GENERALITAT VALENCIANA
CONSELLERIA D'HISENDA I MODEL ECONÒMIC

Direcció General de Tecnologies de la Informació
C/ Castán Tobeñas, 77.
Ciutat Administrativa 9 D'Octubre-Edif.B1 (46018-VALENCIA)

Guía del Servicio Web de consulta del registro de prohibiciones de acceso a los establecimientos de juego (casinos de juego, salas de bingo, salones de juego y locales específicos de apuestas) de la Comunitat Valenciana.

Identificador del proyecto: JOCER-PROHIBIDOS

Identificador del Documento: GuiaDesarrollo

Versión: 04.00

Fecha de entrega: 23/12/2016

GENERALITAT VALENCIANA
CONSELLERIA D'HISENDA I MODEL ECONÒMIC

Direcció General de Tecnologies de la Informació
C/ Castán Tobeñas, 77.
Ciutat Administrativa 9 D'Octubre-Edif.B1 (46018-VALENCIA)

Índice de contenidos

1. Motivación....3
2. Visión características generales del servicio....4
3. Proceso de desarrollo y pruebas....6
4. Proceso de paso a producción....14
5. ANEXO I: PORTECLE: Gestión de keystores....17
6. ANEXO II: Prueba y depuración del servicio mediante SoapUI....19
7. ANEXO III: Obtención del número de serie del certificado digital....26

Direcció General de Tecnologies de la Informació
C/ Castán Tobeñas, 77.
Ciutat Administrativa 9 D'Octubre-Edif.B1 (46018-VALENCIA)

1. Motivación

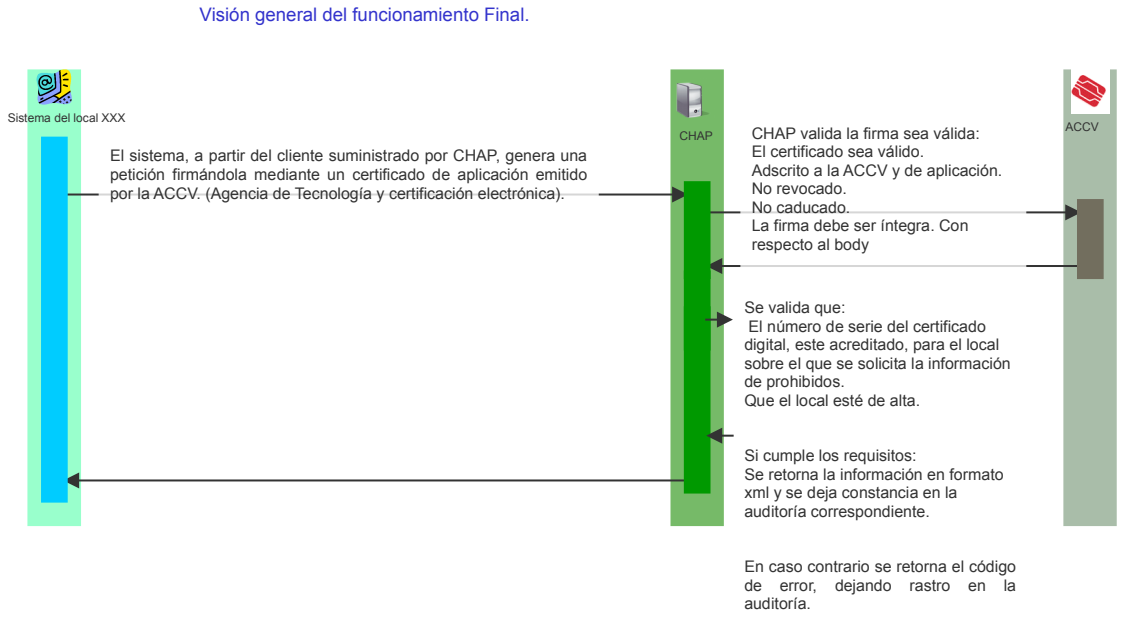
De la necesidad creciente de ofertar la consulta del registro de prohibiciones de acceso a los establecimientos de juego (casinos de juego, salas de bingo, salones de juego y locales específicos de apuestas) de la Comunitat Valenciana, en una tecnología que permita la realización de dicha consulta mediante la comunicación de dos sistemas informáticos, surge el presente servicio web (a partir de ahora WS).

Este WS permitirá a las empresas acreditadas a tal efecto, consultar las personas prohibidas en sus locales, de forma que sus sistemas puedan realizar las consultas pertinentes a los sistemas de la Conselleria de Hacienda y Modelo Económico (A partir de ahora CHME).

La consulta recuperará la información en formato XML, y podrá recuperar la información tanto de un prohibido en concreto dado un local, como la de todos los prohibidos de un local.

2. Visión características generales del servicio

El esquema de funcionamiento general del servicio será el siguiente.



Características generales.

- CHME 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 está realizado con el lenguaje java (versión 1.8 o superior), y más en concreto con Apache CXF.
    - El cliente se suministra en formato de un fichero comprimido ZIP, que contiene el proyecto Eclipse (versión 4.6, Neon) con los archivos fuente necesarios para su ejecución.
    - El cliente es asimismo un proyecto Maven que se puede utilizar de forma independiente a Eclipse.

- Características del WS:
    - Servicio Web síncrono: Se invoca y tras la invocación se obtiene la respuesta.
    - El cliente genera la petición mediante la firma del body del mensaje insertándola en el header de la petición (firma en cabecera SOAP). Mediante el algoritmo http://www.w3c.org/2000/09/xmldsig#rsa-sha1 y http://www.w3c.org/2001/10/xml-exc-c14n#.

- Parámetros de invocación:
  - Provincia del local: Tipo String, ejemplo: 46
  - Municipio del local: Tipo String. ejemplo 250
  - Código de local: Tipo String, ejemplo 5569
  - Criterio de búsqueda: Tipo String, tira de caracteres que acotará la búsqueda del prohibido. Si no se introduce, se recuperarán todos los prohibidos del local. Ej: 19, recuperará todos los prohibidos del local que tengan la tira 19 en su identificador.

Direcció General de Tecnologies de la Informació
C/ Castán Tobeñas, 77.
Ciutat Administrativa 9 D'Octubre-Edif.B1 (46018-VALENCIA)

3. Proceso de desarrollo y pruebas

Para la puesta en marcha del servicio, es necesario que el sistema que hace la invocación 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.

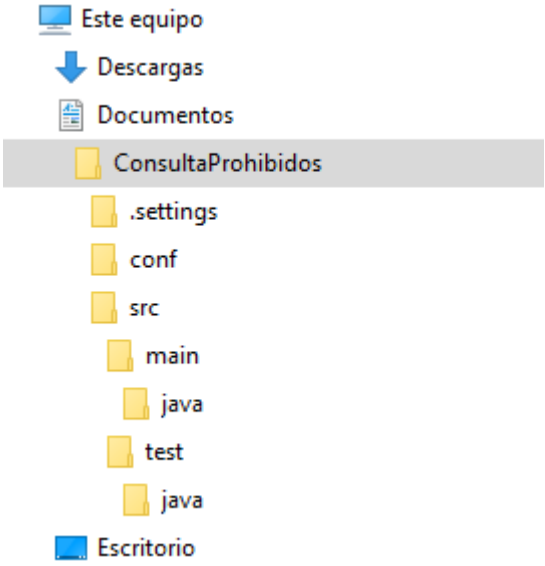
A tal efecto, se ha implantado el servicio en el entorno de pruebas de CHME para la realización de dichas pruebas.

Los pasos recomendados para ello son:

A. Solicitar a CHME acceso al entorno de pruebas. Para ello se debe enviar un correo electrónico a Joc-er (http://www.hisenda.gva.es/web/tributos-y-juego/serviciosgenerales-infogeneral-joc-er, apartado de “Contactar y suscripción”, subapartado “Correo electrónico”), indicando la empresa que desea realizar las pruebas, la dirección/direcciones IP desde la que invocarán al servicio con el fin de abrir el entorno de pruebas y el número de serie del certificado de ciudadano que se utilizará para realizar las pruebas.

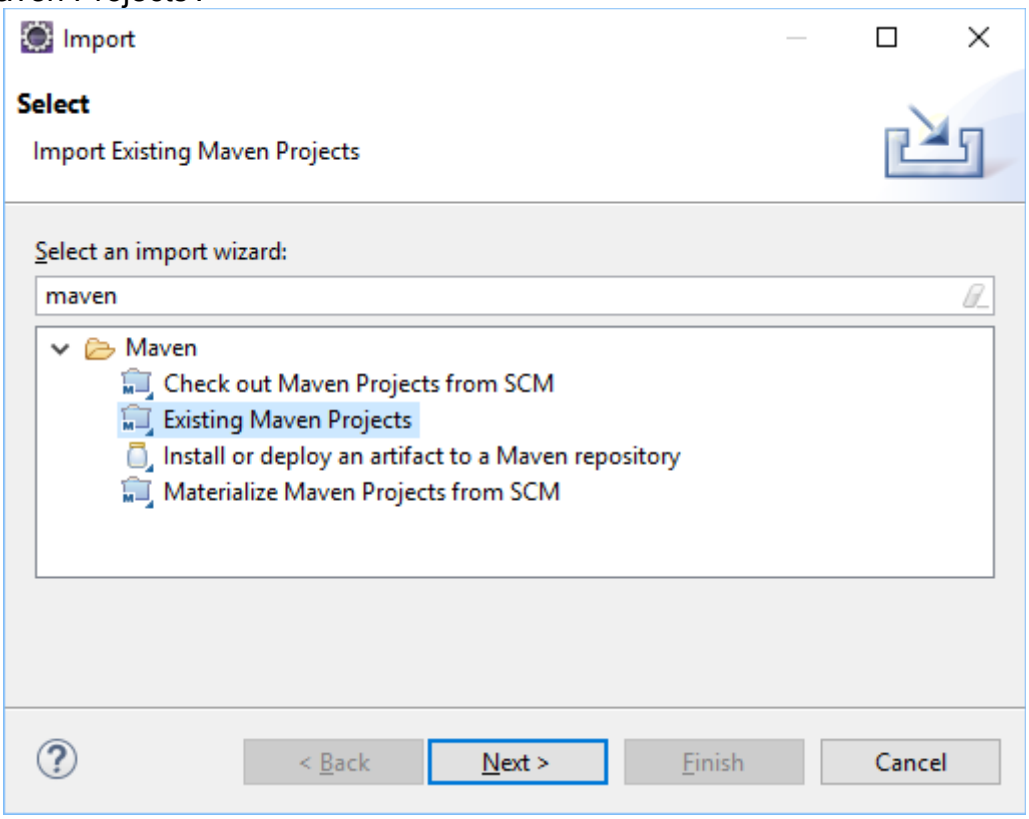
B. Descargar el fichero comprimido con el proyecto eclipse del cliente. Este se encuentra en http://www.hisenda.gva.es/web/tributos-y-juego/serviciosgenerales-infogeneral-joc-er, apartado de “JOC-ER PROHIBIDOS”, subapartado “Documentación y requisitos técnicos”.

   Se propone descomprimirlo en el directorio Documentos quedando la siguiente estructura.

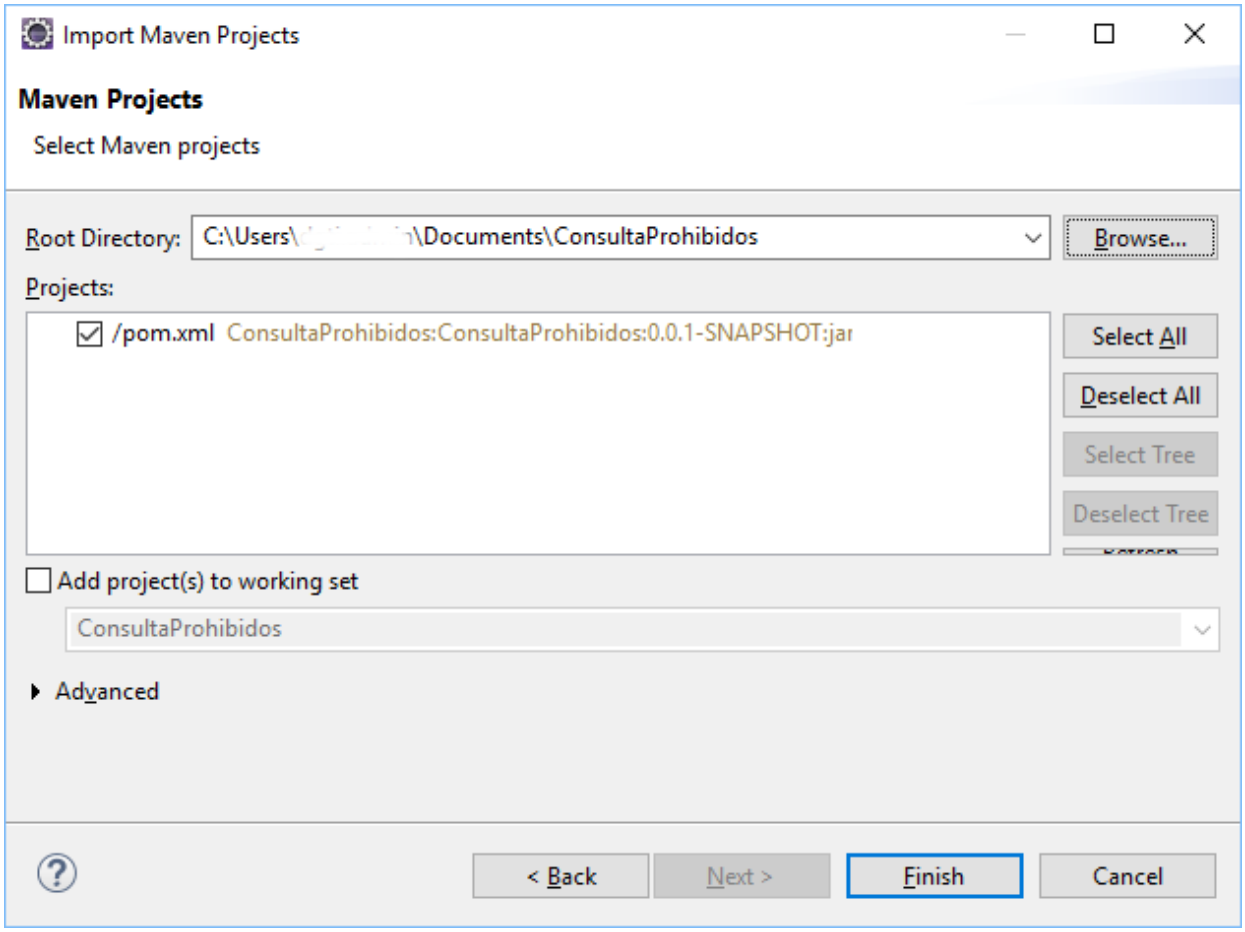


C. Para trabajar con el proyecto se recomienda utilizar el IDE Eclipse, habrá de descargar e instalar la edición Eclipse IDE for Java EE Developers desde el siguiente enlace: https://www.eclipse.org/downloads/eclipse-packages/

D. Una vez instalado importe el proyecto como un proyecto maven, para ello hay que seleccionar la opción de menú File→Import y en ella seleccionar la opción 'Existing Maven Projects':



E. En la siguiente pantalla elija el directorio que acabamos de descargar y deje el resto de opciones por defecto:



F. Consideraciones al proyecto:

- Para la realización de la firma, el proyecto ya contiene un keystore con un certificado de aplicación de pruebas de la ACCV. Se encuentra en: `src\main\resources\keystorepru.jks`

  La clave del keystore es: `keystorepru`
  El alias del certificado es: `prueba - generico _accvcatest_120_`
  El password del certificado 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 no funciona, únicamente está dado de alta como ejemplo. Para probar el servicio hay que poner dentro del keystore un certificado de ciudadano de la ACCV y configurarlo dentro de la aplicación modificando los siguientes ficheros:

- cliente.properties: entradas alias y passCert
- outsecurity_sign.properties: entradas org.apache.ws.security.crypto.merlin.keystore.alias y org.apache.ws.security.crypto.merlin.alias.password

Dicho certificado debe ser dado de alta en el entorno de pruebas de la GVA, para ello se ha de remitir a la CHME tal como se ha indicado en el apartado 3.A.

G. Modificar los ficheros de configuración del proyecto:

- Modificar el fichero WSDL para asegurarse que el endpoint es del entorno de pruebas:
  `src\main\resources\ConsultaProhibidos.wsdl`

```
<WL5G3N0:service name="CONSULTAPROHIBIDOS-service">
  <WL5G3N0:port binding="WL5G3N2:CONSULTAPROHIBIDOS_ptt-binding" name="CONSULTAPROHIBIDOS-port">
    <WL5G3N3:address location="https://instrumental-pre.gva.es/Hacienda/Acuario/AcuarioProhibidos/ConsultaProhibidos"/>
  </WL5G3N0:port>
</WL5G3N0:service>
```

- Asegurarse que el fichero de configuración `src\main\resources\cliente.properties` contiene las opciones de configuración correctas:

```
#Siempre este valor
accion=Signature

#Valor del alias con el que se ha introducido el certificado
# en el keystore
alias=certificado_aplicacion

#password del certificado en el keystore
passCert=hNUK.czC

#ubicación del wsdl
wsdl=ConsultaProhibidos.wsdl
```

- Asegurarse que el fichero de configuración `src\main\resources\outsecurity_sign.properties` contiene las opciones de configuración correctas:

```
#password del keystore
org.apache.ws.security.crypto.merlin.keystore.password=keystorepru

#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=certificado_aplicac
ion

#ubicación del keystore
```

```
org.apache.ws.security.crypto.merlin.file=keystorepru.jks
```

- Asegurarse que la clase principal de invocación, está perfectamente configurada:
  `src\main\java\com\oracle\xmlns\pcbpel\adapter\db\pro_prohibidosws_ws_getprohibidospermisos_af_ps\getprohibidosws_af_ps\consultaprohibidos\CONSULTAPROHIBIDOSPortClient.java`

- Se deben modificar los parámetros de invocación:

  El local (parámetros obligatorios):
  ```
  JAXBElement<String> LocalProv=of.createInputParametersPLOCALPROV("46");
  JAXBElement<String> LocalMun=of.createInputParametersPLOCALMUN("250");
  JAXBElement<String> LocalCod=of.createInputParametersPLOCALCODIGO("5569");
  ```

  Criterio para acotar la búsqueda(opcional):
  ```
  JAXBElement<String> Criterio=of.createInputParametersPNIFCONSULTA("19");
  ```

  Si existe un criterio para acotar la búsqueda, se recuperan únicamente los prohibidos del local tal que el identificador cumpla con dicho criterio.
  En el ejemplo, todos aquellos que tengan la subcadena 19, da igual en que posición, en el identificador.

  Se admiten caracteres comodín: * para un conjunto de caracteres e ¿ para un carácter.

  Ejemplos:
  - 19: Recupera todos los que cumplan *19*.
  - 1?9: Recupera todos los que cumplan *1?9*.

  Si no se introduce criterio de búsqueda, se recuperarán todos los prohibidos del local.

H. Invocación y resultado.

Una vez realizados, todos los cambios de configuración, se puede ejecutar mediante la ejecución de la clase `src\main\java\com\oracle\xmlns\pcbpel\adapter\db\pro_prohibidosws_ws_getprohibidospermisos_af_ps\getprohibidosws_af_ps\consultaprohibidos\CONSULTAPROHIBIDOSPortClient.java` desde el propio Eclipse.

También es posible la ejecución des de una consola del sistema operativo mediante las ordenes:

- mvn clean: limpia los binarios generados de la aplicación, hemos de tener en cuenta que <u>siempre que modifiquemos el keystorepru.jks hemos de realizar una operación de limpieza de binarios (con esta orden o directamente desde Eclipse) para que el keystore modificado se propague al entorno de ejecución</u>.
- mvn test: lanza la ejecución de las operaciones de testeo unitario JUnit

- mvn exec:java -Dexec.mainClass="com.oracle.xmlns.pcbpel.adapter.db.pro_prohibidosws_ws_getprohibidospermisos_af_ps.getprohibidosws_af_ps.consultaprohibidos.CONSULTAPROHIBIDOSPortClient": lanza la ejecución directa de conexión al WS.

Si la ejecución es correcta el resultado vendrá dado por:

Petición:

```
<soap:Body xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-
wssecurity-utility-1.0.xsd" wsu:Id="id-1">
  <InputParameters
xmlns="http://xmlns.oracle.com/pcbpel/adapter/db/OWNPROHI/QPRO_PROHIBIDOSWS_WS/CONSULTAP
ROHIBIDOSWS/">
    <P_LOCAL_PROV>46</P_LOCAL_PROV>
    <P_LOCAL_MUN>250</P_LOCAL_MUN>
    <P_LOCAL_CODIGO>5569</P_LOCAL_CODIGO>
    <P_NIF_CONSULTA>19</P_NIF_CONSULTA>
    <P_PARAPLICA>
      <P_PARAPLICA_ITEM>
        <CODIGO></CODIGO>
        <VALOR></VALOR>
      </P_PARAPLICA_ITEM>
    </P_PARAPLICA>
  </InputParameters>
</soap:Body>
```

Respuesta:

```
<soap-env:Body xmlns:soap-env="http://schemas.xmlsoap.org/soap/envelope/">
<con:OutputParameters xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:con="http://xmlns.oracle.com/pcbpel/adapter/db/OWNPROHI/QPRO_PROHIBIDOSWS_WS/CONSUL
TAPROHIBIDOSWS/">
<con:CONSULTAPROHIBIDOSWS>S</con:CONSULTAPROHIBIDOSWS>
  <con:P_RESULTADO>
    <![CDATA[
      <FICHERO>
        <DOC_SOLIC>16491c96a5447dc1</DOC_SOLIC>
        <NOM_SOLIC>BINGO DE PRUEBAS</NOM_SOLIC>
        <FECHA_CONSULTA>09/08/2012 09:52:37</FECHA_CONSULTA>
        <LOCAL_CONSULTA>BINGO DE PRUEBAS</LOCAL_CONSULTA>
        <COD_SERVICIO>2</COD_SERVICIO>
        <REG>
          <DOCUMENTO>000000X2992519N</DOCUMENTO>
          <NOMBRE>VORONKA  ANATOLIY</NOMBRE>
        </REG>
        <REG>
          <DOCUMENTO>00000029191032F</DOCUMENTO>
          <NOMBRE>ADAN TORRES VICTOR</NOMBRE>
        </REG>
        …..
      </FICHERO>
    ]]>
  </con:P_RESULTADO>
  <con:P_CODERROR/>
  <con:P_DESCERROR/>
</con:OutputParameters>
</soap-env:Body>
```

Si la ejecución es correcta el tag, `<con:CONSULTAPROHIBIDOSWS>` retornará S, y los tags `<con:P_CODERROR/>` y `<con:P_DESCERROR/>` estarán vacíos.

El resultado se recuperará en el tag `</con:P_RESULTADO>` en el que se encontrará un xml con la siguiente estructura:

`<FICHERO>`	Tag de inicio
`<DOC_SOLIC>16491c96a5447dc1</DOC_SOLIC>`	Número de serie del certificado digital que realiza la petición.
`<NOM_SOLIC>BINGO DE PRUEBAS</NOM_SOLIC>`	Nombre del local que realiza la petición. (El enviado en los parámetros de la petición).
`<FECHA_CONSULTA>09/08/2012 09:52:37</FECHA_CONSULTA>`	Fecha en la que se realiza la consulta
`<LOCAL_CONSULTA>BINGO DE PRUEBAS</LOCAL_CONSULTA>`	Nombre del local que realiza la petición. (El enviado en los parámetros de la petición).
`<COD_SERVICIO>2</COD_SERVICIO>`	Tipo de servicio solicitado: 1.- Todos los prohibidos. 2.- Se ha indicado un filtro. Nota: no se indica que filtro.

`<REG>`
`<DOCUMENTO>000000X2992519N</DOCUMENTO>`
`<NOMBRE>VORONKA ANATOLIY</NOMBRE>`
`</REG>`
`<REG>`
`<DOCUMENTO>00000029191032F</DOCUMENTO>`
`<NOMBRE>ADAN TORRES VICTOR</NOMBRE>`
`</REG>`
…..
	Conjunto de repetición con el número de documento y nombre de los prohibidos del local que cumplen el criterio de búsqueda.

`</FICHERO>`	Tag de fin de xml.

I. Gestión de errores.

Si se producen errores, se distinguen dos tipos de errores cada uno informando en un punto diferente.

- <u>Errores de infraestructura:</u> Estos errores son errores de comunicación, de formato, de validación de certificado, etc…que implican que el servicio no llegue a ejecutarse:

  Se capturan en el catch (javax.xml.ws.soap.SOAPFaultException ex) de la invocación.

  Los errores más comunes son:

BEA-XXXXXX	Errores de formato o de validación de firma. Propios del Oracle Service bus.
00106	Error en la validación del certificado.
00107	Error en el tipo de certificado o en la inserción de los logs de auditoría de servicio.
01108	El local no existe
01109	El local existe pero esta de baja.
01110	El usuario no está acreditado en el local. Es decir, el certificado digital no está asociado

	al local que se está consultando (o no se ha acreditado, o la acreditación no se ha tramitado).

- Errores de Aplicación: El servicio se llega a ejecutar, pero con resultado erróneo. En este caso el servicio retorna:

Si la ejecución no es correcta el tag, `<con:CONSULTAPROHIBIDOSWS>` retornará N, y los tags `<con:P_CODERROR/>` y `<con:P_DESCERROR/>` estarán informados, con el error.

Del mismo modo, en el XML que retorna el servicio del tag P_RESULTADO se reflejará el mismo error.

A continuación se muestra un ejemplo de respuesta con error de aplicación:

<con:CONSULTAPROHIBIDOSWS>N</con:CONSULTAPROHIBIDOSWS>	Resultado con error de aplicación
<con:P_RESULTADO>	Inicio del resultado de la aplicación
<FICHERO>	Tag de inicio
<DOC_SOLIC>16491c96a5447dc1</DOC_SOLIC>	Número de serie del certificado digital que realiza la petición.
<NOM_SOLIC>BINGO DE PRUEBAS</NOM_SOLIC>	Nombre del local que realiza la petición. (El enviado en los parámetros de la petición).
<FECHA_CONSULTA>09/08/2012 09:52:37</FECHA_CONSULTA>	Fecha en la que se realiza la consulta
<LOCAL_CONSULTA>BINGO DE PRUEBAS</LOCAL_CONSULTA>	Nombre del local que realiza la petición. (El enviado en los parámetros de la petición).
<COD_SERVICIO>2</COD_SERVICIO>	Tipo de servicio solicitado: 1.- Todos los prohibidos. 2.- Se ha indicado un filtro. Nota: no se indica que filtro.
<ERROR>04:Local de baja</ERROR>	Error de la aplicación
</FICHERO>	Tag de fin de xml.
</con:P_RESULTADO>	Tag de fin de resultado de la aplicación.
<con:P_CODERROR>04</con:P_CODERROR>	Propagación del código de error de la aplicación
<con:P_DESCERROR>Local de baja</con:P_DESCERROR>	Propagación de la descripción del error de la aplicación.
</con:OutputParameters>	

Los posibles errores son:

04	Local de baja en prohibidos pero no en juego.
05	Error al insertar en la auditoría de aplicación.
06	Error no controlado + descripción.

4. Proceso de paso a producción

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

A. Obtención de un Certificado de Aplicación de la ACCV desde la web de la accv (www.accv.es).

   Una vez dentro de la web, seleccionar la pestaña “Empresas”, y dentro de esta seleccionar “Certificados de Aplicación”.

   Hay que observar que en los certificados de aplicación se debe tener en cuenta el texto con el que se solicite el certificado. Se recomienda introducir los siguientes valores en el formulario de solicitud del nuevo certificado de aplicación:

   - **Nombre de la aplicación:** JUEGO
   - **Nombre del servicio:** Nombre de la empresa que está solicitando el certificado.
   - **E-mail:** Correo electrónico de contacto de la empresa que está solicitando el certificado.

   La firma de los documentos tendrá el aspecto siguiente:

ID DOCUMENT / ID DOCUMENTO	msClxk7B0OmjjG.t5fh0xQ$$		PÁGINA / PÁGINA	1 / 1
FIRMAT PER / FIRMADO POR	VALIDESA 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/es/VerificacionCiudadanoAction.action

B. Acreditar dicho certificado ante el Servicio de Juego.
Para ello hay que rellenar la credencial, http://www.hisenda.gva.es/web/tributos-y-juego/serviciosgenerales-infogeneral-joc-er-prohibidos, dentro del apartado “JOC-ER PROHIBIDOS”, haciendo constar:
   - En el campo Razon Social: La Razón social del local.
   - NIF Entidad: nif del titular del local.
   - Número de inscripción en el registro: el número de local en el registro de establecimientos autorizados.
   - Colectivo al que está adscrito: Local
   - Dirección del local.
   - Nombre de usuario: El que se desee que figure en el registro de acreditados. Por ejemplo: El nombre del local.
   - NIF del usuario/nº de serie del certificado: En este caso, el número de serie del certificado. Distinguiendo entre mayúsculas y minúsculas.
   - Datos del representante.
   - Seleccionar como opción el “alta servicio web de consulta de prohibidos” y como tipo de certificado “certificado de aplicación”.

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

En este caso, la acreditación vendrá firmada por el representante.

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 nuevo certificado de producción. Dando pues un valor al password del certificado, al alias del certificado y al password del keystore.
   - 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 de producción es: https://atenea.ha.gva.es/wse/ConsultaProhibidos?WSDL
  hay que cambiarla en el fichero ConsultaProhibidos.wsdl

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 pueden descargar desde la siguiente página: http://www.accv.es/ayuda/descargar-certificados-digitales/

5. ANEXO I: PORTECLE: Gestión de keystores.

- Generación del keystore.

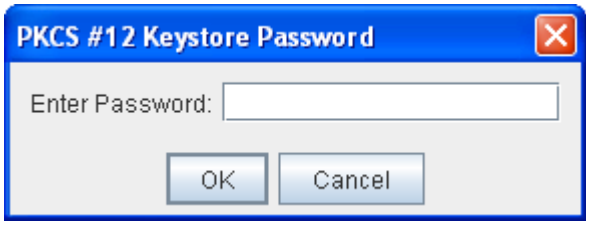
  Si no se dispone de un Java Keystore, deberá generarse uno a partir del certificado de firma válido para realizar la invocación. Para ello se aconseja el uso de la aplicación 'Portecle'.

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

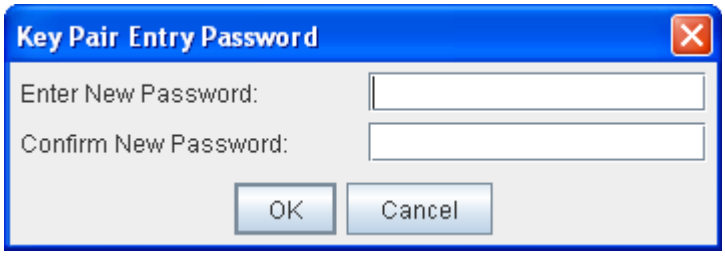
  Nota: Es posible que se deba bajar para la máquina virtual java los ficheros para aplicar "unlimited strength jurisdiction policy files" (http://www.oracle.com/technetwork/java/javase/downloads/jce8-download-2133166.html)

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

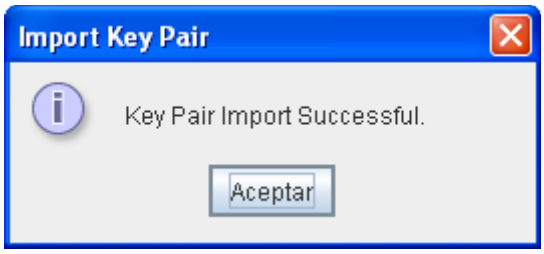
  - Solicita el password del certificado.



  - Vuelve a solicitar el password del certificado.



  Se importa correctamente…

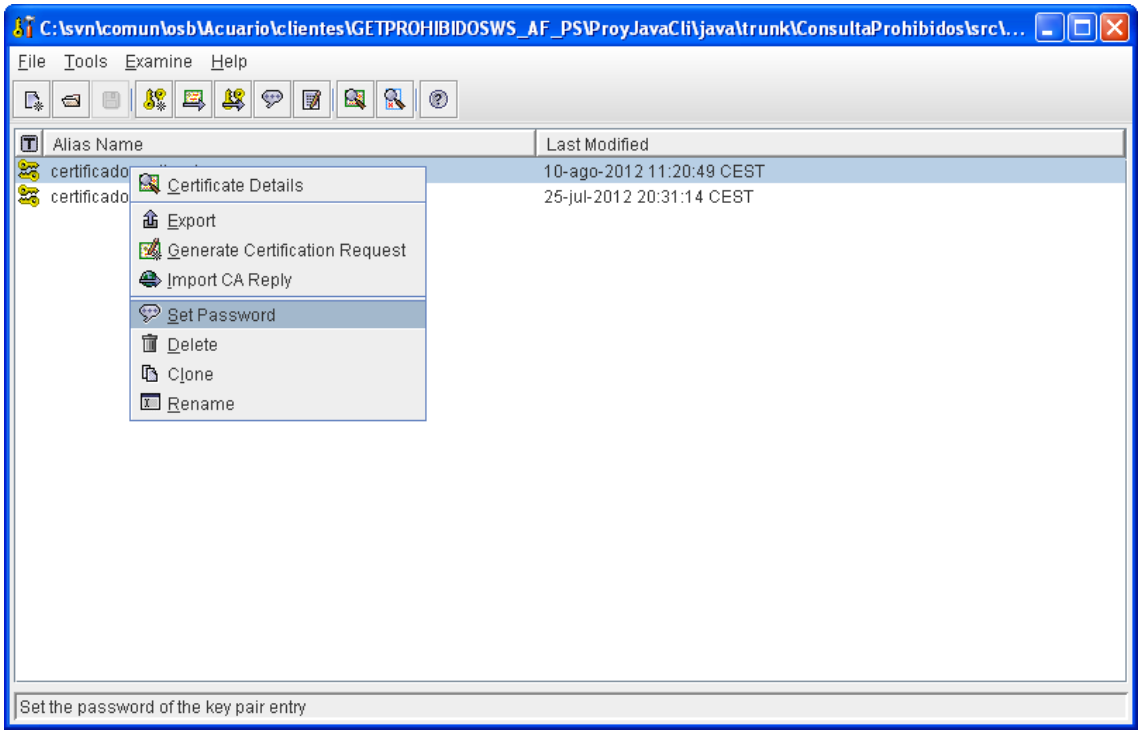


- Al guardar el keystore como fichero solicitará la clave para el keystore.

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

  - En 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.



Direcció General de Tecnologies de la Informació
C/ Castán Tobeñas, 77.
Ciutat Administrativa 9 D'Octubre-Edif.B1 (46018-VALENCIA)

6. ANEXO II: Prueba y depuración del servicio mediante SoapUI

Se compone de los siguientes pasos:

6.1 Instalación del software de testeo del 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.

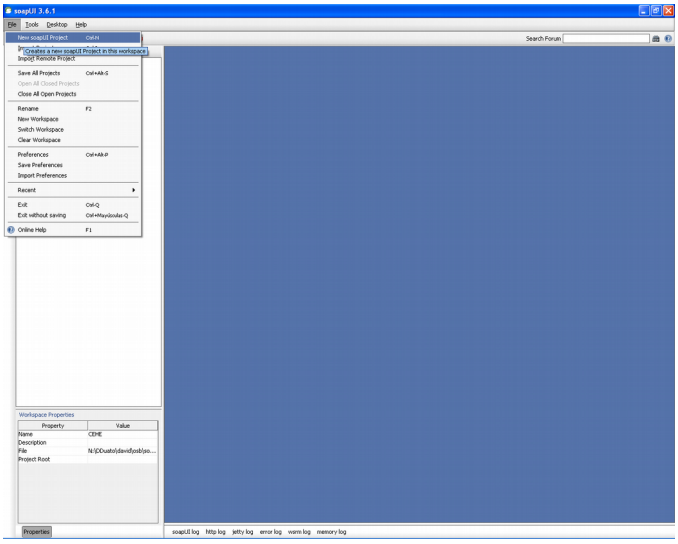
SopaUI se puede obtener de:
http://www.soapui.org/

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

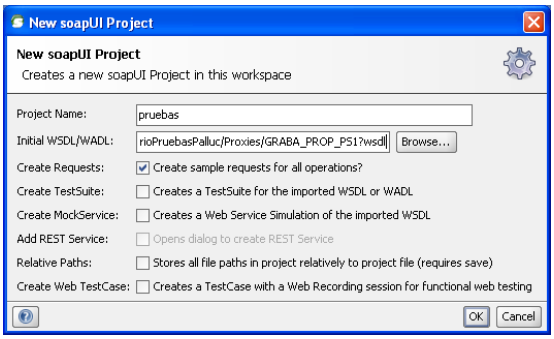
6.2 Testeo del servicio

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.

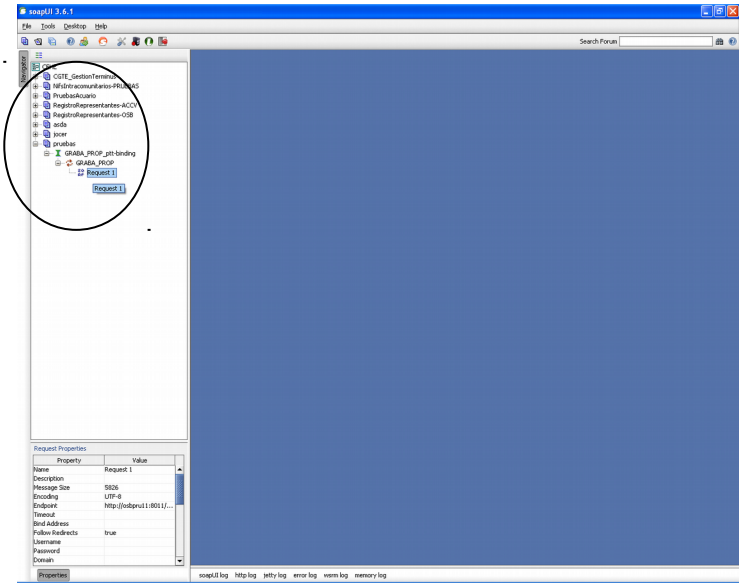


2. Solicitará la introducción del nombre del proyecto, y la url donde se encuentra el WSDL del servicio.



Nota: en pruebas… es como la siguiente…
https://pruebas.ha.gva.es/wse/ConsultaProhibidos?WSDL

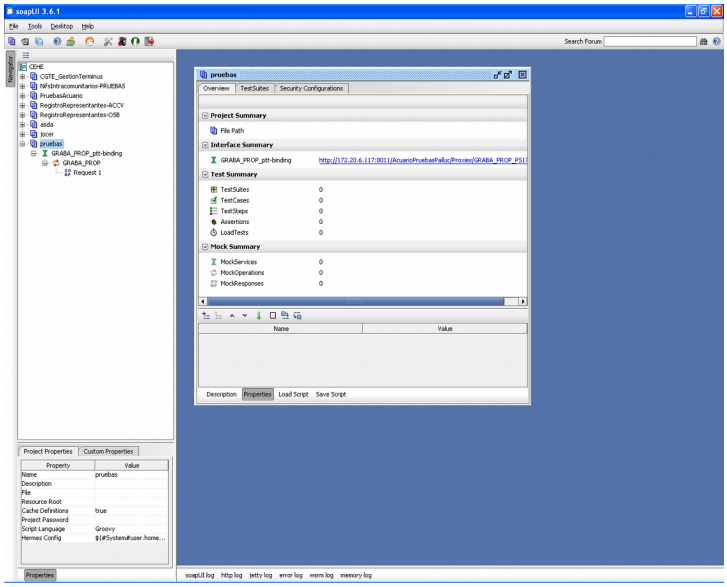
Tras pulsar siguiente, se creará la estructura necesaria para su invocación.



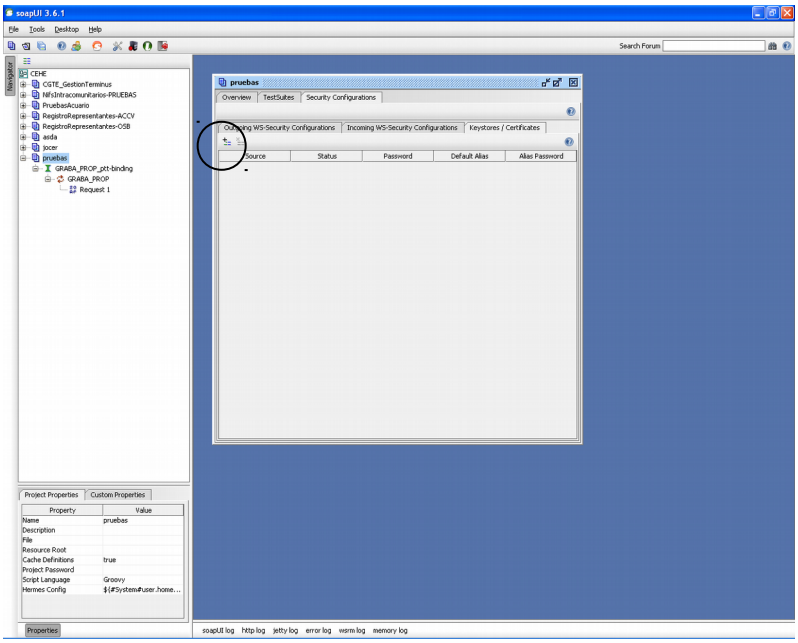
3. Introducir certificados digitales en el almacén de certificados.

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

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



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

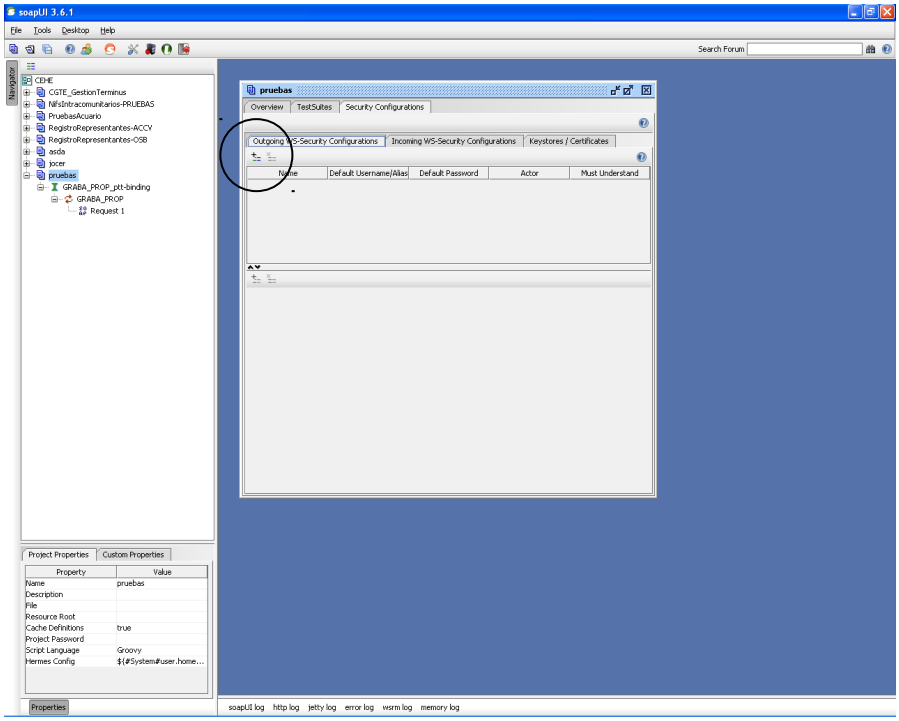


c) Posteriormente presenta una ventana para seleccionar un certificado del Sistema de Ficheros, así como su contraseña.

d) Este proceso, se debe repetir por cada certificado digital que se desea utilizar.

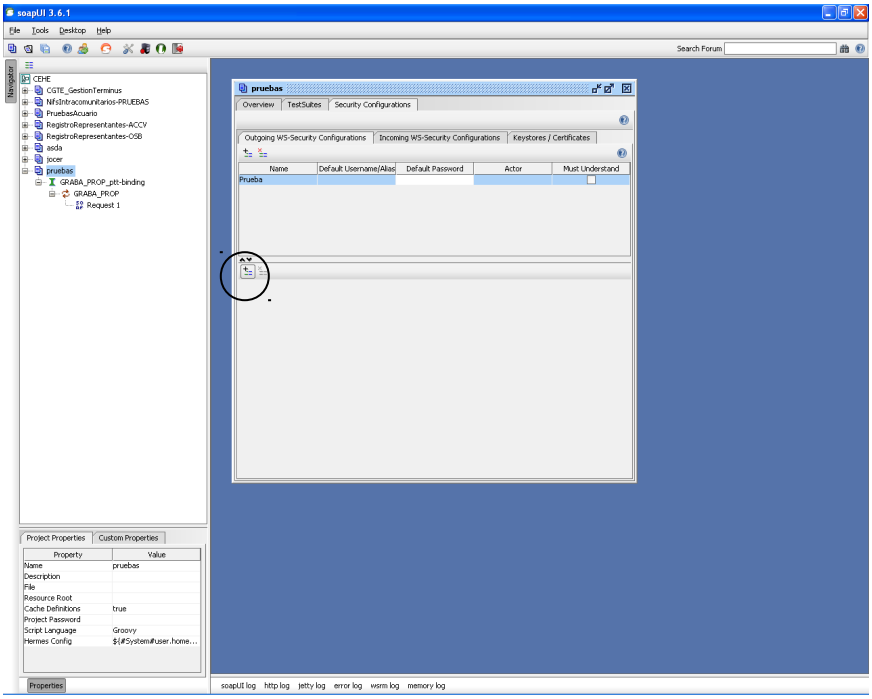
4. Configurar los parámetros de seguridad de salida del certificado.

a) En la misma ventana seleccionamos la pestaña “Outgoing WS-Security Configurations”, y creamos una configuración pulsando el icono de “Crear”.



Nos solicitará un nombre de configuración.

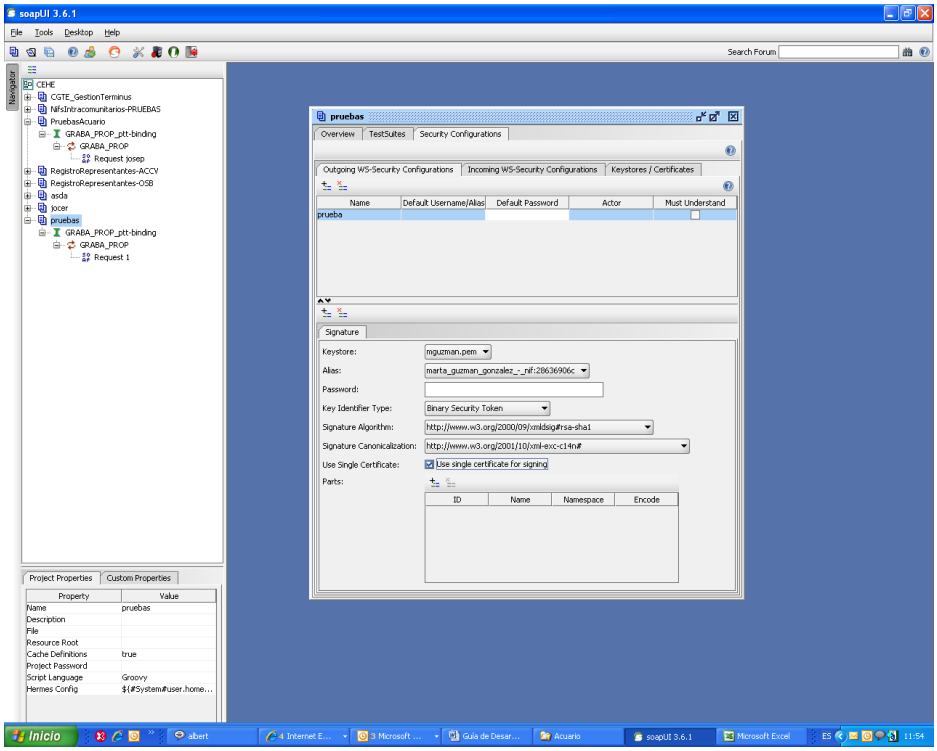
b) En la misma ventana, en la parte inferior, seleccionamos la pestaña “Outgoing WS-Security Configurations”, y seleccionamos crear uno.



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

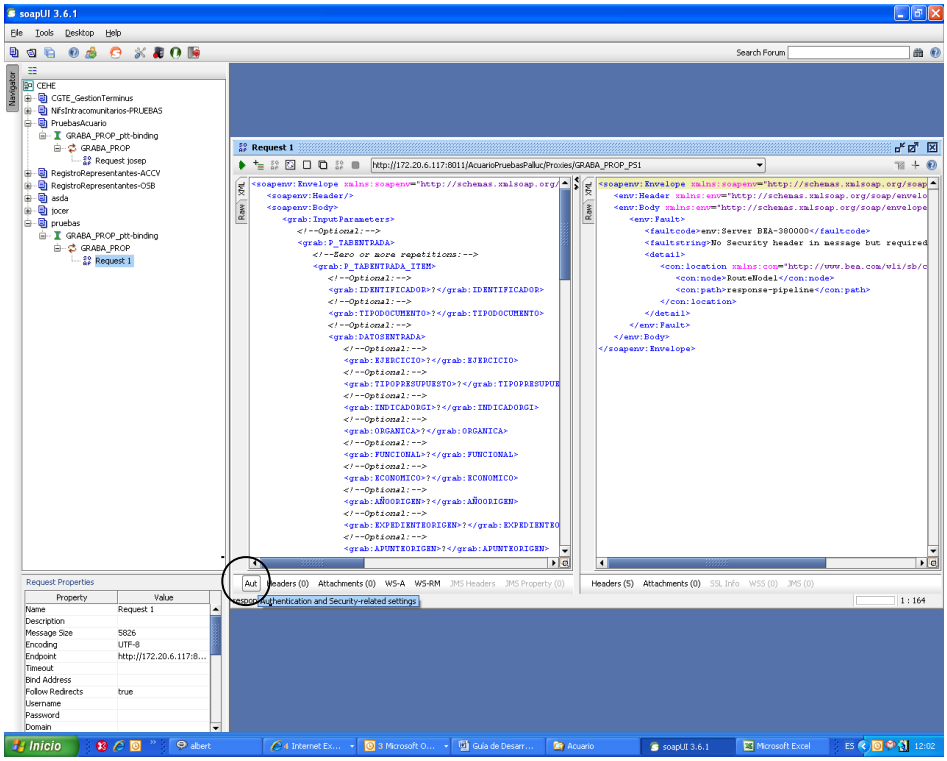
A continuación se presentará la información de configuración, en la que hay que establecer.

- 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



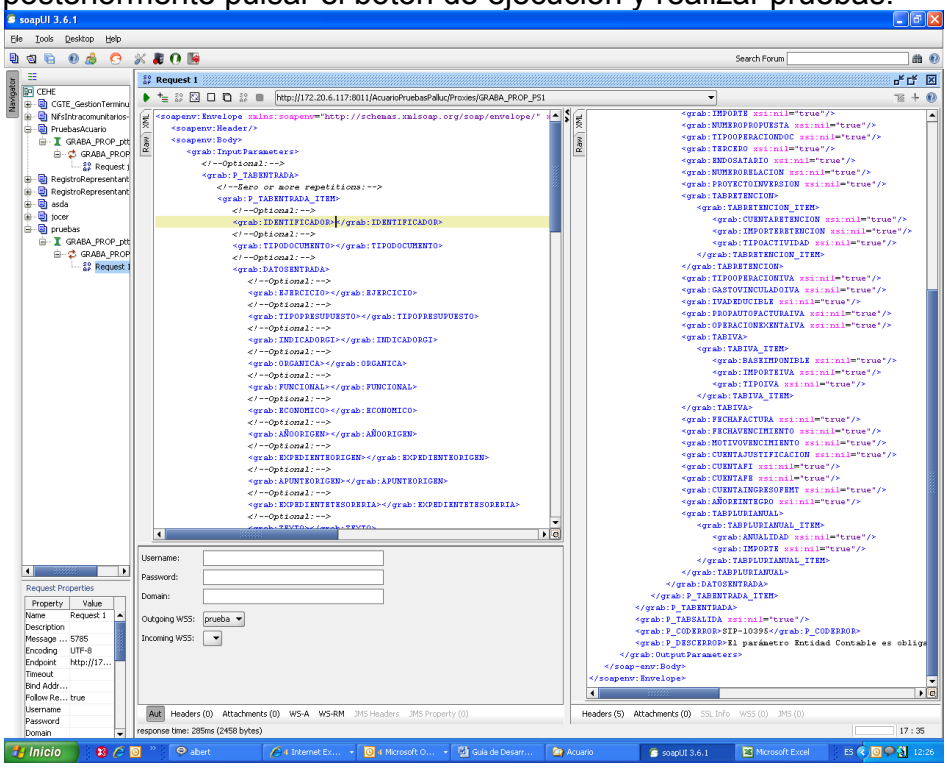
5. Probar el servicio.

   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 “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

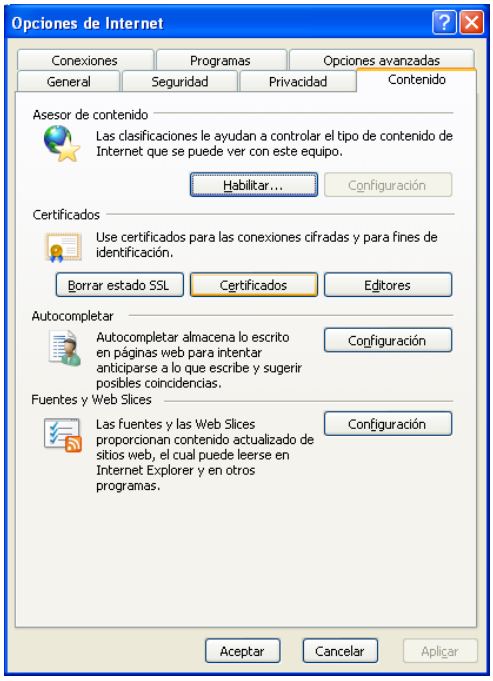
El ejemplo se explicará para el navegador Internet Explorer. Aunque el procedimiento es similar para otros navegadores.

7.1 Incorporar el certificado al navegador

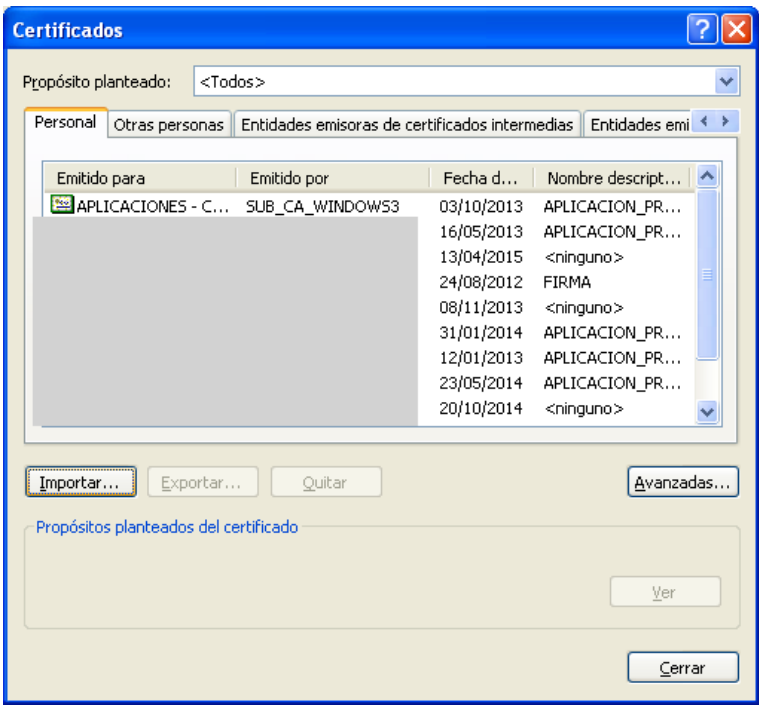
1. El certificado debe estar en soporte de fichero.

2. Abrir el navegador, Internet Explorer.

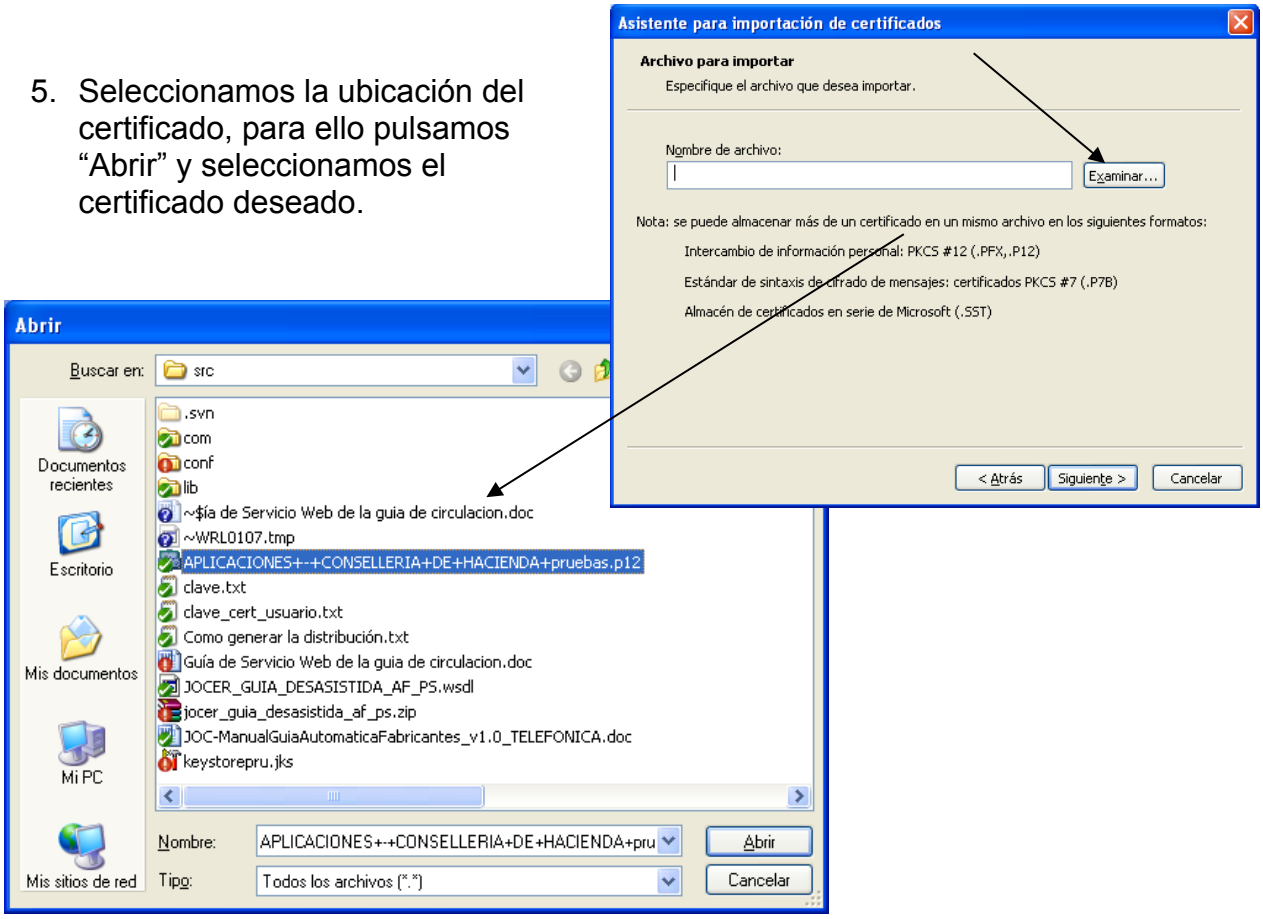
3. Seleccionar del menú Herramientas/Opciones de Internet. Dentro de este seleccionar la pestaña de “Contenido” y pulsar el botón de “Certificados”.



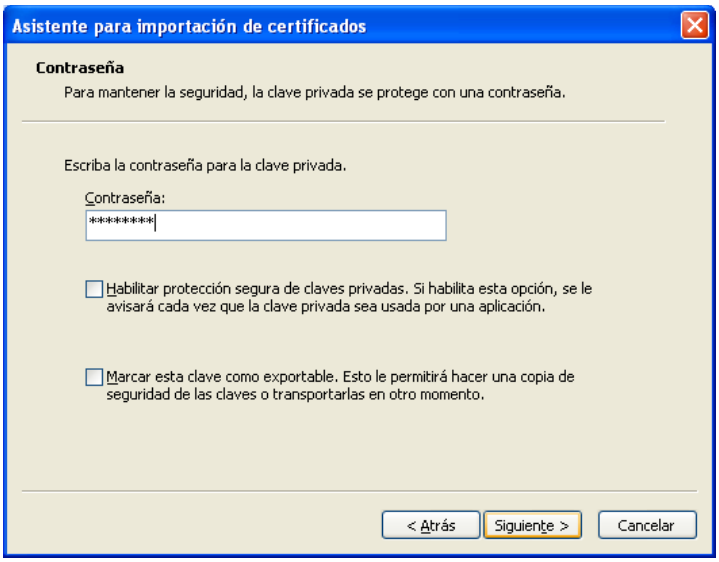
4. Pulsar el botón “Importar”, y se abrirá al asistente para importar el certificado.



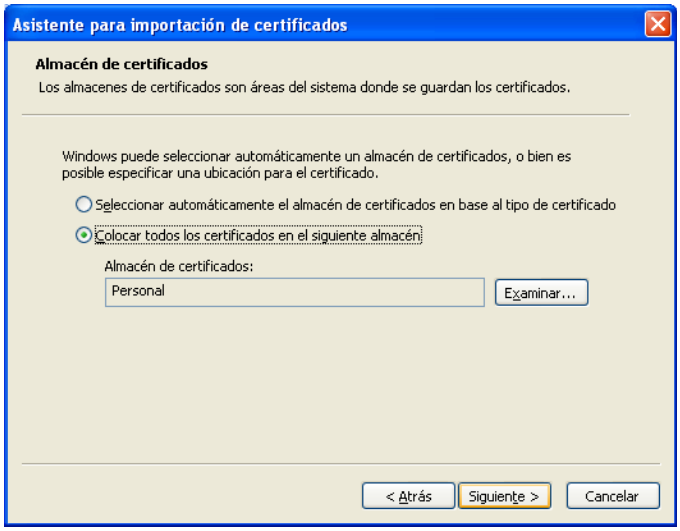
5. Seleccionamos la ubicación del certificado, para ello pulsamos "Abrir" y seleccionamos el certificado deseado.



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

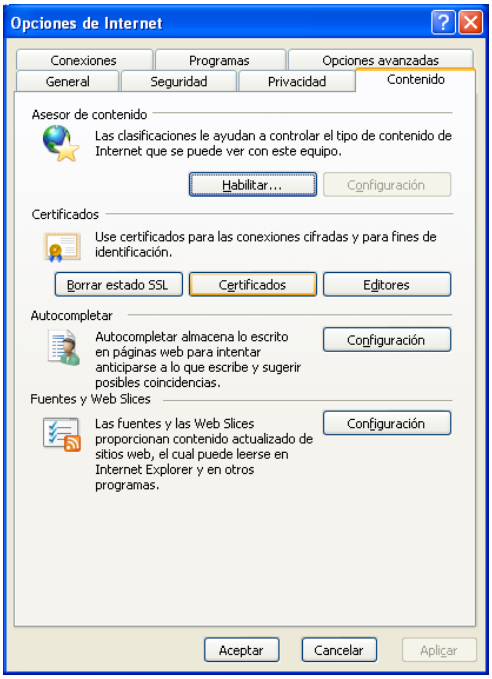


7. Seleccionamos el almacén “Personal”, y pulsamos siguiente y finalizar.



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

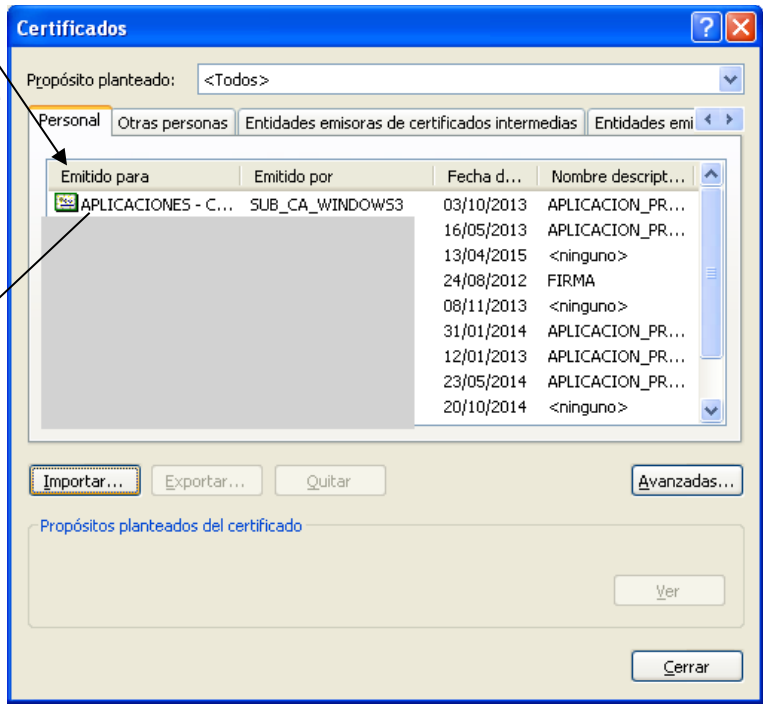
7.2 Ver la información del certificado e imprimir su número de serie.

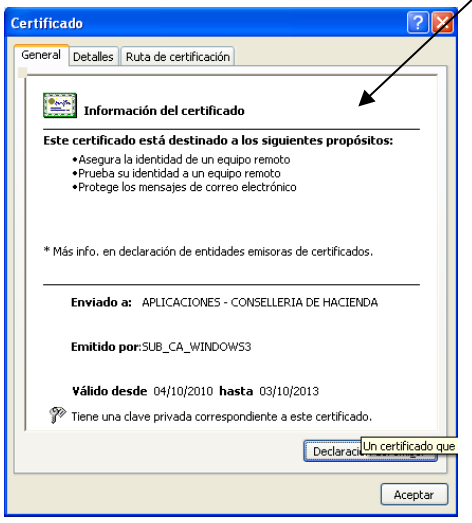


1. Abrir el navegador, Internet Explorer.

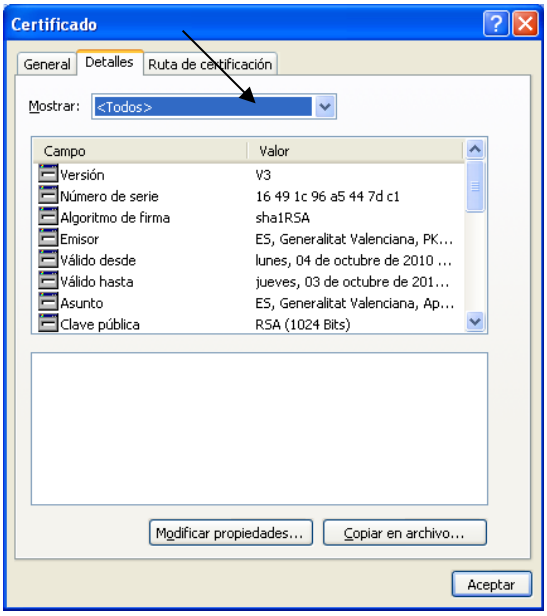
2. Seleccionar del menú Herramientas/Opciones de Internet. Dentro de este seleccionar la pestaña de “Contenido” y pulsar el botón de “Certificados”.

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.

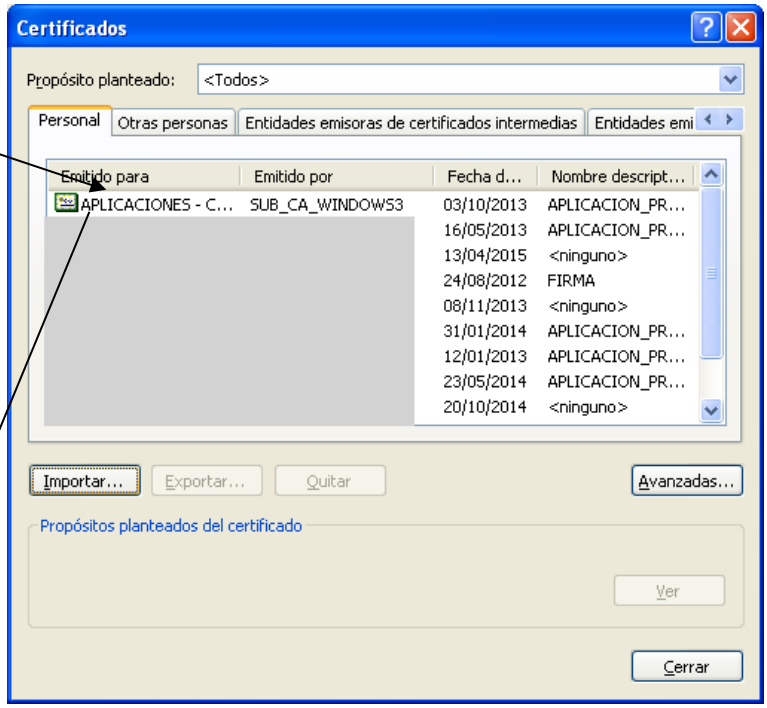
7.3 Suprimir el certificado del navegador.

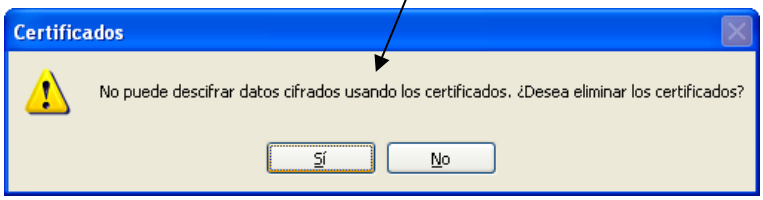
1. Abrir el navegador, Internet Explorer.

Direcció General de Tecnologies de la Informació
C/ Castán Tobeñas, 77.
Ciutat Administrativa 9 D'Octubre-Edif.B1 (46018-VALENCIA)

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.