Raspberry Pi Apache HTTPS

1 le https

Apache 2.2 intègre en standard le module SSL nécessaire au support du HTTP sécurisé (HTTPS). Très important Il ne faut pas oublier de l'activer avec a2enmod ssl

```
root@RaspberryPi:/var/www# a2enmod ssl
root@RaspberryPi:/var/www# service apache2 restart
root@RaspberryPi:/var/www# a2ensite default-ssl
root@RaspberryPi:/var/www# service apache2 restart
```

SSL offre des fonctions fondamentales nécessaires à la communication sécurisée sur Internet et sur tout réseau TCP/IP :
Une connexion SSL permet de chiffrer l'ensemble des données échangées entre un client et un serveur, ce qui apporte un haut niveau de confidentialité. La confidentialité est importante pour les deux parties dans la plupart des transactions privées.
Le certificat est un ensemble d'informations utilisé par la couche SSL pour réaliser l'authentification d'un service, d'une machine ou d'un utilisateur.
Le certificat contient la clé publique de son détenteur et des informations sur son identité. Le certificat est signé électroniquement par une Autorité de Certification (CA) qui atteste son authenticité. La vérification du certificat peut être effectuée par tout service qui possède la clé publique de l'autorité de certification.
L'installation d'Apache a créé un hôte virtuel par défaut utilisant SSL :

```
root@RaspberryPi:/var/www# ls -l /etc/apache2/sites-available/ | grep -i ssl
-rw-r--r-- 1 root root 7251 août  18 07:35 default-ssl
```

le port 443 est utilisé par défaut

```
root@RaspberryPi:/var/www# cat /etc/apache2/sites-available/default-ssl | grep VirtualHost
```



```
<VirtualHost _default_:443>
</VirtualHost>
```

La directive SSLEngine permet d'activer l'utilisation du protocole SSL/TLS :

```
    #   SSL Engine Switch:
    #   Enable/Disable SSL for this virtual host.
    SSLEngine on
    #   SSLCertificateFile directive is needed.
    SSLCertificateFile    /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
```

La directive SSLCertificateFile indique le chemin du certificat.
la directive SSLCertificateKeyFile indique le chemin de la clé privée.
Le certificat x509 peut être lu avec la commande suivante :

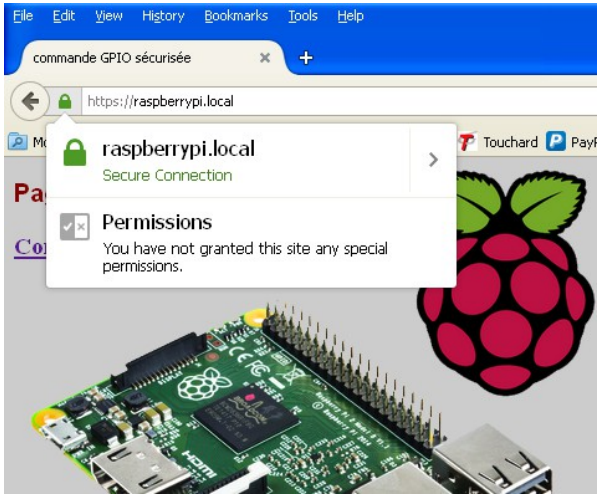
```
openssl  x509  -in  /etc/ssl/certs/ssl-cert-snakeoil.pem   -text

Certificate:
   Data:
      Version: 3 (0x2)
      Serial Number:
         e6:61:ad:4b:4b:b7:e2:6b
   Signature Algorithm: sha256WithRSAEncryption
      Issuer: CN=raspberrypi
      Validity
         Not Before: Oct 12 11:40:14 2015 GMT
         Not After : Oct  9 11:40:14 2025 GMT
      Subject: CN=raspberrypi
      Subject Public Key Info:
         Public Key Algorithm: rsaEncryption
            Public-Key: (2048 bit)
```

Ce certificat est auto-signé : le nom de l'AC signataire du certificat (voir le champ Issuer) est le même que le nom du titulaire du certificat (Subject) : Votre navigateur va vous le faire savoir avec un message d'alerte.

Il suffit maintenant d'activer l'hôte virtuel utilisant SSL, de recharger la configuration d'Apache et de tester l'accès HTTPS :

2 test de l'accès https



Fiche 7 Raspberry Apache https