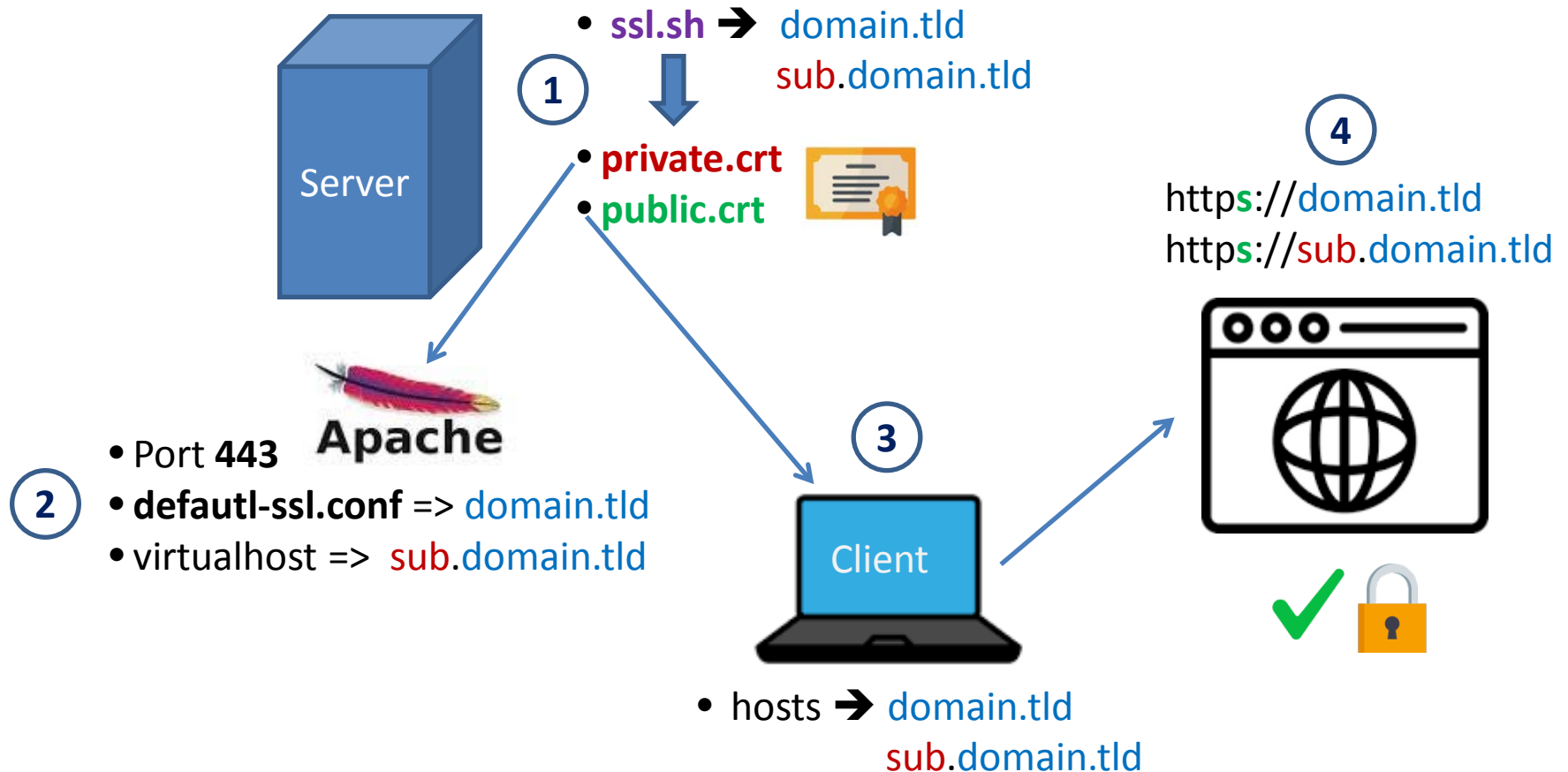
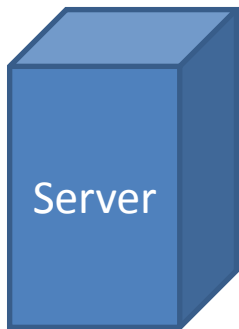


Protocole HTTPS sur un serveur web Apache et sur un client Web



Prérequis

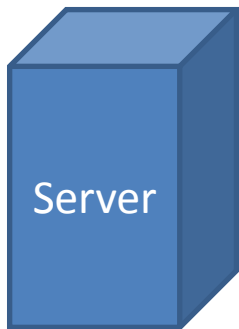


Ubuntu server

- Le fichier **ssl.sh** est disponible dans le dossier RESSOURCES
- Importez ce fichier à la racine du répertoire utilisateur :
 - `/home/ubuntu/ssl.sh`
 - Utilisez FileZilla !
- Donnez des droits d'exécution sur le fichier `ssl.sh` :
 - `chmod +x ./ssl.sh`
- Choisir un nom d'hôte (*par exemple **greta.local***).
- Dans les configurations suivantes, « **domain.tld** » sera remplacé par votre nom d'hôte.
- Dans le cas d'un sous-nom d'hôte (par exemple **www.greta.local**) , sur les configurations suivantes, « **sub.domain.tld** » sera remplacé par le sous-nom d'hôte local.

1

Génération des certificats

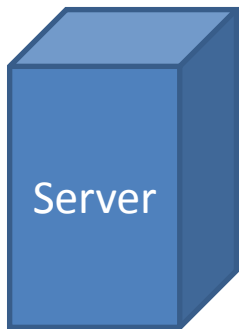


Ubuntu server

```
-> ls ./www
# vos répertoires/fichiers dans c:\www doivent s'afficher !
-> cd && sudo su
-> mkdir /etc/apache2/ssl2
-> ./ssl.sh
    # renseigner le répertoire : /etc/apache2/ssl2
    # renseigner un domaine : domain.tld
    # renseigner un nom : blabla1
    # renseigner une infra : blabla2
# faire une capture après la génération des certificats
-> cd /etc/apache2/ssl2
-> ls
# le fichier « public.crt » doit s'afficher
-> cp public.crt /var/www/html
```

2

Modification de la configuration d'Apache

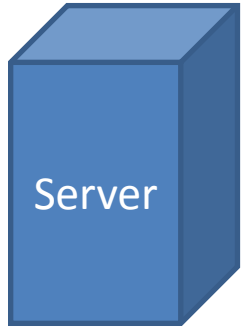


Ubuntu server

```
-> cd /etc/apache2/sites-available  
-> ls  
-> nano default-ssl.conf
```

```
# COMMENTER les lignes (si présentes) :  
#SSLCertificateFile /etc/apache2/ssl/apache.crt  
#SSLCertificateKeyFile /etc/apache2/ssl/apache.key  
#SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem  
#SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key  
  
# Ajouter les autres :  
SSLCertificateFile /etc/apache2/ssl2/server.crt  
SSLCertificateKeyFile /etc/apache2/ssl2/private.key  
SSLCertificateChainFile /etc/apache2/ssl2/server.crt  
  
SSLCACertificatePath /etc/apache2/ssl2/  
SSLCACertificateFile /etc/apache2/ssl2/public.crt
```

2 EN OPTION : Modification de la configuration d'Apache



Ubuntu server

```
#/etc/apache2/sites-available/default-ssl.conf
<IfModule mod_ssl.c>

    <VirtualHost _default_:443>
        ( ... ) /\ voir page précédente pour le contenu de cette partie /\
    </VirtualHost>

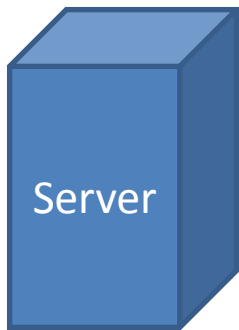
    <VirtualHost *:443>
        ServerName sub.domain.tld
        DocumentRoot /var/www/html

        SSLCertificateFile /etc/apache2/ssl2/domains.crt
        SSLCertificateKeyFile /etc/apache2/ssl2/private.key
        SSLCertificateChainFile /etc/apache2/ssl2/domains.crt
    </VirtualHost>

</IfModule>
```

2

Modification de la configuration d'Apache



Ubuntu server

```
# NANO : enregistrement de default-ssl.conf , et :  
-> a2ensite default-ssl.conf  
-> service apache2 restart
```

3

Importation du certificat sur le client



Windows

```
# Ouvrir le terminal de Windows
```

```
-> certutil -addstore -enterprise -f "Root" C:\www\public.crt
```

```
La signature correspond à la clé publique  
Le certificat "CN=CA_BTSSio, OU=BTSSio, O=Certificat SSL, C=FR" a été ajouté au  
magasin.  
CertUtil: -addstore La commande s'est terminée correctement.
```

3

Importation du certificat sur Firefox



Firefox : paramètres

certi



Général



Accueil



Recherche



Vie privée et sécurité

Résultats de la recherche

Certificats

Lorsqu'un serveur demande votre certificat personnel



En sélectionner un automatiquement



Vous demander à chaque fois



Interroger le répondeur OCSP pour confirmer la validité de vos certificats

certi

Afficher les certificats...

Périphériques de sécurité...

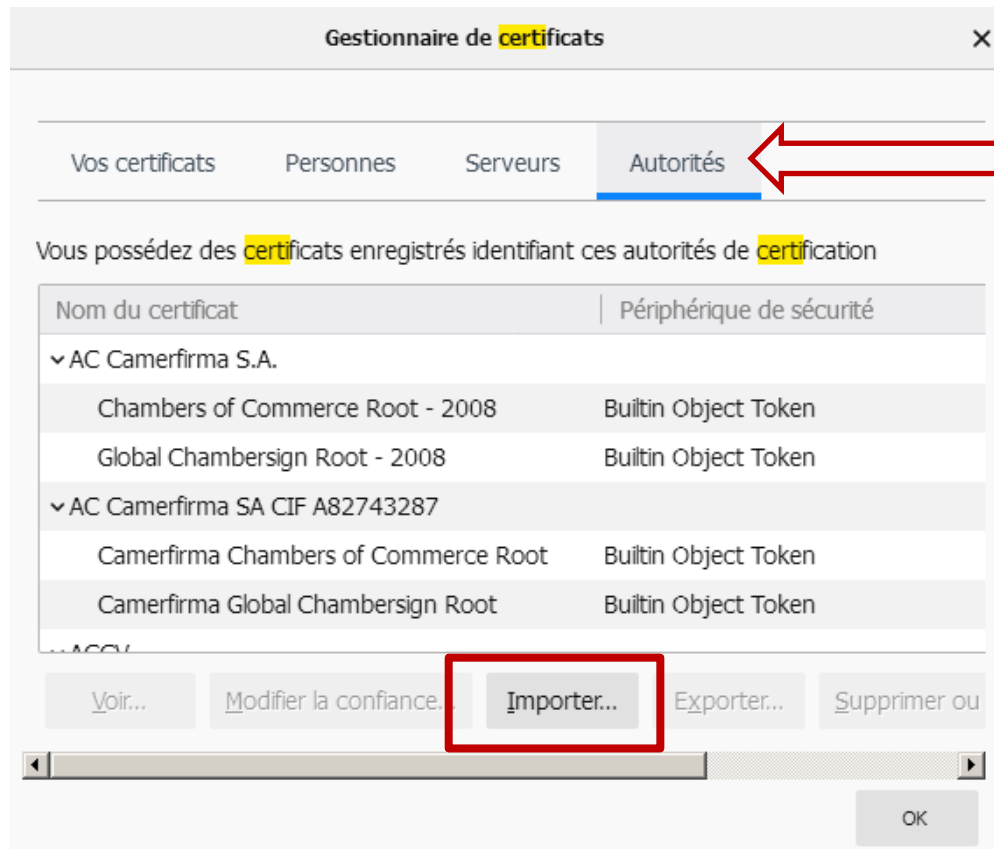
3

Importation du certificat sur Firefox



Firefox : paramètres

- importer « **public.crt** »
- cocher pour « **Site Web** »



3

Modification du fichier « hosts »



Windows

Edition de :

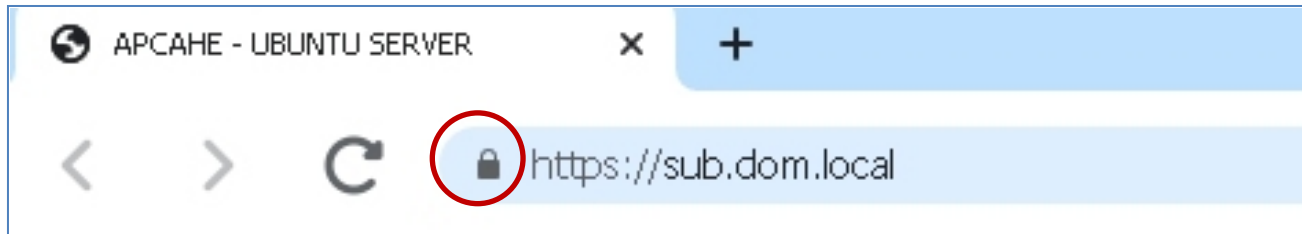
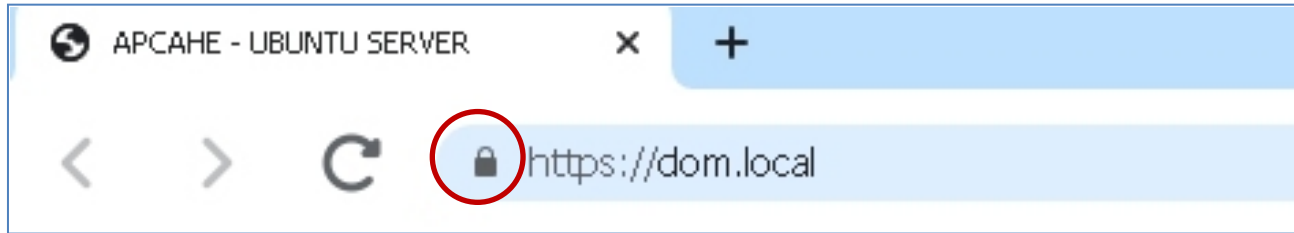
C:\WINDOWS\system32\drivers\etc**hosts**

domain.tld	172.16.120.xxx
sub.domain.tld	172.16.120.xxx

4

test sur un navigateur

- Firefox
- Chromium
- Edge



***Fermez et videz le cache du navigateur s'il est déjà ouvert !
Un hard reboot est parfois requis !***