



How to Order and Install Odette Certificates

Odette CA Help File and User Manual

Contents

<i>Preparation for Ordering an Odette Certificate.....</i>	<i>3</i>
Step 1: Prepare the information you need for the order process	3
Step 2: Generate a Certificate Signing Request	5
<i>Log on to the Odette CA and start the order process</i>	<i>10</i>
<i>Order confirmation</i>	<i>19</i>
<i>Validation and approval process</i>	<i>19</i>
<i>Download the certificate</i>	<i>20</i>
<i>Renew a certificate</i>	<i>21</i>
<i>Annexes</i>	<i>23</i>
1. How to download and install the certificate on your local computer	24
2. How to find your certificate in the Windows keystore after installation	29
3. How to create a CSR with batch files	33
4. How to revoke a certificate	35

Preparation for Ordering an Odette Certificate

What you should know about certificates:

Certificates are used in a Public Key Infrastructure, where an asymmetric key pair is used to protect your data and communication. This key pair consists of a private key and a public key. The private key must remain securely on your computer and is not to be given to any other partner (including Odette). The public key is the one you share with your partners. It bears a number of attributes which basically identify the entity to which it belongs.

A certificate is a public key that has been signed by a Certification Authority (CA), a trusted third party entity, indicating that the information on the certificate has been checked and actually represents the entity that is listed as subject of the certificate.

Your partner's system will use the public key to encrypt information to be sent to you and your system will use the private key to decrypt the information. The decryption process can only be done with the private key; therefore your certificate is useless if you do not possess the private key. Similarly, when you send information, your system uses the appropriate public key (certificate) of your partner to encrypt data and your partner uses his/her private key to decrypt the information.

When ordering an Odette Certificate you should follow the steps below.

Step 1: Prepare the information you need for the order process

1. Certificate Attributes

Common Name (recommended: DHN e.g. edi.xyz.com)	
Email Address	
Location (City, Town)	
Country Code (2 alpha ISO Code)	
State or Province (optional)	
Company Name	
Department / Organisational Unit (optional)	
OFTP2 Server's Domain Host Name DHN (e.g. edi.xyz.com)	
IP Address (optional)	
Odette ID (SSID)	

2. Technical Contact

Name	
Company	
Position	
Email	
Address Line 1	
Address Line 2	
City	
Postal Code	
Telephone Number	

3. Invoicing Address

Invoicing address details, if different from technical contact details and VAT Number (mandatory for companies from the EU).

Name	
Company	
Position	
Email	
Address Line 1	
Address Line 2	
City	
Postal Code	
Telephone Number	
VAT Number	

4. Authentication Contact

Note: Odette uses the Authentication Contact to authorise and confirm that the person ordering the certificate (the Technical Contact) is entitled to obtain a certificate on behalf of the company or business unit. The Authentication Contact must work in the organisation where the certificate will be used, must hold a position giving her/him the necessary authority (e.g. head of EDI department, head of IT, managing director ...) to authenticate the request and must have a company email address in his/her own name (generic addresses such as info@..., or admin@...) are not acceptable

Name	
Company	
Position	
Email	
Address Line 1	
Address Line 2	
City	
Postal Code	
Telephone Number	

Step 2: Generate a Certificate Signing Request

You can use any computer with internet access to prepare the CSR and to order the certificate but please note that if you do not use the computer which is deployed as the OFTP2 server you will need to transfer the certificate to this server at the end of the process.

We believe that the easiest way to generate a CSR is to use open SSL¹.

For Windows users we have prepared a toolkit application that provides you an easy way of preparing the CSR.

The application has been successfully tested on Windows 7 and Windows 8, both versions, 32 bit and 64 bit. Pre-conditions are:

- the right to install software on the computer as a local administrator
- the .net framework 3.5 SP1
- access to the web and the ability to download files

If you do not have sufficient rights on the data exchange server you can *use any desktop computer* for the process and once received the certificate you can transfer private key and public key (certificate) as individual files or as PKC#12 keystore file (.pfx).

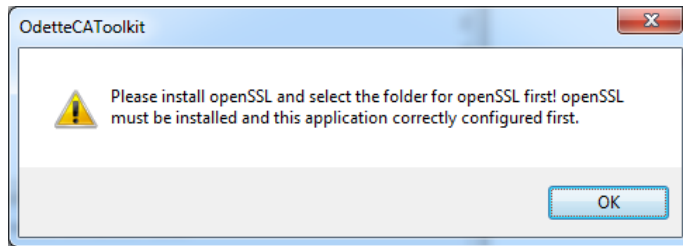
These are the steps to follow:

1. Download Odette CA Tools from [here](http://www.odette.org/repository/odette-ca-tools-win.zip):
<http://www.odette.org/repository/odette-ca-tools-win.zip>
2. Extract the Zip file, preferably to C:\
3. Open the directory with the tools (e.g. C:\Odette-CA-Tools(win)) in Windows explorer.

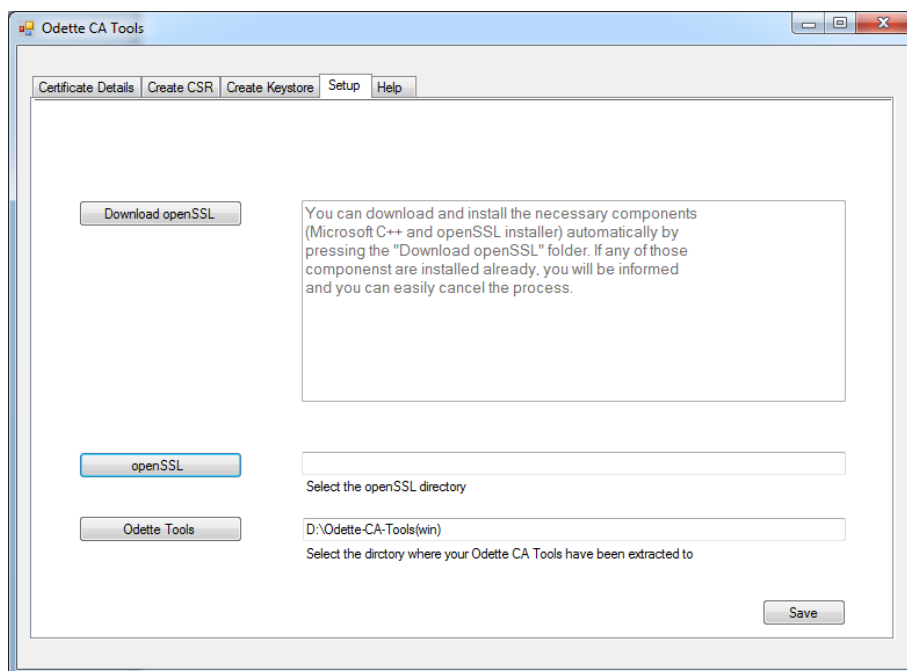
¹ This product includes cryptographic software written by Eric A. Young (eay@cryptsoft.com). This product includes software written by Tim J. Hudson (tjh@cryptsoft.com)

4. Start the programme *OdetteCAToolkit.exe*

Starting the programme for the first time you will see the following notification:

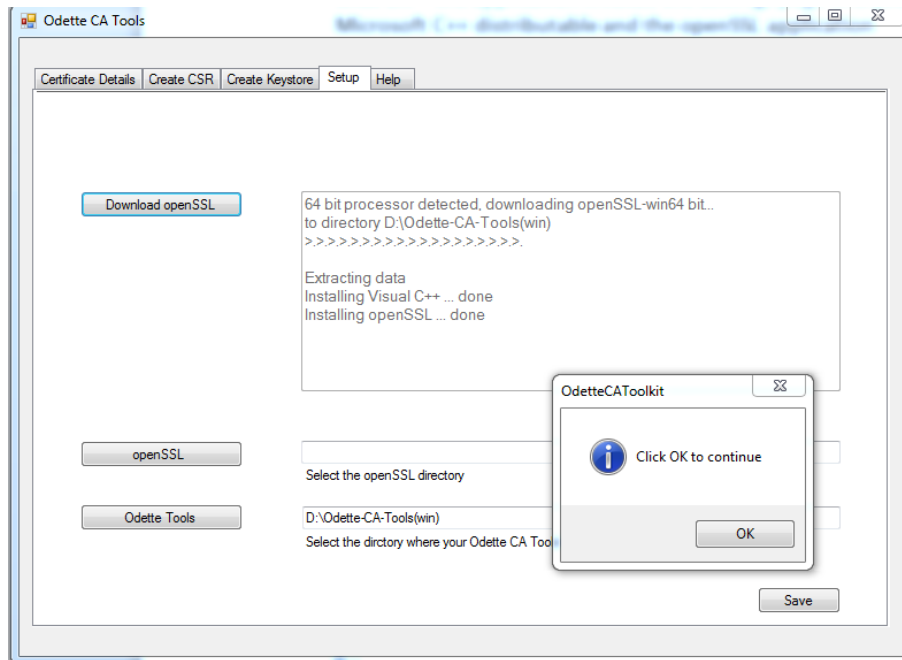


Click OK – the application invokes the *Setup* page and you can download and install the Microsoft C++ distributable and the openssl application



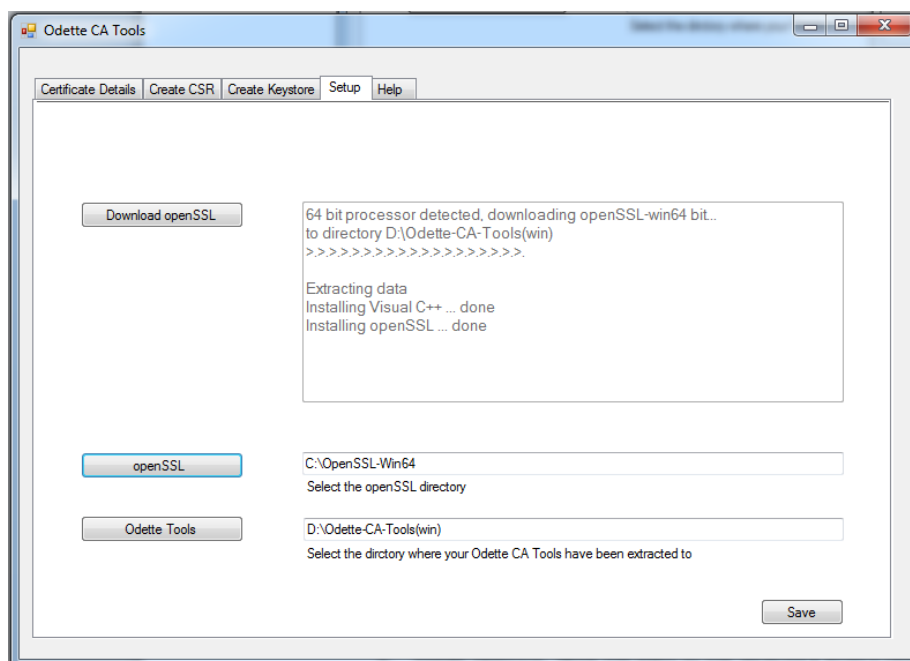
Click the *Download openssl* button and follow the instructions on screen for the installation processes. There will be two separate installations invoked, one for C++ and one for open SSL.

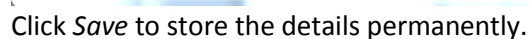
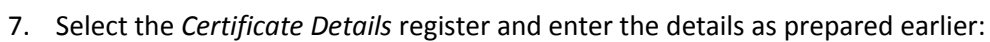
Note down the installation directory of openssl (default is C:\openssl-Win32 or C:\openssl-Win64):



Once you see this information message box the installation of all necessary components has finished.

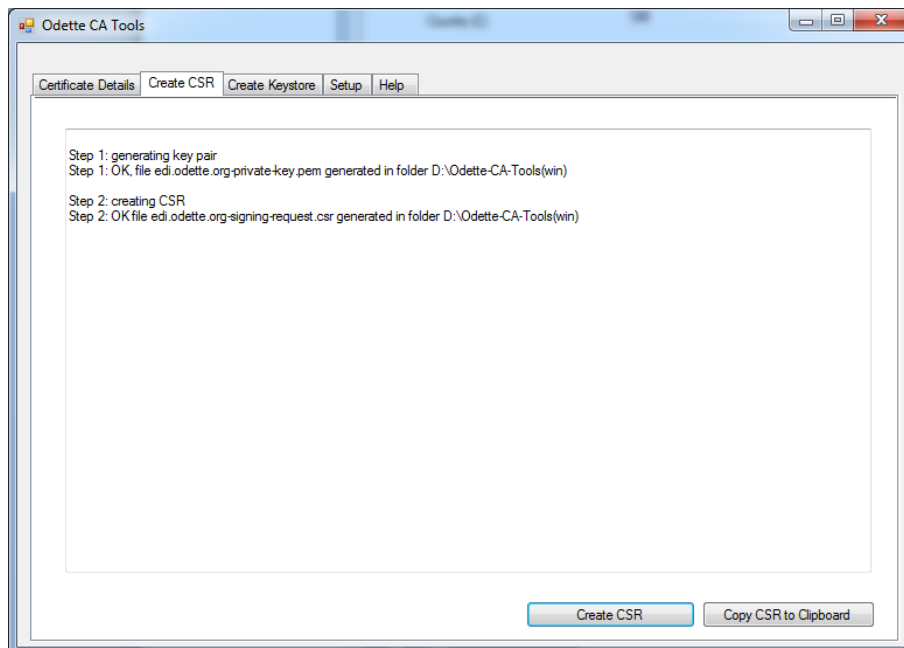
- Click the openssl – button and select the directory where openssl has been installed to (usually C:\OpenSSL-Win32 or C:\OpenSSL-Win64)



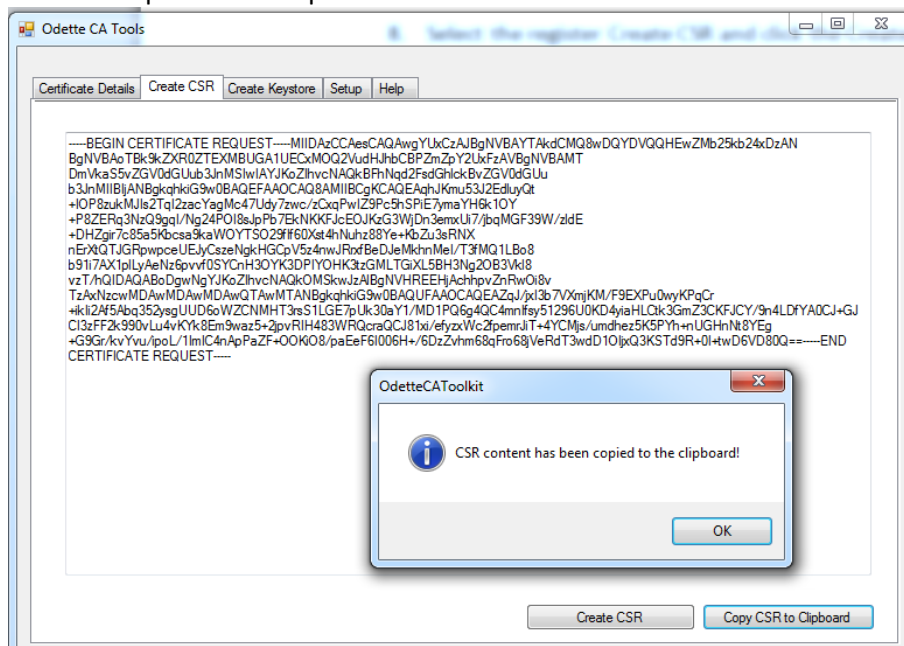


If your Common Name (CN) entry is **not** a domain host name you should tick the box Domain Name in Alternative Subject and provide the domain name here.

8. Select the register Create CSR and click the Create CSR button



9. Press *Copy CSR to Clipboard* – the content will be displayed in the application and copied to the clipboard as well.



If you prefer to use a different tool for creating the CSR, such as Portecle or Keystore Explorer, please refer to these videos:

- [Portecle \(German\)](#)
- [Keystore Explorer \(English\)](#)

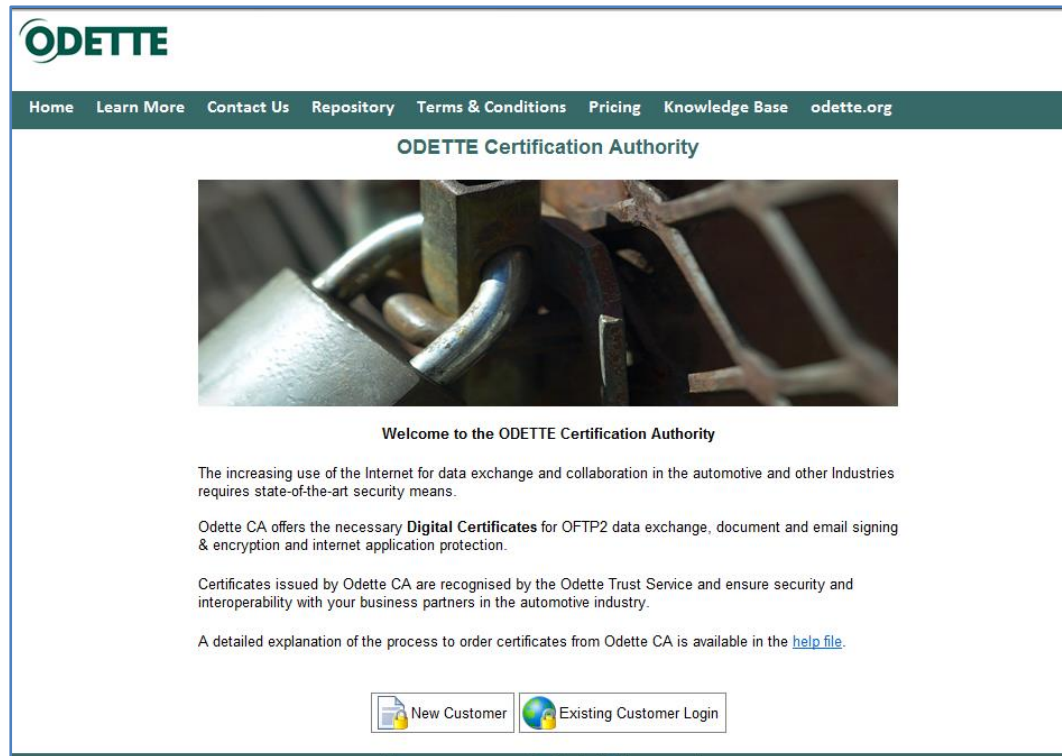
Carry on as described in the next chapter

Note:

If you cannot use the OdetteCAToolkit described above you may use various batch files instead. For detailed instructions please refer to [Annexe Part 3 How to create a CSR with batch files](#)

Log on to the Odette CA and start the order process

Log on to the Odette CA web site via <https://www.odetteca.com>



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

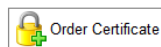
If you are ordering a certificate for the first time, please carefully read the [help file](#) which explains the individual steps of the ordering process.

Preliminary Steps

Due to the increasing complexity of making changes to the various security settings in the different Windows OS environments we have decided to no longer offer customers the option of creating their key pair and Certificate Signing Request (CSR) during the certificate order process.

This means that before ordering or renewing a certificate via this website you will need to create your key pair and CSR with a third party tool, such as openssl, Keystore Explorer or Portecle. You can find detailed instructions on how to create a CSR [here](#).

When you have created your CSR and have it available as a text file, please click the button below to start the certificate order process.



© 2013 ODETTE International Ltd. All rights reserved.
[Privacy Policy](#) | [Cookie Usage](#) | [Terms of Use](#)

Click on *Order Certificate*

You will be prompted to enter the details of the technical contact, who will also be the registered user of the CA website.

Technical Contact Details

Authentication Contact Details

Import CSR

CSR Validation

Order Details

Payment Details

Order Summary

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	* Programme Manager
Email	* jwalther@odette.org
Address Line 1	* 71 Great Peter Street
Address Line 2	
City	* London
Postal Code	* SW1P 2BN
Country	* United Kingdom
Telephone Number	* 0044 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	* 



© 2013 ODETTE International Ltd. All rights reserved.
[Privacy Policy](#) | [Cookie Usage](#) | [Terms of Use](#)

Home Learn More Contact Us Repository Terms & Conditions Pricing Knowledge Base odette.org
--

Technical Contact Details

Authentication Contact Details

Import CSR

CSR Validation

Order Details

Payment Details

Order Summary

Authentication Contact Details

Previous

Next

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 of the certificate 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 requester and the Authentication Contact appear to be the same person.

The Authentication Contact must:

1. Be someone other than the person creating the order.
2. Be employed by the organisation for which the certificate is intended.
3. Hold a position which is able to authenticate and authorise the order made by the requester.
4. Have a company email address in their own name.

Name	* John Carvin
Company	* Odette International
Position	* Managing Director
Email	* jcarvin@odette.org
Address Line 1	* 71 Great Peter Street
Address Line 2	
City	* London
Postal Code	* SW1P 2BN
Country	* United Kingdom
Telephone Number	* +44 20 7344 9220

Previous

Next

©2013 ODETTE International Ltd. All rights reserved.
[Privacy Policy](#) | [Cookie Usage](#) | [Terms of Use](#)

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:

- Belong to the organisation for which the certificate is intended
- Be in a position to authorise the certificate order
- Have a company email address in their own name
- Be a different person from the Technical Contact.

Click 'Next' to continue to the Import CSR Page.

- Technical Contact Details
- Authentication Contact Details
- Import CSR
- CSR Validation
- Order Details
- Payment Details
- Order Summary

Import CSR

Previous   Next

Import Certificate Signing Request

Example CSR:

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

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDDTCCAQECCAQwYwECCABG9NBAYTAkdCMQ8wDQYDVQQHDAZMb25kb24xZDZANBgNVBAoMBk9kZXR0ZTEuY290dGUub3JnMSIwIAYJKoZIhvcNAQkBFhNqd2FsdGh1ckBvZGV0dGUu
b3JnMIBIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr4Q+Hj kNPVYRv1S7
+y0kLPSAfdGIC1JhNmMaAY8OMxmhm09aTyWVzVwTwtpJseWFn3gfF9PZLEVOWB4
Ld2cW1XoOZzOKmoTvDKHfYsQ1gNtcC1Jz1yYz8z7Us+AP6uo4gXVz18ufQ+1jR
KVpUVZw824MIUaBBUG2rBTGC/ qsrjpcqRoZ9fMT0GoZ/ OFf1ibddmx+xERBrq6+D
ntNZpI3k6/pW17sQ3SOLay+A4MarfpoknGcKHApfdmDtc3PH5WMnM5hwfs+zjgQ
dXFGqfTjTo3dM7ZUm59CYjNU3a5kDioxVdWkto5+RRIzDRDJVSKTOn4YYyTl+9+R
wY6UWIDAQABoAAADQYJKoZIhvcNAQEFBQADggEBAGjP1IIRrbhxJ9VI+hyu7BZW
0x1oNbIpFhqnHJwx79xD1TChc1mOcQ5XmdsorFy7UzV+fW6p5dFfmPzK5s5WoU
PdCj d0mJ71bvHej9opd9fk6H/LEM1P2db1RRc/R1D9qXJcwremy/UZ6DD3qB/yA
j7CBbOPK7hGH0FCDNmOycaIq1gR3mL0QRRRRMpdPcJH0FPP+RpPchXwZyXWY1LJE
WwWuS5pMUZSSSuk8K6FKG16/n4gcVH8jEqbf7dm5X/bIX+C5Rh7o4Gt7w+6uN1F
GzG1CBpJMpjcM5tBUCXxn+femJUcl1fTNRQOpdM8gz1XNaFkH80Lx2Q1kKVCf0=
-----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.

```
-----BEGIN CERTIFICATE REQUEST-----
MIICyzCCABMCAQAwYUxkZAJBgNVBAYTAkdCMQ8wDQYDVQQHDAZMb25kb24xZDZANBgNVBAoMBk9kZXR0ZTEuY290dGUub3JnMSIwIAYJKoZIhvcNAQkBFhNqd2FsdGh1ckBvZGV0dGUu
b3JnMIBIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAr4Q+Hj kNPVYRv1S7
+y0kLPSAfdGIC1JhNmMaAY8OMxmhm09aTyWVzVwTwtpJseWFn3gfF9PZLEVOWB4
Ld2cW1XoOZzOKmoTvDKHfYsQ1gNtcC1Jz1yYz8z7Us+AP6uo4gXVz18ufQ+1jR
KVpUVZw824MIUaBBUG2rBTGC/ qsrjpcqRoZ9fMT0GoZ/ OFf1ibddmx+xERBrq6+D
ntNZpI3k6/pW17sQ3SOLay+A4MarfpoknGcKHApfdmDtc3PH5WMnM5hwfs+zjgQ
dXFGqfTjTo3dM7ZUm59CYjNU3a5kDioxVdWkto5+RRIzDRDJVSKTOn4YYyTl+9+R
wY6UWIDAQABoAAADQYJKoZIhvcNAQEFBQADggEBAGjP1IIRrbhxJ9VI+hyu7BZW
0x1oNbIpFhqnHJwx79xD1TChc1mOcQ5XmdsorFy7UzV+fW6p5dFfmPzK5s5WoU
PdCj d0mJ71bvHej9opd9fk6H/LEM1P2db1RRc/R1D9qXJcwremy/UZ6DD3qB/yA
j7CBbOPK7hGH0FCDNmOycaIq1gR3mL0QRRRRMpdPcJH0FPP+RpPchXwZyXWY1LJE
WwWuS5pMUZSSSuk8K6FKG16/n4gcVH8jEqbf7dm5X/bIX+C5Rh7o4Gt7w+6uN1F
GzG1CBpJMpjcM5tBUCXxn+femJUcl1fTNRQOpdM8gz1XNaFkH80Lx2Q1kKVCf0=
-----END CERTIFICATE REQUEST-----
```

Previous   Next

If you have created a key pair and a corresponding CSR with the Odette CA Toolkit application you can simply copy the CSR content from the application to the clipboard and paste it into this form.

If you used a different tool or the manual (Batch) process you should open the CSR text file and copy the content into the corresponding space in the Odette CA application.

Click 'Next' to continue to the CSR Validation Page.

Certificate Usage

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

- | | |
|--|-------------------------------------|
| <input checked="" type="checkbox"/> Show Usage Attributes | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Secure Session (SSL/TLS) | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Email | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Encryption | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> File Signing | <input checked="" type="checkbox"/> |

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.

- | | |
|---|---------------------------|
| <input checked="" type="checkbox"/> Company Name | Odette International Ltd. |
| <input checked="" type="checkbox"/> Location | London |
| <input checked="" type="checkbox"/> Country | GB |
| <input checked="" type="checkbox"/> Email Address | jwalthers@odette.org |
| <input checked="" type="checkbox"/> Organisation Unit | Central Office |
| <input checked="" type="checkbox"/> Common Name | Odette EDI Server |
| <input checked="" type="checkbox"/> Hostname | edi.odette.org |
| <input checked="" type="checkbox"/> OFTP ID (SSID) | oftp://00177000000000A001 |

Previous

Next

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 Details


Check that all your certificate details are correctly submitted. If anything is incorrect, you will need to create a correct CSR and import the CSR once again. 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). This qualified domain name must be shown in the attribute 'Common Name'.

If your CSR does not already contain a SSID for OFTP2 and you intend to use the certificate for OFTP2 data exchange, you should now enter your SSID (aka OFTP ID or Odette ID).

Click 'Next' to continue.

On this page you select the desired validity period of the certificate (1, 2, 3 or 4 years).

Before continuing, you must also accept the Odette CA terms and conditions.


[Home](#)
[Learn More](#)
[Contact Us](#)
[Repository](#)
[Terms & Conditions](#)
[Pricing](#)
[Knowledge Base](#)
[odette.org](#)
[Control Panel](#)

Technical Contact Details

Authentication Contact Details

Import CSR

CSR Validation

Order Details

Payment Details

Order Summary

Order Details

Previous

Next

Certificate Validity Period

Please select the validity period for this certificate.

Validity Period	* 1 Year	
Promotion Code	1 Year	
Total Cost	2 Years	
Promotional Discount	3 Years	Price Exclusive of VAT)
Balance To Pay	4 Years	Price Exclusive of VAT)
		€ 180.00 (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 * ☒

Previous

Next

© 2014 ODETTE International Ltd. All rights reserved.
[Privacy Policy](#) | [Cookie Usage](#) | [Terms of Use](#)

Click *Next* to continue.

Purchase Order: You need to enter an order reference which will be included in 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).

<ul style="list-style-type: none"> Technical Contact Details Authentication Contact Details Import CSR CSR Validation Order Details Payment Details Order Summary 	<h2>Payment Details</h2> <div> Previous Next </div> <h3>Purchase Order Number</h3> <p>Please enter a purchase order number below, this will be displayed on your invoice.</p> <p>Purchase Order Number * PO20140728</p> <h3>Invoicee Address</h3> <p>Please enter an invoicee address if different from Technical Contact address.</p> <p> <input type="checkbox"/> Bill to different address </p> <p> Name * Jörg Walther Company * Odette Email * jwalther@odette.org Address Line 1 * 71 Great Peter Street Address Line 2 City * London Postal Code * SW1P 2BN Country * United Kingdom <input checked="" type="checkbox"/> Telephone Number +44 776 9264 784 </p> <h3>Tax Details</h3> <p>Customers with an invoicee address in a European Union Member State must provide a VAT number including the national prefix e.g. GB123456789</p> <p>VAT Number * GB774159013</p>
---	---

Click *Next* to continue.

Order Summary

[Previous](#)

[Complete Order](#)

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

Email	jwalther@odette.org
Location	London
Country	GB
Organisation	Odette International Ltd.
Department	Central Office
Hostname	edi.odette.org
OFTP2 ID (SSID)	oftp://O0177000000000A001
Common Name	Odette EDI Server

Purchasing Details

Validity Period	1 Year
VAT Number	GB774159013
Promotional Discount	€ 0.00
Net Amount	€ 180.00
VAT Amount	€ 36.00
Total	€ 216.00

Technical Contact Details

Name	Jörg Walther
Company	Odette
Position	PM
Email	jwalther@odette.org
Address	71 Great Peter Street, London, SW1P 2BN, United Kingdom
Telephone	+44 776 9264 784

Authentication Contact Details

Name	John Canvin
Company	Odette

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

Order Completed


[Control Panel](#)

[Print Summary](#)

[Exit](#)

Thank you for your purchase. An order confirmation email has been sent to 'jwalther@odette.org'. Your unique certificate order number is: 4538. 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 receive an email with instructions for downloading and installing your certificate.

Order Summary

Certificate Details

Order Number	4538
Email	jwalther@odette.org
Location	London
Country	United Kingdom
Organisation	Odette International Ltd.
Department	Central Office
Common Name	Odette EDI Server
Hostname	edi.odette.org
OFTP2 ID (SSID)	oftp://O0177000000000A001

Purchasing Details

Validity Period	1 Year
VAT Number	GB774159013
Promotional Discount	€ 0.00
Net Amount	€ 180.00
VAT Amount	€ 36.00
Total	€ 216.00

Technical Contact Details

Name	Jörg Walther
Company	Odette

We recommend to print the order summary and to keep it in your files. You will need this information when you have to renew your certificate at the end of the validity period.

When you click on the Control Panel button, you can logon yourself onto the application using the email and password you have selected during the registration process and you will find your certificates / requests there.



Certificate Control Panel


[My Account](#)

[Logout](#)

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.


[Purchase New Certificate](#)

Certificate ID	Common Name	Status	Certificate Requested	Order Number	Expiry Date	Details	Download	Renew	Revoke
4509	Odette EDI Server	Pending 	28/07/2014 12:46:28	4538					



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: 4538. 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: <https://www.odetteca.com>

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

Certificate Details:

...

Validation and approval process

Shortly after the order has been made, the Odette CA will start the validation process which is based on the Odette CA Certificate Policy.

The Odette CA Registration Authority will validate the information provided in the CSR. Furthermore your authentication contact will receive documents to be signed and returned in order to approve your request and initiate the issuing process. Usually, the return of these documents determines how long it takes to issue the certificate.

Upon approval of the request, the certificate will be issued and you will receive information via email:

Dear [user name],

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

An invoice has been attached to this email. If payment is not received within 30 days of 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>

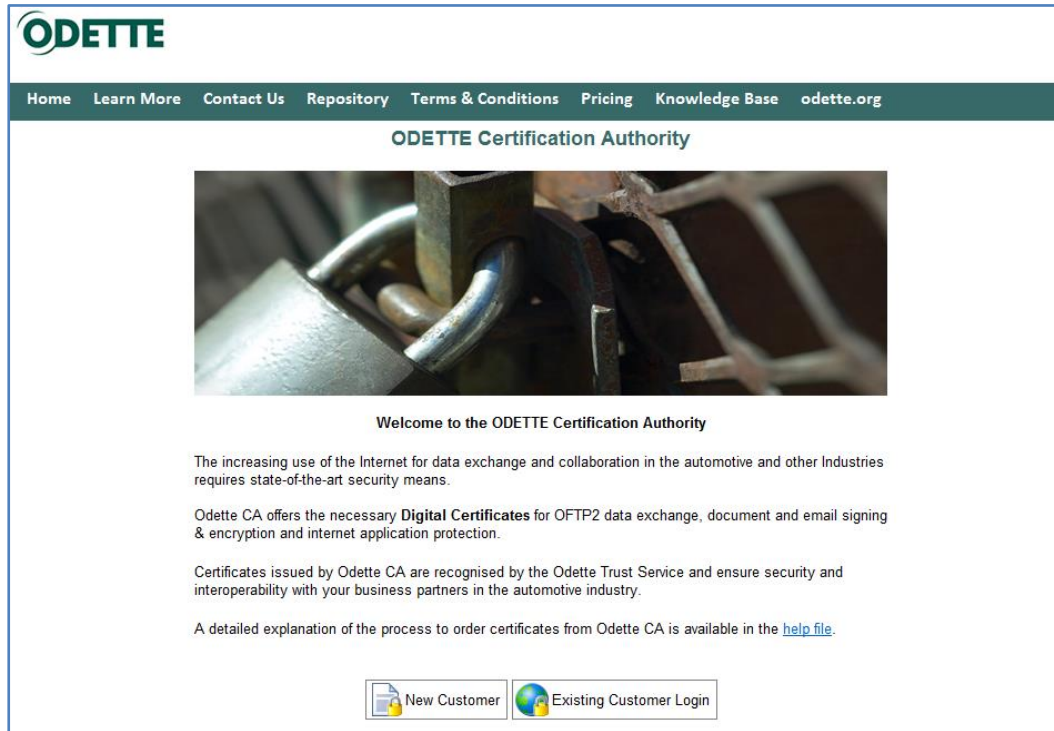
Thank you for choosing ODETTE.

~~~~~

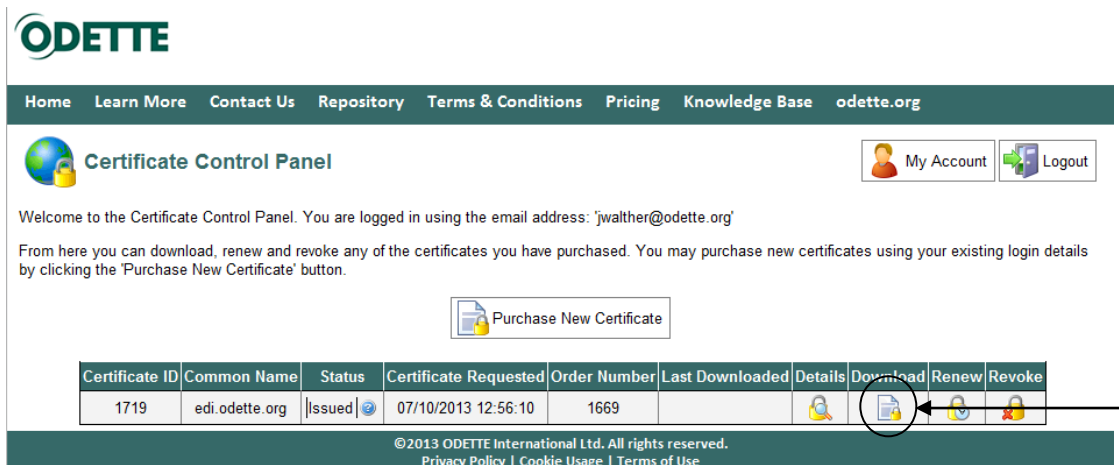
The invoice (pdf) for the certificate will be attached to this email.

## Download the certificate

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



The control panel will show your certificates and their status.



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

Further details on installation of Odette certificates can be found in [Annexe 1](#).

## *Renew a certificate*

### Important Note:

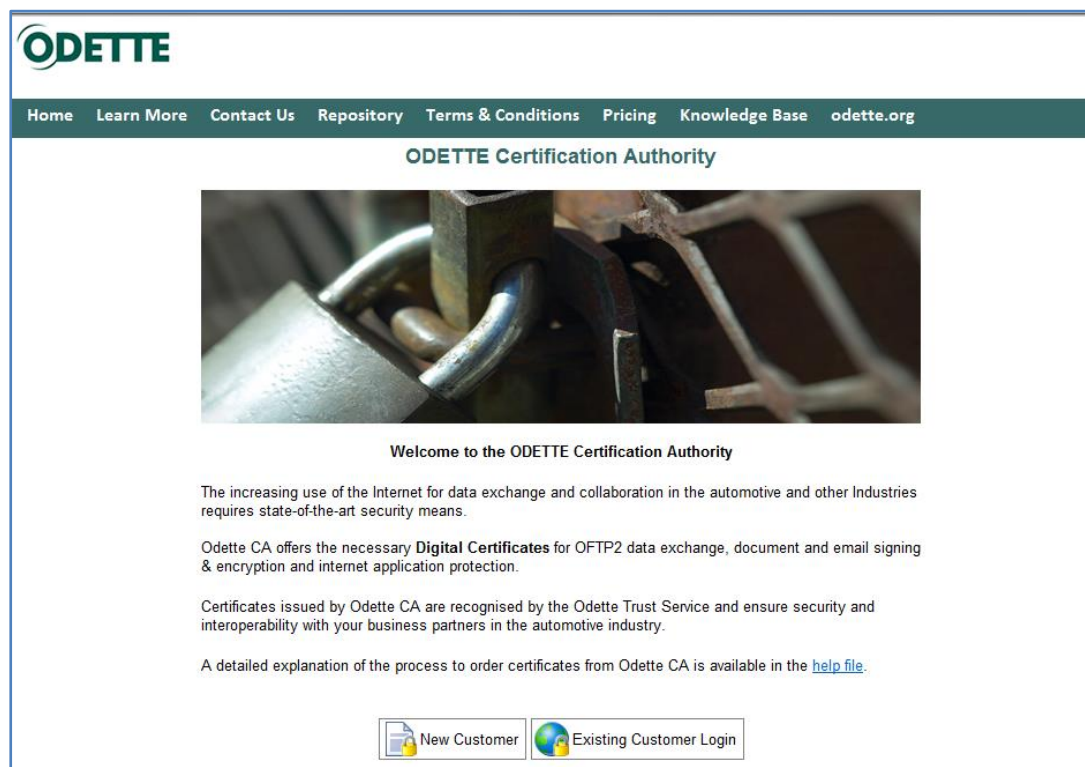
In the environment of the Odette CA *renewal* means to issue a new certificate with the same properties as the previous one. However, to protect your privacy also a renewed certificate requires a new private and public key.

Some OFTP2 software systems use their own key store and are programmed in a way that they only accept a renewed certificate if it refers to the existing private key. In these systems you cannot use the renewal process as described here; instead you must install a **new certificate** when the existing one expires or becomes invalid.

Prepare a new Certificate Signing Request as described in chapter [Generate a Certificate Signing Request](#).

Log into the Odette CA application under <https://www.odetteca.com>.

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



### **Important Note**

Before starting the Renew process, please ensure that your *user details* are correct and up to date. These details will be used as the Technical Contact details for the Certificate Order and cannot be amended during the *Renew* process.

You can check and update your User details by going to the 'My Account' page from your Certificate Control Panel.



## Certificate Control Panel














[My Account](#)

[Logout](#)

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.


[Purchase New Certificate](#)

| Certificate ID | Common Name      | Status     | Certificate Requested | Order Number | Last Downloaded     | Details                                                                             | Download                                                                            | Renew                                                                               | Revoke                                                                              |
|----------------|------------------|------------|-----------------------|--------------|---------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| 3854           | edi3.odette.org  | Downloaded | 22/12/2013 17:04:43   | 3839         | 22/12/2013 17:21:01 |  |  |  |  |
| 1626           | oftp2.odette.org | Downloaded | 09/01/2012 13:35:13   | 1586         | 03/01/2014 08:02:00 |  |  |  |  |
| 1250           | OFTP2 Odette     | Revoked    | 04/08/2011 11:20:05   | 1206         | 04/08/2011 12:52:38 |  |  |  |  |

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.

The portal application will show you the details of your existing certificate. Before you can continue, you must prepare a matching CSR (see Step 2: Generate a Certificate Signing Request).

The Odette CA will check that the new certificate request's attribute values match the existing certificate.

The further process matches the order process (see [here](#) ).

You will receive a confirmation email.

Dear [user name],

Thank you for renewing your existing ODETTE digital certificate.

Your unique certificate order number is: 3845 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>

Should you have any queries of problems please email us at [odetteca@odette.org](mailto:odetteca@odette.org)

### Certificate Details:

\*\*\*\*\*

Order Type: Renewal  
 Certificate Type: Unknown  
 Location: London  
 Country: United Kingdom  
 Organisation: Odette International Ltd  
 Department: CO  
 Common Name: oftp2.odette.org  
 Domain Name/IP Address: oftp2.odette.org  
 OFTP2 ID (SSID): oftp://00177000000000A001000000

### Purchasing Details:

\*\*\*\*\*

...

After re-validating the information provided in the CSR the Odette CA will issue the renewed certificate.

## Annexes

[Part 1 How to download and install the certificate on your local computer](#)

[Part 2 How to find your certificate in the Windows keystore after installation.](#)

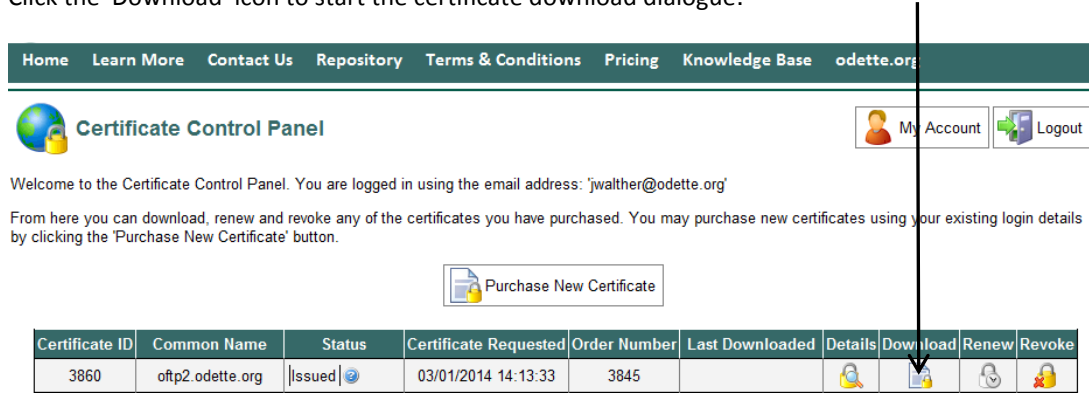
[Part 3 How to create a CSR with batch files](#)

## 1. How to download and install the certificate on your local computer

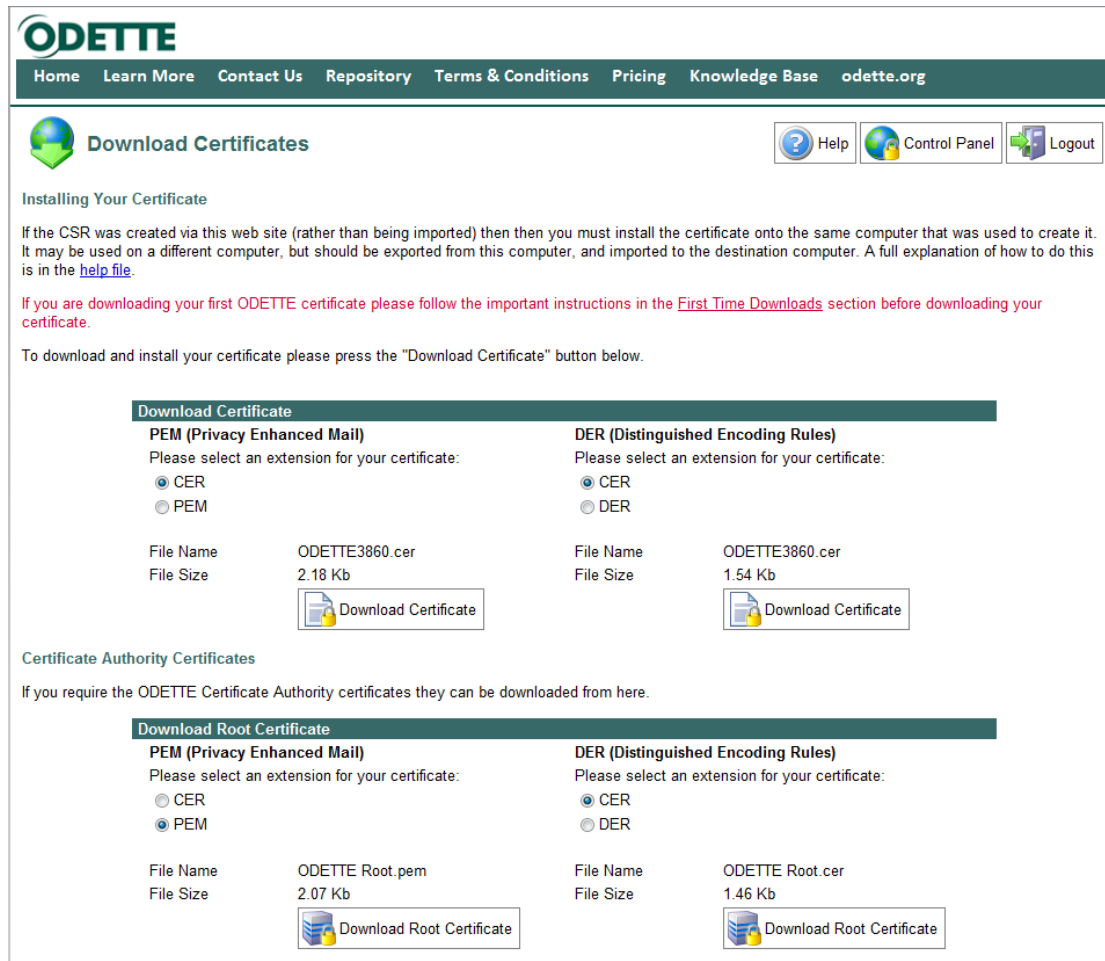
This section provides instructions for users who are downloading and installing a certificate for the first time. The example is for Microsoft Windows. Please follow the instructions relevant to your operating system.

Log into the CA application.

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



| Certificate ID | Common Name      | Status | Certificate Requested | Order Number | Last Downloaded | Details | Download | Renew | Revoke |
|----------------|------------------|--------|-----------------------|--------------|-----------------|---------|----------|-------|--------|
| 3860           | oftp2.odette.org | Issued | 03/01/2014 14:13:33   | 3845         |                 |         |          |       |        |



**Download Certificate**

**PEM (Privacy Enhanced Mail)**  
Please select an extension for your certificate:  
☒ CER  
☐ PEM

File Name: ODETTE3860.cer  
File Size: 2.18 Kb  
[Download Certificate](#)

**DER (Distinguished Encoding Rules)**  
Please select an extension for your certificate:  
☒ CER  
☐ DER

File Name: ODETTE3860.cer  
File Size: 1.54 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.pem  
File Size: 2.07 Kb  
[Download Root Certificate](#)

**DER (Distinguished Encoding Rules)**  
Please select an extension for your certificate:  
☒ CER  
☐ DER

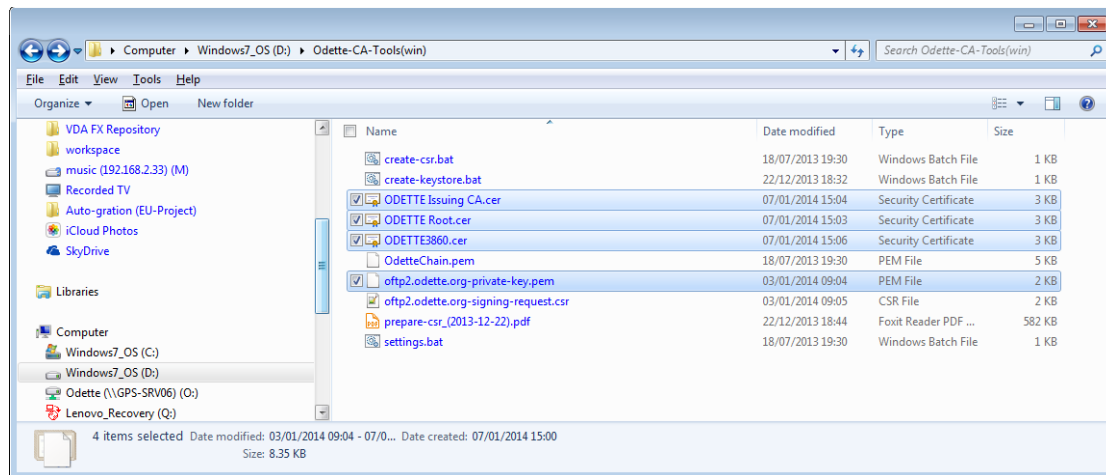
File Name: ODETTE Root.cer  
File Size: 1.46 Kb  
[Download Root Certificate](#)



You can select between two different formats and two 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. **Usually, the PEM format with CER extension should work.**

Store the certificate into the folder where you have your private key, most likely **C:\Odette-CA-Tools(win)**.

If your OFTP2 solution requires individual files for the Root CA, Issuing CA, Public Key and Private Key, then import these files from the above mentioned directory.



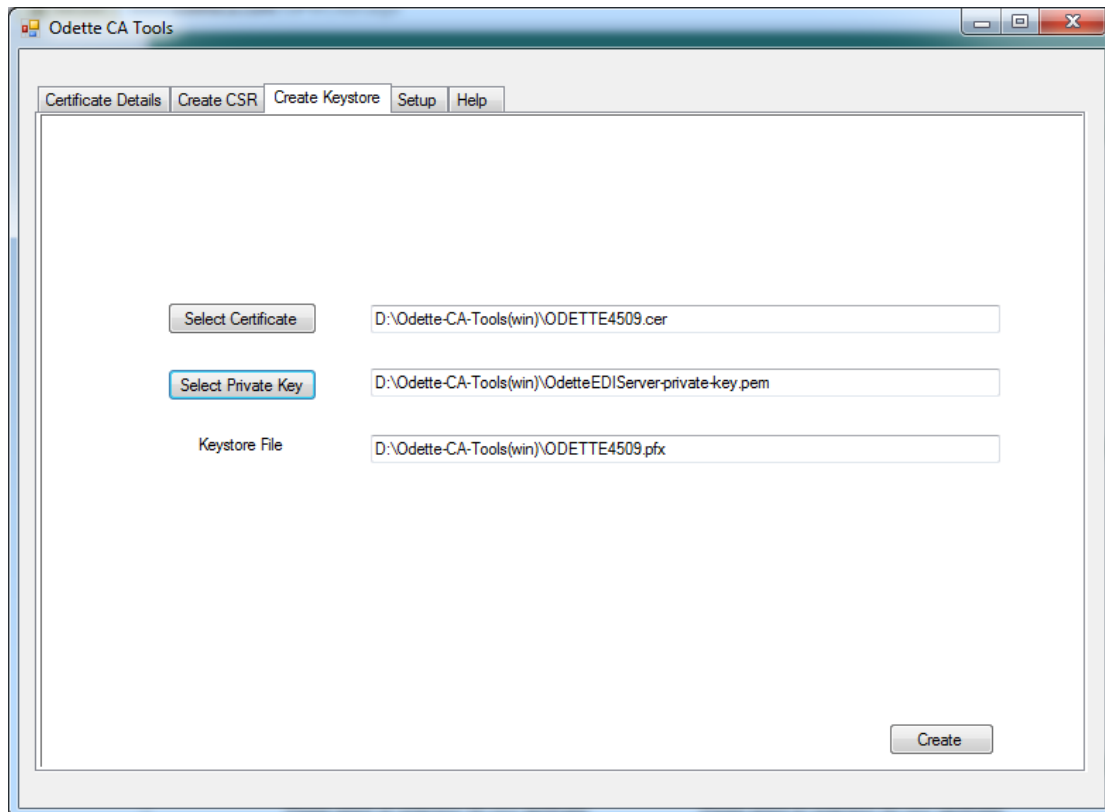
If your OFTP2 software requires a keystore file or uses the Windows keystore continue with the following steps:

#### 1. Create a keystore file

Start the OdetteCAToolkit.exe in the Odette-CA-Tools(win) folder

Select the *Create Keystore* register.

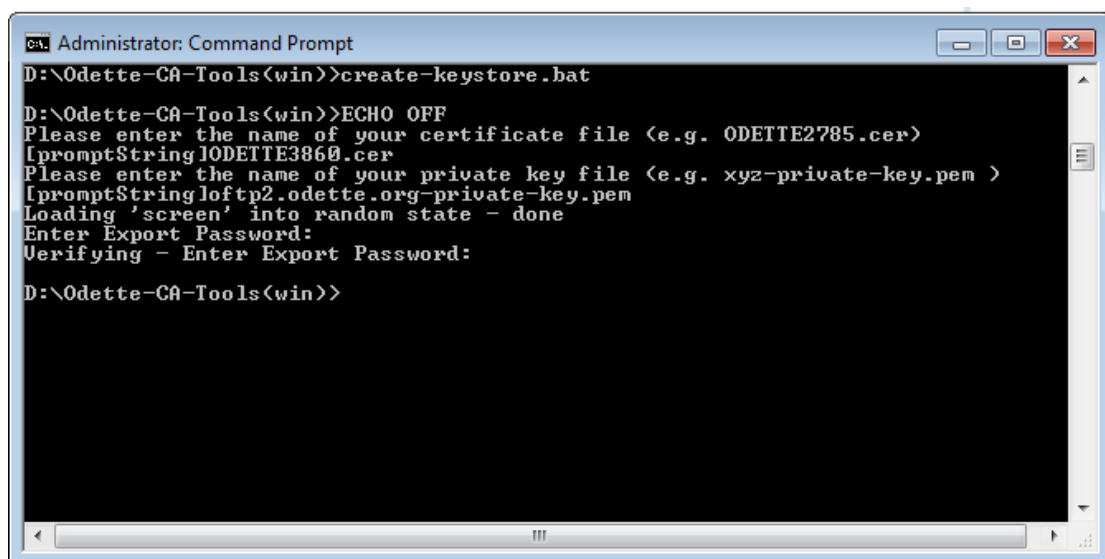
Use the buttons to select the (downloaded) certificate file and the private key file that was generated in conjunction with the creation of the CSR.



The resulting keystore file name will be generated automatically.  
Press *Create* and the application will generate the .pfx file.

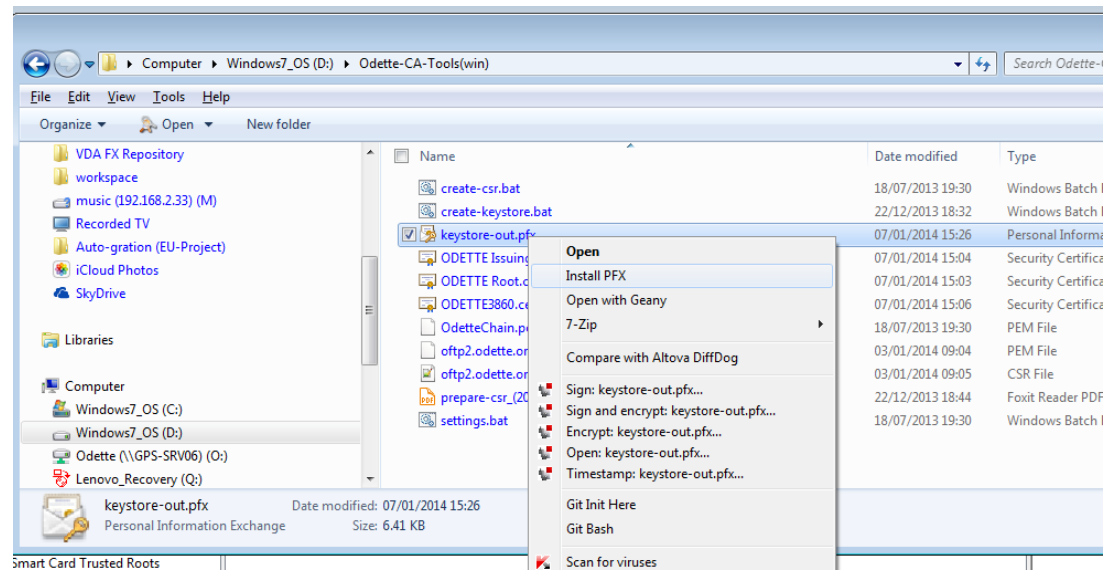
If you cannot use the OdetteCAToolkit application you can start the command line interface as administrator (Start/All Programs/Accessories/Command Prompt – right mouse button, run as Administrator), navigate to the folder with the certificates (e.g. **cd C:\Odette-CA-Tools(win)**) and run the **create-keystore.bat** command.

Enter the file name of your certificate and of the private key file when prompted. Assign a password to the resulting keystore file so that it is protected against un-authorised use.



The process will create a file with the **extension .pfx** (the batch process: keystore-out.pfx) which can be imported into the Windows or your application's keystore.

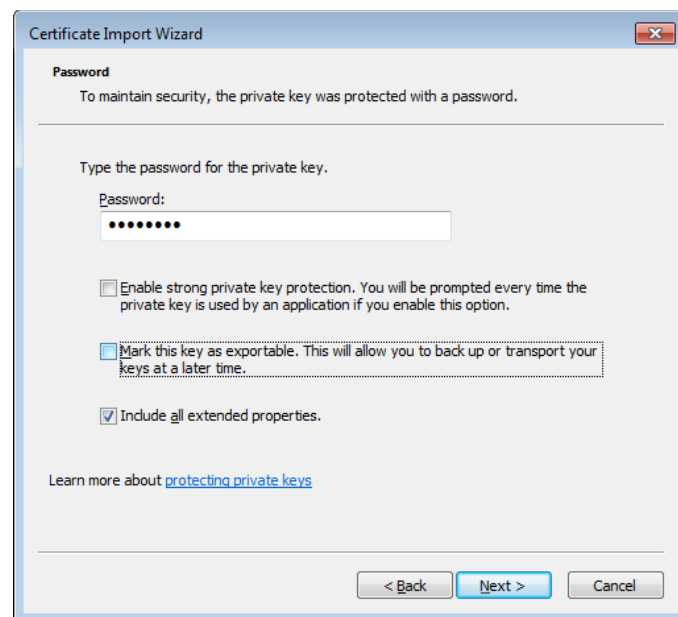
For Windows, click the right mouse button and select install PFX from the context menu.

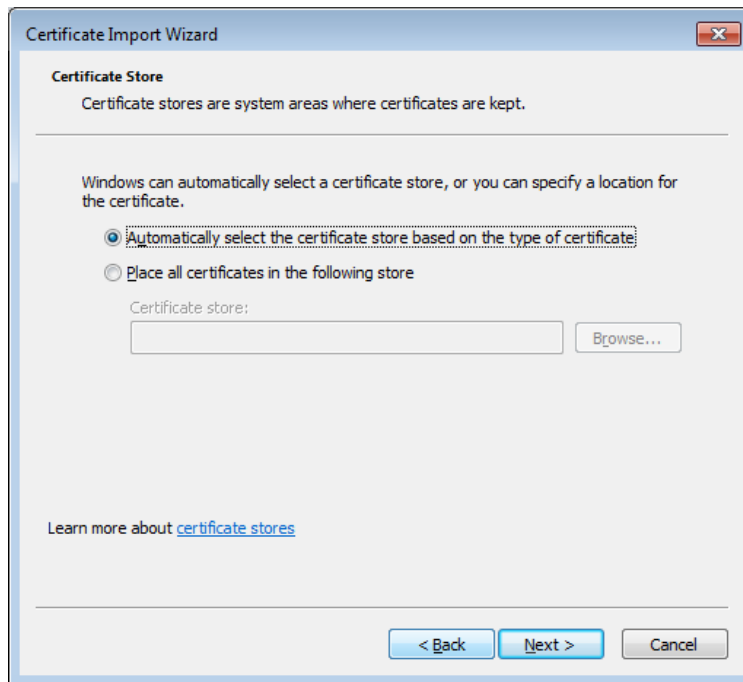


Follow the installation process.

Do not tick the first option (Enable strong private key protection).

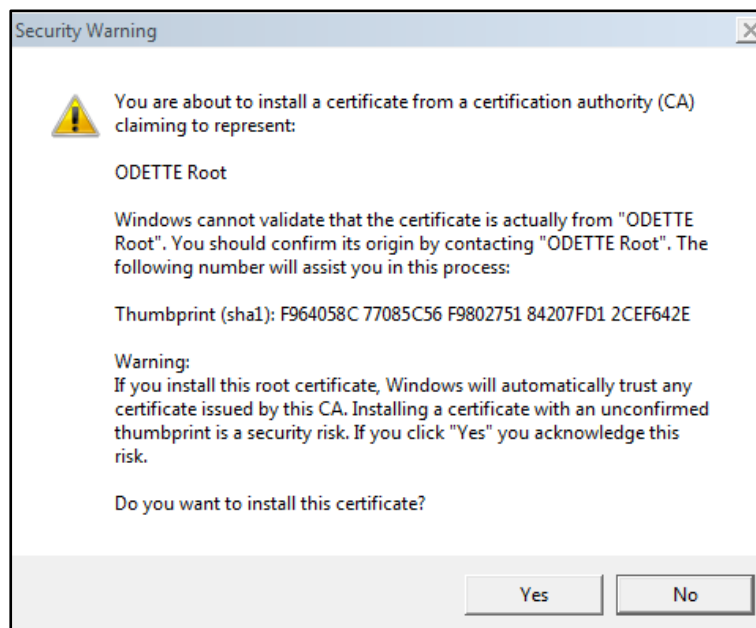
Tick the second option (Mark key as exportable) at your own discretion.





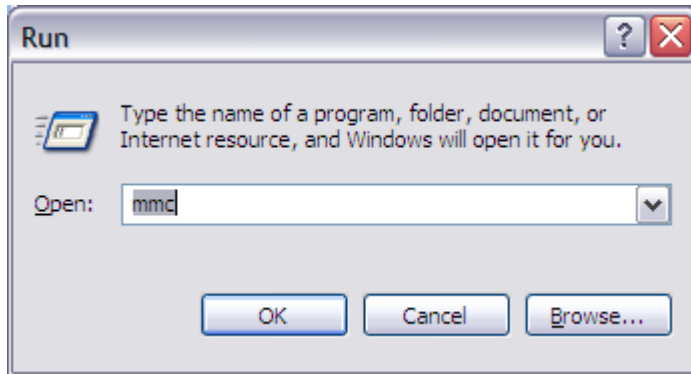
We recommend to use the automatic selection as shown above.

When prompted with this warning, confirm with **Yes**.

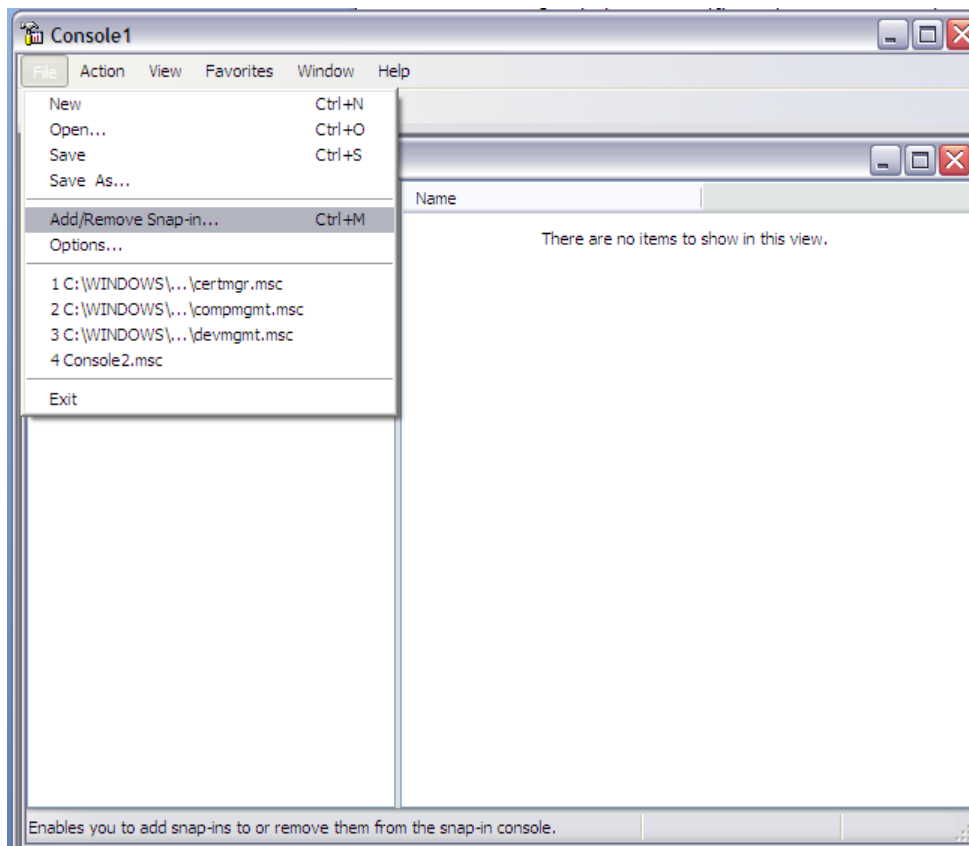


## 2. How to find your certificate in the Windows keystore after installation

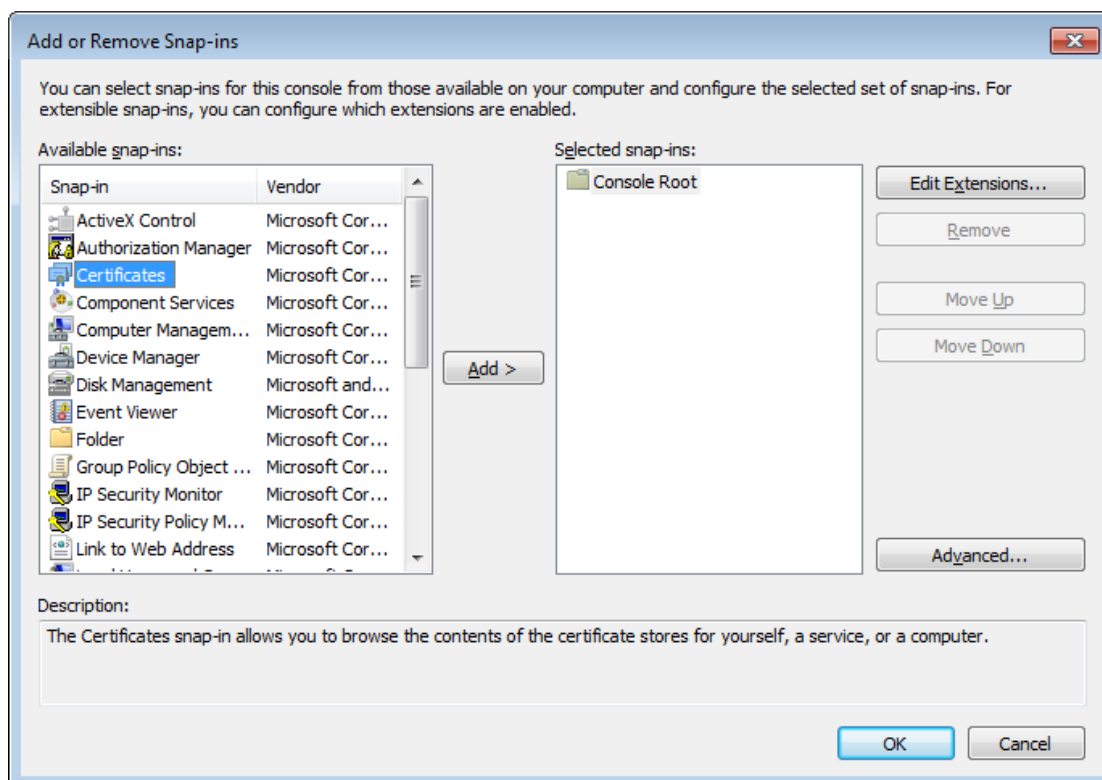
1. Click *Start* and type “mmc” in the entry field. Click *OK*



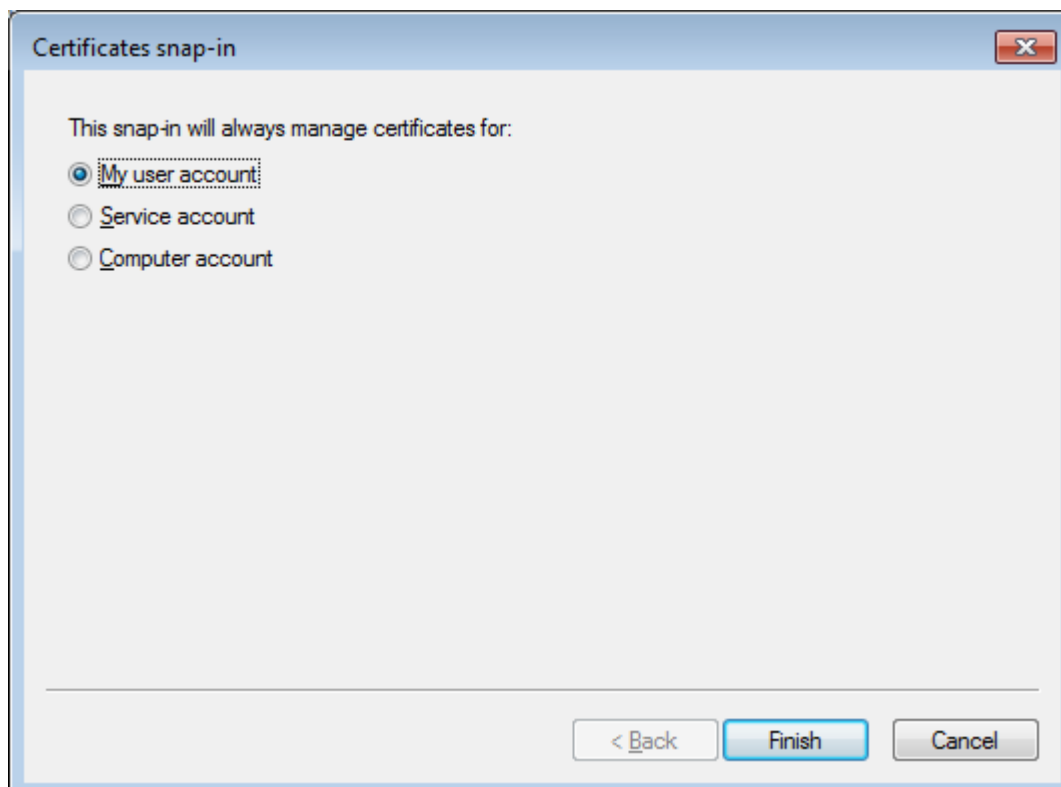
2. The Console will open. Select *File/Add Remove Snap-in*



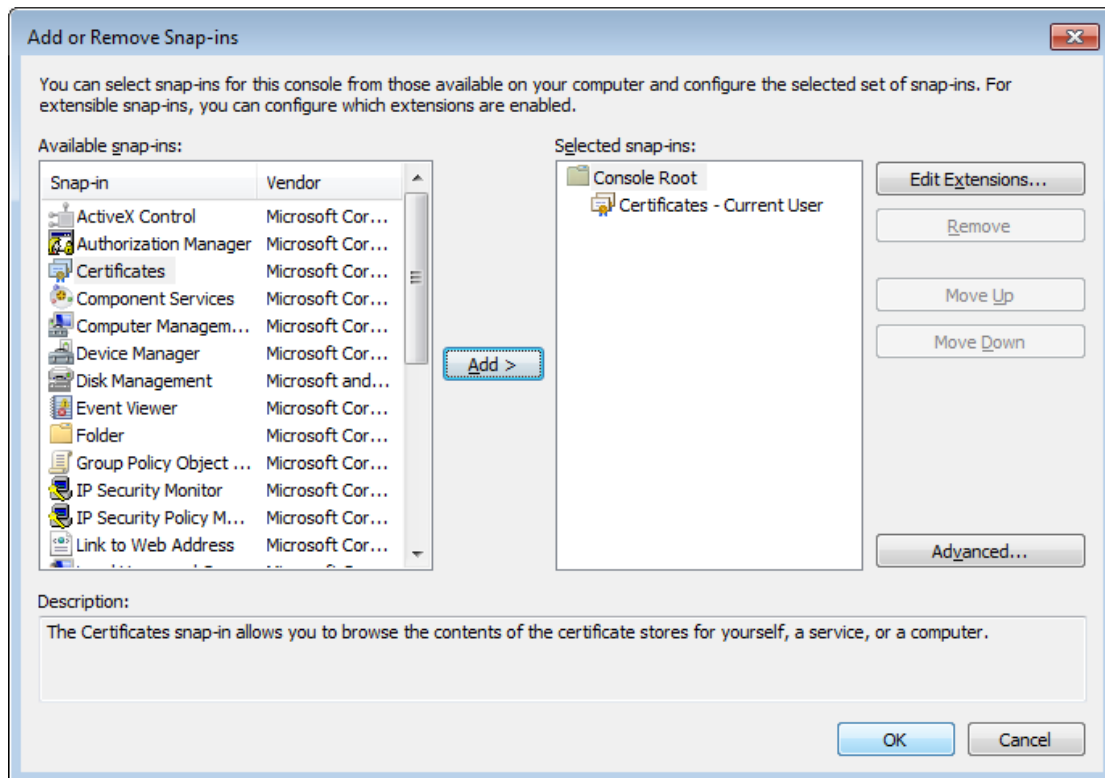
3. Click *Add* and select **Certificates** from the list. Click *Add* again.



- For Windows7 you will usually have to select ***"My user account"***



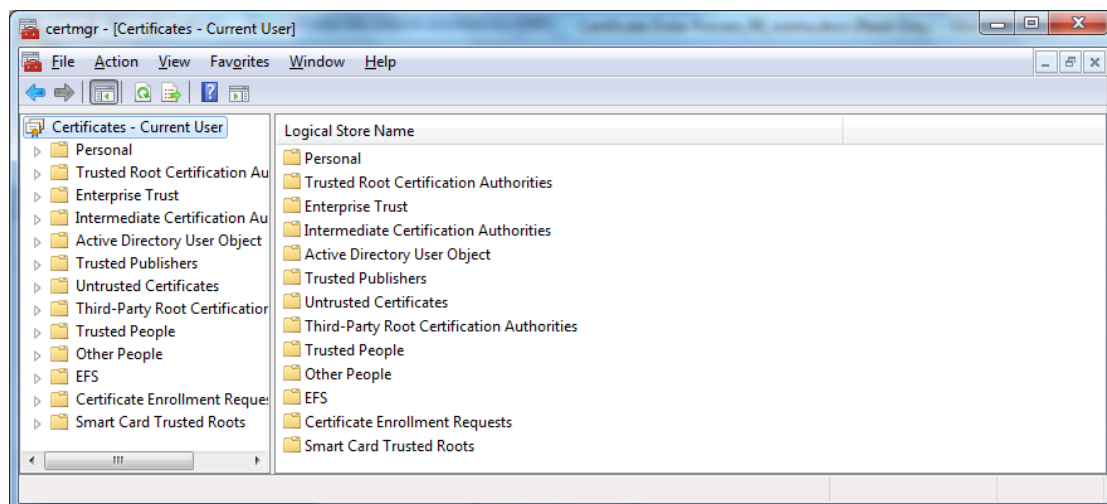
5. Click OK.



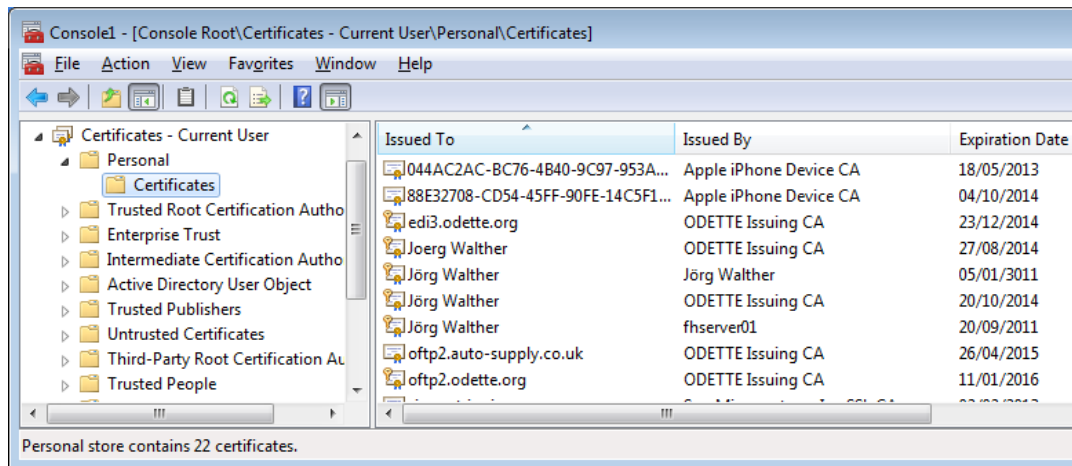
Close the snap-in selection window.

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

You will now see the Windows certificate store:

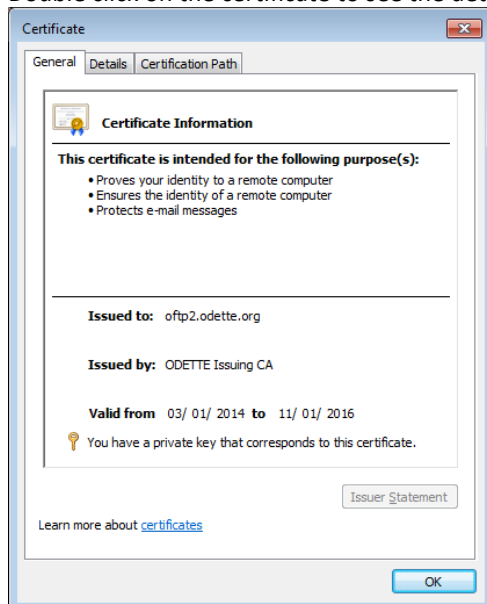


7. Expand Certificates, then expand Personal and select Certificates. You will be able to see the certificate in right panel of the Windows Management Console. This is where your downloaded certificate has been stored.



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.

Double click on the certificate to see the details.



Click OK to close the certificate details window and close the MMC-application.

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



### 3. How to create a CSR with batch files

1. Download openssl from  
 32 Bit Windows: <http://www.odette.org/repository/openssl-win32bit.zip>.  
 64 Bit Windows: <http://www.odette.org/repository/openssl-win64bit.zip>
2. Install the Visual C++ library (included in the downloaded zip file).
3. Install openssl. Note the path to the directory where openssl has been installed.
4. Download Odette CA Tools from [here](http://www.odette.org/repository/odette-ca-tools-win.zip):  
<http://www.odette.org/repository/odette-ca-tools-win.zip>.
5. Extract the Zip file, preferably to C:\
6. Check/edit the file settings.bat in the directory \Odette-CA-Tools(win)  
 The highlighted part in `set OPENSSLDIR=C:\OpenSSL-Win%BITS%` must point to your actual openssl installation directory.
7. Edit the file **odette-ca-csr.cfg** in the directory \Odette-CA-Tools(win) with an text editor and enter the values specific for your certificate (you might see a warning, click run to continue).  
 Note: If your certificate attribute values contain **special characters (e.g. äöüÄÖÜß etc.)** then **edit the file odette-ca-csr-utf8.cfg with an UTF-8 compatible editor** (Notepad++ is recommended), encode the file as UTF-8 without BOM and **run the create-csr-utf8.bat !**

The following example explains the different entry fields; grey lines should not be changed!

**Please replace with your actual certificate details as prepared in Step 1!**

# lines preceded by a #-sign are treated as comments by the interpreter

```
[ req ]
default_bits           = 2048
default_keyfile         = privkey.pem
distinguished_name     = req_distinguished_name
req_extensions         = req_ext

prompt                 = no

[ req_distinguished_name ]
# Country
C                       = GB
# State (default: empty)
#ST                     =
#Location
L                       = MyTown
#Organisation
O                       = My Company
# Organisation Unit
OU                     = My Department
# Common Name
CN                     = edi.mycompany.com
# Email Address
emailAddress           = Info@mycompany.com

[ req_ext ]
subjectAltName         = @alt_names
```

# If none of the below mentioned attributes shall be contained  
 # in your certificate, please enter the #-sign in front of URI.1 and

# in front of req\_extensions (line 5 from top)

[alt\_names]

# HOSTNAME -should be submitted, if the common name is not set to DHN!

DNS.1 = edi.mycompany.com # Put a #-sign in front, if you do not wish to specify this value.

# IP Address

IP = 98.88.46.37 # Put a #-sign in front, if you do not wish to specify this value.

# OFTP ID (SSID) – should always be submitted for OFTP2 certificates

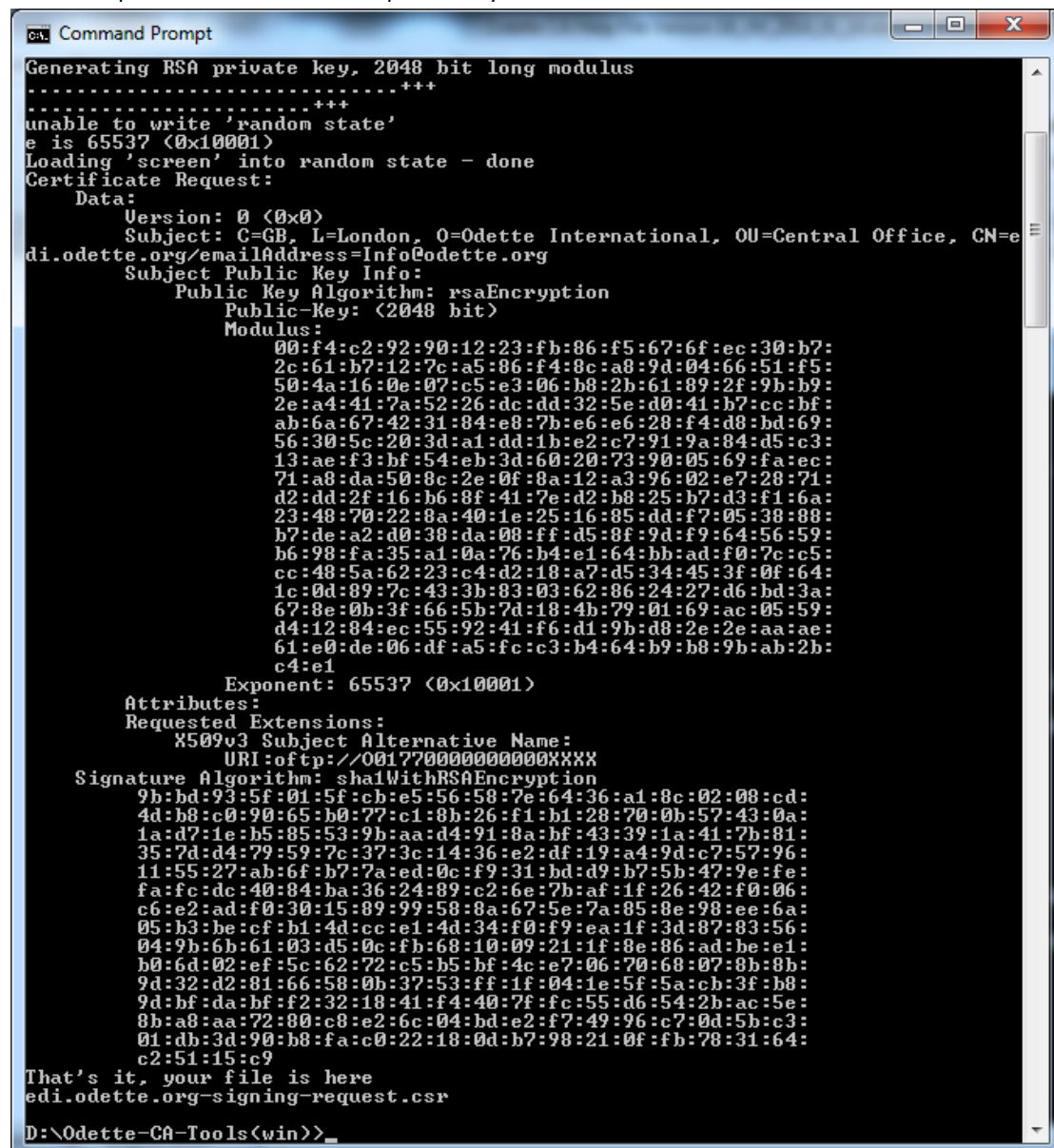
URI.1 = oftp://O017700000000000XXXX

# If you do not have an OFTP2 ID you can order it at <https://oscar.odette.org>

8. Start the command line interface (Start/All Programs/Accessories/Command Prompt) and change to the Odette CA Tools directory (e.g. **cd C:\Odette-CA-Tools(win)** )
9. Run the *create-csr.bat* and create a CSR by using the certificate attributes you have prepared in Step 6. You will be prompted to enter a name.

*Enter the Name:* enter a memorisable name for your certificate files

The batch process will then create a private key file and a CSR file.



```

C:\> Command Prompt
Generating RSA private key, 2048 bit long modulus
.....+++
unable to write 'random state'
e is 65537 (0x10001)
Loading 'screen' into random state - done
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=GB, L=London, O=Odette International, OU=Central Office, CN=edi.odette.org/emailAddress=Info@odette.org
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    Public-Key: (2048 bit)
    Modulus:
      00:f4:c2:92:90:12:23:fb:86:f5:67:6f:ec:30:b7:
      2c:61:b7:12:7c:a5:86:f4:8c:a8:9d:04:66:51:f5:
      50:4a:16:0e:07:c5:e3:06:b8:2b:61:89:2f:9b:b9:
      2e:a4:41:7a:52:26:dc:dd:32:5e:d0:41:b7:cc:bf:
      ab:6a:67:42:31:84:e8:7b:e6:e6:28:f4:d8:bd:69:
      56:30:5c:20:3d:a1:dd:1b:e2:c7:91:9a:84:d5:c3:
      13:ae:f3:bf:54:eb:3d:60:20:73:90:05:69:fa:ec:
      71:a8:da:50:8c:2e:0f:8a:12:a3:96:02:e7:20:71:
      d2:dd:2f:16:b6:8f:41:7e:d2:b8:25:b7:d3:f1:6a:
      23:48:70:22:8a:40:1e:25:16:85:dd:f7:05:38:88:
      b7:de:a2:d0:38:da:08:ff:d5:8f:9d:f9:64:56:59:
      b6:98:fa:35:a1:0a:76:b4:e1:64:bb:ad:f0:7c:c5:
      cc:48:5a:62:23:c4:d2:18:a7:d5:34:45:3f:0f:64:
      1c:0d:89:7c:43:3b:83:03:62:86:24:27:d6:bd:3a:
      67:8e:0b:3f:66:5b:7d:18:4b:79:01:69:ac:05:59:
      d4:12:84:ec:55:92:41:f6:d1:9b:d8:2e:2e:aa:ae:
      61:e0:de:06:df:a5:fc:c3:b4:64:b9:b8:9b:ab:2b:
      c4:e1
    Exponent: 65537 (0x10001)
  Attributes:
    Requested Extensions:
      X509v3 Subject Alternative Name:
        URI: oftp://O017700000000000XXXX
  Signature Algorithm: sha1WithRSAEncryption
    9b:bd:93:5f:01:5f:cb:e5:56:58:7e:64:36:a1:8c:02:08:cd:
    4d:b8:c0:90:65:b0:77:c1:8b:26:f1:b1:28:70:0b:57:43:0a:
    1a:d7:1e:b5:85:53:9b:aa:d4:91:8a:bf:43:39:1a:41:7b:81:
    35:7d:d4:79:59:7c:37:3c:14:36:e2:df:19:a4:9d:c7:57:96:
    11:55:27:ab:6f:b7:7a:ed:0c:f9:31:bd:d9:b7:5b:47:9e:fe:
    fa:fc:dc:40:84:ba:36:24:89:c2:6e:7b:af:1f:26:42:f0:06:
    c6:e2:ad:f0:30:15:89:99:58:8a:67:5e:7a:85:8e:98:ee:6a:
    05:b3:be:cf:b1:4d:cc:e1:4d:34:f0:f9:ea:1f:3d:87:83:56:
    04:9b:6b:61:03:d5:0c:fb:68:10:09:21:1f:8e:86:ad:be:e1:
    b0:6d:02:ef:5c:62:72:c5:b5:bf:4c:e7:06:70:68:07:8b:8b:
    9d:32:d2:81:66:58:0b:37:53:ff:1f:04:1e:5f:5a:cb:3f:b8:
    9d:bf:da:bf:f2:32:18:41:f4:40:7f:fc:55:d6:54:2b:ac:5e:
    0b:ab:aa:72:00:c8:e2:6c:04:bd:e2:f7:49:96:c7:0d:5b:c3:
    01:db:3d:90:b8:fa:c0:22:18:0d:b7:98:21:0f:fb:78:31:64:
    c2:51:15:c9
That's it, your file is here
edi.odette.org-signing-request.csr
D:\Odette-CA-Tools(win)>_
  
```

The system generates two files:


XYZ-private-key.pem and XYZ-signing-request.csr (XYZ stands for the name you entered as file name).



We recommend to keep the **odette-ca-csr.cfg** file with your certificate details safely – you need the same configuration (i.e. attribute values) for any subsequent renewal of the certificate.

#### 4. How to revoke a certificate

If you need to revoke a certificate y any reason, please login at <https://www.odetteca.com> and click the appropriate revoke button in the appropriate certificate row.

You will be prompted to provide the reason for revocation,

 **Revoke Certificate**




 Control Panel  Logout


Certificates can be revoked when they are no longer in use or the private key of the certificate has been compromised. Once a certificate has been revoked it can no longer be used. Revoking a certificate cannot be reversed.

To revoke a certificate please complete the details below and click the 'Revoke Certificate' button. You should then receive an automated e-mail from ODETTE confirming that the certificate has been successfully revoked.

| Selected Certificate |                      |
|----------------------|----------------------|
| Certificate Type     | Company              |
| Email                | info@odette.org      |
| Common Name          | edi2.odette.org      |
| Serial Number        | 5E18F8AD000000000E00 |
| Valid From           | 03/10/2013 13:45:54  |
| Valid Until          | 04/10/2014 13:35:53  |

| User Contact Details |                     |
|----------------------|---------------------|
| Email Address        | jwalther@odette.org |
| Telephone Number     | +44 776 9264 784    |

| Certificate Revocation Reason                                                                              |                                                                         |
|------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
|  Revocation Reason      | * Superseded<br><input type="text" value="Migrated to edi.odette.org"/> |
|  Additional Description | <input type="text"/>                                                    |
|  Revocation Date & Time | * 28 Jul 2014<br>12 : 18                                                |

 Revoke Certificate

Once you pushed the *Revoke Certificate* button the certificate will be marked as revoked in the Odette CA certificate revocation list and cannot be used anymore.