



Plataforma Autnómica de Interoperabilidad

PAI_CONTRATO_INTEGRACION_SAFE_AUTENTICACION_v1_v005

Contrato de Integración para Servicios Web de SAFE
Autenticación



DIRECCI3N GENERAL DE TECNOLOGÍAS
DE LA INFORMACI3N Y LAS COMUNICACIONES

Versi3n 005
Enero de 2021



Índice

1	Control del documento	3
1.1	Informaci3n general	3
1.2	Hist3rico de revisiones	3
1.3	Estado del documento	3
2	Introducci3n	4
2.1	Alcance	4
2.2	Objetivos	4
2.3	Audiencia	4
2.4	Glosario	4
2.5	Referencias	4
3	Descripci3n de la integraci3n	5
3.1	Descripci3n del servicio	5
3.2	Listado de m3todos	5
4	Detalle del servicio Autenticaci3n_v1_00	6
4.1	Obtener informaci3n de autenticaci3n	7
4.1.1	Par3metros Entrada	7
4.1.2	Par3metros Salida	7
4.2	Autenticaci3n con Usuario de LDAP	9
4.2.1	Par3metros Entrada	9
4.2.2	Par3metros Salida	9
4.3	Autenticaci3n con Usuario	10
4.3.1	Par3metros Entrada	10
4.3.2	Par3metros Salida	10
4.4	Autenticaci3n con Firma	11
4.4.1	Par3metros Entrada	11
4.4.2	Par3metros Salida	11
4.5	Mensajes de error y excepciones	12
4.6	Compromiso de servicio	13
4.7	Seguridad del Servicio Web	13
4.7.1	BUS Instrumental	13
5	ANEXOS	14
5.1	WSDL de Autenticaci3n	14

1 Control del documento

1.1 Información general

Título	Contrato de Integración para Servicio Web de SAFE
Creado por	DGTIC
Revisado por	
Lista de distribución	
Nombre del fichero	PAI_CONTRATO_INTEGRACION_SAFE_AUTENTICACION_v1_v005.doc

1.2 Histórico de revisiones

Versión	Fecha	Autor	Observaciones
0	28/07/2014	DGTIC	Versión inicial. Revisión de Contenido. Inclusión de Anexos. Adición de servicio via LDAP. Adición servicio multirepositorio y revisión. Revisión de Contenido. Inclusión de Anexos.
1	22/03/2016	DGTIC	Se ha modificado el nombre del documento, modificado la tabla 'errores devueltos por la plataforma', modificado el wsdl y cambiadas las referencias a las urls de producción y preproducción.
2	11/07/2016	DGTIC	Se adapta al nuevo formato y se añaden URL's del BUS de Innovación. Se separa de SAFE Autorización HDFI y de SAFE Firma
3	16/11/2016	DGTIC	Revisión del formato e inclusión del método interno autenticaConFirma
4	18/01/2017	DGTIC	Se añaden errores 403 y 904 en la tabla de soapfault
5	13/04/2021	DGTIC	Adaptación de la documentación original al formato de la DGTIC.

1.3 Estado del documento

Responsable aprobación	Fecha

2 Introducció

Este documento contiene un contrato de integraci3n asociado al consumo del Servicio Web de SAFE Autenticaci3n de la plataforma eSIRCA. El contrato de integraci3n detalla, los aspectos relacionados con el procedimiento de integraci3n, pudiendo exponer los mecanismos de consulta o consumo, las posibles respuestas o devoluci3n de informaci3n, los formatos a utilizar, etc.

2.1 Alcance

Este documento tiene un enfoque t3cnico y describe lo que hace el servicio y como consumir el mismo. Detalla que par3metros espera y que par3metros o excepciones de error devuelve.

2.2 Objetivos

El objetivo principal del contrato de integraci3n es permitir conocer la definici3n de la estructura de invocaci3n al servicio de SAFE Autenticaci3n. De este modo el usuario final podr3 realizar el consumo del servicios web correctamente.

2.3 Audiencia

Nombre y Apellidos	Rol

Tabla 1: Audiencia

2.4 Glosario

T3rmino	Definici3n
Intermediador	Sistema inform3tico que hace de intermediaci3n entre el consumo directo de un webservice, que es el que ofrece en 3ltima (a efectos del intermediador) instancia la funcionalidad, y el consumidor del servicio.

Tabla 2: Glosario

2.5 Referencias

Referencia	T3tulo

Tabla 3: Referencias

3 Descripci3n de la integraci3n

Nombre del Servicio	Autenticacion_v1_00
Tipo de Integraci3n	Servicio Web
Modo de funcionamiento	N/A
Intermediario	Plataforma Autònoma de Interoperabilitat de la GVA (PAI)
Proveedor del Servicio	DGTIC
Contacto	PAI

Tabla 4: Datos generales de integraci3n

3.1 Descripci3n del servicio

En este manual se incluye la descripci3n de los siguientes caracteristicas del componente:

- 1) Autenticaci3n

El cat3logo de servicios existentes se muestra en la siguiente tabla:

3.2 Listado de m3todos

Se listan los diferentes subservicios/m3todos que ofrece el servicio:

getInformacion: Este m3todo realiza la obtenci3n de los datos de autenticaci3n asociados a un token generado por un usuario autenticado.

autenticaUsuarioLDAPWS: Este m3todo realiza la autenticaci3n de un usuario del LDAP de GVA a trav3s de su identificador de login y de su password, retornando un token generado en servidor.

autenticaUsuarioWS: Este m3todo realiza la autenticaci3n de un usuario de HDFI a trav3s de su identificador de login de HDFI y de su password, retornando un token generado en servidor.

autenticaConFirmaWS: Este m3todo realiza la autenticaci3n de un usuario via certificado digital, este servicio es de uso interno de SAFE. Retorna un token generado en servidor.

4 Detalle del servicio Autenticacion_v1_00

A continuación se detallan los datos de acceso al servicio de Autenticacion_v1_00:

Datos de Acceso al Servicio de Autenticacion_v1_00 en el BUS Instrumental	
Endpoint Pre Producción	https://instrumental-pre.gva.es/pai_bus_ins/SAFE/Autenticacion_v1_00?wsdl
Endpoint Producción	https://instrumental.gva.es/pai_bus_ins/SAFE/Autenticacion_v1_00?wsdl
Tipo de Firma admitida	WS-Security
Respuesta Cifrada	NO

Tabla 5.- Datos de acceso al servicio en el BUS Instrumental

Datos de Acceso al Servicio de Autenticacion_v1_00 en el BUS Innovación	
Endpoint Pre Producción	https://innovacion-pre.gva.es/pai_bus_inno/SAFE/Autenticacion_v1_00?wsdl
Endpoint Producción	https://innovacion.gva.es/pai_bus_inno/SAFE/Autenticacion_v1_00?wsdl
Tipo de Firma admitida	N/A
Respuesta Cifrada	NO

Tabla 6.- Datos de acceso al servicio en el BUS Innovación

IMPORTANTE: Los servicios publicados en el bus de Innovación son para uso exclusivo de aplicaciones de la GVA desplegadas en la infraestructura de la DGTIC.

Todos los mensajes intercambiados deben firmarse y para ello es necesario disponer de un certificado digital que sea reconocido por la PAI (@firma). El tipo de transporte para las operaciones de este servicio es SOAP.

Este servicio contiene las operaciones:

- **getInformacion:** Ver **Error! Reference source not found.**

Obtener información de autenticación

- **autenticaUsuarioLDAPWS:** Ver **Error! Reference source not found.**

Autenticación con Usuario de LDAP

- **autenticaUsuarioWS:** Ver **Error! Reference source not found.**

Autenticación con Usuario

- **autenticaConFirmaWS:** Ver 4.4 *Autenticación con Firma*

4.1 Obtener informaci3n de autenticaci3n

Object[] getInformacion (String token);

Este servicio es el que permite realizar la recogida de informaci3n almacenada al realizar una autenticaci3n en el sistema.

4.1.1 Parámetros Entrada

Ubicaci3n	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripci3n
getInformacionWSR equest/token	token	String	Sí	Sí	Cadena generada aleatoriamente

4.1.2 Parámetros Salida

Ubicaci3n	Nombre	Tipo	Etq. Oblig.	Campo Oblig.	Descripci3n
getInformacionWSR esponse	getInformacion WSResponse	Object[]	Sí	Sí	<p>Retorna un array de datos que incluyen dependiendo del tipo de autenticaci3n:</p> <p>Si tipo es certificado=</p> <ol style="list-style-type: none"> Tipo de autenticaci3n (valor = CERTIFICADO) SERIALNUMBER SUBJECTDN ISSUERDN Nombre Apellido1 Apellido2 NIF CIF Razon Social OID del certificado Tipo de certificado Email <p>Si el tipo es HDFI (USO EXCLUSIVO GVA)=</p> <ol style="list-style-type: none"> Tipo de autenticaci3n (valor = USUARIOPWD) ID de HDFI (si fuera asi) Nombre

					4. Apellido1
					5. Apellido2
					6. NIF
					7. CIF
					8. Razon Social

Ejemplo de XML de entrada

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v2="http://dgm.gva.es/ayf/war/schemas/v2_00">
  <soapenv:Header/>
  <soapenv:Body>
    <v2:getInformacionWSRequest>
      <v2:token>Und0NHVWbmFrVGVCMXR1ZGFHcmp4Zz09</v2:token>
    </v2:getInformacionWSRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
  <v2:getInformacionWSResponse>
    <v2:serialNumber>?</v2:serialNumber>
    <v2:issuerDN>?</v2:issuerDN>
    <v2:subjectDN>?</v2:subjectDN>
    <v2:nombre>?</v2:nombre>
    <v2:apellido1>?</v2:apellido1>
    <v2:apellido2>?</v2:apellido2>
    <v2:nif>?</v2:nif>
    <v2:cif>?</v2:cif>
    <v2:razon_social>?</v2:razon_social>
    <v2:habilitado>?</v2:habilitado>
    <v2:representante>?</v2:representante>
    <v2:oid>?</v2:oid>
    <v2:tipo_aut>?</v2:tipo_aut>
    <v2:idHDFI>?</v2:idHDFI>
    <v2:email>?</v2:email>
    <v2:tipoCertificado>?</v2:tipoCertificado>
    <v2:codEntidad>?</v2:codEntidad>
  </v2:getInformacionWSResponse>
</soapenv:Body>
```

4.2 Autenticación con Usuario de LDAP

String autenticaUsuarioLDAPWS (final String usuarioLDAP, final String pwdLDAP);

Este servicio es el que permite realizar la autenticación a través de un usuario y pwd del LDAP de GVA.

4.2.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
autenticaUsuarioLDAPWSRequest/usuarioLDAP	usuarioLDAP	String	Sí	Sí	Identificador de login de LDAP de un usuario
autenticaUsuarioLDAPWSRequest/pwdLDAP	pwdLDAP	String	Sí	Sí	Password de LDAP asociado al usuario.

4.2.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiqu. Oblig.	Campo Oblig.	Descripción
autenticaUsuarioLDAPWSResponse/token	token	String	Sí	Sí	Cadena generada aleatoriamente

Ejemplo de XML de entrada

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v2="http://dgm.gva.es/ayf/war/schemas/v2_00">
  <soapenv:Header/>
  <soapenv:Body>
    <v2:autenticaUsuarioLDAPWSRequest>
      <v2:usuarioLDAP>?</v2:usuarioLDAP>
      <v2:pwdLDAP>?</v2:pwdLDAP>
    </v2:autenticaUsuarioLDAPWSRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
  <v2:autenticaUsuarioLDAPWSResponse>
    <v2:token>?</v2:token>
  </v2:autenticaUsuarioLDAPWSResponse>
</soapenv:Body>
```

4.3 Autenticación con Usuario

String autenticaUsuarioWS(final String usuario, final String password);

Este servicio es el que permite realizar la autenticación a través de un usuario y pwd de HDFI.

4.3.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
autenticaUsuarioWSRequest/usuario	usuario	List<String[]>	Sí	Sí	Identificador de login de HDFI de un usuario
autenticaUsuarioWSRequest/password	password	String	Sí	Sí	Password de HDFI asociado al usuario.

4.3.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etq. Oblig.	Campo Oblig.	Descripción
autenticaUsuarioWSResponse/token	token	String	Sí	Sí	Cadena generada aleatoriamente

Ejemplo de XML de entrada

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v2="http://dgm.gva.es/ayf/war/schemas/v2_00">
  <soapenv:Header/>
  <soapenv:Body>
    <v2:autenticaUsuarioWSRequest>
      <v2:usuario?</v2:usuario>
      <v2:password?</v2:password>
    </v2:autenticaUsuarioWSRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
  <v2:autenticaUsuarioWSResponse>
    <v2:token?</v2:token>
  </v2:autenticaUsuarioWSResponse>
</soapenv:Body>
```

4.4 Autenticación con Firma

String autenticaConFirmaWS(final byte[] firma);

Este servicio es el que permite realizar la autenticación a través de una firma realizada en cliente.

4.4.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
autenticaConFirmaWSRequest/firma	Firma	Byte[]	Sí	Sí	Firma a utilizar para la autenticación

4.4.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etq. Oblig.	Campo Oblig.	Descripción
autenticaConFirmaWSResponse/token	token	String	Sí	Sí	Cadena generada aleatoriamente

Ejemplo de XML de entrada

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:v2="http://dgm.gva.es/ayf/war/schemas/v2_00">
  <soapenv:Header/>
  <soapenv:Body>
    <v2:autenticaConFirmaWSRequest>
      <v2:firma?</v2:firma>
    </v2:autenticaConFirmaWSRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
  <v2:autenticaConFirmaWSResponse>
    <v2:token?</v2:token>
  </v2:autenticaConFirmaWSResponse>
</soapenv:Body>
```

4.5 Mensajes de error y excepciones

Los mensajes de error y excepciones tratados por el bus. Errores que se devuelven como soap fault

ErrorCode	faultstring	Descripción
0101	Imposible ejecutar el servicio	El servicio esta caído y no se pudo cursar la petición del cliente.
0230	El timestamp de la petición debe ser válido y de hoy o de ayer	Se recibe una petición con un timestamp con formato incorrecto o que no es ni de ayer ni de hoy.
0301	Organismo no autorizado	El certificado o procedimiento utilizados son incorrectos y no se pudo autorizar el consumo al servicio
0302	Certificado caducado	El certificado con el que se ha firmado la petición está caducado.
0303	Certificado revocado	El certificado con el que se ha firmado la petición está revocado.
0305	La firma de la petición no es válida	Se ha recibido una petición en la que la firma no es válida
0307	La petición no tiene nodo firma	La petición llega sin firmar
0309	Error al verificar el certificado	El certificado no se ha podido validar
0310	No se ha podido verificar la CA del certificado	No se pudo validar la autoridad certificadora del certificado con el que se firmó la petición
0401	La estructura del XML recibido no corresponde con el esquema	La petición enviada no cumple la estructura del esquema.
0403	El mensaje no es XML valido	El servicio recibio una mensaje con un XML mal formado
0800	Operación solicitada incorrecta	Se dará cuando se invoque un método que no existe en el servicio.
0807	Falta la cabecera Id_trazabilidad	la petición recibida no contenía el tag Id_trazabilidad en la cabecera SOAP
0808	El usuario en el Id_Trazabilidad no corresponde con el usuario en la cabecera de seguridad O El número de serie del Id_Trazabilidad no corresponde con el certificado de firma	El usuario o núm. De serie que se han incluido en el tag Id_trazabilidad no se corresponden con los que vienen incluidos en la cabecera WS-Security
0904	Error general indefinido	Se ha producido un error inesperado durante la ejecución del servicio

4.6 Compromiso de servicio

A determinar con el proveedor. En todo caso se realizará una aproximación inicial por el equipo de interoperabilidad para definirlo en el bus.

4.7 Seguridad del Servicio Web

Se debe incluir en la cabecera SOAP del mensaje, el elemento `Id_trazabilidad` compuesto según las normas marcadas en el documento “Desarrollo y consumo de servicios web. Buenas prácticas”, que podrá encontrar en el portal de documentación de la PAI, apartado “Cómo usar la plataforma”.

La seguridad de los servicios también incluirá el cifrado de canal HTTP mediante el protocolo Secure Sockets Layer con una clave de longitud mínima de 128 bits. La publicación de los servicios se realizará por tanto por HTTPS.

4.7.1 BUS Instrumental

La seguridad de los servicios web publicados en el BUS Instrumental se llevará a cabo mediante los mecanismos de seguridad descritos en el punto anterior, además de la utilización de WS-Security. La invocación de los servicios web se realizará mediante certificado (X509 Certificate Binary Certificate Token).

5 ANEXOS

5.1 WSDL de Autenticación

```
<?xml version="1.0" encoding="UTF-8"?>
<WL5G3N0:definitions
targetNamespace="http://dgm.gva.es/ayf/war/definitions/v2_00"
xmlns:WL5G3N0="http://schemas.xmlsoap.org/wsdl/"
xmlns:WL5G3N1="http://dgm.gva.es/ayf/war/schemas/v2_00"
xmlns:WL5G3N2="http://dgm.gva.es/ayf/war/definitions/v2_00"
xmlns:WL5G3N3="http://schemas.xmlsoap.org/wsdl/soap/">
  <WL5G3N0:types>
    <xsd:schema attributeFormDefault="unqualified"
elementFormDefault="qualified"
targetNamespace="http://dgm.gva.es/ayf/war/schemas/v2_00"
xmlns:sch="http://dgm.gva.es/ayf/war/schemas/v2_00"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:tns="http://dgm.gva.es/ayf/war/schemas/v2_00"
xmlns:wSDL="http://schemas.xmlsoap.org/wsdl/"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
      <xsd:element name="autenticaConFirmaWSRequest">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="firma"
type="xsd:base64Binary"/>
            <xsd:element name="codigoEntidad"
type="xsd:string"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="autenticaConFirmaWSResponse">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="token" type="xsd:string"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="getInformacionWSRequest">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="token" type="xsd:string"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
      <xsd:element name="getInformacionWSResponse">
        <xsd:complexType>
          <xsd:sequence>
            <xsd:element name="serialNumber"
type="xsd:string"/>
            <xsd:element name="issuerDN" type="xsd:string"/>
            <xsd:element name="subjectDN"
type="xsd:string"/>
            <xsd:element name="nombre" type="xsd:string"/>
          </xsd:sequence>
        </xsd:complexType>
      </xsd:element>
    </xsd:schema>
  </WL5G3N0:types>
</WL5G3N0:definitions>
```

```

type="xsd:string"/>
type="xsd:string"/>
type="xsd:string"/>
type="xsd:string"/>
type="xsd:string"/>
type="xsd:string"/>
type="xsd:string"/>
type="xsd:string"/>
type="xsd:string"/>
type="xsd:string"/>

<xsd:element name="apellido1"
<xsd:element name="apellido2"
<xsd:element name="nif" type="xsd:string"/>
<xsd:element name="cif" type="xsd:string"/>
<xsd:element name="razon_social"
<xsd:element name="habilitado"
<xsd:element name="representante"
<xsd:element name="oid" type="xsd:string"/>
<xsd:element name="tipo_aut" type="xsd:string"/>
<xsd:element name="idHDFI" type="xsd:string"/>
<xsd:element name="email" type="xsd:string"/>
<xsd:element name="tipoCertificado"
<xsd:element name="codEntidad"
  </xsd:sequence>
</xsd:complexType>
</xsd:element>
<xsd:element name="autenticaUsuarioWSRequest">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="usuario" type="xsd:string"/>
      <xsd:element name="password" type="xsd:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="autenticaUsuarioWSResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="token" type="xsd:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="autenticaUsuarioLDAPWSRequest">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="usuarioLDAP"
type="xsd:string"/>
      <xsd:element name="pwdLDAP" type="xsd:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="autenticaUsuarioLDAPWSResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="token" type="xsd:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
</xsd:schema>
</WL5G3N0:types>

```

```
<WL5G3N0:message name="autenticaUsuarioWSRequest">
  <WL5G3N0:part element="WL5G3N1:autenticaUsuarioWSRequest"
name="autenticaUsuarioWSRequest"/>
</WL5G3N0:message>
<WL5G3N0:message name="autenticaUsuarioWSResponse">
  <WL5G3N0:part element="WL5G3N1:autenticaUsuarioWSResponse"
name="autenticaUsuarioWSResponse"/>
</WL5G3N0:message>
<WL5G3N0:message name="getInformacionWSRequest">
  <WL5G3N0:part element="WL5G3N1:getInformacionWSRequest"
name="getInformacionWSRequest"/>
</WL5G3N0:message>
<WL5G3N0:message name="getInformacionWSResponse">
  <WL5G3N0:part element="WL5G3N1:getInformacionWSResponse"
name="getInformacionWSResponse"/>
</WL5G3N0:message>
<WL5G3N0:message name="autenticaConFirmaWSRequest">
  <WL5G3N0:part element="WL5G3N1:autenticaConFirmaWSRequest"
name="autenticaConFirmaWSRequest"/>
</WL5G3N0:message>
<WL5G3N0:message name="autenticaConFirmaWSResponse">
  <WL5G3N0:part element="WL5G3N1:autenticaConFirmaWSResponse"
name="autenticaConFirmaWSResponse"/>
</WL5G3N0:message>
<WL5G3N0:message name="autenticaUsuarioLDAPWSRequest">
  <WL5G3N0:part element="WL5G3N1:autenticaUsuarioLDAPWSRequest"
name="autenticaUsuarioLDAPWSRequest"/>
</WL5G3N0:message>
<WL5G3N0:message name="autenticaUsuarioLDAPWSResponse">
  <WL5G3N0:part element="WL5G3N1:autenticaUsuarioLDAPWSResponse"
name="autenticaUsuarioLDAPWSResponse"/>
</WL5G3N0:message>
<WL5G3N0:portType name="AutenticacionArangiPortType">
  <WL5G3N0:operation name="autenticaUsuarioWS">
    <WL5G3N0:input message="WL5G3N2:autenticaUsuarioWSRequest"
name="autenticaUsuarioWSRequest"/>
    <WL5G3N0:output message="WL5G3N2:autenticaUsuarioWSResponse"
name="autenticaUsuarioWSResponse"/>
  </WL5G3N0:operation>
  <WL5G3N0:operation name="getInformacionWS">
    <WL5G3N0:input message="WL5G3N2:getInformacionWSRequest"
name="getInformacionWSRequest"/>
    <WL5G3N0:output message="WL5G3N2:getInformacionWSResponse"
name="getInformacionWSResponse"/>
  </WL5G3N0:operation>
  <WL5G3N0:operation name="autenticaConFirmaWS">
    <WL5G3N0:input message="WL5G3N2:autenticaConFirmaWSRequest"
name="autenticaConFirmaWSRequest"/>
    <WL5G3N0:output message="WL5G3N2:autenticaConFirmaWSResponse"
name="autenticaConFirmaWSResponse"/>
  </WL5G3N0:operation>
  <WL5G3N0:operation name="autenticaUsuarioLDAPWS">
    <WL5G3N0:input message="WL5G3N2:autenticaUsuarioLDAPWSRequest"
name="autenticaUsuarioLDAPWSRequest"/>
```

```
        <WL5G3N0:output
message="WL5G3N2:autenticaUsuarioLDAPWSResponse"
name="autenticaUsuarioLDAPWSResponse"/>
        </WL5G3N0:operation>
    </WL5G3N0:portType>
    <WL5G3N0:binding name="AutenticacionArangiPortTypeSoap11"
type="WL5G3N2:AutenticacionArangiPortType">
        <WL5G3N3:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http"/>
        <WL5G3N0:operation name="autenticaUsuarioWS">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="autenticaUsuarioWSRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="autenticaUsuarioWSResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="getInformacionWS">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="getInformacionWSRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="getInformacionWSResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="autenticaConFirmaWS">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="autenticaConFirmaWSRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="autenticaConFirmaWSResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="autenticaUsuarioLDAPWS">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="autenticaUsuarioLDAPWSRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="autenticaUsuarioLDAPWSResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
    </WL5G3N0:binding>
    <WL5G3N0:service name="AutenticacionArangiService">
        <WL5G3N0:documentation>OSB Service</WL5G3N0:documentation>
        <WL5G3N0:port binding="WL5G3N2:AutenticacionArangiPortTypeSoap11"
name="AutenticacionArangiPortTypeSoap11">
            <WL5G3N3:address location="https://instrumental-
pre.gva.es/pai_bus_ins/SAFE/Autenticacion_v1_00"/>
        </WL5G3N0:port>
    </WL5G3N0:service>
</WL5G3N0:definitions>
```