



**Gobierno de Canarias**

Consejería de Presidencia,  
Justicia y Seguridad  
Dirección General de  
Telecomunicaciones  
y Nuevas Tecnologías



**Platino**  
Plataforma de Interoperabilidad del  
Gobierno de Canarias

Oficina Técnica PLATINO

Página 1 de 15

## CONSUMO DE LOS SERVICIOS DE PLATINO MEDIANTE SOAPUI

Rev.	Fecha	Descripción	
0	18/05/2009	Redacción inicial	
1	15/07/2009	Corrección del parámetro "use single certificate"	
2	29/12/2011	Añade el parámetro Digest Algorithm, para SoapUI 4.x	
<b>Documento :</b>			
<b>Ubicación en eRoom:</b>			
<b>Preparado por</b>		<b>Revisado por</b>	<b>Aprobado por</b>
D. Gral. de Telecomunicaciones y Nuevas Tecnologías		D. Gral. de Telecomunicaciones y Nuevas Tecnologías	D. Gral. de Telecomunicaciones y Nuevas Tecnologías
<b>Fecha: 15/07/2009</b>		<b>Fecha: 15/07/2009</b>	<b>Fecha: 15/07/2009</b>



**Gobierno  
de Canarias**

Consejería de Presidencia,  
Justicia y Seguridad  
Dirección General de  
Telecomunicaciones  
y Nuevas Tecnologías



**Platino**  
Plataforma de Interoperabilidad del  
Gobierno de Canarias

Consumo de los servicios de Platino mediante soapUI

Página 2 de 15

## ÍNDICE

<b><u>1</u></b>	<b><u>INTRODUCCIÓN</u></b>	<b><u>3</u></b>
<b><u>2</u></b>	<b><u>REQUISITOS</u></b>	<b><u>3</u></b>
<b><u>3</u></b>	<b><u>CONFIGURACIÓN DE SOAPUI</u></b>	<b><u>4</u></b>
3.1	Creación del proyecto	5
3.1.1	Creación de las interfaces	6
3.2	Configuración del proyecto	8
3.3	Configuración de la interfaz	12
3.4	Configuración de soapUI	12
3.5	Prueba de funcionamiento	13
<b><u>ANEXO I</u></b>	<b><u>OBTENER EL ALIAS DEL CERTIFICADO</u></b>	<b><u>15</u></b>

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia y Seguridad Dirección General de Telecomunicaciones y Nuevas Tecnologías	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Consumo de los servicios de Platino mediante soapUI	Página 3 de 15

## 1 INTRODUCCIÓN

Platino ofrece una arquitectura basada en servicios web que permite ofrecer diferentes servicios de forma desacoplada. Además dispone de una capa de seguridad que utiliza la tecnología *Web Service Security* (WSS) para garantizar el acceso seguro a los recursos.

Por otro lado, soapUI es una aplicación gratuita y *open source*, enfocada a la verificación de servicios web, que permite inspeccionarlos, invocarlos o realizar simulaciones.

En este documento se describe como configurar soapUI para poder consumir los servicios de Platino, prestando especial atención a la configuración de la seguridad.

## 2 REQUISITOS

Antes de empezar a configurar la herramienta soapUI debemos disponer de los siguientes elementos:

- **Aplicación soapUI:** Para el presente documento hemos utilizado la versión 2.5.1. Esta aplicación se puede obtener de forma gratuita en [www.soapui.org](http://www.soapui.org)
- **Certificado Platino:** Certificado digital emitido por la CA de Cibercentro que permite identificar el BackOffice en Platino y determinar los permisos para el acceso a los recursos. Se puede obtener más información en <http://www.gobiernodecanarias.org/platino/autenticacion.html>
- **URI de servicio/backoffice/tercero:** Permite identificar al sistema o persona que está realizando la petición al servicio de Platino.
- **Acceso VPN:** Para los usuarios que se encuentren fuera de la red del Gobierno de Canarias será necesario que dispongan de acceso a los servidores de Platino. Para ello deberán seguir los pasos que se explican en <http://www.gobiernodecanarias.org/platino/accesoVPN.html>



### 3 CONFIGURACIÓN DE SOAPUI



Para configurar correctamente la aplicación **soapUI** debemos realizar los siguientes pasos:

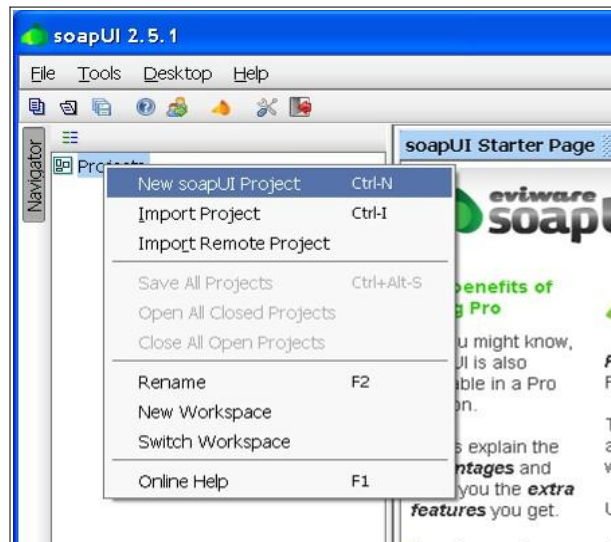
- **Creación del proyecto:** Permite definir un proyecto junto a las interfaces de los servicios de Platino, que contendrá las interfaces de los diferentes *web services* de Platino y sobre el que se aplica la configuración de seguridad
- **Configuración del proyecto:** Permite establecer la configuración para las cabeceras de seguridad que se incluyen en las peticiones a Platino
- **Configuración de la interfaz:** Indica como aplicar la configuración de seguridad a la interfaz de cada servicio
- **Configuración de soapUI:** Datos de configuración de la herramienta
- **Prueba de funcionamiento:** Realización de una prueba para comprobar el correcto funcionamiento de la configuración utilizada



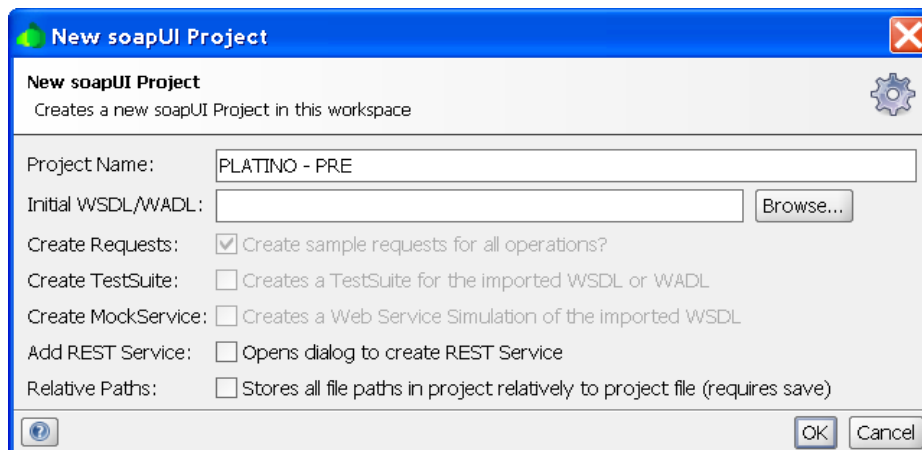
### 3.1 Creación del proyecto

El primer paso consiste en la creación de un proyecto que contendrá todas las interfaces (wsdl) correspondientes a los servicios de Platino. Para ello realizamos los siguientes pasos:

1. Pulsar botón derecho del ratón sobre *Projects* y seleccionar “New soapUI Project / *Ctrl-N*”:



2. Se muestra una ventana en la se debe introducir un nombre para el proyecto. En este caso le daremos el nombre “**PLATINO – PRE**”:

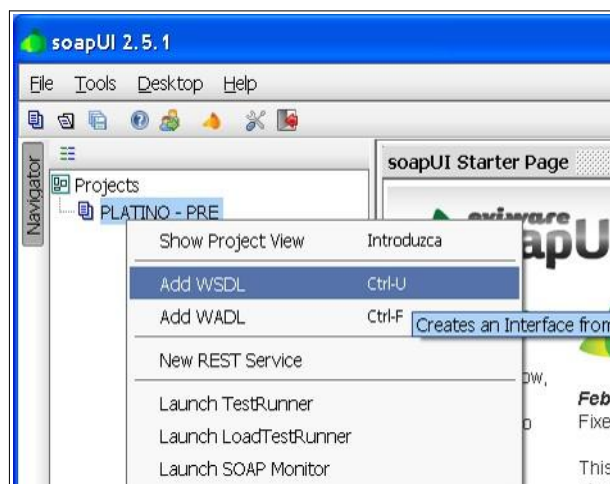


Se puede incluir el *wsdl* de alguno de los servicios. Como en este caso Platino dispone de varios *wsdl*, se muestra a continuación como incluirlos.

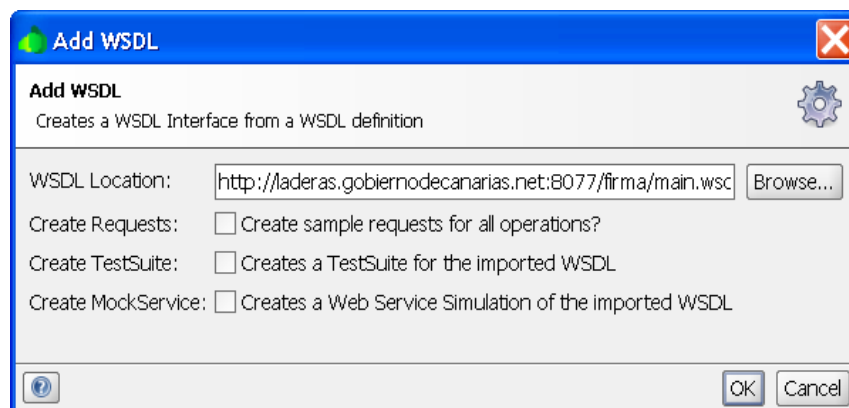
### 3.1.1 Creación de las interfaces

Para añadir el *wsdl* de cada servicio de Platino debemos seguir los siguientes pasos:

1. Pulsar botón derecho del ratón sobre el proyecto y seleccionar “Add WSDL / Ctrl-U”.



2. En la ventana que se muestra a continuación se debe introducir la localización del *wsdl* del servicio a incluir, que puede estar en un archivo o mediante *url*:





En este ejemplo introducimos la *url* del *wSDL* del Servicio de Firma y Sellado de Tiempo: <http://laderas.gobiernodecanarias.net:8077/firma/main.wsdl>. El resultado se muestra en la ventana del proyecto mostrando todos los métodos disponibles en la interfaz:



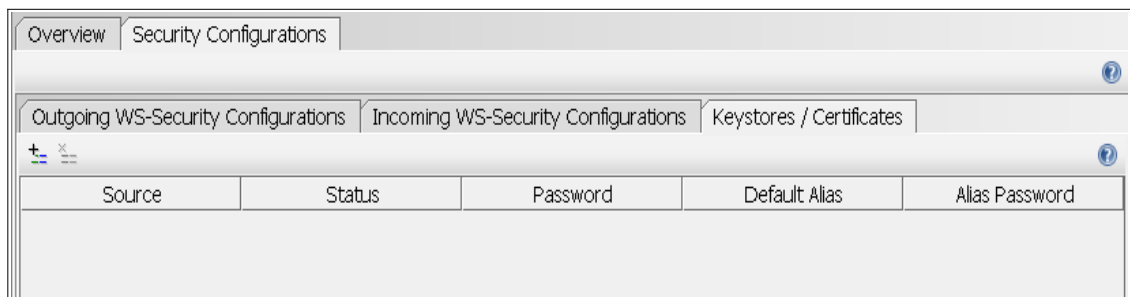
Para poder realizar esta operación es necesario establecer una conexión a la red de Gobierno mediante la *vpn*.


En el documento “**Acceso a los servicios en Pre-explotación**”, disponible en la web de Platino (<http://www.gobiernodecanarias.org/platino/formacion.html>) se describen los *wSDL* de todos los servicios que ofrece Platino. Se podrán incluir los *wSDL* de todos los servicios repitiendo este proceso para cada uno de ellos.

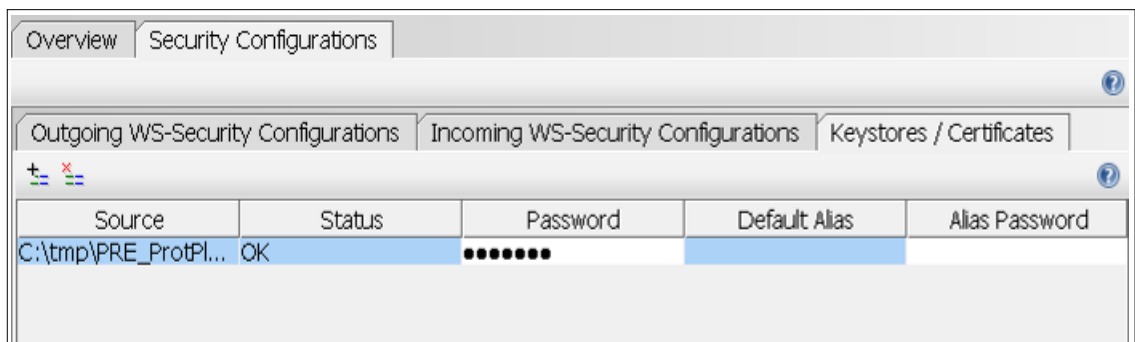
**Nota:** En caso de obtener las *url* de dicho documento, mediante la técnica de *copiar-pegar*, es conveniente revisar que no se introduzcan espacios en blanco al pegar el texto.


### 3.2 Configuración del proyecto

1. Acceder a los certificados del proyecto: Para ello hacemos *double Click* en el nombre del proyecto (*PLATINO-PRE*) y seleccionamos la pestaña *Security Configurations* y a continuación *keystores/Certificates*



2. Añadir el certificado: Al pulsar  se abre una ventana de diálogo que permite seleccionar el certificado de acceso a Platino. Una vez seleccionado pedirá la clave para poder acceder al mismo. El resultado se muestra de la siguiente manera:



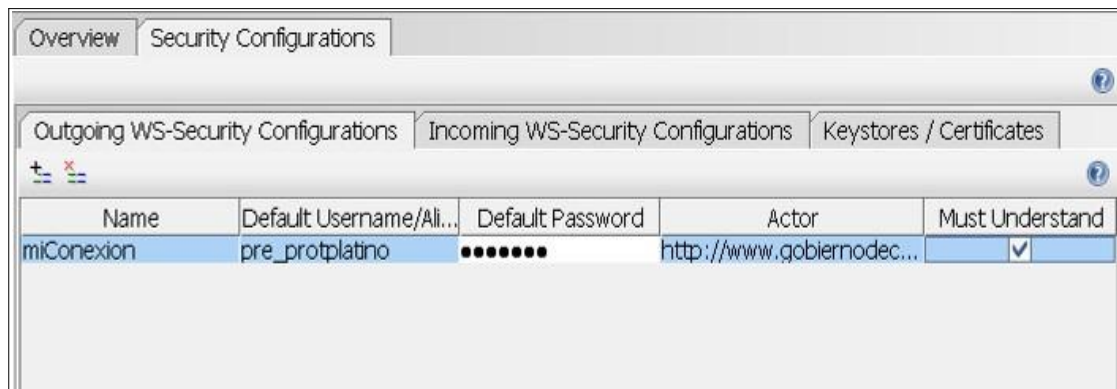
3. Añadir configuración: La pestaña “*Outgoing WS-Security Configurations*” permite establecer la configuración para los mensajes enviados al invocar un servicio. Para ello definimos una nueva configuración pulsando el botón .


Se le asigna un nombre a la configuración y se cumplimentan los campos de la siguiente manera:

<b>Name</b>	<i>Nombre asignado al crearlo. En este ejemplo "miConexion".</i>
<b>Default Username/Alias*</b>	Alias del certificado (ej: pre_protplatino) – Esta información se obtiene del certificado.
<b>Default Password</b>	Contraseña del certificado
<b>Actor</b>	http://www.gobiernodecanarias.org/Platino/Authentication/1.0
<b>Must Understand</b>	VERDADERO

\* Si no se conoce el alias del certificado, el apartado "ANEXO I. OBTENER EL ALIAS DEL CERTIFICADO" explica como obtenerlo.

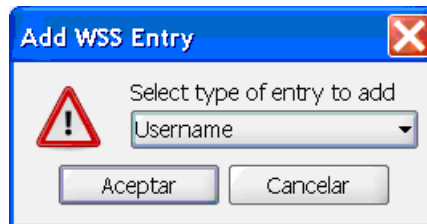
El resultado se muestra de la siguiente manera:



4. **Añadir cabeceras:** Seleccionamos la nueva configuración y en la parte inferior de la pantalla añadimos nuevas *WSS Entry* mediante el botón . En este caso vamos a añadir una entrada "Username" y otra "Signature".

**IMPORTANTE:** Platino es sensible al orden en el que se colocan las cabeceras. Por tanto, esta configuración se debe realizar en el orden correcto, es decir, primero se añade la cabecera "Username" y a continuación la cabecera "Signature". **Si se altera el orden no funcionarán las peticiones.**

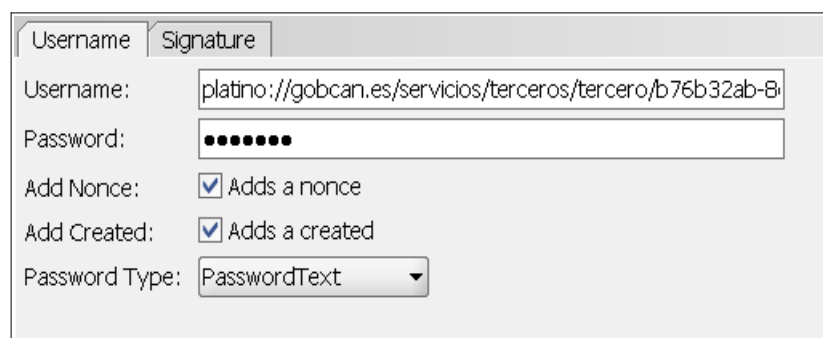
Configuración de “Username”: Permite identificar al responsable de la petición.



A continuación se muestran los valores de los campos:

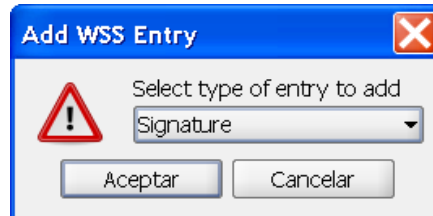
<b>Username</b>	Identifica al peticionario. Los valores deben ser: <ul style="list-style-type: none"> <li>- El tercero que utiliza el BackOffice</li> <li>- La URI del servicio (para las consultas entre servicios)</li> <li>- La URI del BackOffice</li> </ul>
<b>Password</b>	Este valor es <b>ignorado</b> , por lo que no es necesario indicarlo
<b>Add Nonce</b>	Verdadero
<b>Add Created</b>	Verdadero
<b>Password Type</b>	<i>PasswordText</i>

El resultado se muestra de la siguiente manera:





Configuración de "Signature": Permite la firma de la petición soap.



A continuación se muestran los valores de los campos:

<b>Keystore</b>	Menú de selección con el nombre del certificado configurado anteriormente
<b>Alias</b>	Menú de selección con el alias del certificado
<b>Password</b>	Se debe introducir el <i>password</i> del certificado
<b>Key Identifier Type</b>	<i>BinarySecurityToken</i>
<b>Signature Algorithm</b>	<i>default</i>
<b>Signature Canonicalization</b>	<i>Default</i>
<b>Digest Algorithm (*)</b>	http://www.w3.org/2000/09/xmlsig#sha1
<b>Use single certificate</b>	VERDADERO

**(\*) Sólo es necesario su introducción en versiones de SOAP 4.x o superiores.**

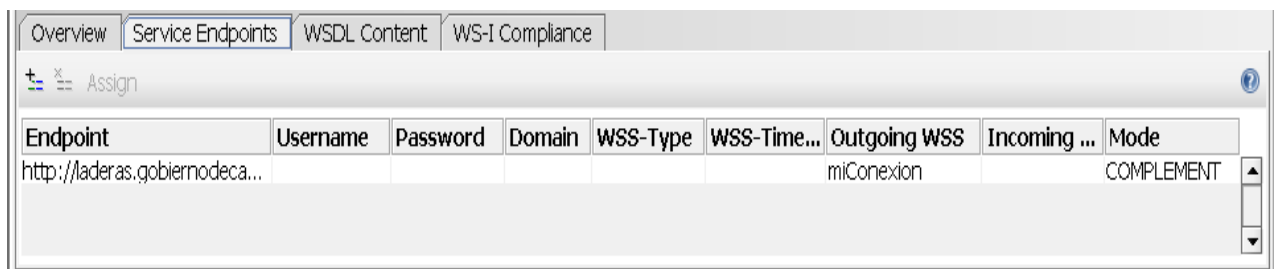
El resultado se muestra de la siguiente manera:

ID	Name	Namespace	Encode

### 3.3 Configuración de la interfaz

Una vez establecida la configuración de seguridad para el proyecto, se debe aplicar a las diferentes interfaces. Para ello se deben realizar los siguientes pasos:

1. Hacemos *doble Click* en el nombre de la interfaz (Ej: *FirmaServiceBinding*) y seleccionamos la pestaña *Service Endpoints*.
2. En la columna *Outgoing WSS* seleccionamos la configuración establecida en el paso anterior (Ej: *miConexion*)



Aunque con esta configuración es suficiente, es conveniente asegurarse que la nueva configuración se aplica a las peticiones realizadas al servicio. Para ello se selecciona el *Endpoint* y tras pulsar el botón *Assign* se muestra una ventana donde se debe seleccionar “ - *All Request* - ”.

Tras aceptar, se aplicará la nueva configuración a todas las llamadas al servicio.

### 3.4 Configuración de soapUI

Dentro de las opciones de configuración de soapUI (*Ctrl-Alt-P*) se deben comprobar los siguientes valores:

#### HTTP Settings

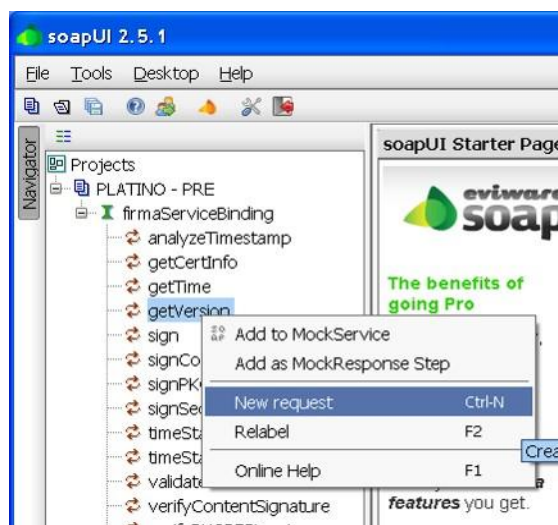
<b>HTTP Version</b>	1.0 o superior
---------------------	----------------



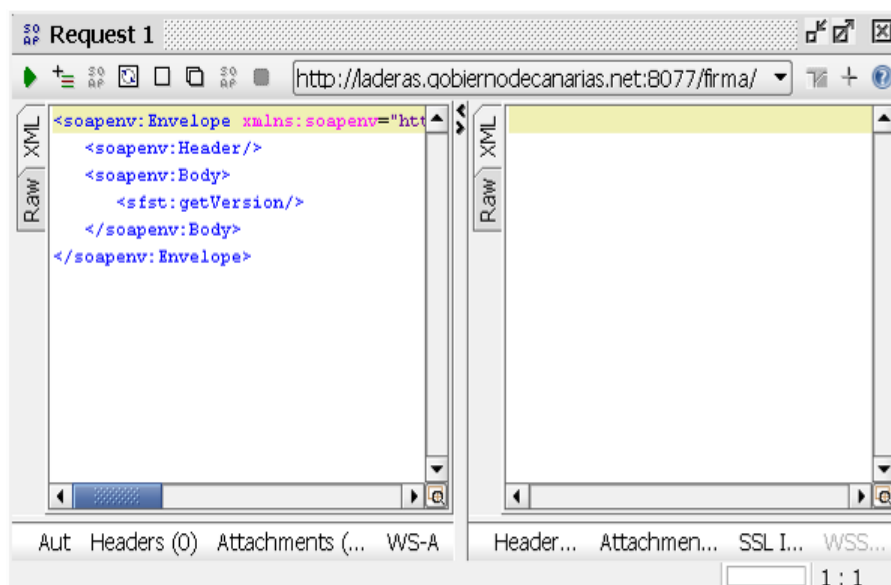
### 3.5 Prueba de funcionamiento

Para verificar que el funcionamiento es correcto debemos realizar una petición al servicio. Para ello realizaremos los siguientes pasos:

1. Pulsar botón derecho del ratón sobre el método para el que vamos a realizar la petición (ej: *getVersion*) y seleccionar “New Request / *Ctrl-N*”:

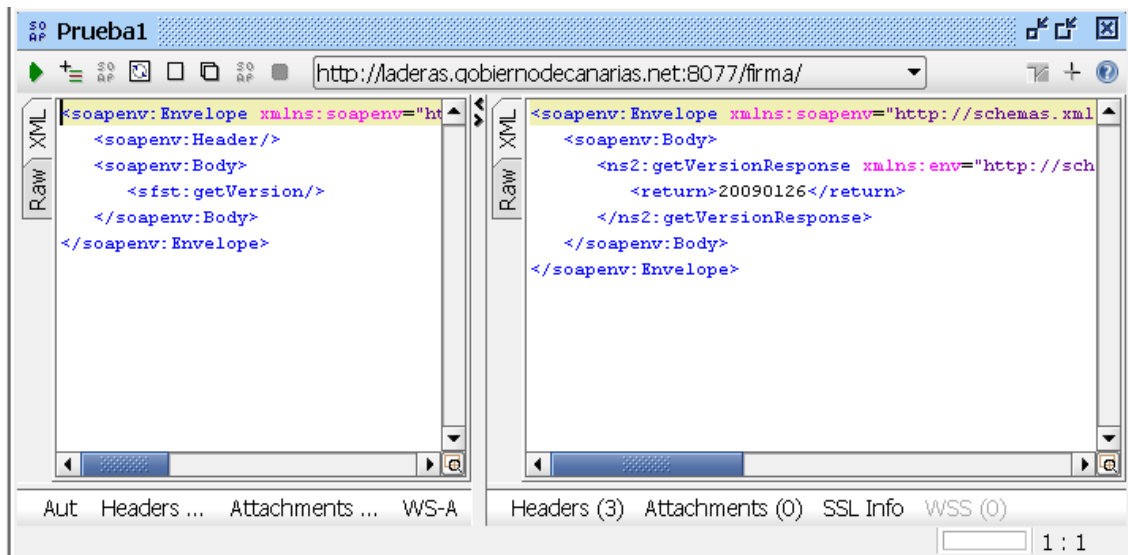


2. Se mostrará una ventana donde se deben introducir los parámetros para la petición. En el caso del método *getVersion()* no es necesario introducir parámetros, por lo que se puede ejecutar la petición pulsando el botón ▶.





3. Si la configuración se ha realizado correctamente se obtendrá un resultado como el que se muestra en la siguiente imagen:





**Gobierno  
de Canarias**

Consejería de Presidencia,  
Justicia y Seguridad  
Dirección General de  
Telecomunicaciones  
y Nuevas Tecnologías



**Platino**  
Plataforma de Interoperabilidad del  
Gobierno de Canarias

Consumo de los servicios de Platino mediante soapUI

Página 15 de 15

## ANEXO I. OBTENER EL ALIAS DEL CERTIFICADO

Para consultar el alias de un certificado se puede utilizar la herramienta keytool de Java, disponible tanto con el JRE como con el JDK. El comando se ejecuta de la siguiente manera:

```
keytool -list -v -storetype PKCS12 -keystore <certificado>
```

<certificado>: Representa el nombre del fichero que contiene el certificado.

Tras ejecutar el comando pedirá la **contraseña** para acceder al certificado y mostrará los siguientes datos, entre los que se encuentra el alias del certificado:

**Tipo de almacén de claves: PKCS12**

Proveedor de almacén de claves: SunJSSE

Su almacén de claves contiene entrada 1

**Nombre de alias: pre\_protplatino**

Fecha de creación: 18-may-2009

Tipo de entrada: keyEntry

Longitud de la cadena de certificado: 3

Certificado[1]:

Propietario: C=ES, O=Gobierno de Canarias, OU=PLATINO - DGTNT,  
CN=PRE\_ProtPlatino

Emisor: C=ES, O=Gobierno de Canarias CA, CN=CiberCentro

Número de serie: 72d224e744ac4c1a