Installation d'une PKI

L'installation se passe pour une machine debian stretch

N'ayant pas réussi à faire valider ma demande de certificat en tant qu'autorité de certification secondaire sur Active Directory (trouvable sur le bonus), j'ai donc fait signé ma demande par une autorité racine autosigné.

1. Autorité de certification racine

Nous allons commencer par crée notre autorité de certification racine. Pour ce faire, on va déplacer le dossier « ca » se trouvant dans notre repository dans le chemin « /root/ » (Être en sudo ou en su).

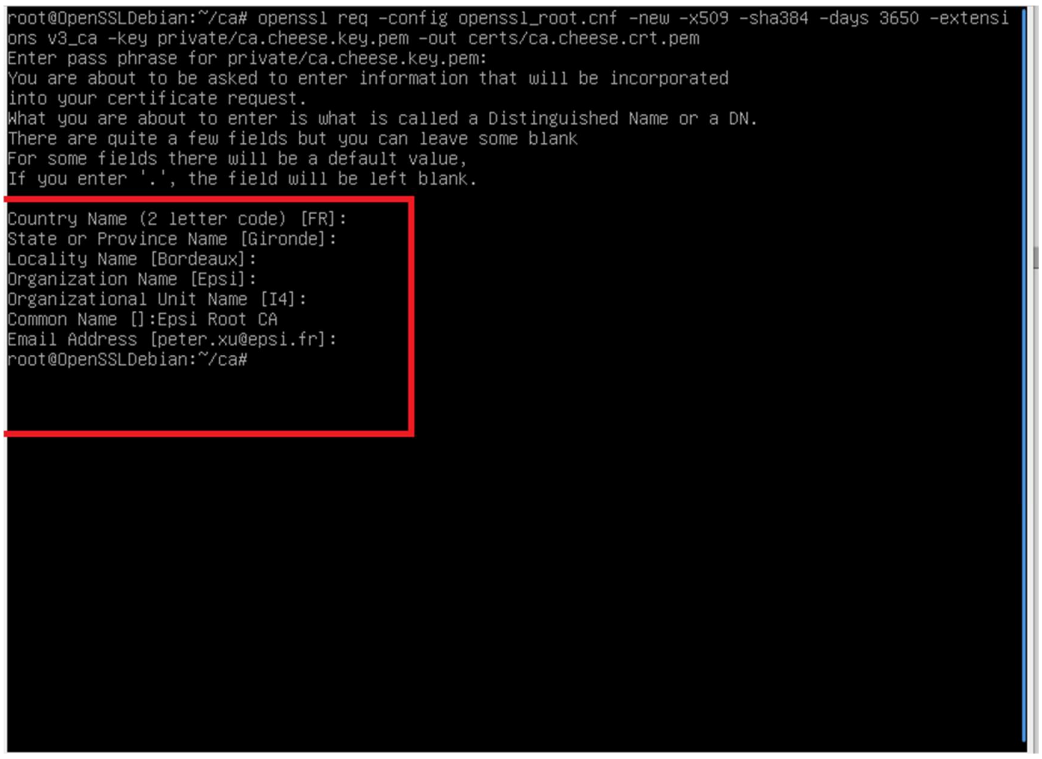
Après cela, se déplacer dans le dossier « /root/ca ».

On va créer notre clé privée en faisant :

```
openssl ecparam -genkey -name secp384r1 | openssl ec -aes256 -out private/ca.cheese.key.pem
```

Maintenant que l'on a notre clé privée dans le dossier « /root/ca/private », on va générer notre certificat auto-signé en faisant :

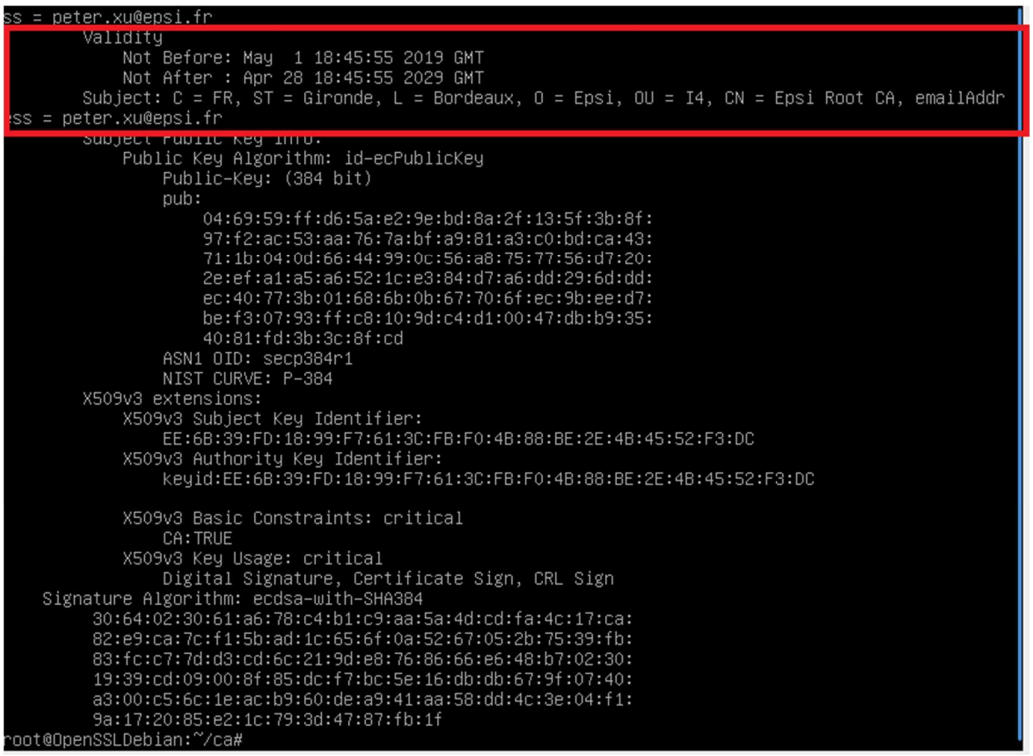
```
openssl req -config openssl_root.cnf -new -x509 -sha384 -extensions v3_ca -key private/ca.cheese.key.pem -out certs/ca.cheese.crt.pem
```



Maintenant que l'on a notre certificat racine dans « /root/ca/certs/ca.cheese.crt.pem » on va pouvoir créer notre certificat secondaire.

Si on veut vérifier notre certificat, on peut faire la commande :

```
openssl x509 -noout -text -in certs/ca.cheese.crt.pem
```



Comme montré sur l'encadré, le certificat contient les informations renseignées au-dessus et sa durée de validité.

2. Autorité de certificat secondaire

On va donc générer notre clé privée et notre demande de certificat en faisant :

```
openssl req -config intermediate/openssl_intermediate.cnf -new -newkey ec:<(openssl ecparam -name secp384r1) -keyout intermediate/private/int.cheese.key.pem -out intermediate/csr/int.cheese.csr
```

```
root@OpenSSLDebian:~/ca# openssl req -config intermediate/openssl_intermediate.cnf -new -newkey ec:<
(openssl ecparam -name secp384r1) -keyout intermediate/private/int.cheese.key.pem -out intermediate/
csr/int.cheese.csr
Generating an EC private key
writing new private key to 'intermediate/private/int.cheese.key.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
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) [US]:FR
State or Province Name [WA]:Gironde
Locality Name [Seattle]:Bordeaux
Organization Name [Grilled Cheese Inc.]:Epsi
Organizational Unit Name [Grilled Cheese Intermediary CA]:I4
Common Name []:Epsi Intermediate CA
Email Address [grilledcheese@yummyinmytummy.us]:peter.xu@epsi.fr
root@OpenSSLDebian:~/ca#
```

Après cela, on fait signer notre demande par notre autorité racine en faisant :

```
openssl ca -config openssl_root.cnf -extensions v3_intermediate_ca -days 3600 -md sha384 -i
n intermediate/csr/int.cheese.csr -out intermediate/certs/int.cheese.crt.pem
```

```
.c:74:fopen('/root/ca/index.txt.attr','r')
140350325370944:error:2006D080:BIO routines:BIO_new_file:no such file:../crypto/bio/bss_file.c:81:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number: 4096 (0x1000)
        Validity
            Not Before: May  1 18:50:19 2019 GMT
            Not After : Mar  9 18:50:19 2029 GMT
        Subject:
            countryName               = FR
            stateOrProvinceName       = Gironde
            organizationName          = Epsi
            organizationalUnitName    = I4
            commonName                = Epsi Intermediate CA
            emailAddress              = peter.xu@epsi.fr
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                3E:95:69:5D:17:D1:2B:55:A2:7F:27:3B:C5:BC:C0:8F:A2:5D:6B:91
            X509v3 Authority Key Identifier:
                keyid:EE:6B:39:FD:18:99:F7:61:3C:FB:F0:4B:88:BE:2E:4B:45:52:F3:DC

            X509v3 Basic Constraints: critical
                CA:TRUE, pathlen:0
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
            X509v3 CRL Distribution Points:

                Full Name:
                  URI:http://crl.grilledcheese.us/whomovedmycheese.crl

            Authority Information Access:
                CA Issuers - URI:http://ocsp.grilledcheese.us/cheddarcheeseroot.crt
                OCSP - URI:http://ocsp.grilledcheese.us/

Certificate is to be certified until Mar  9 18:50:19 2029 GMT (3600 days)
Sign the certificate? [y/n]:_
```

Notre certificat sera signée une fois que l'on valide (en faisant y).

On peut donc vérifié notre certificat en faisant :

```
openssl x509 -noout -text -in intermediate/certs/int.cheese.crt.pem
```

3. Le site internet

Le site tourne sous Python3 avec le framework Flask.

Il y a un fichier « requirements.txt » pour installer les dépendances, il faut faire :

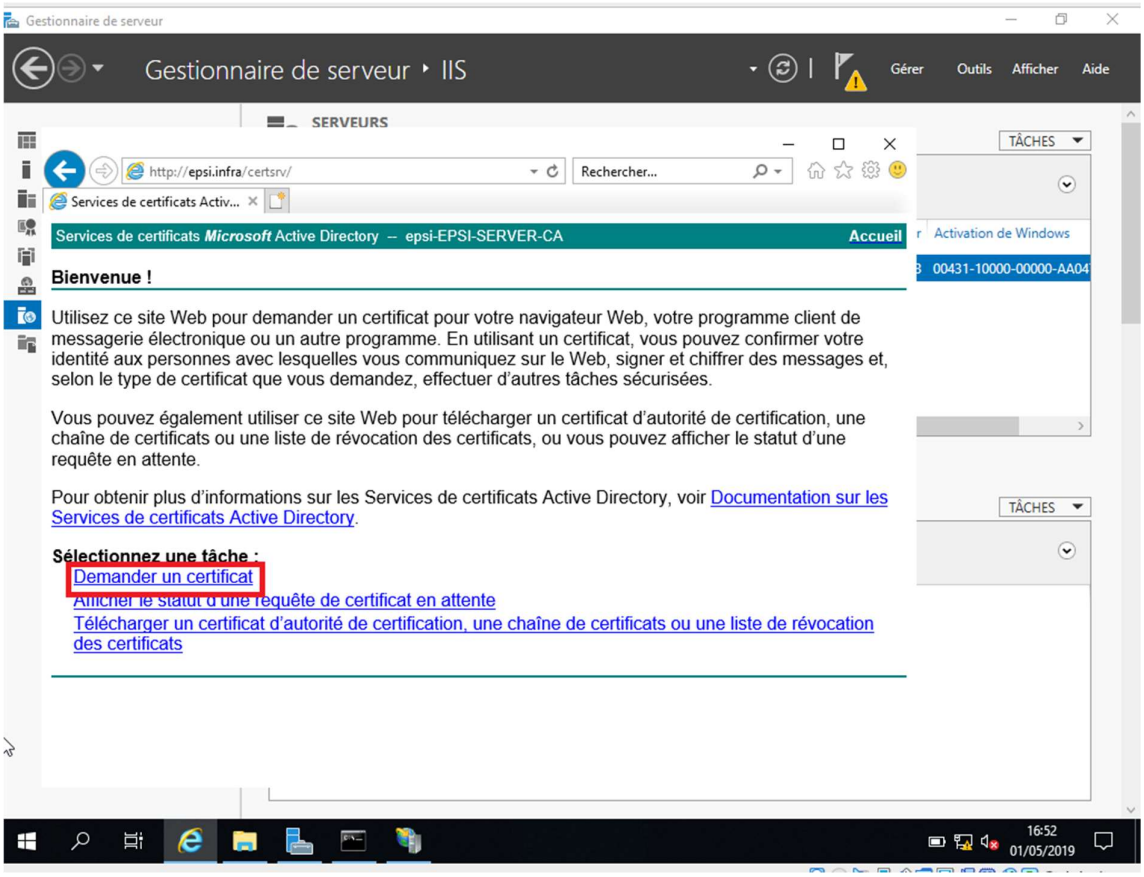
```
pip3 install -r requirements.txt
```

Puis pour lancer le serveur web, il faut faire :

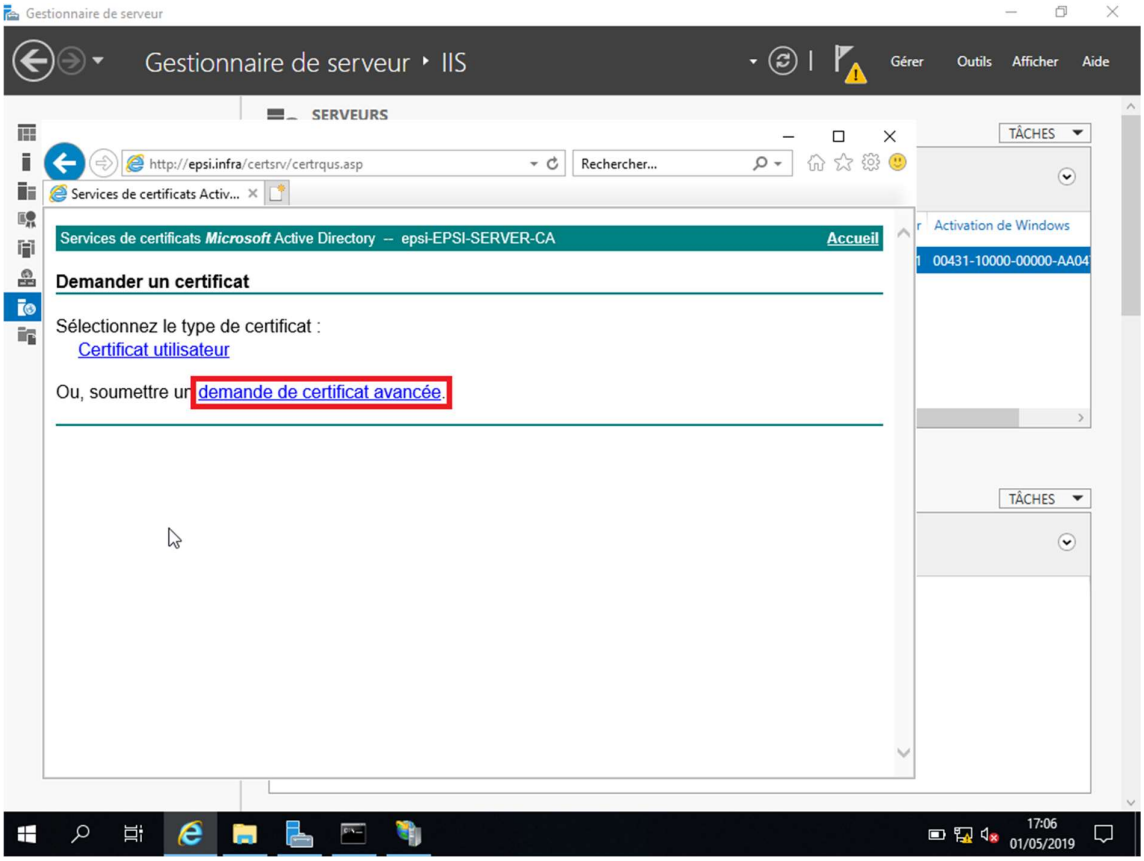
```
python index.py
```

Bonus

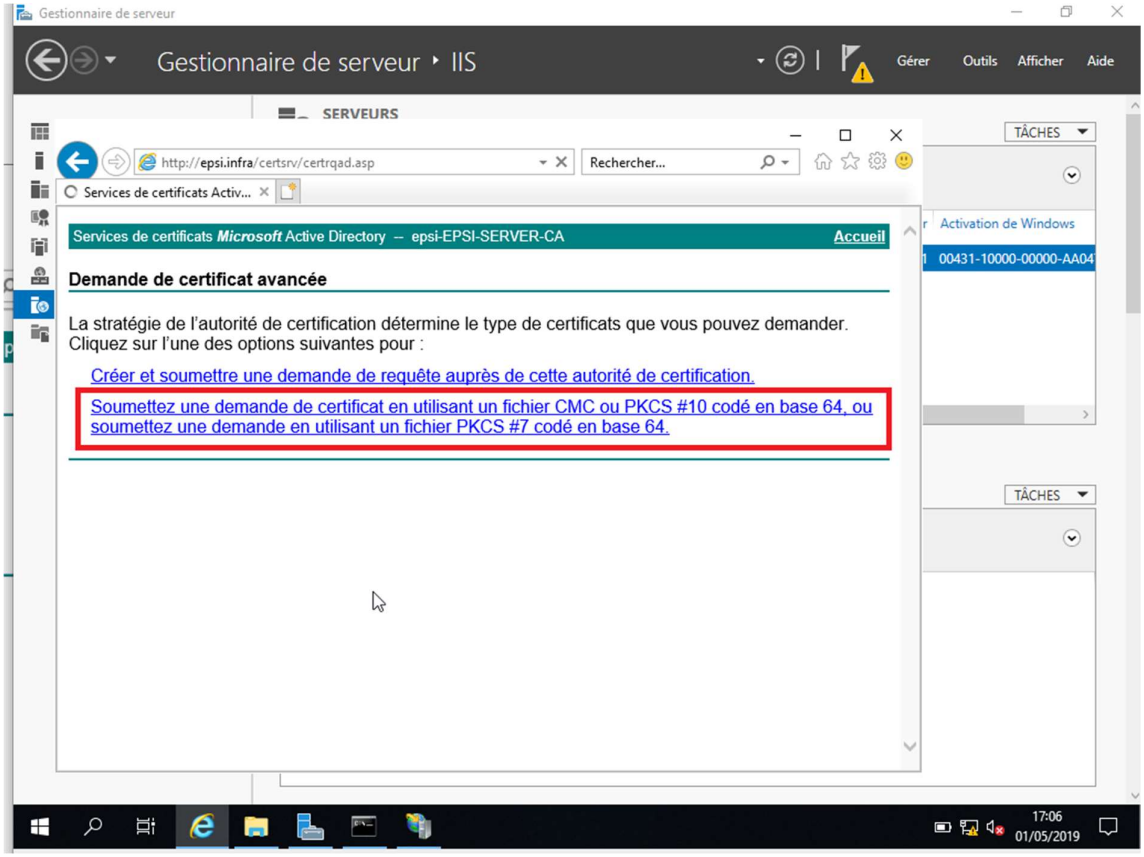
Accédez à la page http://<mon_hote>/certsrv et cliquez sur « Demander un certificat »



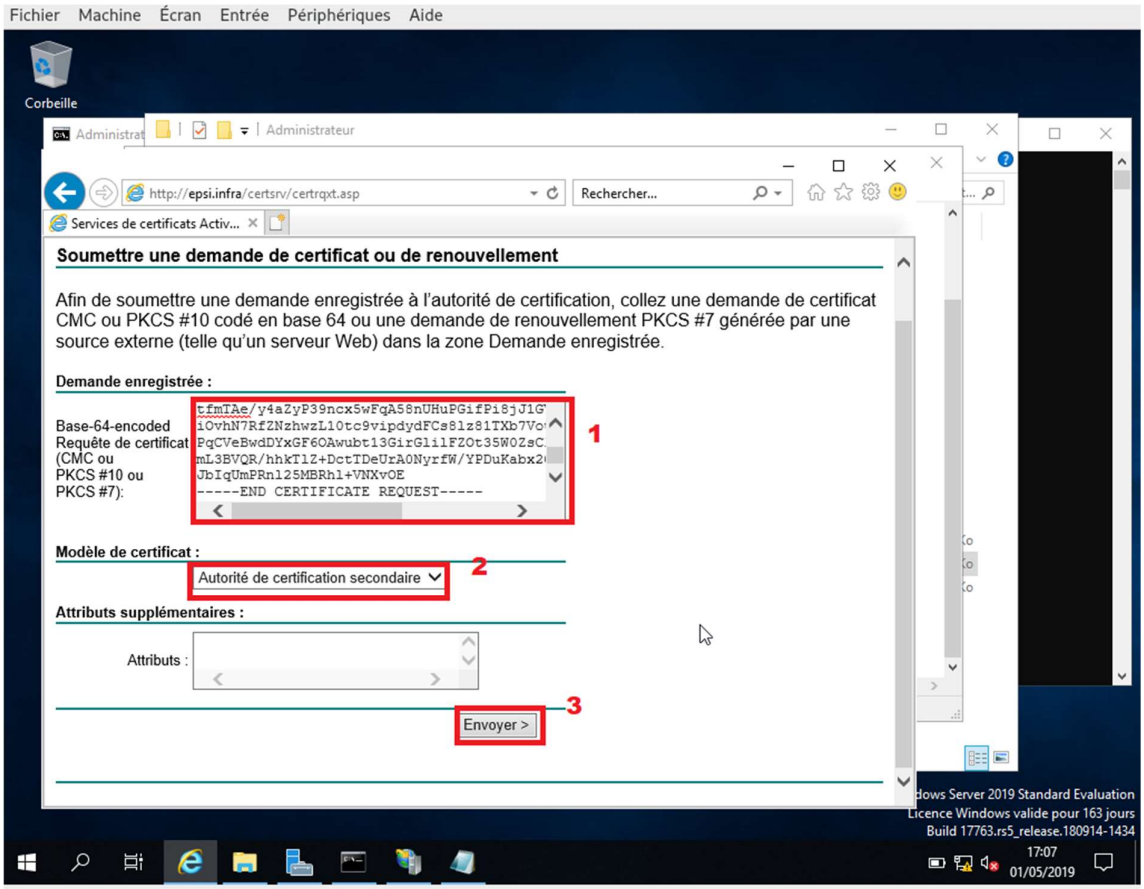
Après cela, vous arriverez sur la page suivante et cliquez sur « Demande de certificat avancée »


Gestionnaire de serveur
Gestionnaire de serveur ‣ IIS
Gérer
Outils
Afficher
Aide
SERVEURS
TÂCHES
http://epsi.infra/certsrv/certrqus.asp
Rechercher...
Services de certificats Activ...
Services de certificats Microsoft Active Directory -- epsi-EPSI-SERVER-CA
Accueil
Demander un certificat
Sélectionnez le type de certificat :
Certificat utilisateur
Ou, soumettre un demande de certificat avancée.
Activation de Windows
00431-10000-00000-AA04
TÂCHES
17:06
01/05/2019

Puis sur « Soumettez une demande de certificat en utilisant un fichier [...] en base 64 »



Collez votre certificat en Base64 dans le champs « Base-64 encoded » comme sur le 1, sélectionnez « Autorité de certificat secondaire » et valider.



Malheureusement, je n'ai pas réussi à télécharger mon certificat, donc je me suis arrêté là.