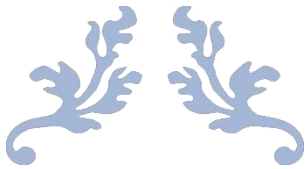


CONFIGURACIÓN HTTPS

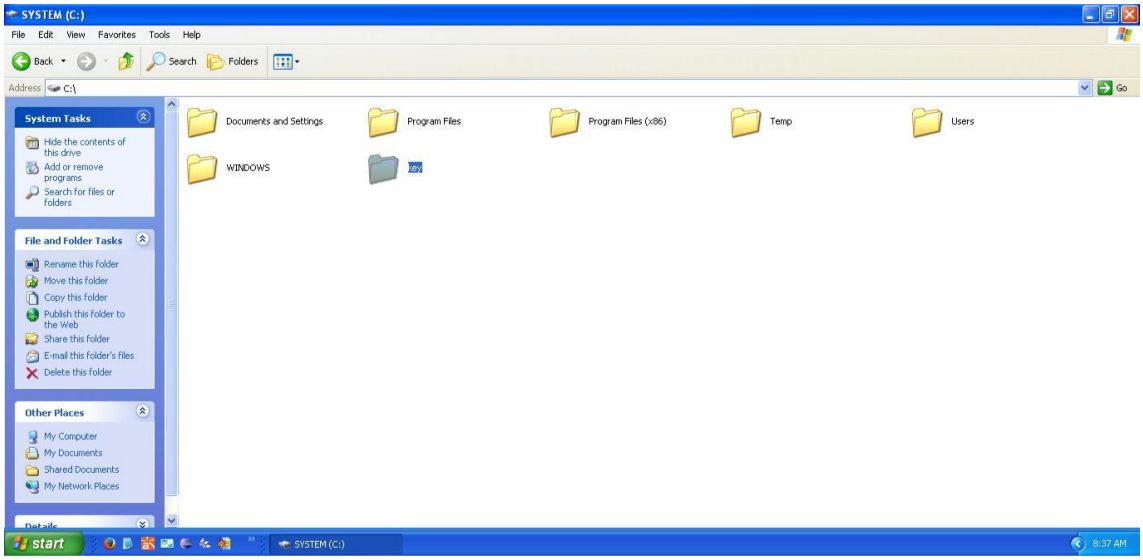
D05

6 DE JUNIO DE 2019

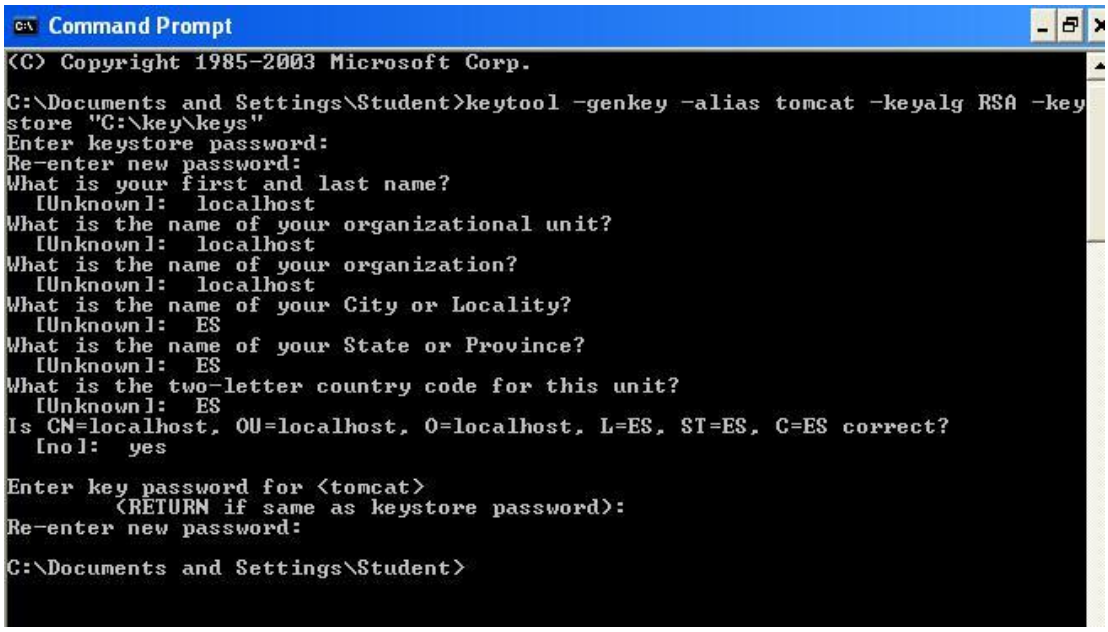
GRUPO 11

Configuración en Developer:

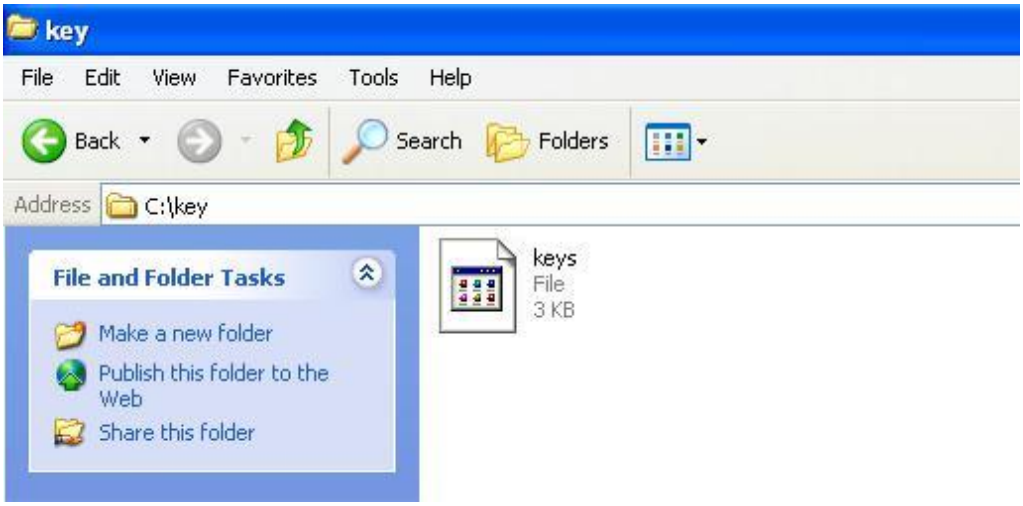
1. Creamos una carpeta en “C:\” llamada key, que será donde generaremos nuestro almacén de claves.



2. Abrimos el terminal cmd y ejecutamos el comando: ***keytool -genkey -alias tomcat -keyalg RSA -keystore "C:\key\keys"*** y completamos con:
    - Contraseña: acmemadruga
    - localhost
    - localhost
    - localhost
    - ES
    - ES
    - ES
    - Yes
    - acmemadruga

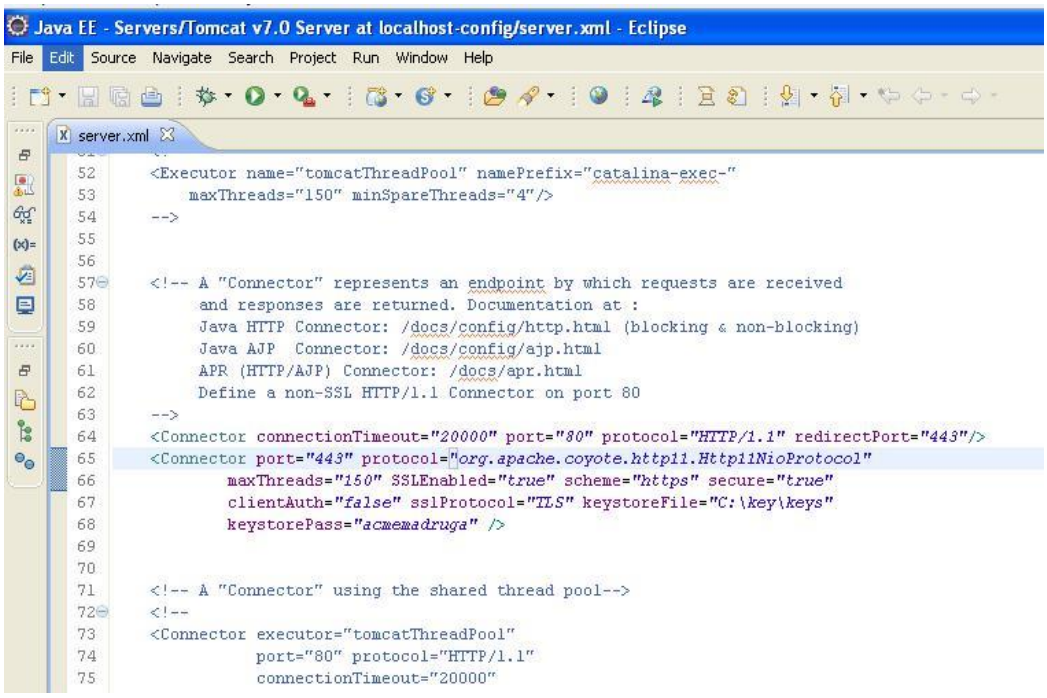


Y se generará nuestro almacén de claves:



3. Ahora procederemos a configurar el tomcat por lo que nos vamos a server.xml y añadimos:

- ***<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="C:\key\keys" keystorePass="acmemadruga" />***

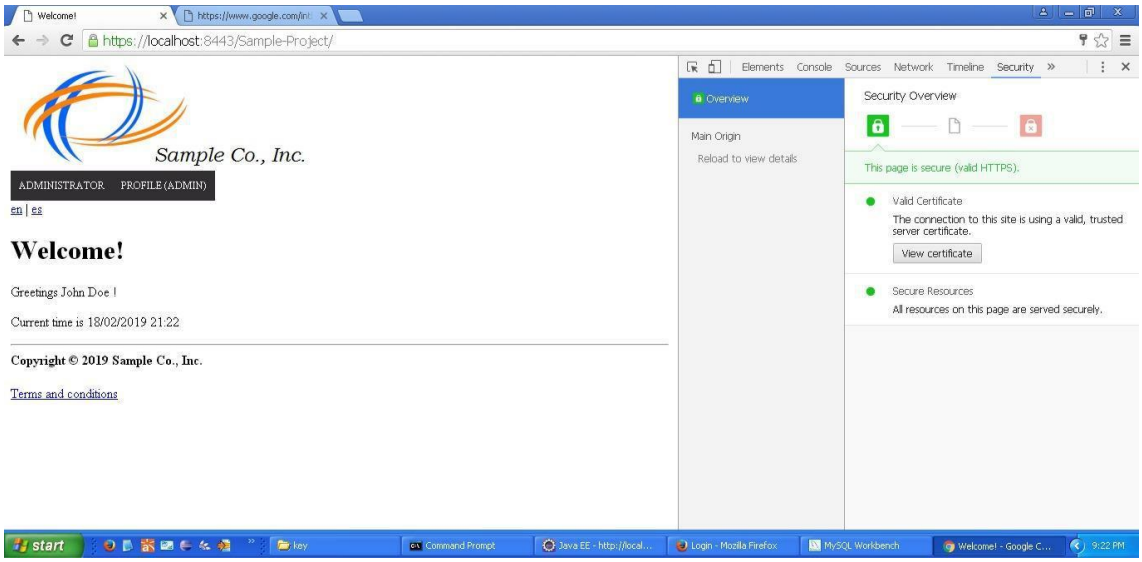


Teniendo en cuenta que ambos puertos sean “443” ya que con el puerto “8443” hemos tenido problemas.

4. El siguiente paso sería irnos a security.xml y añadir ***requires-channel="https".***

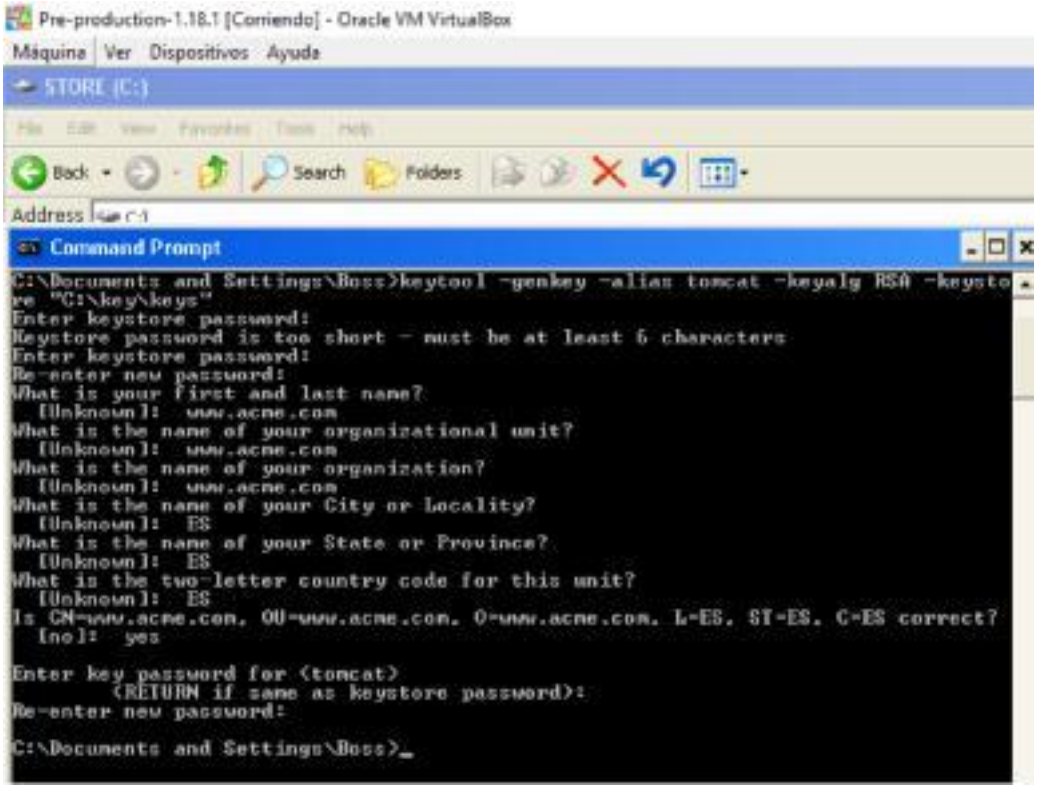
```
98
99      <security:intercept-url pattern="/message/administrator/**" access="hasRole('ADMIN')" />
100     <security:intercept-url pattern="/message/administrator,auditor,customer,nutritionist,trainer/**" access="isAuthenticated()" />
101
102     <security:intercept-url pattern="/miscellaneousRecord/trainer/**" access="hasRole('TRAINER')" />
103     <security:intercept-url pattern="/miscellaneousRecord/**" access="isAuthenticated()" />
104
105     <security:intercept-url pattern="/workingOut/trainer/**" access="hasRole('TRAINER')" />
106     <security:intercept-url pattern="/workingOut/customer/**" access="hasRole('CUSTOMER')" />
107     <security:intercept-url pattern="/workingOut/customer,trainer/**" access="hasAnyRole('CUSTOMER','TRAINER')" />
108
109     <security:intercept-url pattern="/creditCard/customer/**" access="hasRole('CUSTOMER')" />
110
111     <security:intercept-url pattern="/exportData/administrator,auditor,customer,nutritionist,trainer/export.do" access="isAuthenticated()'
112
113     <security:intercept-url pattern="/session/trainer/**" access="hasRole('TRAINER')" />
114
115     <security:intercept-url pattern="/error.do" access="permitAll" />
116
117     <security:intercept-url pattern="/**" access="hasRole('NONE')" requires-channel="https" />
118
119
120     <security:form-login
121         login-page="/security/login.do"
122         password-parameter="password"
123         username-parameter="username"
124         authentication-failure-url="/security/loginFailure.do" />
125
126     <security:logout
127         logout-success-url="/"
128         invalidate-session="true" />
129   </security:http>
```

5. Por último, arrancamos tomcat y comprobamos que use protocolo https.



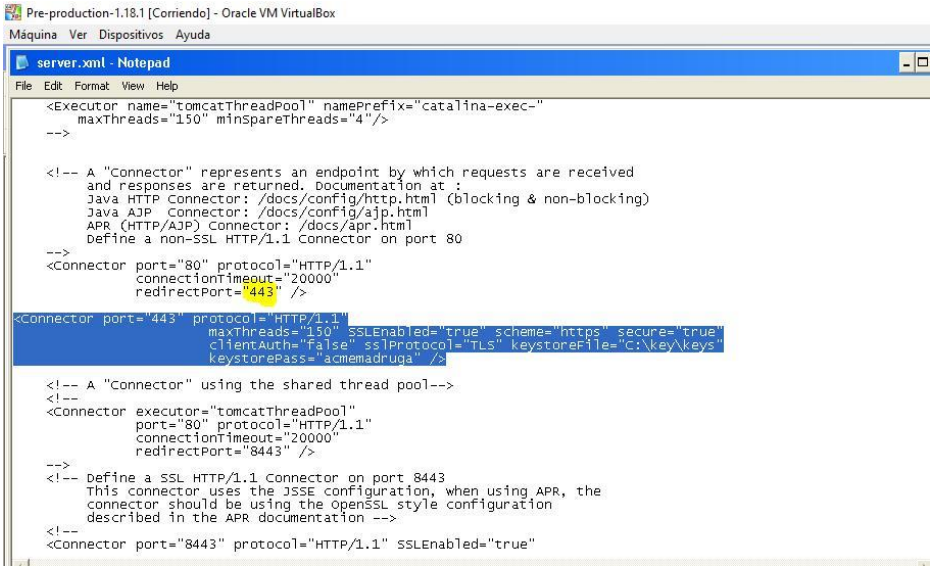
Configuración en Pre-Production:

1. Creamos la carpeta key al igual que en developer.
2. Generamos las claves en la carpeta key de la misma forma que en developer con la diferencia de que en vez de localhost pondremos www.acme.com

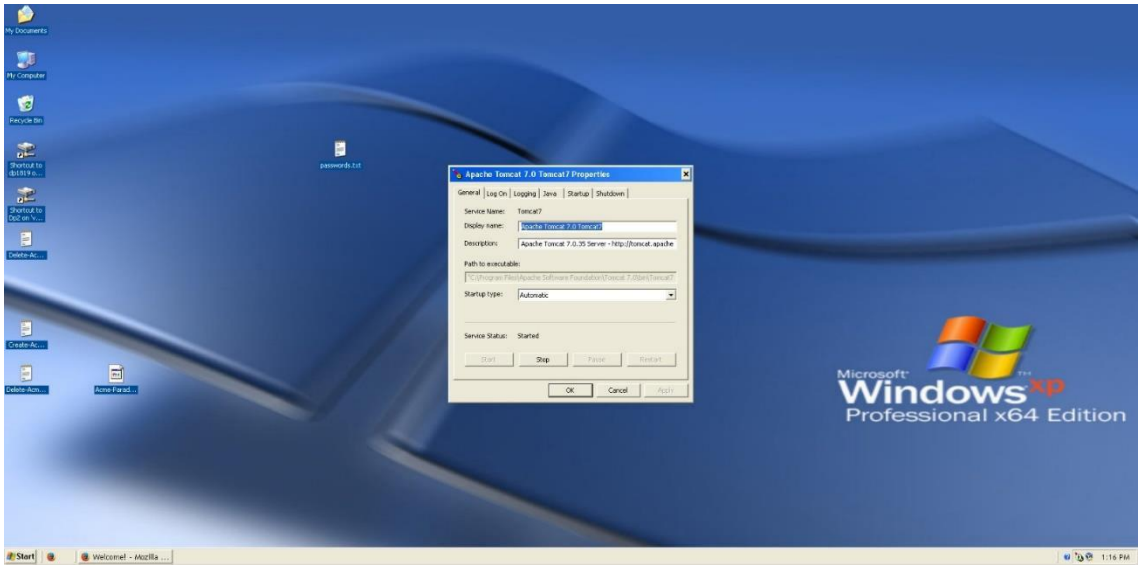


3. Para configurar Tomcat nos iremos al archivo server.xml que se encuentra en ***C:\Program Files\Apache Software Foundation\Tomcat 7.0\conf*** y añadiremos la siguiente información, cambiando de nuevo el puerto a “443” para evitar errores:

    - ***<Connector port="443" protocol="HTTP/1.1" maxThreads="150" SSLEnabled="true" scheme="https" secure="true" clientAuth="false" sslProtocol="TLS" keystoreFile="C:\key\keys" keystorePass="acmemadruga" />***



4. Por último, reiniciamos el servidor Tomcat desde la aplicación “Monitor Tomcat”



5. Y desplegamos nuestro proyecto como se indicó en la última lección de la asignatura DP1 y accedemos con la url www.acme.com: