

## Tomcat en SSL

### Créer le certificat

On utilise ici l'utilitaire **keytool** de java. Vérifier qu'il est accessible sur la ligne de commande. Si ce n'est pas le cas, ajouter le path dans les variables d'environnement.

On se place dans le répertoire de Tomcat.

Ensuite on tape :

```
keytool -genkey -keyalg RSA -storetype PKCS12  
-keystore keystore -keysize 2048
```

Taper **123456** comme mot de passe.

Pour Unité organisationnelle et Entreprise, on met Afpa.

Code pays : FR.

On répond oui à la fin.

On voit qu'on a un fichier **keystore** dans le répertoire. C'est le certificat.

### Utiliser le certificat

Aller dans le répertoire conf et ajouter dans **server.xml**, au niveau des autres Connector, l'entrée suivante :

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http1NioProtocol"  
maxThreads="150" SSLEnabled="true" scheme="https" secure="true"  
keystoreFile="C:/softs/apache-tomcat-8.0.53/keystore" keystorePass="123456"  
clientAuth="false" sslProtocol="TLS" />
```

**(Attention à modifier le path pour adapter à votre machine)**

Sauvegarder **server.xml**

### Vérifier

Arrêter le Tomcat dans Eclipse si besoin est.

Lancer le Tomcat en ligne de commande

Dans Firefox ou Chrome, tapez dans la barre d'url :

<https://localhost:8443>

Là, le browser va vous dire que le certificat n'est pas sûr. Aller dans « Avancé » et autoriser ce certificat.

Au final, la mire de Tomcat va apparaître.

TOUT MARCHE BIEN.

Arrêter maintenant Tomcat en ligne de commande.