Cómo acceder a la información

Modelo de seguridad de los Servicios Web de CEO.

1. Conexión SSL

La conexión a los servicios web de CEO es segura, es decir mediante SSL, por lo tanto habrá que indicar al cliente del servicio que confíe en el certificado de la OEPM. Para clientes tipo .NET, el certificado se obtiene a través del Microsoft Internet Explorer, por lo que bastará con acceder una vez con este navegador a la URL del servicio web. Para clientes JAVA, es necesario importar dentro del repositorio de certificados de confianza "cacerts" el certificado utilizado por la OEPM. Para ello, lo más sencillo es seguir los siguientes pasos:

a) Acceder con un navegador (Internet Explorer, Mozilla Firerox, etc) a la url del servicio web.
b) Una vez accedido, exportar el certificado de la OEPM al disco duro. Por ejemplo, en Mozilla Firefox,
Menu Herramientas→Opciones→Avanzado→Cifrado→Ver Certificados →Servidores.
c) Exportar el certificado *.OEPM.ES como certificado X.509.
d) Importarlo en el repositorio de claves de confianza de la máquina virtual cliente:

```
keytool
-import
-keystore
$JAVA_HOME/jre/lib/security/cacerts
-file
$RUTA_CERTIFICADO_EXPORTADO/oepm.cer
-alias
consultas2.oepm.es
```

e) A veces es necesario añadir la ruta del repositorio como opción de java:

```
-Djavax.net.ssl.trustStore=
/$JAVA_HOME/jre/lib/security/cacerts
```