Secure Socket Layer în *jetty*

Transmisia utilizând *Secure Socket Layer* - SSL (mai nou *Transport Layer Security* - TLS) înseamnă criptarea datelor care circulă între client şi server.

Realizarea presupune

1. Generarea unui fişier de configurare, *xyz_ssl.xml,* care se va plasa în catalogul %JETTY_HOME%etc.

```
<!DOCTYPE Configure PUBLIC "-//Jetty//Configure//EN"
          "http://www.eclipse.org/jetty/configure_9_3.dtd">
<!-- Tweak SsslContextFactory Includes / Excludes -->
<Configure id="sslContextFactory"
       class="org.eclipse.jetty.util.ssl.SslContextFactory">
  <!-- Mitigate SLOTH Attack -->
  <Call name="addExcludeCipherSuites">
    <Arg>
      <Array type="String">
        <Item>.*_RSA_.*SHA1$</Item>
        <Item>.*_RSA_.*SHA$</Item>
        <Item>.*_RSA_.*MD5$</Item>
      </Array>
    </Arg>
  </Call>
</Configure>
```

   Secvenţa *xyz* din denumirea fişierului poate fi modificată dar trebuie să fie diferită de *jetty.*

2. Generarea unui certificat de securitate cu utilitarul `keytool` din distribuţia Java, de exemplu

```
keytool -genkey -alias jetty -keyalg RSA
  -keystore {cale}/keystore
  -dname "cn=SE, ou=cs, o=unitbv, l=brasov, c=RO"
  -keypass 1q2w3e -storepass 1q2w3e
```

   Parametrul `keystore` fixează locaţia şi denumirea fişierului certificatului de securitate.

   Se definesc două parole

   - `keypass` parola certificatului de securitate;
   - `storepass` parola de protecţie a locaţiei certificatului de securitate.

   Parametrul *cale* desemnează calea către catalogul unde în care se crează fişierul *keystore* - certificatul de securitate. Certificatul de securitate se mută în catalogul `JETTY_HOME\etc.`

3. Criptarea parolelor

```
java -cp %JETTY_HOME%\lib\jetty-util-9.3.11.v20160721.jar
  org.eclipse.jetty.util.security.Password <parola>
```

Pentru exemplul certificatului generat mai sus, pentru *parola=1q2w3e* rezultatul este *OBF:1irv1lml1mii1mmc1lj51iur*

4. Completarea fişierului %JETTY_HOME%/start.ini cu secvenţa

```
# Module: https
--module=https
etc/xyz-ssl.xml

# Module: ssl
--module=ssl
jetty.secure.port=8443
jetty.keystore=etc/keystore
jetty.truststore=etc/keystore
jetty.keystore.password=OBF:1irv1lml1mii1mmc1lj51iur
#jetty.keymanager.password=OBF:1irv1lml1mii1mmc1lj51iur
jetty.truststore.password=OBF:1irv1lml1mii1mmc1lj51iur
```

5. După lansarea serverului Web apelarea poate fi

```
https://localhost:8443
http://localhost:8080
```