Certificat

Create CSR CERTIFICATE OPENSSL

1. Install the OpenSSL tool.
2. Run the following command to generate a CSR file:
   openssl req -new -nodes -sha256 -newkey rsa:2048 -keyout ***myprivate.key*** **-out** ***mydomain.csr***
   - **-new** specifies that a new CSR is generated.
   - **-nodes** specifies that the private key file is not encrypted.
   - **-sha256** specifies the digest algorithm.
   - **-newkey rsa:2048** specifies the type and length of the private key.
   - **-keyout** specifies that a private key file is generated. The file name can be customized.
   - **-out** specifies that the name of the CSR file is generated. The name can be customized.
3. Generate a CSR file named **mydomain.csr**.

   Figure 1 Generating a CSR file

```
Generating a 2048 bit RSA private key
....+++
.........................................................................+++
writing new private key to 'myprivate.key'
-----
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) [CN]:CN
State or Province Name (full name) []:ZheJiang
Locality Name (eg, city) [Default City]:HangZhou
Organization Name (eg, company) [Default Company Ltd]:HangZhou xxx Technologies,Inc.
Organizational Unit Name (eg, section) []:IT Dept.
Common Name (eg, your name or your server's hostname) []:www.example.com
Email Address []:

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

The information to be entered is as follows:

Field	Description	Example Value
Country Name	Two-letter code of the country where your company is located. For example, enter **CN** for China.	CN
State or Province Name	The name of the province or state where your company is located.	ZheJiang
Locality Name	The name of the city where your company is located.	HangZhou
Organization Name	The legal name of your company.	HangZhou xxx Technologies, Inc.
Organizational Unit Name	The department of your company that the applicant belongs to	IT Dept.
Common Name	The website domain name you are applying for an SSL certificate for. **NOTE:** • For a certificate with multiple domain names, enter the primary domain name to be associated with the certificate. • For a wildcard-domain certificate, enter the wildcard domain name. Example: *.example.com	www.example.com
Email Address	Email of an applicant. The CSR file password does not need to be entered. Just press **Enter**.	-
A challenge password	CSR file password. The CSR file password does not need to be entered. Just press **Enter**.	-

Certificat PFX EXTRACTION

Convert a pfx certificate to crt and key files

Extract private key

```
openssl pkcs12 -in cert.pfx -nocerts -out cert-encrypted.key
openssl rsa -in cert-encrypted.key -out cert.key
```

The second command removes the requirement to enter the password upon webserver start. Quite useful if you don't want your webserver get stuck with "Enter passphrase" during startup

Extract public key

```
openssl pkcs12 -in cert.pfx -clcerts -nokeys -out cert.crt
```


```
openssl pkcs12 -in cert.pfx -clcerts -nokeys -out cert.crt
```


Generate CA file

```
openssl pkcs12 -in cert.pfx -nokeys -nodes -cacerts -out ca-bundle.crt
```

Usage in httpd config

```
<VirtualHost 192.168.0.1:443>
  ...
  SSLEngine               on
  SSLCertificateFile      /etc/pki/tls/certs/cert.crt
  SSLCACertificateFile    /etc/pki/tls/certs/ca-bundle.crt
  SSLCertificateKeyFile   /etc/pki/tls/private/cert.key
  ...
</VirtualHost>
```

script extract certificat.pfx

```
#!/bin/bash

# mettre son fichier pfx
read -p "Entre le chemin de ton fichier PFX : " pfx_file

if [ -f "$pfx_file" ]; then
  echo "le fichier pfx na pas été trouver"
  exit 1
fi

# mettre le nom du certificat a extraire
read -p "Entre le nom du certificat : " cert_name

# extrait la clé privée
openssl pkcs12 in "$pfx_file" -nocerts -out "${cert_name}-encrypted.key"
openssl rsa in "${cert_name}-encrypted.key" -out "${cert_name}.key"

# extrait le certificat
openssl pkcs12 in "$pfx_file" clcerts nokeys out "${cert_name}.crt"

# extrait le CA
openssl pkcs12 in "$pfx_file" -nokeys nodes cacerts -out "${cert_name}-ca.crt"
```