Sistema Integral Multicanal de Atención al Ciudadano

PAI_CONTRATO_INTEGRACION_SAFE_FIRMA_v1_v004

Contrato de Integración para Servicios Web de SAFE Firma

GENERALITAT VALENCIANA
CONSELLERIA DE HACIENDA Y MODELO ECONÓMICO
DIRECCIO GENERAL DE TECNOLOGIAS
DE LA INFORMACIÓN Y LAS COMUNICACIONES

Versión 004
Enero de 2017

Unió Europea
Fons Europeu de Desenvolupament Regional
Una manera de fer Europa

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

Índice

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_FIRMA_v1_v004.odt

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 Autenticacion
3	16/11/2016	DGTIC	Se añade el contrato de integración del método compleFirma
4	18/01/2017	DGTIC	Se añaden errores 403 y 904 en la tabla de soapfault

1.3 Estado del documento

Responsable aprobación	Fecha

2 Introducción

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

2.1 Alcance

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

2.2 Objetivos

El objetivo principal del contrato de integración es permitir conocer la definición de la estructura de invocación al servicio de SAFE Firma. De este modo el usuario final podrá realizar el consumo del servicios web correctamente.

2.3 Audiencia

Nombre y Apellidos	Rol

Tabla 1: Audiencia

2.4 Glosario

Término	Definición
Intermediador	Sistema informático que hace de intermediación entre el consumo directo de un webservice, que es el que ofrece en última (a efectos del intermediador) instancia la funcionalidad, y el consumidor del servicio.

Tabla 2: Glosario

2.5 Referencias

Referencia	Título

Tabla 3: Referencias

3 Descripción de la integración

Nombre del Servicio	Firma_v1_00
Tipo de Integración	Servicio Web
Modo de funcionamiento	N/A
Intermediario	Plataforma Autonómica de Interoperabilidad de la GVA (PAI)
Proveedor del Servicio	DGTIC
Contacto	PAI

Tabla 4: Datos generales de integración

3.1 Descripción del servicio

En este manual se incluye la descripción de los siguientes características del componente:

1) Firma

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

3.2 Listado de métodos

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

firmarConCertificado: Este método permite realizar un firmado de una cadena/contenido de un documento (byte[]) con el certificado de aplicación.

validarCertificado: Este método permite validar un certificado, su caducidad y si está revocado o no.

validarFirma: Este método permite validar una firma con respecto a un formato de firma en concreto.

obtenerDatosCertificado: Este método permite obtener los datos principales de un certificado en concreto.

validarCertificadoYObtenerDatos: Este método permite validar un certificado, su caducidad y si está revocado o no y además retorna los datos asociados al mismo.

validarFirmaYObtenerDatos: Este método permite validar una firma con respecto a un formato de firma en concreto y retornar la información de su certificado.

coFirmaConCertificado: Este método permite realizar un firma sobre un documento ya firmado con el certificado de aplicación indicado, creando una cofirma sobre esa firma ya existente.

contraFirmaConCertificado: Este método permite realizar un firma sobre un documento ya firmado con el certificado de aplicación indicado, creando una contrafirma sobre esa firma ya existente y sobre el certificado indicado.

validarTodasFirmaYObtenerFirmantes: Este método realiza una validación de cada una de las firmas existentes en el documento firmado en un formato de firma en concreto, retornará si es válida o no, y los datos asociados a cada una de las firmas.

completaFirmas: Este método de uso interno de SAFE, permite completar firmas simples en firmas longevas o con sellado de tiempo.

Como información común a todos los servicios indicar que los valores permitidos en los campos firmaFormato y formatoSubtipo son:

firmaFormato	formatoSubtipo	Descripción
TF02	xades-bes-detached	Formatos de firma xades detached (la firma contiene el documento original)
	xades-t-detached	
	xades-xl-detached	
TF06	pdf	Formatos de firma para pdf
	pades-ltv	

ATF101	pkcs7	Formato de firma PKCS7
ATF102	cms	Formato de firma CMS

4 Detalle del servicio Firma_v1_00

A continuación se detallan los datos de acceso al servicio de Firma_v1_00:

Datos de Acceso al Servicio de Firma_v1_00 en el BUS Instrumental	
Endpoint Pre Producción	https://instrumental-pre.gva.es/pai_bus_ins/SAFE/Firma_v1_00?wsdl
Endpoint Producción	https://instrumental.gva.es/pai_bus_ins/SAFE/Firma_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 Firma_v1_00 en el BUS Innovación	
Endpoint Pre Producción	https://innovacion-pre.gva.es/pai_bus_inno/SAFE/Firma_v1_00?wsdl
Endpoint Producción	https://innovacion.gva.es/pai_bus_inno/SAFE/Firma_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:

- **firmarConCertificado**: Ver 4.1 Firmar con el certificado de una aplicación
- **validarCertificado**: Ver 4.2 Validar un certificado
- **validarFirma**: Ver 4.3 Validar una firma
- **obtenerDatosCertificado**: Ver 4.4 Obtener Datos de un certificado
- **validarCertificadoYObtenerDatos**: Ver 4.5 Validar un certificado y obtener datos
- **validarFirmaYObtenerDatos**: Ver 4.6 Validar una firma y obtener sus datos
- **coFirmaConCertificado**: Ver 4.7 CoFirmar con el certificado de una aplicación
- **contraFirmaConCertificado**: Ver 4.8 ContraFirmar con el certificado de una aplicación

- **validarTodasFirmaYObtenerFirmantes**: Ver 4.9 Validar todas las firmas y obtener los datos de todos los firmantes
- **completaFirma**: Ver

4.1 Firmar con el certificado de una aplicación

byte[]firmarConCertificado(final String idSession, final String idCertificado, final byte[] documento, final String firmaFormato , String formatoSubtipo) ;

Este servicio permite realizar una firma con el certificado de una aplicación, el cual se indica por parámetro sobre un documento y un formato en concreto:

4.1.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
firmarConCertificadoRequest/idSession	idSession	String	Sí	Sí	Identificador univoco de aplicación.
firmarConCertificadoRequest/idCertificado	idCertificado	String	Sí	Sí	Identificador de Certificado a utilizar para el firmado, que identifica unívocamente al certificado aportado y almacenado en SAFE.
firmarConCertificadoRequest/documento	documento	byte[]	Sí	Sí	Array de bytes que contiene la “cadena” a firmar en base 64 en el formato indicado en el parámetro firmaFormato
firmarConCertificadoRequest/firmaFormato	firmaFormato	String	Sí	Sí	Cadena que contiene el nombre del formato de firma a utilizar para realizar la firma. Si el formato indicado no existiera entre los formatos permitidos (definidos en el fichero configuracionConectorFirma.properties), se retornaría un error.
firmarConCertificadoRequest/formatoSubtipo	formatoSubtipo	String	Sí	Sí	Cadena que contiene el nombre del formato de firma del ENI a utilizar para realizar la firma. Si el formato indicado no existiera entre los formatos permitidos, se retornaría un error.

4.1.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
firmarConCertificadoResponse/respons	response	byte[]	Sí	Sí	Array de bytes que contiene la firma realizada. El

e					contenido de este array es un XML de firma creado por el API del conector.

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:firmarConCertificadoRequest>
         <v2:idSession>TRA</v2:idSession>
         <v2:idCertificado>5</v2:idCertificado>
         <v2:documento>SG9sYSBtdW5kbw==</v2:documento>
         <v2:firmaFormato>TF03</v2:firmaFormato>
         <v2:formatoSubtipo>XADES-BES-ATTACHED</v2:formatoSubtipo>
      </v2:firmarConCertificadoRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
   <SOAP-ENV:Body>
                                          <ns2:firmarConCertificadoResponse
xmlns:ns2="http://dgm.gva.es/ayf/war/schemas/v2_00">
         <ns2:response>[firma realizada]</ns2:response>
      </ns2:firmarConCertificadoResponse>
   </SOAP-ENV:Body>
```

El parámetro idCertificado corresponde a un identificador asociado a un certificado almacenado en servidor y proporcionado por la aplicación invocante. Antes de solicitar una firma en servidor con un certificado en concreto, se deberá proporcionar al equipo de SAFE , tanto certificado como clave, para que lo incluyan en el sistema y le proporcione el codigo identificador del mismo, así como identificador de sesión a usar para las peticiones. Con esto se permitirá que coexistan mas de un certificado por aplicación, ya que cada uno de ellos tendrá un identificador univoco. El modo de proporcionar esta información al equipo de SAFE se explica con más detalle en el anexo (Firma delegada en SAFE).

4.2 Validar un certificado

int validarCertificado(final byte[] certificado);

Este servicio permite validar un certificado indicado por parámetro, este servicio valida su caducidad, y su estado.

4.2.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
validarCertificadoRequest/certificado	certificado	byte[]	Sí	Sí	Array de bytes en base 64 que contiene el certificado validar.

4.2.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
validarCertificadoResponse/response	response	int	Sí	Sí	Entero que contiene la validez del certificado. Los valores que se pueden retornar son: Certificado válido = 0 Información insuficiente = -1 Firma inválida = -2 Fallo en la petición = -3 Fallo en la respuesta = -4 Codigo de error general = -5 Codigo error certificado nulo = -6 Certificado caducado/revocado = -7

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:validarCertificadoRequest>
         <v2:certificado>certificado</v2:certificado>
      </v2:validarCertificadoRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<SOAP-ENV:Body>
     <ns2:validarCertificadoResponse
xmlns:ns2="http://dgm.gva.es/ayf/war/schemas/v2_00">
          <ns2:response>-5</ns2:response>
     </ns2:validarCertificadoResponse>
</SOAP-ENV:Body>
```

4.3 Validar una firma

boolean validarFirma(byte[] firma, byte[] documentoOriginal, final String firmaFormato , String formatoSubtipo) ;

Este servicio realiza una validación de una firma en un formato de firma en concreto, únicamente retornará si es válida o no.

4.3.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
validarFirmaRequest/firma	firma	byte[]	Sí	Sí	Array de bytes en base 64 que contiene la firma a validar.
validarFirmaRequest/documentoOriginal	documentoOriginal	byte[]	Sí	Sí	Array de bytes en base 64 que contiene el documento original a validar en el caso de que el formato de firma indicado sea detached.
validarFirmaRequest/firmaFormato	firmaFormato	String	Sí	Sí	Cadena que contiene el nombre del formato de firma a utilizar para realizar la firma. Si el formato indicado no existiera entre los formatos permitidos (definidos en el fichero configuracionConectorFirma.properties), se retornaría un error.
validarFirmaRequest/formatoSubtipo	formatoSubtipo	String	No	No	Cadena que contiene el nombre del formato de firma del ENI a utilizar para realizar la firma. Si el formato indicado no existiera entre los formatos permitidos, se retornaría un error.

4.3.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
validarFirmaResponse/valida	valida	boolean	Sí	Sí	Retorna si es valida o no la firma con respecto al formato de firma indicado por parámetro de entrada.

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:validarFirmaRequest>
         <v2:firma>firma</v2:firma>
         <v2:documentoOriginal>doc_original</v2:documentoOriginal>
         <v2:firmaFormato>TF02</v2:firmaFormato>
         <!--Optional:-->
         <v2:formatoSubtipo>XADES-BES-DETACHED</v2:formatoSubtipo>
      </v2:validarFirmaRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
     <v2:validarFirmaResponse>
```

```
            <v2:valida>?</v2:valida>
        </v2:validarFirmaResponse>
</soapenv:Body>
```

4.4 Obtener Datos de un certificado

Object[] obtenerDatosCertificado(final byte[] certificado);

Este servicio se mantiene como operación atómica y por compatibilidad con la plataforma de interoperabilidad que necesita únicamente esta información.

4.4.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
obtenerDatosCertificadoRequest/certificado	certificado	byte[]	Sí	Sí	Array de bytes que contiene el certificado en base 64, del cual se va a extraer el contenido.

4.4.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
obtenerDatosCertificadoResponse	serialNumber	String	Sí	Sí	SerialNumber
obtenerDatosCertificadoResponse	issuerDN	String	Sí	Sí	IssuerDN
obtenerDatosCertificadoResponse	subjectDN	String	Sí	Sí	SubjectDN

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:obtenerDatosCertificadoRequest>
         <v2:certificado>certificado</v2:certificado>
      </v2:obtenerDatosCertificadoRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
   <soapenv:Body>
      <v2:obtenerDatosCertificadoResponse>
         <v2:serialNumber>?</v2:serialNumber>
         <v2:issuerDN>?</v2:issuerDN>
         <v2:subjectDN>?</v2:subjectDN>
```

```
    </v2:obtenerDatosCertificadoResponse>
</soapenv:Body>
```

4.5 Validar un certificado y obtener datos

Object[] validarCertificadoYObtenerDatos(final byte[] certificado);

Este servicio permite validar un certificado indicado por parámetro, este servicio valida su caducidad, y su estado, además de retornar la información asociada.

4.5.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
validarCertificadoYObtenerDatosRequest/certificado	certificado	byte[]	Sí	Sí	Array de bytes que contiene el certificado en base 64 a validar.

4.5.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
validarCertificadoYObtenerDatosRequest	validarCertificadoYObtenerDatosRequest	Object[]	Sí	Sí	Retornará la información extraíble del certificado en el caso de que sea válido. Dentro del array de datos aparece el campo response que indica la respuesta de la operación. Los valores que se pueden retornar son: Certificado válido = 0 Información insuficiente = -1 Firma inválida = -2 Fallo en la petición = -3 Fallo en la respuesta = -4 Codigo de error general = -5 Codigo error certificado nulo = -6 Certificado caducado/revocado = -7

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:validarCertificadoYObtenerDatosRequest>
         <v2:certificado>certificado</v2:certificado>
```

```
      </v2:validarCertificadoYObtenerDatosRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
     <v2:validarCertificadoYObtenerDatosResponse>
          <v2:response>?</v2:response>
          <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:email>?</v2:email>
          <v2:tipoCertificado>?</v2:tipoCertificado>
     </v2:validarCertificadoYObtenerDatosResponse>
</soapenv:Body>
```

4.6 Validar una firma y obtener sus datos

Object[]validarFirmaYObtenerDatos(byte[] firma, byte[] documentoOriginal, final String firmaFormato , String formatoSubtipo) ;

Este servicio realiza una validación de una firma en un formato de firma en concreto, retornará si es válida o no, y los datos asociados a la misma.

4.6.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
validarFirmaYObtenerDatosRequest/firma	firma	byte[]	Sí	Sí	Array de bytes en base 64 que contiene la firma a validar.
validarFirmaYObtenerDatosRequest/documentoOriginal	documentoOriginal	byte[]	Sí	Sí	Array de bytes en base 64 que contiene el documento original a validar en el caso de que el formato de firma indicado sea detached.
validarFirmaYObtenerDatosRequest/firmaFormato	firmaFormato	String	Sí	Sí	Cadena que contiene el nombre del formato de firma a utilizar para realizar la firma. Si el formato indicado no existiera entre los formatos permitidos (definidos en el fichero

					configuracionConectorFirma.properties), se retornaría un error.
validarFirmaYObtenerDatosRequest/formatoSubtipo	formatoSubtipo	String	No	No	Cadena que contiene el nombre del formato de firma del ENI a utilizar para realizar la firma. Si el formato indicado no existiera entre los formatos permitidos, se retornaría un error.

4.6.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
validarFirmaYObtenerDatosResponse	validarFirmaYObtenerDatosResponse	Object[]	Sí	Sí	Retornará la información extraíble del certificado en el caso de que sea válido.

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:validarFirmaYObtenerDatosRequest>
         <v2:firma>firma</v2:firma>
         <v2:documentoOriginal>doc_original</v2:documentoOriginal>
         <v2:firmaFormato>TF02</v2:firmaFormato>
         <!--Optional:-->
         <v2:formatoSubtipo></v2:formatoSubtipo>
      </v2:validarFirmaYObtenerDatosRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
     <v2:validarFirmaYObtenerDatosResponse>
          <v2:valida>?</v2:valida>
          <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:email>?</v2:email>
          <v2:tipoCertificado>?</v2:tipoCertificado>
     </v2:validarFirmaYObtenerDatosResponse>
</soapenv:Body>
```

4.7 CoFirmar con el certificado de una aplicación

byte[]coFirmaConCertificado(final String idSession, final String idCertificado, final byte[] firma, final byte[] documento, final String firmaFormato, final String formatoSubtipo);

Este servicio permite realizar una cofirma con el certificado de una aplicación, el cual se indica por parámetro sobre un documento y un formato en concreto:

4.7.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
coFirmaConCertificadoRequest/idSession	idSession	String	Sí	Sí	Identificador univoco de aplicación.
coFirmaConCertificadoRequest/idCertificado	idCertificado	String	Sí	Sí	Identificador de Certificado a utilizar para el firmado, que identifica unívocamente al certificado aportado y almacenado en SAFE.
coFirmaConCertificadoRequest/firma	firma	byte[]	Sí	Sí	Firma en base 64 previa.
coFirmaConCertificadoRequest/documento	documento	byte[]	Sí	Sí	Array de bytes en base 64 que contiene la “cadena” a firmar en el formato indicado en el parámetro firmaFormato
coFirmaConCertificadoRequest/firmaFormato	firmaFormato	String	Sí	Sí	Cadena que contiene el nombre del formato de firma a utilizar para realizar la firma. Si el formato indicado no existiera entre los formatos permitidos (definidos en el fichero configuracionConectorFirma.properties), se retornaría un error.
coFirmaConCertificadoRequest/subtipoFirma	subtipoFirma	String	Sí	Sí	Cadena que contiene el subtipo (si se quiere indicar) a utilizar con el formato ENI indicado.

4.7.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
coFirmaConCertificadoResponse	coFirmaConCertificadoResponse	byte[]	Sí	Sí	Array de bytes que contiene la firma realizada. El contenido de este array es un XML de firma creado por el API del conector.

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:coFirmaConCertificadoRequest>
         <v2:idSession>?</v2:idSession>
         <v2:idCertificado>?</v2:idCertificado>
         <v2:firma>?</v2:firma>
         <v2:documento>?</v2:documento>
         <v2:firmaFormato>?</v2:firmaFormato>
         <v2:formatoSubtipo>?</v2:formatoSubtipo>
      </v2:coFirmaConCertificadoRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
     <v2:coFirmaConCertificadoResponse>
          <v2:response>cid:189720910893</v2:response>
     </v2:coFirmaConCertificadoResponse>
</soapenv:Body>
```

El parámetro idCertificado corresponde a un identificador asociado a un certificado almacenado en servidor y proporcionado por la aplicación invocante.

Antes de solicitar una firma en servidor con un certificado en concreto, se deberá proporcionar al equipo de SAFE, tanto certificado como clave, para que lo incluyan en el sistema y le proporcione el codigo identificador del mismo, así como identificador de sesión a usar para las peticiones. Con esto se permitirá que coexistan mas de un certificado por aplicación, ya que cada uno de ellos tendrá un identificador univoco. El modo de proporcionar esta información al equipo de SAFE se explica con más detalle en el anexo (Firma delegada en SAFE).

4.8 ContraFirmar con el certificado de una aplicación

byte[] contraFirmaConCertificado(final String idSession, final String idCertificado, final byte[] firma, final String firmaFormato, final String formatoSubtipo, final boolean todo, final byte[] certificadoAContrafirmar);

Este servicio permite realizar una contrafirma con el certificado de una aplicación, el cual se indica por parámetro sobre un documento y un formato en concreto:

4.8.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
contraFirmaConCertificadoRequest/idSession	idSession	String	Sí	Sí	Identificador univoco de aplicación.
contraFirmaConCer	idCertificado	String	Sí	Sí	Identificador de Certificado a utilizar para el firmado, que identifica unívocamente al

tificadoRequest/idCertificado					certificado aportado y almacenado en SAFE.
contraFirmaConCertificadoRequest/firma	firma	byte[]	Sí	Sí	Firma en base 64 previa.
contraFirmaConCertificadoRequest/firmaFormato	firmaFormato	String	Sí	Sí	Cadena que contiene el nombre del formato de firma a utilizar para realizar la firma. Si el formato indicado no existiera entre los formatos permitidos (definidos en el fichero configuracionConectorFirma.properties), se retornaría un error.
contraFirmaConCertificadoRequest/subtipoFirma	subtipoFirma	String	Sí	Sí	Cadena que contiene el subtipo (si se quiere indicar) a utilizar con el formato ENI indicado.
contraFirmaConCertificadoRequest/todo	todo	boolean	Sí	Sí	Si todo= false y certificadoAContraFirmar==null CONTRAFIRMAMOS la ultima firma Si todo= false y certificadoAContraFirmar!=null CONTRAFIRMAMOS el certificado que nos indican
contraFirmaConCertificadoRequest/certificadoAContrafirmar	certificadoAContrafirmar	byte[]	Sí	Sí	Certificado usado para contrafirmar

4.8.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
contraFirmaConCertificadoResponse	contraFirmaConCertificadoResponse	byte[]	Sí	Sí	Array de bytes que contiene la firma realizada. El contenido de este array es un XML de firma creado por el API del conector.

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:contraFirmaConCertificadoRequest>
         <v2:idSession>?</v2:idSession>
         <v2:idCertificado>?</v2:idCertificado>
         <v2:firma>?</v2:firma>
         <v2:firmaFormato>?</v2:firmaFormato>
         <v2:formatoSubtipo>?</v2:formatoSubtipo>
```

```
            <v2:todo>?</v2:todo>
            <v2:certificadoAContraFirmar>?</v2:certificadoAContraFirmar>
        </v2:contraFirmaConCertificadoRequest>
    </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
     <v2:contraFirmaConCertificadoResponse>
          <v2:response>cid:1006642413855</v2:response>
     </v2:contraFirmaConCertificadoResponse>
</soapenv:Body>
```

El parámetro idCertificado corresponde a un identificador asociado a un certificado almacenado en servidor y proporcionado por la aplicación invocante.

Antes de solicitar una firma en servidor con un certificado en concreto, se deberá proporcionar al equipo de SAFE, tanto certificado como clave, para que lo incluyan en el sistema y le proporcione el codigo identificador del mismo, así como identificador de sesión a usar para las peticiones. Con esto se permitirá que coexistan mas de un certificado por aplicación, ya que cada uno de ellos tendrá un identificador univoco. El modo de proporcionar esta información al equipo de SAFE se explica con más detalle en el anexo (Firma delegada en SAFE).

4.9 Validar todas las firmas y obtener los datos de todos los firmantes

Object[]validarTodasFirmaYObtenerFirmantes(final byte[] firma, final byte[] documentoOriginal, final String firmaFormato, final String formatoSubtipo);

Este servicio realiza una validación de cada una de las firmas existentes en el documento firmado en un formato de firma en concreto, retornará si es válida o no, y los datos asociados a cada una de las firmas.

4.9.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
validarTodasFirmaYObtenerFirmantesRequest/firma	firma	byte[]	Sí	Sí	Array de bytes en base 64 que contiene la firma a validar.
validarTodasFirmaYObtenerFirmantesRequest/documentoOriginal	documentoOriginal	byte[]	Sí	Sí	Array de bytes en base 64 que contiene el documento original a validar en el caso de que el formato de firma indicado sea detached.
validarTodasFirmaYObtenerFirmantesRequest/firmaFormato	firmaFormato	String	Sí	Sí	Cadena que contiene el subtipo (si se quiere indicar) a utilizar con el formato ENI indicado.
validarTodasFirmaYObtenerFirmantesRequest/formatoSubti	formatoSubtipo	String	Sí	Sí	Cadena que contiene el nombre del formato de firma del ENI a utilizar para realizar

po					la firma. Si el formato indicado no existiera entre los formatos permitidos, se retornaría un error.

4.9.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
validarTodasFirmaYObtenerFirmantesResponse	Valida	String	Sí	Sí	Indica si las firmas son todas validas
validarTodasFirmaYObtenerFirmantesResponse	listaFirmantes	firmantes[]	Si	Si	Array que contiene una lista de objetos firmantes que contienen: - issuerDN - serialNumber - nombre - oid - tipoCertificado

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:validarTodasFirmaYObtenerFirmantesRequest>
         <v2:firma>?</v2:firma>
         <v2:documentoOriginal>?</v2:documentoOriginal>
         <v2:firmaFormato>?</v2:firmaFormato>
         <v2:formatoSubtipo>?</v2:formatoSubtipo>
      </v2:validarTodasFirmaYObtenerFirmantesRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Envelope xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/">
   <soapenv:Header/>
   <soapenv:Body>
                              <ns2:validarTodasFirmaYObtenerFirmantesResponse
xmlns:ns2="http://dgm.gva.es/ayf/war/schemas/v2_00">
         <ns2:valida>true</ns2:valida>
         <ns2:listaFirmantes>
            <ns2:firmantes>
               <ns2:issuerDN></ns2:issuerDN>
               <ns2:serialNumber></ns2:serialNumber>
               <ns2:subjectDN></ns2:subjectDN>
               <ns2:nombre></ns2:nombre>
               <ns2:oid></ns2:oid>
               <ns2:tipoCertificado></ns2:tipoCertificado>
            </ns2:firmantes>
```

```
            ...
            </ns2:listaFirmantes>
         </ns2:validarTodasFirmaYObtenerFirmantesResponse>
      </soapenv:Body>
   </soapenv:Envelope>
```

4.10 Completar Firma

byte[] completaFirma(final byte[] firma, final String formato);

Este servicio realiza una completitud de la firma indicada al formato indicado. Este servicio es de uso interno de SAFE.

4.10.1 Parámetros Entrada

Ubicación	Nombre	Tipo	Etiqueta Obligatoria	Campo Obligatorio	Descripción
completFirmaRequest/firma	firma	byte[]	Sí	Sí	Array de bytes en base 64 que contiene la firma a completar.
completaFirmaRequest/formato	Formato	String	Sí	Sí	Cadena que contiene el nombre del formato de firma a utilizar para realizar la completitud de firma. Si el formato indicado no existiera entre los formatos permitidos, se retornaría un error.

4.10.2 Parámetros Salida

Ubicación	Nombre	Tipo	Etiq. Oblig.	Campo Oblig.	Descripción
completaFirmaResponse	response	byte[]	Sí	Sí	Array de bytes que contiene la firma compeltada. El contenido de este array es un XML de firma creado por el API del conector.

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:completaFirmaRequest>
         <v2:firma>?</v2:firma>
         <v2:formato>?</v2:formato>
      </v2: completaFirmaRequest >
   </soapenv:Body>
</soapenv:Envelope>
```

Ejemplo de XML de salida

```
<soapenv:Body>
     <v2:completaFirmaResponse>
          <v2:response>cid:1006642413855</v2:response>
     </v2:completaFirmaResponse>
</soapenv:Body>
```

4.11 Mensajes de error y excepciones

Los mensajes de error y excepciones asociados a SAFE están controlados de la siguiente manera.

4.11.1 Errores en servicios web

1. Cuando un servicio de busqueda no encuentra información asociada a la busqueda planteada se retorna una respuesta vacía y no una excepción.
2. Cuando un servicio retorna un error de la librería, retorna la misma codificación que retorna la librería.

4.11.2 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	El usuario o núm. De serie que se han incluido en el tag

	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	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 ejecucion del servicio

4.12 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.

4.13 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.

4.13.1 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).

4.14 Ejemplo de Invocación a los servicios

Un ejemplo de uso y de invocación de los servicios, por ejemplo de Firma, se realizaría creando un cliente del servicio web asociado a través del wsdl que se proporciona, su aspecto general una vez generado el cliente a través del IDE seleccionado sería:

```
//URL donde está publicado el servicio en el bus
String endpoint  = "https://instrumental-pre.gva.es/pai_bus_ins/SAFE/Firma_v1_00?
wsdl";

FirmaArangiService service = new FirmaArangiService(new URL (endpoint));
FirmaArangiPortType port = service.getFirmaArangiPortTypeSoap11();
```

```
FirmarCertificadoServerRequest request = new FirmarCertificadoServerRequest();

//Recogemos el contenido del documento
byte[] documentoTexto= UtilidadesGeneralesSAFE.getBytesFromFile(new
File("d:/pruebas_arangi/documento.txt"));

//Configuramos el servicio
request.setDocumento(documentoTexto);
request.setFirmaFormato("TF03");
//*************************************************************************

//Invocamos el firmado en servidor
FirmarCertificadoServerResponse response = port.firmarCertificadoServer(request);
byte[] respuesta = response.getResponse(); //Retorna el XML de la firma generada
//*************************************************************************
```

4.15 Firma delegada en SAFE

La firma delegada en SAFE es una firma que se realiza en el entorno de servidor de SAFE con certificados que proporcionan las entidades firmantes.

Internamente la firma delegada usa el certificado y la clave encriptada proporcionada para firmar en nombre del solicitante de la firma.

SAFE únicamente conoce el identificador de certificado asi como el identificador de aplicación que desea utilizar el mismo. Si esta aplicación no tuviera permisos para utilizarlo, no se podrá realizar la firma. Asimismo, hay que destacar que este servicio no es un servicio público sino que es un servicio proporcionado a través de políticas de acceso estrictas de la plataforma de interoperabilidad.

Para poder realizar una firma delegada es necesario conocer 2 datos que únicamente se entregan en el momento en que se inserta en SAFE el certificado proporcionado y que solo conocen el solicitante y la persona encargada de insertar el certificado. Estos dos datos son:

- Identificador de aplicación
- Identificador de certificado

Ni la contraseña ni el certificado van a estar disponibles de forma externa ni se va a saber la localización de los mismos, ambos elementos están en bbdd y esta información esta encriptada y no está disponible para su consulta. Por lo que el certificado entregado por la entidad para realizar firmas delegadas vía SAFE no será accesible bajo ningun concepto por vía externa, es decir, el único modo de uso del certificado es a través de una petición al servicio de firma firmarConCertificado que está protegido a través de la politica de acceso definida por la Plataforma Autonómica de Interoperabilidad (PAI) para este servicio.

El uso de este certificado para firma delegada se realizará únicamente a través del servicio firmarConCertificado (Error: no se encuentra la fuente de referencia Error: no se encuentra la fuente de referencia).

Un ejemplo de uso es:

```
//URL donde está publicado el servicio en el bus
String endpoint  = "https://instrumental-pre.gva.es/pai_bus_ins/SAFE/Firma_v1_00?
wsdl";

FirmaArangiService service = new FirmaArangiService(new URL (endpoint));
FirmaArangiPortType port = service.getFirmaArangiPortTypeSoap11();
FirmarConCertificadoRequest request = new FirmarConCertificadoRequest();

//Recogemos el contenido del documento
byte[] documentoTexto= UtilidadesGeneralesSAFE.getBytesFromFile(new
File("d:/pruebas_arangi/documento.txt"));

//Configuramos el servicio
request.setDocumento(documentoTexto);
request.setFirmaFormato("TF03");
request.setFormatoSubtipo("xades-t-attached");
//Identificador de certificado a utilizar
request.setIdCertificado("5");
//Identificador de aplicacion
request.setIdSession("TRA");
//*************************************************************************

//Invocamos el firmado en servidor
FirmarConCertificadoResponse response = port.firmarConCertificado(request);
byte[] respuesta = response.getResponse(); //Retorna el XML de la firma generada
//*************************************************************************
```

5 ANEXOS

5.1 WSDL de Firma

```
<?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:complexType name="datos">
                    <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:element name="apellido1" type="xsd:string"/>
                         <xsd:element name="apellido2" type="xsd:string"/>
                         <xsd:element name="nif" type="xsd:string"/>
                         <xsd:element name="cif" type="xsd:string"/>
                         <xsd:element name="razon_social" type="xsd:string"/>
                         <xsd:element name="habilitado" type="xsd:string"/>
                         <xsd:element name="representante" type="xsd:string"/>
                         <xsd:element name="oid" type="xsd:string"/>
                         <xsd:element name="email" type="xsd:string"/>
                         <xsd:element name="tipoCertificado"
type="xsd:string"/>
                    </xsd:sequence>
               </xsd:complexType>
               <xsd:complexType name="firmantes">
                    <xsd:sequence>
                         <xsd:element maxOccurs="unbounded" name="firmante"
type="tns:datos"/>
                    </xsd:sequence>
               </xsd:complexType>
               <xsd:element name="contraFirmaConCertificadoResponse">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="response"
type="xsd:base64Binary"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="contraFirmaConCertificadoRequest">
                    <xsd:complexType>
                         <xsd:sequence>
```

```
                              <xsd:element name="idSession"
type="xsd:string"/>
                              <xsd:element name="idCertificado"
type="xsd:string"/>
                              <xsd:element name="firma"
type="xsd:base64Binary"/>
                              <xsd:element name="firmaFormato"
type="xsd:string"/>
                              <xsd:element name="formatoSubtipo"
type="xsd:string"/>
                              <xsd:element name="todo" type="xsd:boolean"/>
                              <xsd:element name="certificadoAContraFirmar"
type="xsd:base64Binary"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="coFirmaConCertificadoResponse">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="response"
type="xsd:base64Binary"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="coFirmaConCertificadoRequest">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="idSession"
type="xsd:string"/>
                              <xsd:element name="idCertificado"
type="xsd:string"/>
                              <xsd:element name="firma"
type="xsd:base64Binary"/>
                              <xsd:element name="documento"
type="xsd:base64Binary"/>
                              <xsd:element name="firmaFormato"
type="xsd:string"/>
                              <xsd:element name="formatoSubtipo"
type="xsd:string"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="firmarConCertificadoRequest">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="idSession"
type="xsd:string"/>
                              <xsd:element name="idCertificado"
type="xsd:string"/>
                              <xsd:element name="documento"
type="xsd:base64Binary"/>
                              <xsd:element name="firmaFormato"
type="xsd:string"/>
                              <xsd:element name="formatoSubtipo"
type="xsd:string"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
```

```
            <xsd:element name="firmarConCertificadoResponse">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element name="response"
type="xsd:base64Binary"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="obtenerDatosCertificadoRequest">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element name="certificado"
type="xsd:base64Binary"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="obtenerDatosCertificadoResponse">
                <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:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="validarCertificadoResponse">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element name="response" type="xsd:int"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="validarCertificadoRequest">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element name="certificado"
type="xsd:base64Binary"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="validarCertificadoYObtenerDatosRequest">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element name="certificado"
type="xsd:base64Binary"/>
                    </xsd:sequence>
                </xsd:complexType>
            </xsd:element>
            <xsd:element name="validarCertificadoYObtenerDatosResponse">
                <xsd:complexType>
                    <xsd:sequence>
                        <xsd:element name="response" type="xsd:int"/>
                        <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:element name="apellido1"
type="xsd:string"/>
                              <xsd:element name="apellido2"
type="xsd:string"/>
                              <xsd:element name="nif" type="xsd:string"/>
                              <xsd:element name="cif" type="xsd:string"/>
                              <xsd:element name="razon_social"
type="xsd:string"/>
                              <xsd:element name="habilitado"
type="xsd:string"/>
                              <xsd:element name="representante"
type="xsd:string"/>
                              <xsd:element name="oid" type="xsd:string"/>
                              <xsd:element name="email" type="xsd:string"/>
                              <xsd:element name="tipoCertificado"
type="xsd:string"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="validarFirmaRequest">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="firma"
type="xsd:base64Binary"/>
                              <xsd:element name="documentoOriginal"
type="xsd:base64Binary"/>
                              <xsd:element name="firmaFormato"
type="xsd:string"/>
                              <xsd:element minOccurs="0" name="formatoSubtipo"
type="xsd:string"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="validarFirmaResponse">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="valida" type="xsd:boolean"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="validarFirmaYObtenerDatosRequest">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="firma"
type="xsd:base64Binary"/>
                              <xsd:element name="documentoOriginal"
type="xsd:base64Binary"/>
                              <xsd:element name="firmaFormato"
type="xsd:string"/>
                              <xsd:element minOccurs="0" name="formatoSubtipo"
type="xsd:string"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="validarFirmaYObtenerDatosResponse">
```

```
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="valida" type="xsd:boolean"/>
                              <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:element name="apellido1"
type="xsd:string"/>
                              <xsd:element name="apellido2"
type="xsd:string"/>
                              <xsd:element name="nif" type="xsd:string"/>
                              <xsd:element name="cif" type="xsd:string"/>
                              <xsd:element name="razon_social"
type="xsd:string"/>
                              <xsd:element name="habilitado"
type="xsd:string"/>
                              <xsd:element name="representante"
type="xsd:string"/>
                              <xsd:element name="oid" type="xsd:string"/>
                              <xsd:element name="email" type="xsd:string"/>
                              <xsd:element name="tipoCertificado"
type="xsd:string"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="validarTodasFirmaYObtenerFirmantesRequest">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="firma"
type="xsd:base64Binary"/>
                              <xsd:element name="documentoOriginal"
type="xsd:base64Binary"/>
                              <xsd:element name="firmaFormato"
type="xsd:string"/>
                              <xsd:element minOccurs="0" name="formatoSubtipo"
type="xsd:string"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="validarTodasFirmaYObtenerFirmantesResponse">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="valida" type="xsd:boolean"/>
                              <xsd:element maxOccurs="unbounded"
name="listaFirmantes" type="tns:firmantes"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="completaFirmaRequest">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="firma"
type="xsd:base64Binary"/>
                              <xsd:element name="formato" type="xsd:string"/>
                         </xsd:sequence>
```

```
                    </xsd:complexType>
               </xsd:element>
               <xsd:element name="completaFirmaResponse">
                    <xsd:complexType>
                         <xsd:sequence>
                              <xsd:element name="response"
type="xsd:base64Binary"/>
                         </xsd:sequence>
                    </xsd:complexType>
               </xsd:element>
          </xsd:schema>
     </WL5G3N0:types>
     <WL5G3N0:message name="firmarConCertificadoResponse">
          <WL5G3N0:part element="WL5G3N1:firmarConCertificadoResponse"
name="firmarConCertificadoResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="contraFirmaConCertificadoResponse">
          <WL5G3N0:part element="WL5G3N1:contraFirmaConCertificadoResponse"
name="contraFirmaConCertificadoResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarCertificadoResponse">
          <WL5G3N0:part element="WL5G3N1:validarCertificadoResponse"
name="validarCertificadoResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarFirmaYObtenerDatosRequest">
          <WL5G3N0:part element="WL5G3N1:validarFirmaYObtenerDatosRequest"
name="validarFirmaYObtenerDatosRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="contraFirmaConCertificadoRequest">
          <WL5G3N0:part element="WL5G3N1:contraFirmaConCertificadoRequest"
name="contraFirmaConCertificadoRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="obtenerDatosCertificadoRequest">
          <WL5G3N0:part element="WL5G3N1:obtenerDatosCertificadoRequest"
name="obtenerDatosCertificadoRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="completaFirmaResponse">
          <WL5G3N0:part element="WL5G3N1:completaFirmaResponse"
name="completaFirmaResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarFirmaYObtenerDatosResponse">
          <WL5G3N0:part element="WL5G3N1:validarFirmaYObtenerDatosResponse"
name="validarFirmaYObtenerDatosResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarFirmaRequest">
          <WL5G3N0:part element="WL5G3N1:validarFirmaRequest"
name="validarFirmaRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="firmarConCertificadoRequest">
          <WL5G3N0:part element="WL5G3N1:firmarConCertificadoRequest"
name="firmarConCertificadoRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="obtenerDatosCertificadoResponse">
          <WL5G3N0:part element="WL5G3N1:obtenerDatosCertificadoResponse"
name="obtenerDatosCertificadoResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="coFirmaConCertificadoResponse">
```

```
          <WL5G3N0:part element="WL5G3N1:coFirmaConCertificadoResponse"
name="coFirmaConCertificadoResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarCertificadoRequest">
          <WL5G3N0:part element="WL5G3N1:validarCertificadoRequest"
name="validarCertificadoRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="completaFirmaRequest">
          <WL5G3N0:part element="WL5G3N1:completaFirmaRequest"
name="completaFirmaRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarFirmaResponse">
          <WL5G3N0:part element="WL5G3N1:validarFirmaResponse"
name="validarFirmaResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarCertificadoYObtenerDatosRequest">
          <WL5G3N0:part
element="WL5G3N1:validarCertificadoYObtenerDatosRequest"
name="validarCertificadoYObtenerDatosRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="coFirmaConCertificadoRequest">
          <WL5G3N0:part element="WL5G3N1:coFirmaConCertificadoRequest"
name="coFirmaConCertificadoRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarTodasFirmaYObtenerFirmantesRequest">
          <WL5G3N0:part
element="WL5G3N1:validarTodasFirmaYObtenerFirmantesRequest"
name="validarTodasFirmaYObtenerFirmantesRequest"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarCertificadoYObtenerDatosResponse">
          <WL5G3N0:part
element="WL5G3N1:validarCertificadoYObtenerDatosResponse"
name="validarCertificadoYObtenerDatosResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:message name="validarTodasFirmaYObtenerFirmantesResponse">
          <WL5G3N0:part
element="WL5G3N1:validarTodasFirmaYObtenerFirmantesResponse"
name="validarTodasFirmaYObtenerFirmantesResponse"/>
     </WL5G3N0:message>
     <WL5G3N0:portType name="FirmaArangiPortType">
          <WL5G3N0:operation name="firmarConCertificado">
               <WL5G3N0:input message="WL5G3N2:firmarConCertificadoRequest"
name="firmarConCertificadoRequest"/>
               <WL5G3N0:output message="WL5G3N2:firmarConCertificadoResponse"
name="firmarConCertificadoResponse"/>
          </WL5G3N0:operation>
          <WL5G3N0:operation name="contraFirmaConCertificado">
               <WL5G3N0:input
message="WL5G3N2:contraFirmaConCertificadoRequest"
name="contraFirmaConCertificadoRequest"/>
               <WL5G3N0:output
message="WL5G3N2:contraFirmaConCertificadoResponse"
name="contraFirmaConCertificadoResponse"/>
          </WL5G3N0:operation>
          <WL5G3N0:operation name="validarCertificado">
               <WL5G3N0:input message="WL5G3N2:validarCertificadoRequest"
name="validarCertificadoRequest"/>
```

```
            <WL5G3N0:output message="WL5G3N2:validarCertificadoResponse"
name="validarCertificadoResponse"/>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="validarFirmaYObtenerDatos">
            <WL5G3N0:input
message="WL5G3N2:validarFirmaYObtenerDatosRequest"
name="validarFirmaYObtenerDatosRequest"/>
            <WL5G3N0:output
message="WL5G3N2:validarFirmaYObtenerDatosResponse"
name="validarFirmaYObtenerDatosResponse"/>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="obtenerDatosCertificado">
            <WL5G3N0:input message="WL5G3N2:obtenerDatosCertificadoRequest"
name="obtenerDatosCertificadoRequest"/>
            <WL5G3N0:output
message="WL5G3N2:obtenerDatosCertificadoResponse"
name="obtenerDatosCertificadoResponse"/>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="completaFirma">
            <WL5G3N0:input message="WL5G3N2:completaFirmaRequest"
name="completaFirmaRequest"/>
            <WL5G3N0:output message="WL5G3N2:completaFirmaResponse"
name="completaFirmaResponse"/>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="validarFirma">
            <WL5G3N0:input message="WL5G3N2:validarFirmaRequest"
name="validarFirmaRequest"/>
            <WL5G3N0:output message="WL5G3N2:validarFirmaResponse"
name="validarFirmaResponse"/>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="coFirmaConCertificado">
            <WL5G3N0:input message="WL5G3N2:coFirmaConCertificadoRequest"
name="coFirmaConCertificadoRequest"/>
            <WL5G3N0:output message="WL5G3N2:coFirmaConCertificadoResponse"
name="coFirmaConCertificadoResponse"/>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="validarCertificadoYObtenerDatos">
            <WL5G3N0:input
message="WL5G3N2:validarCertificadoYObtenerDatosRequest"
name="validarCertificadoYObtenerDatosRequest"/>
            <WL5G3N0:output
message="WL5G3N2:validarCertificadoYObtenerDatosResponse"
name="validarCertificadoYObtenerDatosResponse"/>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="validarTodasFirmaYObtenerFirmantes">
            <WL5G3N0:input
message="WL5G3N2:validarTodasFirmaYObtenerFirmantesRequest"
name="validarTodasFirmaYObtenerFirmantesRequest"/>
            <WL5G3N0:output
message="WL5G3N2:validarTodasFirmaYObtenerFirmantesResponse"
name="validarTodasFirmaYObtenerFirmantesResponse"/>
        </WL5G3N0:operation>
    </WL5G3N0:portType>
    <WL5G3N0:binding name="FirmaArangiPortTypeSoap11"
type="WL5G3N2:FirmaArangiPortType">
        <WL5G3N3:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http"/>
        <WL5G3N0:operation name="firmarConCertificado">
```

```
            <WL5G3N3:operation/>
            <WL5G3N0:input name="firmarConCertificadoRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="firmarConCertificadoResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="contraFirmaConCertificado">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="contraFirmaConCertificadoRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="contraFirmaConCertificadoResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="validarCertificado">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="validarCertificadoRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="validarCertificadoResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="validarFirmaYObtenerDatos">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="validarFirmaYObtenerDatosRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="validarFirmaYObtenerDatosResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="obtenerDatosCertificado">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="obtenerDatosCertificadoRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="obtenerDatosCertificadoResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="completaFirma">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="completaFirmaRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="completaFirmaResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="validarFirma">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="validarFirmaRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
```

```
            <WL5G3N0:output name="validarFirmaResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="coFirmaConCertificado">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="coFirmaConCertificadoRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="coFirmaConCertificadoResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="validarCertificadoYObtenerDatos">
            <WL5G3N3:operation/>
            <WL5G3N0:input name="validarCertificadoYObtenerDatosRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output name="validarCertificadoYObtenerDatosResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
        <WL5G3N0:operation name="validarTodasFirmaYObtenerFirmantes">
            <WL5G3N3:operation/>
            <WL5G3N0:input
name="validarTodasFirmaYObtenerFirmantesRequest">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:input>
            <WL5G3N0:output
name="validarTodasFirmaYObtenerFirmantesResponse">
                <WL5G3N3:body use="literal"/>
            </WL5G3N0:output>
        </WL5G3N0:operation>
    </WL5G3N0:binding>
    <WL5G3N0:service name="FirmaArangiService">
        <WL5G3N0:documentation>OSB Service</WL5G3N0:documentation>
        <WL5G3N0:port binding="WL5G3N2:FirmaArangiPortTypeSoap11"
name="FirmaArangiPortTypeSoap11">
            <WL5G3N3:address location="https://instrumental-
pre.gva.es/pai_bus_ins/SAFE/Firma_v1_00"/>
        </WL5G3N0:port>
    </WL5G3N0:service>
</WL5G3N0:definitions>
```