Grillet Jean-Dorian (jean-dorian.grillet@ens-rennes.fr)
Farhi-Rivasseau Alice (alice.farhi-rivasseau@ens-rennes.fr)
Bichon-Reynaud Martin (martin.bichon-reynaud@ens-rennes.fr)

Fiche de méthode sur les certificats auto-signés

I. Installation apache et openssl

- Télécharger openSSL : https://openssl-library.org/source/

```
sudo apt update
sudo apt install apache2
sudo a2enmod ssl
sudo systemctl restart apache2
```

II. Création d'un VirtualHost https sous apache

Un virtualhost permet d'accéder à un serveur local avec son nom, et non avec son port, ce qui est nécessaire pour tester le certificat avec un nom de domaine. On crée ici un serveur https à l'adresse `127.0.0.2:443`, et le nom de domaine associé `btsciel_test`. Ces paramètres peuvent bien sûr être changés, auquel cas, il faudra les remplacer dans les commandes suivantes.

A. Configuration du VirtualHost

On commence par créer le fichier de configuration du VirtualHost dans `/etc/apache2/sites-available`:

```
sudo nano /etc/apache2/sites-available/btsciel_test.conf
```

dans lequel on écrit :

```
<VirtualHost 127.0.0.2:443>
   ServerName btsciel_test
   DocumentRoot /var/www/btsciel_test

   SSLEngine on
   SSLCertificateFile /etc/ssl/certs/btsciel_test/apache-selfsigned.crt
   SSLCertificateKeyFile /etc/ssl/private/btsciel_test/apache-selfsigned.key
</VirtualHost>
```

B. Création du certificat

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 \
 -keyout /etc/ssl/private/btsciel_test/apache-selfsigned.key \
 -out /etc/ssl/certs/btsciel_test/apache-selfsigned.crt
```

C. Création d'une page de test

- `sudo mkdir /var/www/btsciel_test`
- `sudo nano /var/www/btsciel_test/index.html`
  et écrire `<h1>it worked!</h1>` (par exemple).

D. Activer la configuration

- `sudo a2ensite btsciel_test.conf`
- `sudo systemctl reload apache2`

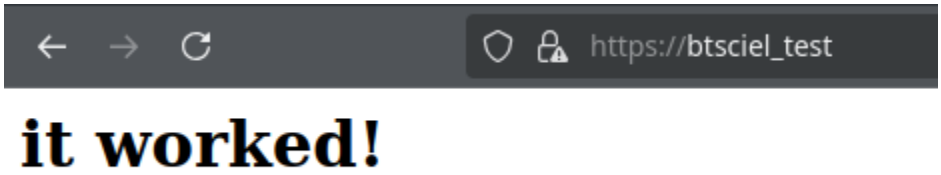
E. Ajouter le domaine aux hosts

- `sudo a2enmod rewrite`
- `sudo ufw allow "Apache Full"`
- `sudo nano /etc/hosts`

```
127.0.0.1   localhost
127.0.0.2   btsciel_test
```

F. Tester

Vous pouvez tester en allant à l'adresse https://btsciel_test. Si tout a fonctionné, vous devez obtenir le cadenas à gauche de votre barre d'adresse.



G. Problèmes courants/débogage

- Si le pare feu bloque apache, et que vous utilisez ufw : `sudo ufw allow "Apache Full"`
- Pour voir les erreurs de configuration apache : `sudo apache2ctl configtest`
- Pour lister les vhosts de Apache : `sudo apache2ctl -t -D DUMP_VHOSTS`
- L'erreur `apache2: Could not reliably determine the server's fully qualified domain name` est normale

III. Création de l'autorité de certification (facultatif)

Cette partie n'est pas nécessaire dans le cas de la génération de certificats auto-signés.

> Le but de cette partie est de créer une nouvelle autorité de certification.

On peut suivre la procédure décrite ici : https://arminreiter.com/2022/01/create-your-own-certificate-authority-ca-using-openssl/.

IV. Sources

[1] Comment créer un certificat SSL auto-signé pour Apache dans Ubuntu 20.04, DigitalOcean. 2020.
[2] How to Set Up Apache Virtual Hosts on Ubuntu, Medium. 2024
[3] What are the differences between .pem, .csr, .key, .crt and other such file extensions?, Crypto Stackexchange. 2021
[4] Create your own Certificate Authority (CA) using OpenSSL, arminreiter. 2022
[5] Public – Private key encryption using OpenSSL, R.I. Pienaar, 2006
[6] Symétrique et asymétrique : pourquoi deux types de chiffrement ?, primx,