

Guía de Servicio Web de generación de la guía  
de transporte para empresas  
fabricantes/importadores de máquinas recreativas y  
de azar de la Comunitat Valenciana.

Identificador del proyecto: JOCER

Identificador del Documento: GuiaDesarrollo

Versión: 01.01

Fecha de entrega: 04/01/2013

## Índice.

|  |           |
|--|-----------|
| <b>1 MOTIVACIÓN.....</b>   | <b>3</b>  |
| <b>2 CARACTERÍSTICAS GENERALES DEL SERVICIO.....</b>                               | <b>4</b>  |
| <b>3 PROCESO DE DESARROLLO Y PRUEBAS.....</b>                                      | <b>11</b> |
| <b>4 PROCESO DE PASO A PRODUCCIÓN.....</b>   | <b>18</b> |
| <b>5 ANEXO I: PORTECLE: GESTIÓN DE KEYSTORES.....</b>                              | <b>20</b> |
| <b>6 ANEXO II. PRUEBA Y DEPURACIÓN DEL SERVICIO MEDIANTE SOAPUI.<br/>.....</b>     | <b>22</b> |
| <b>7 ANEXO III. OBTENCIÓN DEL NÚMERO DE SERIE DEL CERTIFICADO<br/>DIGITAL.....</b> | <b>29</b> |

## **1 Motivación**

Con motivo de la implantación del proyecto JOC-ER, (tramitación telemática de los expedientes de juego administrativo), se detecta la necesidad de ofertar a las empresas fabricantes/importadoras de máquinas recreativas y de azar, la posibilidad de integrar con sus sistemas la generación de la guía de circulación emitida por los fabricantes, al producirse la venta de una máquina a una empresa operadora que va a operar dentro de la comunidad.

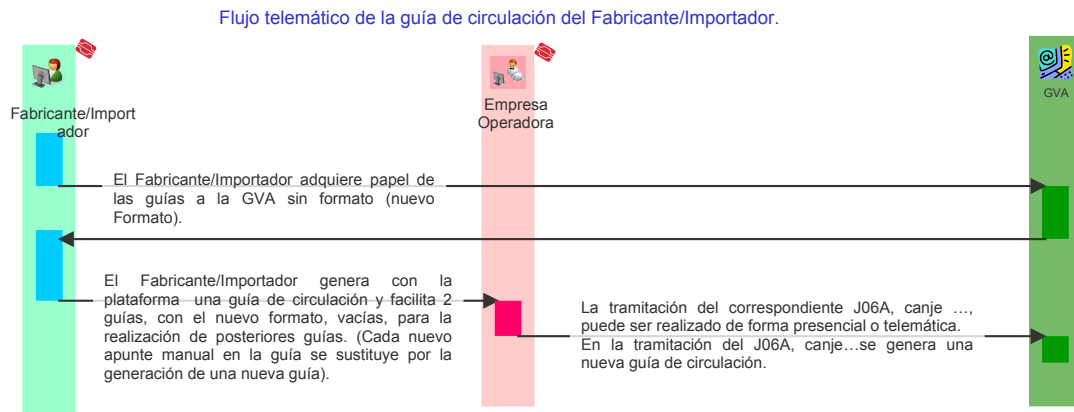
Aunque existe la posibilidad en la que los fabricantes/importadores puedan emitir dicha guía mediante la plataforma de tramitación JOC-ER, se oferta la posibilidad de obtener dicha guía mediante la comunicación máquina a máquina, sin necesidad de intervención humana, con el fin de automatizar dichos procesos productivos.

Para ello la Consellería de Hacienda y Administración Pública (a partir de ahora CHAP), ofrecerá dicha posibilidad mediante un servicio web (a partir de ahora WS).

Este WS permitirá a las empresas fabricantes/importadoras acreditadas a tal efecto, emitir las guías de circulación de las máquinas cuyos modelos estén homologados dentro del ámbito de la Comunidad, de forma desasistida.

## 2 Características generales del servicio.

### 2.1 Esquema de funcionamiento actual mediante JOC-ER.



1

En la aplicación JOC-ER, desde el punto de vista del fabricante, se traduce en:

Una vez conectado al sistema, el usuario...

**Paso 1:** Seleccionamos el modelo del registro de modelos. Rellenamos la información de los contadores.

**Paso 2:** Introducimos el número de papel de la FNMT sobre el que se imprimirá la guía.

**Paso 3:** Firma el fabricante/importador e imprime.

**DATOS DEL PRODUCTO SELECCIONADO**

|  |   |           |
|--|---|-----------|
| RAZÓN SOCIAL DEL FABRICANTE:                     | Nº REGISTRO DEL FABRICANTE DE MÁQUINAS RECREATIVAS Y AZAR EN LA CEDE: | V-41      |
| PROVINCIA DEL FABRICANTE:                        | LOCALIDAD DEL FABRICANTE:   | CATARROJA |
| MODELO DE LA MÁQUINA:                            | TIPO DE LA MÁQUINA:   | B         |
| Nº REGISTRO EN EL REGISTRO DE MODELOS DE TRAMIT: | NÚMERO DE SERIE DE LA MÁQUINA:  |           |
| SERIE DE LA MÁQUINA:                             | NÚMERO DE SERIE DEL CONTADOR:   |           |
| SERIE DEL CONTADOR:                              |   |           |
| MODELO DEL CONTADOR:                             |   |           |

Continuar

**EXPEDIENTE: (6175) - GUÍA DE CIRCULACIÓN**

Fase: DATOS DE LA GUÍA DE CIRCULACIÓN

Estas son las tareas de la fase del expediente en la que se encuentra. Para volver a una ya realizada basta con seleccionarla.

DATOS DE LA GUÍA DE CIRCULACIÓN ▶ RECUPERACIÓN DEL NÚMERO DE PAPEL

**RECUPERACIÓN DEL NÚMERO DE PAPEL**

NÚMERO DE PAPEL:

16000

Continuar

**GUÍA DE CIRCULACIÓN DE MÁQUINAS RECREATIVAS TIPO B**

|                    |               |                      |                  |
|--------------------|---------------|----------------------|------------------|
| Modelo/Modelo:     | AMERICAN POOL | Nº Registro/Regist.: | JOC0000000000358 |
| Tipos/Tipos:       | B-2304--      | Nº Regist./Regist.:  | B96200449        |
| Contador/Contador: | 10            | Localidad/Localidad: | CATARROJA        |
| Modelo/Modelo:     | 10            | Provincia/Provincia: | VALENCIA         |
| Serie/Serie:       | 10            |                      |                  |

En calidad de: INTERESADA

Nº Identidad: 2806990C

Firma: GUARDA GUARDIA GONZALEZ

Estado: RESIDENTE

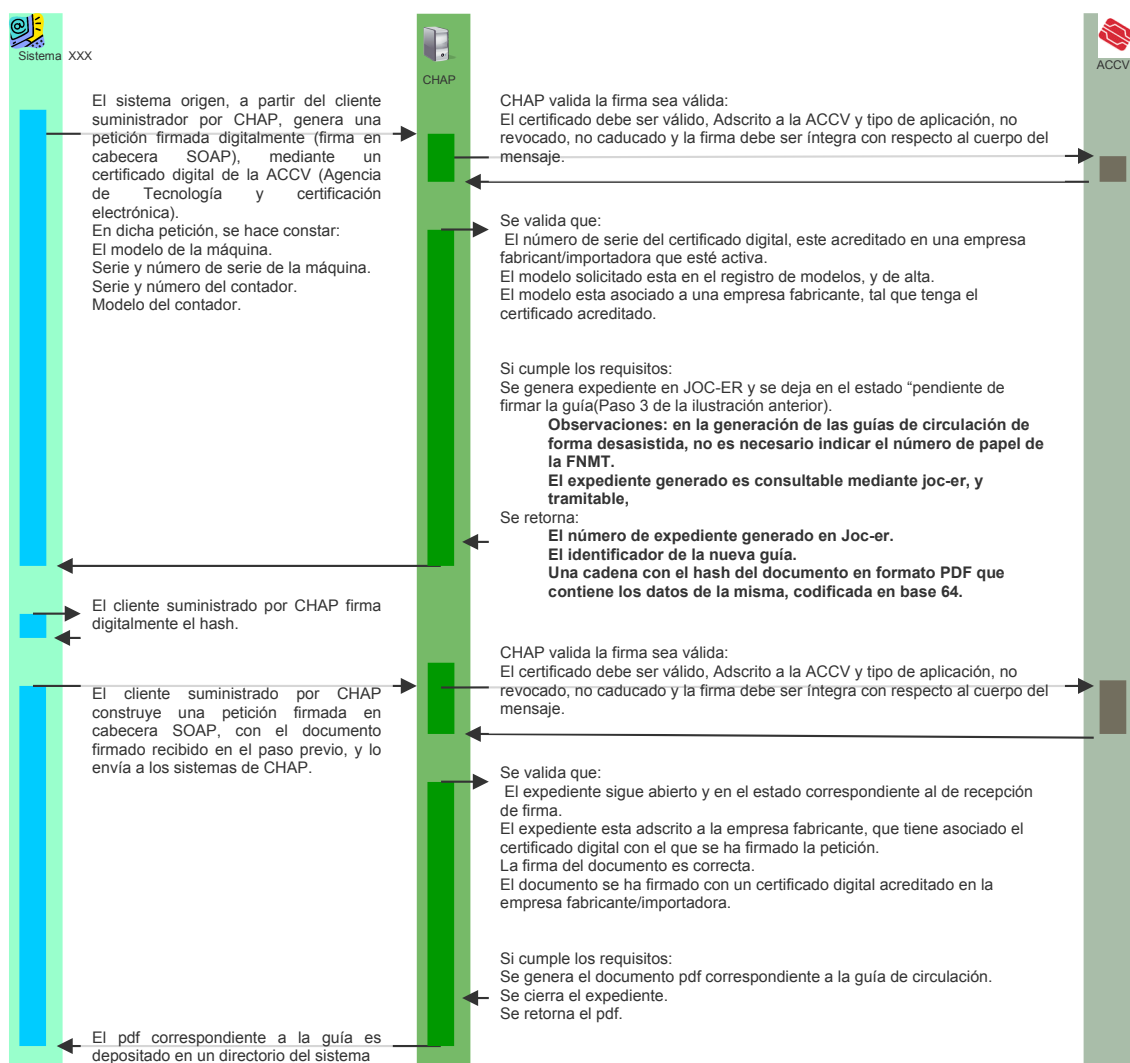
1

Esto implica que un usuario de la empresa fabricante/importadora acreditada en JOC-ER, debe acceder y realizar la tramitación anteriormente mostrada.

Este hecho impide la automatización del proceso, debido a la necesaria intervención humana.

## 2.2 Esquema de funcionamiento general del servicio.

Visión general del funcionamiento del servicio web.



## 2.3 Características generales.

### **2.3.1 Cliente.**

CHAP suministra un cliente de invocación, que realiza la construcción de la petición, la invocación de la misma, así como la recepción del resultado.

- El cliente esta realizado con el lenguaje java (versión 1.5 o superior), y más en concreto con Apache CXF, de libre distribución y código abierto, que permite la generación del código cliente y la securización de las llamadas de manera sencilla y eficiente
- El cliente se suministra en formato de un fichero comprimido ZIP, que contiene el proyecto eclipse (versión Indigo) con los fuentes necesarios para su ejecución.

### **2.3.2 Características del WS.**

- Los dos servicios web invocados, (petición inicial, y envío del hash firmado) son síncronos. Se invocan, y tras la invocación se obtiene la respuesta.
- Las peticiones están securizadas mediante la firma del cuerpo del mensaje insertándola en el cabecera de la petición. (Firma en cabecera SOAP). Mediante el algoritmo <http://www.w3c.org/2000/09/xmlsig#rsa-sha1> y <http://www.w3c.org/2001/10/xml-exc-c14n#>.

### **2.3.3 Consideraciones sobre firma electrónica de la guía.**

Como se ha comentado anteriormente, las empresas fabricantes deben firmar la guía de circulación en uno de los pasos del proceso de obtención del documento. En realidad no se firma el documento completo, sino un resumen del mismo (hash) obtenido mediante el algoritmo SHA1. Es por ello, que para facilitar el proceso a los fabricantes, y para agilizar la comunicación con el servicio (el hash del documento es más pequeño que el mismo, por lo que la respuesta del servicio será más rápida), el servicio web devolverá directamente el hash a firmar y no el documento.

Una vez recibido el hash el fabricante procederá a su firma. Existen numerosos formatos de firma. El empleado por la plataforma de tramitación Joc-er, y que será el que se deberá emplear en la firma de las guías por parte de los fabricantes, es el formato CMS detached. Dicho formato es una evolución del PKCS#7 y usa una codificación ASN.1. El calificativo detached hace referencia a que el documento firmado y la propia firma electrónica se almacenan en dos archivos diferentes, por lo que son necesarios ambos para poder realizar su validación.

En el cliente de ejemplo suministrado se proporciona también una API Java para realizar la firma CMS del hash de la guía, basada en la librería BouncyCastle<sup>1</sup>, de libre distribución y código abierto, que proporciona una amplia colección de clases para la implementación de aplicaciones criptográficas.

### 2.3.4 Efectos en JOC-ER

Como se puede observar, en las ilustraciones anteriores, existe una correlación entre la tramitación en JOC-ER y los servicios web invocados. De forma que se puede observar en JOC-ER, los efectos de los servicios web invocados.

Tras la ejecución del primer WS, además de recibir como resultado el hash de la guía a firmar, obtenemos el identificador del expediente generado en JOC-ER.

Si buscamos el expediente generado en JOC-ER, mediante la opción de búsqueda de expedientes, obtendremos que el expediente se encuentra abierto y en el punto de pendiente de la firma por parte del fabricante.

## Búsqueda de expedientes

| Listado de expedientes  |            |   |                         |                 |   |
|---|------------|---|-------------------------|-----------------|---|
|   |            |   | Registros 1 a 10 de 234 |                 |   |
| << < 1 2 3 4 5 6 7 8 9 10 > >>  |            |   |                         |                 |   |
|   | Expediente | Título  | Alta                    | Fase            |   |
|  | (7421)     | GUIA DE CIRCULACIÓN PARA EL FABRICANTE/IMPORTADOR | 10/08/2012              | GENERACION GUIA |  |
|  | (7420)     | GUIA DE CIRCULACIÓN PARA EL FABRICANTE/IMPORTADOR | 10/08/2012              | DATOS GUIA      |  |
|  | (7419)     | GUIA DE CIRCULACIÓN PARA EL FABRICANTE/IMPORTADOR | 10/08/2012              | GENERACION GUIA |  |
|  | (7418)     | GUIA DE CIRCULACIÓN PARA EL FABRICANTE/IMPORTADOR | 10/08/2012              | DATOS GUIA      |  |

Pulsando la lupa:

| EXPEDIENTE: (7421) - GUIA DE CIRCULACIÓN PARA EL FABRICANTE/IMPORTADOR  |            |           |         |            |         |
|---|------------|-----------|---------|------------|---------|
| Fase: GENERACIÓN DE LA GUÍA DE CIRCULACIÓN  |            |           |         |            |         |
| Estas son las tareas de la fase del expediente en la que se encuentra. Para volver a una ya realizada basta con seleccionarla.  |            |           |         |            |         |
| GUIA DE CIRCULACIÓN ► RECEPCIÓN DE LA GUÍA DE CIRCULACIÓN PARA FAB./IMP.  |            |           |         |            |         |
| Recepcion de la documentación   |            |           |         |            |         |
| A continuación, se muestran los documentos correspondientes al procedimiento que el/la interesado/a tiene asociados. Para poder seguir con la tramitación, seleccione el documento que desea consultar. |            |           |         |            |         |
| Nombre  | Fecha      | Inc./Gen. | Estado  | F.firma    | Usuario |
| GUIA DE CIRCULACIÓN PARA EL FABRICANTE/IMPORTADOR   | 10/08/2012 | GENERADO  | FIRMADO | 10/08/2012 | EMPRESA |

Obtenemos el expediente considerado...

<sup>1</sup> <http://www.bouncycastle.org/>

Conselleria de Hacienda y Administración Pública. Generalitat Valenciana - Windows Internet Explorer

http://pruebas.ha.gva.es/jocer/jocer/es/ComprobacionTramitacionCiudadanoAction/comprobarCondicionesAccionesTareaDocumento

WSGC7423

GUÍA DE CIRCULACIÓN DE MÁQUINAS RECREATIVAS TIPO B / GUÍA DE CIRCULACIÓN DE MÁQUINAS RECREATIVAS TIPO B

|   |               |                   |            |
|---|---------------|-------------------|------------|
| DATOS DE LA MÁQUINA (DATOS DE LA MÁQUINA)   | Modelo/Modelo | GOLD STRIKE       |            |
|   | Tipus/Tipo    | Núm. Reg/Núm. Reg | CV-B-200-- |
|   | Serie/Serie   | Núm./Núm.         | 11         |
| DATOS DEL FABRICANTE / DATOS DEL FABRICANTE | Modelo/Modelo | 14                |            |
|   | Serie/Serie   | Número/Número     | 10         |

|                                     |  |                     |           |
|-------------------------------------|--|---------------------|-----------|
| DATOS DE LA GUÍA (DATOS DE LA GUÍA) | Núm. Guía/Núm. Guía                    | JOC000000000803     |           |
|                                     | Nom o raó social/Nombre o razón social |                     |           |
|                                     | Fabricante-1 de pruebas (no desguace)  |                     |           |
|                                     | Núm. Registro/Núm. Registro            | NIF/NIF             | A58699513 |
|                                     | Localitat/Localidad                    | Provincia/Provincia | BARCELONA |

CERTIFIQUE: Que les dades consignades son les registrades en la

| Orden | En calidad de | N. Identidad | Firmante | Estado    |
|-------|---------------|--------------|----------|-----------|
| 1     | INTERESADO/A  | 19890211Z    | asdasd   | PENDIENTE |

Para poder continuar la tramitación del expediente debe firmar el documento electrónicamente con su certificado digital o e-DNI, para ello deberá pulsar el botón de firma. A continuación se le indicarán datos de la firma en una ventana de confirmación. Pulse aceptar e introduzca la clave del certificado si procede. Hecho esto quedará finalizado el proceso de firma. Podrá ver el documento firmado en cualquier momento.

Va a iniciar el proceso de firma electrónica, espere unos momentos hasta que aparezca la ventana de confirmación.

**Firmar**

Llegados a este punto, incluso podríamos finalizar el expediente en JOC-ER y no mediante los servicios WEB.

Lógicamente, si finalizamos el expediente mediante WS, podremos observar que el mismo está finalizado.

### 2.3.5 Consideraciones sobre el número de papel de la Fábrica Nacional de Moneda y Timbre (FNMT).

Como el objetivo es generar las guías de forma desasistida, no se solicitará el número de papel de la FNMT. Este será generado de forma automática. No teniendo que coincidir en su impresión con el número de papel que figure en el propio papel (Este es el único caso en el que se levanta la restricción).

Los números de papel generados estarán formados por:

WSGC+un número que coincidirá con el identificador del expediente.



### 2.3.6 Consideraciones sobre los certificados.

En todo el proceso, podrían estar involucrados dos certificados digitales, (aunque al final se opte por la opción de utilizar sólo uno, que realizará ambas funciones).

- Certificado para firmar el envío de las peticiones, con el objetivo de securizar el sistema.

Es el certificado con el que se firmará el cuerpo del mensaje, viajando dicha firma en la cabecera del mismo.

En su recepción se valida que la firma sea válida, (íntegra, firma no caducada, no revocada y del tipo de certificado correcto) y adscrita a una empresa fabricante/importadora que esté de alta en el registro de fabricantes/importadores de máquinas recreativas y de azar.

A tal efecto, estos certificados deberán estar en soporte de fichero, ya que deben estar ubicados en un sistema de ficheros accesible por la máquina que ejecuta el cliente.

Sólo serán aceptados certificados de aplicación emitidos por la ACCV o entidades conveniadas con esta, en soporte de fichero (no en tarjeta criptográfica).

El resto de certificados no son aceptados.

- Certificado para firmar la guía de circulación.

Este certificado, es el encargado de firmar la guía de circulación suministrada por el primer servicio web.

Sólo se admiten certificados de aplicación emitidos por la ACCV o entidades conveniadas con esta, en soporte de fichero.

Hay que observar que en los certificados de aplicación al firmar la guía, se debe tener en cuenta que en el pie de firma de la guía figurará el texto con el que se solicite el certificado. Dicho texto se corresponde con el nombre de la aplicación, y la empresa, en el formulario de la ACCV de solicitud de certificado.

**Aunque el texto es libre se recomienda solicitarlo con:  
Juego – Nombre de Empresa.**

NPSC - Windows Internet Explorer

https://npsc.accv.es:8450/npsc/solicitud/nuevaSolicitudAPP.do

Archivo Edición Ver Favoritos Herramientas Ayuda

Favoritos Petición de Compilaciones (2) Petición de Compilaciones WebServices en Axis (III), ... WebServices en Axis (III), ... WebServices en Axis (III), ... Sitios sugeridos

NPSC Inicio Fuentes Leer correo Imprimir Página Seguridad Herramientas Ayuda

Agencia de Tecnología y Certificación Electrónica

**Certificados para aplicaciones** MARTA GUZMAN GONZALEZ - NIF:28636906C

**Datos personales**

- Sol. certificado **Aplicación**
- Sol. certificado Código
- Sol. certificado SSL
- Sol. certificado VPN
- Sol. certificado Sede
- Sol. certificado Sello
- Solicitudes pendientes
- Solicitudes aprobadas
- Solicitudes rechazadas
- Mis certificados
- Mis permisos
- Ayuda
- Seleccionar idioma
- Salir

**Datos de la Solicitud de Certificado de Aplicación**

El uso de este certificado está restringido a **Identificación de Aplicaciones, y a la firma electrónica y/o cifrado de datos por parte de éstas**, pertenecientes a la **Generalitat Valenciana**, a **entidades y organismos vinculados a ella**, o a alguna Administración Pública con la que haya establecido **convenio de certificación**.

Las normas que rigen el uso de estos certificados se recogen en la Política de Certificación asociada.

Nombre Completo de la Aplicación/Servicio:

Email del Certificado:

**Nombre Completo de la Aplicación/Servicio:** Nombre completo de la Aplicación de la que se solicita el certificado separado por un espacio, guión y otro espacio del Nombre completo del Servicio de Desarrollo solicitante del certificado, incluyendo la Conselleria u Organismo al que pertenece. Este nombre es el que se incluirá en la petición de certificado. Debe ir en mayúsculas y no contener otro guión.

Por ejemplo: APLICACION 1 - SERVICIO 2 CONSELLERIA X.

Enviar

| ID DOCUMENT / ID DOCUMENTO             | msClxk7B0OmjiG.t5fh0xQ\$\$                         |                          | PÁGINA / PÁGINA     | 1 / 1   |
|--|--|--------------------------|---------------------|---|
| FIRMA PER / FIRMA POR                  | VALIDES CERTIF. FIRMANT / VALIDEZ CERTIF. FIRMANTE | DATA FIRMA / FECHA FIRMA | ID FIRMA / ID FIRMA |  |
| APLICACIONES - CONSELLERIA DE HACIENDA | 04/10/2010 - 03/10/2013                            | 11/08/2012 20:14:43      | 1344708883594       |   |

Documento firmado digitalmente. Para verificar la validez de la firma acceda a <https://pruebas.ha.gva.es/jocer/jocer/VerificacionCiudadanoAction.action>

- Recomendación:

Se utilizará el mismo certificado de aplicación tanto para securizar como para firmar la guía de circulación del fabricante, de este modo se simplifica la acreditación.

### 2.3.7 Acreditación y Acceso.

Se verá en puntos posteriores.

### 3 Proceso de desarrollo y pruebas.

Para la puesta en marcha del servicio, es necesario que el sistema invocante realice las modificaciones pertinentes para poder integrar el cliente en su sistema.

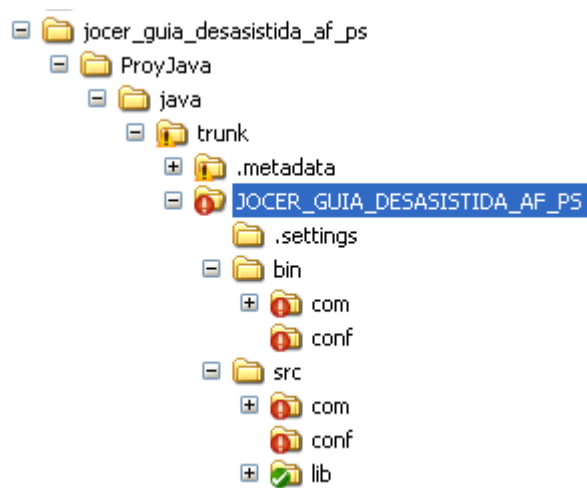
Para ello y como primer paso se deben realizar las pruebas pertinentes en un entorno de desarrollo.

A tal efecto, se ha implantado el servicio en el entorno de pruebas de CHAP para la realización de dichas pruebas.

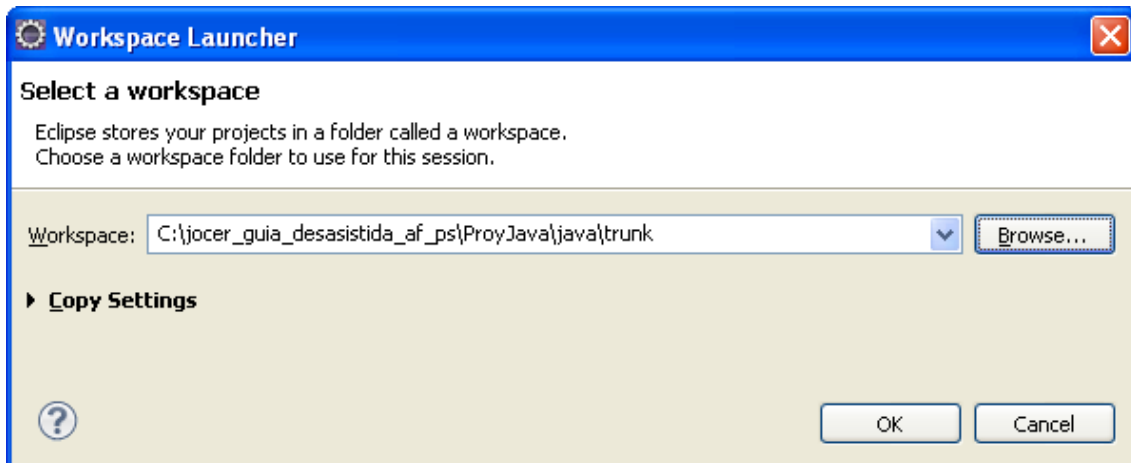
Los pasos recomendados para ello son:

- A. Solicitar a CHAP acceso al entorno de pruebas. Para ello se debe enviar un correo electrónico a JOC-ER ([www.joc-er.es](http://www.joc-er.es), apartado de “Contactar y suscripción”, subapartado “Correo electrónico”), indicando la empresa que desea realizar las pruebas, y la dirección-direcciones IP desde la que invocarán al servicio con el fin de abrir el entorno de pruebas.
- B. Descargar el fichero comprimido con el proyecto eclipse del cliente. Este se encuentra en [www.joc-er.es](http://www.joc-er.es), apartado de “Documentación y requisitos técnicos”.

Se propone descomprimirlo en el directorio `c:\jocer_guia_desasistida_af_ps` quedando la siguiente estructura.



- C. Se recomienda trabajar con el IDE eclipse INDIGO. Al abrir dicho IDE, seleccionar como WorkSpace el directorio:



#### D. Consideraciones al proyecto:

- Para la realización de la firma, tanto para securizar, como para firmar las guías, el proyecto ya contiene un keystore con un certificado de aplicación de pruebas de la ACCV. Se encuentra en C:\jocer\_guia\_desasistida\_af\_ps\ProyJava\java\trunk\JOCER\_GUIA\_DESASISTIDA\_AF\_PS\src\keystorepru.jks.

La clave del keystore es: keystorepru

El alias del certificado de aplicación es: certificado\_aplicacion

El password del certificado de aplicación es es: hNUK.czC

Dicho keystore se ha construido mediante la aplicación web Portecle, en el anexo I se encuentra una explicación más detallada sobre como gestionar dichos keystores mediante dicha aplicación.

Este certificado ya ha sido dado de alta en el sistema de pruebas, y asignado una empresa fabricante de pruebas, con un modelo, en concreto el CV-B-200--, evidentemente los datos obtenidos son de pruebas.

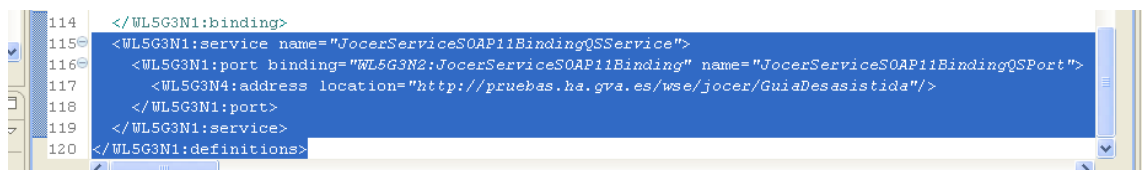
Se facilita un certificado de ciudadano en C:\jocer\_guia\_desasistida\_af\_ps\ProyJava\java\trunk\JOCER\_GUIA\_DESASISTIDA\_AF\_PS\src\USUARIO\_APELLIDO\_-\_NIF\_M\_SUB\_CA\_WINDOWS.p12 con la clave 0563233, para acceder a JOC-ER, en el entorno de pruebas y tramitar como tal empresa fabricante las guías, y observar el resultado de la invocación de los servicios web.

La url es <http://pruebas.ha.gva.es/jocer/jocer/es/AccesoAction!accesoCiudadano.action>

En el proyecto se facilita en el directorio C:\jocer\_guia\_desasistida\_af\_ps\ProyJava\java\trunk\JOCER\_GUIA\_DESASISTIDA\_AF\_PS\src, el certificado incluido dentro del keystore (Ficheros: APLICACIONES++CONSELLERIA+DE+HACIENDA+pruebas.p12), así como su clave (Fichero: clave.txt).

**E. Modificar los ficheros de configuración del proyecto:**

- Modificar el fichero WSDL para asegurarse que el end-point es del entorno de pruebas:  
C:\jocer\_guia\_desasistida\_af\_ps\ProyJava\java\trunk\JOCER\_GUIA\_DESASISTIDA\_AF\_PS\src\JOCER\_GUIA\_DESASISTIDA\_AF\_PS.wsdl



- Asegurarse que la clase Constantes (C:\jocer\_guia\_desasistida\_af\_ps\ProyJava\java\trunk\JOCER\_GUIA\_DESASISTIDA\_AF\_PS\src\com\oracle\xmlns\pcbpel\adapter\db\util\Constantes.java), contiene la ruta correcta a los ficheros de configuración:

```
public static final String PROPERTY_FILE =  
    "/jocer_guia_desasistida_af_ps/ProyJava/java/trunk/JOCER_GUIA_DESASISTIDA_AF_PS/src/conf/cliente.properties";  
  
public static final String OUTSECURITY_PROPERTY_FILE =  
    "outsecurity_sign.properties";  
  
public static final String CHARSET = "UTF-8";
```

- Asegurarse que el fichero de configuración C:\jocer\_guia\_desasistida\_af\_ps\ProyJava\java\trunk\JOCER\_GUIA\_DESASISTIDA\_AF\_PS\src\conf\cliente.properties contiene las opciones de configuración correctas:

```
#####  
#Valores para firmar el cuerpo del mensaje en cabecera SOAP  
#####  
  
#Siempre este valor  
accion=Signature  
  
# alias del certificado en el keystore  
alias=certificado_aplicacion  
  
#password del certificado en el keystore  
passCert=hNUK.czC
```

```
#####  
#ubicación del wsdl  
#####  
wsdl=/jocer_guia_desasistida_af_ps/ProyJava/java/trunk/JOCER_  
GUIA_DESASISTIDA_AF_PS/src/JOCER_GUIA_DESASISTIDA_AF_PS.wsdl
```

```
#####  
# Datos para firmar la guía de circulación  
#####  
keyStore=/jocer_guia_desasistida_af_ps/ProyJava/java/trunk/JO  
CER_GUIA_DESASISTIDA_AF_PS/src/keystorepru.jks  
keyStoreType=jks  
keyStorePassword=keystorepru  
keyStoreCertAlias=certificado_aplicacion  
keyStoreCertPassword=hNUK.czC
```

```
#####  
# Directorio donde el cliente dejará las guías  
#####  
# Ruta en la que se almacenarán las guías firmadas,  
retornadas por el segundo ws  
destinationPath=/tmp/joc-er/guias
```

- Asegurarse que el fichero de configuración C:\jocer\_guia\_desasistida\_af\_ps\ProyJava\java\trunk\JOCER\_GUIA\_DESASISTIDA\_AF\_PS\src\outsecurity\_sign.properties contiene las opciones de configuración correctas:

```
#####  
#Valores para firmar el cuerpo del mensaje en cabecera SOAP  
#####  
#password del keystore  
org.apache.ws.security.crypto.merlin.keystore.password=keysto  
repru
```

```
#password del certificado  
org.apache.ws.security.crypto.merlin.alias.password=hNUK.czC
```

```
#Valor del alias con el que se ha introducido el certificado  
# en el keystore  
org.apache.ws.security.crypto.merlin.keystore.alias=certifica  
do_aplicacion
```

```
#ubicación del keystore  
org.apache.ws.security.crypto.merlin.file=/jocer_guia_desasis  
tida_af_ps/ProyJava/java/trunk/JOCER_GUIA_DESASISTIDA_AF_PS/s  
rc/keystorepru.jks
```

- Asegurarse que la clase principal de invocación, está perfectamente configurada:

```
C:\jocer_guia_desasistida_af_ps\ProyJava\java\trunk\JOCER_GUI  
A_DESASISTIDA_AF_PS\src\com\tsol\tramita\interconexion\jocer\
```

```
objetosws\JocerServicePortType_JocerServiceSOAP11BindingQSPor  
t_Client.java
```

- Los parámetros de invocación:

El modelo de la máquina, obligatorios:

```
miMaquina.setCv("S");  
Nota: Indicador "S" o "N", si el modelo lleva CV o no.  
miMaquina.setTipoMaquina("B");  
long x=200;  
miMaquina.setNumeroRegistroModelo(x);  
miMaquina.setLetraModelo("-");
```

Los contadores de la máquina, obligatorios:

```
miMaquina.setNumeroSerieContador("10");  
miMaquina.setNumeroSerieMaquina("11");  
miMaquina.setSerieContador("12");  
miMaquina.setSerieMaquina("13");  
miMaquina.setModeloContador("14");
```

## F. Invocación y resultado.

Una vez realizados, todos los cambios de configuración, se puede ejecutar mediante la ejecución de la clase C:\jocer\_guia\_desasistida\_af\_ps\ProyJava\java\trunk\JOCER\_GUIA\_DESASISTIDA\_AF\_PS\src\com\tsol\tramita\interconexion\jocer\objetosws\JocerServicePortType\_JocerServiceSOAP11BindingQSPort\_Client.java desde el propio eclipse.

Si la ejecución es correcta el resultado vendrá dado por (Nota: en este ejemplo, sólo se incluyen las partes de mensaje significativas para la explicación):

```
10-ago-2012 11:33:33 org.apache.cxf.service.factory.ReflectionServiceFactoryBean  
buildServiceFromWSDL  
INFO: Creating Service  
{http://objetosws.jocer.interconexion.tramita.tsol.com}JocerServiceSOAP11BindingQSServ  
ice from WSDL:  
file:/C:/jocer_guia_desasistida_af_ps/ProyJava/java/trunk/JOCER_GUIA_DESASISTIDA_AF_PS/s  
rc/JOCER_GUIA_DESASISTIDA_AF_PS.wsdl  
Invocando solicitarGuiaCirculacion...  
10-ago-2012 11:33:35  
org.apache.cxf.services.JocerServiceSOAP11BindingQSService.JocerServiceSOAP11BindingQSPo  
rt.JocerServicePortType  
INFO: Outbound Message  
-----  
ID: 1  
Address: http://pruebas.ha.gva.es/wse/jocer/GuiaDesasistida  
Encoding: UTF-8  
Content-Type: text/xml  
Headers: {Accept=[*/*], SOAPAction=["urn:solicitarGuiaCirculacion"]}  
  
<soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-  
wssecurity-utility-1.0.xsd" wsu:Id="id-1">  
<ns2:solicitarGuiaCirculacionRequest  
xmlns="http://beansintercambio.jocer.interconexion.tramita.tsol.com"  
xmlns:ns2="http://objetosws.jocer.interconexion.tramita.tsol.com">
```

```
<ns2:datosMaquina>
  <serieMaquina>13</serieMaquina>
  <numeroSerieMaquina>11</numeroSerieMaquina>
  <serieContador>12</serieContador>
  <numeroSerieContador>10</numeroSerieContador>
  <modeloContador>14</modeloContador>
  <numeroRegistroModelo>200</numeroRegistroModelo>
  <tipoMaquina>B</tipoMaquina>
  <letraModelo>-</letraModelo>
  <cv>S</cv>
</ns2:datosMaquina>
</ns2:solicitarGuiaCirculacionRequest>
</soap:Body>
-----
10-ago-2012 11:34:12
org.apache.cxf.services.JocerServiceSOAP11BindingQSService.JocerServiceSOAP11BindingQSPo
rt.JocerServicePortType
INFO: Inbound Message
-----
ID: 1
Response-Code: 200
Encoding: UTF-8
Content-Type: text/xml; charset=utf-8
<soapenv:Body><ns2:solicitarGuiaCirculacionResponse
xmlns:ns2="http://objetosws.jocer.interconexion.tramita.tsol.com">
<ns2:solicitudGuia>
  <ns1:idDocumento>3190</ns1:idDocumento>
  <ns1:refExpediente>7425</ns1:refExpediente>
  <ns1:hashGuia>07q1+xGamNXOJgADEZYfxQAHIlQ=</ns1:hashGuia>
</ns2:solicitudGuia>
<ns2:descripcionError xsi:nil="1"/>
</ns2:solicitarGuiaCirculacionResponse>
</soapenv:Body>
-----
Datos de la solicitud obtenidos:
  * Hash: 07q1+xGamNXOJgADEZYfxQAHIlQ=
  * ID. Documento: 3190
  * Ref. Expediente: 7425
```

Como se puede observar, se obtiene:

- Una representación hash de la guía que se firmará.
- Un identificador interno del documento.
- Una referencia al expediente JOC-ER abierto y que es consultable.

Firmando la guía....

Se firma la guía..

Invocando solicitarDocumentoFirmado...

Se invoca al segundo WS, enviando la guía firmada..

```
10-ago-2012 11:34:12
org.apache.cxf.services.JocerServiceSOAP11BindingQSService.JocerServiceSOAP11BindingQSPo
rt.JocerServicePortType
INFO: Outbound Message
-----
ID: 2
Address: http://pruebas.ha.gva.es/wse/jocer/GuiaDesasistida
Encoding: UTF-8
Content-Type: text/xml
Headers: {Accept=[*/*], SOAPAction=["urn:solicitarDocumentoFirmado"]}
Payload: <soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="id-3">
<ns2:solicitarDocumentoFirmadoRequest>
  <ns2:solicitudDocumentoFirmado>
    <idDocumento>3190</idDocumento>
```



```
<firma>MIHEAYJKoZIhvcNAQcCoIIHA.....TCCBv0CAQExCzAJBgUrDgMCGGUAMAsGC</firma>
</ns2:solicitudDocumentoFirmado>
</ns2:solicitarDocumentoFirmadoRequest></soap:Body>
-----
12-ago-2012 11:34:28
org.apache.cxf.services.JocerServiceSOAP11BindingQSService.JocerServiceSOAP11BindingQSPo
rt.JocerServicePortType
INFO: Inbound Message
-----
ID: 2
Response-Code: 200
Encoding: UTF-8
Content-Type: text/xml; charset=utf-8
Headers: {connection=[keep-alive], Content-Length=[10529], content-type=[text/xml;
charset=utf-8], Date=[Sun, 12 Aug 2012 09:34:13 GMT], Server=[Apache/2.0.64 (Unix)
mod_jk/1.2.27 mod_onsint/1.0], Via=[1.0 prurproxy01.ha.gva.es (squid/3.1.8)], X-
Cache=[MISS from prurproxy01.ha.gva.es], X-Cache-Lookup=[MISS from
prurproxy01.ha.gva.es:80], X-Powered-By=[Servlet/2.5 JSP/2.1]}
Payload: <soapenv:Body>
<ns2:solicitarDocumentoFirmadoResponse>
<ns2:documentoFirmado>
  <ns1:firmado>JVBERi0xLjQKJeLj.....z9MKMyAwIG9iaia8PC9G</ns1:firmado>
  <ns1:original>JVBERi0xLjQKJeLj.....jz9MKNCaWIG9iaia8PC9GaWw0ZXIvRmxh</ns1:original>
</ns2:documentoFirmado>
<ns2:descripcionError xsi:nil="1"/>
</ns2:solicitarDocumentoFirmadoResponse>
</soapenv:Body>
-----
  Guía de circulación guardada correctamente en /tmp/joc-er/guias
```

En el directorio establecido a tal efecto en la configuración, se dejarán dos archivos:

- GC\_GUIA\_7426.pdf. La guía sin firmar.
- GC\_GUIA\_7426\_firmado.pdf. La guía firmada y que será la que se imprima.

#### G. Gestión de errores.

Hay que observar que si se producen errores no en la invocación al servicio web de solicitud, sino en los pasos posteriores de firma o de envío de dicha firma y recepción de la guía, se tendrá como efecto colateral que se quedará el expediente abierto en JOC-ER correspondiente a la primera invocación.

Esto, en si mismo no representa un problema, aunque si se recomienda entrar periódicamente a la plataforma y hacer limpieza de dichos expedientes mediante su cancelación.

## 4 Proceso de paso a producción.

Para el proceso de paso a producción se deben seguir los siguientes pasos.

- A. Obtención del certificado de aplicación de la ACCV. Según la configuración deseada.
- B. Acreditar dicho/s certificado ante el Servicio de Juego.

Para ello hay que rellenar la credencial, [www.joc-er.es](http://www.joc-er.es), dentro del apartado “Procedimiento para utilizar el sistema JOC-ER y alta en el sistema”, haciendo constar:

- En el campo Razón Social: La Razón social de la empresa fabricante.
- NIF Entidad: Nif de la empresa fabricante.
- Número de inscripción en el registro de fabricante/importadores de máquinas recreativas y de azar: el número de registro correspondiente.
- Colectivo al que está adscrito: Fabricante/Importador
- Dirección.
- Nombre de usuario: El que se desee que figure en el registro de acreditados.
- NIF del usuario/n de serie del certificado:
  - Para el uso del WS se debe introducir, el número de serie del certificado. Distinguiendo entre mayúsculas y minúsculas. (Independientemente si se de aplicación o de ciudadano).
- Datos del representante:
- Seleccionar la opción “Alta para el servicio web de generación de la guía de circulación del fabricante”.
- Como tipo de certificado seleccionar, “Certificado de Aplicación”.

Una vez acreditado, se le informará ya sea vía correo electrónico o telefónicamente del alta en el sistema del certificado.

Nota: Para evitar errores de transcripción del número de serie del certificado digital, se solicitará que se entregue como documentación anexa a la credencial, una impresión en papel del número de serie del certificado de aplicación. La forma de obtenerla se encuentra en el anexo 3.

C. Modificar el cliente para producción.

- Crear el keystore, según el anexo I, mediante la aplicación portecle por ejemplo, con el o los nuevos certificados de producción. Dando pues un valor a los valores de parámetros correspondientes.
- Incluir el nuevo keystore en el cliente.
- Modificar los ficheros de configuración establecidos en el apartado anterior, con los nuevos valores.
- Implantar en producción.
  
- La url para producción es la misma que la de pruebas pero cambiando el rootContext a: <https://atenea.ha.gva.es>

Nota: No olvidar, para el caso de producción, cargar en el cacerts de la jvm que ejecuta la máquina los certificados raíz de la accv. Se recomienda cargarlos en el siguiente orden:

- Rootca.cer
- ACCVRAIZ1.cer
- Accv-ca1.cer
- Accv-ca2.cer
- Accv-ca3.cer
- ACCVCA110.cer
- ACCVCA120.cer

## 5 Anexo I: PORTECLE: Gestión de keystores.

- Generación del keystore.

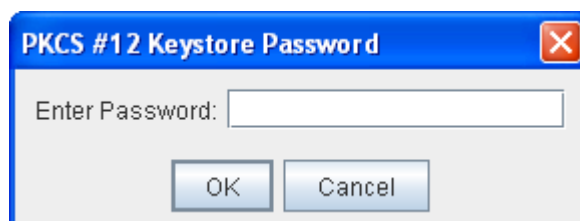
Si no se dispone de la Java Keystore, deberá generarse una a partir del certificado de firma válido para realizar la invocación. Para ello se aconseja el uso de la aplicación 'Portecle'.

Puede descargarse desde: <http://portecle.sourceforge.net/> , botón 'Launch'.

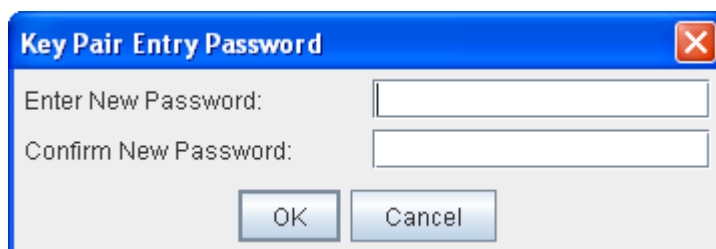
Nota: Es posible que se deba bajar para la máquina virtual java los ficheros para aplicar "unlimited strength jurisdiction policy files"

Con las opciones 'File' → 'New keystore' de tipo JKS, y posteriormente, 'Tools' → 'Import key pair' para adjuntar el certificado de firma.

- Solicita el password del certificado.



- Vuelve a solicitar el password del certificado.



Se importa correctamente...

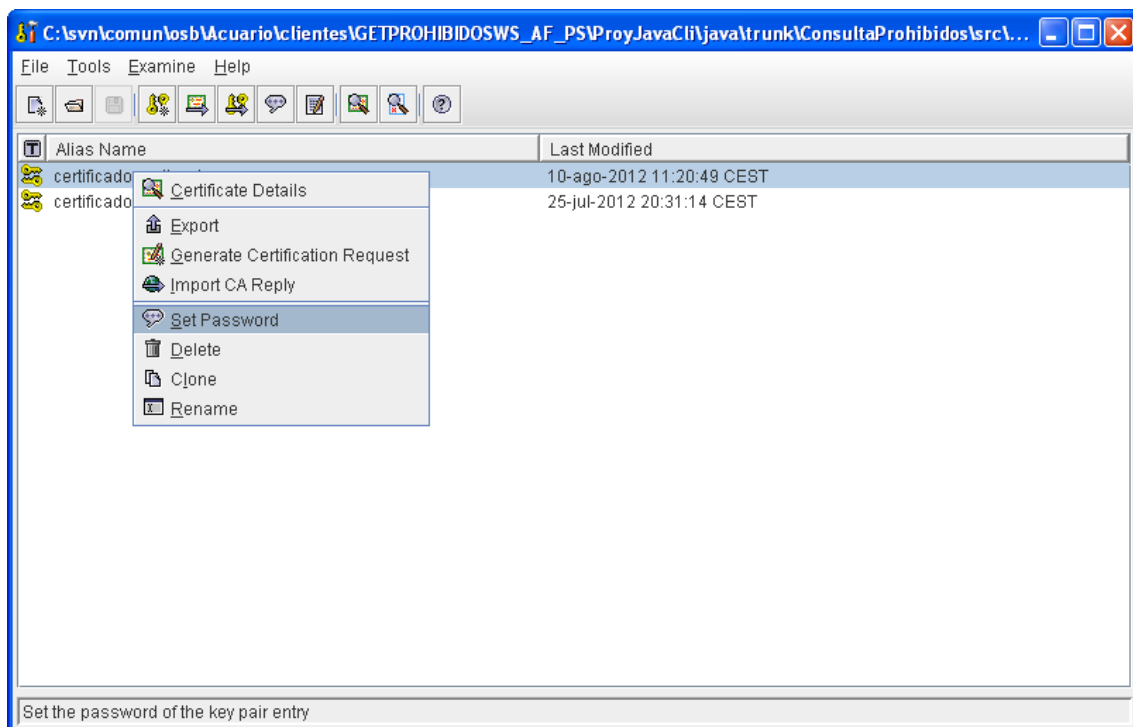


- Al guardar el keystore como fichero solicitará, la clave para el keystore.

De este modo, en los ficheros de configuración hay que tener en cuenta que:

- Cliente.properties: Va la clave del certificado.
- En outsecurity\_sign.properties: van la del certificado y la del keystore.

Nota: Para asegurarse que los passwords de los certificados son correctos, pulsar sobre el certificado con el boton derecho del ratón y cambiar el password.



## **6 ANEXO II. Prueba y depuración del servicio mediante SoapUI.**

Se compone de los siguientes pasos:

### **6.1.1 Instalación del software de testeo de ws**

Recomendamos SoapUI, aunque, evidentemente, cualquier otro software de testeo es válido.

Se recomienda este software, por las facilidades que ofrece en:

- Generar peticiones de invocación.
- Generar pruebas de extress.
- Generar el código java cliente de invocación.

Sopauí por ejemplo se puede obtener de:

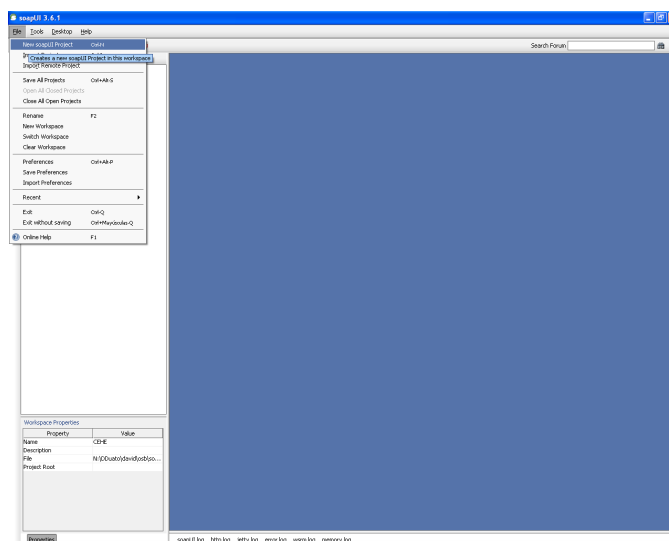
<http://www.soapui.org/>

Con esta herramienta se puede invocar al servicio, realizar pruebas de stress, etc.

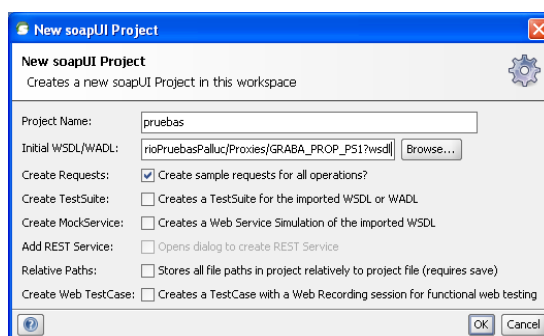
### **6.1.2 Testeo del servicio**

En este punto, se dan unas pinceladas para la prueba del servicio, para ello:

1. Creamos de un nuevo proyecto SoapUI.  
Pulsar la opción de menú “File” correspondiente.

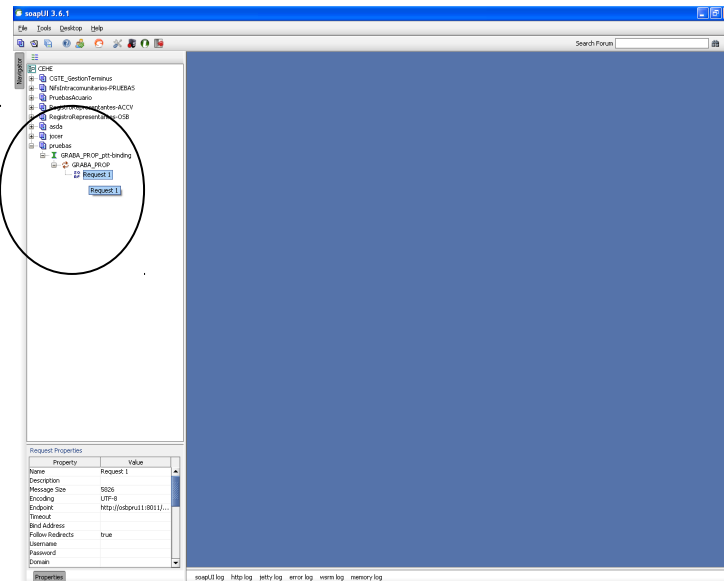


2. Solicitará la introducción del nombre del proyecto, y la url donde se encuentra el WSDL del servicio.



Nota: en pruebas... es como la siguiente...  
<http://pruebas.ha.gva.es/wse/ConsultaProhibidos?WSDL>

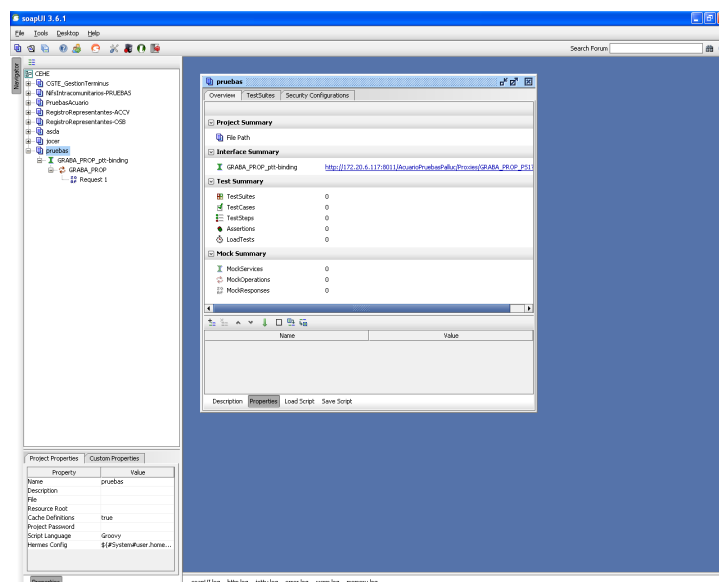
Tras pulsar siguiente, se creará la estructura necesaria para su invocación.



### 3. Introducir certificados digitales en el almacén de certificados.

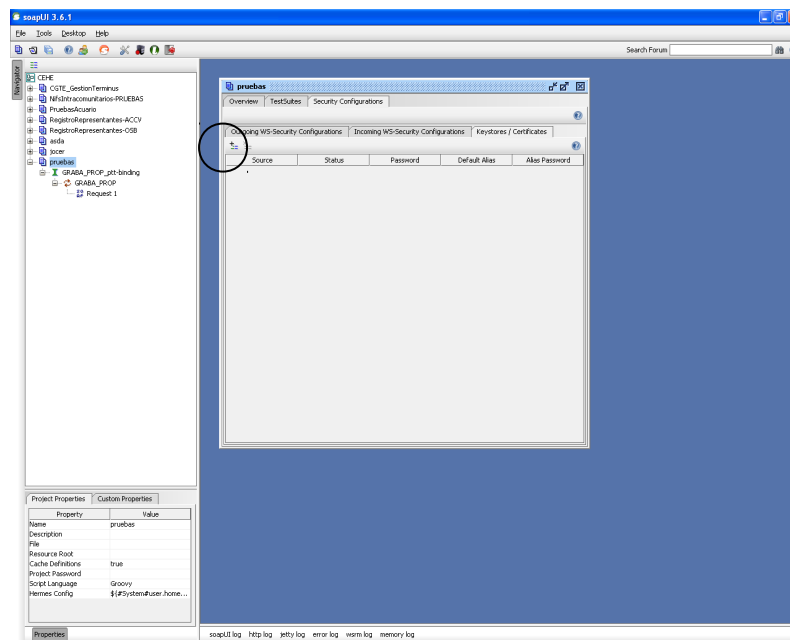
Esta opción, permite la introducción de los diferentes certificados con los que se realizarán las pruebas.

- Para ello pulsamos con el botón derecho sobre el proyecto (en el ejemplo Pruebas).

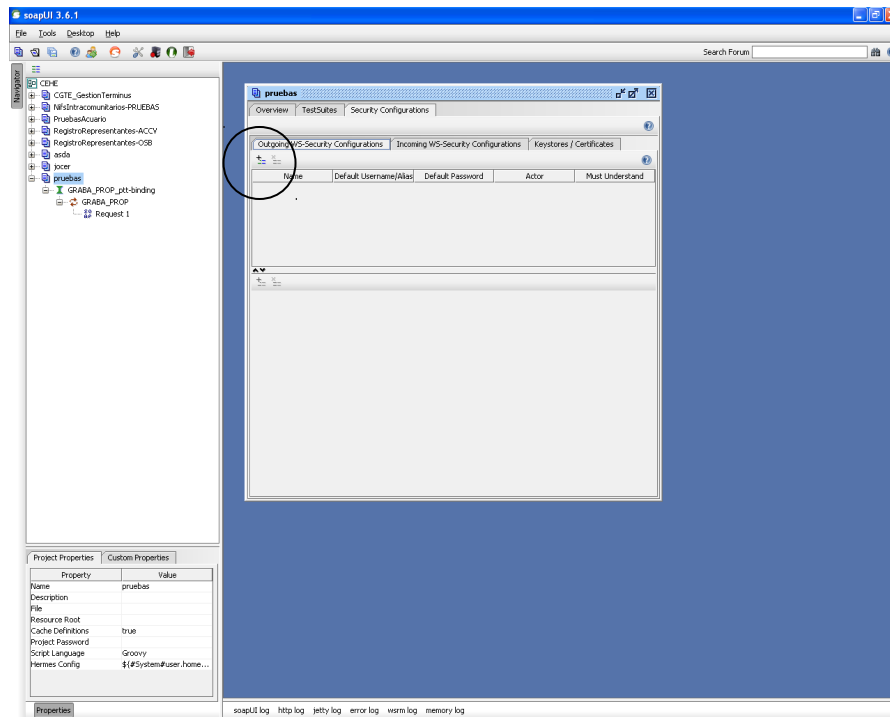


- Y seleccionamos la pestaña “Security Configurations” y dentro de esta “Keystore/Certificates”, pulsando el icono de “crear”.



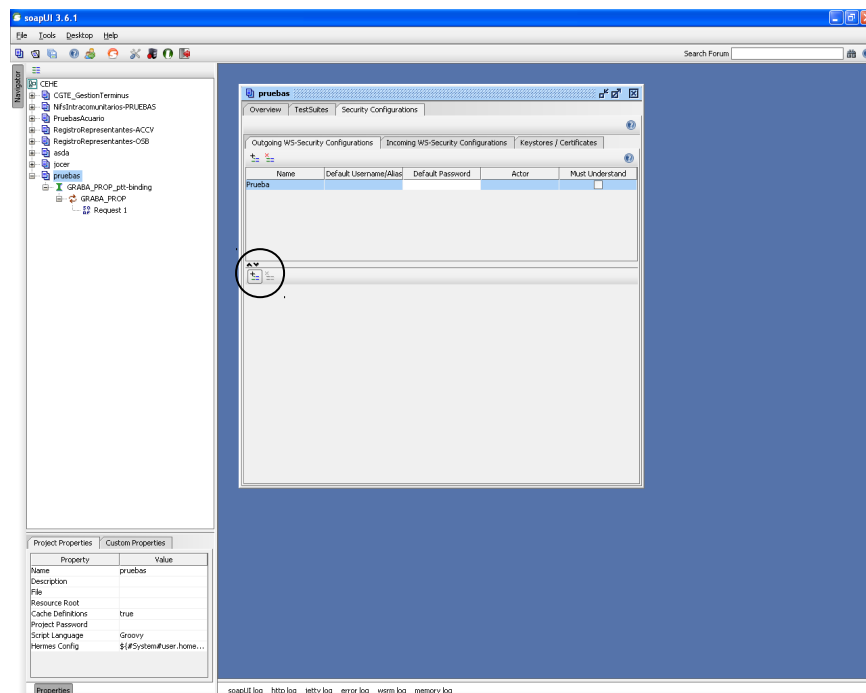


- c) Posteriormente presenta una ventana para seleccionar un certificado del Sistema de Ficheros, así como su contraseña.
  - d) Este proceso, se debe repetir por cada certificado digital que se desea utilizar.
4. Configurar los parámetros de seguridad de salida del certificado.
- a) En la misma ventana seleccionamos la pestaña de “Outgoing WS-Security Configurations”, y creamos una configuración, pulsando el icono de “Crear”.

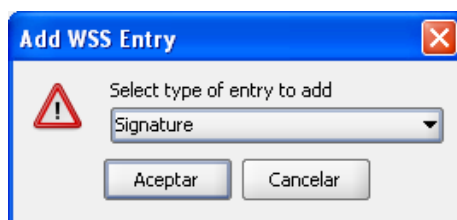


Nos solicitará un nombre de configuración.

- b) En la misma ventana, en la parte inferior, seleccionamos la pestaña de “Outgoing WS-Security Configurations”, y seleccionamos crear uno.

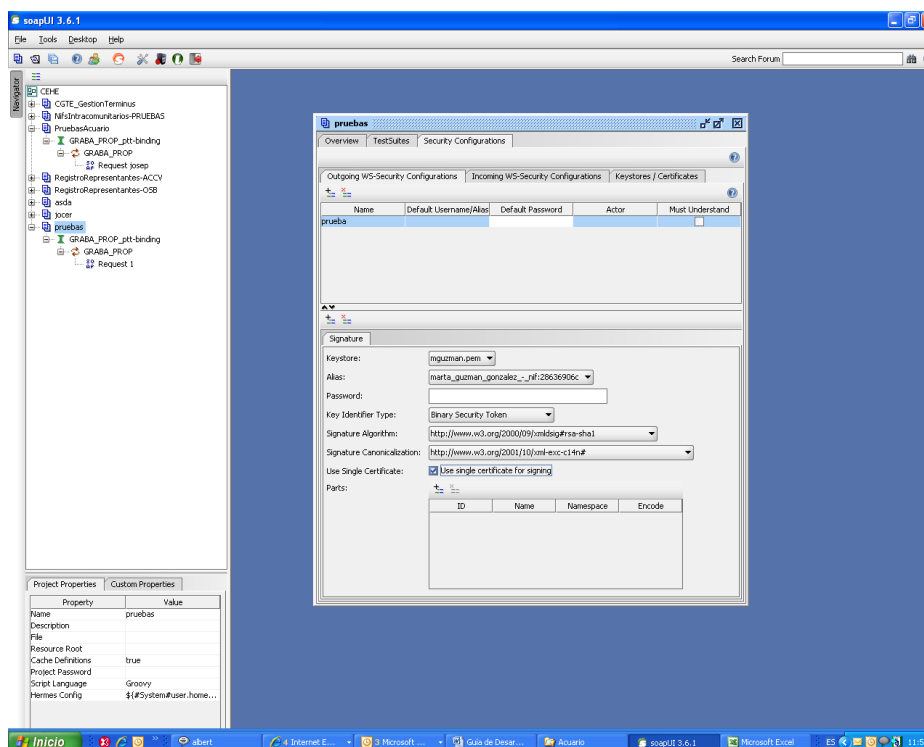


Solicitará el tipo de entrada, hay que introducir “Firma” (Signature).



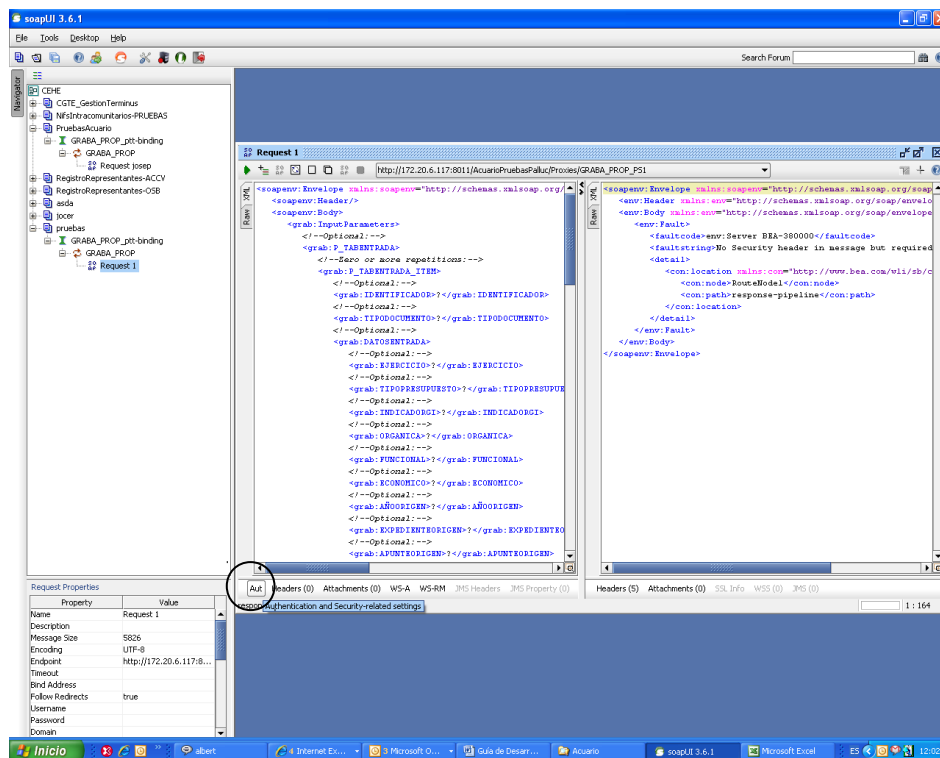
A continuación se presentará la información de configuración, en la que hay que establecer.

- El certificado con el que se firmará la petición. Para ello presenta una combo con los certificados introducidos en el KeyStore.
- Key Identifier Type: Binary Security Token
- Signature Algorithm: <http://www.w3.org/2000/09/xmldsig#rsa-sha1>
- Signature Canonicalization: <http://www.w3.org/2001/10/xml-exc-c14n#>
- Use Single Certificate: Seleccionado

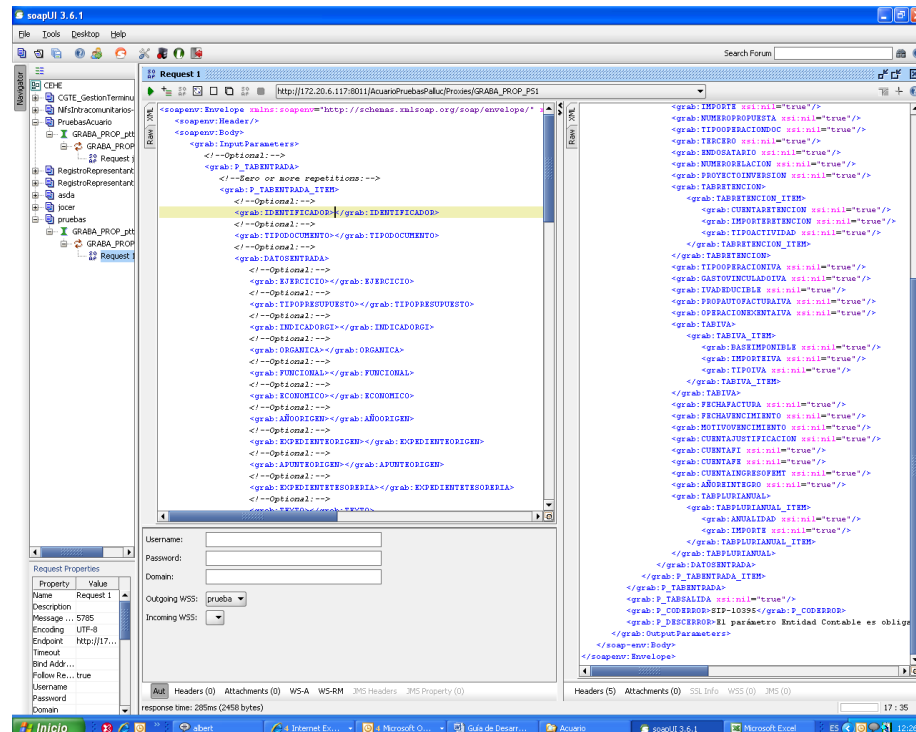


## 5. Probar el servicio.

Una vez configurado, ya se puede probar el servicio. Se pulsa dos veces sobre la petición y aparecerá la pantalla de parámetros.



Seleccionamos el botón de “Aut” y procedemos a seleccionar una de las configuraciones de seguridad de salida.



Para posteriormente pulsar el botón de ejecución y realizar pruebas.

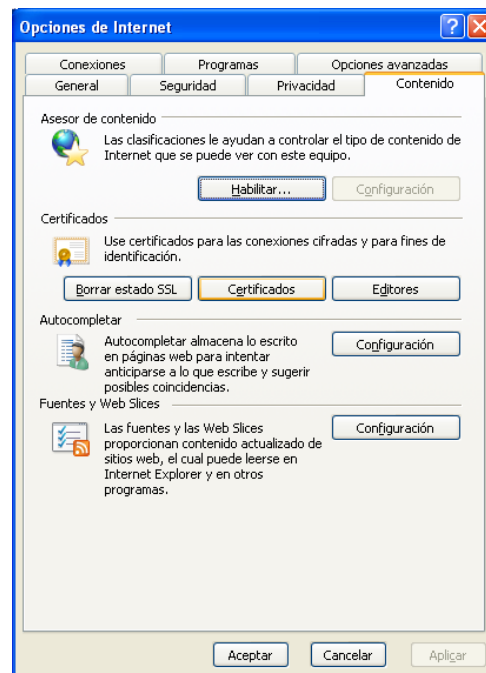
## 7 ANEXO III. Obtención del número de serie del certificado digital.

El ejemplo se explicará para el navegador Internet Explorer. Aunque el procedimiento es similar para otros navegadores.

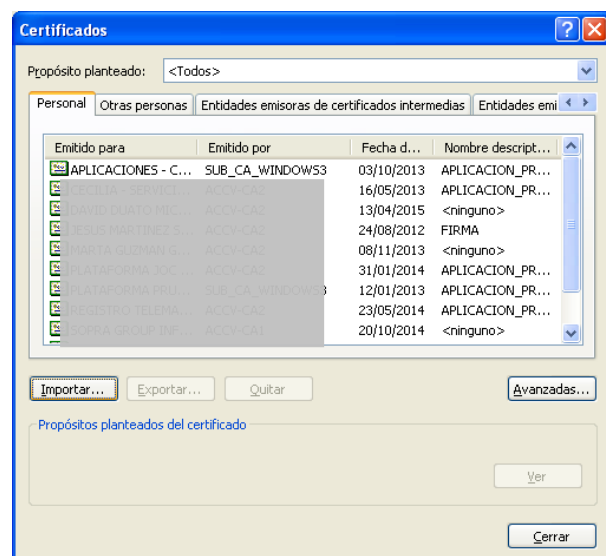
### 7.1 Incorporar el certificado al navegador.

1. El certificado debe estar en soporte de fichero.
2. Abrir el navegador, Internet Explorer.

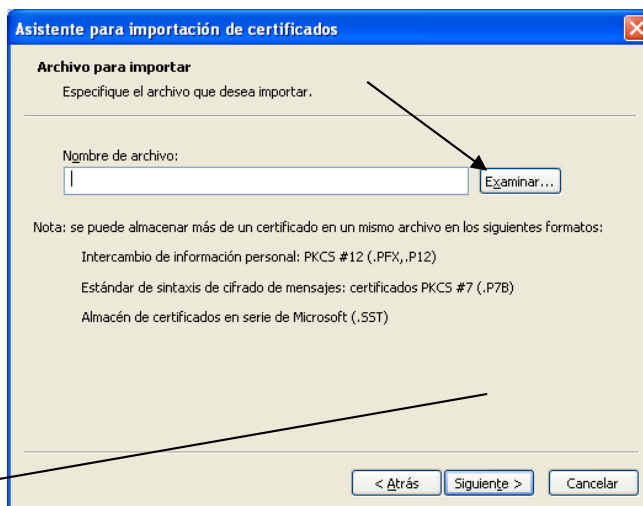
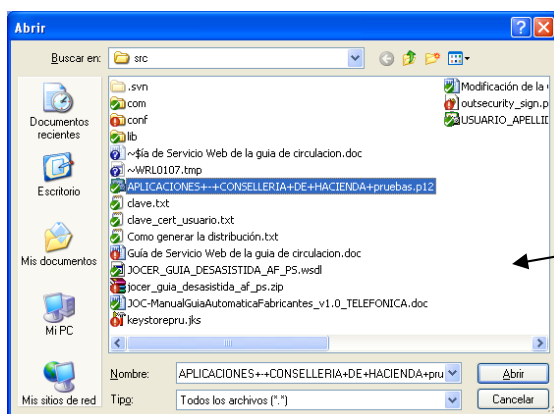
3. Seleccionar del menú Herramientas/Opciones de Internet. Dentro de este seleccionar la pestaña de “Contenido” y pulsar el botón de “Certificados”.



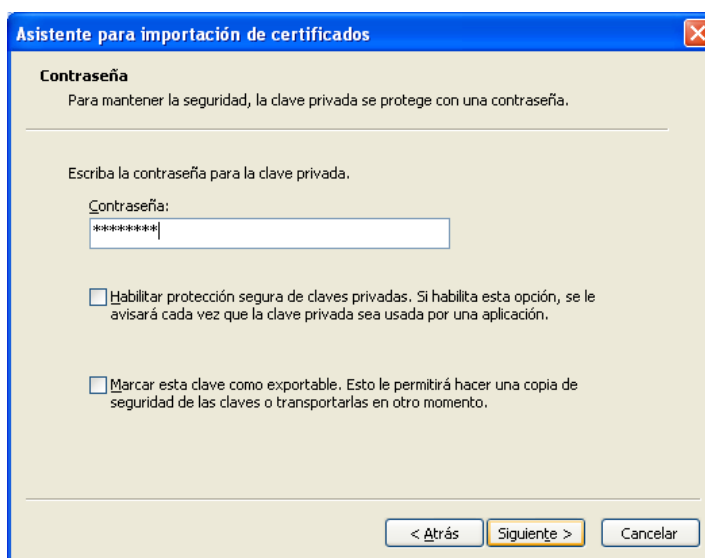
4. Pulsar el botón “Importar”, y se abrirá al asistente para importar el certificado.



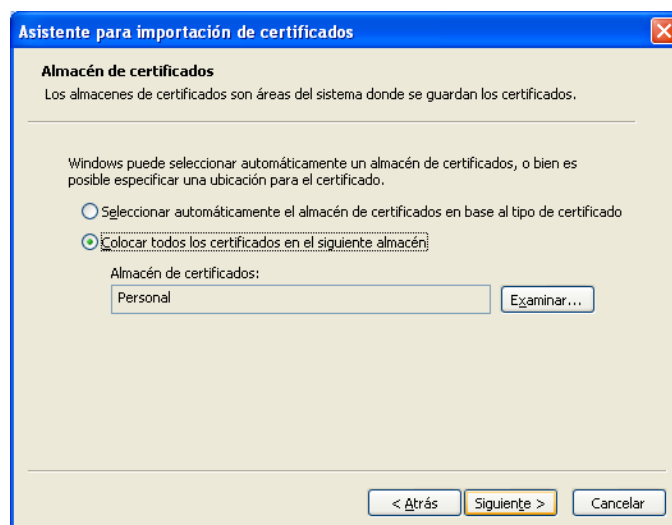
5. Seleccionamos la ubicación del certificado, para ello pulsamos “Abrir” y seleccionamos el certificado deseado.



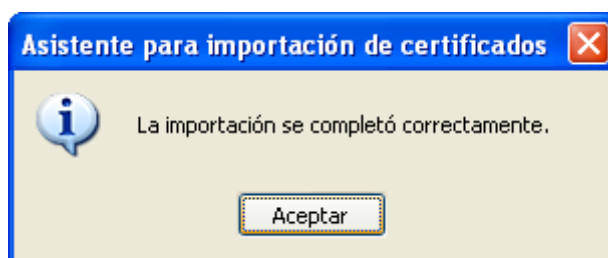
6. Pulsamos el botón “Siguiente”, y nos solicitará la clave del certificado. La introducimos y pulsamos el botón “Siguiente”.



7. Seleccionamos el almacén “Personal”, y pulsamos siguiente y finalizar.



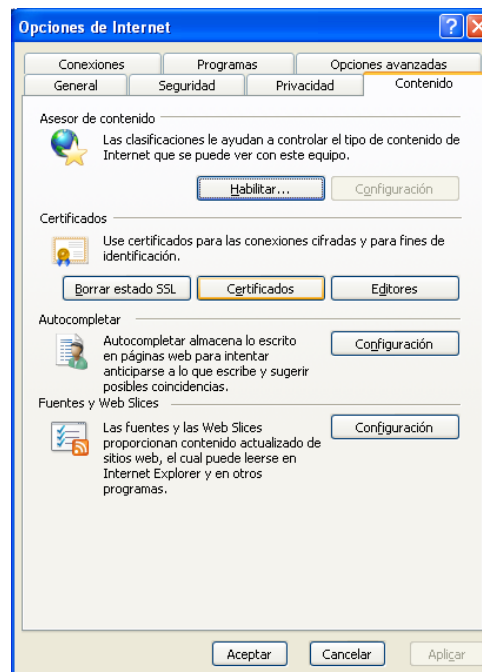
8. Si todo ha ido correctamente, se nos mostrará el mensaje que la importación ha ido correctamente.



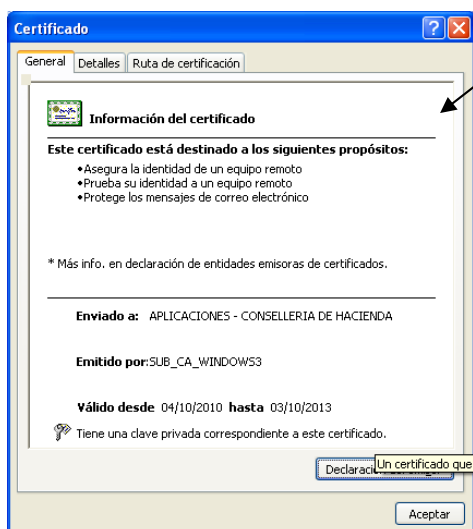
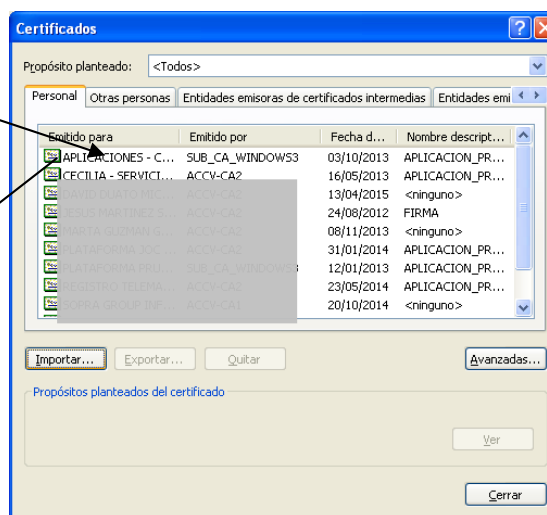
## 7.2 Ver la información del certificado e imprimir su número de serie.

1. Abrir el navegador, Internet Explorer.

2. Seleccionar del menú Herramientas/Opciones de Internet. Dentro de este seleccionar la pestaña de “Contenido” y pulsar el botón de “Certificados”.



3. Pulsar dos veces con el ratón sobre el certificado del que se desee visualizar la información.





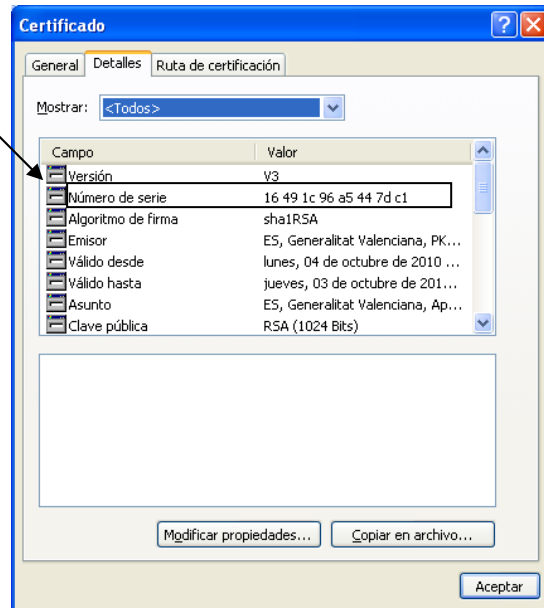
4. Seleccionar la pestaña detalles, y muestra la información del número de serie del certificado.

Tal y como se muestra en dicha ventana, se debe escribir en la credencial. Distinguiendo Mayúsculas y minúsculas. Nota: Se pueden obviar los espacios en blanco.

Con el fin de evitar errores en la credencial, es conveniente imprimir dicha pantalla y adjuntarla en la credencial.

Para ello, pulsar sobre la ventana para asegurarse que es la ventana activa, a continuación pulsar la tecla “Alt” y sin soltarla, la tecla “Imp Pantalla”, esto copiará la imagen de la ventana en el portapapeles.

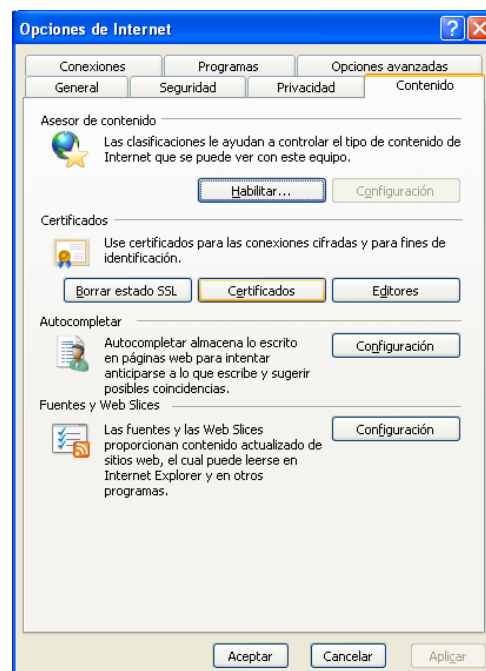
Abrir un editor de texto, por ejemplo Word, y pegar la imagen e imprimirla.



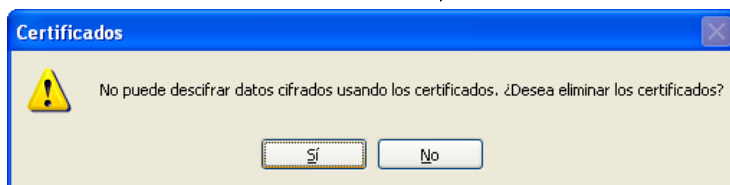
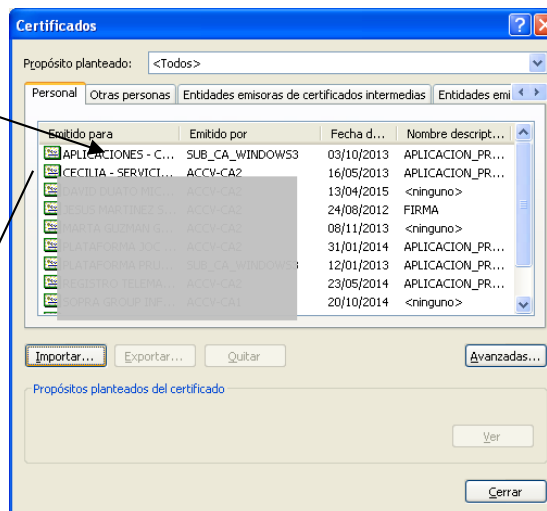
## 7.3 Suprimir el certificado del navegador.

1. Abrir el navegador, Internet Explorer.

2. Seleccionar del menú Herramientas/Opciones de Internet. Dentro de este seleccionar la pestaña de “Contenido” y pulsar el botón de “Certificados”.



3. Seleccionar el certificado a eliminar, y pulsar la tecla de “Suprimir”. Se le informará que se procederá a eliminar el certificado.



Al pulsar “Sí” se eliminará el certificado.