Signature de code / signature d'un JAR

Page de documentation plus nécessaire à esup-sgc-client

Depuis sa version 2.0, esup-sgc-client ne demande plus à ce que les jar soient signés ; en effet l'usage de Java Web Start (JNLP) a été abandonné puisque cette technologie est dépréciée en Java.

Le(s) client(s) esup-sgc correspondent maintenant à des jar présentant des applications Java. Actuellement, ces jars doivent être packagés par les établissements eux-mêmes.

renater / digicert

Au travers de Renater, notre communauté a la possibilité d'obtenir un certificat de signature de code via https://www.digicert.com/secure/ .

Ce certificat est individuel, il est donné à une personne pour signer du code, cette personne peut demander un tel certificat via https://www.digicert.com/secure/ **en passant par son RSSI**.

Plus d'information sur le site de Renater autour de l'accès à ce service : https://services.renater.fr/tcs/certcentral/orders/request-certificate/request-cs

Cette documentation reprend finalement en partie la documentation donnée ici par digicert : https://www.digicert.com/code-signing/java-code-signing-guide.htm

La signature du jar est appelée dans les tâches maven sign (intégrée au packaging mvn package). Dans le fichier pom.xml de votre application (esup-sgc-client, esup-sgc-client-zxp3, ...) vous trouvez une configuration de ce type :

```
<configuration>
  <keystore>src/etc/keystore.jks</keystore>
  <alias>server</alias>
  <storepass>leocarte</storepass>
  <keypass>leocarte</keypass>
 </configuration>
```

Le fichier src/etc/keystore.jks doit contenir un certificat de signature de code.

Pour le constituer un certain nombre d'étapes sont à réaliser.

Vous devez premièrement générer un keystore :

```
 keytool -genkeypair -dname "CN=Université de Rouen, L=MONT SAINT AIGNAN, C=FR" -alias mykeystore -keyalg RSA -keysize 2048 -keystore keystore.jks -validity 3650 -storetype JCEKS
```

Ici, et pour l'exemple, on tapera esupesup comme mot de passe à chaque fois.

Vous générez ensuite un CSR :

```
keytool -certreq -alias mykeystore -keyalg RSA -file keystore.csr -keystore keystore.jks -storetype JCEKS
```

Une fois le CSR obtenu et depuis l'interface digicert https://www.digicert.com/secure/ (dont vous aurez préalablement demandé un accès à votre RSSI) vous pouvez demander un 'Code Signing Certificate'.

Cette demande se fait par formulaire dans lequel on vous demande le CSR préalablement généré (contenu du fichier keystore.csr dans notre exmple ici).

Une fois obtenu/validé, vous pouvez télécharger le certificat (ou plutôt les certificats) sous forme d'un (seul) fichier p7b (Best format for Sun Java).

Vous importez ensuite ce fichier dans votre keystore :

```
keytool -importcert -alias mykeystore -trustcacerts -file universit___de_rouen.p7b -keystore keystore.jks -storetype JCEKS
```

Si vous avez suivi ces instructions, votre fichier pom.xml doit finalement être modifié pour avoir cette configuration :

```
<configuration>
  <keystore>src/etc/keystore.jks</keystore>
  <alias>mykeystore</alias>
  <storepass>esupesup</storepass>
  <keypass>esupesup</keypass>
  <storetype>JCEKS</storetype>
</configuration>
```