

# Certificats pour EzGED

**IMPORTANT** Dans tous les cas si vous êtes amenés à générer des CSR (demande de certificat numérique, préformatées). Il est impératif de faire une sauvegarde de la machine et de l'environnement qui a permis de générer cette CSR, car la plupart du temps, seule cette machine pourra à nouveau générer une CSR ou extraire la clé privée du certificat et la clé publique en vue de configurer EzGED.

## Certificat SSL (HTTPS dans apache)

Ce certificat est destiné à encrypter la liaison et à protéger votre client des hackers en tout genre. Il protège la communication entre le navigateur du client et votre serveur. Il est nécessaire voir vital, dès que vous ouvrez votre EzGED à l'extérieur.

### Certificats de confiance

Un certificat est dit de confiance si le navigateur (qui va vérifier la validité du certificat) connaît l'autorité de certification qui l'a émis.

Nous vous conseillons Comodo comme fournisseur de certificat SSL environ 80 euros /an si vous le prenez pour 3 ans.

Pré-Requis :

Disposer d'une IP FIXE  
CONNAITRE LE NOM COMPLET DE L'URL DONT VOUS VOUS SERVIREZ POUR  
HEBERGER LA GED  
exemple ged.masociete.fr où masociete.fr est le domaine internet  
de votre société.  
Il faudra avoir la possibilité de lier sur votre serveur DNS  
ged.masociete.fr à votre ip fixe.

Lien d'achat du certificat : <https://ssl.comodo.com/comodo-ssl-certificate.php>

cliquez sur le bouton orange comodo ssl get now

Remplissez le formulaire :



The screenshot shows a form titled "Select Certificate Terms" with four rows of selection options:

Select the region you are located in	Europe
Select Certificate Type	Single Domain Certificate
Enter The Domain Name	ged.masociete.fr
Select the terms of your certificate	2 Yrs. €19.95 (or Save 23%)

Puis suivez la procédure.

## Certificats auto-signé

Il faut installer la dernière version d'OpenSSL.

Un certificat auto-signé est un certificat que vous générez vous-même. Il est important de noter qu'il n'est en rien (à attributs équivalents) moins protecteur qu'un certificat émis par une autorité certifiée. MAIS il ne sera pas connu des navigateurs des clients. Ces derniers seront invités à reconnaître explicitement votre certificat comme étant de confiance.

On va tout d'abord générer une clé privée:

```
openssl genrsa -des3 -out mydomain.key 1024
```

mydomain est à remplacer préféablement par l'url d'accès à EZGED (exemple: monserveurged.fr)

On nous demande de saisir une "pass phrase" (i.e un mot de passe). On choisit le mot de passe de notre choix.

On génère ensuite le fichier .csr (une demande de signature de certificat):

```
openssl req -new -key mydomain.key -out mydomain.csr -config  
c:\openssl\share\openssl.cnf
```

*c:\openssl\* est à remplacer avec le chemin vers lequel vous aurez installé OpenSSL

Puisque c'est auto-signé, nous prenons en charge nous-même la demande pour générer le certificat:

```
openssl x509 -req -days 730 -in mydomain.csr -signkey mydomain.key -out  
mydomain.crt
```

Nous avons presque terminé. Nous avons un fichier certificat et une clé privée. Cette dernière étant protégée par mot de passe nous allons la déchiffrée ainsi:

```
copy mydomain.key mydomain.key.org  
openssl rsa -in mydomain.key.org -out mydomain.key
```

Remarques:

- La procédure pour générer et installer un certificat est également disponible ici: <http://updates.nchp.net/doc/installhttps.pdf>
- Cette procédure est valable si l'on souhaite générer un certificat auto-signé à usage de signature.

## Installation

Que ce soit un certificat émis par une autorité de certification ou un certificat auto-signé vous devez avoir en votre possession:

- Un fichier contenant le certificat (et sa clé publique) au format .crt
- Un fichier contenant la clé privée "décryptée" <sup>1)</sup>

Dans le fichier de configuration Apache (Ex: C:\nchp\Apache2\conf\httpd.conf), ajoutez les directives suivantes :

(Où 192.168.XXX.XXX est à remplacer par l'adresse IP de votre serveur EzGED)

En début de fichier, là où doit se trouver déjà une instruction *Listen*

```
Listen 192.168.XXX.XXX:443
```

Localisez la ligne suivante et décommentez-la (= enlevez le signe # qui la précède)

```
LoadModule ssl_module modules/mod_ssl.so
```

En fin de fichier, après les définitions d'Alias déjà existante :

```
NameVirtualHost 192.168.XXX.XXX:443
<VirtualHost 192.168.XXX.XXX:443>
DocumentRoot c:/nchp/usr/local/nchp/ezged/www
ServerName 192.168.XXX.XXX
SSLEngine On
SSLOptions +FakeBasicAuth +ExportCertData +StrictRequire
SSLCertificateFile c:/nchp/etc/nchp/ezged/mydomain.crt
SSLCertificateKeyFile c:/nchp/etc/nchp/ezged/mydomain.key
</VirtualHost>
```

Sauvegardez le fichier et il ne vous reste plus qu'à relancer Apache:

```
net stop apache2.2
net start apache2.2
```

## Signature de masse

C'est le tampon numérique de la société au nom de la personne morale.

vous le trouverez chez Chambersign Negocio environ 800 euros pour 3 ans

<http://www.chambersign.fr/certificat-cachet-serveur-negocio/>

Il est demandé par le gérant de la société

Pièces nécessaires :

Justificatif de la nomination du représentant légal ou de l'autorité habilitée (maire, président, directeur générale, procès-verbal ....) ou extrait kbis

Copie de la pièce d'identité en cours de validité du représentant légal ou de l'autorité habilitée datée et signée de moins de trois mois

Copie de la pièce d'identité en cours de validité du demandeur du certificat (gestionnaire du certificat) datée et signée de moins de trois

mois

## Installation

Pour signer les PDF, avec signature incluse dans le PDF Dans votre fichier de configuration instance.conf ajouter les lignes suivantes dans la section [ezged]

```
pdfsignp12path = c:\nchp\etc\nchp\ezged\moncertificat.p12
pdfsignp12pass = votre mot de passe
pdfsignp12mask = 1
```

# Le certificat client pour signer au coup par coup les documents

1)

une clé privée étant protégée par mot de passe, on va en extraire le contenu qui ne sera plus protégé par mot de passe

From:  
<https://wiki.ezdev.fr/> - **EzGED Wiki**

Permanent link:  
<https://wiki.ezdev.fr/doku.php?id=certificats&rev=1503497970>



Last update: **2023/03/17 09:56**