Serveur d’autorité de certification

1. Certificat auto signé de l’autorité

Installation d’openssl:

```
#apt install openssl
```

création de l'arborescence utile pour le stockage des clés et certificat généré:

```
#mkdir /etc/ssl/{certs,crl,newcerts,private}
```

Création de la clé privée de l'autorité de certification:

```
#openssl genrsa -des3 -out /etc/ssl/private/ca.key 4096
```

On renseigne une passphrase.

Génération du certificat auto-signé de l'autorité de certification:

```
#openssl req -new -x509 -days 365 -key /etc/ssl/private/ca.key -out
/etc/ssl/ca.crt
```

2. Génération de certificat pour un client

Création de la clé privée du client :

```
#openssl genrsa -out /etc/ssl/private/<nomServ>.key 4096
```

Création de la demande de certificat:

```
#openssl req -new -key /etc/ssl/private/<nomServ>.key -out
/etc/ssl/newcerts/<nomServ>Dem.csr -sha256  [-addext "subjectAltName =
DNS:<nomDNS>"]
```

Informations demandés:

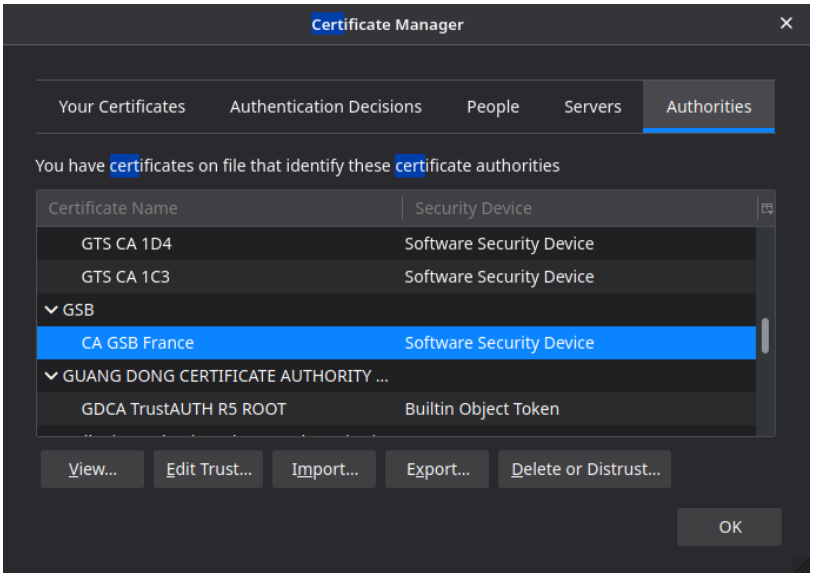
```
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) []: <IP ou nom de domaine si valide>
Email Address []:
```

Production du certificat signé par l'autorité de certification:

```
#openssl x509 -req -days 365 -in /etc/ssl/newcerts/<nomServ>Dem.csr -CA
/etc/ssl/ca.crt -CAkey /etc/ssl/private/ca.key -CAcreateserial -out
/etc/ssl/certs/<nomServ>.crt
```

3. Ajout d'une autorité de certification

Afin de faire confiance à l'autorité de certification, On ajoute son certificat dans les paramètres du navigateur:



Après cela, le certificat des serveurs seront vérifié par le certificat importé.