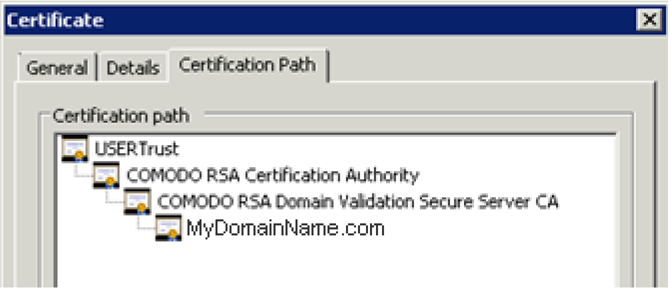
Trouble shooting

1. I received only one file (.crt or cer) which contains MydomainName.com Certificate

Look at the path in the certificate properties. If your certificate is at the root, then you don’t have any intermediate certificate.
You must only import the .cer ou crt you received.

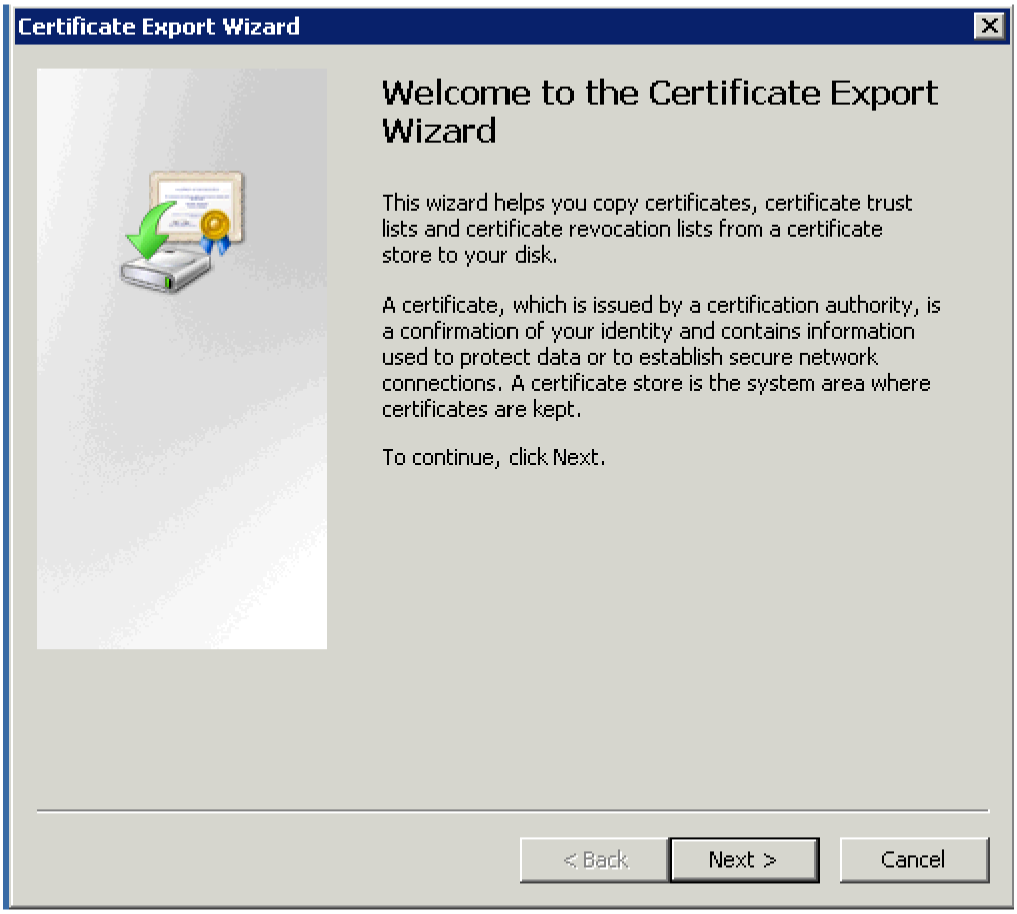
If the path contains others intermediates certificates, then they will be needed. You can export theses certificates included in yours and create a file by certificate.



USERTrust
COMODO RSA Certification Authority
COMODO RSA Domain Validation Secure Server CA
MyDomainName.com

You can export each certificate listed in the path and get one file per certificate.

Double click on the certificate you want to export. Then go to Details / Copy to file.



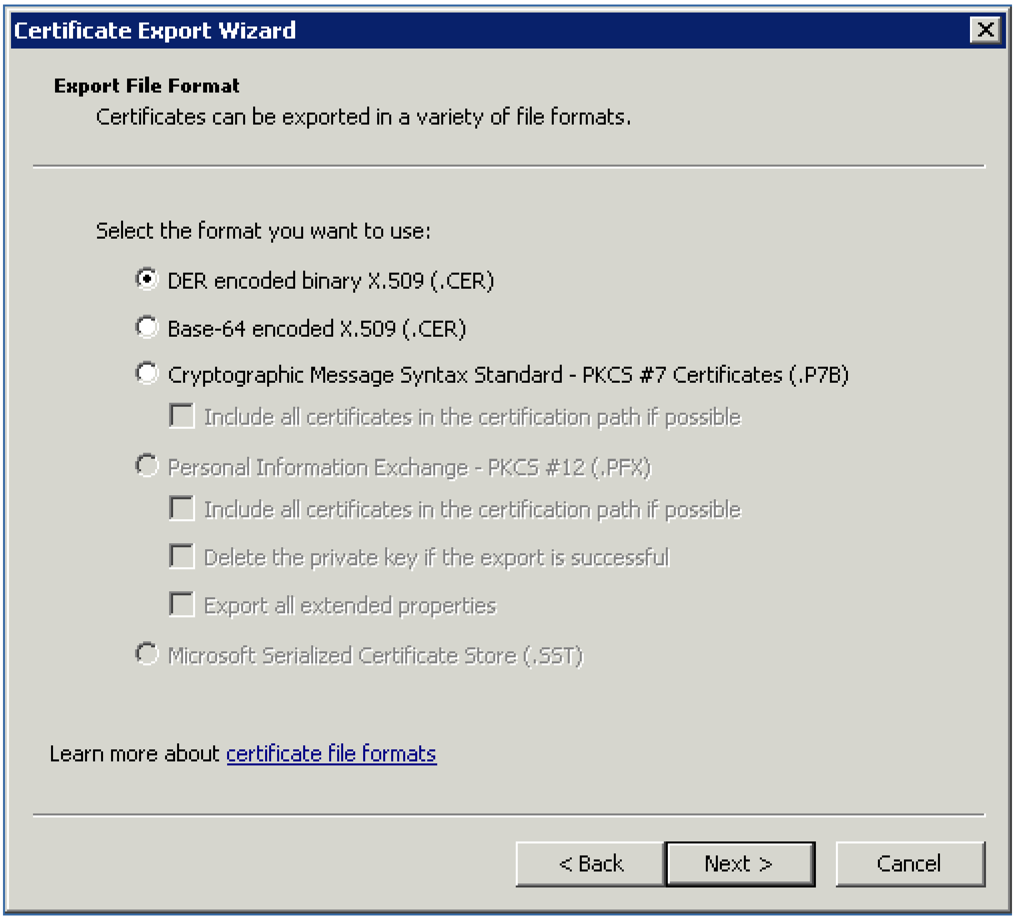
Certificate Export Wizard

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 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

Click next. Default values are ok. Click next until you have to give a name. Confirm your exportation.
The result is a file .cer containing only the certificate exported. Repeat this exportation for each level of the path.

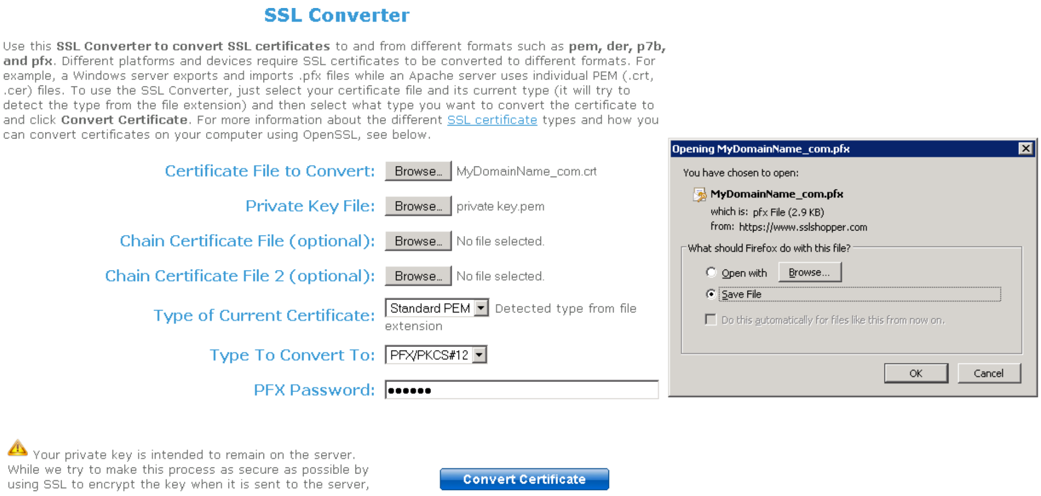
2. My private key is .pem. I cannot import my private key in Portecle

You can convert your .pem in pfx format with Tools or online sites. For example, on this site:
https://www.sslshopper.com/ssl-converter.html

You must have your Private Key and your certificate (e.g. MyDomainName.com)

Browse to select the certificate to convert and the Private Key that goes with it. Current certificate type is PEM. Type to convert to is PFX (PKCS#12).
As .pfx is a secured format, you must enter a password. You can choose whatever you want, but, at least, you will have to set it to 'secret'.
So you should enter the password 'secret'.

The result is a .pfx format that you will be able to import in Portecle. As we saw in the installation section, this Private Key imported in Portecle must receive a CA Reply. See section Installation / CA reply for further information.



SSL Converter

Use this **SSL Converter to convert SSL certificates** to and from different formats such as **pem, der, p7b, and pfx**. Different platforms and devices require SSL certificates to be converted to different formats. For example, a Windows server exports and imports .pfx files while an Apache server uses individual PEM (.crt, .cer) files. To use the SSL Converter, just select your certificate file and its current type (it will try to detect the type from the file extension) and then select what type you want to convert the certificate to and click **Convert Certificate**. For more information about the different SSL certificate types and how you can convert certificates on your computer using OpenSSL, see below.

Certificate File to Convert: Browse... MyDomainName_com.crt
Private Key File: Browse... private key.pem
Chain Certificate File (optional): Browse... No file selected.
Chain Certificate File 2 (optional): Browse... No file selected.
Type of Current Certificate: Standard PEM Detected type from file extension
Type To Convert To: PFX/PKCS#12
PFX Password: ••••••

Your private key is intended to remain on the server. While we try to make this process as secure as possible by using SSL to encrypt the key when it is sent to the server,

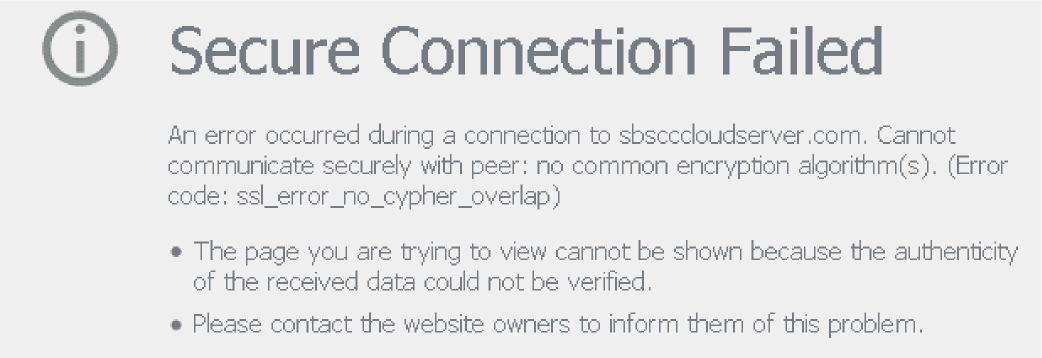
Opening MyDomainName_com.pfx

You have chosen to open:
MyDomainName_com.pfx
which is: pfx File (2.9 KB)
from: https://www.sslshopper.com

What should Firefox do with this file?
○ Open with Browse...
● Save File
□ Do this automatically for files like this from now on.

3. HTTPS errors

SSL error no cypher overlaps.



Secure Connection Failed

An error occurred during a connection to sbscccloudserver.com. Cannot communicate securely with peer: no common encryption algorithm(s). (Error code: ssl_error_no_cypher_overlap)

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

The Private Key or the Key Pair has not been imported in cert.jks or is invalid. Other errors types give the same screen with another error code.
Take a look at this code error. It concerns the certificate and something with it that goes wrong.
It is usually because one of the fields of the certificate is not valid or blank. Have a look to your certificate Properties and Request.
Verify that all the fields are correct. Report to section how to do a Request for more information.

4. Notice concerning Terminal Service Plus and Microsoft IIS web server

Please refer to our documentation about using IIS with Terminal Service Plus

However, here is some important information about IIS and certificates:

When using IIS, the certificate has to be installed in the keystore cert.jks. This must be done in the same way as if we were using Terminal Service Plus Web Server, and as described in the previous chapter.

Don't bind the 443 HTTPS port IN IIS, as this is the Terminal Service Plus Web server that handles the HTTPS protocol, the certificate and its encryption.
Not any bind has to be created on port 443. So, IIS must only have port 81 bound.

We are free to use IIS Request Tool to create the Private Key and the CA Request. It is simple to export the Private Key from IIS (IIS/Default site/Certificates) in the .pfx format and import it in cert.jks as described in the previous chapter.

Back to HTTPS, SSL & Certificates Tutorial Summary