Cómo acceder a la información

Modelo de seguridad de los servicios web de INVENES.

1. Conexión SSL.

La conexión a los servicios web de INVENES 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 maquina virtual cliente:

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

2. Token de acceso.

Todo usuario que desee hacer uso de los servicios web de INVENES debe solicitar un usuario y contraseña cumplimentando el correspondiente **formulario anexo**. El personal de la OEPM se pondrá en contacto con el usuario para facilitarle los datos solicitados.

Una vez recibidos los datos, siempre que se quiera utilizar el servicio de búsqueda, el primer paso a dar es solicitar un Token de acceso valido para el día mediante la función doLogin(…). Este Token de acceso, de formato cadena, tendrá la estructura <IDUSUARIO>XXXXXXXXXX, se debe pasar como primer parámetro de las funciones getBases(…), getSearchFields(…) y doSearch(…).

El Token tiene una duración máxima de 8 horas, transcurrido este tiempo, será necesario solicitar un nuevo Token realizando una nueva llamada a la función doLogin(…).