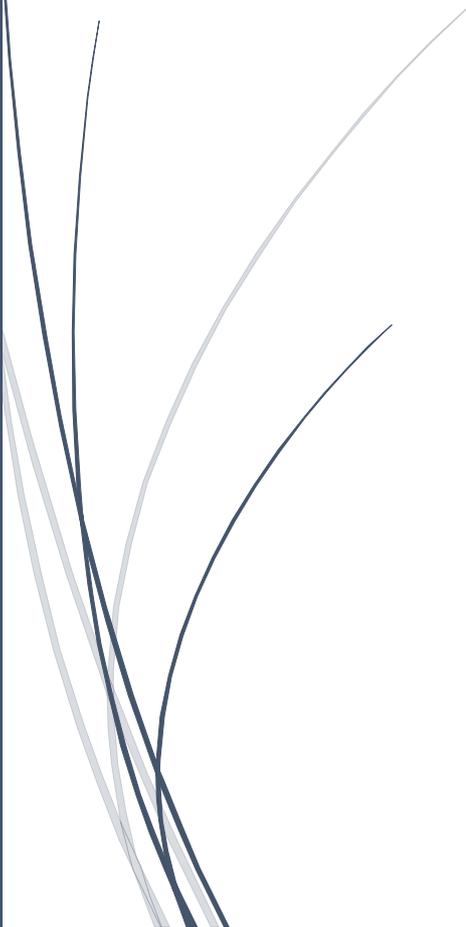




CSI - Utilisation certificat pour
<https>



Steevy PARIS

Introduction

Dans le cadre de la mise en place d'une connexion sécurisée entre un serveur web et ses utilisateurs, l'utilisation d'un certificat SSL/TLS est essentielle. Ce document présente les différentes étapes permettant de générer un certificat SSL auto-signé, de l'installer sur un serveur Apache2, et de configurer le navigateur Firefox pour reconnaître ce certificat comme fiable. L'objectif est d'assurer une communication chiffrée via le protocole HTTPS, même dans un environnement de test ou de développement local. Nous verrons ainsi comment générer la clé privée, créer la demande de signature (CSR), signer le certificat, et configurer Apache2 pour qu'il utilise ces éléments. Une vérification finale sur le navigateur permettra de confirmer la mise en place correcte du certificat.

1. Génération du certificat

Génération d'une clé privée :

➤ `openssl genrsa -des3 -out private.key 3072`

Génération d'un certificat SSL à partir de la clé privée :

➤ `sudo openssl req -new -key private.key -out kali.csr`

Génération d'un crt :

➤ `sudo openssl x509 -req -days 30 -in kali.csr -signkey private.key -out kali.crt`

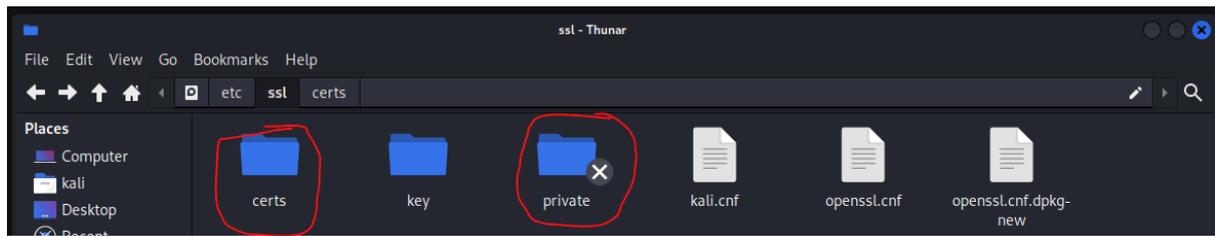
Création du .pem:

➤ `cat moncertificat.key moncertificat.crt
chaine_intermediaire.crt > moncertificat.pem`

1. Mettre le certificat sur un serveur apache2

Mettre le certificat ainsi que la clé priver dans le dossier correspondant

/etc/ssl



Configuration du serveur Apache :

➤ `sudo nano /etc/apache2/sites-available/default-ssl.conf`

Mettre le lien vers les clés ici :

```
SSLCertificateFile      /etc/ssl/certs/kali.crt
SSLCertificateKeyFile   /etc/ssl/private/private.key
```

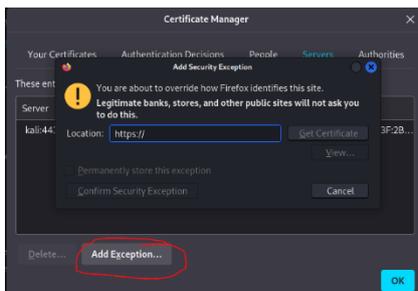
Enfin :

1. `a2enmod ssl`
2. `a2ensite default-ssl`
3. `systemctl reload apache2`
4. `systemctl restart apache2`

Configuration de FireFox:

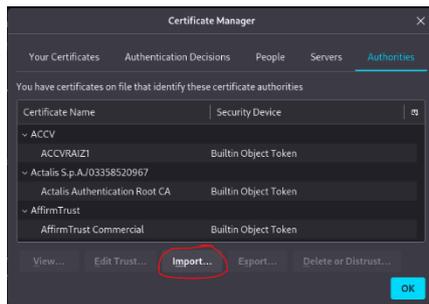
Settings>Private&Sécurité>Certificates>Server

[Mettre l'url du site internet]



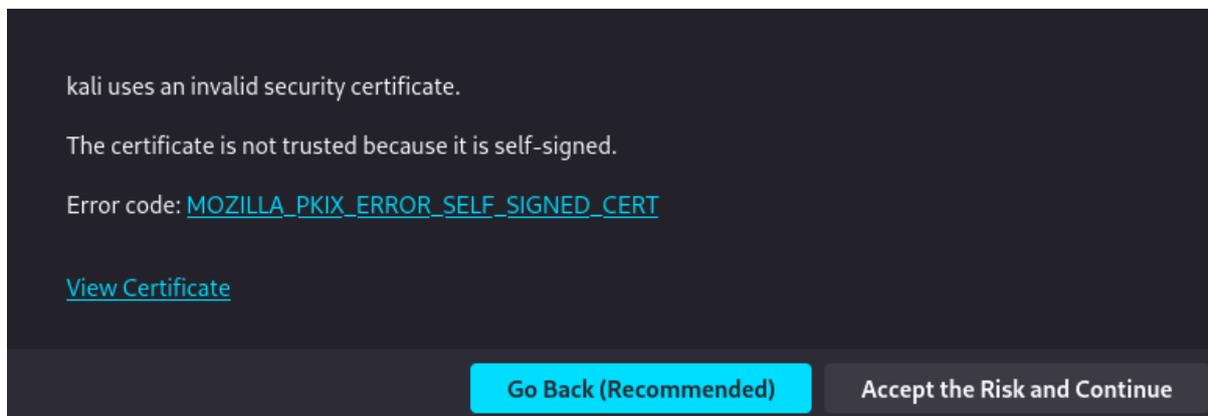
Settings>Private&Sécurité>Certificat

[Mettre le certificat]



Après avoir ajouté le certificat SSL ainsi que la clé privée sur le serveur Apache, nous constatons que le site est accessible en utilisant HTTPS.

Exemple : <https://10.212.209.54/>



Après avoir ajouté le certificat au magasin des certificat on observe que le message d'erreur n'apparaît plus

