
**DOCUMENTACIÓN TÉCNICA
DIVISIÓN INFORMÁTICA**

**Desarrollo de Sistemas
Arquitectos en Aplicaciones**



Consumo de Web Services de DGI

CÓDIGO: T-5.020.00.001.001

	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

Índice

1. Objetivo.....	4
2. Alcance.....	4
3. Responsables.....	4
4. Descripción.....	4
4.1. Requisitos.....	4
4.2. Autenticación	5
4.3. Consumo mediante SOAPUI 5.0.....	5
5. Registros.....	5
6. Excepciones.....	5
7. Referencias.....	5
8. Anexos.....	6
8.1. Anexo 1 - Ejemplo de consumo:.....	6
8.2. Anexo 2 - Consumo mediante SOAPUI 5.0 :.....	6

	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

1. Objetivo

El objetivo de este documento es disponer de un estándar para el consumo de los servicios Web expuestos por DGI en Internet.

2. Alcance

Se aplica a todas las autenticaciones que se realizan con el fin de consumir los servicios Web que ofrece DGI. No alcanza a la autorización que depende de cada servicio.

3. Responsables

Son responsables de su cumplimiento los desarrolladores, arquitectos de sistemas, analistas de negocio y jefes de proyecto de la División Informática

4. Descripción

Los Web services expuestos fueron desarrollados cumpliendo los siguientes estándares:

- SOAP 1.1
- WS Security 1.1
- X509 Token Profile v 1.0

Están expuestos mediante un canal de cifrado utilizando HTTPS (TLS 1.2) y un certificado emitido por una autoridad certificadora internacional para DGI, como certificado de sitio.

Los clientes deben validar la autenticidad del sitio de DGI mediante la validez de su certificado, para lo que deben almacenar en la(s) máquinas desde la(s) cual(es) se consume el web service el certificado de la autoridad certificadora internacional.

Mediante una adecuada validación de la cadena de confianza y el estado de la CRLs (Certificates Revocation Lists), se podrá verificar la autenticidad del sitio de DGI, donde se encuentran los servicios web.

Este mecanismo es automático cuando se utiliza un navegador como Mozilla Firefox para acceder al sitio web. A la hora de implementar un cliente para el consumo de un web service, dependerá de la tecnología a utilizar (Java, .NET, etc.) y si el cliente realiza la validación o no.

4.1. Requisitos

Los organismos interesados en el consumo de los web services o clientes **deben contar con un certificado de persona jurídica emitido por PKI Uruguay**, asociado a un par de claves (pública y privada), generadas utilizando RSA como algoritmo de clave asimétrico.

Deben contar con la debida seguridad para el almacenamiento y gestión de las claves.

Actualmente los organismos que emiten certificados PKI Uruguay son El Correo Uruguayo y Abitab.

	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

4.2. Autenticación

El cliente debe autenticarse y la solicitud de consumo de los web services debe cumplir lo siguiente:

1. Firmada utilizando la clave privada del organismo mediante el uso de WS-Security 1.1, con Binary Security Tokens (ver sección 6.3 del estándar) y utilizando X509 Token Profile.

2. La firma debe ser generada utilizando RSA (2048 bits) como algoritmo asimétrico, y SHA-2 como algoritmo de digest. Son válidas cualquiera de las variantes dentro de esta restricción, incluyendo el tamaño del digest (256, 385 o 512 bits). Por una lista de algoritmos existentes referirse al RFC 6931. Es posible utilizar cualquiera de las variantes en cuanto a algoritmos de canonicalización.

3. Incluir el certificado X509v3 del organismo

Ver Anexo 1

4.3. Consumo mediante SOAPUI 5.0

Previo al consumo, el cliente debe contar con su par de claves (pública y privada) almacenadas en un keystore apropiado.

El keystore puede ser generado de varias formas. La herramienta ampliamente utilizada para eso es OpenSSL <https://www.openssl.org/>. También existen herramientas gráficas como por ejemplo Portecle <http://portecle.sourceforge.net/>.

SOAPUI es una herramienta que permite trabajar con web services y se puede descargar una versión gratuita de su sitio oficial: <https://www.soapui.org/>

Ver Anexo 2

5. Registros

No aplica

6. Excepciones

No aplica

7. Referencias

- <https://www.w3.org/TR/2000/NOTE-SOAP-20000508/>
- <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>
- <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf>
- <https://www.soapui.org/>
- <https://tools.ietf.org/html/rfc6931>

	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

8. Anexos

8.1. Anexo 1 - Ejemplo de consumo:

```
<soapenv:Envelope xmlns:cva="CVA_FE" xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">

  <soapenv:Header><wsse:Security xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd" xmlns:wsu="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd"><ds:Signature Id="SIG-61257991E53D68CB9A152147347136230"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:SignedInfo><ds:CanonicalizationMethod
  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces PrefixList="cva soapenv"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" /></ds:CanonicalizationMethod><ds:SignatureMethod
  Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" /><ds:Reference URI="#id-
  61257991E53D68CB9A152147347136129"><ds:Transforms><ds:Transform
  Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"><ec:InclusiveNamespaces PrefixList="cva"
  xmlns:ec="http://www.w3.org/2001/10/xml-exc-c14n#" /></ds:Transform></ds:Transforms><ds:DigestMethod
  Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" /><ds:DigestValue>GQn4RcOweJDURE7QMvU0+E2j+II=</ds:
  DigestValue></ds:Reference></ds:SignedInfo><ds:SignatureValue>RliD/BGF9lr1r1SDB3aRrDQKeTgzeBGU+uNwvNy
  DJwr0noDFs57Gdk+yLc6T7o73HrDKPo6F1W7lnh
  X3DggvWKfuR6kiPFF1NeD+dJkRX7MM/kahOr6byI0H1xxHRPmDMO75bXGyytmIb6G54a9ae/+FFa
  Khypt02RDpj+wtIyGHXjf+0UXaWCRk9CApiQQgZ79CZ54pBb9oKOLhA4I1/cNaVhDzqcWryTbdj0
  yuoF9M+oTNTJom3N4FnT0LHzWtLCO6WwbfBN3REG62UUScG9LbDdjIJPXgaJ0Eb0bix+VIYrVCRc
  emd293yx7gXyaiFK8thFRiyHfhJAe/eQr//Vsg==</ds:SignatureValue><ds:KeyInfo Id="KI-
  61257991E53D68CB9A152147347136127"><wsse:SecurityTokenReference wsu:Id="STR-
  61257991E53D68CB9A152147347136128"><wsse:KeyIdentifier EncodingType="http://docs.oasis-
  open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0#Base64Binary"
  ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-
  1.0#X509v3">MIIDDjCCafagAwIBAgIEWqQWjTANBgkqhkiG9w0BAQsFADBJMQswCQYDVQQGEwJVWTEEMMAoGA1UECgwDREdJMOWw
  CgYDVQQQLDANSVQxHjAcBgNVBAMMFXYWVjYS5ydXQuZGdpLmdlYi5leTAeFw0xODAzMTUxNTUxNDFAFw0xODAzMTUxNTUxNDFA
  MEKxCzAJBgNVBAYTA1VZMQswCgYDVQQKIDANER0kxODAKBgNVBAsMA1JVVDDeMBwGA1UEAwVcHj1ZWJhLnJldC5kZ2kuZ3ViLnV5
  MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAu/EJtuJ5lKiYie3uTex4uuubSqIra6Y/oVrhtHO5smHT3lu6VhPctQ
  8kVXi/VZdOemQleq38FFSI2pDmIdgathO6cakM4u+yo7UeT0to8W8Eq8hQtd7RzmZLVsoL0rjtQSHjVKjax+aq5L588mfmycDkKR
  lzCfBaDhncCvAiWs/
  +apMMZ1cVPgHkVXucum7LVUPFrPbZdjR5x5wOJOEUelyvz5i9I8FITipMytO/WiCfhTjbu6gpxQph6u+gzTxq/o8GfceXArxPr4b
  TxL6tiWDBxSLKwCp6qB2xf+jE8P6m9x1lhWxrlm26ZgTbNUZUFSrUy+qkyBXaytxh9RdwIDAQABMA0GCSqGSIb3DQEBCwUAA4IBA
  QAe/NL1+y1/lz9pS0x88fx1q6kvpw0YyJEHwALJX0QcN/k2FEcHrTNm+SjJM2ilN1Lnp3Me4FfOV9g6pcpAlw7GNfFp7n/DdTe7
  wWCzIVmjCjloO/mvu93UOwOIF4LhTDCmdur5b61JAPdtEfO+UY4pKXBNLaPxlgBKmiqWHA8gaj+yV5qy9WiGSudfPHO03YMD8Aee
  YDB24sNiNpATj5VTbvzZUSH0LymSFHzYvJWj+ypbJGVtTqtWmTChuYdzjPCz5PiXtDxGAW14mdeO5cE7DRYzifl/q4WaSbgwwQ/co
  YRj/Q7OAb+o0QCUTYJEiCDKdVlw84Qo+RaM8G5rBa3R</wsse:KeyIdentifier></wsse:SecurityTokenReference></ds:K
  eyInfo></ds:Signature></wsse:Security></soapenv:Header>

  <soapenv:Body wsu:Id="id-61257991E53D68CB9A152147347136129" xmlns:wsu="http://docs.oasis-
  open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd">

    <cva:CVA_WS.Execute>

      <cva:Ruc>219000090011</cva:Ruc>

    </cva:CVA_WS.Execute>

  </soapenv:Body>
</soapenv:Envelope>
```

En rosado: firma de la solicitud.

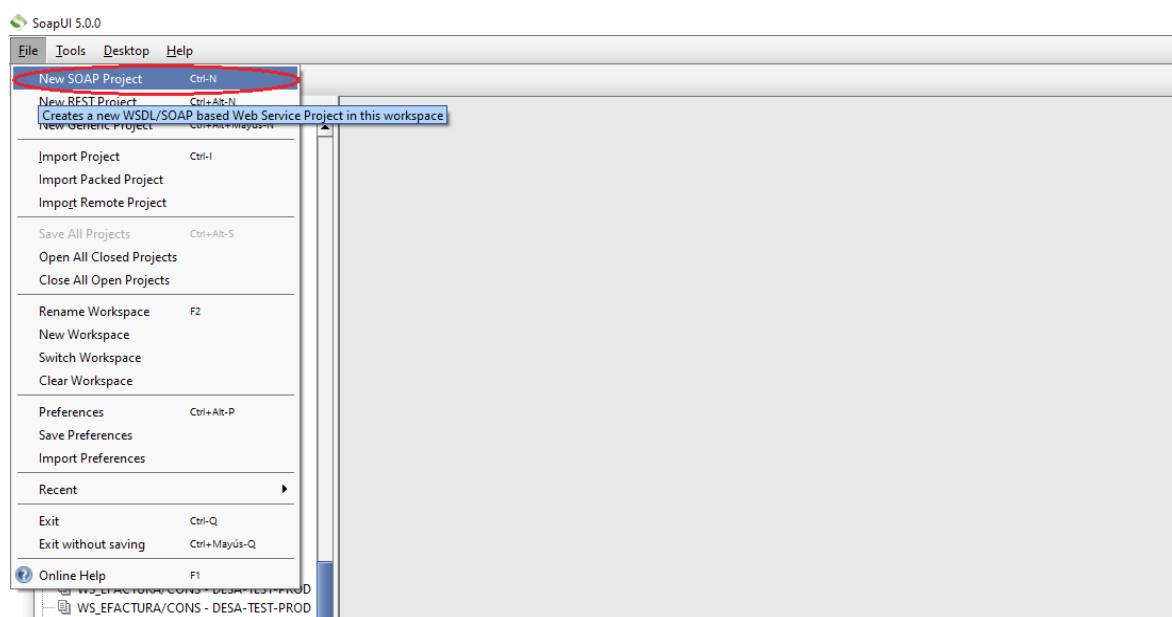
En amarillo: certificado X509v3 del organismo

	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

8.2. Anexo 2 - Consumo mediante SOAPUI 5.0 :

SOAPUI es una herramienta para el consumo de web services. Existe una versión gratuita que se puede bajar del sitio <https://www.soapui.org/>

- 1) Luego de instalar la herramienta, ejecutarla y crear un nuevo proyecto:



- 2) Indicar la URL del WSDL asociado al web service SOAP que se desea consumir.

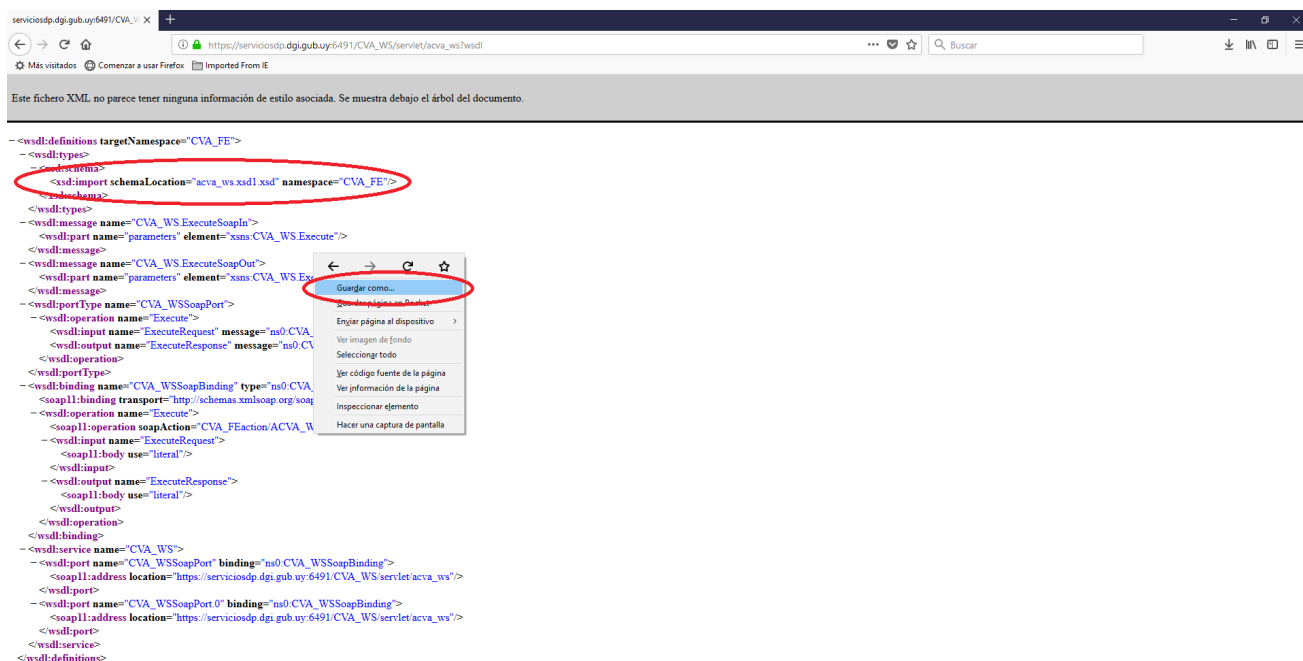
A modo de ejemplo, consumiremos el servicio para obtener el estado del Certificado de Vigencia Anual de una empresa.

La URL del servicio en producción es:

https://serviciosdp.dgi.gub.uy:6491/CVA_WS/servlet/acva_ws?wsdl

	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

- 3) Ingresando dicha URL en un navegador web, se puede ver la descripción del servicio WSDL. El WSDL correspondiente puede hacer referencia a otros XSDs que lo complementan. Hacer click con el botón derecho del ratón, y guardar el WSDL localmente en alguna ruta conocida.



	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

- 4) Ingresar a la URL de cada uno de los xsd referenciados. Para ello hay que agregar el nombre del xsd al final de la URL sin la última parte.

En este caso, la URL sin la última parte:

https://serviciosdp.dgi.gub.uy:6491/CVA_WS/servlet/

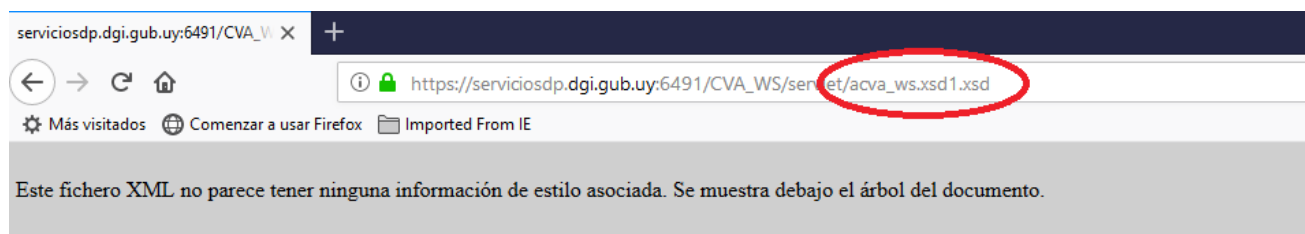
El nombre del xsd es: acva_ws.xsd1.xsd

Lo que queda finalmente en

https://serviciosdp.dgi.gub.uy:6491/CVA_WS/servlet/acva_ws.xsd1.xsd

Hacer click con el botón derecho del ratón, y guardar cada uno de los xsd referenciados localmente en la misma ruta que la utilizada en el punto 5 (donde se guardó el wsdl).

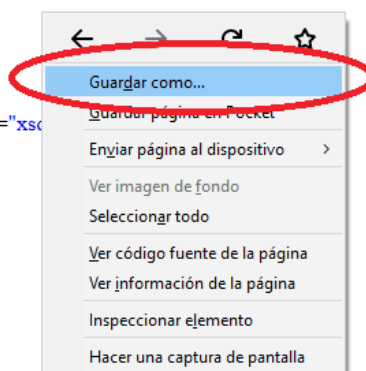
Asegurarse que la extensión del archivo sea .xsd



```

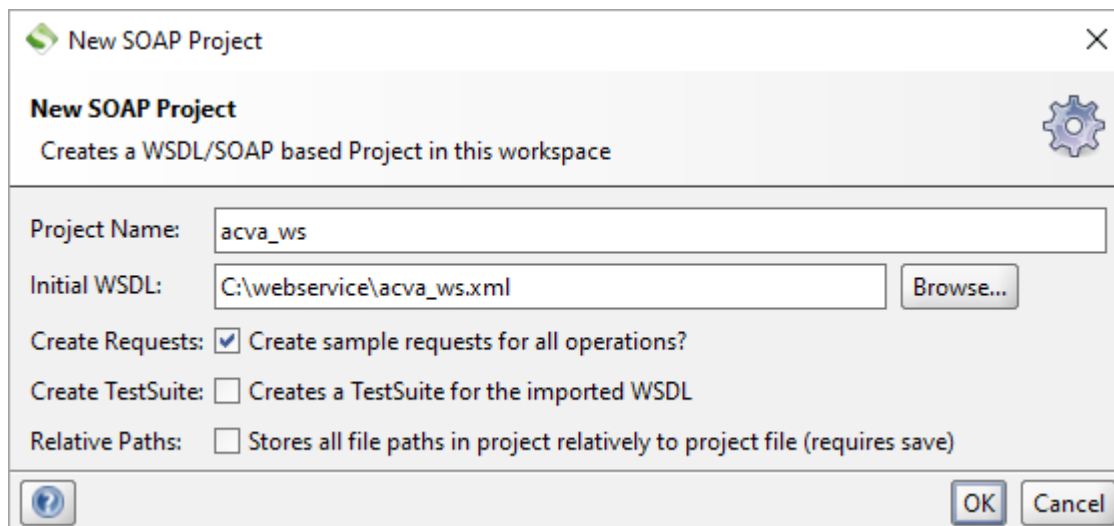
- <schema targetNamespace="CVA_FE" elementFormDefault="qualified">
  <import namespace="WS_CVA"/>
  <import namespace="CVA_WS_BE"/>
  - <element name="CVA_WS.Execute">
    - <complexType>
      - <sequence>
        <element minOccurs="1" maxOccurs="1" name="Ruc" type="xsd:string"/>
      </sequence>
    </complexType>
  </element>
  - <element name="CVA_WS.ExecuteResponse">
    - <complexType>
      - <sequence>
        <element minOccurs="1" maxOccurs="1" name="Retornotxt" type="xsd:string"/>
      </sequence>
    </complexType>
  </element>
</schema>

```



	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

- 5) Crear un nuevo Proyecto SOAP en SOAPUI, indicar el nombre del proyecto y el wsdl que se guardó anteriormente en el punto 3.



New SOAP Project

Creates a WSDL/SOAP based Project in this workspace

Project Name:

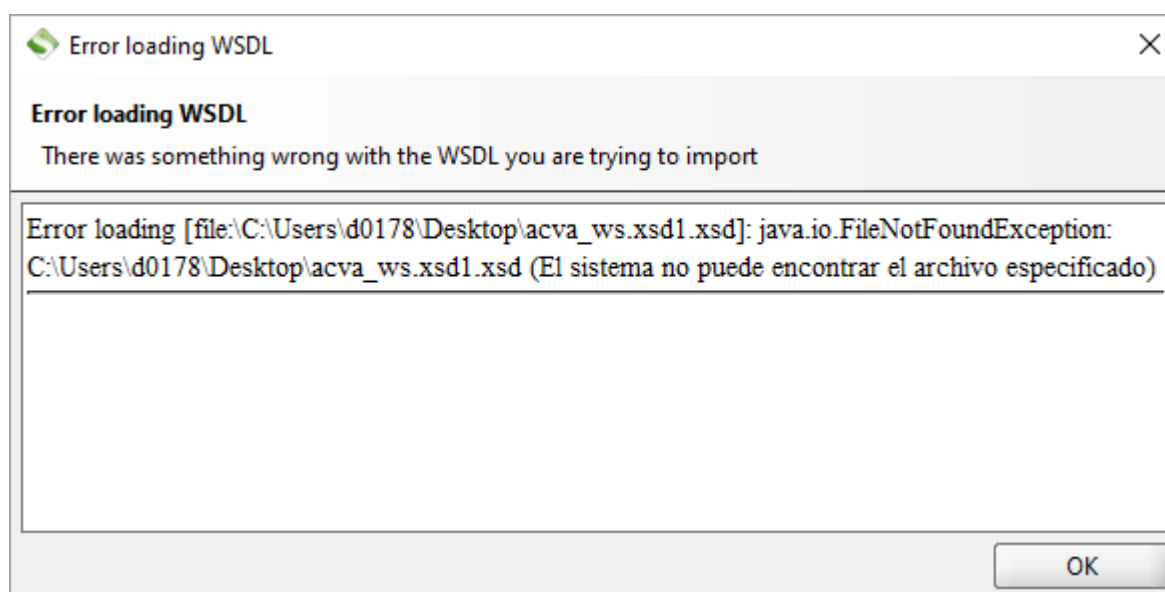
Initial WSDL:

Create Requests: ☒ Create sample requests for all operations?

Create TestSuite: ☐ Creates a TestSuite for the imported WSDL

Relative Paths: ☐ Stores all file paths in project relatively to project file (requires save)

Si al importar el proyecto, se genera el siguiente error, es porque los archivos xsd no se encuentran en la misma ruta (directorio) donde está el wsdl, o dichos archivos se guardaron con otra extensión (posiblemente .xml)



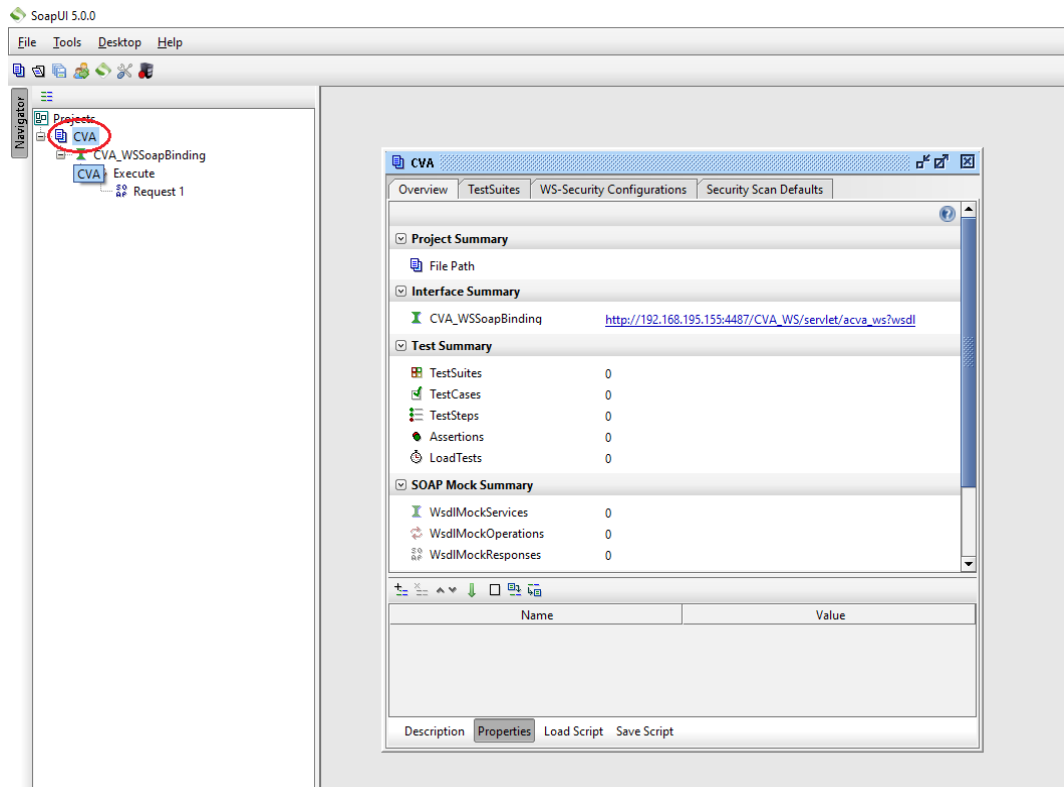
Error loading WSDL

There was something wrong with the WSDL you are trying to import

Error loading [file:C:\Users\d0178\Desktop\acva_ws.xsd1.xsd]: java.io.FileNotFoundException: C:\Users\d0178\Desktop\acva_ws.xsd1.xsd (El sistema no puede encontrar el archivo especificado)

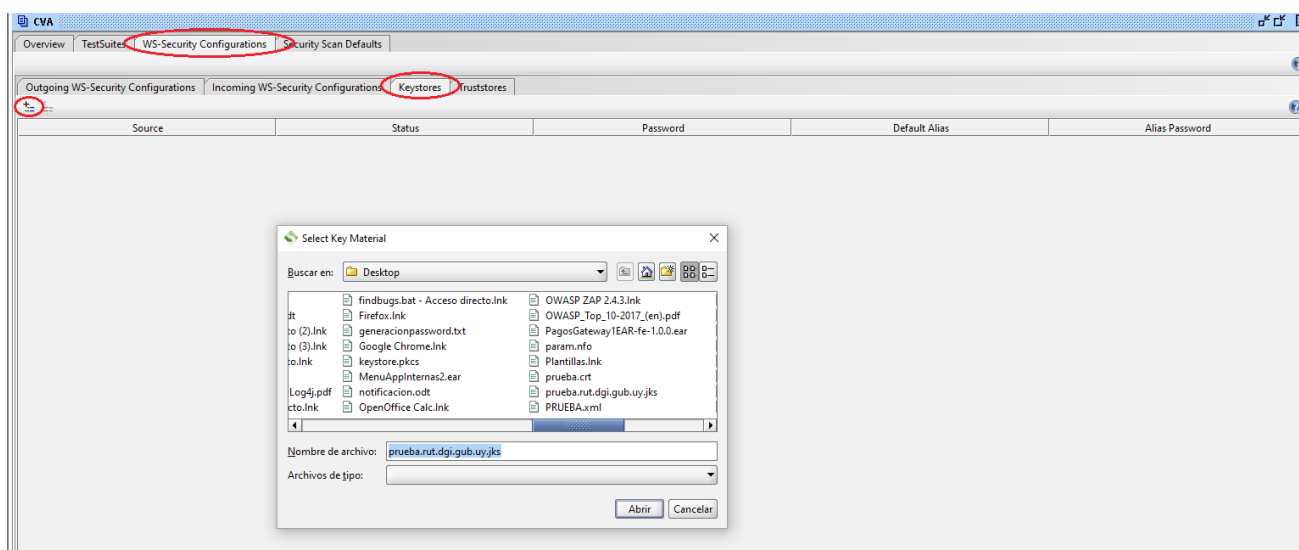
	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

6) Hacer doble click en el proyecto creado.



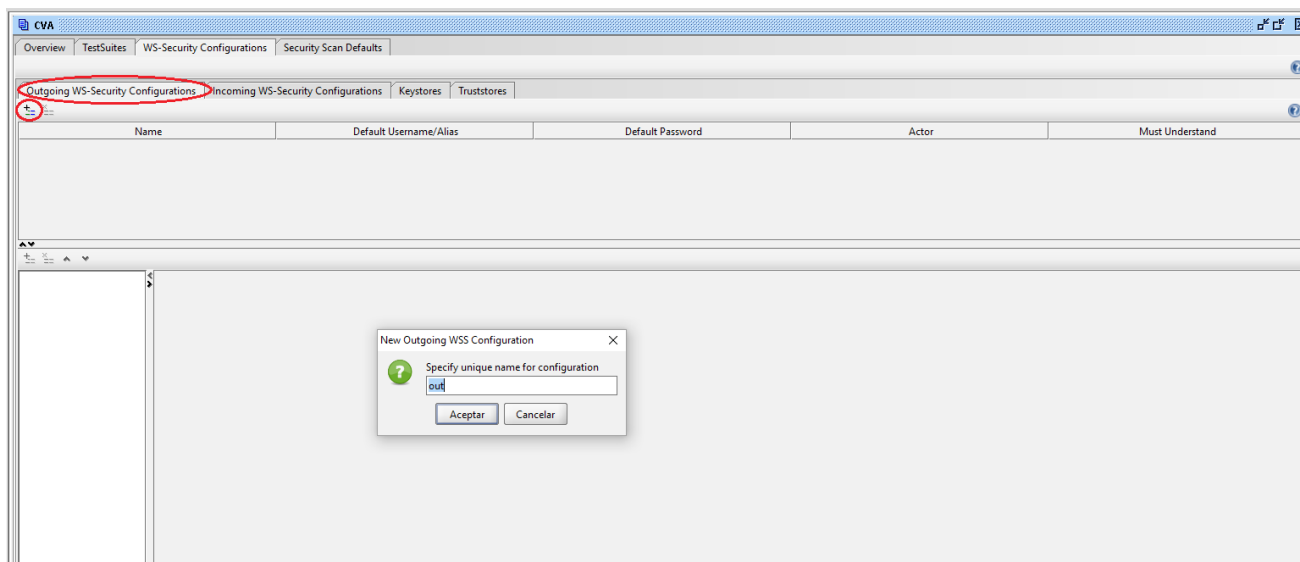
	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

- 7) Ir a la solapa “WS-Security Configurations”, luego a “Keystores” y finalmente seleccionar el botón “+” para agregar un nuevo almacén de claves (keystore). Deberá seleccionar el keystore donde se encuentra el par de claves (pública y privada) del organismo.

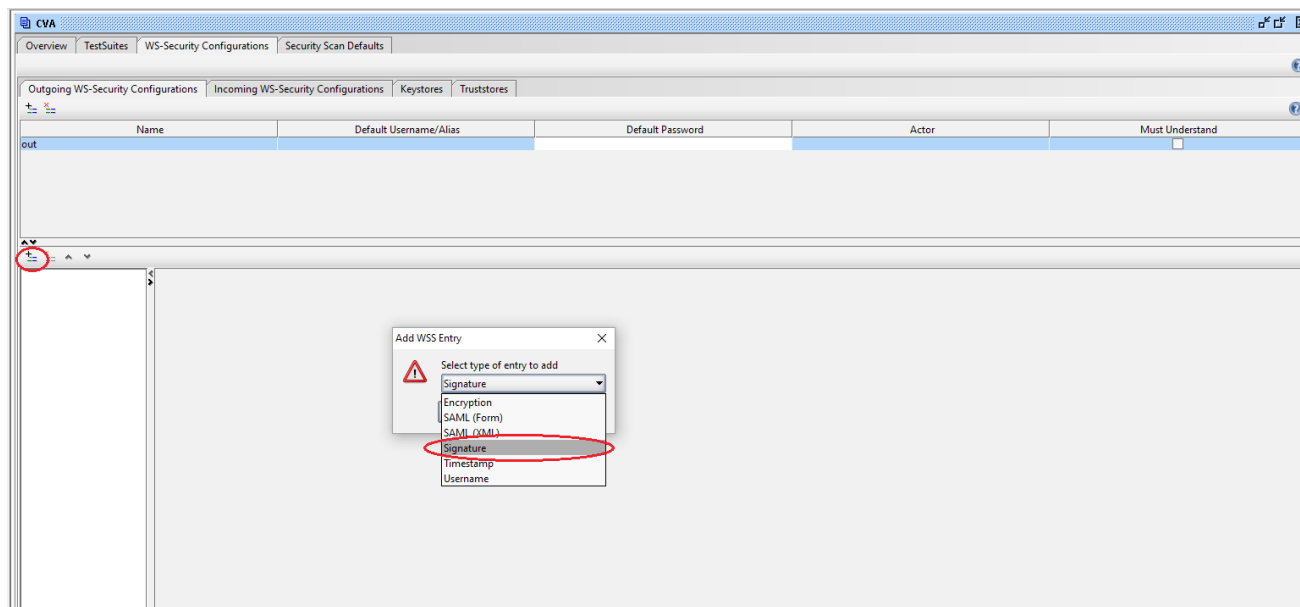


	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

- 8) Luego ir a la solapa “Outgoing WS-Security Configurations”. Crear una nueva entrada con el botón “+”.



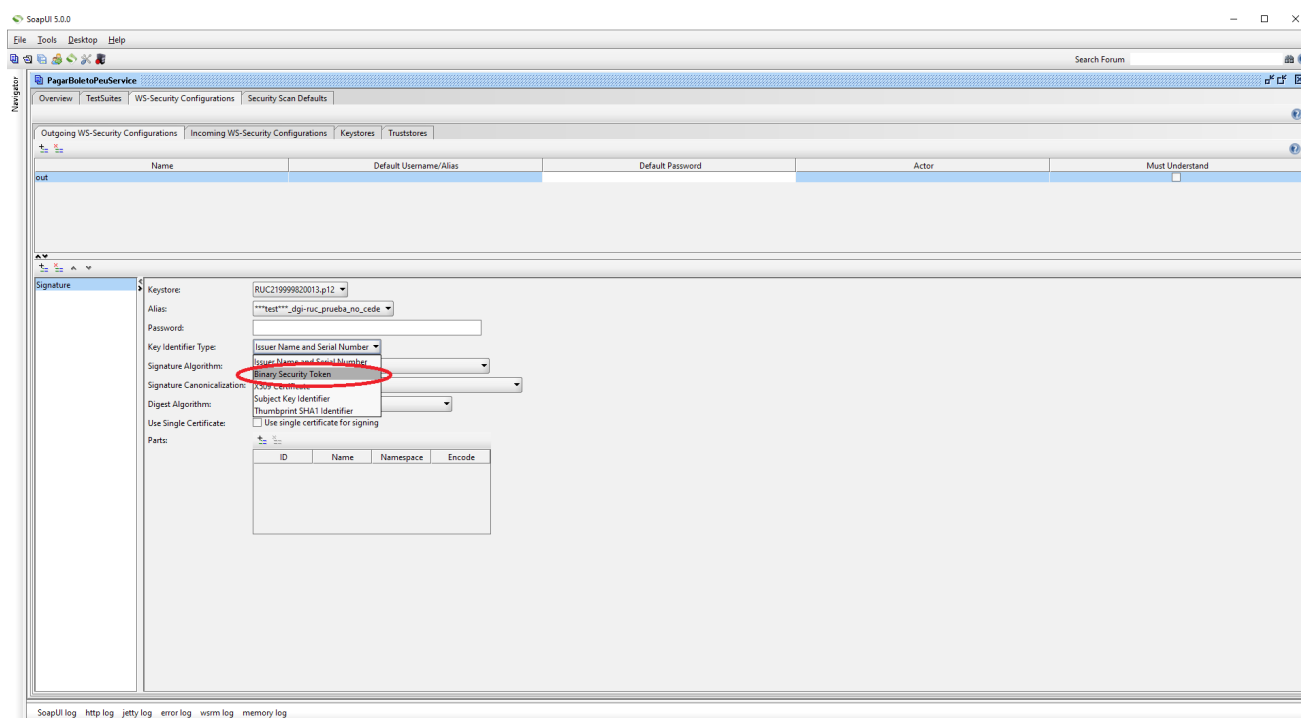
- 9) Seleccionar el objeto creado en el punto 5, luego hacer click sobre el botón “+” y seleccionar “Signature”.



	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

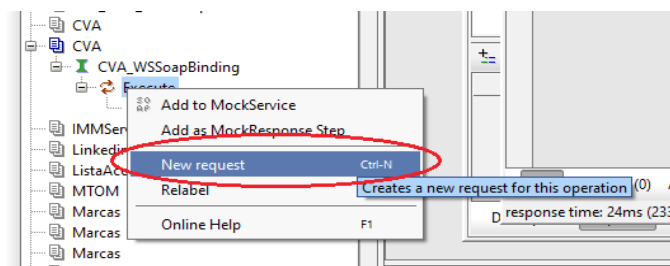
10) Indicar

1. el keystore configurado previamente,
2. el alias asociado al par de clave público y privado y
3. el password.
4. En Key Identifier type seleccionar “Binary Security Token”.
5. Indicar los algoritmos a utilizar. Recordar que en el punto 4.2 de este documento, se definió los algoritmos que se pueden utilizar. En este caso en particular podemos seleccionar:
 - Signature Algorithm: <http://www.w3.org/2001/04/xmldsig-more#rsa-sha256>
 - Signature Canonicalization: default
 - Digest Algorithm: <http://www.w3.org/2001/04/xmlenc#sha256>

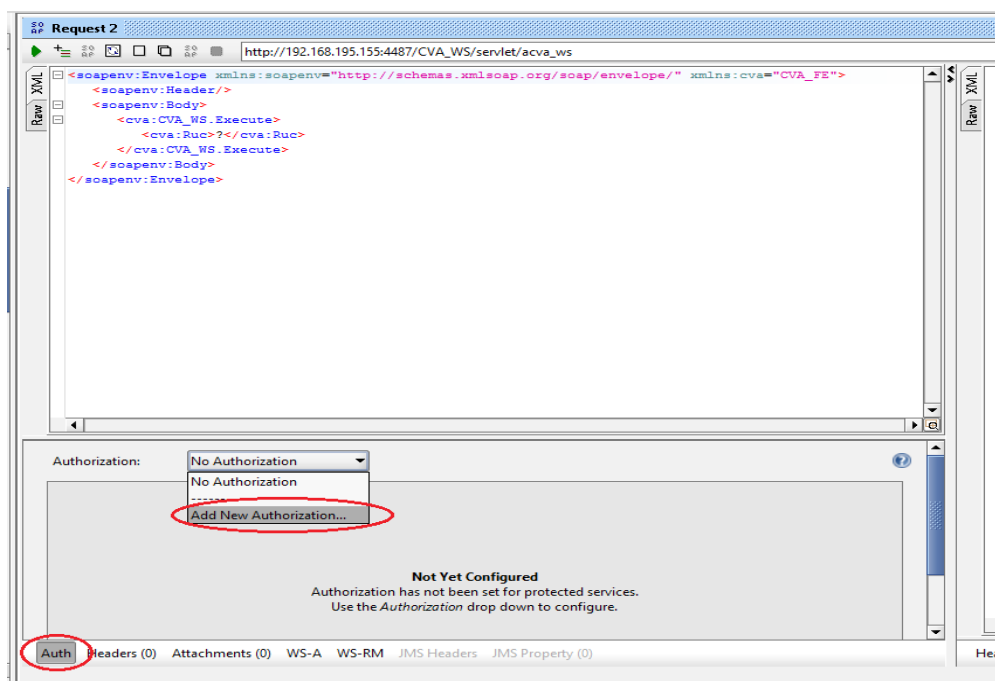


	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

- 11) Luego será necesario crear un nuevo request para el proyecto. Si no se crea un nuevo request, es posible que la nueva configuración no tenga efecto. Los cambios de aquí en adelante deben aplicarse a este nuevo request.

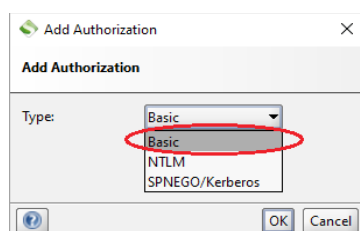


- 12) Hacer doble click para abrir el request, seleccionar la solapa “Auth”. Luego en “Authorization” seleccionar “Add New Authorization”.

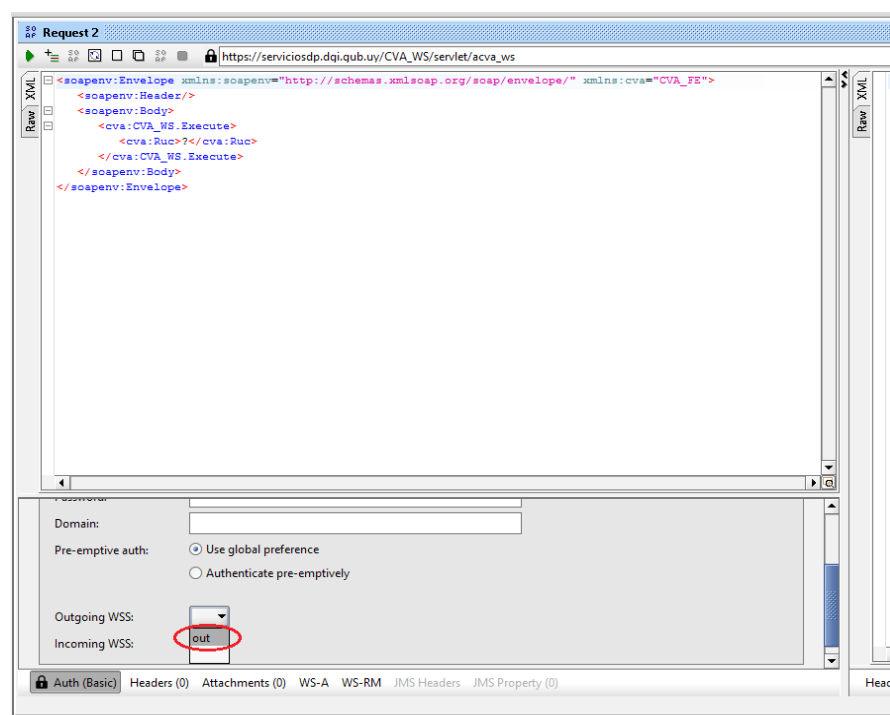


	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018

13) Seleccionar “Basic” como tipo de autorización:



14) En “Outgoing WSS” seleccionar la entrada definida en el paso 8

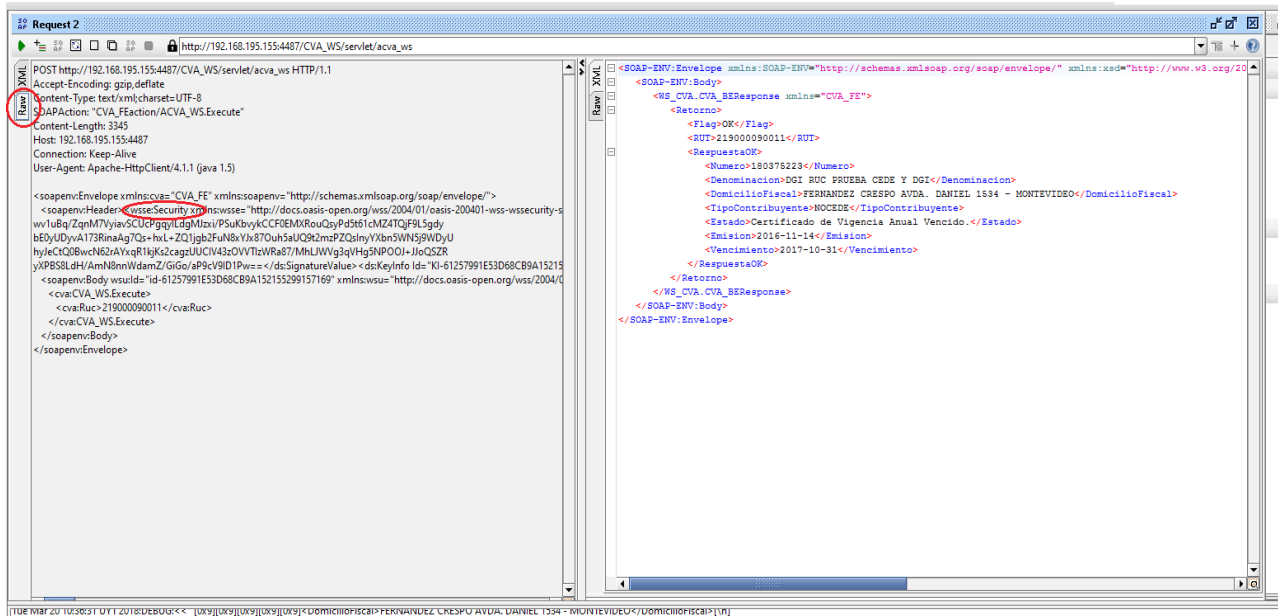


15) Luego de configurado el request

1. completar los datos necesarios (parámetros de entrada) para ejecutar el webservice (en este caso el RUT)
2. Hacer click en el botón verde de “Play”
3. verificar que se pueda consumir correctamente. El resultado debe ser como el de la siguiente imagen.

Pueden corroborar que el request quedó firmado correctamente yendo a la solapa “Raw” del request y verificando que aparece el elemento “WS-Security” como parte del cabezal de SOAP.

 DIRECCIÓN GENERAL IMPOSITIVA	Documentación Técnica DIVISION INFORMÁTICA – Desarrollo de Sistemas–Arquitectos en Aplicaciones	CÓDIGO:	T-5.020.00.001.001
		VERSIÓN:	01.02
	Consumo de Web Services de DGI	FECHA:	28/05/2018



16) En caso de error en la configuración de la firma, la respuesta será la siguiente “codigo: 99, No se ha(n) podido verificar la(s) firma(s)”. Esto puede deberse a un problema en la configuración. Asegurarse de que se cumplió con el paso 8.

