start the validation process.

The validation is based on Odette CA Certificate Policy. Upon approval of the request you will receive information via email:

```
Dear [user name],

We are pleased to inform you that your certificate with order reference of: xx has now
been issued. This means that your identity has been confirmed and you may download and
start using the certificate.

If payment has not been received after 30 days from the date of this email your
certificate will be revoked and will cease to be valid.

To download and start using your certificate please login to your account control
panel and follow the on screen instructions. To log in please navigate your browser to
the following address: https://www.odetteca.com
```

12. Download and install the certificate

Click *Existing Customer Login* to log into the CA application with your user credentials.



ODETTE Certification Authority

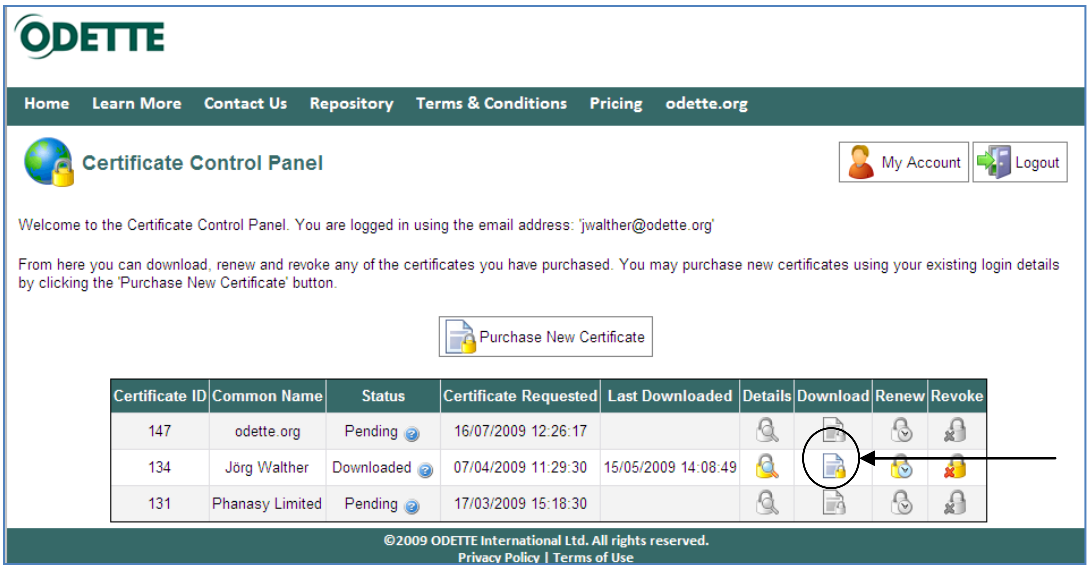
Welcome to the ODETTE Certification Authority

The increasing use of the Internet for data exchange and collaboration in the automotive and other Industries requires state-of-the-art security means.

Odette CA offers the necessary **Digital Certificates** for OFTP2 data exchange, document and email signing & encryption and internet application protection.

Certificates issued by Odette CA are recognised by the Odette Trust Service and ensure security and interoperability with your business partners in the automotive industry.

A detailed explanation of the process to order certificates from Odette CA is available in the help file.



Certificate Control Panel

Welcome to the Certificate Control Panel. You are logged in using the email address: 'jwalther@odette.org'

From here you can download, renew and revoke any of the certificates you have purchased. You may purchase new certificates using your existing login details by clicking the 'Purchase New Certificate' button.

Certificate ID	Common Name	Status	Certificate Requested	Last Downloaded	Details	Download	Renew	Revoke
147	odette.org	Pending	16/07/2009 12:26:17		🔍	📄	🔒	🔒
134	Jörg Walther	Downloaded	07/04/2009 11:29:30	15/05/2009 14:08:49	🔍	📄	🔒	🔒
131	Phanasy Limited	Pending	17/03/2009 15:18:30		🔍	📄	🔒	🔒

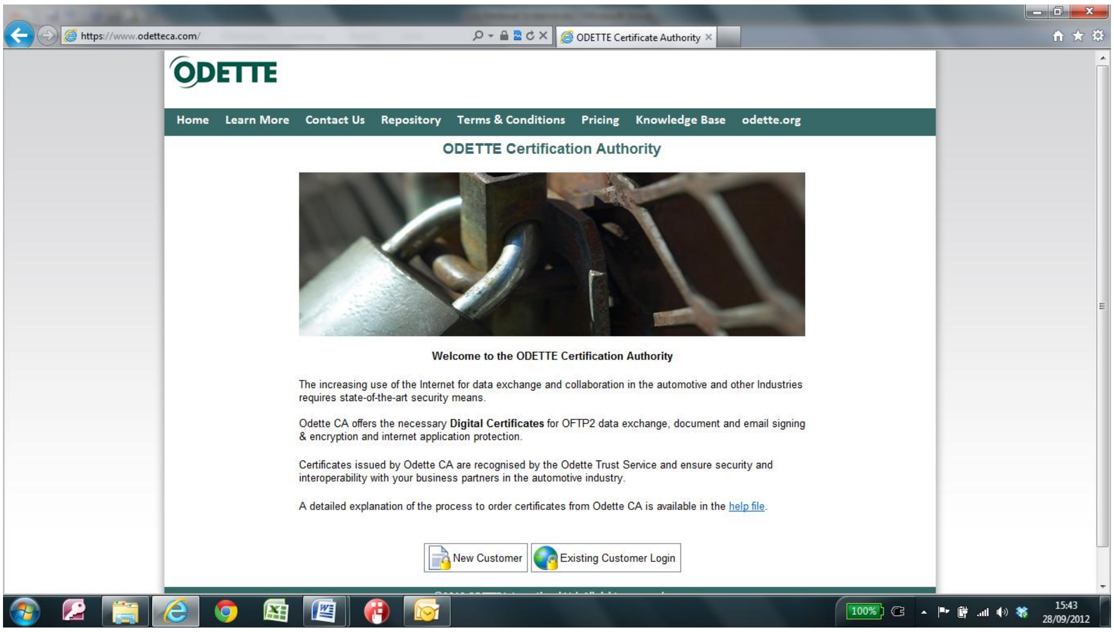
©2009 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

Click the Download icon alongside the appropriate certificate to start the download process.

To install the certificate, follow the instructions in annexe 1 (for CSR created online) or annexe 7 (for CSR created with an external tool).

13. Renew a certificate

Click *Existing Customer Login* to log into the CA application with your user credentials.



ODETTE Certification Authority

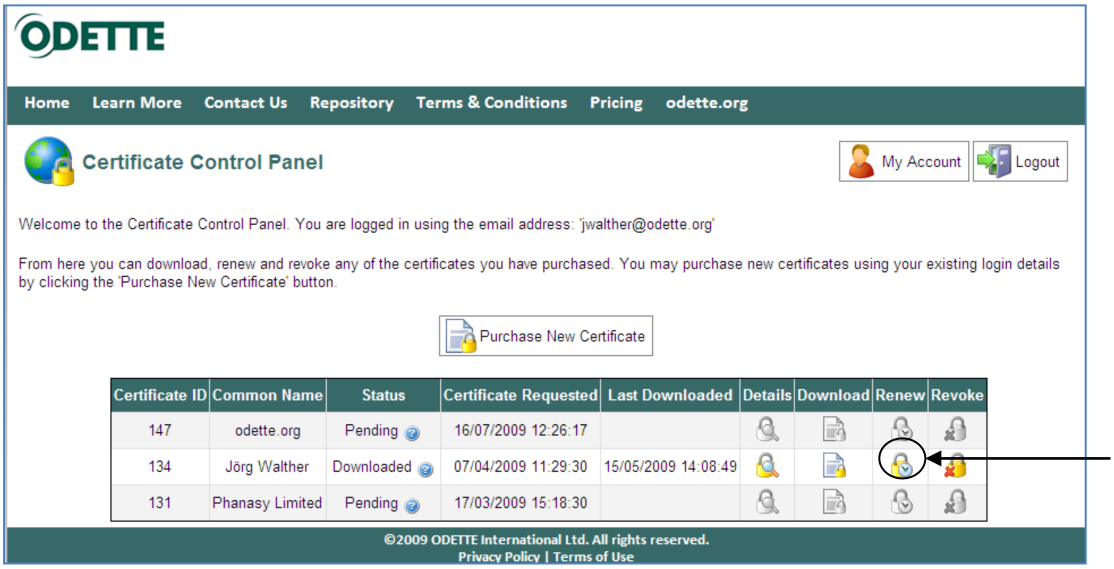
Welcome to the ODETTE Certification Authority

The increasing use of the Internet for data exchange and collaboration in the automotive and other Industries requires state-of-the-art security means.

Odette CA offers the necessary **Digital Certificates** for OFTP2 data exchange, document and email signing & encryption and internet application protection.

Certificates issued by Odette CA are recognised by the Odette Trust Service and ensure security and interoperability with your business partners in the automotive industry.

A detailed explanation of the process to order certificates from Odette CA is available in the help file.



Certificate Control Panel

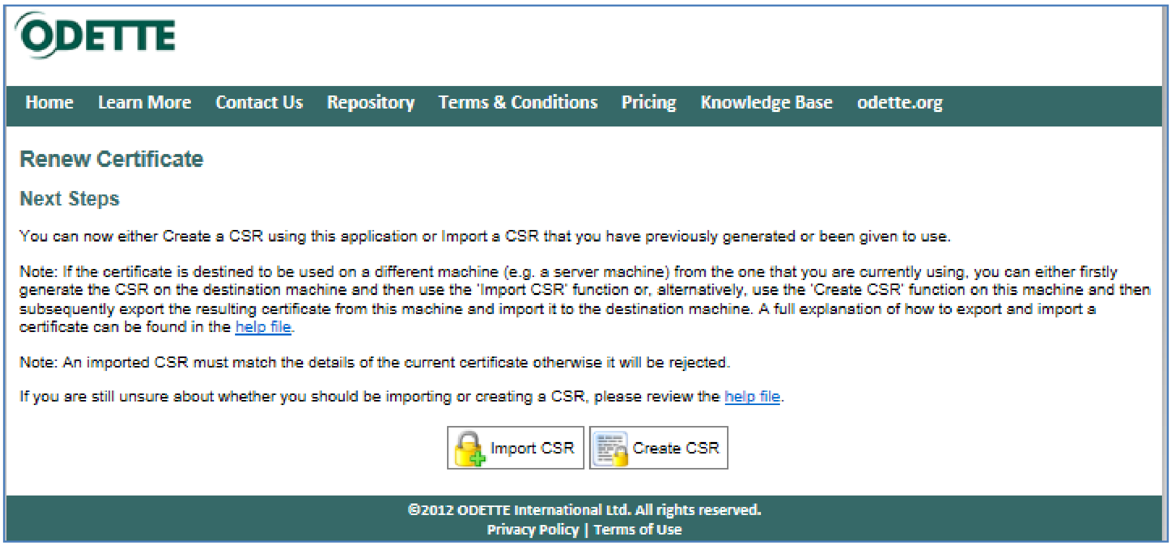
Welcome to the Certificate Control Panel. You are logged in using the email address: 'jwalther@odette.org'

From here you can download, renew and revoke any of the certificates you have purchased. You may purchase new certificates using your existing login details by clicking the 'Purchase New Certificate' button.

Certificate ID	Common Name	Status	Certificate Requested	Last Downloaded	Details	Download	Renew	Revoke
147	odette.org	Pending	16/07/2009 12:26:17					
134	Jörg Walther	Downloaded	07/04/2009 11:29:30	15/05/2009 14:08:49				
131	Phanasy Limited	Pending	17/03/2009 15:18:30					

©2009 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

Click the Renew icon of the certificate you want to renew. Please note that Renewal can only be carried out during the period **starting 60 days before** the expiry date of the current certificate and **ending 30 days after** the expiry date. Outside of this period, the Renew icon will be greyed out and the function will be unavailable.



Renew Certificate

Next Steps

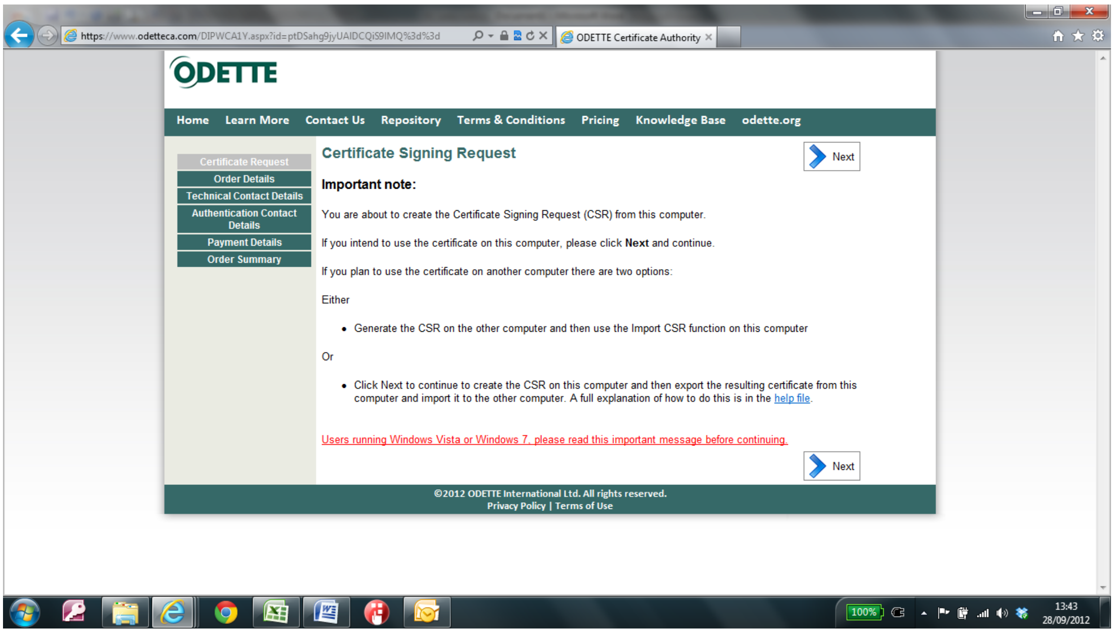
You can now either Create a CSR using this application or Import a CSR that you have previously generated or been given to use.

Note: If the certificate is destined to be used on a different machine (e.g. a server machine) from the one that you are currently using, you can either firstly generate the CSR on the destination machine and then use the 'Import CSR' function or, alternatively, use the 'Create CSR' function on this machine and then subsequently export the resulting certificate from this machine and import it to the destination machine. A full explanation of how to export and import a certificate can be found in the help file.

Note: An imported CSR must match the details of the current certificate otherwise it will be rejected.

If you are still unsure about whether you should be importing or creating a CSR, please review the help file.

You again have the choice of importing a separately created CSR or creating the CSR on-line during the Renewal process.
If you chose on-line creation then the stored certificate details will be used to create the CSR (for separate off-line generation of the CSR see chapter 4).


https://www.odetteca.com/DIPWCA1Y.aspx?id=ptDSahg9jyUAIDCQiS9IMQ%3d%3d
ODETTE Certificate Authority
ODETTE
Home
Learn More
Contact Us
Repository
Terms & Conditions
Pricing
Knowledge Base
odette.org
Certificate Request
Order Details
Technical Contact Details
Authentication Contact Details
Payment Details
Order Summary
Next
Next
©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use
100%
13:43
28/09/2012

Certificate Signing Request

Important note:

You are about to create the Certificate Signing Request (CSR) from this computer.

If you intend to use the certificate on this computer, please click **Next** and continue.

If you plan to use the certificate on another computer there are two options:

Either

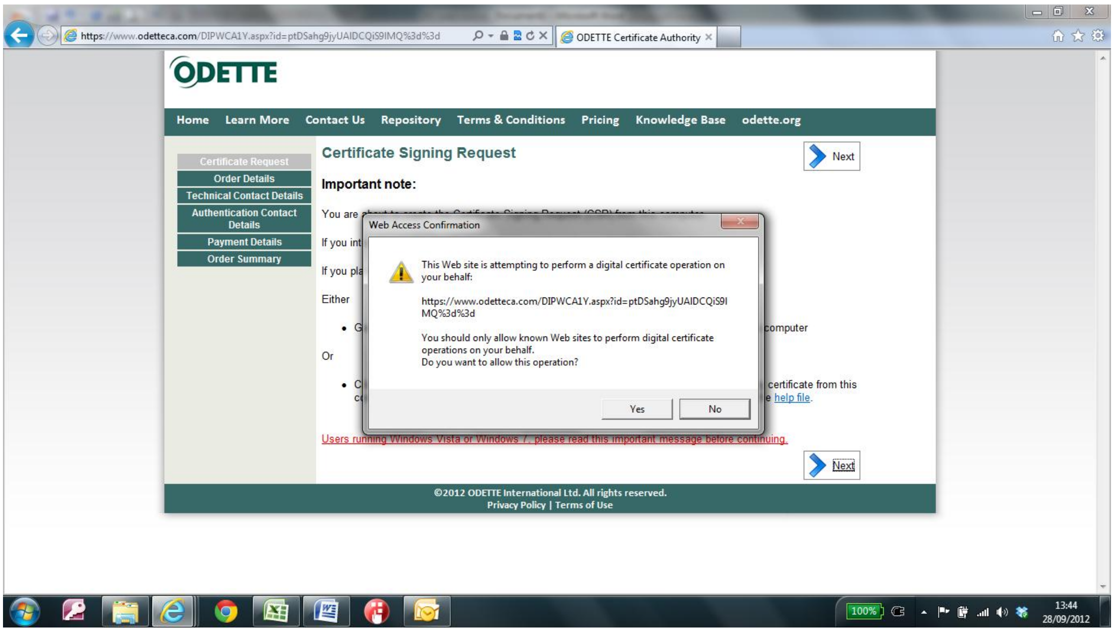
- Generate the CSR on the other computer and then use the Import CSR function on this computer

Or

- Click Next to continue to create the CSR on this computer and then export the resulting certificate from this computer and import it to the other computer. A full explanation of how to do this is in the help file.

Users running Windows Vista or Windows 7, please read this important message before continuing.

Click *Next* to continue



https://www.odetteca.com/DIPWCA1Y.aspx?id=ptDSahg9jyUAIDCQiS9IMQ%3d%3d

ODETTE Certificate Authority

Certificate Signing Request

Important note:

You are

If you int

If you pla

Either

- G

Or

- C

computer

certificate from this

help file.

Users running Windows Vista or Windows 7, please read this important message before continuing.

Web Access Confirmation

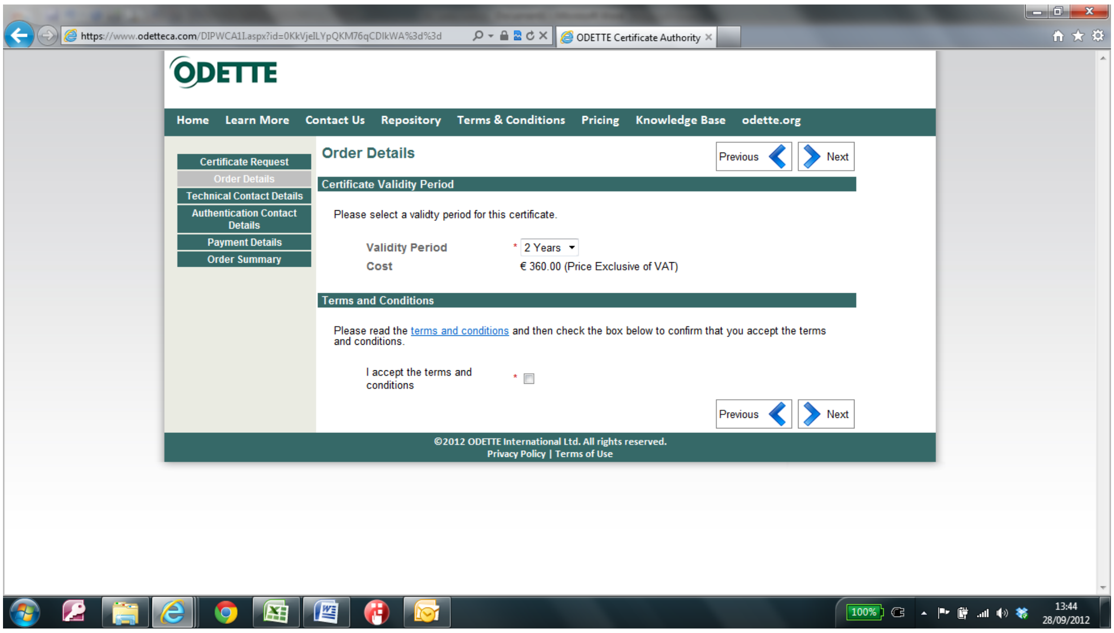
This Web site is attempting to perform a digital certificate operation on your behalf:

https://www.odetteca.com/DIPWCA1Y.aspx?id=ptDSahg9jyUAIDCQiS9IMQ%3d%3d

You should only allow known Web sites to perform digital certificate operations on your behalf.
Do you want to allow this operation?

©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

Click *Yes* to continue.



https://www.odetteca.com/DIPWCA1I.aspx?id=0KkVjeILYpQKM76qCDlkWA%3d%3d

ODETTE Certificate Authority

Order Details

Certificate Validity Period

Please select a validty period for this certificate.

Validity Period * 2 Years

Cost € 360.00 (Price Exclusive of VAT)

Terms and Conditions

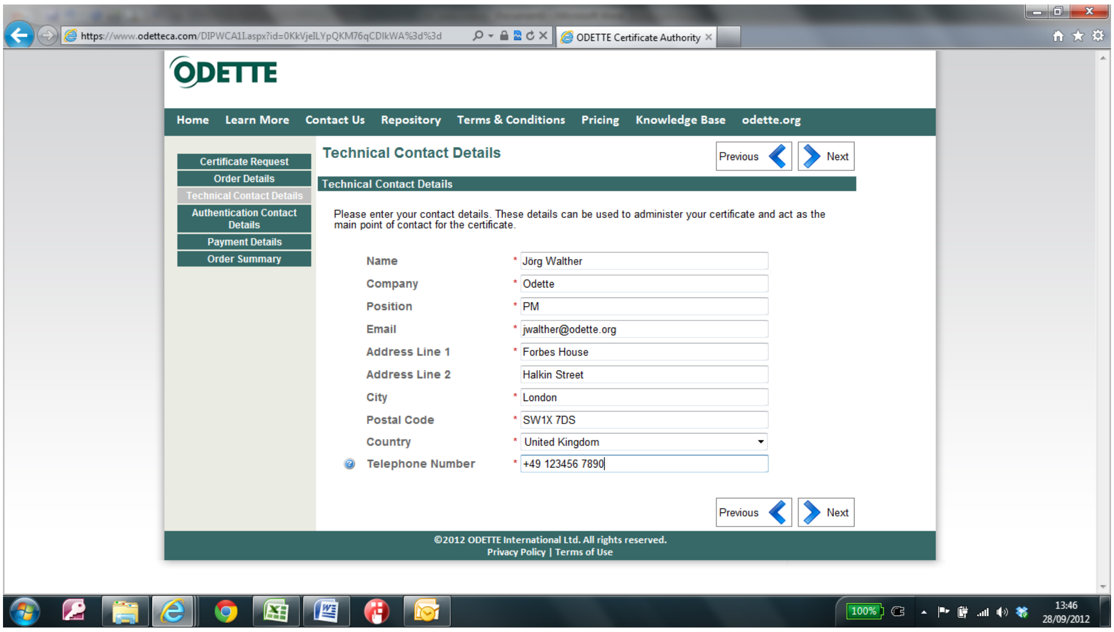
Please read the terms and conditions and then check the box below to confirm that you accept the terms and conditions.

I accept the terms and conditions * □

©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

On this page you select the desired validity period of the renewed certificate (1 to 4 years).

Accept the terms and conditions and click *Next* to continue.


https://www.odetteca.com/DIPWCA11.aspx?id=0KkVjelLYpQKM76qCDlkWA%3d%3d
ODETTE Certificate Authority
ODETTE
Home
Learn More
Contact Us
Repository
Terms & Conditions
Pricing
Knowledge Base
odette.org
Certificate Request
Order Details
Technical Contact Details
Authentication Contact Details
Payment Details
Order Summary
Previous
Next
©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use
100%
13:46
28/09/2012

Technical Contact Details

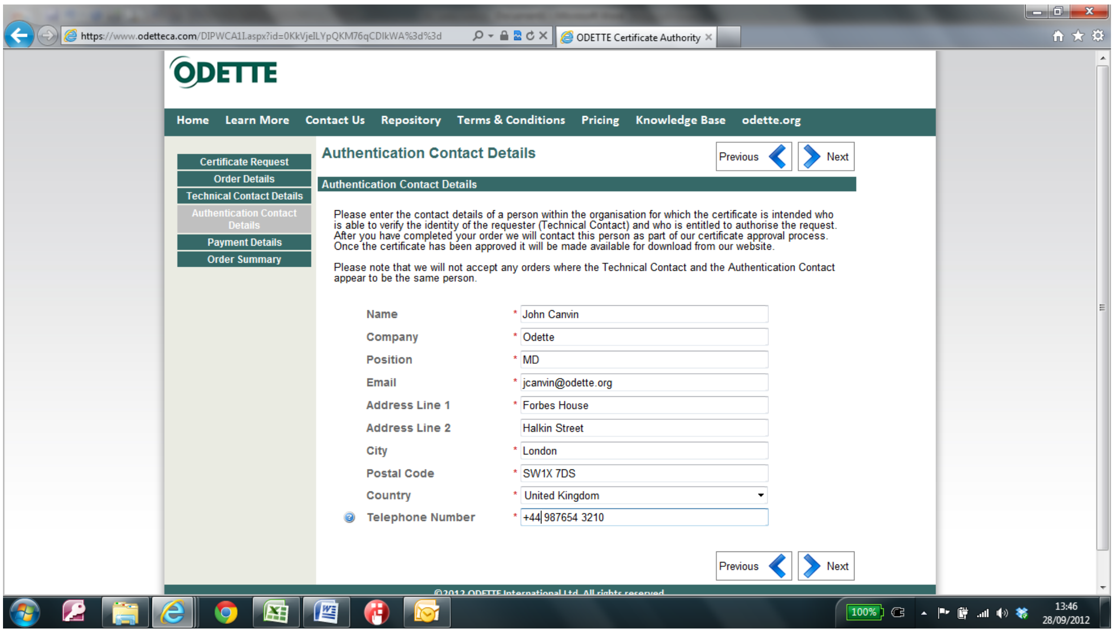
Technical Contact Details

Please enter your contact details. These details can be used to administer your certificate and act as the main point of contact for the certificate.

Name	* Jörg Walther
Company	* Odette
Position	* PM
Email	* jwalther@odette.org
Address Line 1	* Forbes House
Address Line 2	Halkin Street
City	* London
Postal Code	* SW1X 7DS
Country	* United Kingdom
Telephone Number	* +49 123456 7890

The Technical Contact details are pre-populated from the order of the certificate that is being renewed. Please check these carefully and update them if required.

Click *Next* to continue.


https://www.odetteca.com/DIPWCA11.aspx?id=0KkVjelLYpQKM76qCDlkWA%3d%3d
ODETTE Certificate Authority
ODETTE
Home
Learn More
Contact Us
Repository
Terms & Conditions
Pricing
Knowledge Base
odette.org
Certificate Request
Order Details
Technical Contact Details
Authentication Contact Details
Payment Details
Order Summary
Previous
Next
©2012 ODETTE International Ltd. All rights reserved.
100%
13:46
28/09/2012

Authentication Contact Details

Authentication Contact Details

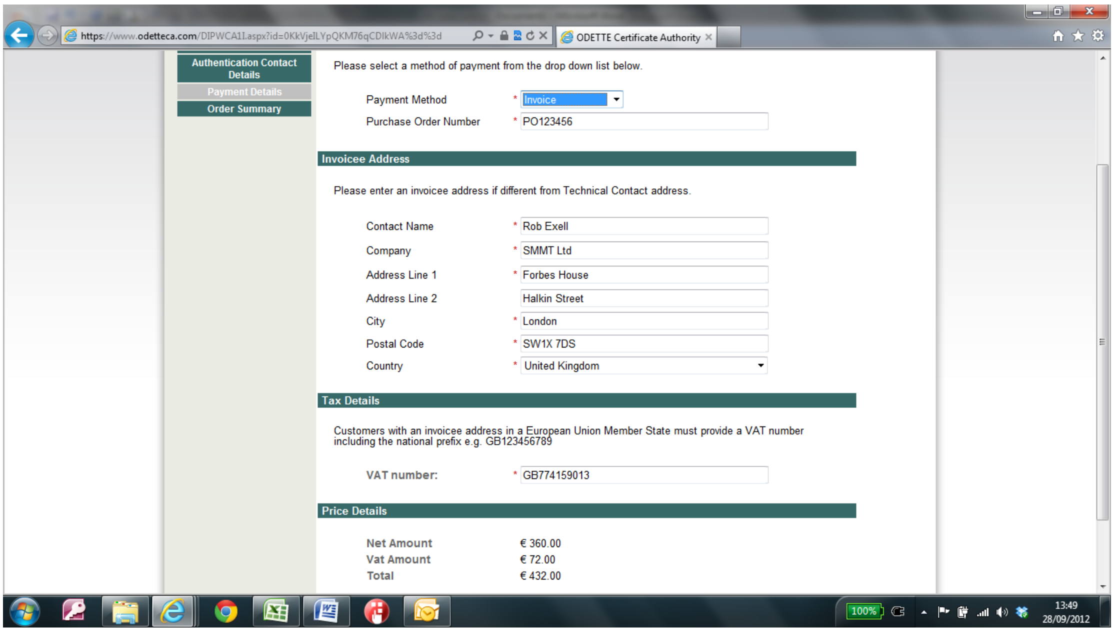
Please enter the contact details of a person within the organisation for which the certificate is intended who is able to verify the identity of the requester (Technical Contact) and who is entitled to authorise the request. After you have completed your order we will contact this person as part of our certificate approval process. Once the certificate has been approved it will be made available for download from our website.

Please note that we will not accept any orders where the Technical Contact and the Authentication Contact appear to be the same person.

Name	* John Canvin
Company	* Odette
Position	* MD
Email	* jcanvin@odette.org
Address Line 1	* Forbes House
Address Line 2	Halkin Street
City	* London
Postal Code	* SW1X 7DS
Country	* United Kingdom
Telephone Number	* +44 987654 3210

The Authentication Contact details are pre-populated from the order of the certificate that is being renewed. Please check these carefully and update them if required.

Click *Next* to continue.



https://www.odetteca.com/DIPWCA1I.aspx?id=0KkVjeILYpQKM76qCDIkWA%3d%3d
ODETTE Certificate Authority
Authentication Contact Details
Payment Details
Order Summary
100%
13:49
28/09/2012

Please select a method of payment from the drop down list below.

Payment Method	* Invoice
Purchase Order Number	* PO123456

Invoicee Address

Please enter an invoicee address if different from Technical Contact address.

Contact Name	* Rob Exell
Company	* SMMT Ltd
Address Line 1	* Forbes House
Address Line 2	Halkin Street
City	* London
Postal Code	* SW1X 7DS
Country	* United Kingdom

Tax Details

Customers with an invoicee address in a European Union Member State must provide a VAT number including the national prefix e.g. GB123456789

VAT number:	* GB774159013

Price Details

Net Amount	€ 360.00
Vat Amount	€ 72.00
Total	€ 432.00

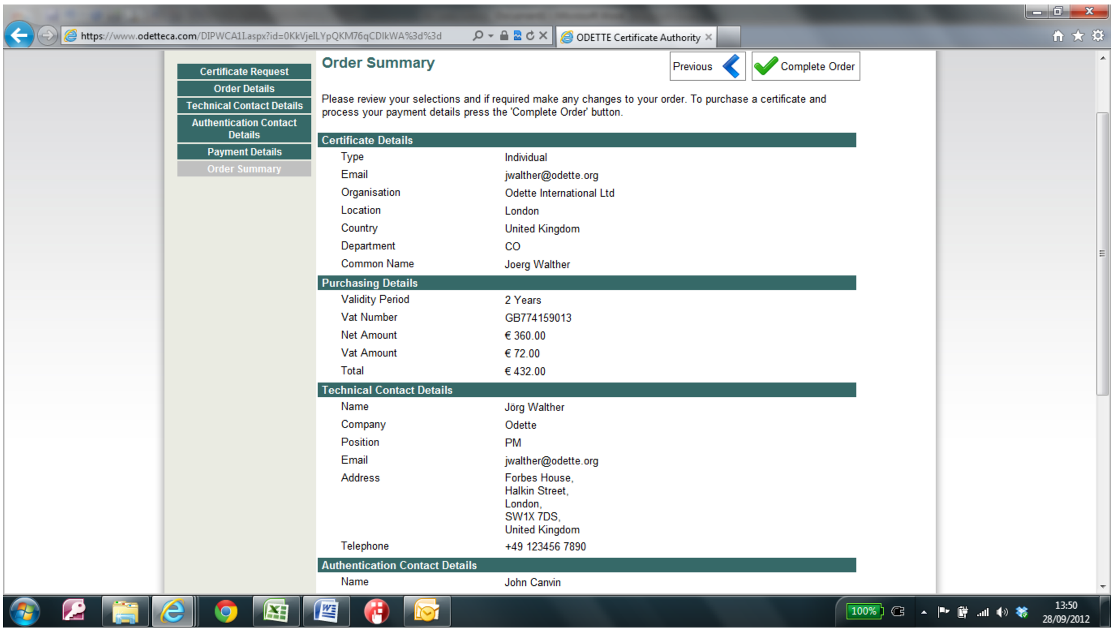
Payment Method: For a Renewal the only choice is ‘Invoice’.

Purchase Order: You can enter any purchase order number you wish to have included as a reference on your invoice.

By default, the invoicing address is the one entered for the Technical Contact. If you wish the invoice to be sent to a different address or a different company, tick the box “Bill to new address” and enter the different address data.

Companies situated in the EU must provide their VAT registration number (including the appropriate country prefix).

Click *Next* to continue.



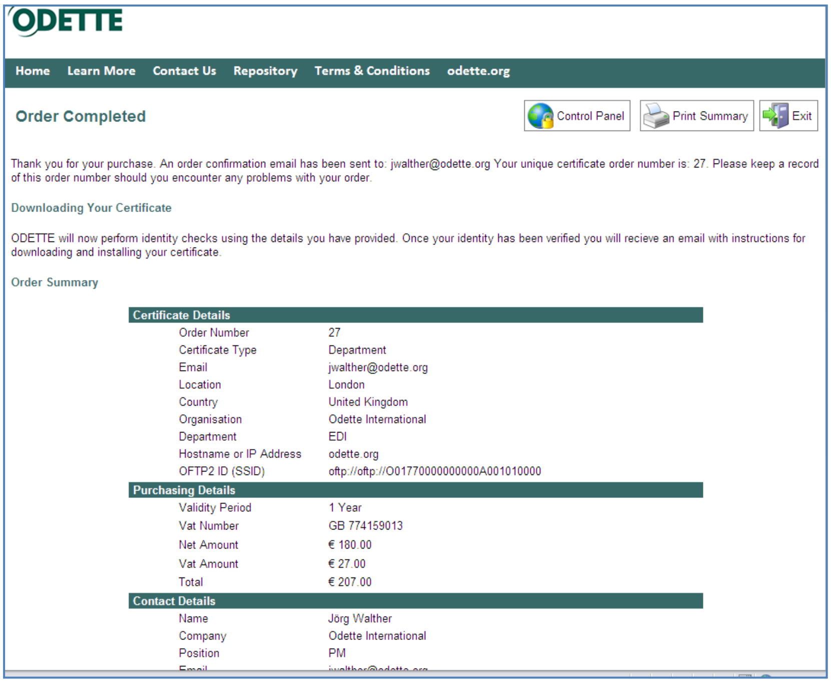
https://www.odetteca.com/DIPWCA1I.aspx?id=0KkVjeILYpQKM76qCDIkWA%3d%3d
ODETTE Certificate Authority
Certificate Request
Order Details
Technical Contact Details
Authentication Contact Details
Payment Details
Order Summary
Previous
Complete Order
100%
13:50
28/09/2012

Order Summary

Please review your selections and if required make any changes to your order. To purchase a certificate and process your payment details press the 'Complete Order' button.

Certificate Details	
Type	Individual
Email	jwalther@odette.org
Organisation	Odette International Ltd
Location	London
Country	United Kingdom
Department	CO
Common Name	Joerg Walther
Purchasing Details	
Validity Period	2 Years
Vat Number	GB774159013
Net Amount	€ 360.00
Vat Amount	€ 72.00
Total	€ 432.00
Technical Contact Details	
Name	Jörg Walther
Company	Odette
Position	PM
Email	jwalther@odette.org
Address	Forbes House, Halkin Street, London, SW1X 7DS, United Kingdom
Telephone	+49 123456 7890
Authentication Contact Details	
Name	John Canvin

You will see the summary of your order. Check it carefully and, if OK, click *Complete Order*.



Order Completed

Thank you for your purchase. An order confirmation email has been sent to: jwalther@odette.org Your unique certificate order number is: 27. Please keep a record of this order number should you encounter any problems with your order.

Downloading Your Certificate

ODETTE will now perform identity checks using the details you have provided. Once your identity has been verified you will recieve an email with instructions for downloading and installing your certificate.

Order Summary

Certificate Details	
Order Number	27
Certificate Type	Department
Email	jwalther@odette.org
Location	London
Country	United Kingdom
Organisation	Odette International
Department	EDI
Hostname or IP Address	odette.org
OFTP2 ID (SSID)	oftp://oftp://O01770000000000A001010000
Purchasing Details	
Validity Period	1 Year
Vat Number	GB 774159013
Net Amount	€ 180.00
Vat Amount	€ 27.00
Total	€ 207.00
Contact Details	
Name	Jörg Walther
Company	Odette International
Position	PM
Email	jwalther@odette.org

You will receive a confirmation email with the invoice (pdf) attached.

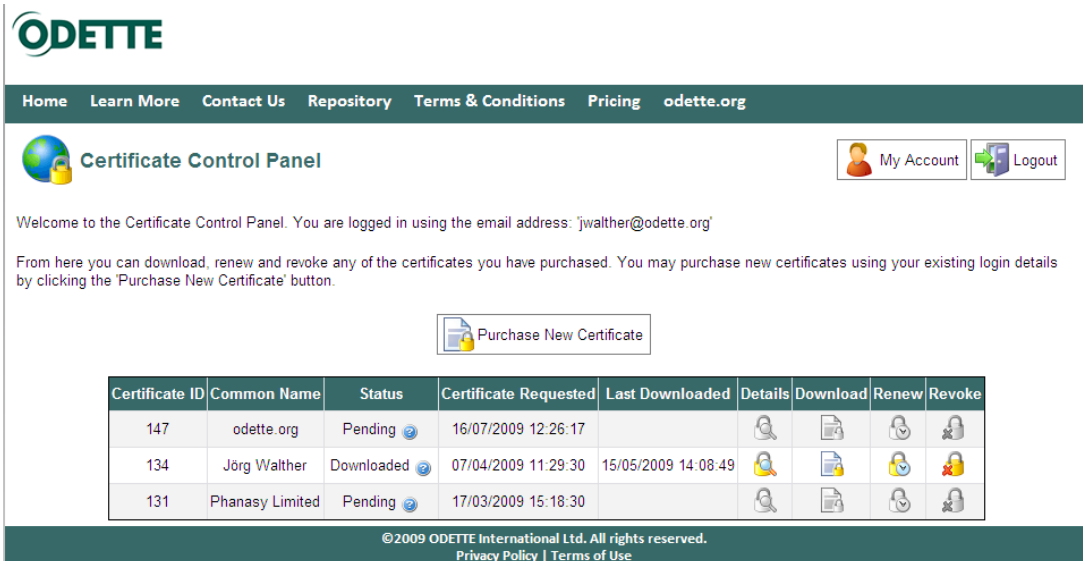
Annexes

How to download and install the certificate on your local computer (CSR has been generated on-line)

This section provides instructions for users who are downloading and installing a certificate for the first time. The example is for Microsoft Windows. Please follow the instructions relevant to your operating system.

Log into the CA application.

Click the 'Download' icon to start the certificate download dialogue.



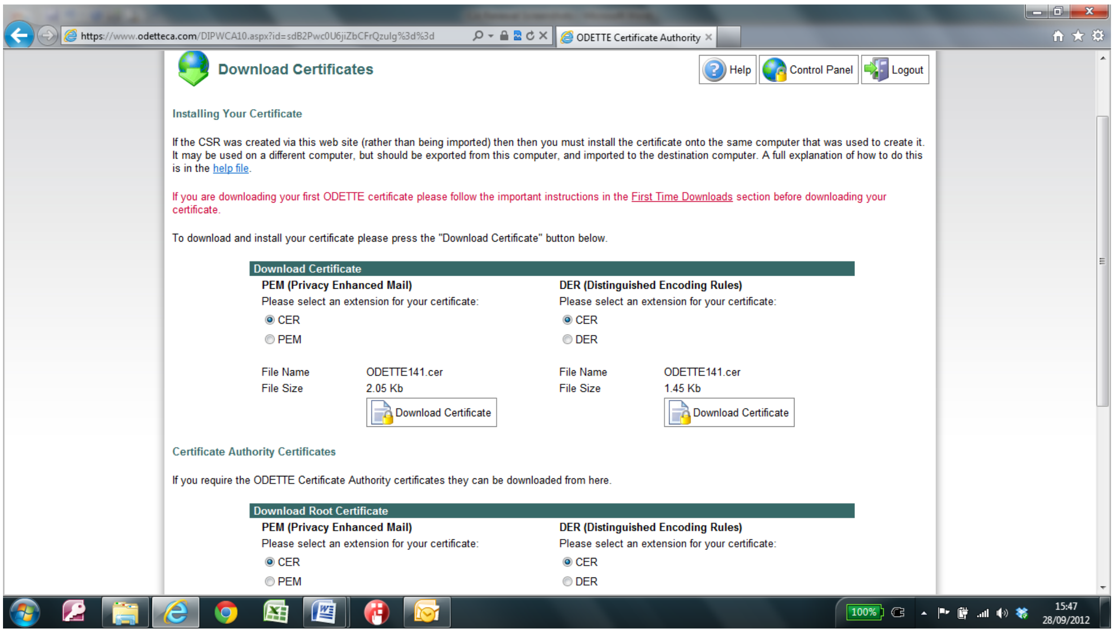
Certificate Control Panel

Welcome to the Certificate Control Panel. You are logged in using the email address: 'jwalther@odette.org'

From here you can download, renew and revoke any of the certificates you have purchased. You may purchase new certificates using your existing login details by clicking the 'Purchase New Certificate' button.

Certificate ID	Common Name	Status	Certificate Requested	Last Downloaded	Details	Download	Renew	Revoke
147	odette.org	Pending	16/07/2009 12:26:17					
134	Jörg Walther	Downloaded	07/04/2009 11:29:30	15/05/2009 14:08:49				
131	Phanasy Limited	Pending	17/03/2009 15:18:30					

©2009 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use


https://www.odetteca.com/DIPWCA10.aspx?id=sdB2Pwc0U6jiZbCFrQzulg%3d%3d
ODETTE Certificate Authority
Help
Control Panel
Logout

Download Certificates

Installing Your Certificate

If the CSR was created via this web site (rather than being imported) then then you must install the certificate onto the same computer that was used to create it. It may be used on a different computer, but should be exported from this computer, and imported to the destination computer. A full explanation of how to do this is in the help file.

If you are downloading your first ODETTE certificate please follow the important instructions in the First Time Downloads section before downloading your certificate.

To download and install your certificate please press the "Download Certificate" button below.

Download Certificate

PEM (Privacy Enhanced Mail)		DER (Distinguished Encoding Rules)	
Please select an extension for your certificate:		Please select an extension for your certificate:	
● CER		● CER	
○ PEM		○ DER	
File Name	ODETTE141.cer	File Name	ODETTE141.cer
File Size	2.05 Kb	File Size	1.45 Kb
	Download Certificate		Download Certificate

Certificate Authority Certificates

If you require the ODETTE Certificate Authority certificates they can be downloaded from here.

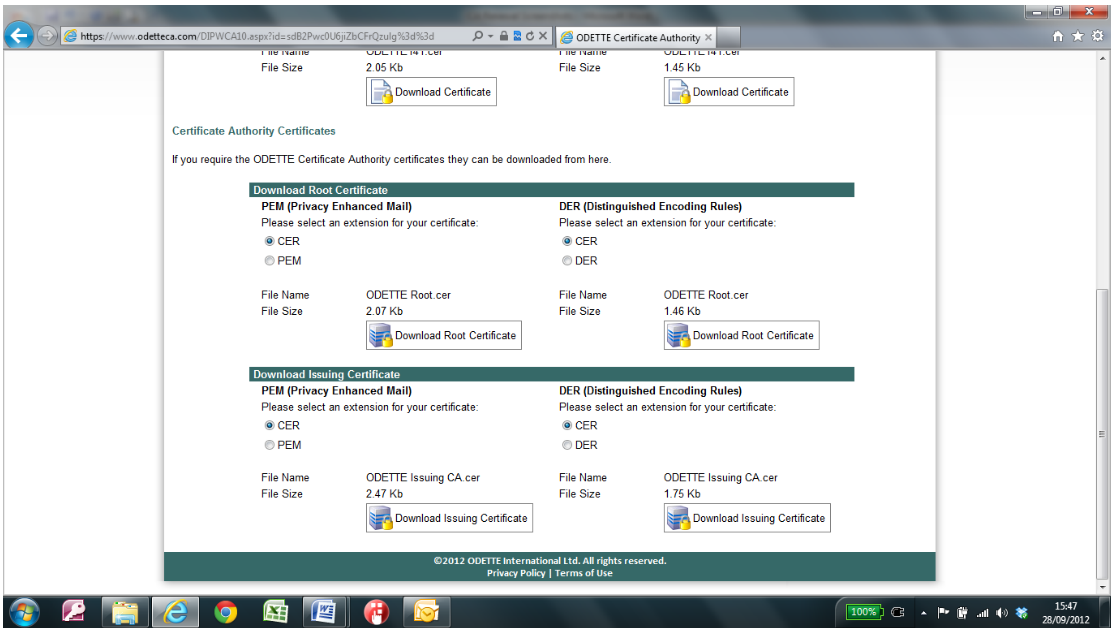
Download Root Certificate

PEM (Privacy Enhanced Mail)	DER (Distinguished Encoding Rules)
Please select an extension for your certificate:	Please select an extension for your certificate:
● CER	● CER
○ PEM	○ DER

You can select between 2 different formats and 2 different extensions. Select the one that meets the requirements of your keystore software or of your business partner, if you have to submit / upload it in a specific format.

See below for instructions on how to install your Odette Certificate plus the prior installation of the Odette Root and Issuing Certificates, if not already done.

Installing the Root Certificate



https://www.odetteca.com/DIPWCA10.aspx?id=sdB2Pwc0U6jiZbCFrQzulg%3d%3d

ODETTE Certificate Authority

File Size	2.05 Kb	File Size	1.45 Kb
	Download Certificate		Download Certificate

Certificate Authority Certificates

If you require the ODETTE Certificate Authority certificates they can be downloaded from here.

Download Root Certificate

PEM (Privacy Enhanced Mail)		DER (Distinguished Encoding Rules)	
Please select an extension for your certificate:		Please select an extension for your certificate:	
● CER		● CER	
○ PEM		○ DER	
File Name	ODETTE Root.cer	File Name	ODETTE Root.cer
File Size	2.07 Kb	File Size	1.46 Kb
	Download Root Certificate		Download Root Certificate

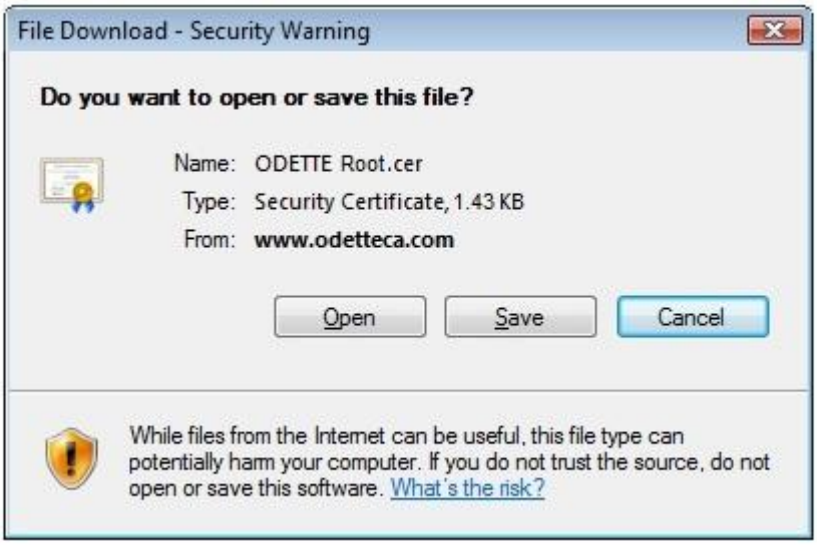
Download Issuing Certificate

PEM (Privacy Enhanced Mail)		DER (Distinguished Encoding Rules)	
Please select an extension for your certificate:		Please select an extension for your certificate:	
● CER		● CER	
○ PEM		○ DER	
File Name	ODETTE Issuing CA.cer	File Name	ODETTE Issuing CA.cer
File Size	2.47 Kb	File Size	1.75 Kb
	Download Issuing Certificate		Download Issuing Certificate

©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

1. Click *Download Root Certificate*.

2. At the following dialogue, click *Open*.



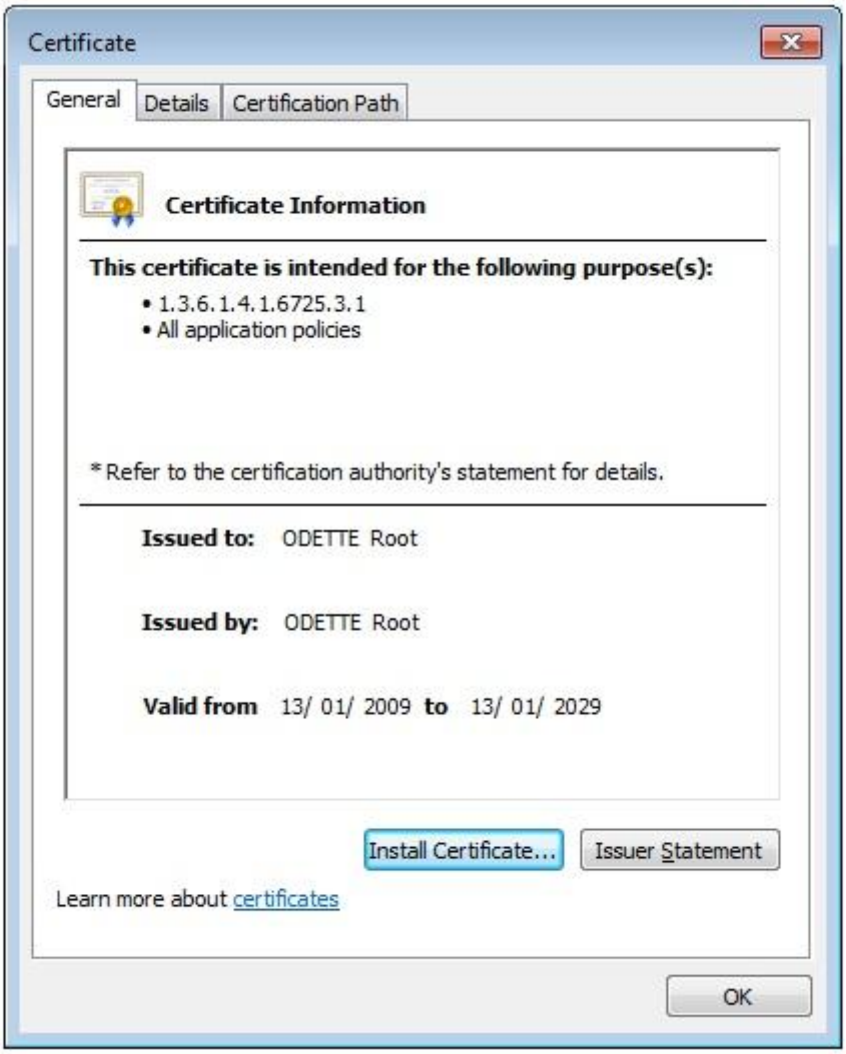
File Download - Security Warning

Do you want to open or save this file?

Name: ODETTE Root.cer
Type: Security Certificate, 1.43 KB
From: **www.odetteca.com**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

3. At the following dialogue, click *Install Certificate*.



Certificate Information

This certificate is intended for the following purpose(s):

- 1.3.6.1.4.1.6725.3.1
- All application policies

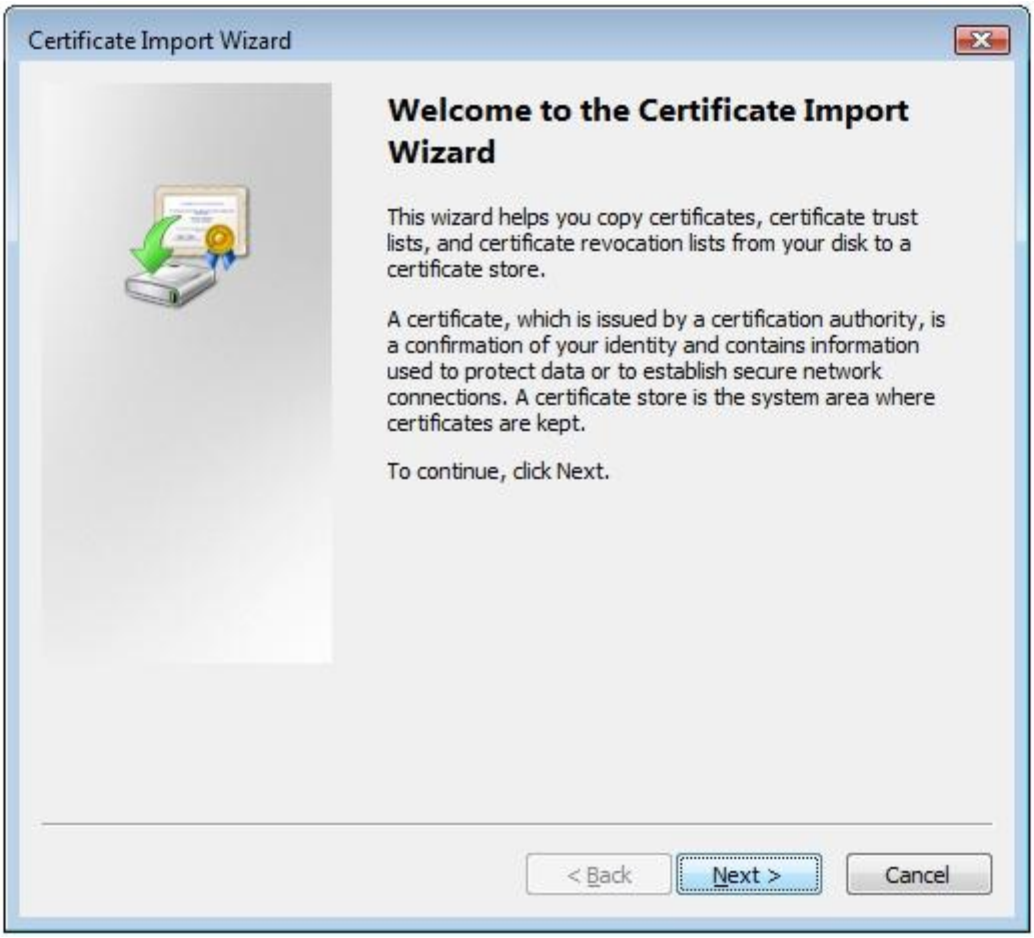
* Refer to the certification authority's statement for details.

Issued to: ODETTE Root

Issued by: ODETTE Root

Valid from 13/ 01/ 2009 to 13/ 01/ 2029

4. This will then show the 'Certificate Import Wizard', click *Next*.



Certificate Import Wizard

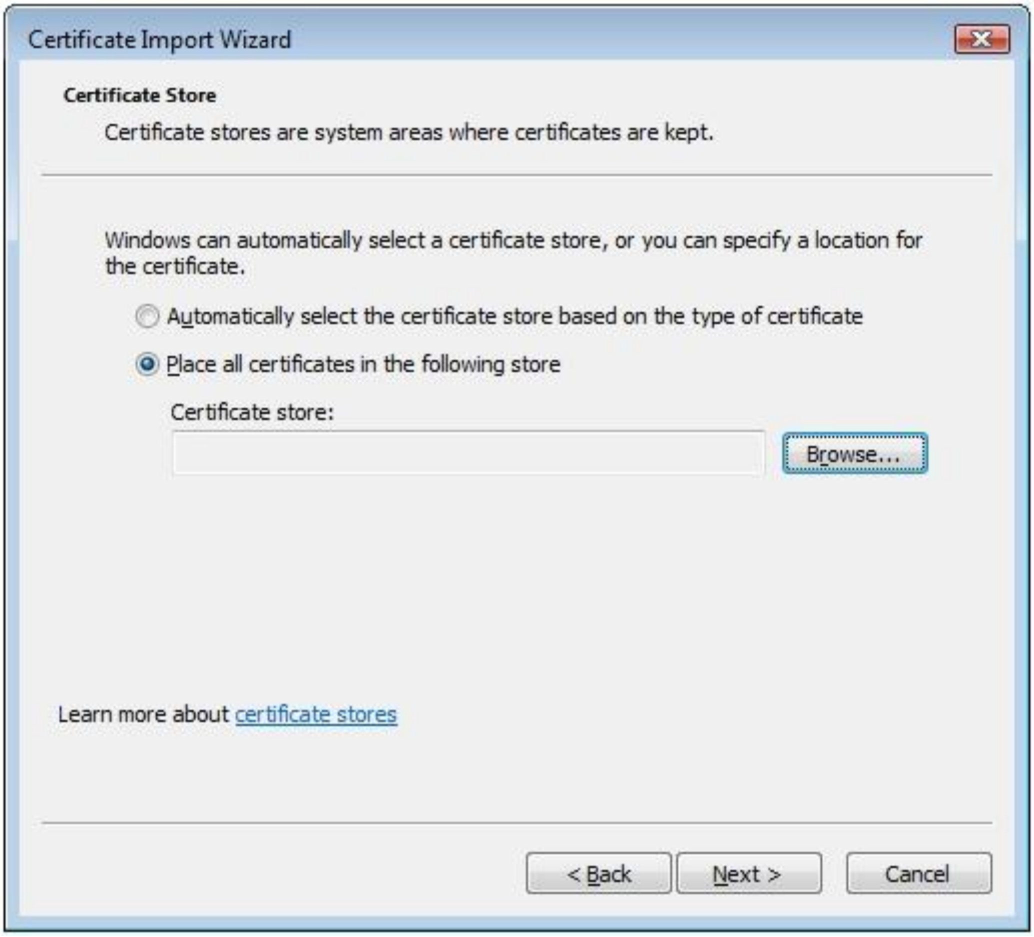
Welcome to the Certificate Import Wizard

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.

5. Select 'Place all certificates in the following store' and click *Browse*.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

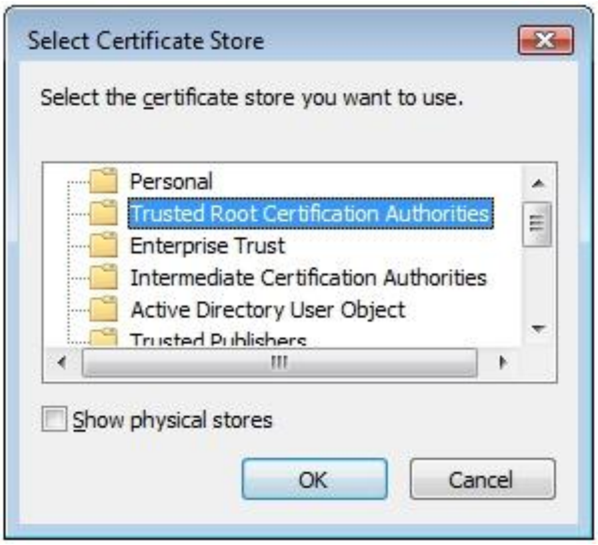
Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

6. Select 'Trusted Root Certification Authorities' store and click *OK*.

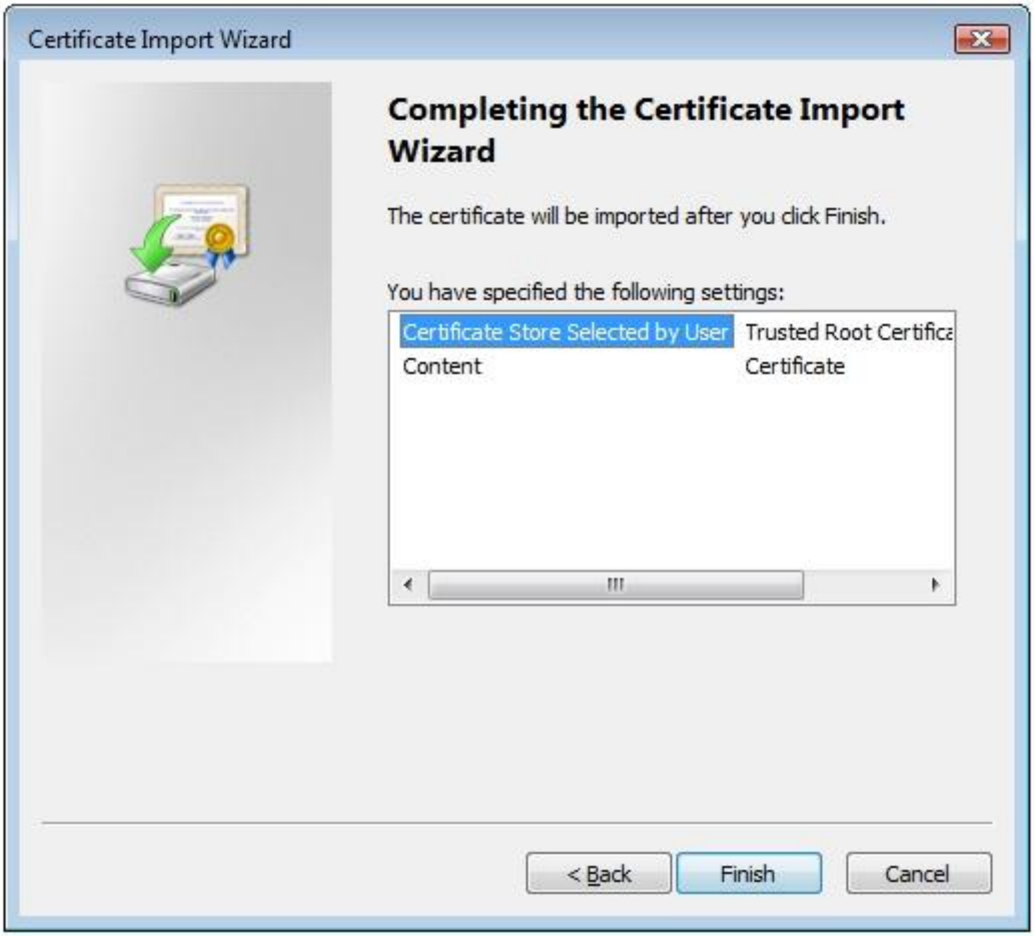


Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
□ Show physical stores
OK
Cancel

7. At the following screen click *Finish*.



Certificate Import Wizard

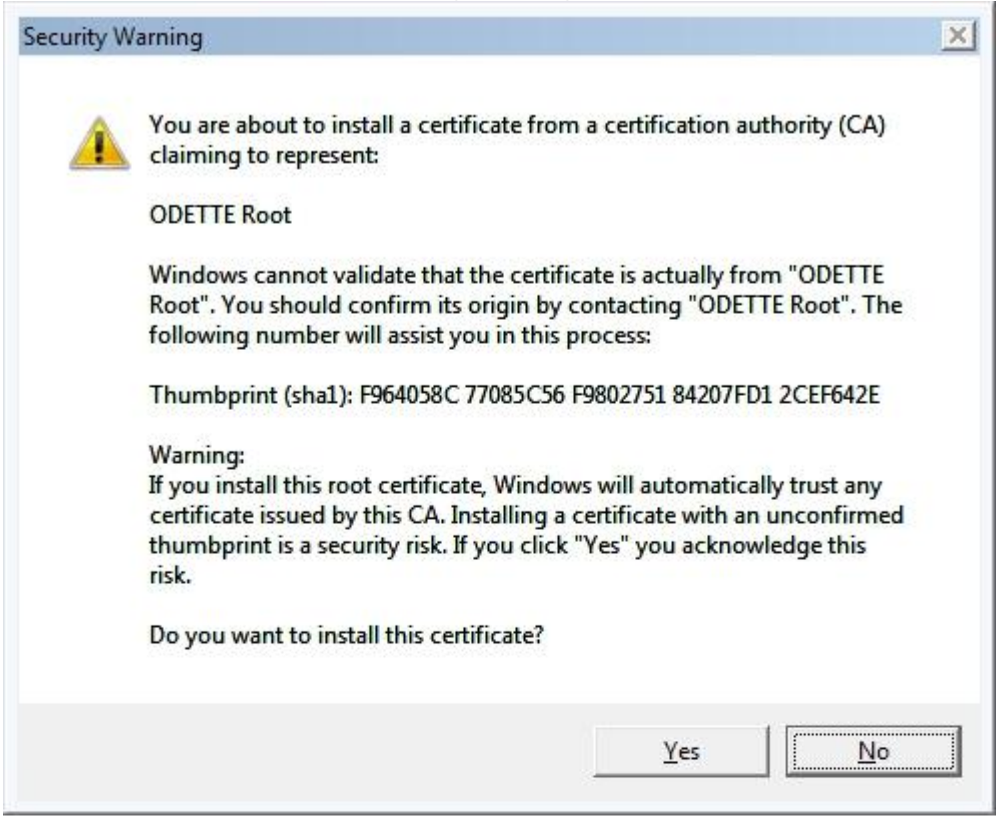
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate

8. When presented with the following message click *Yes*.



Security Warning

You are about to install a certificate from a certification authority (CA) claiming to represent:

ODETTE Root

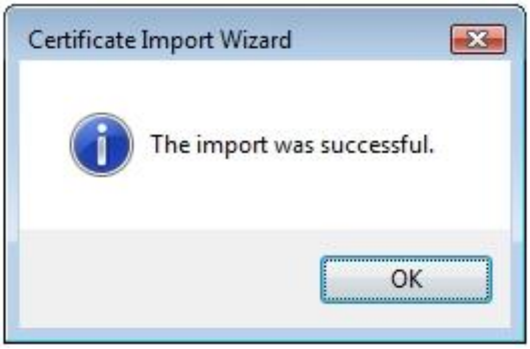
Windows cannot validate that the certificate is actually from "ODETTE Root". You should confirm its origin by contacting "ODETTE Root". The following number will assist you in this process:

Thumbprint (sha1): F964058C 77085C56 F9802751 84207FD1 2CEF642E

Warning:
If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.

Do you want to install this certificate?

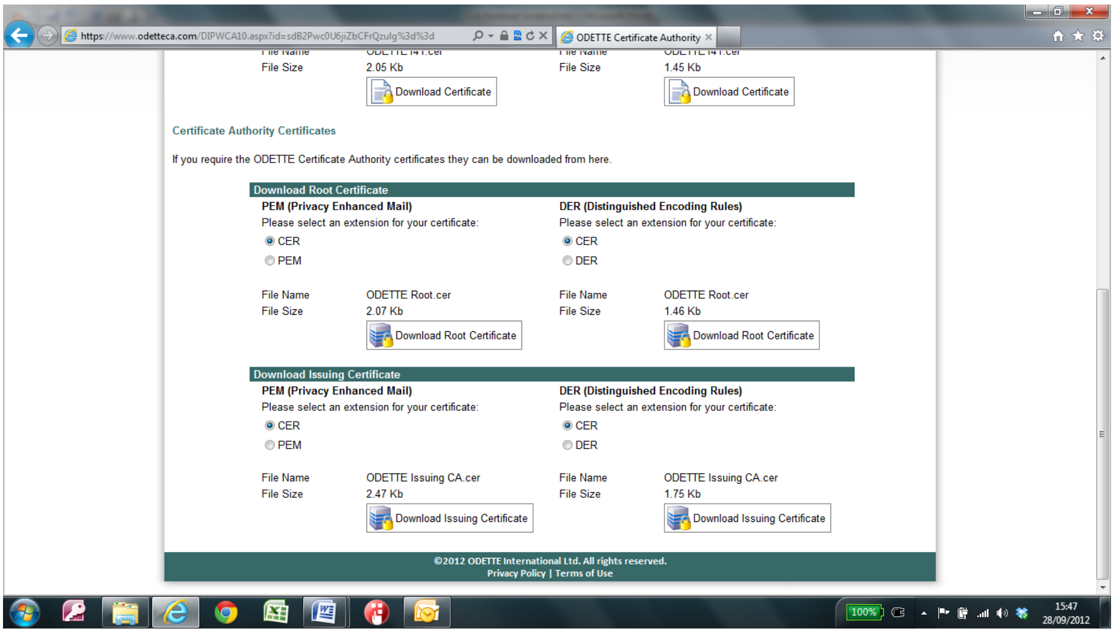
9. When the following screen is displayed the root certificate has been installed. Click *OK* and continue with installing the Issuing Certificate by following the next set of instructions.



Certificate Import Wizard

The import was successful.

Installing the Issuing Certificate



https://www.odetteca.com/DIPWCA10.aspx?id=sdB2Pwc0U6jiZbCFrQzulg%3d%3d

ODETTE Certificate Authority

File Name ODETTE 141.cer
File Size 2.05 Kb
Download Certificate

File Name ODETTE 141.cer
File Size 1.45 Kb
Download Certificate

Certificate Authority Certificates

If you require the ODETTE Certificate Authority certificates they can be downloaded from here.

Download Root Certificate

PEM (Privacy Enhanced Mail)
Please select an extension for your certificate:
● CER
○ PEM

File Name ODETTE Root.cer
File Size 2.07 Kb
Download Root Certificate

DER (Distinguished Encoding Rules)
Please select an extension for your certificate:
● CER
○ DER

File Name ODETTE Root.cer
File Size 1.46 Kb
Download Root Certificate

Download Issuing Certificate

PEM (Privacy Enhanced Mail)
Please select an extension for your certificate:
● CER
○ PEM

File Name ODETTE Issuing CA.cer
File Size 2.47 Kb
Download Issuing Certificate

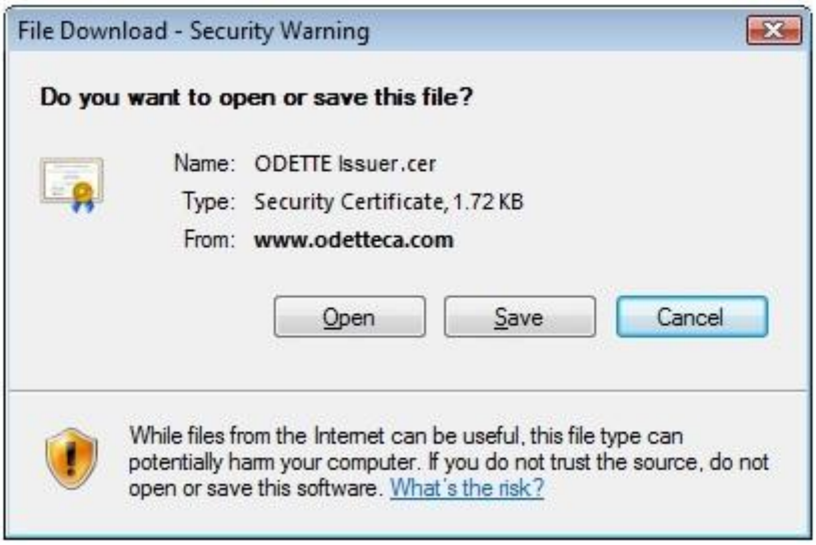
DER (Distinguished Encoding Rules)
Please select an extension for your certificate:
● CER
○ DER

File Name ODETTE Issuing CA.cer
File Size 1.75 Kb
Download Issuing Certificate

©2012 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

1. Click *Download Issuing Certificate*.

2. At the following dialogue, click Open.



File Download - Security Warning

Do you want to open or save this file?

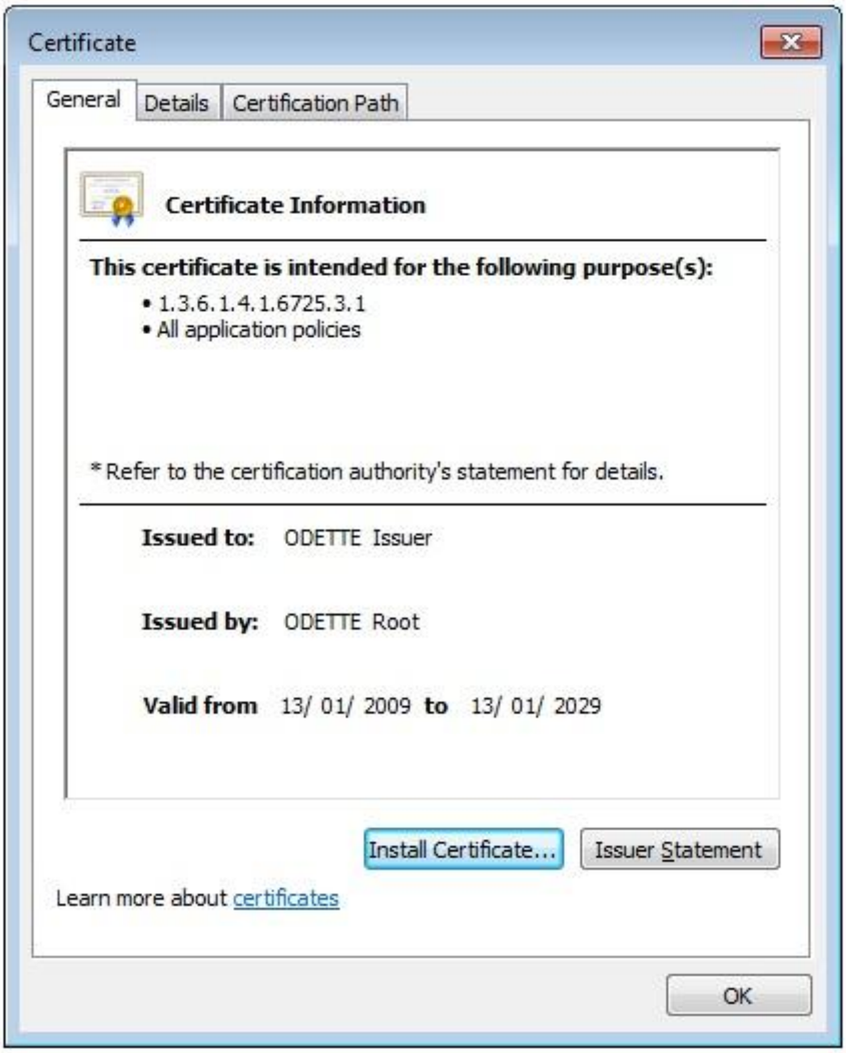
Name: ODETTE Issuer.cer

Type: Security Certificate, 1.72 KB

From: **www.odetteca.com**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

3. At the following dialogue, click *Install Certificate*.



Certificate

Certificate Information

This certificate is intended for the following purpose(s):

- 1.3.6.1.4.1.6725.3.1
- All application policies

* Refer to the certification authority's statement for details.

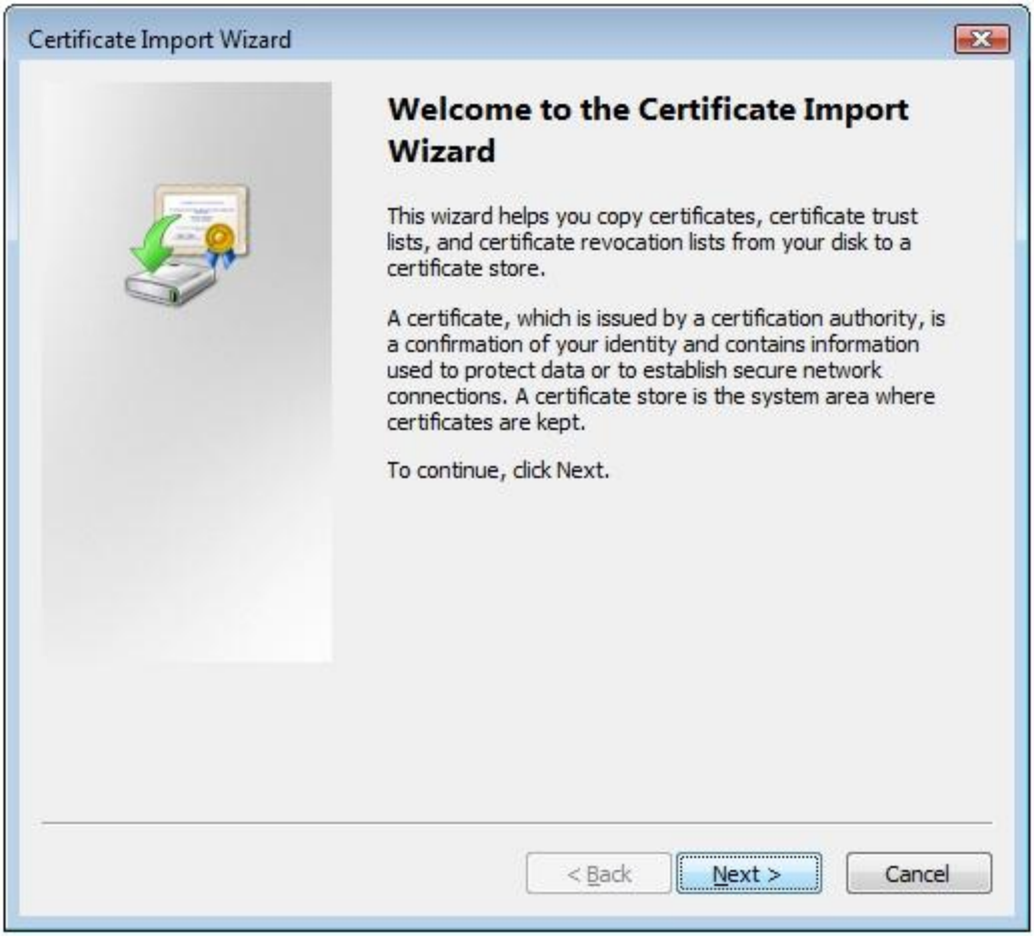
Issued to: ODETTE Issuer

Issued by: ODETTE Root

Valid from 13/ 01/ 2009 **to** 13/ 01/ 2029

Learn more about certificates

4. This will then show the 'Certificate Import Wizard', click *Next*.



Certificate Import Wizard

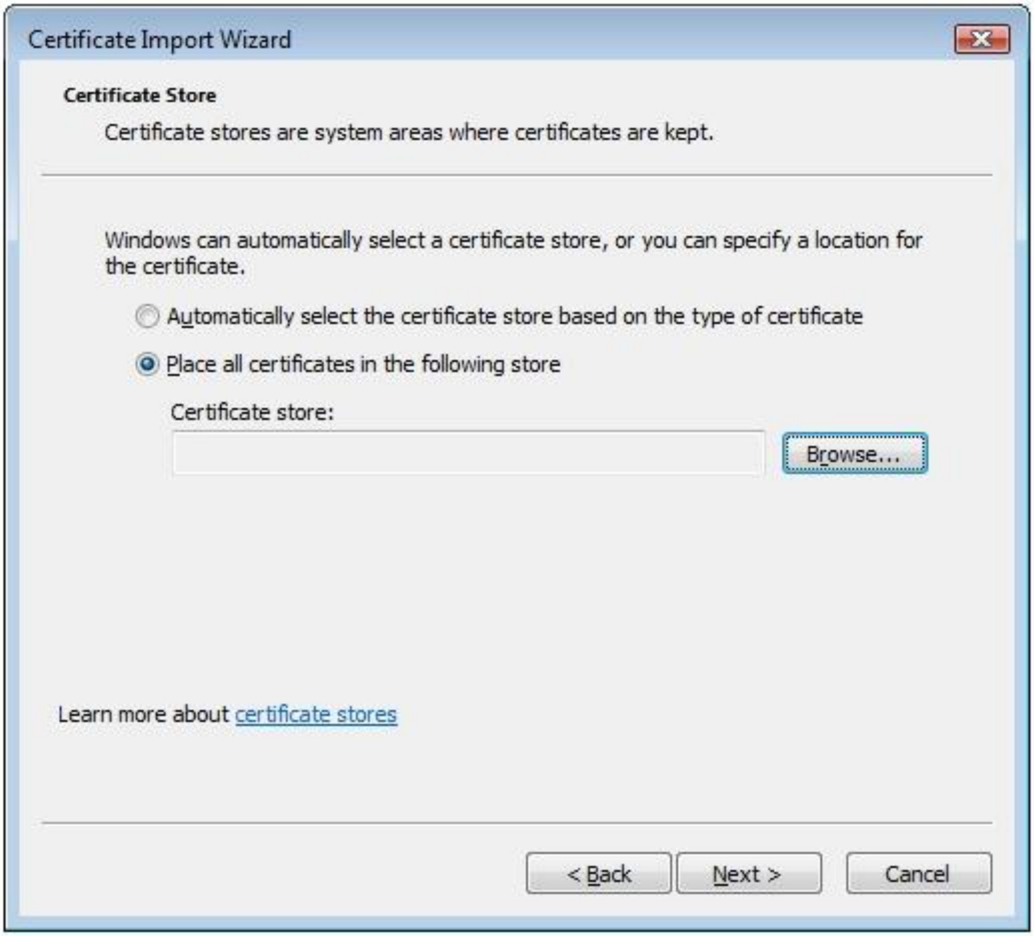
Welcome to the Certificate Import Wizard

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.

5. Select 'Place all certificates in the following store' and click *Browse*.



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 the certificate.

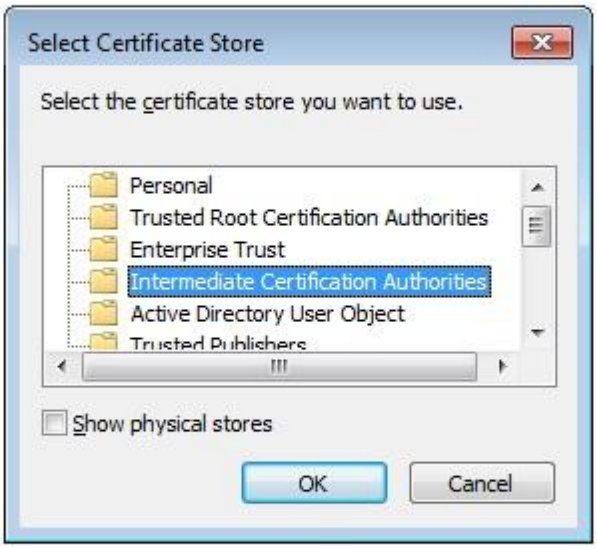
○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Learn more about certificate stores

6. Select the 'Intermediate Certification Authorities' store and click *OK*.



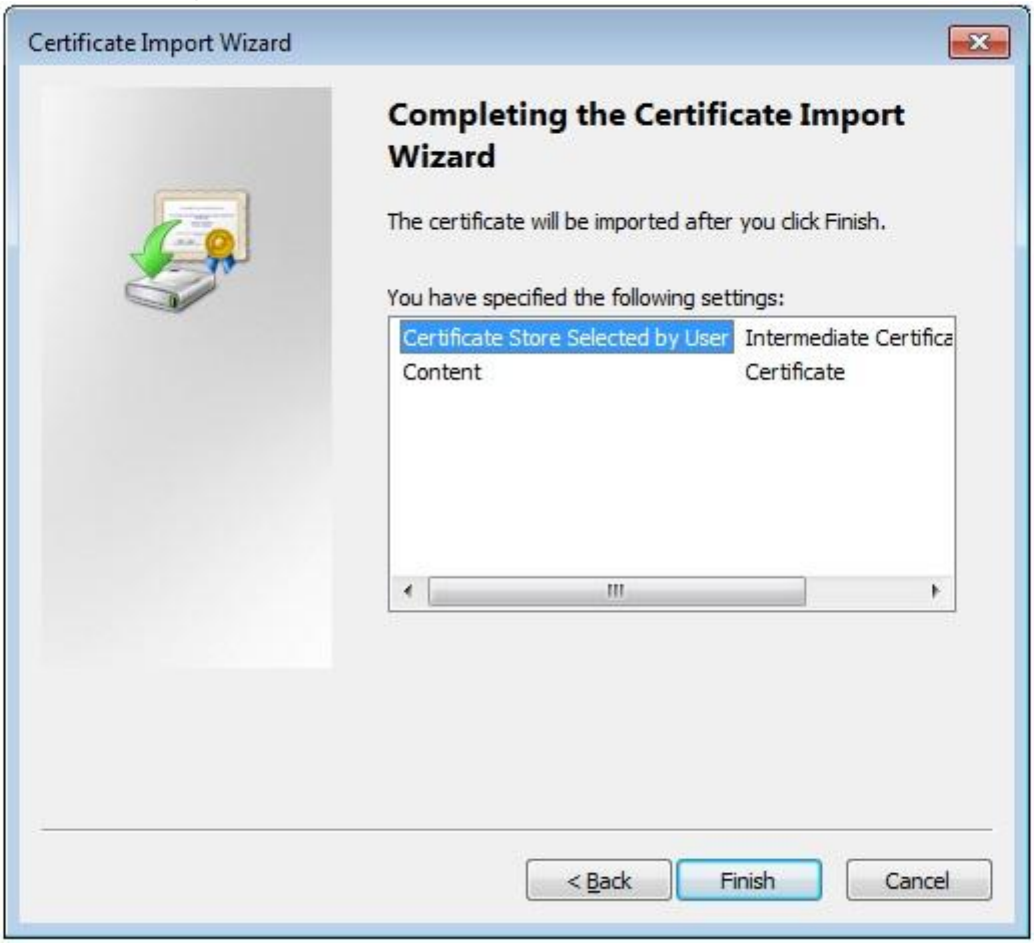
Select Certificate Store

Select the certificate store you want to use.

- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers

□ Show physical stores

7. At the following screen click *Finish*.



Certificate Import Wizard

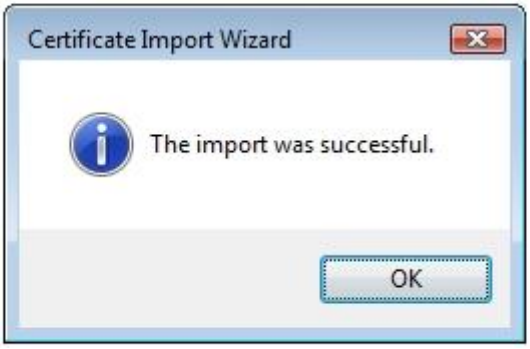
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Intermediate Certifica
Content	Certificate

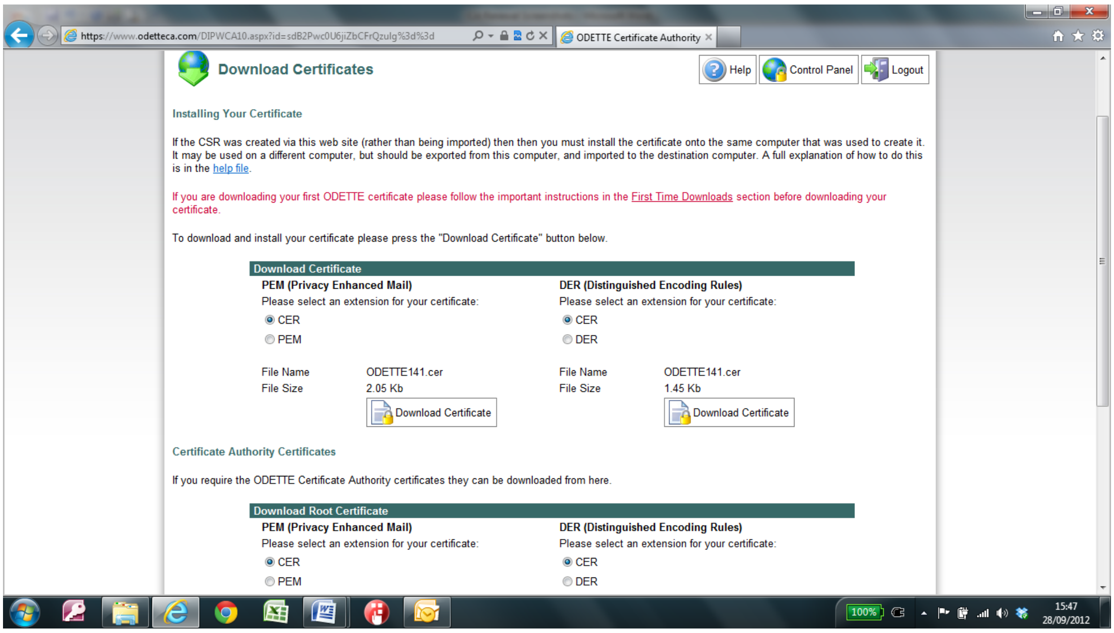
8. When the following screen is displayed the root certificate has been installed. Click *OK* and continue with installing your own Odette certificate by following the next set of instructions.



Certificate Import Wizard

The import was successful.

Installing Your Odette Certificate


https://www.odetteca.com/DIPWCA10.aspx?id=sdB2Pwc0U6jiZbCFrQzulg%3d%3d
ODETTE Certificate Authority
Help
Control Panel
Logout
Download Certificate
Download Certificate
15:47
28/09/2012

Download Certificates

Installing Your Certificate

If the CSR was created via this web site (rather than being imported) then then you must install the certificate onto the same computer that was used to create it. It may be used on a different computer, but should be exported from this computer, and imported to the destination computer. A full explanation of how to do this is in the help file.

If you are downloading your first ODETTE certificate please follow the important instructions in the First Time Downloads section before downloading your certificate.

To download and install your certificate please press the "Download Certificate" button below.

Download Certificate

PEM (Privacy Enhanced Mail)		**DER (Distinguished Encoding Rules)**	
Please select an extension for your certificate:		Please select an extension for your certificate:	
● CER		● CER	
○ PEM		○ DER	
File Name	ODETTE141.cer	File Name	ODETTE141.cer
File Size	2.05 Kb	File Size	1.45 Kb

Certificate Authority Certificates

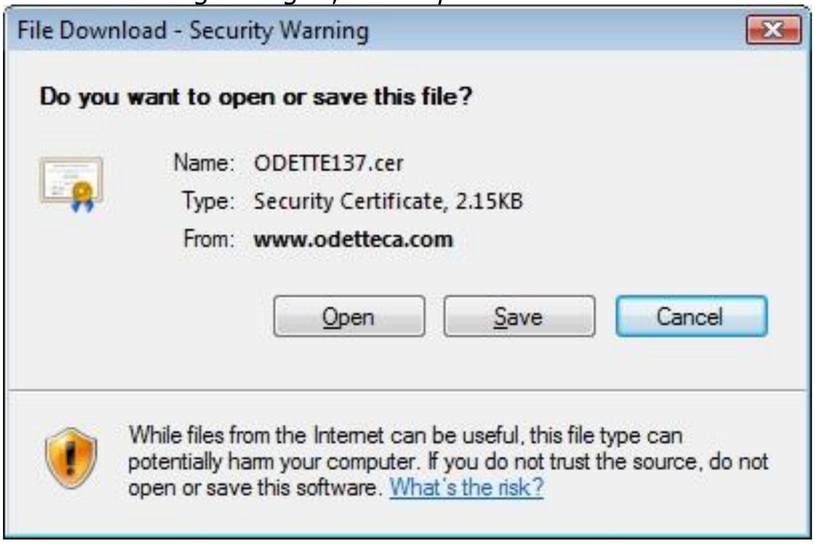
If you require the ODETTE Certificate Authority certificates they can be downloaded from here.

Download Root Certificate

PEM (Privacy Enhanced Mail)	**DER (Distinguished Encoding Rules)**
Please select an extension for your certificate:	Please select an extension for your certificate:
● CER	● CER
○ PEM	○ DER

1. Click *Download Certificate*.

2. At the following dialogue, click *Open*.



File Download - Security Warning

Do you want to open or save this file?

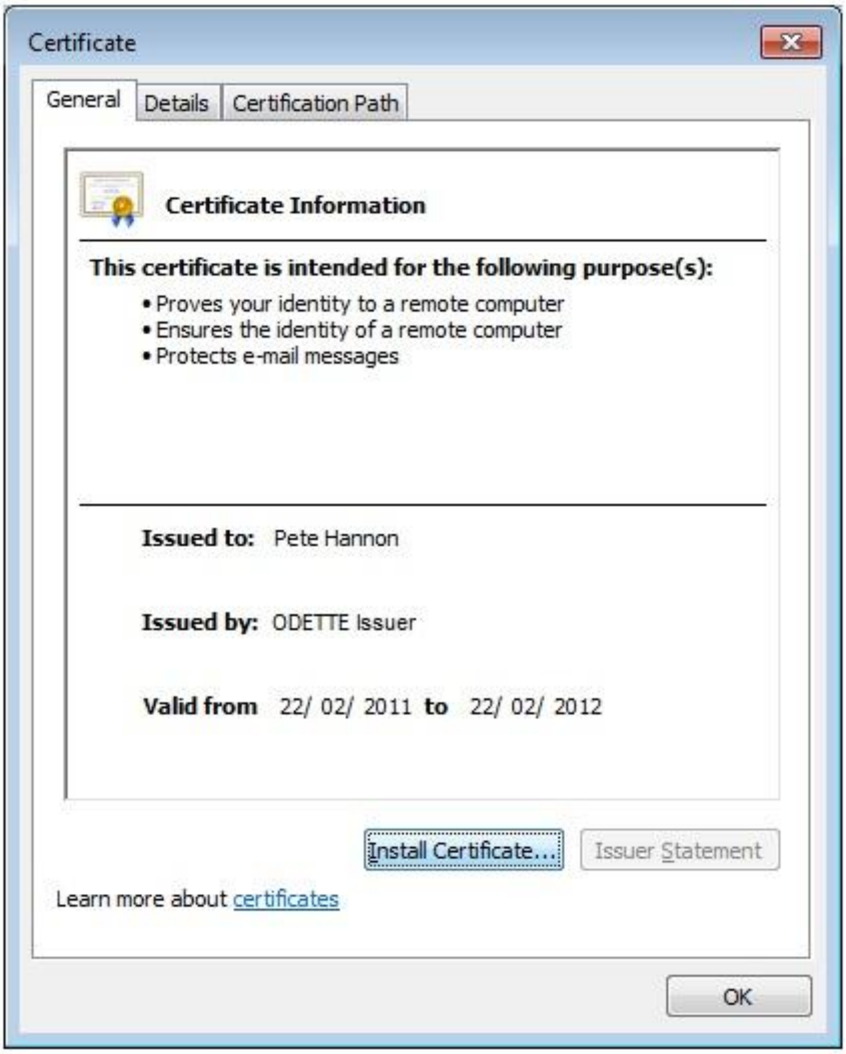
Name: ODETTE137.cer

Type: Security Certificate, 2.15KB

From: **www.odetteca.com**

While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not open or save this software. What's the risk?

3. At the following dialogue, click *Install Certificate*.



Certificate Information

This certificate is intended for the following purpose(s):

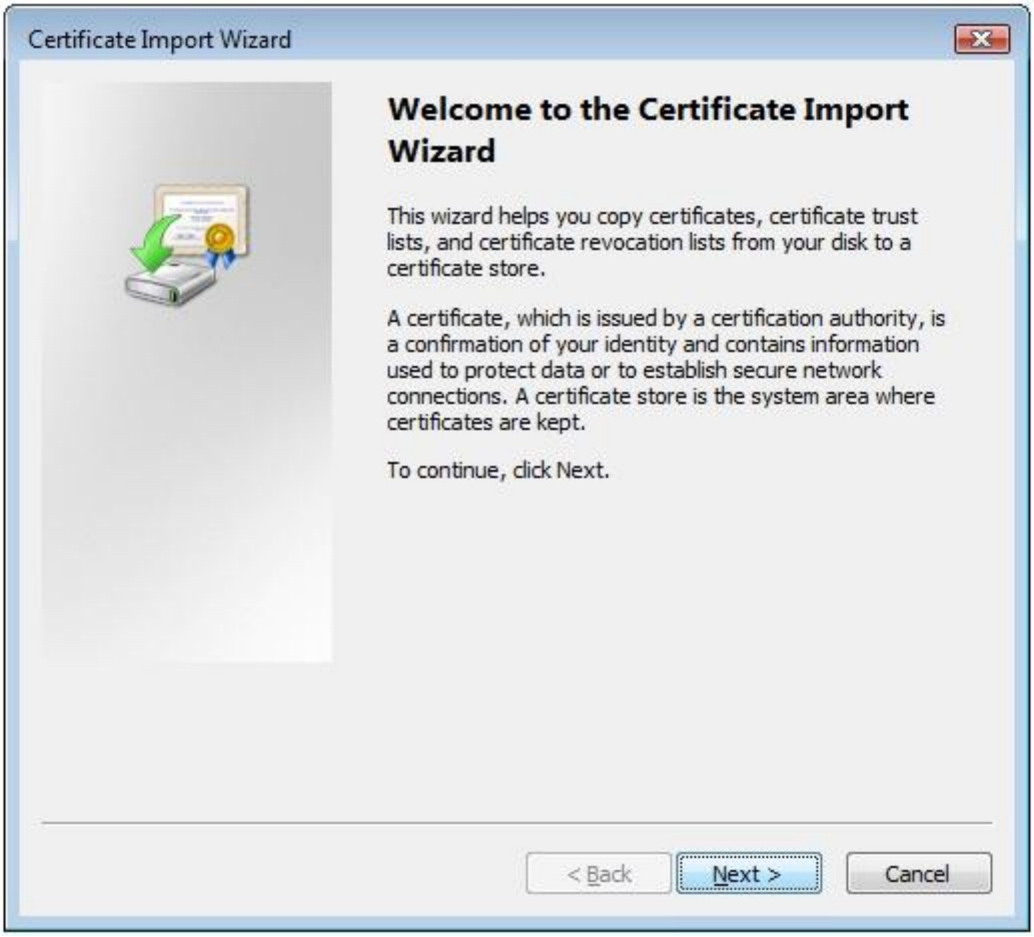
- Proves your identity to a remote computer
- Ensures the identity of a remote computer
- Protects e-mail messages

Issued to: Pete Hannon

Issued by: ODETTE Issuer

Valid from 22/ 02/ 2011 **to** 22/ 02/ 2012

4. This will then show the 'Certificate Import Wizard', click *Next*.



Certificate Import Wizard

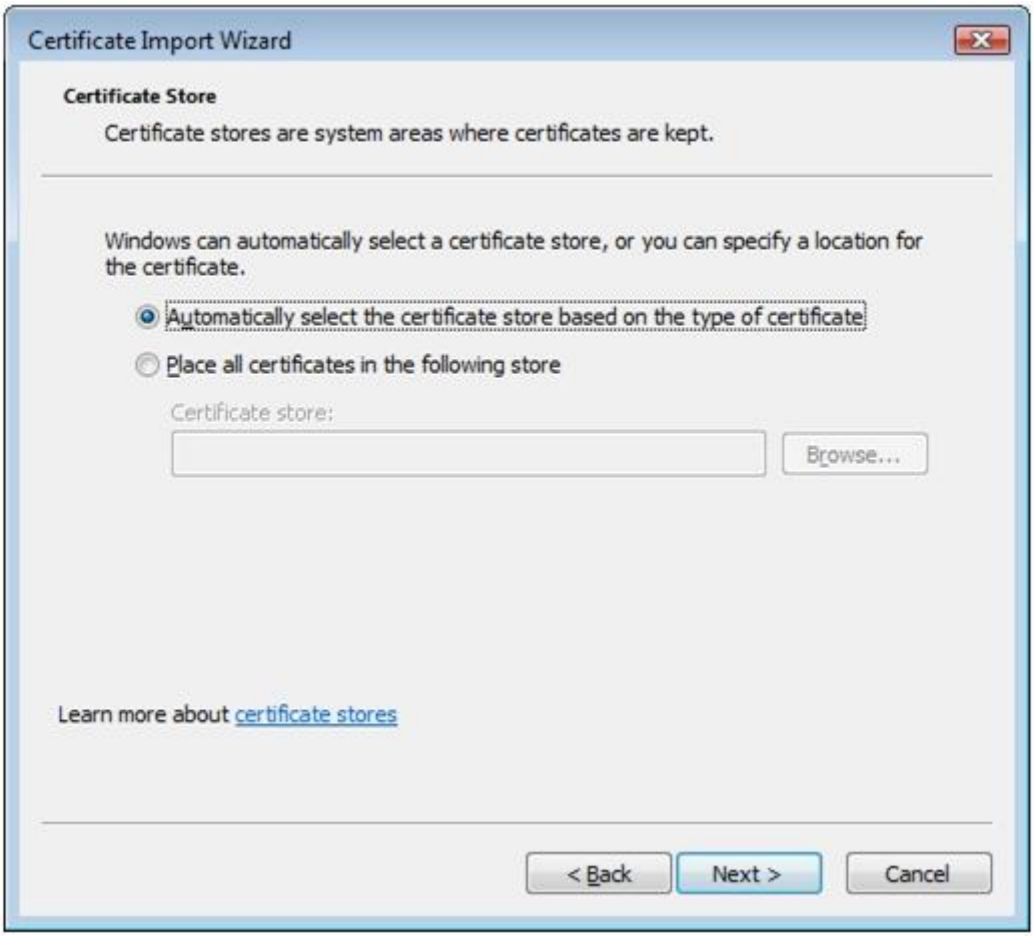
Welcome to the Certificate Import Wizard

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.

5. Ensure that the option ‘Automatically select a certificate store...’ is selected and then click *Next*.



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 the certificate.

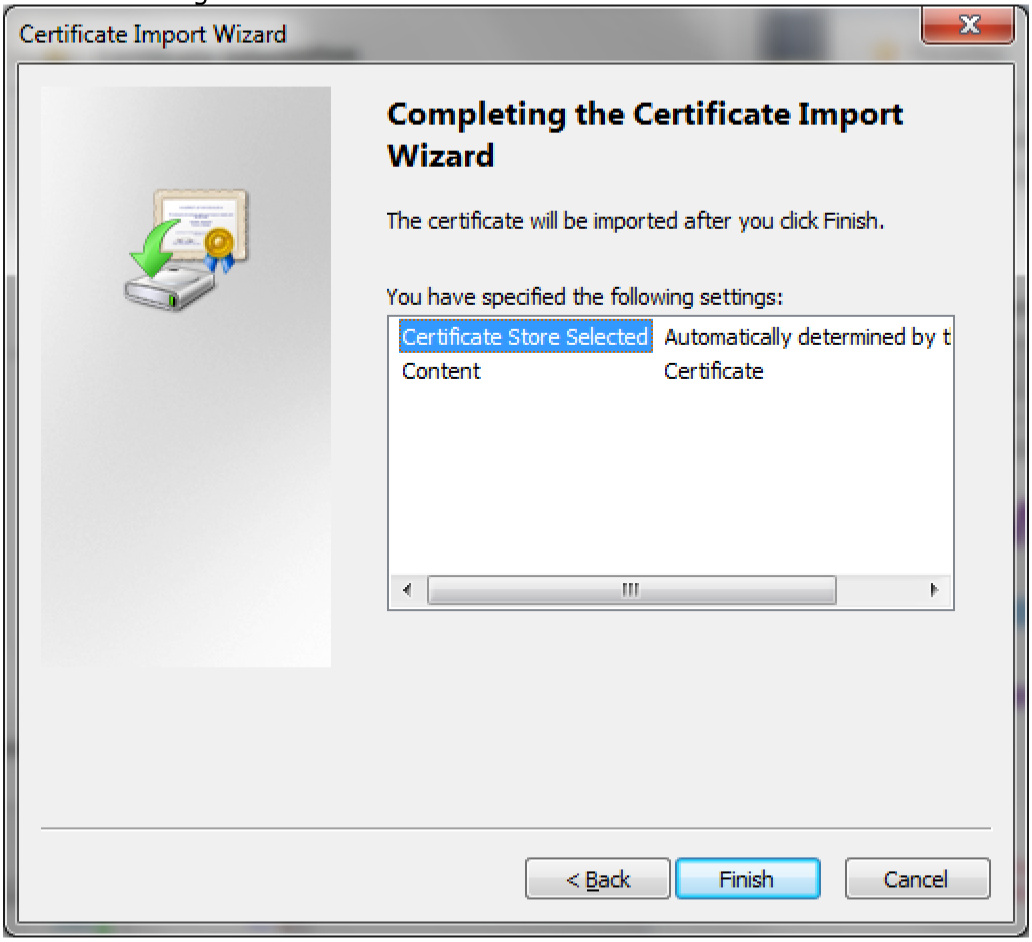
● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

Certificate store:

Learn more about certificate stores

6. At the following screen click *Finish*.



Certificate Import Wizard

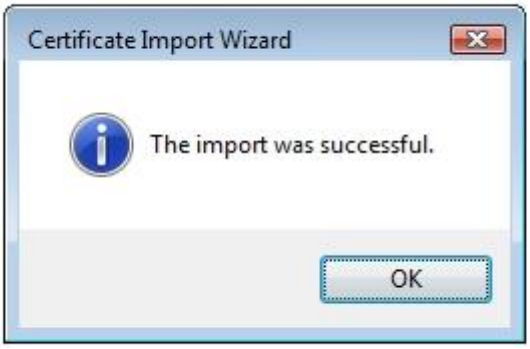
Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected	Automatically determined by t
Content	Certificate

7. When the following screen is displayed your own Odette Certificate has been successfully installed. Click *OK*.

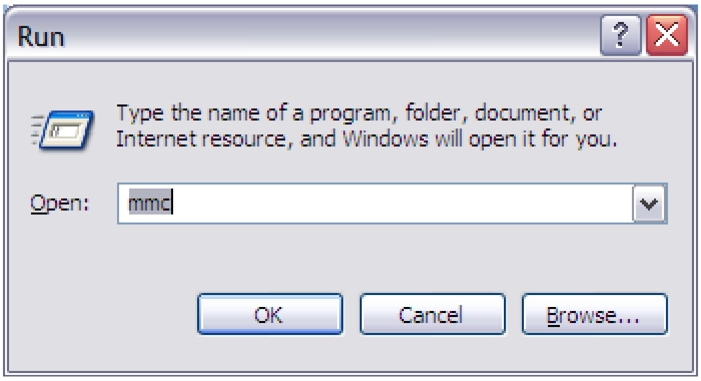


Certificate Import Wizard

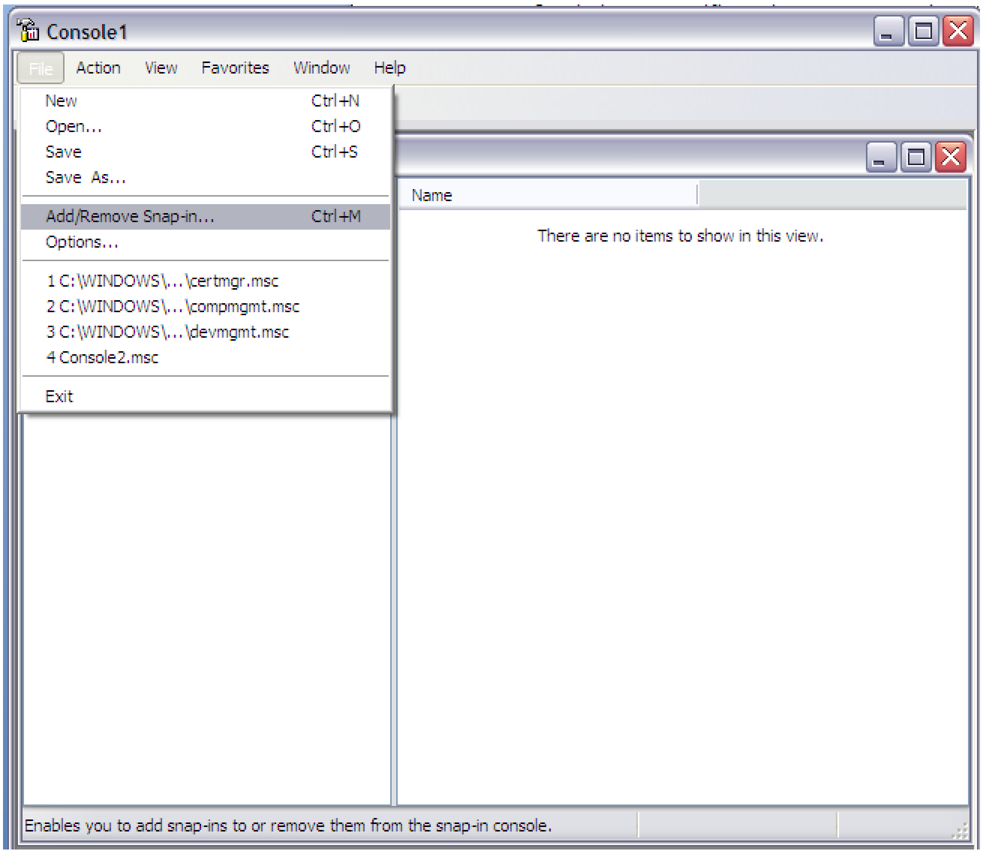
The import was successful.

How to find your certificate in the Windows keystore after downloading and installation

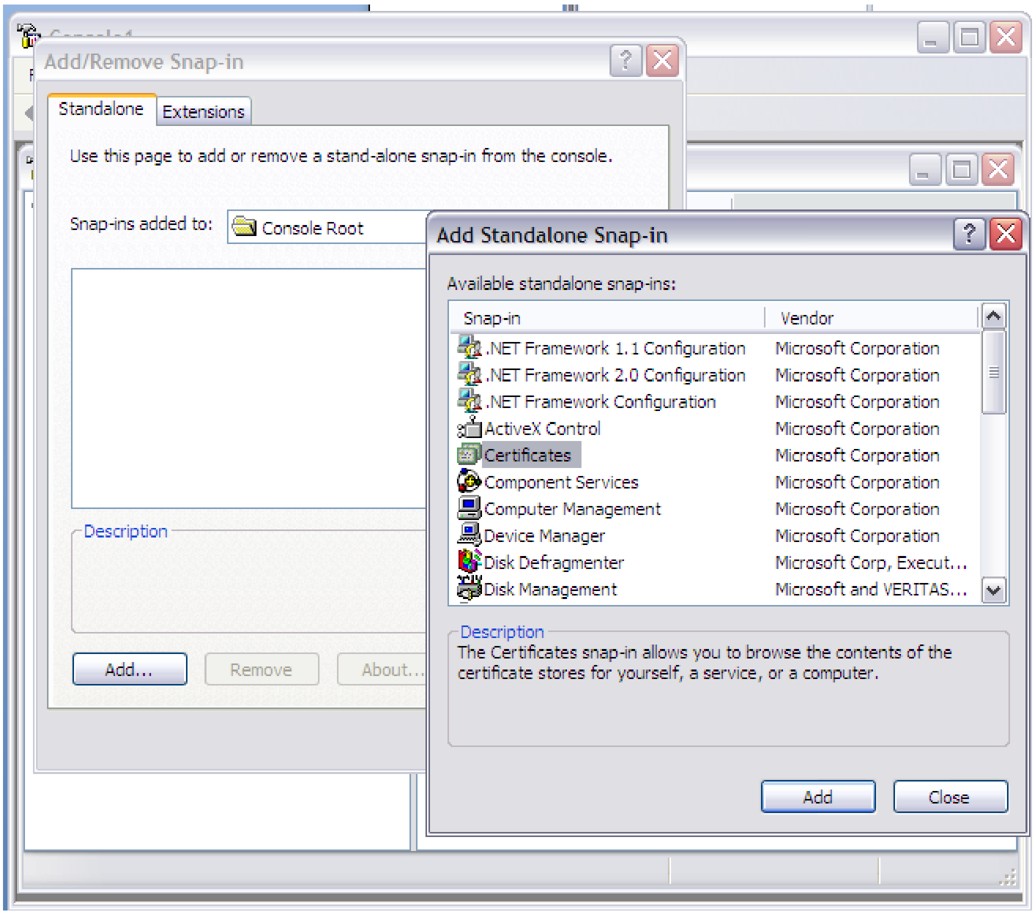
1. Click *Start* and select run. Type "mmc" in the entry field. Click *OK*


Run
?
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:
mmc
OK
Cancel
Browse...

2. The Console will open. Select File/Add Remove Snap-in


Console1
File
Action
View
Favorites
Window
Help
New Ctrl+N
Open... Ctrl+O
Save Ctrl+S
Save As...
Add/Remove Snap-in... Ctrl+M
Options...
1 C:\WINDOWS\...\certmgr.msc
2 C:\WINDOWS\...\compmgmt.msc
3 C:\WINDOWS\...\devmgmt.msc
4 Console2.msc
Exit
Name
There are no items to show in this view.
Enables you to add snap-ins to or remove them from the snap-in console.

3. Click *Add* and select ***Certificates*** from the list. Click *Add* again.



Use this page to add or remove a stand-alone snap-in from the console.

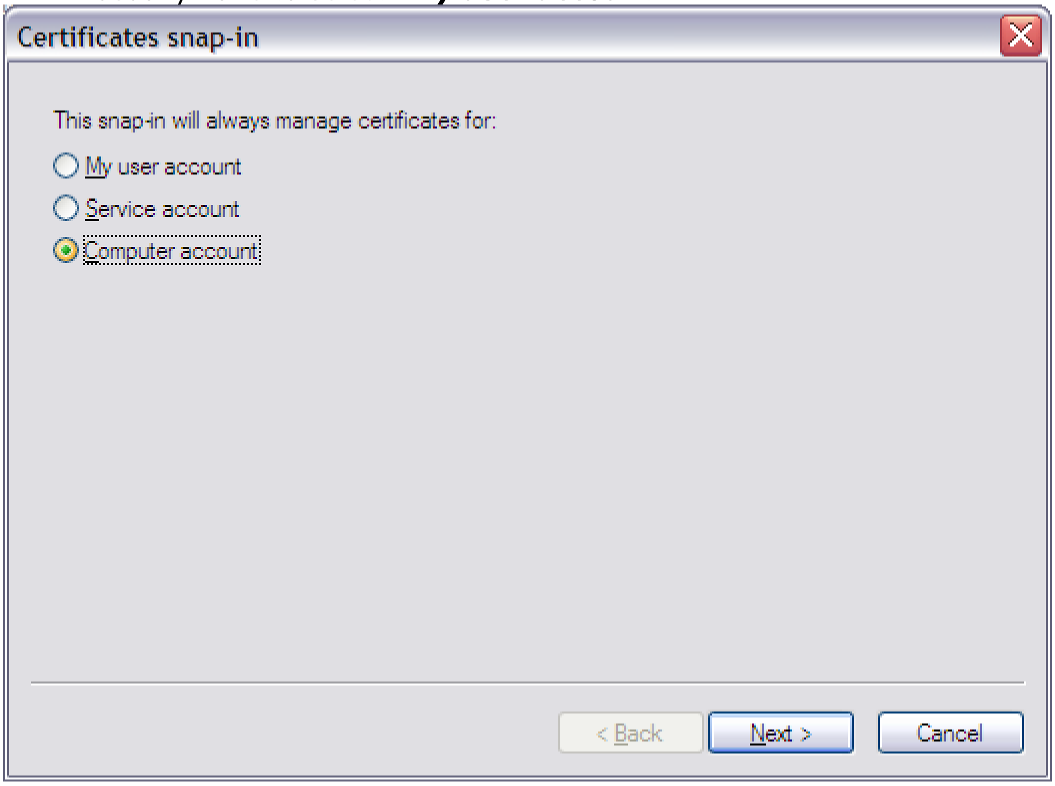
Snap-ins added to: Console Root

Available standalone snap-ins:

Snap-in	Vendor
.NET Framework 1.1 Configuration	Microsoft Corporation
.NET Framework 2.0 Configuration	Microsoft Corporation
.NET Framework Configuration	Microsoft Corporation
ActiveX Control	Microsoft Corporation
Certificates	Microsoft Corporation
Component Services	Microsoft Corporation
Computer Management	Microsoft Corporation
Device Manager	Microsoft Corporation
Disk Defragmenter	Microsoft Corp, Execut...
Disk Management	Microsoft and VERITAS...

Description
The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

4. For Windows XP, select "***Computer account"***, for Windows7 you will usually have to select ***"My user account"***



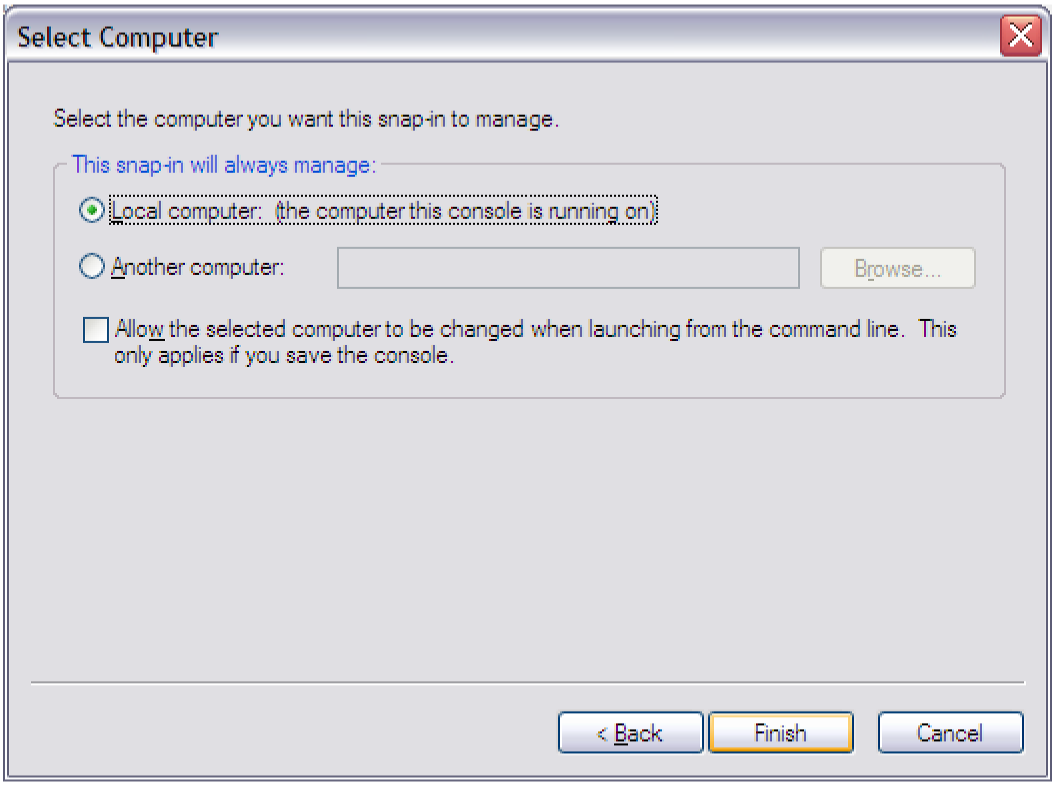
This snap-in will always manage certificates for:

○ My user account

○ Service account

● Computer account

5. Select ***Local Computer*** and click *Finish*.



Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

● Local computer: (the computer this console is running on)

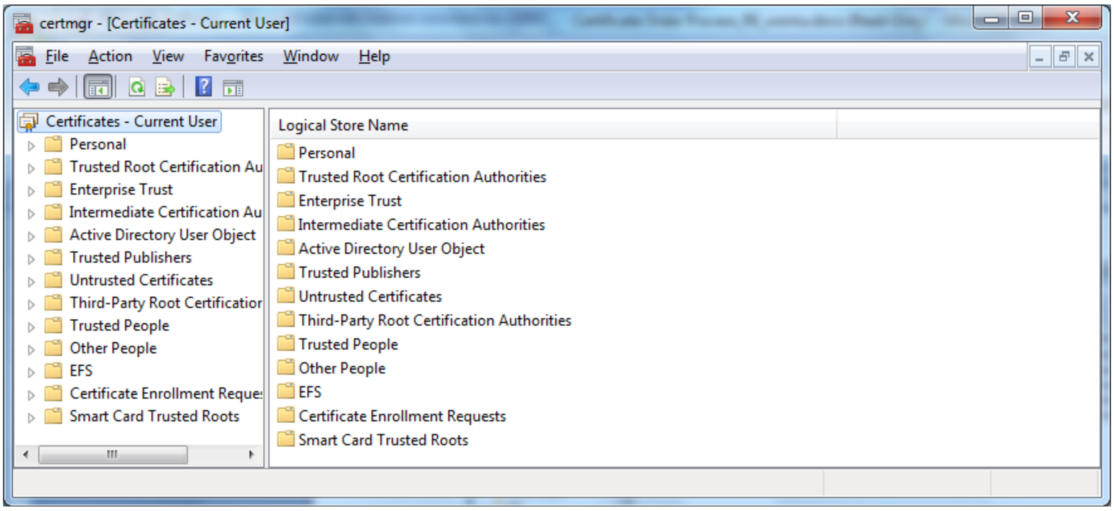
○ Another computer: Browse...

□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

Close the snap-in selection window.

6. Click *OK* to close the Add/Remove Snap-in dialog.

You will now see the Windows certificate store:

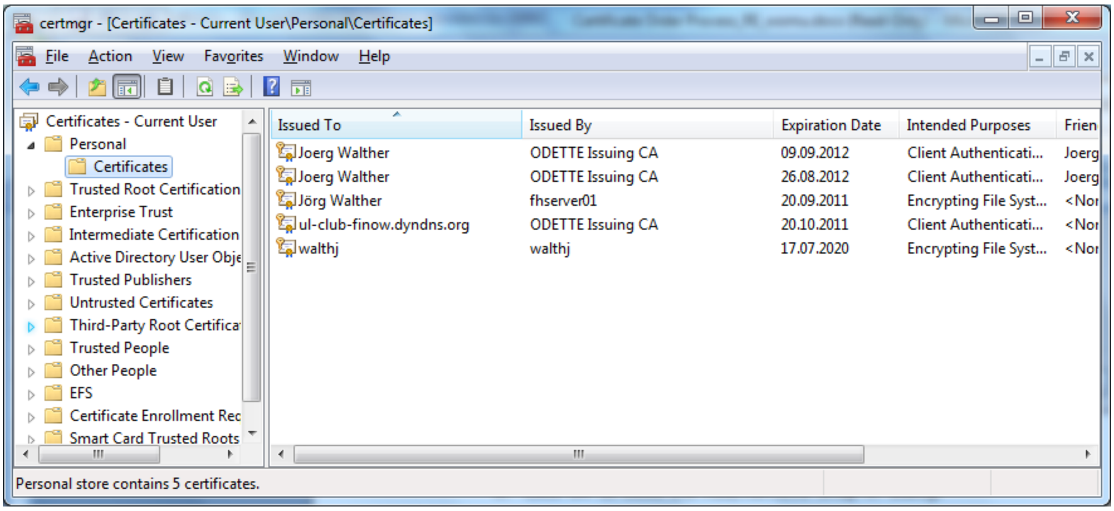


certmgr - [Certificates - Current User]

Certificates - Current User
- Personal
- Trusted Root Certification Au
- Enterprise Trust
- Intermediate Certification Au
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certificatior
- Trusted People
- Other People
- EFS
- Certificate Enrollment Reque:
- Smart Card Trusted Roots

Logical Store Name
- Personal
- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates
- Third-Party Root Certification Authorities
- Trusted People
- Other People
- EFS
- Certificate Enrollment Requests
- Smart Card Trusted Roots

7. Expand Certificates, then expand Personal and select Certificates. You will be able to see the certificate in right panel of the Windows Management Console. This is where your downloaded certificate has been stored.



certmgr - [Certificates - Current User\Personal\Certificates]

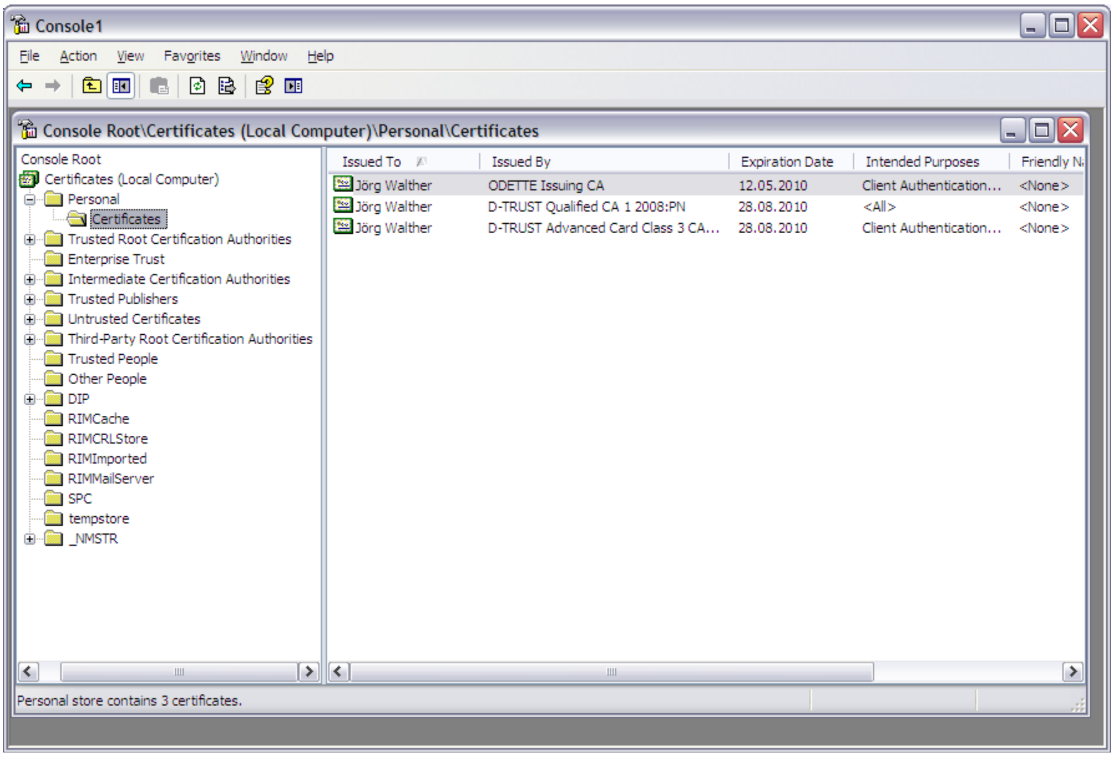
- Certificates - Current User
  - Personal
    - Certificates
  - Trusted Root Certification
  - Enterprise Trust
  - Intermediate Certification
  - Active Directory User Obje
  - Trusted Publishers
  - Untrusted Certificates
  - Third-Party Root Certifica
  - Trusted People
  - Other People
  - EFS
  - Certificate Enrollment Rec
  - Smart Card Trusted Roots

Issued To	Issued By	Expiration Date	Intended Purposes	Frien
Joerg Walther	ODETTE Issuing CA	09.09.2012	Client Authenticati...	Joerg
Joerg Walther	ODETTE Issuing CA	26.08.2012	Client Authenticati...	Joerg
Jörg Walther	fhserver01	20.09.2011	Encrypting File Syst...	<Nor
ul-club-finow.dyndns.org	ODETTE Issuing CA	20.10.2011	Client Authenticati...	<Nor
walthj	walthj	17.07.2020	Encrypting File Syst...	<Nor

Personal store contains 5 certificates.

The little key on the upper left corner of the certificate symbol indicates that you have the certificate and the matching private key in your certificate store (only valid for Windows7)

In Windows XP the certificate snap in looks like this:



Console1

Console Root\Certificates (Local Computer)\Personal\Certificates

- Console Root
  - Certificates (Local Computer)
    - Personal
      - Certificates
    - Trusted Root Certification Authorities
    - Enterprise Trust
    - Intermediate Certification Authorities
    - Trusted Publishers
    - Untrusted Certificates
    - Third-Party Root Certification Authorities
    - Trusted People
    - Other People
    - DIP
    - RIMCache
    - RIMCRLStore
    - RIMImported
    - RIMMailServer
    - SPC
    - tempstore
    - _NMSTR

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly N
Jörg Walther	ODETTE Issuing CA	12.05.2010	Client Authentication...	<None>
Jörg Walther	D-TRUST Qualified CA 1 2008:PN	28.08.2010	<All>	<None>
Jörg Walther	D-TRUST Advanced Card Class 3 CA...	28.08.2010	Client Authentication...	<None>

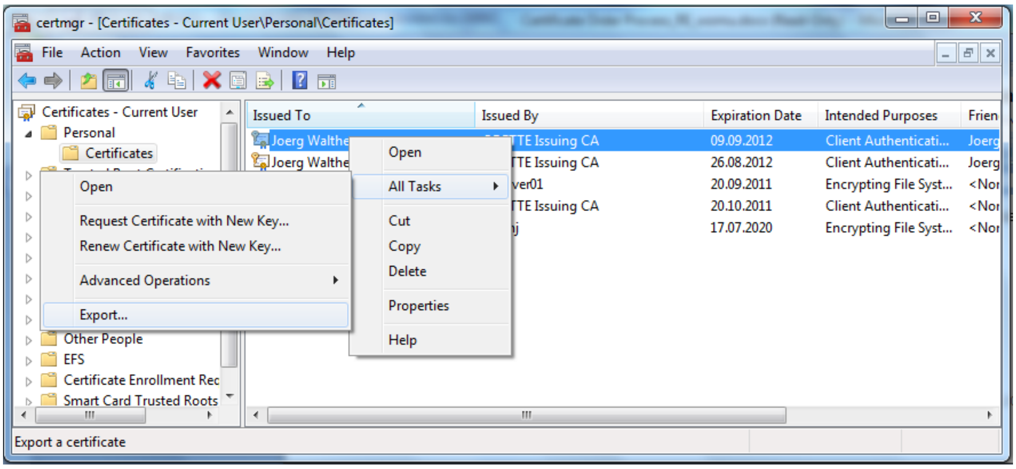
Personal store contains 3 certificates.

Double click on the certificate to see the details.

At this point, if you wish, you can save the Console as a shortcut so that it can be accessed quickly in future.

How to export a certificate including the private key from one Windows machine to another (Windows keystore)

1. The following example explains the export on Windows7.
   Open the Management console.



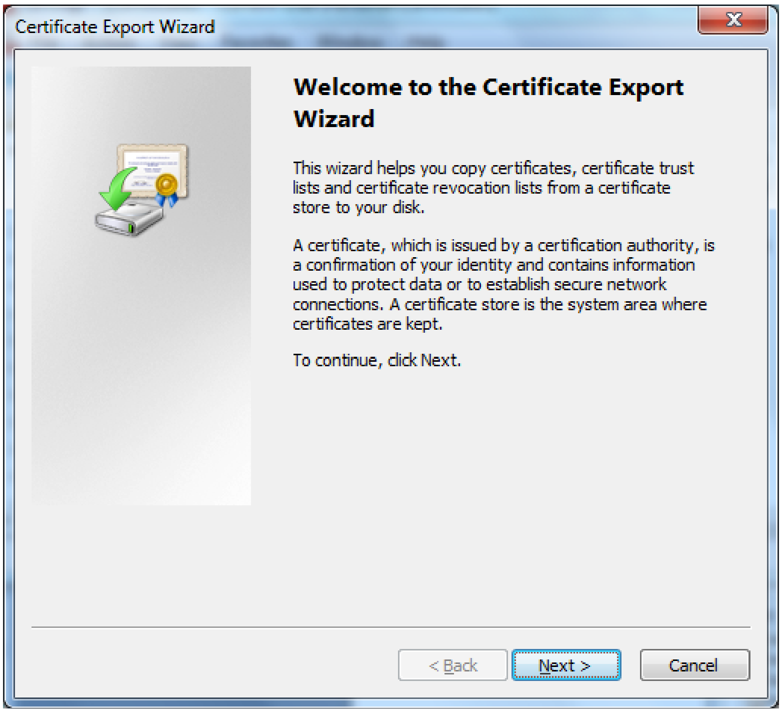
certmgr - [Certificates - Current User\Personal\Certificates]

Issued To	Issued By	Expiration Date	Intended Purposes	Frien
Joerg Walthe	...TTE Issuing CA	09.09.2012	Client Authenticati...	Joerg
Joerg Walthe	...TTE Issuing CA	26.08.2012	Client Authenticati...	Joerg
	...ver01	20.09.2011	Encrypting File Syst...	<Nor
	...TTE Issuing CA	20.10.2011	Client Authenticati...	<Nor
	...j	17.07.2020	Encrypting File Syst...	<Nor

Export a certificate

Select the certificate, right mouse button, All Tasks, Export.

2. On the Certificate dialogue that appears, select the Details tab and click *Copy to File*. The export wizard starts; click ***Next***



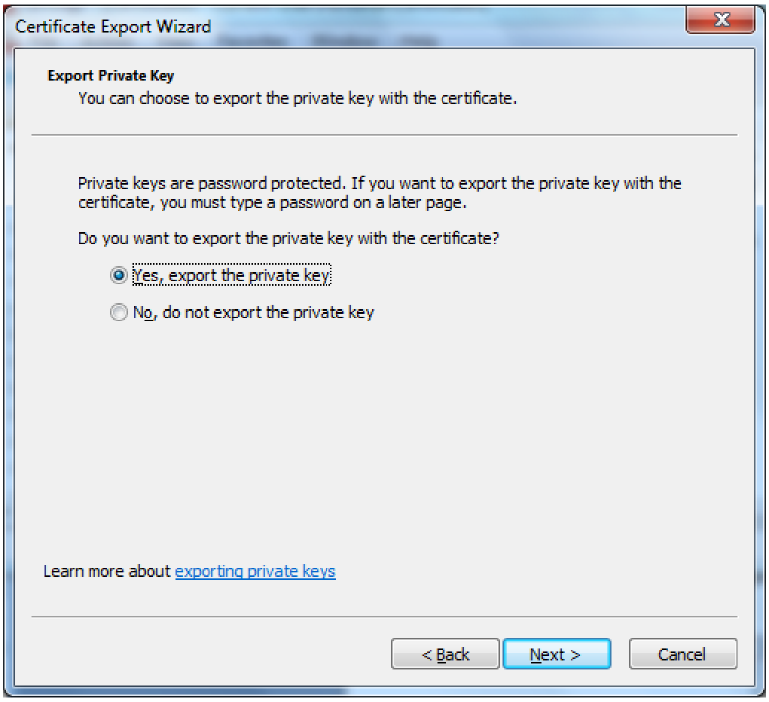
Certificate Export Wizard

Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

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.



Certificate Export Wizard

Export Private Key
You can choose to export the private key with the certificate.

Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.

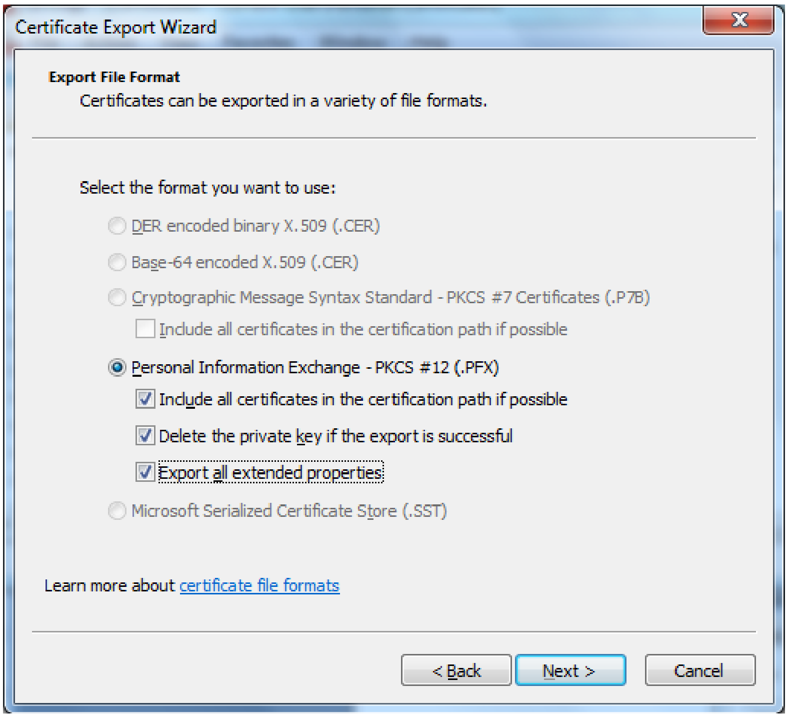
Do you want to export the private key with the certificate?

● Yes, export the private key

○ No, do not export the private key

Learn more about exporting private keys

You will need the public key and the private key on the other computer. The public key is used by your business partners to encrypt messages sent to you and the private key will be used by your system to decrypt the messages.
Select ***Yes, export the private key*** and click *Next*



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

○ DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

● Personal Information Exchange - PKCS #12 (.PFX)

☑ Include all certificates in the certification path if possible

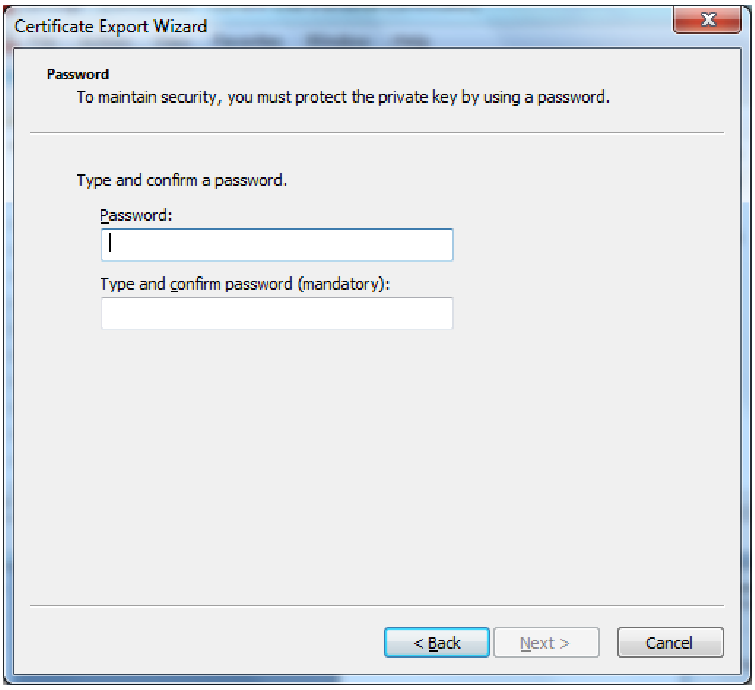
☑ Delete the private key if the export is successful

☑ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

Continue as shown above and click *Next*. For security reasons you should delete the private key from the current machine.


Certificate Export Wizard

Password

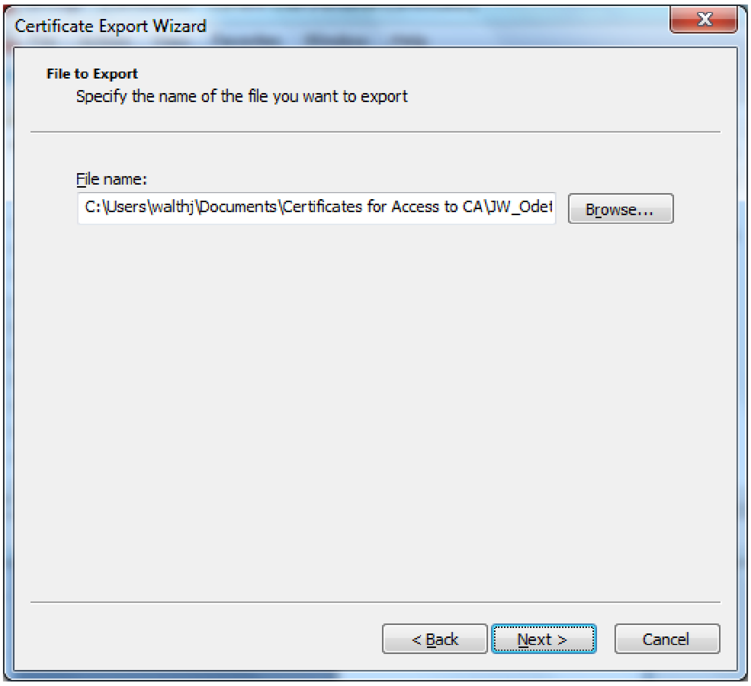
To maintain security, you must protect the private key by using a password.

Type and confirm a password.

Password:

Type and confirm password (mandatory):

Provide a password to protect the private key and click *Next*.


Certificate Export Wizard

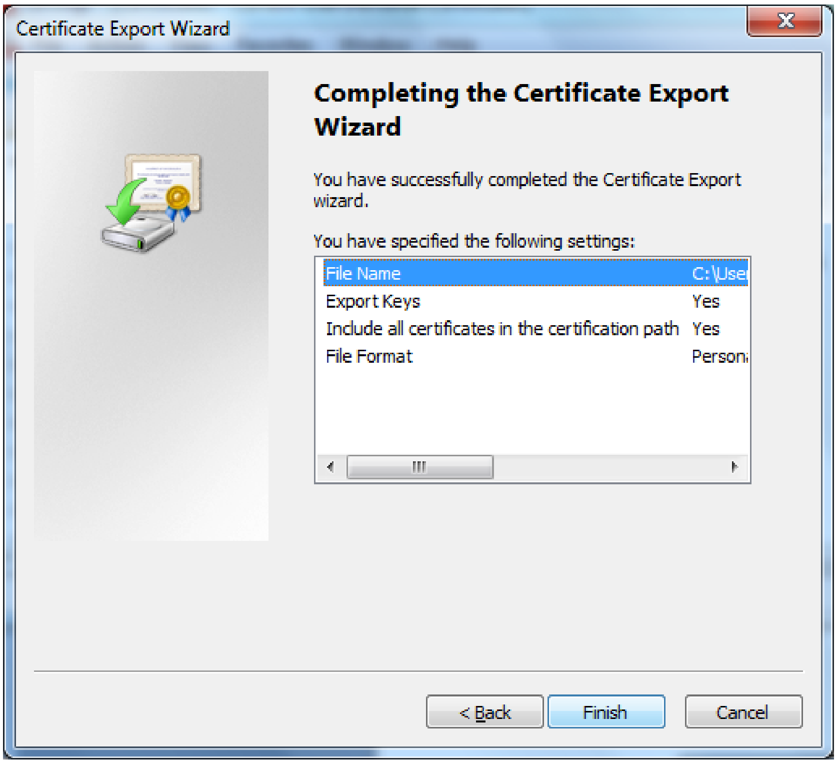
File to Export

Specify the name of the file you want to export

File name: C:\Users\walthj\Documents\Certificates for Access to CA\JW_Odet

On the next dialogue, provide the full filepath and filename of the file you want to export i.e. where the certificate will be stored. Once the filepath and name has been provided, click *Next*.

You should then see confirmation that the certificate has been successfully exported. Click *Finish*.



Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

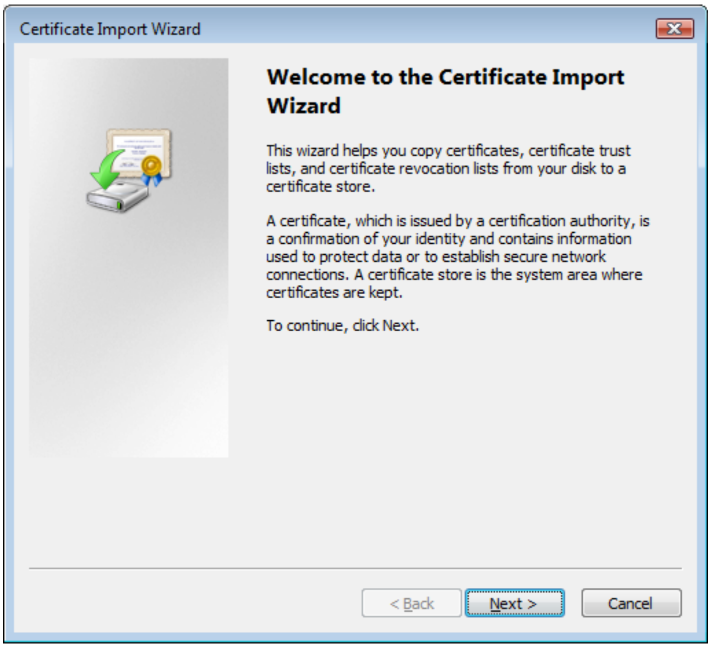
You have specified the following settings:

File Name	C:\Use
Export Keys	Yes
Include all certificates in the certification path	Yes
File Format	Person

If you could not transfer the certificate securely to the target computer over a network (e.g. via a local area network) then use a secure means such as a USB stick to transport the certificate to the target computer.

How to import the certificate on the target computer

On the new machine, double click on the .pfx file. This starts the certificate Import Wizard. Click *Next*.



Certificate Import Wizard

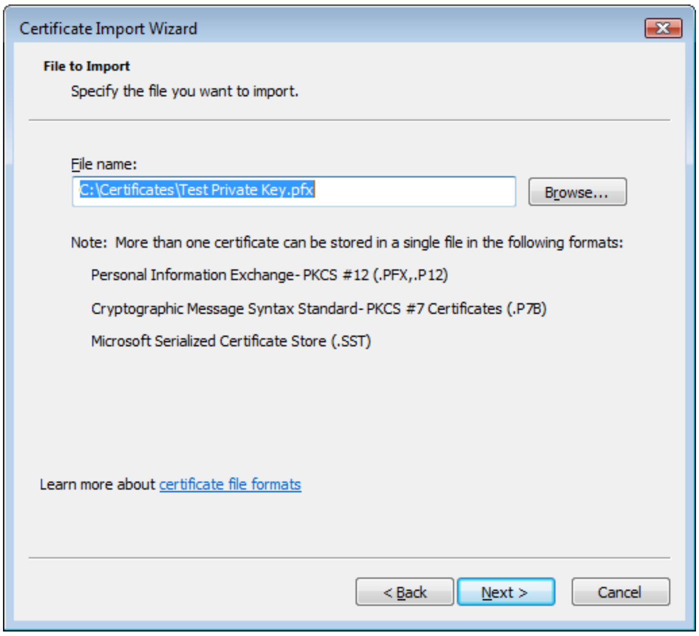
Welcome to the Certificate Import Wizard

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.

3. The next dialogue will show you the current location of the .pfx file. Click *Next*.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name: C:\Certificates\Test Private Key.pfx

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

Personal Information Exchange- PKCS #12 (.PFX,.P12)

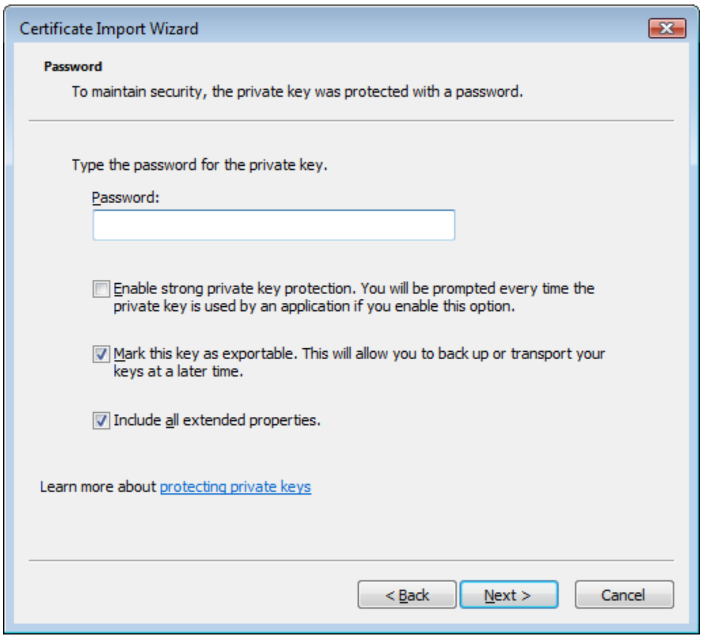
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

4. On the next dialogue, provide the password with which you protected the certificate earlier.
   Select “Include all extended properties”.
   Select “Mark this key as exportable” to enable you to export the certificate again in future. This may be useful if the machine on which you intend to

use the certificate becomes unusable, or if you move the application which uses the certificate to a different machine.
There is no need to select "Enable strong private key protection."
Click *Next*.



Certificate Import Wizard

Password

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

Type the password for the private key.

Password:

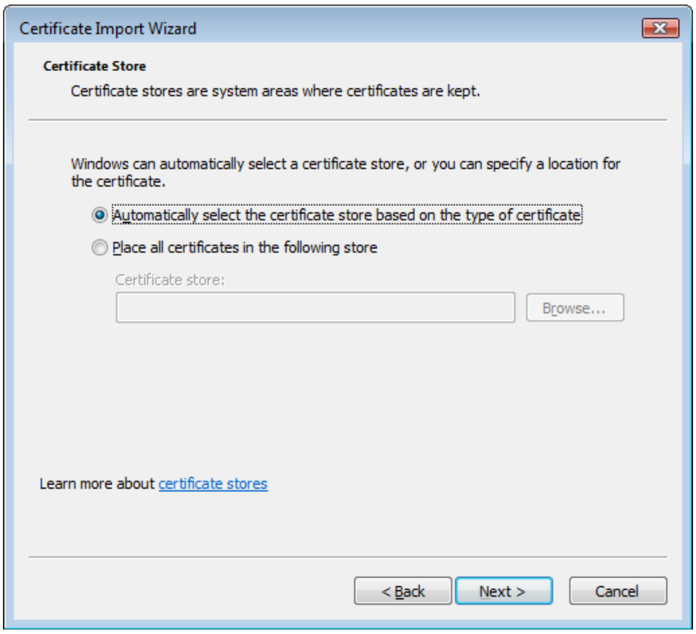
□ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

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

☑ Include all extended properties.

Learn more about protecting private keys

5. Select "Automatically select the certificate store based on the type of certificate".
   Click *Next*, then *Finish*. The certificate will then be imported to the appropriate certificate store on the new machine.



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 the certificate.

● Automatically select the certificate store based on the type of certificate

○ Place all certificates in the following store

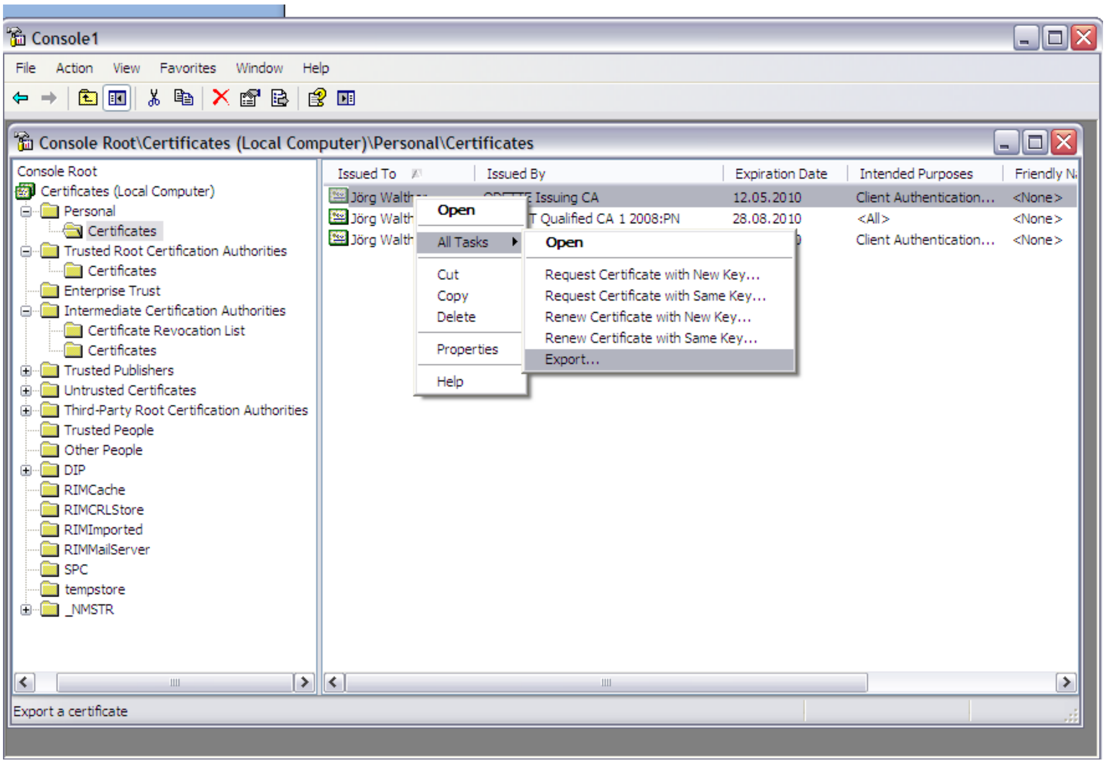
Certificate store:

Learn more about certificate stores

How to export your public key from the Windows keystore

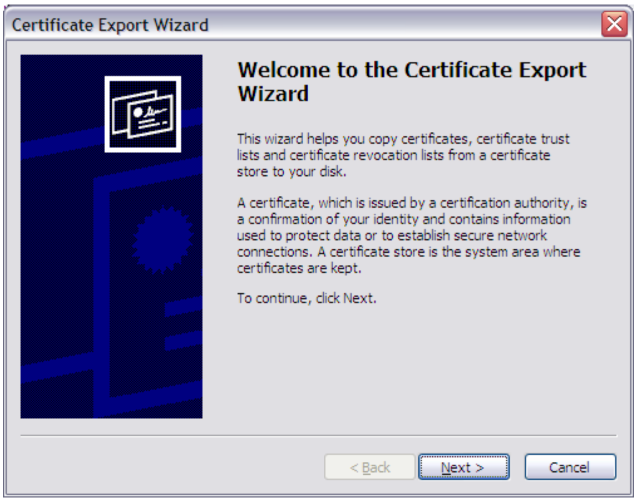
Once you have downloaded your certificate, you need to provide the public key part of the certificate to all partners with whom you will communicate using this certificate. Having your public key will enable your partners to decrypt files you send to them and to encrypt files they send to you.

1. Select the certificate in the management console and select Export from the context menu (right mouse button) to invoke the export wizard.


Console1
File Action View Favorites Window Help
Console Root\Certificates (Local Computer)\Personal\Certificates
Console Root
Certificates (Local Computer)
Personal
Certificates
Trusted Root Certification Authorities
Certificates
Enterprise Trust
Intermediate Certification Authorities
Certificate Revocation List
Certificates
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
Trusted People
Other People
DIP
RIMCache
RIMCRLStore
RIMImported
RIMMailServer
SPC
tempstore
_NMSTR
Open
All Tasks
Cut
Copy
Delete
Properties
Help
Open
Request Certificate with New Key...
Request Certificate with Same Key...
Renew Certificate with New Key...
Renew Certificate with Same Key...
Export...
Export a certificate

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly N...
Jörg Walth	Issuing CA	12.05.2010	Client Authentication...	<None>
Jörg Walth	T Qualified CA 1 2008:PN	28.08.2010	<All>	<None>
Jörg Walth			Client Authentication...	<None>

2. This starts the Certificate Export Wizard. Click *Next*.



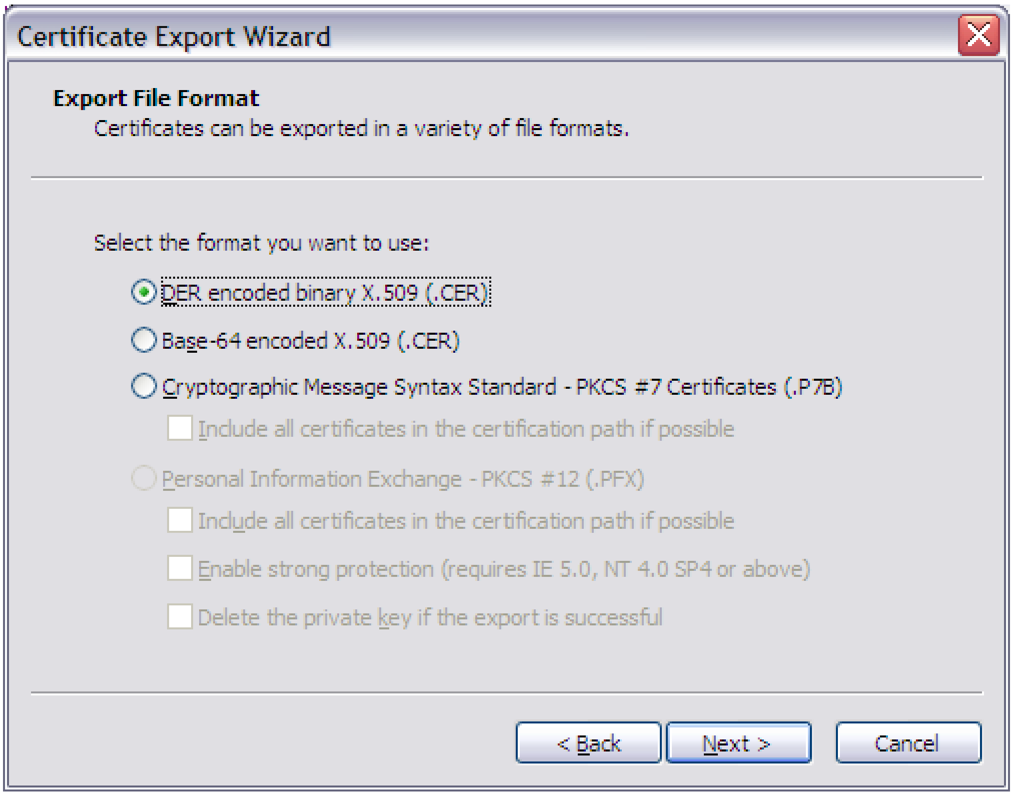
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

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.

3. Select the file format (DER encoded) and click *Next*



Certificate Export Wizard

Export File Format
Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

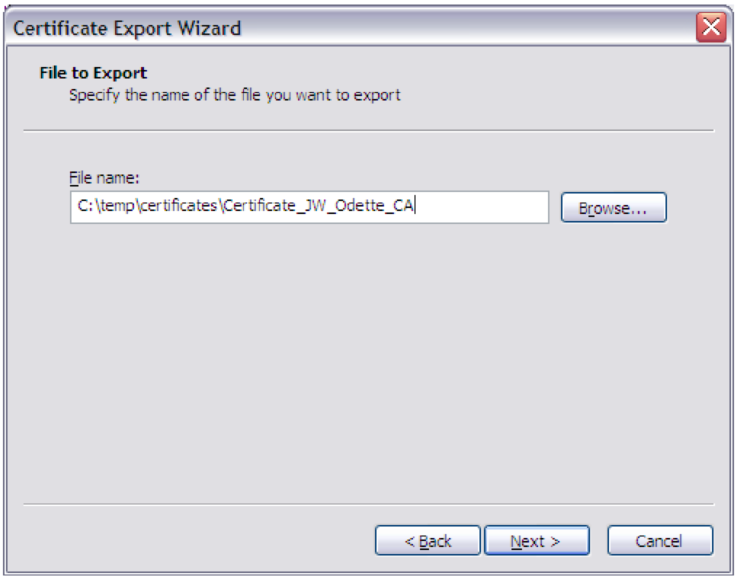
○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

□ Enable strong protection (requires IE 5.0, NT 4.0 SP4 or above)

□ Delete the private key if the export is successful

4. On the next dialogue, provide the full path and filename of the public key you want to export i.e. where the public key will be stored in readiness for sending to your communication partners. Pls. note: the target directory must already exist, it will not be created by the wizard “on the fly”. Type it in or use the Browse button. The file must be exported as a .cer file if you selected the DER file format above.
Once the file path and name has been provided, click *Next*.

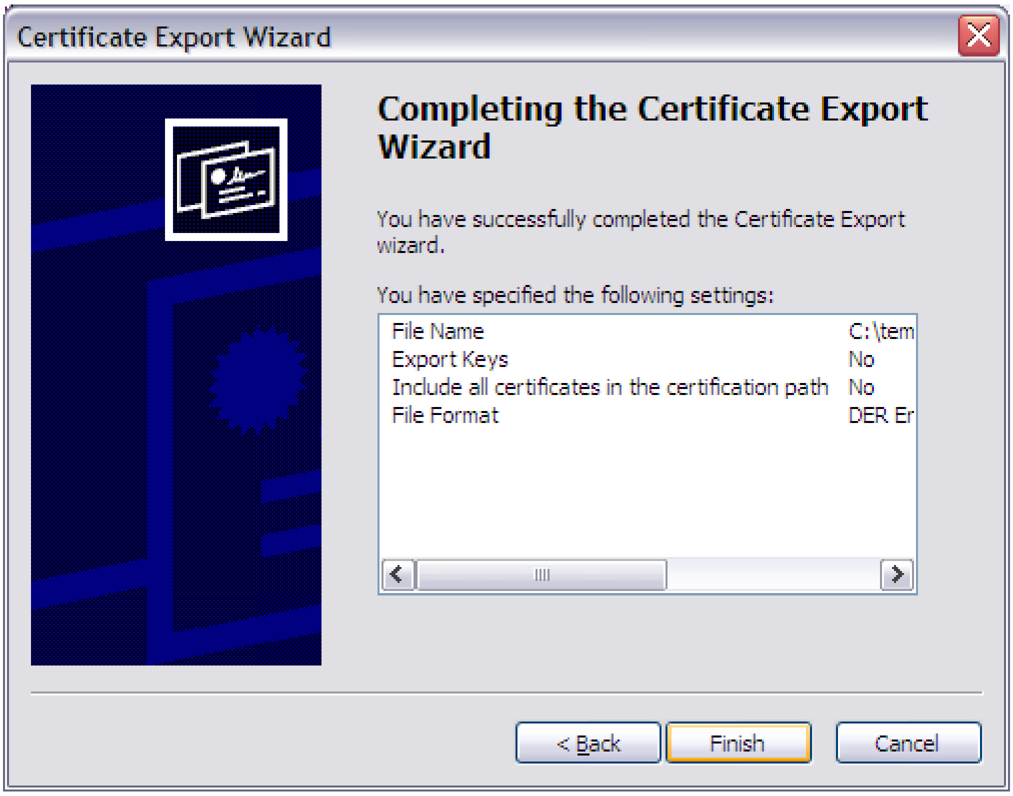


Certificate Export Wizard

File to Export
Specify the name of the file you want to export

File name:
C:\temp\certificates\Certificate_JW_Odette_CA

5. You should then see confirmation that the certificate has been successfully exported. Click *Finish*.



Certificate Export Wizard

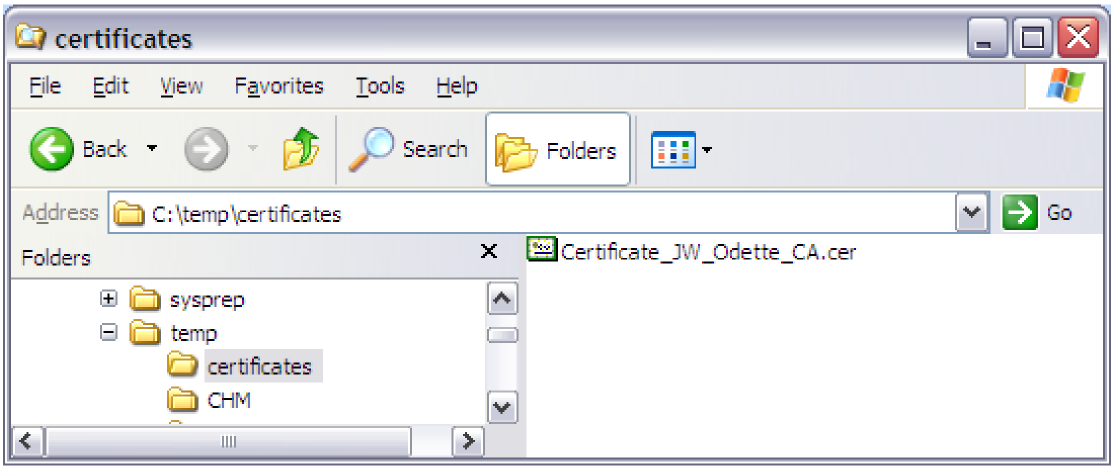
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\tem
Export Keys	No
Include all certificates in the certification path	No
File Format	DER Er

You will find the certificate in the target directory and you can then send it to your business partners.



certificates

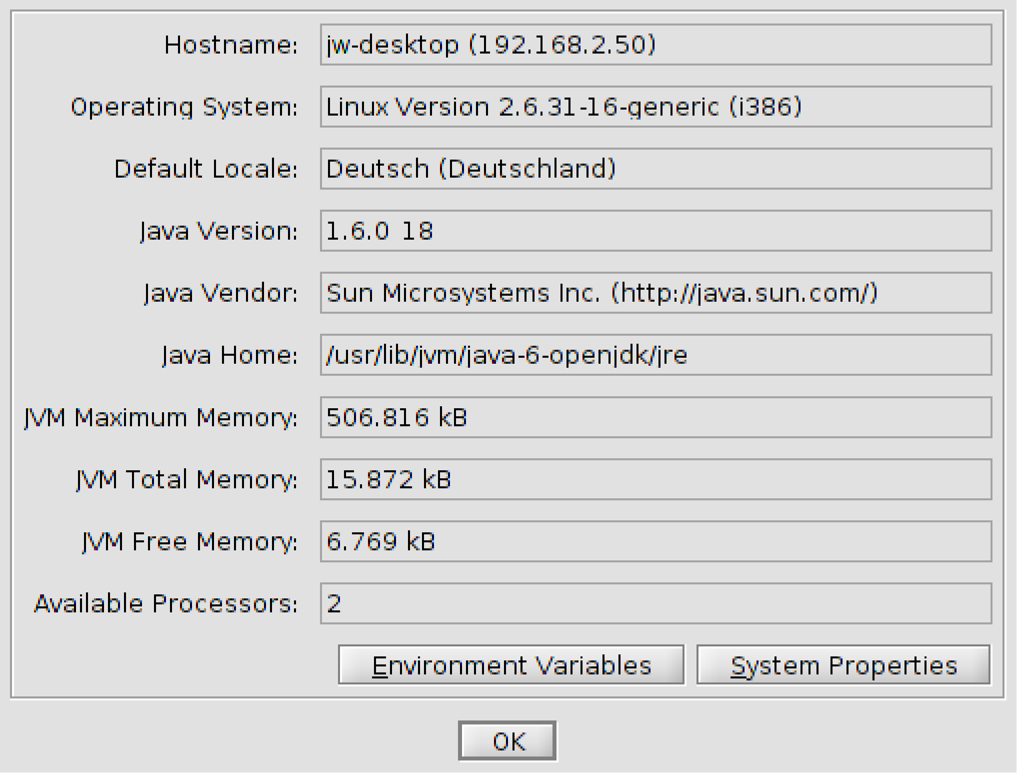
Address C:\temp\certificates

Certificate_JW_Odette_CA.cer

How to create a certificate signing request (CSR) on a Linux or Windows machine with an external tool

The example explains how to create a CSR and obtain an Odette CA certificate using a Linux machine. However, the same steps can be performed on a Windows system.

The machine used as OFTP2 server for the process has the following parameters: Debian Linux Ubuntu V10.04 with Gnome GUI.
The machine runs behind a firewall in a private network. The OFTP2 server can be contacted from the internet under oftp2.dydns.info (dynamic DNS assignment to an ADSL IP address):



Hostname: jw-desktop (192.168.2.50)
Operating System: Linux Version 2.6.31-16-generic (i386)
Default Locale: Deutsch (Deutschland)
Java Version: 1.6.0 18
Java Vendor: Sun Microsystems Inc. (http://java.sun.com/)
Java Home: /usr/lib/jvm/java-6-openjdk/jre
JVM Maximum Memory: 506.816 kB
JVM Total Memory: 15.872 kB
JVM Free Memory: 6.769 kB
Available Processors: 2

Preparation:

You can either use a command line tool or a tool with a GUI. Both processes are described in the document. The command line tool is openssl, which is part of the UBUNTU standard package and should be available on your computer.

If you prefer a graphical tool, you may use

- Portecle http://sourceforge.net/projects/portecle or
- KeyStore Explorer: http://www.lazgosoftware.com/kse/downloads.html

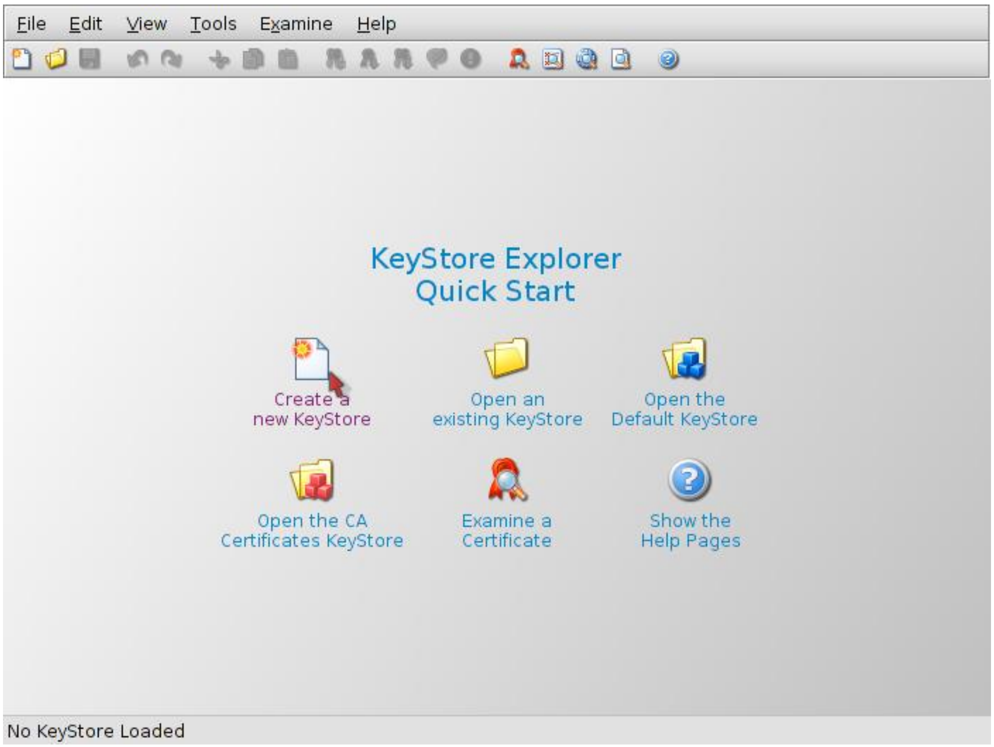
Both programs are freeware and are available for Linux and Windows. They use the JAVA Runtime Engine and Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files. Both are available at http://www.oracle.com/technetwork/java/javase/downloads/index.html

Install the Linux or Windows package (depending on your OS) and start the program.

Example 1:
Generation of private key and CSR with the program Portecle
This process is described in a short video at http://forum.odette.org/repository/CSR_with_Portecle-de.mp4 (German version)

Example 2:
Generation of private key and CSR with the program KeyStore Explorer:

Step1: Generation of a private key:



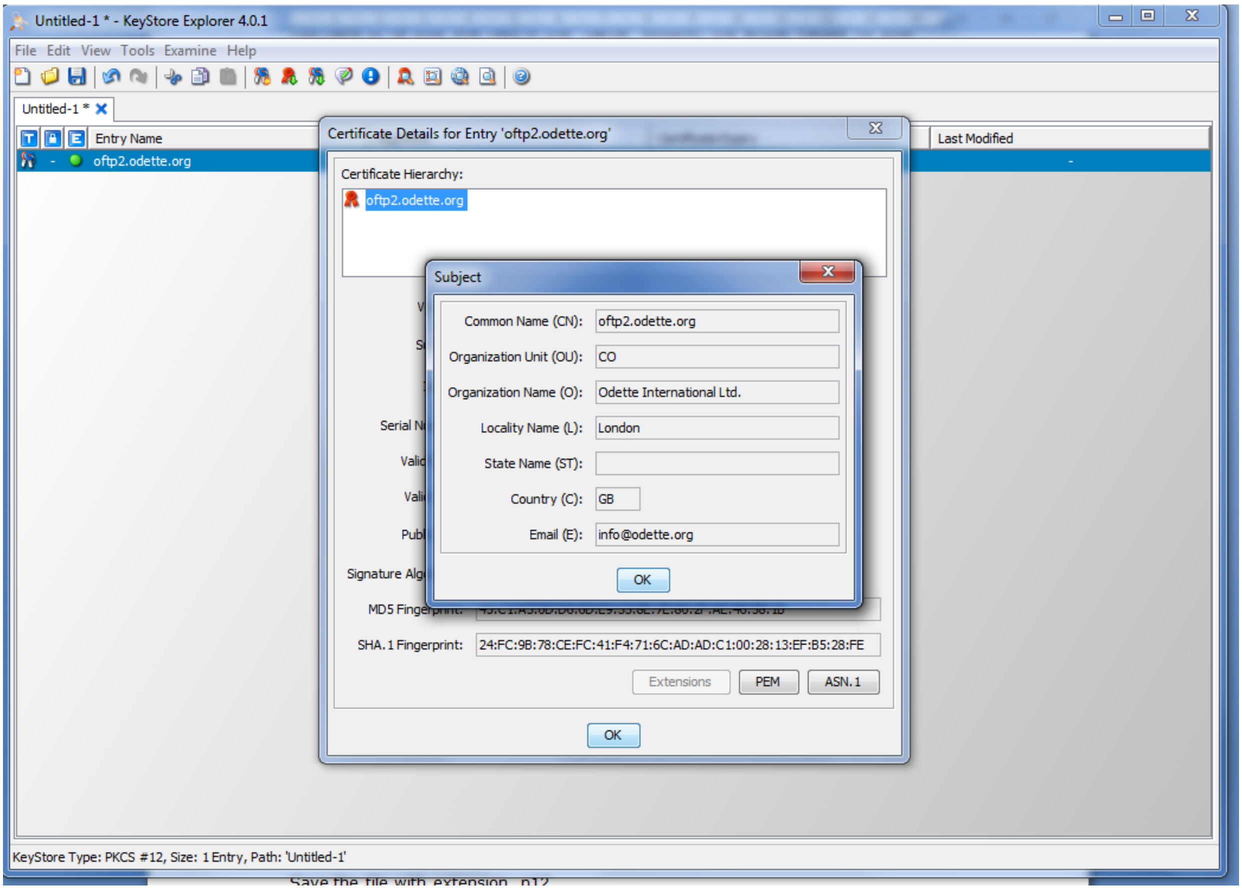
Select “Create a new KeyStore” - chose PKCS12

Then use Tools / Generate Key pair to create a new private and public key pair.

Select algorithm RSA, key size 2048 and continue.

Assign values to the subject attributes.

We strongly recommend to use only Latin (ASCII) characters or digits for any values entered here in the Name window.


Untitled-1 * - KeyStore Explorer 4.0.1
File Edit View Tools Examine Help
Untitled-1 *
Entry Name
Last Modified
Certificate Details for Entry 'oftp2.odette.org'
Certificate Hierarchy:
Extensions
PEM
ASN.1
OK
Subject
OK

oftp2.odette.org

Common Name (CN): oftp2.odette.org

Organization Unit (OU): CO

Organization Name (O): Odette International Ltd.

Locality Name (L): London

State Name (ST):

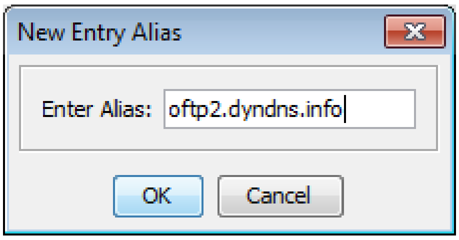
Country (C): GB

Email (E): info@odette.org

SHA.1 Fingerprint: 24:FC:9B:78:CE:FC:41:F4:71:6C:AD:AD:C1:00:28:13:EF:B5:28:FE

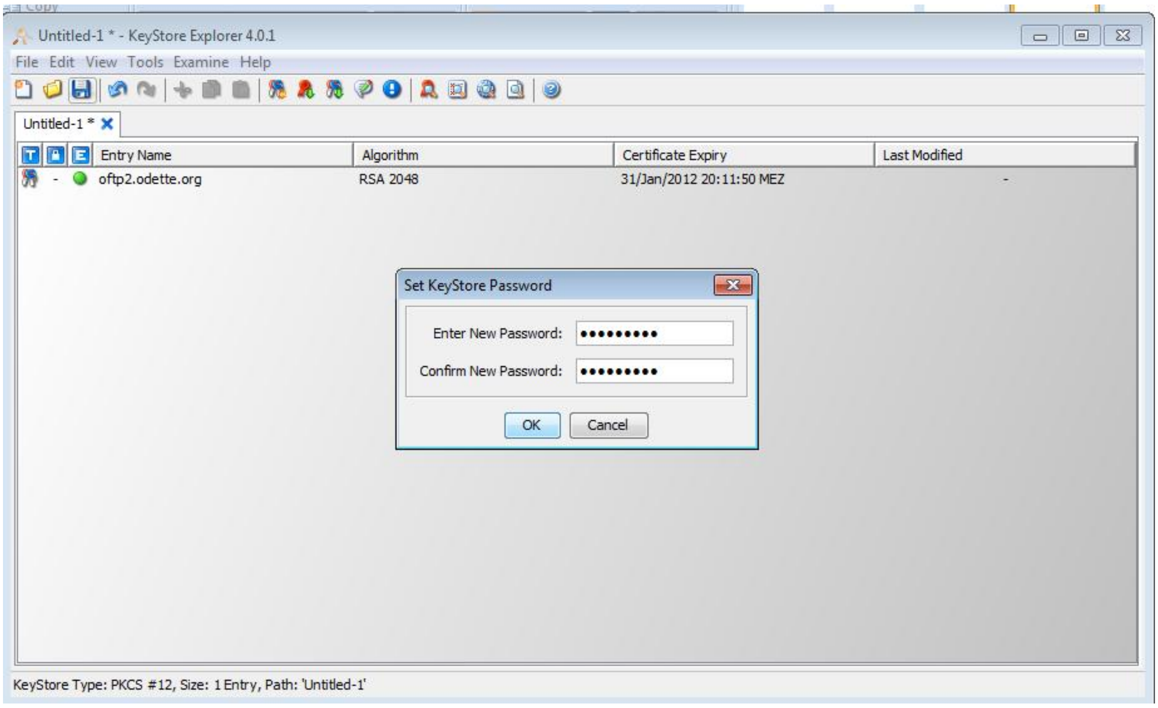
KeyStore Type: PKCS #12, Size: 1 Entry, Path: 'Untitled-1'

Assign an alias name to your key pair, e.g. the DNS of your OFTP2 server:



Enter Alias: oftp2.dyndns.info

Save the key store. You will be asked for a password to protect your keystore against non-authorised access.


Untitled-1 * - KeyStore Explorer 4.0.1
File Edit View Tools Examine Help
Untitled-1 *
OK
Cancel

Entry Name	Algorithm	Certificate Expiry	Last Modified
oftp2.odette.org	RSA 2048	31/Jan/2012 20:11:50 MEZ	-

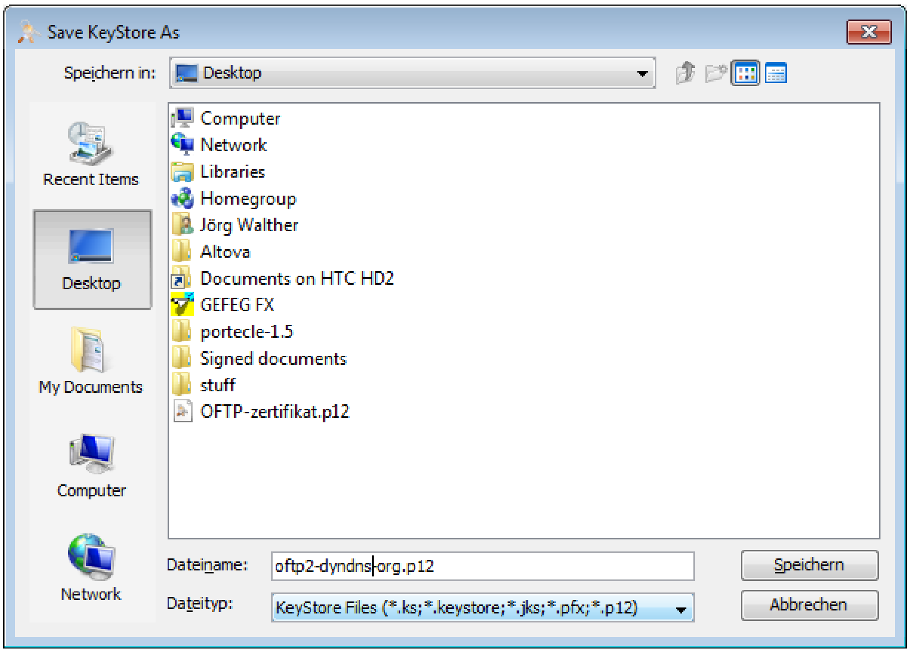
Set KeyStore Password

Enter New Password: •••••••••

Confirm New Password: •••••••••

KeyStore Type: PKCS #12, Size: 1 Entry, Path: 'Untitled-1'

Save the file with extension .p12



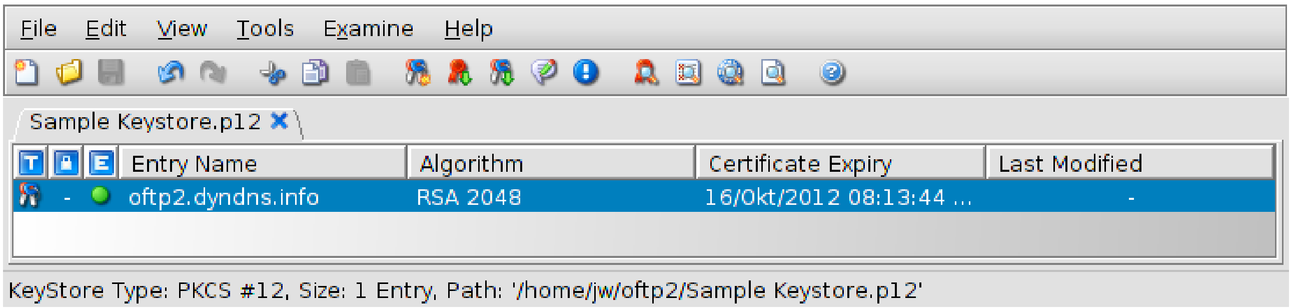
Speichern in: Desktop

Dateiname: oftp2-dyndns.org.p12

Dateityp: KeyStore Files (*.ks;*.keystore;*.jks;*.pfx;*.p12)

Step 2 : Generation of the CSR

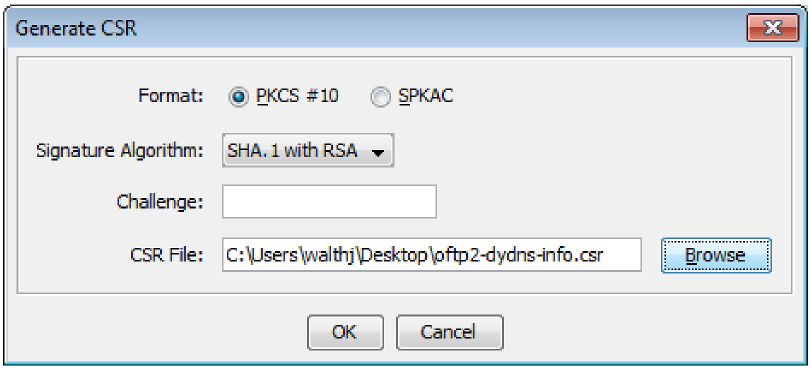
Select the entry in the keystore, right mouse button, “Generate CSR”



T	🔒	E	Entry Name	Algorithm	Certificate Expiry	Last Modified
	-	●	oftp2.dyndns.info	RSA 2048	16/Okt/2012 08:13:44 ...	-

KeyStore Type: PKCS #12, Size: 1 Entry, Path: '/home/jw/oftp2/Sample Keystore.p12'

Select Format (PKCS#10), signature algorithm (SHA.1 with RSA) and the output file:



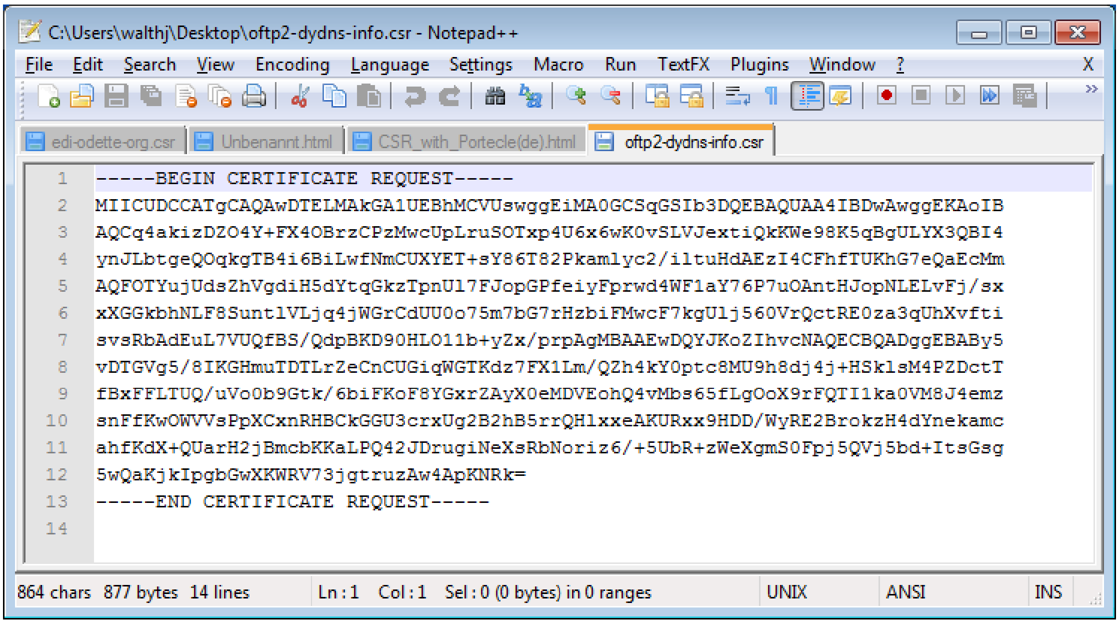
Format: ● PKCS #10 ○ SPKAC

Signature Algorithm: SHA.1 with RSA

Challenge:

CSR File: C:\Users\walthj\Desktop\oftp2-dydns-info.csr

As a result you will get a text file with the CSR:



```
-----BEGIN CERTIFICATE REQUEST-----
MIICUDCCATgCAQAwDTELMAkGA1UEBhMCVUswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCq4akizDZO4Y+FX4OBrzCPzMwcUpLruSOTxp4U6x6wK0vSLVJextiQkKWe98K5qBgULYX3QBI4
ynJLbtgeQOqkgTB4i6BiLwfNmCUXYET+sY86T82Pkamlyc2/iltuHdAEzI4CFhfTUKhG7eQaEcMm
AQFOTYujUdsZhVgdiH5dYtqGkzTpnUl7FJopGPfeiyFprwd4WF1aY76P7uOAntHJopNLELvFj/sx
xXGGkbhNLF8SuntlVLjq4jWGrCdUU0o75m7bG7rHzbiFMwcF7kgUlj560VrQctRE0za3qUhXvfti
svsRbAdEuL7VUQfBS/QdpBKD90HLO11b+yZx/prpAgMBAAEwDQYJKoZIhvcNAQECBQADggEBABy5
vDTGVg5/8IKGHmuTDTLrZeCnCUGiqWGTKdz7FX1Lm/QZh4kY0ptc8MU9h8dj4j+HSklsM4PZDctT
fBxFFLTUQ/uVo0b9Gtk/6biFKoF8YGxrZAyX0eMDVEohQ4vMbs65fLgOoX9rFQTI1ka0VM8J4emz
snFfKwOWVVsPpXCxnRHBCkGGU3crxUg2B2hB5rrQHlxxeAKURxx9HDD/WyRE2BrokzH4dYnekamc
ahfKdX+QUarH2jBmcbKKaLPQ42JDrugiNeXsRbNoriz6/+5UbR+zWeXgmS0Fpj5QVj5bd+ItsGsg
5wQaKjkIpgbGwXKWRV73jgtruzAw4ApKNRk=
-----END CERTIFICATE REQUEST-----
```

864 chars 877 bytes 14 lines Ln : 1 Col : 1 Sel : 0 (0 bytes) in 0 ranges UNIX ANSI INS

Example 3:
Generation of the private key and CSR With the program openssl:

Step 1: Generation of a private key:

1. Open a terminal session
2. Change to super-user mode (su)
3. Change to directory /etc/sll (Ubuntu, in other Linux systems it can also be /usr/local/ssl .
4. Run ***openssl genrsa -des3 -out private-key.pem 2048***
   This command generates a 2048 bit private key and stores it in the /etc/ssl directory. During the generation you will be asked to enter a password to protect the eccess to your private key.

Step 2: Generation of the certificate signing request:

1. Run ***openssl req -new -key private-key.pem -out oftp2-dyndns-info.csr***

During the process you may be asked for several inputs:

Example:

```
Enter pass phrase for private-key.pem: **********
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]: GB
State or Province Name (full name) [Some-State]:London
Locality Name (eg, city) []:London
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Odette
Organizational Unit Name (eg, section) []:Central Office
Common Name (eg, YOUR name) []:oftp2.dyndns.info
Email Address []:jwalther@odette.org
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:.
An optional company name []:Odette International
```

Again, all values will be overwritten by the values entered during the certificate order process (see **Error! Reference source not found.**)

Step: 3 Order the certificate

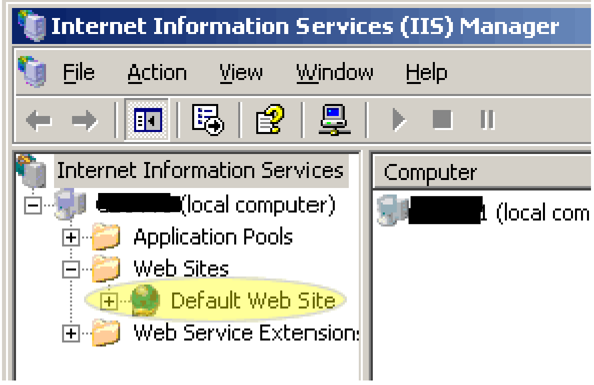
After these preparations, you can order the certificate at https://www.odetteca.com

Follow the steps as described in Certificate Order Process

How to generate a CSR on IIS 6 Microsoft Windows Server 2003

Follow these instructions to generate a Private Key and CSR. You must have at least Service Pack 1 installed.

1. Open the **Internet Information Services (IIS) Manager**. From the **Start** button select **Programs** > **Administrative Tools** > **Internet Information Services Manager**.
2. In **IIS Manager**, double-click the local computer, and then double-click the **Web Sites** folder.
3. **Right-click** the Web site for which you want to request a certificate, and then click **Properties**. By default it will be Default Web Site, yours may be different.



4. Select the **Directory Security** tab and click **Server Certificate** in the **Secure communications** section.
5. Click **Next** in the **Welcome to the Web Server Certificate Wizard** window.
6. Select **Create a new certificate**, Click **Next**.
7. Select **Prepare the request now, but send it later**.
8. At the **Name and Security Settings** screen, fill in the **friendly name** field for the new certificate

   Tip: the friendly name can be any name that helps you remember what this certificate is for when you see it in a list later. We recommend using your domain as the friendly name, such as mysite.com.

9. Select **bit length 2048**. Click **Next**.
10. Leave the 'Select cryptographic service provider (CSP) for this certificate' **unchecked**. Click **Next**.
11. You will be asked for several pieces of info which will be used by Odette CA to create your new certificate. These fields must match the information given in screen 1, Certificate Details. The following characters should not be used when typing in your CSR input: < > ~ ! @ # $ % ^ / \ ( ) ? , & .

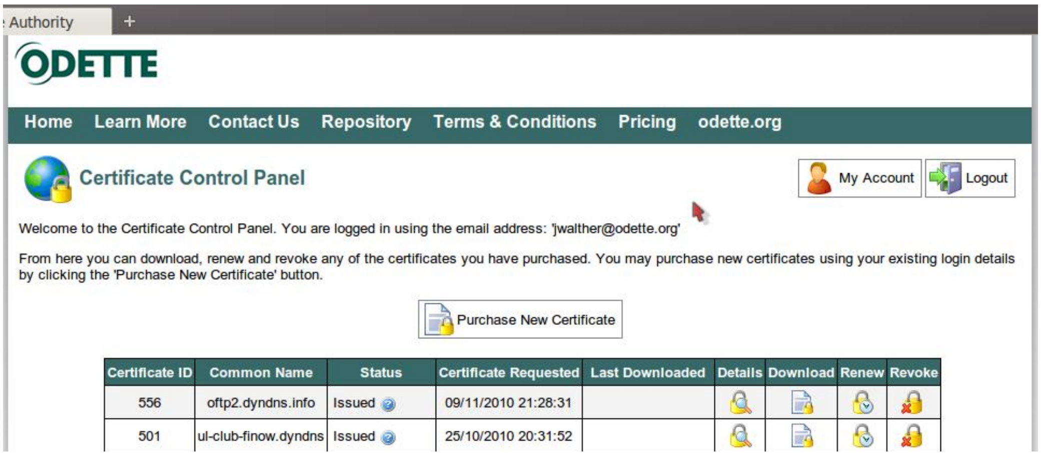
12. Specify the organizational unit. Do not include http:// nor https://. Refer to the CSR legend in the right-hand column of this page for examples. If this is wrong, your certificate will not work properly. Click **Next**.
13. Enter your Geographical Information for Country, State, and City. **Do not abbreviate** States and Cities. Click **Next**.
14. In the **Certificate Request File Name** box enter the path and file name where you want to save your CSR. You can use the default of c:\certreq.txt. Remember where you save it, you'll need to be able to find this CSR file later. Click **Next**.
15. Review the data on the Request File Summary screen and click **Next**.
16. Click **Finish** to complete the Wizard.

Now, from a simple text editor such as Notepad (do not use Word), open the CSR file you just created at c:\certreq.txt (your path/filename may be different). You will need to copy-and-paste the contents of this file, including the top and bottom lines, into the relevant box during the online order process.

How to download and to install the certificate on a Linux or Windows machine, if you have created the CSR with an external application

After the validation process you will receive an email notification that your certificate has been issued and is ready for download.

Log into the CA application and you will see the certificate control panel. Click the Download button for your certificate.



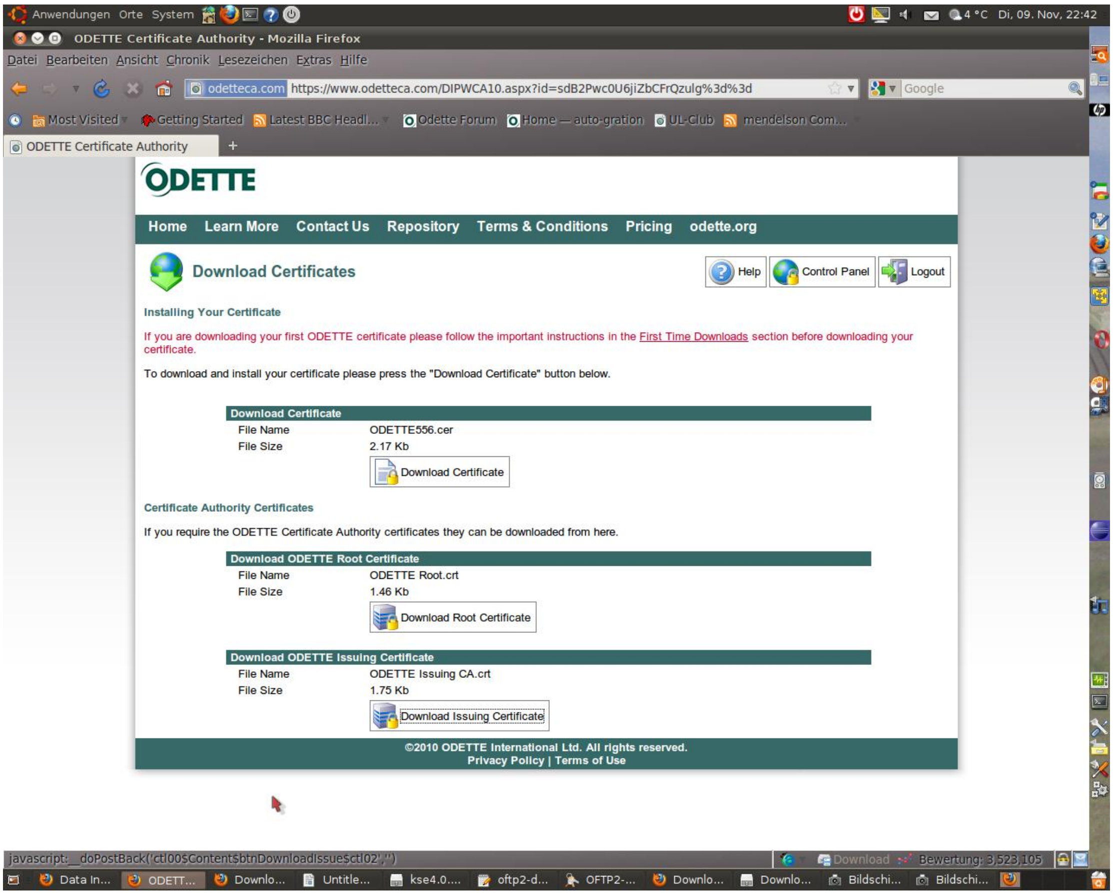
Certificate Control Panel

Welcome to the Certificate Control Panel. You are logged in using the email address: 'jwalther@odette.org'

From here you can download, renew and revoke any of the certificates you have purchased. You may purchase new certificates using your existing login details by clicking the 'Purchase New Certificate' button.

Certificate ID	Common Name	Status	Certificate Requested	Last Downloaded	Details	Download	Renew	Revoke
556	oftp2.dyndns.info	Issued	09/11/2010 21:28:31					
501	ul-club-finow.dyndns	Issued	25/10/2010 20:31:52					

You will be forwarded to another page from where you can download your certificate and Odette CA’s Root and Issuing certificate.



odetteca.com https://www.odetteca.com/DIPWCA10.aspx?id=sdB2Pwc0U6jiZbCFrQzulg%3d%3d

Download Certificates

Installing Your Certificate

If you are downloading your first ODETTE certificate please follow the important instructions in the First Time Downloads section before downloading your certificate.

To download and install your certificate please press the "Download Certificate" button below.

Download Certificate	
File Name	ODETTE556.cer
File Size	2.17 Kb

Certificate Authority Certificates

If you require the ODETTE Certificate Authority certificates they can be downloaded from here.

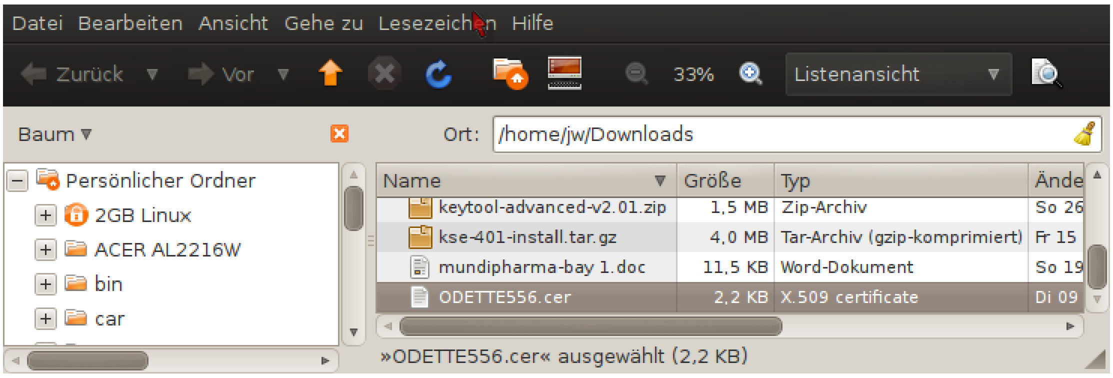
Download ODETTE Root Certificate	
File Name	ODETTE Root.crt
File Size	1.46 Kb

Download ODETTE Issuing Certificate	
File Name	ODETTE Issuing CA.crt
File Size	1.75 Kb

©2010 ODETTE International Ltd. All rights reserved.
Privacy Policy | Terms of Use

javascript:__doPostBack('ctl00$Content$btnDownloadIssue$ctl02','')

Store your certificate on your hard disk.



Ort: /home/jw/Downloads

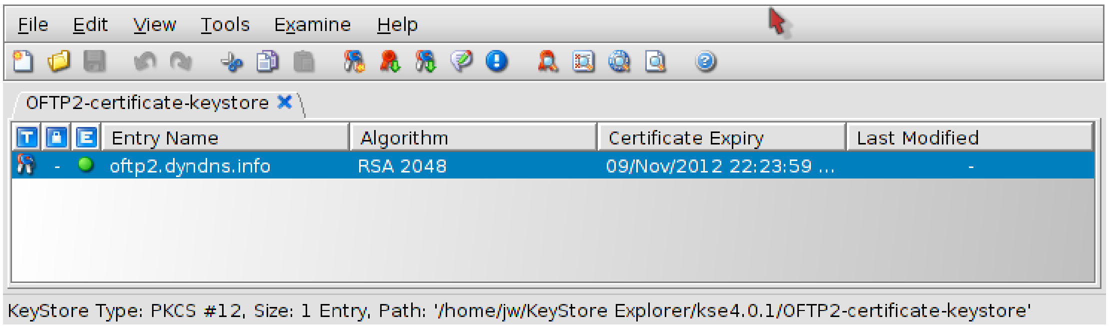
Name	Größe	Typ	Ände
keytool-advanced-v2.01.zip	1,5 MB	Zip-Archiv	So 26
kse-401-install.tar.gz	4,0 MB	Tar-Archiv (gzip-komprimiert)	Fr 15
mundipharma-bay 1.doc	11,5 KB	Word-Dokument	So 19
ODETTE556.cer	2,2 KB	X.509 certificate	Di 09

»ODETTE556.cer« ausgewählt (2,2 KB)

If you have used openssl to generate your private key, you have now both files, the private key and the certificate on your hard disk.
If you use the certificate for OFTP2 data communication, refer to your software vendors instruction to import the private key and the certificate into your application.

In case your software expects the private key and the certificate in a different format, such as pfx, you may want to carry out the following steps:

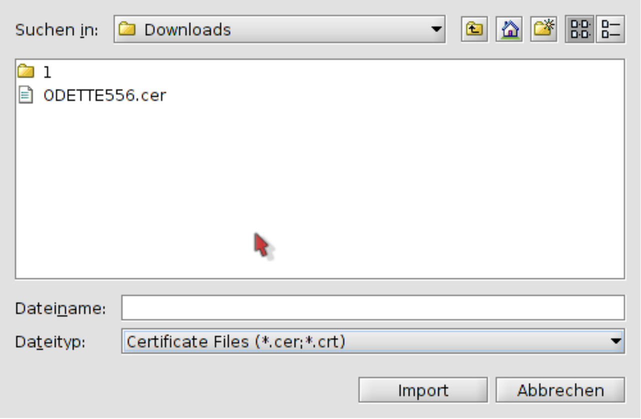
Open the Keystore Explorer application and load the key store that you have created earlier .



T	🔒	E	Entry Name	Algorithm	Certificate Expiry	Last Modified
	-	●	oftp2.dyndns.info	RSA 2048	09/Nov/2012 22:23:59 ...	-

KeyStore Type: PKCS #12, Size: 1 Entry, Path: '/home/jw/KeyStore Explorer/kse4.0.1/OFTP2-certificate-keystore'

Import your certificate through right mouse button / Import CA-Reply.



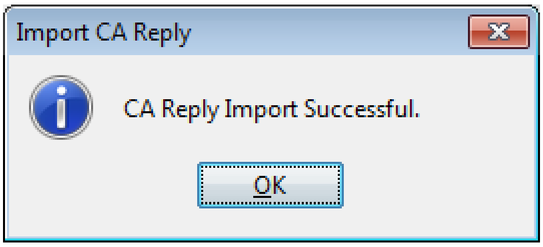
Suchen in: Downloads

1
ODETTE556.cer

Dateiname:

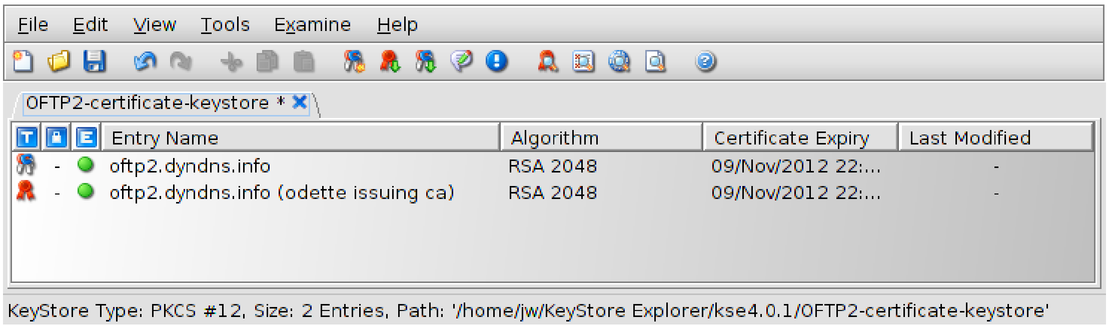
Dateityp: Certificate Files (*.cer;*.crt)

Select the certificate file and click *Import.*



CA Reply Import Successful.

Your key store will then contain the private key and the matching certificate.


File Edit View Tools Examine Help
OFTP2-certificate-keystore *

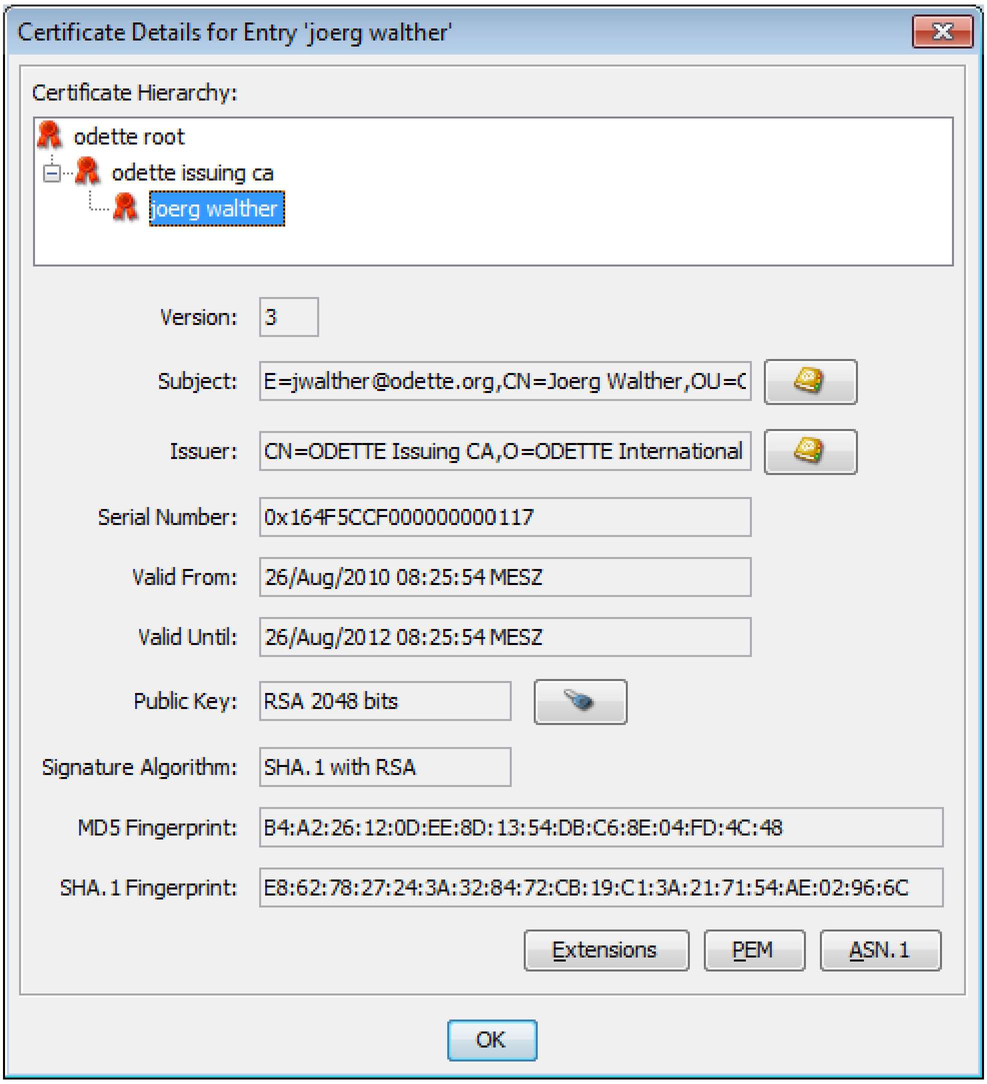
T	🔒	E	Entry Name	Algorithm	Certificate Expiry	Last Modified
	-	●	oftp2.dyndns.info	RSA 2048	09/Nov/2012 22:...	-
	-	●	oftp2.dyndns.info (odette issuing ca)	RSA 2048	09/Nov/2012 22:...	-

KeyStore Type: PKCS #12, Size: 2 Entries, Path: '/home/jw/KeyStore Explorer/kse4.0.1/OFTP2-certificate-keystore'

Repeat the process for the Odette Root and the Odette Issuing CA certificates.

Verify the completeness of your key store by selecting your key pair, right mouse button, View Details / Certificate Chain

The result should show the complete chain from Odette Root to your individual key



Certificate Details for Entry 'joerg walther'

Certificate Hierarchy:

- odette root
  - odette issuing ca
    - joerg walther

Version: 3

Subject: E=jwalther@odette.org,CN=Joerg Walther,OU=C

Issuer: CN=ODETTE Issuing CA,O=ODETTE International

Serial Number: 0x164F5CCF000000000117

Valid From: 26/Aug/2010 08:25:54 MESZ

Valid Until: 26/Aug/2012 08:25:54 MESZ

Public Key: RSA 2048 bits

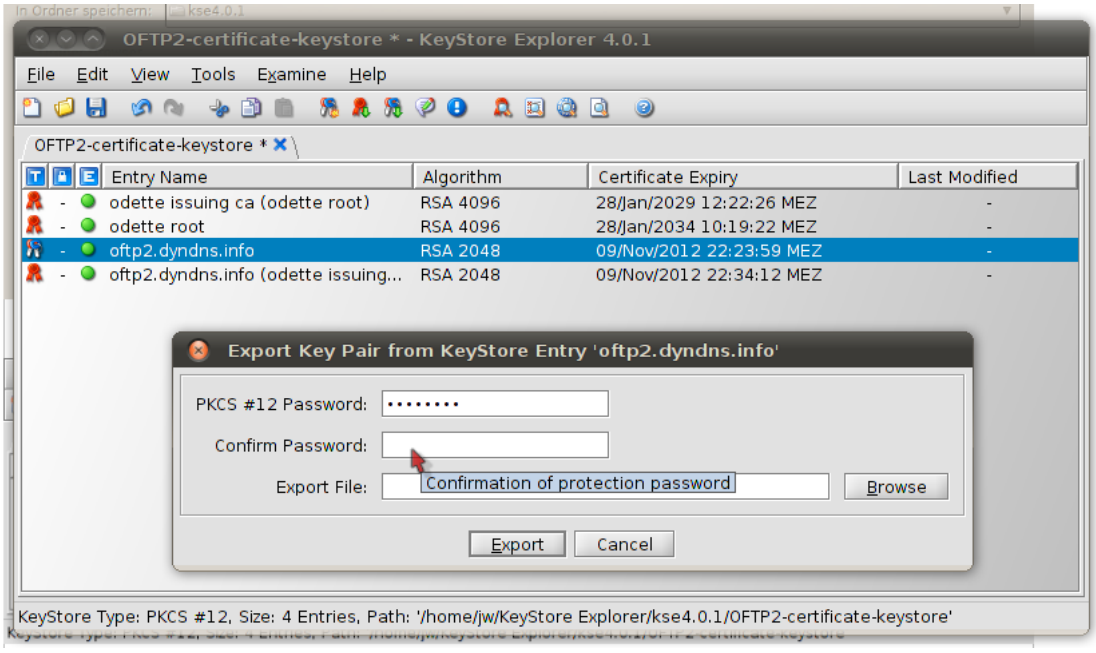
Signature Algorithm: SHA.1 with RSA

MD5 Fingerprint: B4:A2:26:12:0D:EE:8D:13:54:DB:C6:8E:04:FD:4C:48

SHA.1 Fingerprint: E8:62:78:27:24:3A:32:84:72:CB:19:C1:3A:21:71:54:AE:02:96:6C

How to export public and private key from an external application (e.g. to be transferred to another computer or imported into your OFTP2 software key store)

You can use the export function under the Tools menu item to create a pfx file that contains your public key (certificate) and your private key.


OFTP2-certificate-keystore * - KeyStore Explorer 4.0.1
File
Edit
View
Tools
Examine
Help
OFTP2-certificate-keystore *
Export Key Pair from KeyStore Entry 'oftp2.dyndns.info'
Browse
Export
Cancel

			Entry Name	Algorithm	Certificate Expiry	Last Modified
	-	●	odette issuing ca (odette root)	RSA 4096	28/Jan/2029 12:22:26 MEZ	-
	-	●	odette root	RSA 4096	28/Jan/2034 10:19:22 MEZ	-
	-	●	oftp2.dyndns.info	RSA 2048	09/Nov/2012 22:23:59 MEZ	-
	-	●	oftp2.dyndns.info (odette issuing...	RSA 2048	09/Nov/2012 22:34:12 MEZ	-

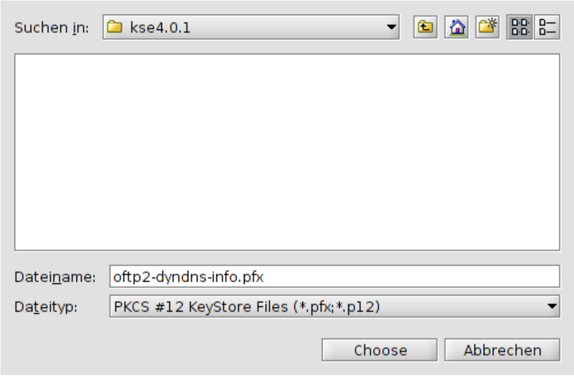
PKCS #12 Password: •••••••••

Confirm Password:

Export File:

Confirmation of protection password

KeyStore Type: PKCS #12, Size: 4 Entries, Path: '/home/jw/KeyStore Explorer/kse4.0.1/OFTP2-certificate-keystore'



Suchen in: kse4.0.1

Dateiname: oftp2-dyndns-info.pfx

Dateityp: PKCS #12 KeyStore Files (*.pfx;*.p12)

Assign a suitable file name and save your key-pair.

Attention:

You should **never give the private key to a business partner**! It must always stay in a safe location on your computer.

If you use the certificate for OFTP2 data exchange, your certificate will be exchanged with your business partners through the protocol and there is no need to exchange anything manually.

If you need to provide your certificate to a business partner for other applications, send them only the certificate file downloaded from the Odette CA website!