part of eex group

epexspot

CTS++ Certificates

10.01.2022
Status: Final

Version: 0.5

Table of Contents

1. Introduction

1.1 Audience

This document is intended for customers who will use CTS++, EPEX SPOT Market Operators and EPEX SPOT IT Team.

1.2 Purpose

This documentation provides information about certificates needed to connect to CTS++
It provides the technical information about certificates, the certificate management process and the process to obtain a certificate.

1.3 Changes History Table

Date	Version	Change description
14.10.2021	V0.1	Initiate document
22.11.2021	V0.2	Update with NGESO return
06.11.2021	V0.3	Updated
13.12.2021	V0.4	Included additional screenshots and a step by step guide for the OpenSSL method and alternative solution
10.01.2022	V0.5	Added '.pem file' in 3.1.4 and Section 5.1

2. Certification rules and process

2.1 General information

The certificate needed for CTS++ is a signed public key:

- generated by a trusted Certificate Authority (CA)
- based in a certificate signing request customers send to EPEX
- which is created by the customer using the private key

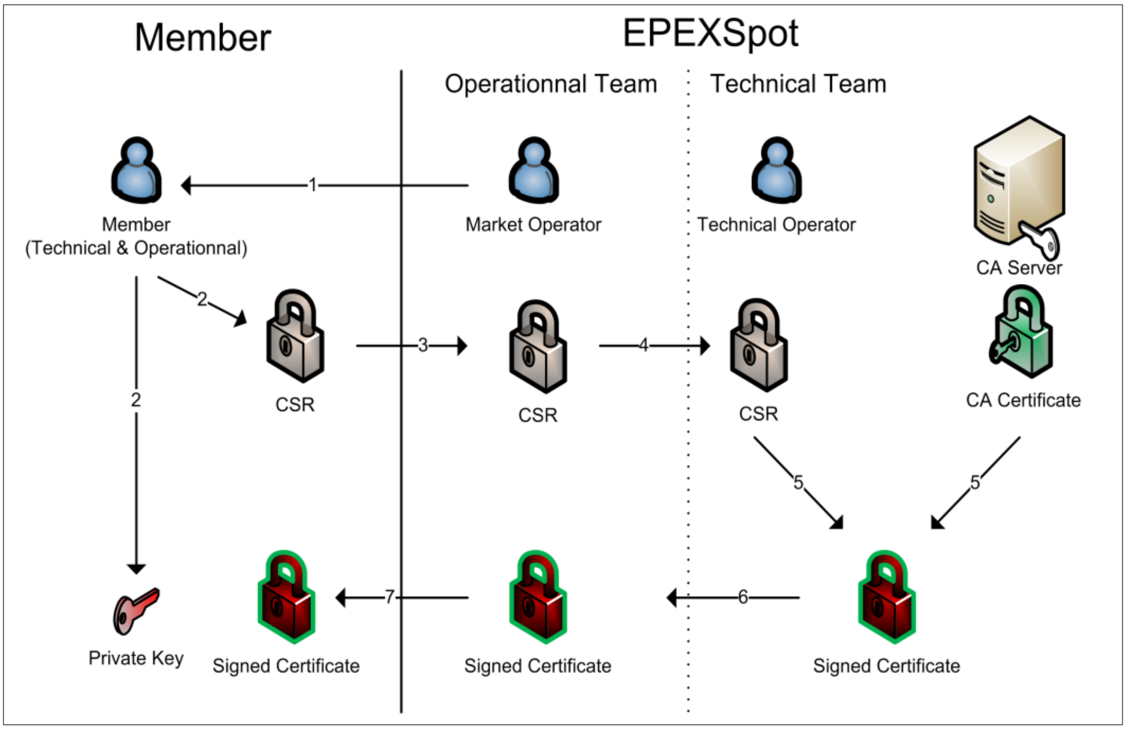
Customers have to generate the private key. Once the private key has been generated it can be used to generate the "Certificate Signing Request" file (CSR), as explained below.

Your private key should never be provided to anyone. Should for any reason the private part of the certificate be shared outside of the member, EPEX SPOT will not be able to guarantee the member identity.

The below sections will guide you through the required steps to obtain a signed certificate from EPEX and generate the mandatory technical file (keystore).

2.2 Certification process

The following schema describes the certification process for customers:



Steps:

1. Market Operators **validate the Member identity** (referred below as the “customer”).
2. **The member first generates the private key,** and once the key has been generated **the CSR can be generated using** that private key.
3. **The member sends by email the CSR file** to Market Operators **but does NOT share the private key.**
4. Market Operators validate the CSR file and if the checks are successful will transfer it to a Technical Operator otherwise will ask the member to perform the necessary changes
5. Market Operators transfer the CSR file to a Technical Operator in order to get the certificate signed.
6. The Technical Operator uses the CSR file and the Certificate Authority (CA) certificate to **generate the Signed certificate** (.pem file).
7. The Technical Operator transfers the signed certificate (.pem file) to Market Operators.
8. **Market Operators send by email the signed certificate (.pem file) to the Member.**
9. **What to do with the signed certificate (.pem file)? :** please refer to section 3 explaining how to build the Key Store you need to be able to connect to CTS++, using both the private key generated at step #2 and the signed certificate (.pem file).

2.3 CSR Creation Rules

Each certificate is unique and is identified by a combination of Country Name / Organization Name / Common Name.

This information is used by EPEX SPOT IT for the validation of the CSR and the generation of the signed certificate.

The following conditions must be met for the creation of the CSR:

- Only **ASCII** characters are accepted
- **Country Name** (2 letter code) : Must respect the country of the company (Validated by Operators),
- **Organization Name** (eg, company): Must meet the company name without any spaces.
- **Common Name:** Your email address which is registered on CTS++ and used for login

Example:

Will Smith
Energy Trading Limited
Will.Smith@energytrading.com

Country: GB
Organization Name: energytradinglimited
Common Name: will.smith@energytrading.com

(No capital letters are allowed in organization name and common name)

2.4 Revocation of certificate

In case the member would like to revoke a certificate (e.g. if the private key got exposed), the process is as follows:

- The member contacts Market Operators, who validate the member identity
- The member provides the **Country Name / Organization Name / Common Name** combination which identifies the certificate to be revoked
- The member is contacted (by email) by Market Operators to confirm the revocation of his certificate

Once revoked, a certificate cannot be used anymore.

2.5 Expiration and Renewal of a certificate

The certificates are valid for 1 year.

EPEX Market operators monitor PRODUCTION certificates expiry dates and informs customers one month before the expiry date.

The validity period of a certificate cannot be extended and a new CSR should be provided to EPEXSPOT to generate a new signed certificate.

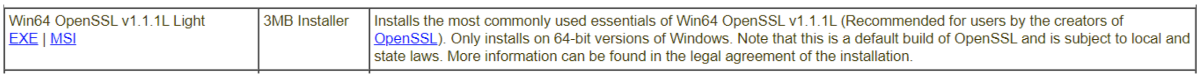
Note: The same **“Country Name / Organization Name / Common Name”** combination can be used for the new CSR.

3. Full Certificate process

3.1 Install OpenSSL and Certificate Creation

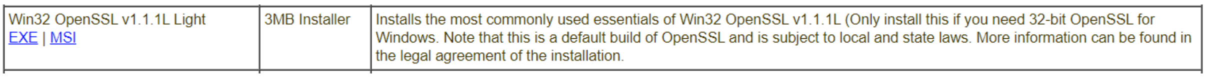
To perform certain cryptographic operations (creation of a private key, generation of a CSR, conversion of a certificate ...) on a Windows computer we can use the OpenSSL tool.

- Go to this website: Download link for OpenSSL
- Scroll down the page and choose the version (in .EXE):
    - Win64 OpenSSL v1.X.X : if your OS is 64 bits click the EXE link below:



Win64 OpenSSL v1.1.1L Light EXE | MSI	3MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.1.1L (Recommended for users by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

-
    - Win32 OpenSSL v1.X.X : if your OS is 32 bits clock the EXE link below:



Win32 OpenSSL v1.1.1L Light EXE | MSI	3MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.1.1L (Only install this if you need 32-bit OpenSSL for Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

Note that for some versions of Windows systems, you may need to install "Visual C ++ 2008 Redistributable".

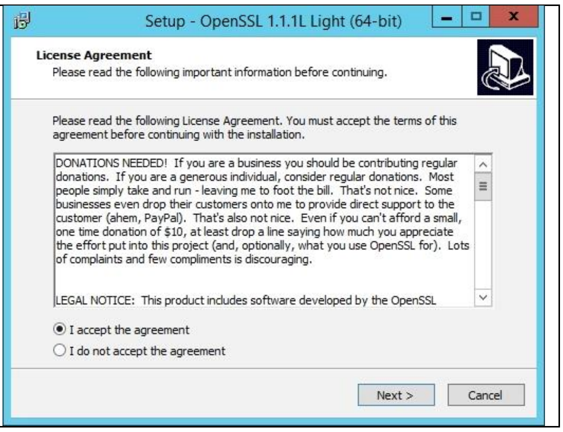
3.1.1 Use OpenSSL on a Windows machine

By default, OpenSSL for Windows is installed in the following directory:

- If you have installed Win64 OpenSSL v1.X.X: C:\Program Files\OpenSSL-Win64\
- If you have installed Win32 OpenSSL v1.X.X: C:\Program Files (x86)\OpenSSL-Win32\

3.1.2 Installation

Once downloaded, please follow the step by step guide below;

Accept the License Agreement and click “Next”	

Setup - OpenSSL 1.1.1L Light (64-bit)

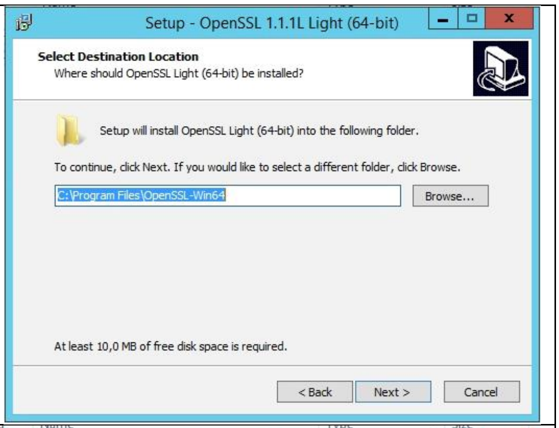
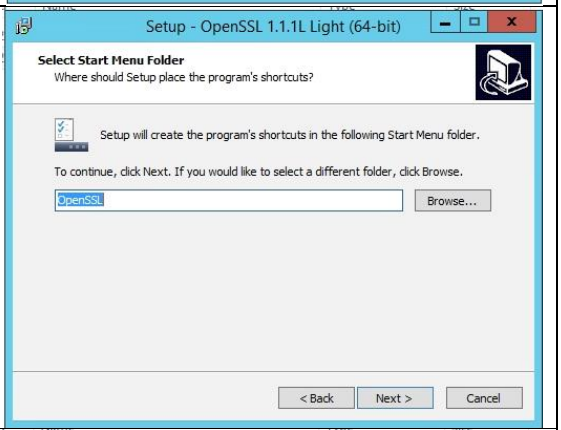
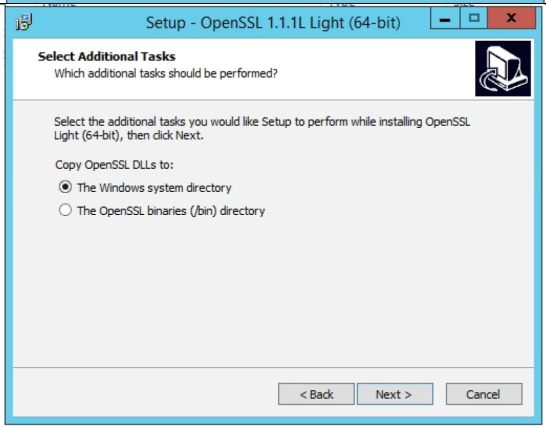
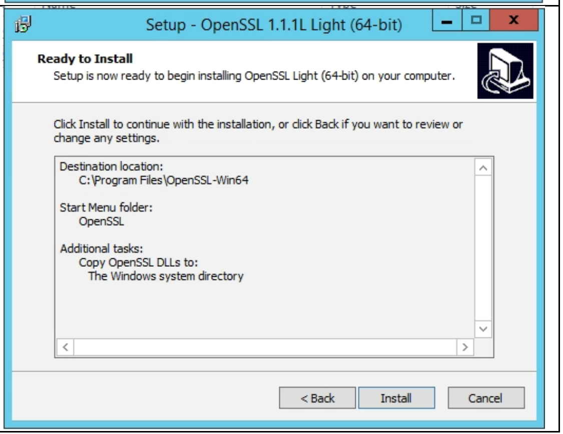
License Agreement
Please read the following important information before continuing.

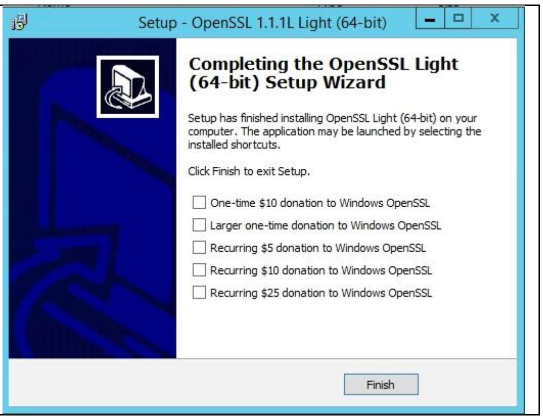
Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

DONATIONS NEEDED! If you are a business you should be contributing regular donations. If you are a generous individual, consider regular donations. Most people simply take and run - leaving me to foot the bill. That's not nice. Some businesses even drop their customers onto me to provide direct support to the customer (ahem, PayPal). That's also not nice. Even if you can't afford a small, one time donation of $10, at least drop a line saying how much you appreciate the effort put into this project (and, optionally, what you use OpenSSL for). Lots of complaints and few compliments is discouraging.

LEGAL NOTICE: This product includes software developed by the OpenSSL

● I accept the agreement
○ I do not accept the agreement

Click “Next”	 Setup - OpenSSL 1.1.1L Light (64-bit) **Select Destination Location** Where should OpenSSL Light (64-bit) be installed? Setup will install OpenSSL Light (64-bit) into the following folder. To continue, click Next. If you would like to select a different folder, click Browse. C:\Program Files\OpenSSL-Win64 At least 10,0 MB of free disk space is required.
Click “Next”	 Setup - OpenSSL 1.1.1L Light (64-bit) **Select Start Menu Folder** Where should Setup place the program's shortcuts? Setup will create the program's shortcuts in the following Start Menu folder. To continue, click Next. If you would like to select a different folder, click Browse. OpenSSL
Click “Next”	 Setup - OpenSSL 1.1.1L Light (64-bit) **Select Additional Tasks** Which additional tasks should be performed? Select the additional tasks you would like Setup to perform while installing OpenSSL Light (64-bit), then click Next. Copy OpenSSL DLLs to: ● The Windows system directory ○ The OpenSSL binaries (/bin) directory
Click “Install”	 Setup - OpenSSL 1.1.1L Light (64-bit) **Ready to Install** Setup is now ready to begin installing OpenSSL Light (64-bit) on your computer. Click Install to continue with the installation, or click Back if you want to review or change any settings. Destination location: C:\Program Files\OpenSSL-Win64 Start Menu folder: OpenSSL Additional tasks: Copy OpenSSL DLLs to: The Windows system directory

Uncheck “One-time $10 donation” And click “Finish”	 Setup - OpenSSL 1.1.1L Light (64-bit) **Completing the OpenSSL Light (64-bit) Setup Wizard** Setup has finished installing OpenSSL Light (64-bit) on your computer. The application may be launched by selecting the installed shortcuts. Click Finish to exit Setup. □ One-time $10 donation to Windows OpenSSL □ Larger one-time donation to Windows OpenSSL □ Recurring $5 donation to Windows OpenSSL □ Recurring $10 donation to Windows OpenSSL □ Recurring $25 donation to Windows OpenSSL Finish

3.1.3 Generate the private key (.key) and the CSR (Certificate Signing Request)

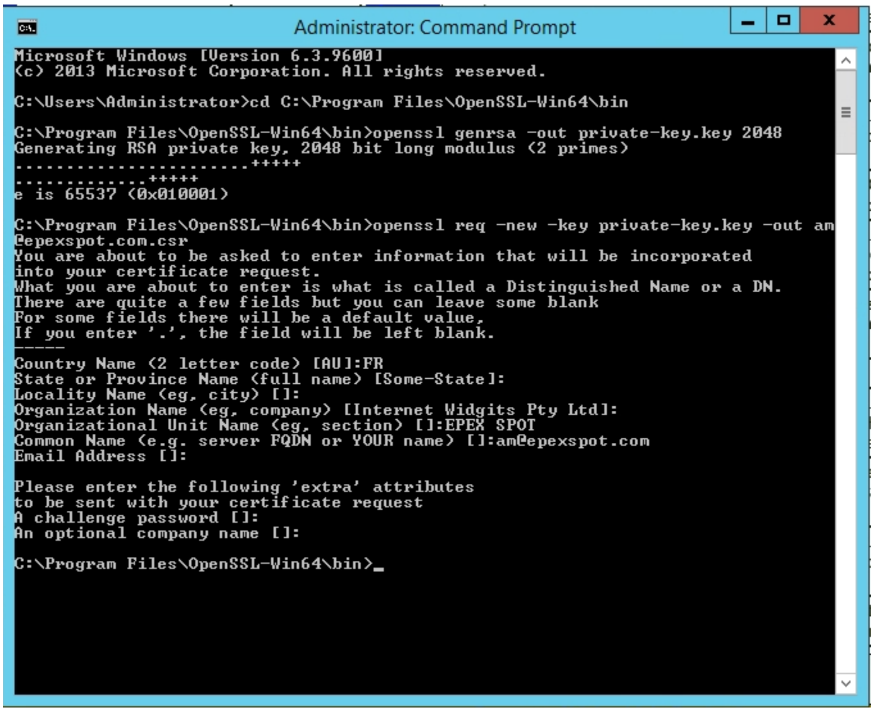
As part of obtaining (or renewing or reissue) a certificate, you will have to generate a private key and the associated CSR.

1. To launch OpenSSL, open a command prompt with Administrators rights (right click - Run as ...). Go to the "bin" subdirectory from the OpenSSL installation folder:

   - If you have installed Win64 OpenSSL:
     cd C:\Program Files\OpenSSL-Win64\bin

   - If you have installed Win32 OpenSSL:
     cd C:\Program Files (x86)\OpenSSL-Win32\bin

You will have the following window open:

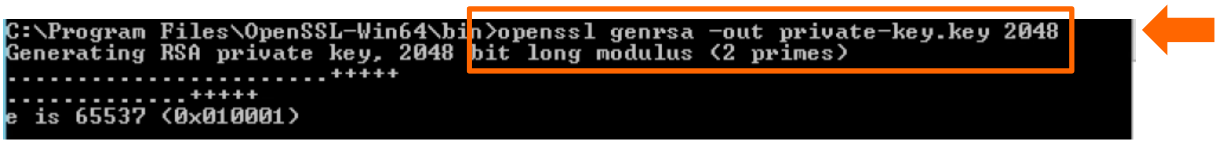


Administrator: Command Prompt

```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\Program Files\OpenSSL-Win64\bin

C:\Program Files\OpenSSL-Win64\bin>openssl genrsa -out private-key.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
........................+++++
..............+++++
e is 65537 (0x010001)

C:\Program Files\OpenSSL-Win64\bin>openssl req -new -key private-key.key -out am
@epexspot.com.csr
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]:FR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:EPEX SPOT
Common Name (e.g. server FQDN or YOUR name) []:am@epexspot.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

C:\Program Files\OpenSSL-Win64\bin>_
```

2. To create the private key, you type the following:

openssl genrsa -out private-key.key 2048



```
C:\Program Files\OpenSSL-Win64\bin>openssl genrsa -out private-key.key 2048
Generating RSA private key, 2048 bit long modulus (2 primes)
......................+++++
............+++++
e is 65537 (0x010001)
```

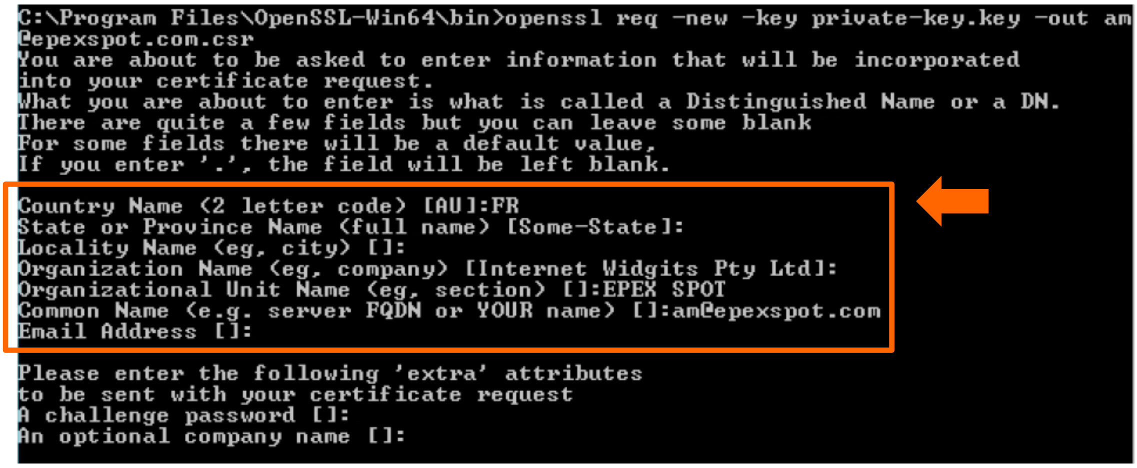
3. The private key will now be generated.

4. Create the Certificate request and type the following:

openssl req -new -key private-key.key -out [Common Name].csr

5. Add the following details in the fields:

Country Name : GB
State or Province Name : leave empty
Locality Name : leave empty
Organization Name : leave empty
Organization Unit Name : Your company name
Common Name : Your email address
Email Address : leave empty
A challenge password : leave empty
An optional Company name : leave empty



```
C:\Program Files\OpenSSL-Win64\bin>openssl req -new -key private-key.key -out am
@epexspot.com.csr
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]:FR
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:EPEX SPOT
Common Name (e.g. server FQDN or YOUR name) []:am@epexspot.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

6. A public/private key pair has now been created.

7. The private key (i.e. private-key.key) is stored locally on the computer *(in C:\Program Files\OpenSSL-Win64\bin or C:\Program Files (x86)\OpenSSL-Win32\bin)*. This private key is used for decryption.

8. **The public portion, in the form of a Certificate Signing Request (i.e. [email address].csr), need to be send to EPEX Market Operators via email to cts-fra-operation@epexspot.com**.

9. After EPEX Market Operators will authorize the csr and provide you with a .pem file. Please follow the instruction in the next section below.

3.1.4

3.1.4 Generate the PFX

1. After receiving the .pem file from EPEX Market Operators, place it in the same directory as the .csr and .key. *(in C:\Program Files\OpenSSL-Win64\bin or C:\Program Files (x86)\OpenSSL-Win32\bin).*

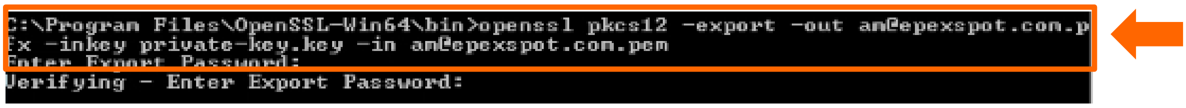
2. Open the command prompt again with Administrators rights (right click - Run as ...). Go to the "bin" subdirectory from the OpenSSL installation folder:

   - If you have installed Win64 OpenSSL:
     cd C:\Program Files\OpenSSL-Win64\bin

   - If you have installed Win32 OpenSSL:
     cd C:\Program Files (x86)\OpenSSL-Win32\bin

3. To generate the PFX file from the certificate and Private key, type the following:
   (leave the two "Password" field empty)

openssl pkcs12 -export -out [Common Name]**.pfx -inkey** private-key.key **-in** [Common Name]**.pem**



```
C:\Program Files\OpenSSL-Win64\bin>openssl pkcs12 -export -out am@epexspot.com.p
fx -inkey private-key.key -in am@epexspot.com.pem
Enter Export Password:
Verifying - Enter Export Password:
```

3.1.5 Install the PFX in Windows

1. Double click on the .pfx file

2. follow the instructions

3.2 Alternative solution - use an online tool

<u>Only if the above OpenSSL method mentioned in Section 3.1 does not work</u>, we suggest to make use of an online tool for the CSR certification and conversion.

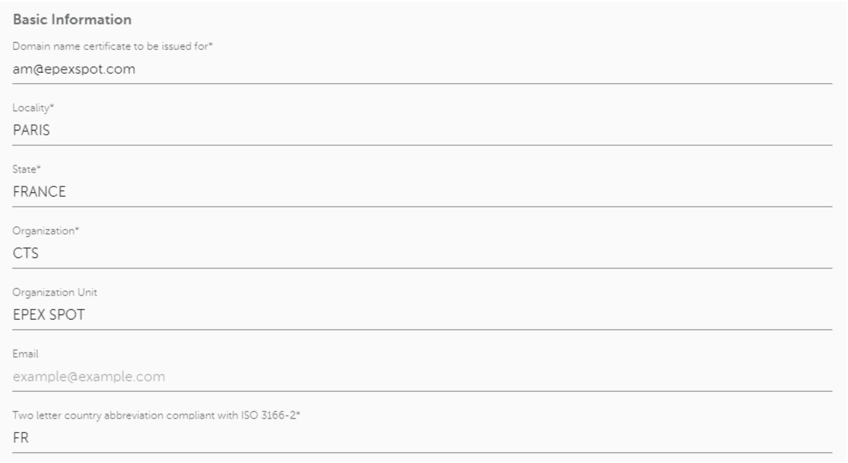
3.2.1 Generate the private key (.key) and the CSR (Certificate Signing Request)

The follow steps should be followed:

1. To create the CSR certification user the following link: https://decoder.link/csr_generator

2. Fill in the fields below:

Domain name certificate to be issued for* : your email address
Locality* : Your city
State* : your State / country
Organization* : CTS
Organization Unit : your company
Two letter country abbreviation compliant with ISO 3166-2* : GB



Basic Information

Domain name certificate to be issued for*
am@epexspot.com

Locality*
PARIS

State*
FRANCE

Organization*
CTS

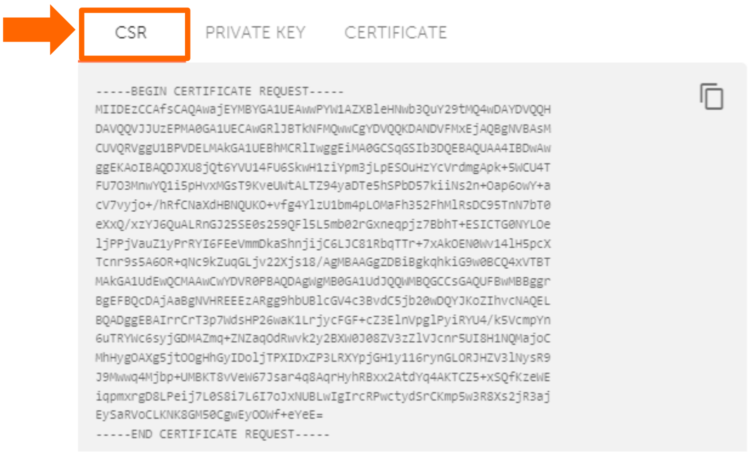
Organization Unit
EPEX SPOT

Email
example@example.com

Two letter country abbreviation compliant with ISO 3166-2*
FR

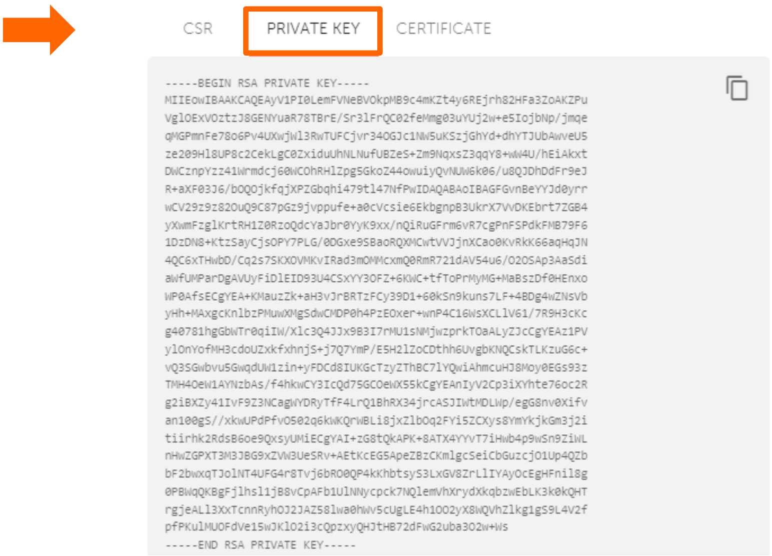
3. Click on “GENERATE”

4. Save the CSR part: copy and paste below in a notepad, and save as: email address.csr



```
-----BEGIN CERTIFICATE REQUEST-----
MIIDEzCCAfsCAQAwajEYMBYGA1UEAwwPYW1AZXBleHNwb3QuY29tMQ4wDAYDVQQH
DAVQQVJJUzEPMA0GA1UECAwGRlJBTkNFMQwwCgYDVQQKDANDVFMxEjAQBgNVBAsM
CUVQRVggU1BPVDELMAkGA1UEBhMCRlIwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQDJXU8jQt6YVU14FU6SkwH1ziYpm3jLpESOuHzYcVrdmgApk+5WCU4T
FU7O3MnwYQ1i5pHvxMGsT9KveUWtALTZ94yaDTe5hSPbD57kiiNs2n+Oap6owY+a
cV7vyjo+/hRfCNaXdHBNQUKO+vfg4YlzU1bm4pLOMaFh352FhMlRsDC95TnN7bT0
eXxQ/xzYJ6QuALRnGJ25SE0s259QFl5L5mb02rGxneqpjz7BbhT+ESICTG0NYLOe
ljPPjVauZ1yPrRYI6FEeVmmDkaShnjijC6LJC81RbqTTr+7xAkOEN0Wv14lH5pcX
Tcnr9s5A6OR+qNc9kZuqGLjv22Xjs18/AgMBAAGgZDBiBgkqhkiG9w0BCQ4xVTBT
MAkGA1UdEwQCMAAwCwYDVR0PBAQDAgWgMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggr
BgEFBQcDAjAaBgNVHREEEzARgg9hbUBlcGV4c3BvdC5jb20wDQYJKoZIhvcNAQEL
BQADggEBAIrrCrT3p7WdsHP26waK1LrjycFGF+cZ3ElnVpglPyiRYU4/k5VcmpYn
6uTRYWc6syjGDMAZmq+ZNZaqOdRwvk2y2BXW0J08ZV3zZlVJcnr5UI8H1NQMajoC
MhHygOAXg5jtOOgHhGyIDoljTPXIDxZP3LRXYpjGH1y116rynGLORJHZV3lNysR9
J9Mwwq4Mjbp+UMBKT8vVeW67Jsar4q8AqrHyhRBxx2AtdYq4AKTCZ5+xSQfKzeWE
iqpmxrgD8LPeij7L0S8i7L6I7oJxNUBLwIgIrcRPwctydSrCKmp5w3R8Xs2jR3aj
EySaRVoCLKNK8GM50CgwEyOOWf+eYeE=
-----END CERTIFICATE REQUEST-----
```

5. Save the Private Key part: copy and paste below in a notepad, save as: private-key.key



```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAyV1PI0LemFVNeBVOkpMB9c4mKZt4y6REjrh82HFa3ZoAKZPu
Vgl0ExVOztzJ8GENYuaR78TBrE/Sr3lFrQC02feMmg03uYUj2w+e5IojbNp/jmqe
qMGPmnFe78o6Pv4UXwjWl3RwTUFCjvr34OGJc1NW5uKSzjGhYd+dhYTJUbAwveU5
ze209Hl8UP8c2CekLgC0ZxiduUhNLNufUBZeS+Zm9NqxsZ3qqY8+wW4U/hEiAkxt
DWCznpYzz41Wrmdcj60WCOhRHlZpg5GkoZ44owuiyQvNUW6k06/u8QJDhDdFr9eJ
R+aXF03J6/bOQOjkfqjXPZGbqhi479tl47NfPwIDAQABAoIBAGFGvnBeYYJd0yrr
wCV29z9z82OuQ9C87pGz9jvppufe+a0cVcsie6EkbgnpB3UkrX7VvDKEbrt7ZGB4
yXwmFzglKrtRH1Z0RzoQdcYaJbr0YyK9xx/nQiRuGFrm6vR7cgPnFSPdkFMB79F6
1DzDN8+KtzSayCjsOPY7PLG/0DGxe9SBaoRQXMCwtVVJjnXCao0KvRkK66aqHqJN
4QC6xTHwbD/Cq2s7SKXOVMKvIRad3mOMMcxmQ0RmR721dAV54u6/O2OSAp3AaSdi
aWfUMParDgAVUyFiDlEID93U4CSxYY3OFZ+6KWC+tfToPrMyMG+MaBszDf0HEnxo
WP0AfsECgYEA+KMauzZk+aH3vJrBRTzFCy39D1+60kSn9kuns7LF+4BDg4wZNsVb
yHh+MAxgcKnlbzPMuwXMgSdwCMDP0h4PzEOxer+wnP4C16WsXCLlV61/7R9H3cKc
g40781hgGbWTr0qiIW/Xlc3Q4JJx9B3I7rMU1sNMjwzprkTOaALyZJcCgYEAz1PV
ylOnYofMH3cdoUZxkfxhnjS+j7Q7YmP/E5H2lZoCDthh6UvgbKNQCskTLKzuG6c+
vQ3SGwbvu5GwqdUW1zin+yFDCd8IUKGcTzyZThBC7lYQwiAhmcuHJ8Moy0EGs93z
TMH4OeW1AYNzbAs/f4hkwCY3IcQd75GCOeWX55kCgYEAnIyV2Cp3iXYhte76oc2R
g2iBXZy41IvF9Z3NCagWYDRyTfF4LrQ1BhRX34jrcASJIWtMDLWp/egG8nv0Xifv
an100gS//xkwUPdPfvO502q6kWKQrWBLi8jxZlbOq2FYi5ZCXys8YmYkjkGm3j2i
tiirhk2RdsB6oe9QxsyUMiECgYAI+zG8tQkAPK+8ATX4YYvT7iHwb4p9wSn9ZiWL
nHwZGPXT3M3JBG9xZVW3UeSRv+AEtKcEG5ApeZBzCKmlgcSeiCbGuzcjO1Up4QZb
bF2bwxqTJolNT4UFG4r8Tvj6bRO0QP4kKhbtsyS3LxGV8ZrLlIYAyOcEgHFnil8g
0PBWqQKBgFjlhsl1jB8vCpAFb1UlNNycpck7NQlemVhXrydXkqbzwEbLK3k0kQHT
rgjeALl3XxTcnnRyhOJ2JAZ58lwa0hWv5cUgLE4h1OO2yX8WQVhZlkg1gS9L4V2f
pfPKulMUOFdVe15wJKlO2i3cQpzxyQHJtHB72dFwG2uba3O2w+Ws
-----END RSA PRIVATE KEY-----
```

6. Click on “I have copied the private key, close the windows”

7. **<u>The public portion, in the form of a Certificate Signing Request (i.e. [email address].csr), need to be send to Market Operators via email to cts-fra-operation@epexspot.com.</u>**

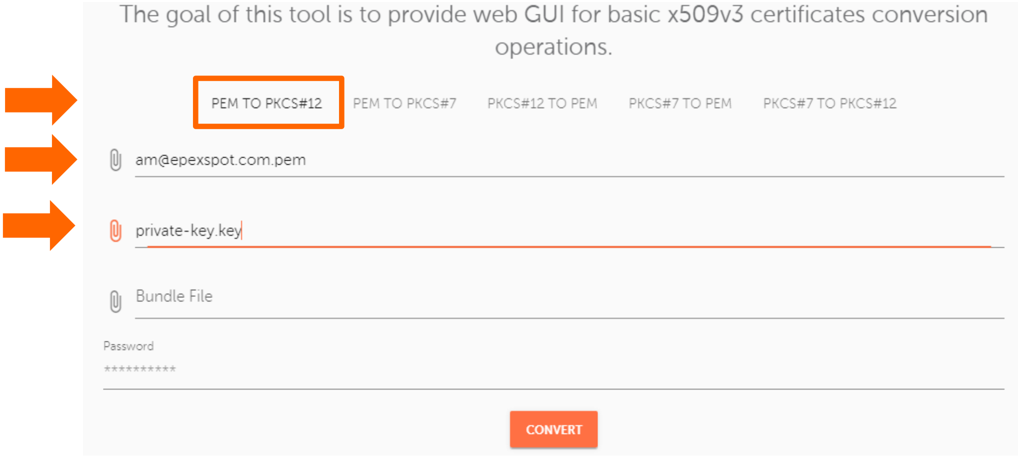
3.2.2 Generate the PFX

1. After receiving the certificate (.pem file) from EPEX Market Operators, use the following link: https://decoder.link/converter

2. Click on “Certificate file” and chose the file email address.pem, received from EPEX Market Operators

3. Click on “Key File” and chose the file private-key.key

4. Click on “CONVERT”



The goal of this tool is to provide web GUI for basic x509v3 certificates conversion operations.

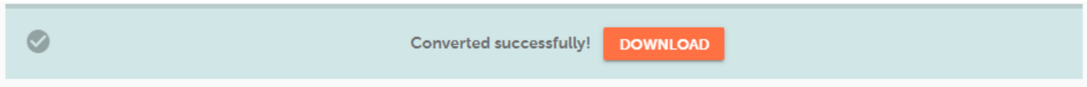
am@epexspot.com.pem

private-key.key

Bundle File

Password
****

5. Click on “Download”



Converted successfully!

3.2.3 Install the PFX in Windows

1. Open the zip downloaded in the previous step

2. Double click on the .pfx file and follow the instructions

4. Example

An EPEX platform user, Will Smith, wants to create a CSR and is required to install the Client certificate on his browser. Will Smith works for the company Energy Trading Ltd in the UK and is registered on the CTS++ auction platform with the following username/email address: will.smith@energytrading.com.

Following the instructions above in Section 3.1, Will Smith will be using the following commands;

4.1 Generate the private key (.key) and the CSR (Certificate Signing Request)

```
cd *OpenSSL base folder* \bin
openssl genrsa -out private-key.key 2048
openssl req -new -key private-key.key -out [Common Name].csr

Example:

cd *OpenSSL base folder* \bin
openssl genrsa -out private-key.key 2048
openssl req -new -key private-key.key -out will.smith@energytrading.com.csr
```

Fill in the required fields:

- **Country Name:** Must respect the country of the company
- **Organizational Unit:** the company name
- **Common Name:** email address

Example

- *Country Name: GB*
- *Organizational Unit: energytradinglimited*
- *Common Name: will.smith@energytrading.com*

(No capital letters are allowed in organization name and common name)

4.2 Generate the PFX

```
cd *OpenSSL base folder* \bin
openssl pkcs12 -export -out [Common Name].pfx -inkey private-key.key -in [Common Name].pem

Example:

cd *OpenSSL base folder* \bin
openssl pkcs12 -export -out will.smith@energytrading.com.pfx -inkey private-key.key -in
will.smith@energytrading.com.pem
```

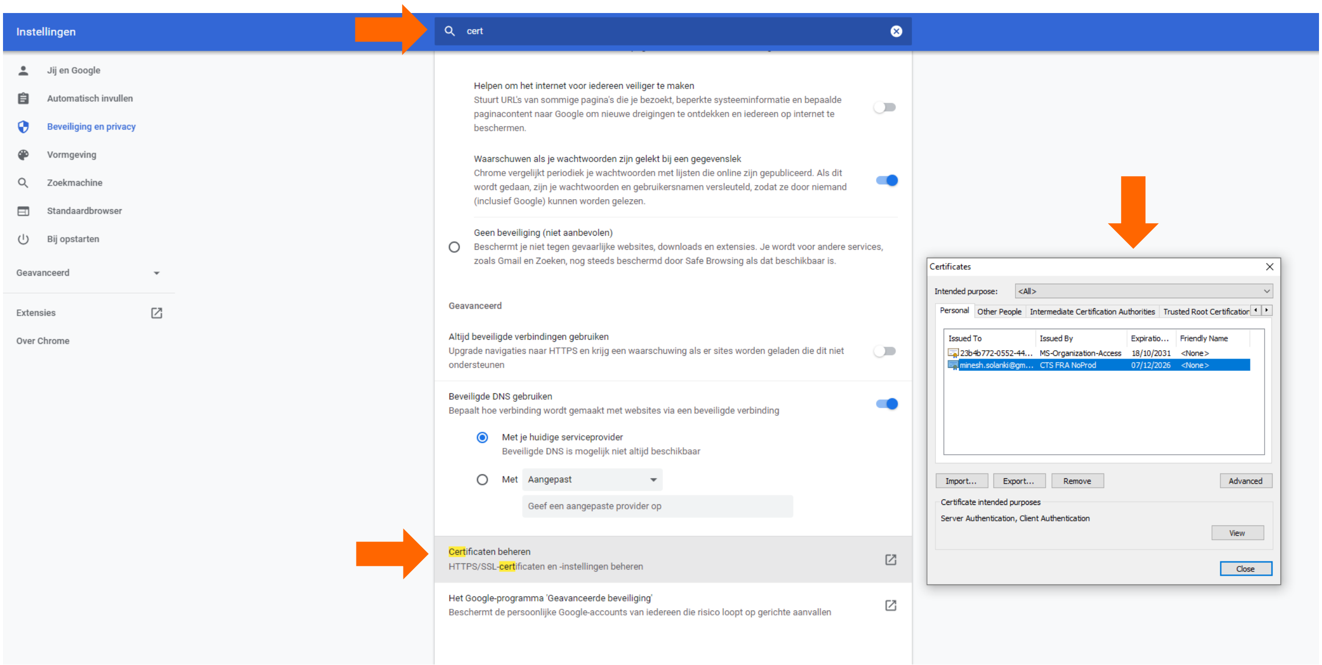
5. Troubleshooting

Contact your local IT support or send an email to EPEX market Operators **cts-fra-operation@epexspot.com**.

5.1 How to check if your Certificate has been installed into your browser?

We recommend the following steps to check if you have installed the certificate in your browser:

1. Go to ‘Brower Settings’
2. Search for ‘’Certificates’’
3. Click on ‘Manage Certificates’
4. Verify if the Certificate has been Installed



cert

Helpen om het internet voor iedereen veiliger te maken
Stuurt URL's van sommige pagina's die je bezoekt, beperkte systeeminformatie en bepaalde paginacontent naar Google om nieuwe dreigingen te ontdekken en iedereen op internet te beschermen.

Waarschuwen als je wachtwoorden zijn gelekt bij een gegevenslek
Chrome vergelijkt periodiek je wachtwoorden met lijsten die online zijn gepubliceerd. Als dit wordt gedaan, zijn je wachtwoorden en gebruikersnamen versleuteld, zodat ze door niemand (inclusief Google) kunnen worden gelezen.

○ Geen beveiliging (niet aanbevolen)
Beschermt je niet tegen gevaarlijke websites, downloads en extensies. Je wordt voor andere services, zoals Gmail en Zoeken, nog steeds beschermd door Safe Browsing als dat beschikbaar is.

Geavanceerd

Altijd beveiligde verbindingen gebruiken
Upgrade navigaties naar HTTPS en krijg een waarschuwing als er sites worden geladen die dit niet ondersteunen

Beveiligde DNS gebruiken
Bepaalt hoe verbinding wordt gemaakt met websites via een beveiligde verbinding

● Met je huidige serviceprovider
Beveiligde DNS is mogelijk niet altijd beschikbaar

○ Met Aangepast
Geef een aangepaste provider op

Certificaten beheren
HTTPS/SSL-certificaten en -instellingen beheren

Het Google-programma 'Geavanceerde beveiliging'
Beschermt de persoonlijke Google-accounts van iedereen die risico loopt op gerichte aanvallen

Certificates

Intended purpose: <All>

Personal | Other People | Intermediate Certification Authorities | Trusted Root Certificatior

Issued To	Issued By	Expiratio...	Friendly Name
23b4b772-0552-44...	MS-Organization-Access	18/10/2031	<None>
minesh.solanki@gm...	CTS FRA NoProd	07/12/2026	<None>

Certificate intended purposes
Server Authentication, Client Authentication