



Sistema Integral Multicanal de Atención al Ciudadano

e-SIRCA-DISEÑO-
CONTRATO_INTEGRACION_WS_SAFE_EXT_v1

Contrato de Integración para Servicios Web externos
de SAFE

Índice

1	Control del documento	3
1.1	Información general	3
1.2	Histórico de revisiones	3
1.3	Estado del documento	3
2	Introducción	4
2.1	Alcance	4
2.2	Objetivos	4
2.3	Audiencia	4
2.4	Glosario	4
2.5	Referencias	4
3	Descripción de la integración	5
3.1	Descripción del servicio	5
3.2	Detalle del servicio	6
3.2.1	Autenticación	6
3.2.1.1	Obtener información de autenticación	6
3.2.2	Firma	9
3.2.2.1	Firmar con el certificado de SAFE	9
3.2.2.2	Firmar con el certificado de una aplicación	10
3.2.2.3	Validar un certificado	11
3.2.2.4	Validar una firma	13
3.2.2.5	Validar una firma SMIME	14
3.2.2.6	Obtener Datos de un certificado	15
3.2.2.7	Validar un certificado y obtener datos	17
3.2.2.8	Validar una firma y obtener sus datos	18
3.2.2.9	Validar una firma y obtener sus datos SMIME	20
3.2.2.10	CoFirmar con el certificado de una aplicación	22
3.2.2.11	ContraFirmar con el certificado de una aplicación	23
3.2.2.12	Validar todas las firmas y obtener los datos de todos los firmantes	25
3.2.3	Mensajes de error y excepciones	26
3.2.3.1	Errores en servicios web	26
3.3	Compromiso de servicio	27
3.4	Seguridad del Servicio Web	27
4	ANEXOS	28
4.1	WSDL de los subsistemas	28
4.1.1	WSDL de Autenticación	28
4.1.2	WSDL de Firma	31
4.2	Ejemplo de Invocación a los servicios	40
4.3	Firma delegada en SAFE	41

1 Control del documento

1.1 Información general

Título	Contrato de Integración para Servicio Web de SAFE
Creado por	S2Grupo
Revisado por	
Lista de distribución	
Nombre del fichero	e-SIRCA-DISEÑO- CONTRATO_INTEGRACION_WS_SAFE_AUTENTICACION_Y_FIRMA_INT_v1 _v006.doc

1.2 Histórico de revisiones

Versión	Fecha	Autor	Observaciones
1	03/07/2012	DGTI	Versión inicial
2	--	S2grupo	Revisión del documento
3	30/05/2014	S2grupo	Revisión del documento
4	06/08/2014	S2grupo	Revisión del documento
5	16/01/2015	S2grupo	Revisión del documento y solución de erratas
6	19/01/2015	S2grupo	Revisión del documento y solución de erratas

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 Autenticación y Firma Electronica 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. 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	AutenticacionArangi_v1, FirmaArangi_v1
Tipo de Integración	Servicio Web
Modo de funcionamiento	N/A
Intermediario	Plataforma de Interoperabilidad GVA
Proveedor del Servicio	
Contacto	Responsables de interoperabilidad

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
- 2) Autenticación

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

SUBSISTEMA	SERVICIO
FIRMA	POLITICA CERTIFICADO
	firmarCertificadoServer(final byte[] documento, String firmaFormato, String formatoSubtipo)
	firmarConCertificado(final String idSession, final String idCertificado, final byte[] documento, final String firmaFormato, String formatoSubtipo)
	obtenerDatosCertificado(byte[] certificado)
	validarCertificado(byte[] certificado)
	validarFirma(byte[] firma, byte[] documentoOriginal, final String firmaFormato, String formatoSubtipo)
	validarCertificadoYObtenerDatos(final byte[] certificado)
	validarFirmaYObtenerDatos(byte[] firma, byte[] documentoOriginal, final String firmaFormato, String formatoSubtipo)
	validarFirmaSMIME(final byte[] tokenValidacion, final byte[] docAValidar)
	validarFirmaSMIMEYObtenerDatos (final byte[] tokenValidacion, final byte[] docAValidar)
	coFirmaConCertificado(final String idSession, final String idCertificado, final byte[] firma, final byte[] documento, final String firmaFormato, final String formatoSubtipo)
	contraFirmaConCertificado(final String idSession, final String idCertificado, final byte[] firma, final String firmaFormato, final String formatoSubtipo, final boolean todo, final byte[] certificadoAContrafirmar)
	validarTodasFirmaYObtenerFirmantes(final byte[] firma, final byte[] documentoOriginal, final String firmaFormato, final String formatoSubtipo)

AUTENTICACION	POLITICA CERTIFICADO
	getInformacionWS(String token)

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	
TF03	xades-bes-attached	Formatos de firma xades attached (la firma no contiene el documento original)
	xades-t-attached	
	xades-xl-attached	
TF06	pdf	Formatos de firma para pdf
	pades-ltv	
ATF101	pkcs7	Formato de firma PKCS7
ATF102	cms	Formato de firma CMS

3.2 Detalle del servicio

3.2.1 Autenticacion

Código	AutenticacionArangi_v1_00
wsdl	https://preinterint.gva.es/eSirca_Bus/ins/Proxy/SAFE/AutenticacionArangi_v1_00?wsdl - Preproducción https://interint.gva.es/eSirca_Bus/ins/Proxy/SAFE/AutenticacionArangi_v1_00?wsdl Producción
Descripción	Existe un conjunto de servicios publicados que ofrecen la funcionalidad de autenticación necesaria. Estos servicios pueden ser consumidos para obtener las credenciales de un usuario:

3.2.1.1 Obtener información de autenticación

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

Servicio
Object[] getInformacion (String token)
Descripción

Este método realiza la obtención de los datos de autenticación asociados a un token generado por un usuario autenticado.			
Parámetros de Entrada			
	Tipo	Descripción	
	token	String	Cadena generada aleatoriamente
Respuesta			
	Tipo	Descripción	
	Object[]	Object[]	<p>Retorna un array de datos que incluyen dependiendo del tipo de autenticación:</p> <p>Si tipo es certificado=</p> <ol style="list-style-type: none"> 1. Tipo de autenticación (valor = CERTIFICADO) 2. SERIALNUMBER 3. SUBJECTDN 4. ISSUERDN 5. Nombre 6. Apellido1 7. Apellido2 8. NIF 9. CIF 10. Razon Social 11. OID del certificado 12. Tipo de certificado 13. Email <p>Si el tipo es HDFI (USO EXCLUSIVO GVA)=</p> <ol style="list-style-type: none"> 1. Tipo de autenticación (valor = USUARIOPWD) 2. ID de HDFI (si fuera asi) 3. Nombre 4. Apellido1 5. Apellido2 6. NIF 7. CIF 8. Razon Social
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre><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></pre>			
XML de Salida			

```
<xsd:element name="getInformacionWSResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="1" name="serialNumber" type="xsd:string"/>
      <xsd:element minOccurs="1" name="issuerDN" type="xsd:string"/>
      <xsd:element minOccurs="1" name="subjectDN" type="xsd:string"/>
      <xsd:element minOccurs="1" name="nombre" type="xsd:string"/>
      <xsd:element minOccurs="1" name="apellido1" type="xsd:string"/>
      <xsd:element minOccurs="1" name="apellido2" type="xsd:string"/>
      <xsd:element minOccurs="1" name="nif" type="xsd:string"/>
      <xsd:element minOccurs="1" name="cif" type="xsd:string"/>
      <xsd:element minOccurs="1" name="razon_social" type="xsd:string"/>
      <xsd:element minOccurs="1" name="habilitado" type="xsd:string"/>
      <xsd:element minOccurs="1" name="representante" type="xsd:string"/>
      <xsd:element minOccurs="1" name="oid" type="xsd:string"/>
      <xsd:element minOccurs="1" name="tipo_aut" type="xsd:string"/>
      <xsd:element minOccurs="1" name="idHDFI" type="xsd:string"/>
      <xsd:element minOccurs="1" name="email" type="xsd:string"/>
      <xsd:element minOccurs="1" name="tipoCertificado" type="xsd:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```


3.2.2 Firma

Código	FirmaArangi_v1_00
wsdl	https://preinterint.gva.es/eSirca_Bus/ins/Proxy/SAFE/FirmaArangi_v1_00?wsdl <i>Preproducción</i> https://interint.gva.es/eSirca_Bus/ins/Proxy/SAFE/FirmaArangi_v1_00?wsdl <i>Producción</i>
Descripción	Existe un conjunto de servicios publicados que ofrecen la funcionalidad de firma y validación necesaria.

3.2.2.1 Firmar con el certificado de SAFE

Este servicio permite realizar una firma con el certificado de servidor de SAFE sobre un documento y un formato en concreto:

Servicio			
byte[]firmarCertificadoServer(final byte[] documento, String firmaFormato, String formatoSubtipo)			
Descripción			
Este método permite realizar un firmado de una cadena/contenido de un documento (byte[]) con el certificado de aplicación de SAFE			
Parámetros de Entrada			
		Tipo	Descripción
	documento	byte[]	Array de bytes que contiene la "cadena" en base 64 a firmar en el formato indicado en el parámetro firmaFormato
	firmaFormato	String	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.
	formatoSubtipo	String	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.
Respuesta			
		Tipo	Descripción
	byte[]	byte[]	Array de bytes que contiene la firma realizada. El contenido de este array es un XML de firma creado por el API del conector.
Seguridad			
Mecanismo de seguridad WS-Security			

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:firmarCertificadoServerRequest>
      <v2:documento>SG9sYSBtdW5kbw==</v2:documento>
      <v2:firmaFormato>TF03</v2:firmaFormato>
      <v2:formatoSubtipo>XADES-BES-ATTACHED</v2:formatoSubtipo>
    </v2:firmarCertificadoServerRequest>
  </soapenv:Body>
</soapenv:Envelope>
    
```

XML de Salida

```

<xsd:element name="firmarCertificadoServerResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="1" name="response" type="xsd:base64Binary"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
    
```

3.2.2.2 Firmar con el certificado de una aplicación

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:

Servicio			
byte[]firmarConCertificado(final String idSession, final String idCertificado, final byte[] documento, final String firmaFormato , String formatoSubtipo)			
Descripción			
Este método permite realizar un firmado de una cadena/contenido de un documento (byte[]) con el certificado de aplicación.			
Parámetros de Entrada			
		Tipo	Descripción
	idSession	String	Identificador univoco de aplicación.
	idCertificado	String	Identificador de Certificado a utilizar para el firmado, que identifica unívocamente al certificado aportado y almacenado en SAFE.
	documento	byte[]	Array de bytes que contiene la “cadena” a firmar en base 64 en el formato indicado en el parámetro firmaFormato
	firmaFormato	String	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.
	formatoSubtipo	String	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.
Respuesta			
		Tipo	Descripción
	byte[]	byte[]	Array de bytes que contiene la firma realizada. El contenido de este array es un XML de firma creado por el API del conector.
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre> <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> </pre>			
XML de Salida			
<pre> <xsd:element name="firmarConCertificadoResponse"> <xsd:complexType> <xsd:sequence> <xsd:element minOccurs="1" name="response" type="xsd:base64Binary"/> </xsd:sequence> </xsd:complexType> </xsd:element> </pre>			

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 código 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 unívoco. El modo de proporcionar esta información al equipo de SAFE se explica con más detalle en el anexo (Firma delegada en SAFE).

3.2.2.3 Validar un certificado

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

Servicio
int validarCertificado(final byte[] certificado);

Descripción			
Este método permite validar un certificado, su caducidad y si está revocado o no.			
Parámetros de Entrada			
		Tipo	Descripción
	certificado	byte[]	Array de bytes en base 64 que contiene el certificado validar.
Respuesta			
		Tipo	Descripción
	int	int	<p>Entero que contiene la validez del certificado.</p> <p>Los valores que se pueden retornar son:</p> <p>RESULT_VALID = 0</p> <p>RESULT_CERTIFICATE_NOT_BELONGS_TRUSTED_CAS = 1</p> <p>RESULT_CERTIFICATE_NOT_ACTIVE = 2</p> <p>RESULT_CERTIFICATE_REVOKED = 3</p> <p>RESULT_CERTIFICATE_UNKNOWN = 4</p> <p>RESULT_CERTIFICATE_CANNOT_BE_VALIDATED = 5</p> <p>RESULT_CERTIFICATE_CHAIN_VALIDATION_INVALID = 6</p> <p>RESULT_SIGNATURE_NOT_MATCH_DATA = 7</p> <p>RESULT_REFERENCE_DIGEST_NOT_MATCH_DATA = 8</p> <p>RESULT_INVALID = 9</p> <p>RESULT_TIMESTAMP_INVALID = 10</p> <p>Estos errores son propios de la librería de ARANGI.</p>
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre><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></pre>			
XML de Salida			
<pre><xsd:element name="validarCertificadoResponse"> <xsd:complexType> <xsd:sequence> <xsd:element minOccurs="1" name="response" type="xsd:int"/> </xsd:sequence> </xsd:complexType> </xsd:element></pre>			

3.2.2.4 Validar una firma

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

Servicio			
boolean validarFirma(byte[] firma, byte[] documentoOriginal, final String firmaFormato , String formatoSubtipo)			
Descripción			
Este método permite validar una firma con respecto a un formato de firma en concreto			
Parámetros de Entrada			
		Tipo	Descripción
	firma	byte[]	Array de bytes en base 64 que contiene la firma a validar.
	documentoOriginal	byte[]	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.
	firmaFormato	String	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.
	formatoSubtipo	String	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.
Respuesta			
		Tipo	Descripción
	boolean	boolean	Retorna si es valida o no la firma con respecto al formato de firma indicado por parámetro de entrada.
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre> <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>TF03</v2:firmaFormato> <!--Optional:--> <v2:formatoSubtipo>XADES-BES-DETACHED</v2:formatoSubtipo> </v2:validarFirmaRequest> </soapenv:Body> </soapenv:Envelope> </pre>			
XML de Salida			

```

<xsd:element name="validarFirmaResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="1" name="valida" type="xsd:boolean"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
  
```

3.2.2.5 Validar una firma SMIME

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

Servicio			
boolean validarFirmaSMIME(final byte[] tokenValidacion, final byte[] docAValidar)			
Descripción			
Este método permite validar una firma SMIME con respecto a un token de validación y el documento original.			
Parámetros de Entrada			
		Tipo	Descripción
	tokenValidacion	byte[]	Array de bytes en base 64 que contiene la firma a validar.
	docAValidar	byte[]	Array de bytes en base 64 que contiene el documento a validar contra su firma.
Respuesta			
		Tipo	Descripción
	boolean	boolean	Retorna si es valida o no la firma.
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre> <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:validarFirmaSMIMERequest> <v2:tokenValidacion>tokenValidacion</tokenValidacion> <v2:docAValidar>DocumentoAValidar</docAValidar> </v2:validarFirmaSMIMERequest> </soapenv:Body> </soapenv:Envelope> </pre>			
XML de Salida			
<pre> <xsd:element name="validarFirmaSMIMEResponse"> <xsd:complexType> <xsd:sequence> <xsd:element minOccurs="1" name="valida" type="xsd:boolean"/> </xsd:sequence> </xsd:complexType> </xsd:element> </pre>			

```

    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

```

3.2.2.6 Obtener Datos de un certificado

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

Servicio																			
Object[] obtenerDatosCertificado(final byte[] certificado)																			
Descripción																			
Este método permite obtener los datos principales de un certificado en concreto.																			
Parámetros de Entrada																			
		Tipo	Descripción																
	certificado	byte[]	Array de bytes que contiene el certificado en base 64, del cual se va a extraer el contenido.																
Respuesta																			
		Tipo	Descripción																
	Object[]	Object[]	Array de objetos que contiene los siguientes datos en sus posiciones: <table><tr><td>0</td><td>SerialNumber</td></tr><tr><td>1</td><td>IssuerDN</td></tr><tr><td>2</td><td>SubjectDN</td></tr><tr><td>3</td><td>PolicyOID</td></tr></table>	0	SerialNumber	1	IssuerDN	2	SubjectDN	3	PolicyOID								
			0	SerialNumber															
			1	IssuerDN															
			2	SubjectDN															
			3	PolicyOID															
			Si el tipo del certificado es de persona/ciudadano : <table><tr><td>4</td><td>NIF</td></tr><tr><td>5</td><td>Nombre</td></tr><tr><td>6</td><td>Primer apellido</td></tr><tr><td>7</td><td>Segundo apellido</td></tr><tr><td>8</td><td>Null</td></tr><tr><td>9</td><td>Null</td></tr><tr><td>10</td><td>Email</td></tr><tr><td>11</td><td>Tipo certificado 0</td></tr></table>	4	NIF	5	Nombre	6	Primer apellido	7	Segundo apellido	8	Null	9	Null	10	Email	11	Tipo certificado 0
			4	NIF															
			5	Nombre															
			6	Primer apellido															
			7	Segundo apellido															
			8	Null															
			9	Null															
10	Email																		
11	Tipo certificado 0																		
Si el tipo de certificado es de empleado público : <table><tr><td>4</td><td>NIF</td></tr><tr><td>5</td><td>Nombre</td></tr></table>	4	NIF	5	Nombre															
4	NIF																		
5	Nombre																		

			<table border="1"> <tr><td>6</td><td>Primer apellido</td></tr> <tr><td>7</td><td>Segundo apellido</td></tr> <tr><td>8</td><td>Null</td></tr> <tr><td>9</td><td>Null</td></tr> <tr><td>10</td><td>Email</td></tr> <tr><td>11</td><td>Tipo certificado 5</td></tr> </table> <p>Si el tipo de certificado es de sede:</p> <table border="1"> <tr><td>4</td><td>EntityNIF</td></tr> <tr><td>5</td><td>EntityName</td></tr> <tr><td>6</td><td>Null</td></tr> <tr><td>7</td><td>Null</td></tr> <tr><td>8</td><td>Null</td></tr> <tr><td>9</td><td>Null</td></tr> <tr><td>10</td><td>Email</td></tr> <tr><td>11</td><td>Tipo certificado 3</td></tr> </table> <p>Si el tipo de certificado es de sello:</p> <table border="1"> <tr><td>4</td><td>EntityNIF</td></tr> <tr><td>5</td><td>EntityName</td></tr> <tr><td>6</td><td>Null</td></tr> <tr><td>7</td><td>Null</td></tr> <tr><td>8</td><td>Null</td></tr> <tr><td>9</td><td>Null</td></tr> <tr><td>10</td><td>Email</td></tr> <tr><td>11</td><td>Tipo certificado 4</td></tr> </table> <p>Si el tipo de certificado es de aplicacion:</p> <table border="1"> <tr><td>4</td><td>Null</td></tr> <tr><td>5</td><td>CommonName</td></tr> <tr><td>6</td><td>Null</td></tr> <tr><td>7</td><td>Null</td></tr> <tr><td>8</td><td>Null</td></tr> <tr><td>9</td><td>Null</td></tr> <tr><td>10</td><td>Email</td></tr> <tr><td>11</td><td>Tipo certificado 2</td></tr> </table> <p>Si el tipo de certificado es de entidad:</p> <table border="1"> <tr><td>4</td><td>Null</td></tr> </table>	6	Primer apellido	7	Segundo apellido	8	Null	9	Null	10	Email	11	Tipo certificado 5	4	EntityNIF	5	EntityName	6	Null	7	Null	8	Null	9	Null	10	Email	11	Tipo certificado 3	4	EntityNIF	5	EntityName	6	Null	7	Null	8	Null	9	Null	10	Email	11	Tipo certificado 4	4	Null	5	CommonName	6	Null	7	Null	8	Null	9	Null	10	Email	11	Tipo certificado 2	4	Null
6	Primer apellido																																																																
7	Segundo apellido																																																																
8	Null																																																																
9	Null																																																																
10	Email																																																																
11	Tipo certificado 5																																																																
4	EntityNIF																																																																
5	EntityName																																																																
6	Null																																																																
7	Null																																																																
8	Null																																																																
9	Null																																																																
10	Email																																																																
11	Tipo certificado 3																																																																
4	EntityNIF																																																																
5	EntityName																																																																
6	Null																																																																
7	Null																																																																
8	Null																																																																
9	Null																																																																
10	Email																																																																
11	Tipo certificado 4																																																																
4	Null																																																																
5	CommonName																																																																
6	Null																																																																
7	Null																																																																
8	Null																																																																
9	Null																																																																
10	Email																																																																
11	Tipo certificado 2																																																																
4	Null																																																																

				5	CommonName	
				6	Null	
				7	Null	
				8	CIF	
				9	Razon social	
				10	Email	
				11	Tipo certificado 1	
Seguridad						
Mecanismo de seguridad WS-Security						
Xml de Entrada						
<pre><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></pre>						
XML de Salida						
<pre><xsd:element name="obtenerDatosCertificadoResponse"> <xsd:complexType> <xsd:sequence> <xsd:element minOccurs="1" name="serialNumber" type="xsd:string"/> <xsd:element minOccurs="1" name="issuerDN" type="xsd:string"/> <xsd:element minOccurs="1" name="subjectDN" type="xsd:string"/> </xsd:sequence> </xsd:complexType> </xsd:element></pre>						

3.2.2.7 Validar un certificado y obtener datos

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

Servicio			
Object[] validarCertificadoYObtenerDatos(final byte[] certificado);			
Descripción			
Este método permite validar un certificado, su caducidad y si está revocado o no y además retorna los datos asociados al mismo.			
Parámetros de Entrada			
	Tipo	Descripción	
	certificado	byte[]	Array de bytes que contiene el certificado en base 64 a validar.

Respuesta			
		Tipo	Descripción
	Object[]	Object[]	Retornará la información extraíble del certificado en el caso de que sea válido.
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre> <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> </pre>			
XML de Salida			
<pre> <xsd:element name="validarCertificadoYObtenerDatosResponse"> <xsd:complexType> <xsd:sequence> <xsd:element minOccurs="1" name="response" type="xsd:int"/> <xsd:element minOccurs="1" name="serialNumber" type="xsd:string"/> <xsd:element minOccurs="1" name="issuerDN" type="xsd:string"/> <xsd:element minOccurs="1" name="subjectDN" type="xsd:string"/> <xsd:element minOccurs="1" name="nombre" type="xsd:string"/> <xsd:element minOccurs="1" name="apellido1" type="xsd:string"/> <xsd:element minOccurs="1" name="apellido2" type="xsd:string"/> <xsd:element minOccurs="1" name="nif" type="xsd:string"/> <xsd:element minOccurs="1" name="cif" type="xsd:string"/> <xsd:element minOccurs="1" name="razon_social" type="xsd:string"/> <xsd:element minOccurs="1" name="habilitado" type="xsd:string"/> <xsd:element minOccurs="1" name="representante" type="xsd:string"/> <xsd:element minOccurs="1" name="oid" type="xsd:string"/> <xsd:element minOccurs="1" name="email" type="xsd:string"/> <xsd:element minOccurs="1" name="tipoCertificado" type="xsd:string"/> </xsd:sequence> </xsd:complexType> </xsd:element> </pre>			

3.2.2.8 Validar una firma y obtener sus datos

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.

Servicio
Object[] validarFirmaYObtenerDatos(byte[] firma, byte[] documentoOriginal, final String firmaFormato , String formatoSubtipo)
Descripción
Este método permite validar una firma con respecto a un formato de firma en concreto y retornar la

información de su certificado.

Parámetros de Entrada

	Tipo	Descripción
firma	byte[]	Array de bytes en base 64 que contiene la firma a validar.
documentoOriginal	byte[]	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.
firmaFormato	String	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.
formatoSubtipo	String	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.

Respuesta

	Tipo	Descripción
Object[]	Object[]	Retornará la información extraíble del certificado en el caso de que sea válido.

Seguridad

Mecanismo de seguridad WS-Security

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>TF03</v2:firmaFormato>
      <!--Optional:-->
      <v2:formatoSubtipo></v2:formatoSubtipo>
    </v2:validarFirmaYObtenerDatosRequest>
  </soapenv:Body>
</soapenv:Envelope>
```

XML de Salida

```
<xsd:element name="validarFirmaYObtenerDatosResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element minOccurs="1" name="valida" type="xsd:boolean"/>
      <xsd:element minOccurs="1" name="serialNumber" type="xsd:string"/>
      <xsd:element minOccurs="1" name="issuerDN" type="xsd:string"/>
      <xsd:element minOccurs="1" name="subjectDN" type="xsd:string"/>
      <xsd:element minOccurs="1" name="nombre" type="xsd:string"/>
      <xsd:element minOccurs="1" name="apellido1" type="xsd:string"/>
      <xsd:element minOccurs="1" name="apellido2" type="xsd:string"/>
      <xsd:element minOccurs="1" name="nif" type="xsd:string"/>
      <xsd:element minOccurs="1" name="cif" type="xsd:string"/>
      <xsd:element minOccurs="1" name="razon social" type="xsd:string"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

```

    <xsd:element minOccurs="1" name="habilitado" type="xsd:string"/>
    <xsd:element minOccurs="1" name="representante" type="xsd:string"/>
    <xsd:element minOccurs="1" name="oid" type="xsd:string"/>
    <xsd:element minOccurs="1" name="email" type="xsd:string"/>
    <xsd:element minOccurs="1" name="tipoCertificado" type="xsd:string"/>
  </xsd:sequence>
</xsd:complexType>
</xsd:element>

```

3.2.2.9 Validar una firma y obtener sus datos SMIME

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

Servicio			
Object[] validarFirmaSMIMEYObtenerDatos (final byte[] tokenValidacion, final byte[] docAValidar)			
Descripción			
Este método permite validar una firma SMIME con respecto a un token de validación y el documento original.			
Parámetros de Entrada			
		Tipo	Descripción
	tokenValidacion	byte[]	Array de bytes en base 64 que contiene la firma a validar.
	docAValidar	byte[]	Array de bytes en base 64 que contiene el documento a validar contra su firma.
Respuesta			
		Tipo	Descripción
	Object[]	Object[]	Retornará la información extraíble del certificado en el caso de que sea válido.
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre> <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:validarFirmaSMIMEYObtenerDatosRequest> <v2:tokenValidacion>cid:1049381270527</v2:tokenValidacion> <v2:docAValidar>cid:1178495771075</v2:docAValidar> </v2:validarFirmaSMIMEYObtenerDatosRequest> </soapenv:Body> </soapenv:Envelope> </pre>			
XML de Salida			
<pre> <xsd:element name="validarFirmaSMIMEYObtenerDatosResponse"> <xsd:complexType> </pre>			

```
<xsd:sequence>
  <xsd:element minOccurs="1" name="valida" type="xsd:boolean"/>
  <xsd:element minOccurs="1" name="serialNumber" type="xsd:string"/>
  <xsd:element minOccurs="1" name="issuerDN" type="xsd:string"/>
  <xsd:element minOccurs="1" name="subjectDN" type="xsd:string"/>
  <xsd:element minOccurs="1" name="nombre" type="xsd:string"/>
  <xsd:element minOccurs="1" name="apellido1" type="xsd:string"/>
  <xsd:element minOccurs="1" name="apellido2" type="xsd:string"/>
  <xsd:element minOccurs="1" name="nif" type="xsd:string"/>
  <xsd:element minOccurs="1" name="cif" type="xsd:string"/>
  <xsd:element minOccurs="1" name="razon_social" type="xsd:string"/>
  <xsd:element minOccurs="1" name="habilitado" type="xsd:string"/>
  <xsd:element minOccurs="1" name="representante" type="xsd:string"/>
  <xsd:element minOccurs="1" name="oid" type="xsd:string"/>
  <xsd:element minOccurs="1" name="email" type="xsd:string"/>
  <xsd:element minOccurs="1" name="tipoCertificado" type="xsd:string"/>
</xsd:sequence>
</xsd:complexType>
</xsd:element>
```

3.2.2.10 CoFirmar con el certificado de una aplicación

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:

Servicio			
byte[]coFirmaConCertificado(final String idSession, final String idCertificado, final byte[] firma, final byte[] documento, final String firmaFormato, final String formatoSubtipo)			
Descripción			
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.			
Parámetros de Entrada			
		Tipo	Descripción
	idSession	String	Identificador univoco de aplicación.
	idCertificado	String	Identificador de Certificado a utilizar para el firmado, que identifica unívocamente al certificado aportado y almacenado en SAFE.
	firma	byte[]	Firma en base 64 previa.
	documento	byte[]	Array de bytes en base 64 que contiene la “cadena” a firmar en el formato indicado en el parámetro firmaFormato
	firmaFormato	String	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.
	subtipoFirma	String	Cadena que contiene el subtipo (si se quiere indicar) a utilizar con el formato ENI indicado.
Respuesta			
		Tipo	Descripción
	byte[]	byte[]	Array de bytes que contiene la firma realizada. El contenido de este array es un XML de firma creado por el API del conector.
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre><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></pre>			

```

    </v2:coFirmaConCertificadoRequest>
  </soapenv:Body>
</soapenv:Envelope>

```

XML de Salida

```

<xsd:element name="coFirmaConCertificadoResponse">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="response" type="xsd:base64Binary"
minOccurs="1"/></xsd:element>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

```

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 código identificador del mismo, así como identificador de sesión a usar para las peticiones. Con esto se permitirá que coexistan más de un certificado por aplicación, ya que cada uno de ellos tendrá un identificador unívoco. El modo de proporcionar esta información al equipo de SAFE se explica con más detalle en el anexo (Firma delegada en SAFE).

3.2.2.11 ContraFirmar con el certificado de una aplicación

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:

Servicio			
byte[] contraFirmaConCertificado(final String idSession, final String idCertificado, final byte[] firma, final String firmaFormato, final String formatoSubtipo, final boolean todo, final byte[] certificadoAContrafirmar)			
Descripción			
Este método permite realizar una 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.			
Parámetros de Entrada			
		Tipo	Descripción
	idSession	String	Identificador unívoco de aplicación.
	idCertificado	String	Identificador de Certificado a utilizar para el firmado, que identifica unívocamente al certificado aportado y almacenado en SAFE.
	firma	byte[]	Firma en base 64 previa.
	firmaFormato	String	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.
	subtipoFirma	String	Cadena que contiene el subtipo (si se quiere indicar) a utilizar con el formato ENI indicado.

	todo	Boolean	Si todo= false y certificadoAContraFirmar==null → CONTRAFIRMAMOS la ultima firma Si todo= false y certificadoAContraFirmar!=null → CONTRAFIRMAMOS el certificado que nos indican
	certificadoAContrafirmar	byte[]	Certificado usado para contrafirmar
Respuesta			
		Tipo	Descripción
	byte[]	byte[]	Array de bytes que contiene la firma realizada. El contenido de este array es un XML de firma creado por el API del conector.
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre><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></pre>			
XML de Salida			
<pre><xsd:element name="contraFirmaConCertificadoResponse"> <xsd:complexType> <xsd:sequence> <xsd:element name="response" type="xsd:base64Binary" minOccurs="1"></xsd:element> </xsd:sequence> </xsd:complexType> </xsd:element></pre>			

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 código 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).

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

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.

Servicio			
Object[] validarTodasFirmaYObtenerFirmantes(final byte[] firma, final byte[] documentoOriginal, final String firmaFormato, final String formatoSubtipo)			
Descripción			
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.			
Parámetros de Entrada			
		Tipo	Descripción
	firma	byte[]	Array de bytes en base 64 que contiene la firma a validar.
	documentoOriginal	byte[]	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.
	firmaFormato	String	Cadena que contiene el subtipo (si se quiere indicar) a utilizar con el formato ENI indicado.
	formatoSubtipo	String	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.
Respuesta			
		Tipo	Descripción
	Object[]	Object[]	Retornará la información extraíble de los certificados en el caso de que sean válidos.
Seguridad			
Mecanismo de seguridad WS-Security			
Xml de Entrada			
<pre> <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> </pre>			
XML de Salida			
<pre> <xsd:element name="validarTodasFirmaYObtenerFirmantesResponse"> <xsd:complexType> </pre>			

```

    <xsd:sequence>
      <xsd:element name="valida" type="xsd:boolean" minOccurs="1"></xsd:element>
      <xsd:element name="listaFirmantes" type="tns:firmantes" minOccurs="1"
maxOccurs="unbounded"></xsd:element>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>

<xsd:complexType name="firmantes">
  <xsd:sequence>
    <xsd:element name="firmante" type="tns:datos" minOccurs="1"
maxOccurs="unbounded"></xsd:element>
  </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="datos">
  <xsd:sequence>
    <xsd:element name="serialNumber" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="issuerDN" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="subjectDN" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="nombre" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="apellido1" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="apellido2" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="nif" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="cif" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="razon_social" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="habilitado" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="representante" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="oid" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="email" type="xsd:string" minOccurs="1"></xsd:element>
    <xsd:element name="tipoCertificado" type="xsd:string" minOccurs="1"></xsd:element>
  </xsd:sequence>
</xsd:complexType>

```

3.2.3 Mensajes de error y excepciones

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

3.2.3.1 Errores en servicios web

1. Cuando un servicio de búsqueda no encuentra información asociada a la búsqueda planteada se retorna una respuesta vacía y no una excepción.
2. Cuando un servicio retorna un error de ARANGI, retorna la misma codificación que retorna ARANGI, como es el caso del **servicio de validación de certificados**:

ValidationResult. <i>RESULT_CERTIFICATE_CANNOT_BE_VALIDATED</i>	Resultado de la validación: El certificado no puede ser validado.
ValidationResult.	Resultado de la validación: La cadena de confianza del

<i>RESULT_CERTIFICATE_CHAIN_VALIDATION_INVALID</i>	certificado no es válida.
ValidationResult. <i>RESULT_CERTIFICATE_NOT_ACTIVE</i>	Resultado de la validación: El certificado no ha comenzado su periodo de validez o ya ha expirado.
ValidationResult. <i>RESULT_CERTIFICATE_NOT_BELONGS_TRUSTED_CAS</i>	Resultado de la validación: El certificado no pertenece a la lista de CAs de confianza.
ValidationResult. <i>RESULT_CERTIFICATE_REVOKED</i>	Resultado de la validación: El certificado está revocado.
ValidationResult. <i>RESULT_CERTIFICATE_UNKNOWN</i>	Resultado de la validación: El certificado es desconocido.
ValidationResult. <i>RESULT_INVALID</i>	Resultado de la validación: El resultado no es válido.
ValidationResult. <i>RESULT_REFERENCE_DIGEST_NOT_MATCH_DATA</i>	Resultado de la validación: Alguno de los hash de las referencias que luego se firman no se corresponde con la parte del XML a que hacen referencia.
ValidationResult. <i>RESULT_SIGNATURE_NOT_MATCH_DATA</i>	Resultado de la validación: Los datos no se corresponden con el hash de la firma.
ValidationResult. <i>RESULT_VALID</i>	Resultado de la validación: El certificado es válido.
Cualquier otro valor	Resultado de la validación: Indefinido.

3.3 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.

3.4 Seguridad del Servicio Web

La seguridad de los servicios web se llevará a cabo mediante el mecanismo de seguridad WS-Security. La invocación de los servicios web se realizará mediante certificado (X509 Certificate Binary Certificate Token).

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 ANEXOS

4.1 WSDL de los subsistemas

A continuación incluimos los WSDL de cada uno de los servicios publicados, dividido en subsistemas:

4.1.1 WSDL de Autenticación

```
<?xml version="1.0" encoding="UTF-8"?><wsdl:definitions
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
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/definitions/v2_00"
targetNamespace="http://dgm.gva.es/ayf/war/definitions/v2_00">
  <wsdl:types xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://dgm.gva.es/ayf/war/schemas/v2_00" attributeFormDefault="unqualified"
elementFormDefault="qualified"
targetNamespace="http://dgm.gva.es/ayf/war/schemas/v2_00"><xsd:element
name="autenticaConFirmaWSRequest" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="firma" type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="codigoEntidad"
type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="autenticaConFirmaWSResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="token" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="getInformacionWSRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="token" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="getInformacionWSResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="serialNumber" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="issuerDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="subjectDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nombre" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="apellido1" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="apellido2" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="cif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="razon_social" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="habilitado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="representante"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="oid"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="tipo_aut"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="idHDFI"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="email"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="tipoCertificado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="codEntidad" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="autenticaUsuarioWSRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="usuario" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="password" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="autenticaUsuarioWSResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
```

```

xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="token" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
d:element name="autenticaUsuarioLDAPWSRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="usuarioLDAP" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="pwdLDAP" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
d:element name="autenticaUsuarioLDAPWSResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="token" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element></x
sd:schema>
</wsdl:types>
<wsdl:message name="autenticaUsuarioWSResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:autenticaUsuarioWSResponse" name="autenticaUsuarioWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="getInformacionWSResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:getInformacionWSResponse" name="getInformacionWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="autenticaConFirmaWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:autenticaConFirmaWSResponse" name="autenticaConFirmaWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="autenticaConFirmaWSRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:autenticaConFirmaWSRequest" name="autenticaConFirmaWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="getInformacionWSRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:getInformacionWSRequest" name="getInformacionWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="autenticaUsuarioWSRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:autenticaUsuarioWSRequest" name="autenticaUsuarioWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="autenticaUsuarioLDAPWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:autenticaUsuarioLDAPWSRequest" name="autenticaUsuarioLDAPWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="autenticaUsuarioLDAPWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:autenticaUsuarioLDAPWSResponse"
name="autenticaUsuarioLDAPWSResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:portType name="AutenticacionArangiPortType"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:operation name="autenticaUsuarioWS" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:input message="tns:autenticaUsuarioWSRequest" name="autenticaUsuarioWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:input>
<wsdl:output message="tns:autenticaUsuarioWSResponse" name="autenticaUsuarioWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:output>
</wsdl:operation>
<wsdl:operation name="getInformacionWS" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:input message="tns:getInformacionWSRequest" name="getInformacionWSRequest"
    
```

```

xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:getInformacionWSResponse" name="getInformacionWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="autenticaConFirmaWS" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:autenticaConFirmaWSRequest" name="autenticaConFirmaWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:autenticaConFirmaWSResponse" name="autenticaConFirmaWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="autenticaUsuarioLDAPWS" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:autenticaUsuarioLDAPWSRequest"
name="autenticaUsuarioLDAPWSRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:autenticaUsuarioLDAPWSResponse"
name="autenticaUsuarioLDAPWSResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
</wsdl:portType>
<wsdl:binding name="AutenticacionArangiPortTypeSoap11" type="tns:AutenticacionArangiPortType"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
  <wsdl:operation name="autenticaUsuarioWS" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="autenticaUsuarioWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
      </wsdl:input>
      <wsdl:output name="autenticaUsuarioWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
        <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
        </wsdl:output>
      </wsdl:operation>
      <wsdl:operation name="getInformacionWS" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
        <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
        <wsdl:input name="getInformacionWSRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
          <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
          </wsdl:input>
          <wsdl:output name="getInformacionWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
            <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
            </wsdl:output>
          </wsdl:operation>
          <wsdl:operation name="autenticaConFirmaWS" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
            <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
            <wsdl:input name="autenticaConFirmaWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
              <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
              </wsdl:input>
              <wsdl:output name="autenticaConFirmaWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
                <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
                </wsdl:output>
              </wsdl:operation>
              <wsdl:operation name="autenticaUsuarioLDAPWS" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
                <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
                <wsdl:input name="autenticaUsuarioLDAPWSRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
                  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
                  </wsdl:input>
                  <wsdl:output name="autenticaUsuarioLDAPWSResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
                    <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
                    </wsdl:output>
                  </wsdl:operation>

```



```
</wsdl:binding>
<wsdl:service name="AutenticacionArangiService" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:port binding="tns:AutenticacionArangiPortTypeSoap11"
name="AutenticacionArangiPortTypeSoap11" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:address
location="http://safe.gva.es:80/SAFEear/AutenticacionARANGIWAr/AutenticacionArangiService/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:port>
  </wsdl:service>
</wsdl:definitions>
```

4.1.2 WSDL de Firma

```
<?xml version="1.0" encoding="UTF-8"?><wsdl:definitions
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
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/definitions/v2_00"
targetNamespace="http://dgm.gva.es/ayf/war/definitions/v2_00">
  <wsdl:types xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:tns="http://dgm.gva.es/ayf/war/schemas/v2_00" attributeFormDefault="unqualified"
elementFormDefault="qualified"
targetNamespace="http://dgm.gva.es/ayf/war/schemas/v2_00"><xsd:complexType name="datos"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="serialNumber" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="issuerDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="subjectDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nombre" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="apellido1" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="apellido2" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="cif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="razon social" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="habilitado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="representante"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="oid"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="email"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="tipoCertificado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType><xsd:complexType
name="firmantes" xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element maxOccurs="unbounded" name="firmante"
type="tns:datos"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType><xsd:element
name="firmarCertificadoServerRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="documento"
type="xsd:base64Binary" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="firmaFormato" type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
minOccurs="0" name="formatoSubtipo" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="contraFirmaConCertificadoResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="response"
type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="contraFirmaConCertificadoRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="idSession" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="idCertificado"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="firma"
type="xsd:base64Binary" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element></xsd:definitions>
```

```
name="firmaFormato" type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="formatoSubtipo" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="todo" type="xsd:boolean"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="certificadoAContraFirmar"
type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="coFirmaConCertificadoResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="response"
type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="coFirmaConCertificadoRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="idSession" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="idCertificado"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="firma"
type="xsd:base64Binary" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="documento" type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="firmaFormato" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="formatoSubtipo"
type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="firmarCertificadoServerResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="response"
type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="firmarConCertificadoRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="idSession" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="idCertificado"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="documento"
type="xsd:base64Binary" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="firmaFormato" type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="formatoSubtipo" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="firmarConCertificadoResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="response"
type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="obtenerDatosCertificadoRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="certificado"
type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="obtenerDatosCertificadoResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="serialNumber" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="issuerDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="subjectDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="validarCertificadoResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="response" type="xsd:int"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="validarCertificadoRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="certificado"
type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
```



```
d:element name="validarCertificadoYObtenerDatosRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="certificado"
type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="validarCertificadoYObtenerDatosResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="response" type="xsd:int"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="serialNumber" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="issuerDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="subjectDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nombre" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="apellido1" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="apellido2" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="cif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="razon_social" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="habilitado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="representante"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="oid"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="email"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="tipoCertificado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="validarFirmaRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="firma" type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="documentoOriginal"
type="xsd:base64Binary" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="firmaFormato" type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
minOccurs="0" name="formatoSubtipo" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="validarFirmaResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="valida" type="xsd:boolean"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="validarFirmaSMIMERequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="tokenValidacion"
type="xsd:base64Binary" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="docAValidar" type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="validarFirmaSMIMEResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="valida" type="xsd:boolean"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="validarFirmaYObtenerDatosRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="firma" type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="documentoOriginal"
type="xsd:base64Binary" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="firmaFormato" type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
minOccurs="0" name="formatoSubtipo" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:element name="validarFirmaYObtenerDatosResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="valida" type="xsd:boolean"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="serialNumber" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="issuerDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="subjectDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nombre" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="apellido1" type="xsd:string"
```

```
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="apellido2" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="cif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="razon_social" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="habilitado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="representante"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="oid"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="email"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="tipoCertificado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="validarTodasFirmaYObtenerFirmantesRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="firma" type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="documentoOriginal"
type="xsd:base64Binary" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="firmaFormato" type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
minOccurs="0" name="formatoSubtipo" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="validarTodasFirmaYObtenerFirmantesResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="valida" type="xsd:boolean"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element maxOccurs="unbounded"
name="listaFirmantes" type="tns:firmitantes"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="validarFirmaSMIMEYObtenerDatosRequest"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="tokenValidacion"
type="xsd:base64Binary" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="docAValidar" type="xsd:base64Binary"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element><xsd:
element name="validarFirmaSMIMEYObtenerDatosResponse"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:complexType
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:sequence
xmlns:xsd="http://www.w3.org/2001/XMLSchema"><xsd:element name="valida" type="xsd:boolean"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="serialNumber" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="issuerDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="subjectDN" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nombre" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="apellido1" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="apellido2" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="nif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="cif" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="razon_social" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="habilitado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="representante"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="oid"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element name="email"
type="xsd:string" xmlns:xsd="http://www.w3.org/2001/XMLSchema"/><xsd:element
name="tipoCertificado" type="xsd:string"
xmlns:xsd="http://www.w3.org/2001/XMLSchema"/></xsd:sequence></xsd:complexType></xsd:element></xsd:
schema>
</wsdl:types>
<wsdl:message name="validarFirmaSMIMEYObtenerDatosRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:validarFirmaSMIMEYObtenerDatosRequest"
name="validarFirmaSMIMEYObtenerDatosRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="firmarConCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:firmarConCertificadoResponse" name="firmarConCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="contraFirmaConCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
```

```
<wsdl:part element="sch:contraFirmaConCertificadoResponse"
name="contraFirmaConCertificadoResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="validarCertificadoResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:validarCertificadoResponse" name="validarCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="validarFirmaYObtenerDatosRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:validarFirmaYObtenerDatosRequest"
name="validarFirmaYObtenerDatosRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="contraFirmaConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:contraFirmaConCertificadoRequest"
name="contraFirmaConCertificadoRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="validarFirmaSMIMEResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:validarFirmaSMIMEResponse" name="validarFirmaSMIMEResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="obtenerDatosCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:obtenerDatosCertificadoRequest"
name="obtenerDatosCertificadoRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="validarFirmaYObtenerDatosResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:validarFirmaYObtenerDatosResponse"
name="validarFirmaYObtenerDatosResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="validarFirmaRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:validarFirmaRequest" name="validarFirmaRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="firmarConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:firmarConCertificadoRequest" name="firmarConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="validarFirmaSMIMERequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:validarFirmaSMIMERequest" name="validarFirmaSMIMERequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="obtenerDatosCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:obtenerDatosCertificadoResponse"
name="obtenerDatosCertificadoResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="validarFirmaSMIMEYObtenerDatosResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:validarFirmaSMIMEYObtenerDatosResponse"
name="validarFirmaSMIMEYObtenerDatosResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
</wsdl:part>
</wsdl:message>
<wsdl:message name="coFirmaConCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<wsdl:part element="sch:coFirmaConCertificadoResponse" name="coFirmaConCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
```

```

    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="validarCertificadoRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:part element="sch:validarCertificadoRequest" name="validarCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="validarFirmaResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:part element="sch:validarFirmaResponse" name="validarFirmaResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="validarCertificadoYObtenerDatosRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:part element="sch:validarCertificadoYObtenerDatosRequest"
name="validarCertificadoYObtenerDatosRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="coFirmaConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:part element="sch:coFirmaConCertificadoRequest" name="coFirmaConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="validarTodasFirmaYObtenerFirmantesRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:part element="sch:validarTodasFirmaYObtenerFirmantesRequest"
name="validarTodasFirmaYObtenerFirmantesRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="validarCertificadoYObtenerDatosResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:part element="sch:validarCertificadoYObtenerDatosResponse"
name="validarCertificadoYObtenerDatosResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="firmarCertificadoServerResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:part element="sch:firmarCertificadoServerResponse"
name="firmarCertificadoServerResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="firmarCertificadoServerRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:part element="sch:firmarCertificadoServerRequest"
name="firmarCertificadoServerRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    </wsdl:part>
  </wsdl:message>
  <wsdl:message name="validarTodasFirmaYObtenerFirmantesResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:part element="sch:validarTodasFirmaYObtenerFirmantesResponse"
name="validarTodasFirmaYObtenerFirmantesResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    </wsdl:part>
  </wsdl:message>
  <wsdl:portType name="FirmaArangiPortType" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <wsdl:operation name="validarFirmaSMIMEYObtenerDatos"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <wsdl:input message="tns:validarFirmaSMIMEYObtenerDatosRequest"
name="validarFirmaSMIMEYObtenerDatosRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      </wsdl:input>
      <wsdl:output message="tns:validarFirmaSMIMEYObtenerDatosResponse"
name="validarFirmaSMIMEYObtenerDatosResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      </wsdl:output>
    </wsdl:operation>
    <wsdl:operation name="firmarConCertificado" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <wsdl:input message="tns:firmarConCertificadoRequest" name="firmarConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      </wsdl:input>
      <wsdl:output message="tns:firmarConCertificadoResponse"
name="firmarConCertificadoResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">

```

```

</wsdl:output>
</wsdl:operation>
<wsdl:operation name="contraFirmaConCertificado"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:contraFirmaConCertificadoRequest"
name="contraFirmaConCertificadoRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:contraFirmaConCertificadoResponse"
name="contraFirmaConCertificadoResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="validarCertificado" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:validarCertificadoRequest" name="validarCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:validarCertificadoResponse" name="validarCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="validarFirmaYObtenerDatos"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:validarFirmaYObtenerDatosRequest"
name="validarFirmaYObtenerDatosRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:validarFirmaYObtenerDatosResponse"
name="validarFirmaYObtenerDatosResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="validarFirmaSMIME" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:validarFirmaSMIMERequest" name="validarFirmaSMIMERequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:validarFirmaSMIMEResponse" name="validarFirmaSMIMEResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="obtenerDatosCertificado"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:obtenerDatosCertificadoRequest"
name="obtenerDatosCertificadoRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:obtenerDatosCertificadoResponse"
name="obtenerDatosCertificadoResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="validarFirma" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:validarFirmaRequest" name="validarFirmaRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:validarFirmaResponse" name="validarFirmaResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="coFirmaConCertificado" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:coFirmaConCertificadoRequest" name="coFirmaConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:coFirmaConCertificadoResponse"
name="coFirmaConCertificadoResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="validarCertificadoYObtenerDatos"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:validarCertificadoYObtenerDatosRequest"
name="validarCertificadoYObtenerDatosRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:validarCertificadoYObtenerDatosResponse"
name="validarCertificadoYObtenerDatosResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>

```



```
<wsdl:operation name="validarTodasFirmaYObtenerFirmantes"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:validarTodasFirmaYObtenerFirmantesRequest"
name="validarTodasFirmaYObtenerFirmantesRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:validarTodasFirmaYObtenerFirmantesResponse"
name="validarTodasFirmaYObtenerFirmantesResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
<wsdl:operation name="firmarCertificadoServer"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:input message="tns:firmarCertificadoServerRequest"
name="firmarCertificadoServerRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:input>
  <wsdl:output message="tns:firmarCertificadoServerResponse"
name="firmarCertificadoServerResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  </wsdl:output>
</wsdl:operation>
</wsdl:portType>
<wsdl:binding name="FirmaArangiPortTypeSoap11" type="tns:FirmaArangiPortType"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"
xmlns:soap="http://schemas.xmlsoap.org/soap/">
  <wsdl:operation name="validarFirmaSMIMEYObtenerDatos"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="validarFirmaSMIMEYObtenerDatosRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
      </wsdl:input>
    <wsdl:output name="validarFirmaSMIMEYObtenerDatosResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
      </wsdl:output>
    </wsdl:operation>
  <wsdl:operation name="firmarConCertificado" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="firmarConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
      </wsdl:input>
    <wsdl:output name="firmarConCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
      </wsdl:output>
    </wsdl:operation>
  <wsdl:operation name="contraFirmaConCertificado"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="contraFirmaConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
      </wsdl:input>
    <wsdl:output name="contraFirmaConCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
      </wsdl:output>
    </wsdl:operation>
  <wsdl:operation name="validarCertificado" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="validarCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
      </wsdl:input>
    <wsdl:output name="validarCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
      </wsdl:output>
    </wsdl:operation>
  <wsdl:operation name="validarFirmaYObtenerDatos"
```

```

xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="validarFirmaYObtenerDatosRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:input>
    <wsdl:output name="validarFirmaYObtenerDatosResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="validarFirmaSMIME" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="validarFirmaSMIMERequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:input>
    <wsdl:output name="validarFirmaSMIMEResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="obtenerDatosCertificado"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="obtenerDatosCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:input>
    <wsdl:output name="obtenerDatosCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="validarFirma" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="validarFirmaRequest" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:input>
    <wsdl:output name="validarFirmaResponse" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
      <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="coFirmaConCertificado" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="coFirmaConCertificadoRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:input>
    <wsdl:output name="coFirmaConCertificadoResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="validarCertificadoYObtenerDatos"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="validarCertificadoYObtenerDatosRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:input>
    <wsdl:output name="validarCertificadoYObtenerDatosResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="validarTodasFirmaYObtenerFirmantes"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/">
    <wsdl:input name="validarTodasFirmaYObtenerFirmantesRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">

```

```
<soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" />
</wsdl:input>
<wsdl:output name="validarTodasFirmaYObtenerFirmantesResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" />
</wsdl:output>
</wsdl:operation>
<wsdl:operation name="firmarCertificadoServer"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <soap:operation soapAction="" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" />
  <wsdl:input name="firmarCertificadoServerRequest"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" />
  </wsdl:input>
  <wsdl:output name="firmarCertificadoServerResponse"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:body use="literal" xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" />
  </wsdl:output>
</wsdl:operation>
</wsdl:binding>
<wsdl:service name="FirmaArangiService" xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
  <wsdl:port binding="tns:FirmaArangiPortTypeSoap11" name="FirmaArangiPortTypeSoap11"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
    <soap:address location="http://safe.gva.es:80/SAFEear/FirmaARANGIWAr/FirmaArangiService/"
xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/" />
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

4.2 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://preinterint.gva.es/eSirca_Bus/ins/Proxy/SAFE/FirmaArangi_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
//*****
```


4.3 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 así como el identificador de aplicación que desea utilizar el mismo. Si esta aplicación no tuviera permisos para utilizarlo, no se podrá realizar la firma. Así mismo 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 bdd y esta información está 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 ningún 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 política de acceso definida por la Plataforma de interoperabilidad o PAI para este servicio.

El uso de este certificado para firma delegada se realizará únicamente a través del servicio `firmarConCertificado` (0

Firmar con el certificado de una aplicación).

Un ejemplo de uso es:

```
//URL donde está publicado el servicio en el bus
String endpoint =
"https://preinterint.gva.es/eSirca_Bus/ins/Proxy/SAFE/FirmaArangi_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
//*****
```