



**Gobierno  
de Canarias**

Consejería de Presidencia,  
Justicia e Igualdad



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

Interoperabilidad de los servicios telemáticos de la  
Administración Pública de la CAC

Página 1 de 69

**MARCO DE REFERENCIA PARA LA  
PLATAFORMA DE INTEROPERABILIDAD**

**VOLÚMEN IV: MANUAL DEL DESARROLLADOR**

**SERVICIO DE FIRMA ELECTRÓNICA Y SELLADO DE  
TIEMPO**

**Historial de revisiones en la siguiente página**

<b>Documento :</b>	Servicio de Firma Electrónica y Sellado de Tiempo – Manual del Desarrollador	
<b>Ubicación en eRoom:</b>		
<b>Preparado por</b>	<b>Revisado por</b>	<b>Aprobado por</b>
D. Gral. de Telecomunicaciones y Nuevas Tecnologías	D. Gral. de Telecomunicaciones y Nuevas Tecnologías	D. Gral. de Telecomunicaciones y Nuevas Tecnologías
<b>Fecha:</b> 20/10/2011	<b>Fecha:</b> 20/10/2011	<b>Fecha:</b> 20/10/2011



Rev.	Fecha	Descripción
0	12/12/2007	Versión Inicial
1	13/06/2008	Actualización del documento.
2	16/06/2008	Se añade el método getCertInfo en el lado del servidor. Se añaden los posibles códigos de retorno del método validateCert
3	04/08/2008	Corrección de una errata en el apartado 3.8
4	26/08/2008	Se incorporan dos nuevos CU: "Firmar Contenido" y "Validar Firma Contenido"
5	01/09/2008	Se incorpora un apartado con los cambios incorporados en la última versión
6	15/10/2008	Se actualiza el documento hasta la versión v20081024
7	03/02/2009	Se actualiza el documento hasta la versión v20090126
8	09/02/2009	Se incorpora apartado Error: No se encuentra la fuente de referencia para documentar configuración en Internet Explorer para componente cliente de firma
9	15/07/2009	Se actualiza el documento hasta la versión v20090707
10	01/09/2009	Se actualiza el documento hasta la versión v20090901
11	05/01/2010	Se añade el apartado 5.3 INFORMACIÓN EXTRAÍDA DE LOS CERTIFICADOS para detallar la información extraída de los certificados
12	23/03/2010	Se actualiza el documento hasta la versión v20100323
13	21/06/2010	Se actualiza el documento hasta la versión v20100621
14	17/09/2010	Se actualiza el documento hasta la versión v20100917 en el que se actualiza el componente WebSigner a la versión 5.6.0.4.
15	17/09/2010	Se realizan correcciones en el documento.
16	19/10/2010	Se actualiza el documento hasta la versión v20101019 en el que se actualiza el componente WebSigner a la versión 5.6.0.4.
17	05/11/2010	Se actualiza el documento hasta la versión v20101105 en el que se adapta a la nueva interfaz del SGRDE.
18	26/01/2011	Se actualiza el documento hasta la versión v20110126 en el que se actualiza el componente WebSigner a la versión 5.6.0.9 y se adapta el servicio para su consumo por parte de la plataforma Atlas.
19	28/01/2011	Se actualiza el apartado 5.3 Información Extraída de los Certificados.
20	12/05/2011	Se actualiza el documento hasta la versión v20110512 en el que se actualiza el componente WebSigner a la versión 5.7.1.1.



**Gobierno  
de Canarias**

Consejería de Presidencia,  
Justicia e Igualdad



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

Vol. IV Manual del desarrollador  
Servicio de Firma Electrónica y Sellado de Tiempo

Página 3 de 69

21	16/06/2011	Se introducen mejoras correctivas.
22	21/07/2011	Se actualiza el documento hasta la versión v20110721 en el que se actualiza el componente WebSigner a la versión 5.7.3.0 y el módulo de ASF a la 4.1.1.125
23	01/09/2011	Se introducen adaptaciones solicitadas por el Cabildo de Tenerife, y mejoras correctivas
24	20/10/2011	Se introducen mejoras correctivas asociadas a los resolvers de firma.

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 4 de 69

## ÍNDICE

<b><u>1 INTRODUCCIÓN.....</u></b>	<b><u>6</u></b>
1.1 CAMBIOS EN EL DOCUMENTO RESPECTO A VERSIONES ANTERIORES...	7
<b><u>2 VERSIÓN DEL SERVICIO.....</u></b>	<b><u>11</u></b>
<b><u>3 CASOS DE USO.....</u></b>	<b><u>12</u></b>
3.1 CU-FST-01: FIRMA XML SIGNATURE.....	16
3.2 CU-FST-02: OBTENER INFORMACIÓN DE UN CERTIFICADO.....	17
3.3 CU-FST-03: VALIDAR FIRMA XML SIGNATURE.....	18
3.4 CU-FST-04: FIRMA PKCS#7.....	20
3.5 CU-FST-05: VALIDAR FIRMA PKCS#7.....	21
3.6 CU-FST-20: FIRMA XML SIGNATURE SECUENCIAL.....	22
3.7 CU-FST-06: FIRMA XML SIGNATURE.....	23
3.8 CU-FST-07: VALIDAR UN CERTIFICADO.....	26
3.9 CU-FST-08: VALIDAR FIRMA XML SIGNATURE.....	29
3.10 CU-SFT-09: TIMESTAMP.....	31
3.11 CU-FST-10: FIRMA PKCS#7.....	34
3.12 CU-FST-11: VALIDAR FIRMA PKCS#7.....	36
3.13 CU-SFT-12: GETTIME.....	39
3.14 CU-SFT-13: GETVERSION.....	40
3.15 CU-SFT-14: OBTENER INFORMACIÓN DE UN CERTIFICADO.....	42
3.16 CU-FST-15: FIRMA CONTENIDO.....	44
3.17 CU-FST-16: VALIDAR FIRMA CONTENIDO.....	47
3.18 CU-FST-17: ANALIZAR TIMESTAMP.....	49
3.19 CU-SFT-18: TIMESTAMP DE FIRMA.....	52
3.20 CU-SFT-19: FIRMA SECUENCIAL.....	55
<b><u>4 CONTROL DE EXCEPCIONES .....</u></b>	<b><u>59</u></b>
4.1 SignatureServiceException.....	59
<b><u>5 INFORMACIÓN ADICIONAL DEL SERVICIO.....</u></b>	<b><u>60</u></b>

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 5 de 69

<a href="#">5.1 TIPOS DE DATOS.....</a>	<a href="#">60</a>
<a href="#">5.1.1 ValidateCertResult.....</a>	<a href="#">60</a>
<a href="#">5.2 FIRMAS MÚLTIPLES.....</a>	<a href="#">61</a>
<a href="#">5.2.1 Firma Múltiple Paralela.....</a>	<a href="#">61</a>
<a href="#">5.3 INFORMACIÓN EXTRAÍDA DE LOS CERTIFICADOS.....</a>	<a href="#">61</a>
<a href="#">5.3.1 Introducción.....</a>	<a href="#">61</a>
<a href="#">5.3.2 Tipos de certificados.....</a>	<a href="#">62</a>
<a href="#">5.3.3 Descripción de los campos extraídos del certificado.....</a>	<a href="#">64</a>
<a href="#">5.3.4 Información extraída de cada tipo de certificado.....</a>	<a href="#">65</a>
<a href="#">6 EJEMPLO DE INTEGRACIÓN.....</a>	<a href="#">69</a>
<a href="#">6.1 CONFIGURACIÓN.....</a>	<a href="#">69</a>

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 6 de 69

## 1 INTRODUCCIÓN

El servicio de firma electrónica y sellado de tiempo proporciona una serie de funcionalidades a los ciudadanos, a los backoffices y al resto de servicios integrados en PLATINO.

Estas funcionalidades principales son: la firma de documentos, la validación de un certificado, la validación de la firma de un documento, la autenticación y el sellado de tiempo (timestamp).

Para llevar a cabo cualquier interacción con el Servicio de Firma Electrónica y Sellado de Tiempo es imprescindible hacer uso de algún certificado electrónico, expedido por una autoridad certificadora reconocida, que identifique al ciudadano que está interactuando con la Administración.

El Servicio de Firma Digital y Sellado de Tiempo implementa el tipo de firma denominado "firma electrónica reconocida", y usará el formato de firma denominado XMLSignature, permitiendo además la posibilidad de realizar multifirma secuencial, es decir, incorporar firma electrónica a un documento firmado previamente, y multifirma paralela, pudiendo firmarse un documento por varias personas al mismo tiempo.

Todos los ciudadanos tienen la posibilidad de obtener un certificado de usuario, ya sea a través del DNI electrónico como solicitándolo a alguna autoridad certificadora.

### **Consola de Administración de Advanced Signature Framework**

Como se ha comentado previamente, este servicio funcionará como una fachada de la solución desarrollada por la empresa TB-Solutions con nombre "Advanced Signature Framework". Este aplicativo incluye una consola de administración a través de la que se deben llevar a cabo las tareas propias de configuración de los aspectos relacionados con la firma electrónica.

Entre estas tareas podemos destacar la administración de las Autoridades Certificadoras aceptadas por el módulo de firma, las diferentes listas de revocación de certificados electrónicos, los servidores de TimeStamp, los certificados permitidos para las diferentes aplicaciones, etc.

Toda esta información queda recogida en el documento elaborado por TB-Solutions con nombre "Manual de Usuario Consola de Administración.pdf".

 <p><b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad</p>	 <p><b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias</p>
<p>Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo</p>	<p>Página 7 de 69</p>

## 1.1 CAMBIOS EN EL DOCUMENTO RESPECTO A VERSIONES ANTERIORES

La actual versión del servicio **v20111020**, con respecto a la versión anterior v20110901, incorpora los siguientes cambios:

- Se introducen adaptaciones en los resolvers de firma.

La actual versión del servicio **v20110901**, con respecto a la versión anterior v20110721, incorpora los siguientes cambios:

- Se introducen adaptaciones solicitadas por el Cabildo de Tenerife
- Se incluyen mejoras correctivas.

La actual versión del servicio **v20110721**, con respecto a la versión anterior v20110616, incorpora los siguientes cambios:

- Se actualiza la versión del componente de firma en cliente Websigner a la versión 5.7.3.0.
- Se actualiza la versión del modulo de ASF a la versión 4.1.1.125

La actual versión del servicio **v20110616**, con respecto a la versión anterior v20100512, incorpora los siguientes cambios:

- Se introducen mejoras correctivas menores.

La actual versión del servicio **v20110512**, con respecto a la versión anterior v20110126, incorpora los siguientes cambios:

- Se actualiza la versión del componente de firma en cliente Websigner a la versión 5.7.1.1.

La actual versión del servicio **v20110126**, con respecto a la versión anterior v20101105, incorpora los siguientes cambios:

 <p><b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad</p>	 <p><b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias</p>
<p>Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo</p>	<p>Página 8 de 69</p>

- Se actualiza la versión del componente de firma en cliente Websigner a la versión 5.6.0.9.
- Se adapta el servicio para su consumo por parte de Atlas.

La actual versión del servicio **v20101105**, con respecto a la versión anterior v20101019, incorpora los siguientes cambios:

- Se actualiza el cliente del Servicio de Gestión de Repositorio de Documentos Electrónicos.
- Se igualan los entornos del componente de firma en cliente para Explotación y Pre-Explotación.

La actual versión del servicio **v20101019**, con respecto a la versión anterior v20100917, incorpora los siguientes cambios:

- Se actualiza la distribución de los javascript en el contexto estático de producción. Este cambio es transparente al desarrollador.

La actual versión del servicio **v20100917**, con respecto a la versión anterior v20100623, incorpora los siguientes cambios:

- Se actualiza el componente de WebSigner de la versión 5.1.04 a la versión 5.6.0.4
- Con respecto a la versión anterior del manual del desarrollador se elimina el apartado 5.3 “Configurar Internet Explorer para Firma en Cliente”, ya que con la nueva versión del componente de WebSigner esta configuración no es requerida.

La actual versión del servicio **v20100621**, con respecto a la versión anterior v20100623, incorpora los siguientes cambios:

- Se actualiza el servicio de firma para la resolución de incidencias asociadas a la verificación de firmas en formato XMLSignature y PKCS7.

 <p><b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad</p>	 <p><b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias</p>
<p>Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo</p>	<p>Página 9 de 69</p>

La actual versión del servicio **v20100323**, con respecto a la versión anterior v20090901, incorpora los siguientes cambios:

- Se realiza la firma del WebSigner (ActiveX y Applet) con un certificado de Gobierno de Canarias emitido por la autoridad certificadora VeriSign.

La actual versión del servicio **v20090901**, con respecto a la versión anterior v20090707, incorpora los siguientes cambios:

- Se actualiza el cliente del Servicio de Gestión de Repositorio de Documentos Electrónicos.

La actual versión del servicio **v20090707**, con respecto a la versión anterior v20090126, incorpora los siguientes cambios:

- Se permite realizar firmas de documentos bajo el protocolo https, tanto en servidor como en cliente (usando Internet Explorer)
- Se permite realizar firmas a través de un proxy
- Se permite realizar firmas de URLs que incorporan redirección
- Se mejora la validación de sellos de tiempo
- Se corrige un bug que impedía realizar firmas de documentos del repositorio de documentos electrónicos de Platino

La actual versión del servicio v20090126, con respecto a la versión anterior v20081015, incorpora los siguientes cambios:

- Se amplía la funcionalidad del “CU-FST-06 Firma XML Signature” para permitir la firma de documentos almacenados en el Servicio de Gestión de Repositorio de Documentos Electrónicos (SGRDE), identificados por su URI.
- Se añade un nuevo Caso de uso “CU-FST-18 Timestamp de Firma” que permite realizar el sellado de tiempo de una firma.

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 10 de 69

- En el método `verifyPKCS7Signature`, se modifica el tipo de datos del parámetro que permite aportar el documento a validar, antiguamente era de tipo `String` y a partir de esta versión será de tipo `byte[]`.
- Se amplía la funcionalidad del “CU-FST-06 Firma XML Signature” para dar soporte a firma múltiples en el caso de firmar documentos almacenados en el SGRDE.
- Se amplía la funcionalidad del “CU-FST-06 Firma XML Signature” para que las firmas incluyan la fecha y hora (no oficial) en la que se realizó la firma.
- Se amplía la funcionalidad del “CU-FST-08 Validar firma XML Signature” para dar soporte a la validación de firmas múltiples.
- Se amplía la funcionalidad del “CU-FST-16 Validar firma Contenido” para dar soporte a la validación de firmas múltiples.
- Se añade el apartado “5.2. Firma Múltiple” donde se detalla el formato para las firmas múltiples de Platino.
- Se actualiza el caso de uso “CU-FST-03 Validar firma XML Signature” para definir el nuevo applet de validación de firmas XML en cliente.
- Se añade un nuevo Caso de uso “CU-FST-19 Firma Secuencial” que permite realizar la firma secuencial en servidor de un documento.
- Se añade un nuevo Caso de uso “CU-FST-20 Firma XMLSignature Secuencial” que permite realizar la firma secuencial en cliente.
- Se añade el apartado 5.3 Configurar Internet Explorer para Firmar en Cliente, donde se enumeran los pasos para instalar el ActiveX de firma cuando usamos Internet Explorer.

La versión del servicio v20081015, con respecto a la versión anterior del servicio v20080902, incorpora los siguientes cambios:

- Se corrigen ciertas erratas en los apartados 3.8, 3.9 que indicaban que los parámetros debían proporcionarse codificados en Base64 cuando no es cierto.

 <p><b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad</p>	 <p><b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias</p>
<p>Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo</p>	<p>Página 11 de 69</p>

- Se actualizan en el apartado "3.14 - Obtener Información de un Certificado" los nuevos valores de retorno del método.
- Se implementa el método getTime, que devuelve la fecha actual del servidor de sellado de tiempo de la FNMT.
- Se sustituye el valor de retorno del método getTime para que devuelva Date en lugar de String
- Se implementa el método timestamp, que realiza la firma y sellado de tiempo de un documento.
- Se incorpora un nuevo método analyzeTimestamp, que es capaz de analizar el sello de tiempo existente en una firma.

La versión del servicio v20080902, con respecto a la versión anterior del servicio v20080630, incorpora los siguientes cambios:

- Se corrige una errata en el apartado 3.8, que no reflejaba que el método devolvía un booleano indicando la validez de la firma.
- Se incorporan dos nuevos métodos que permiten firmar y validar (en formato XML Signature - Detached) el contenido de un documento independientemente de su ubicación:
  - signContent: Firma XML detached por contenido.
  - verifyContentSignature: Validación de la firma XML Signature Detached por contenido.

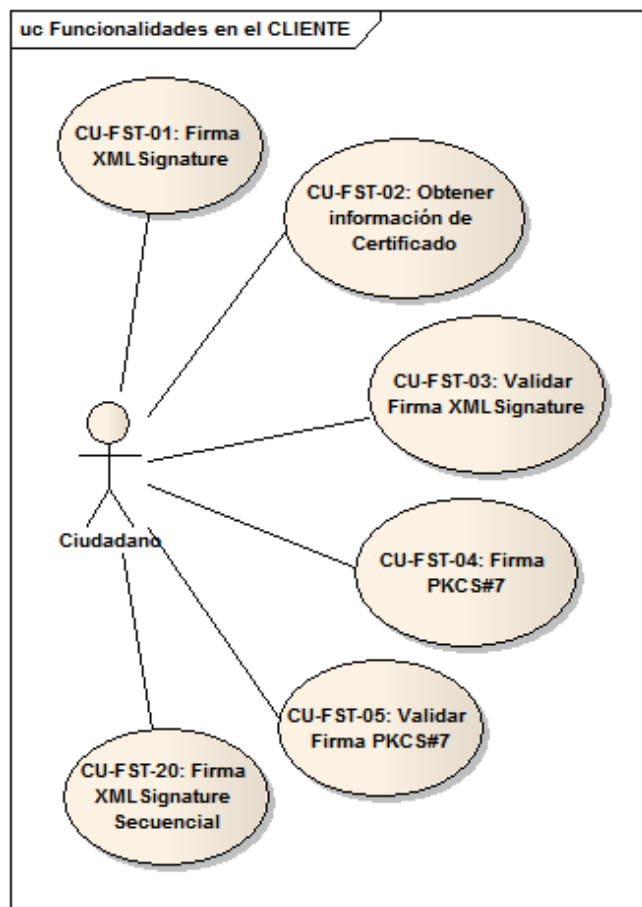
## 2 VERSIÓN DEL SERVICIO

Este documento corresponde a la versión **20111020** del servicio.



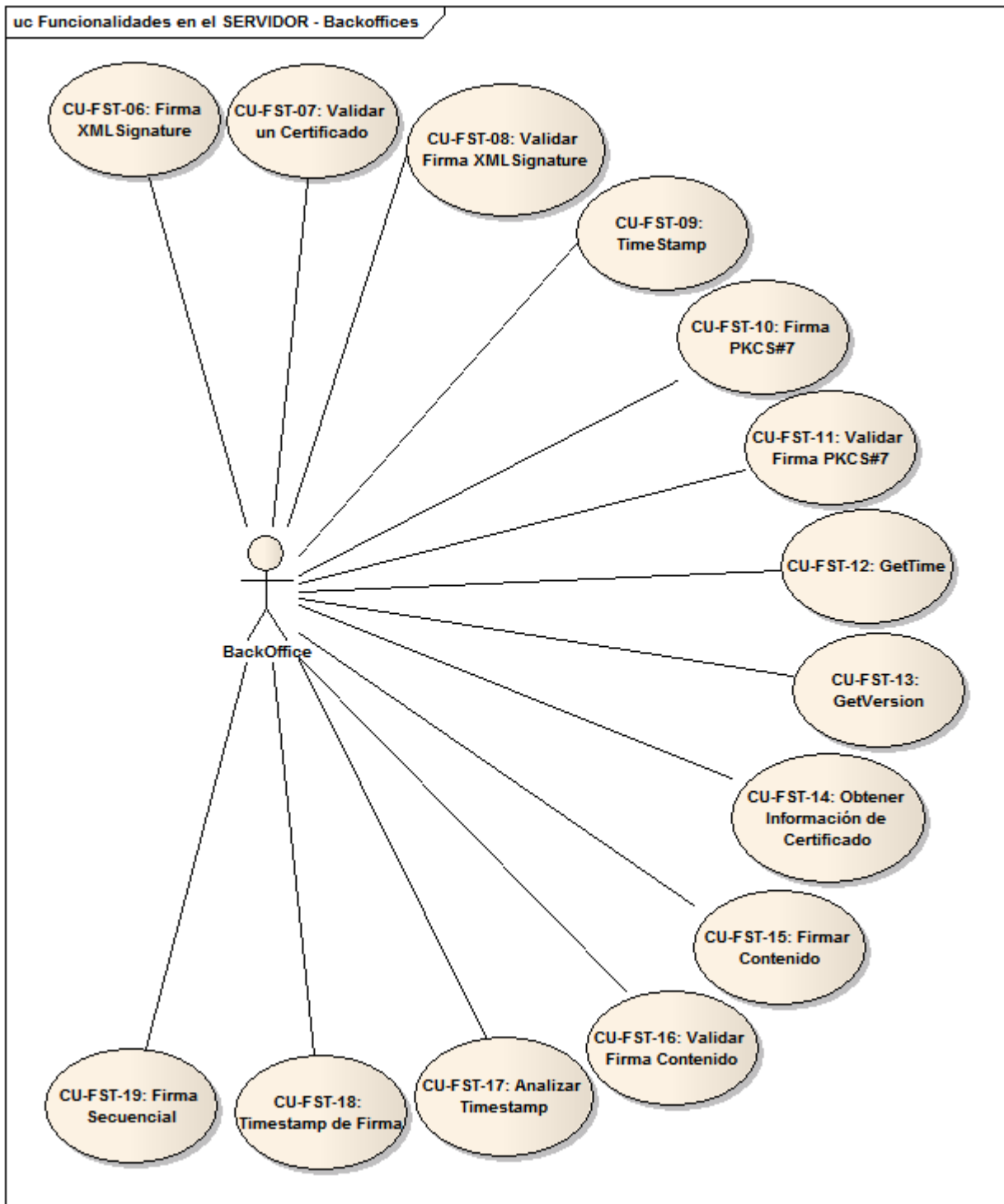
### 3 CASOS DE USO

A continuación se muestra el diagrama de casos de uso del servicio de Firma electrónica y Sellado de tiempo:



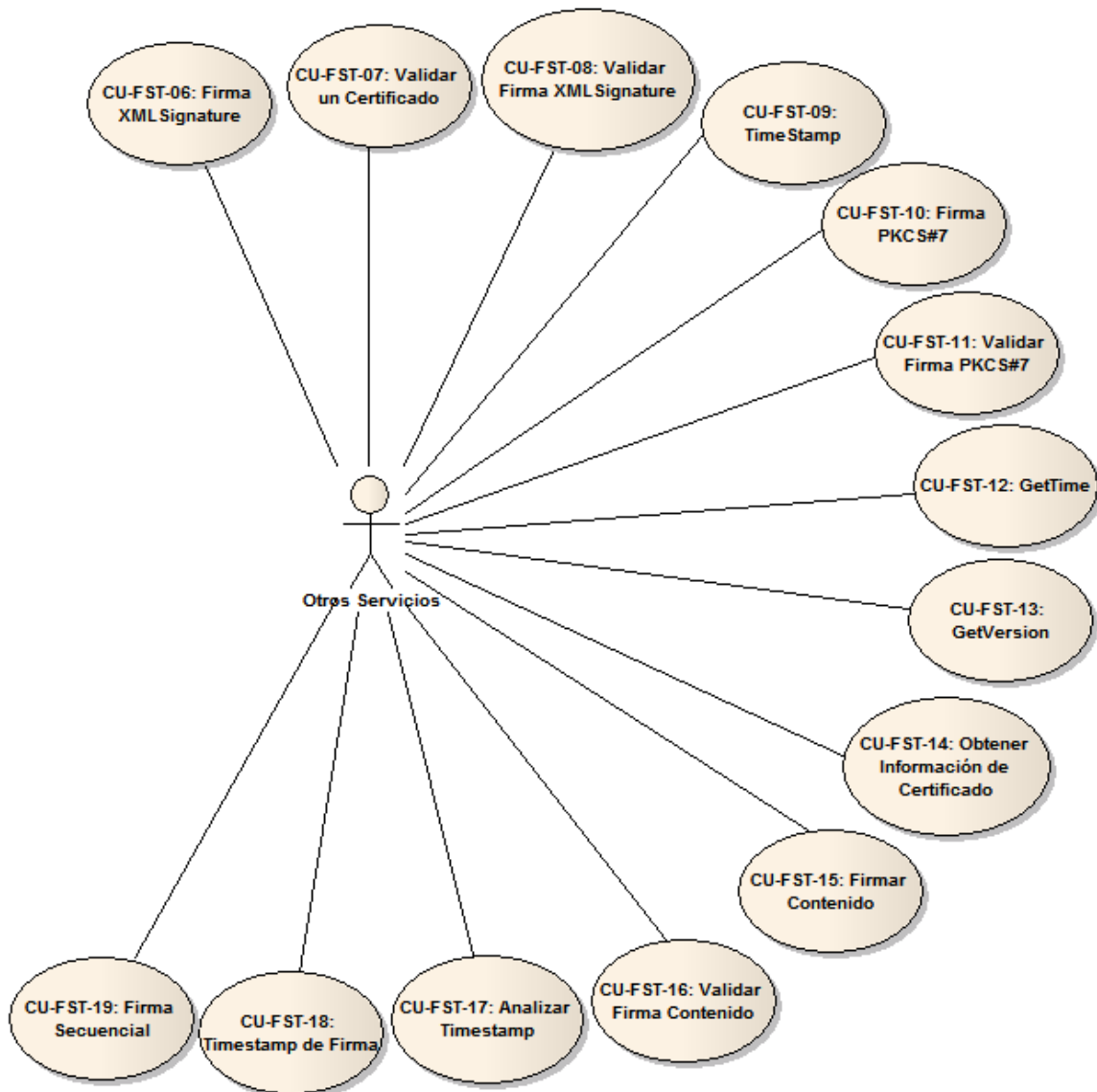


uc Funcionalidades en el SERVIDOR - Backoffices






uc Funcionalidades en el SERVIDOR - Servicios



 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 15 de 69

El servicio de firma electrónica y sellado de tiempo permite realizar las siguientes operaciones:

Operaciones en el cliente	Operaciones en el servidor
<ul style="list-style-type: none"> <li>• getCertInfo</li> <li>• signFile</li> <li>• signPKCS7</li> <li>• checkSignature</li> <li>• checkPKCS7Signature</li> <li>• signSequential</li> </ul>	

### 3.1 CU-FST-01: FIRMA XML SIGNATURE

Este caso de uso permite a los ciudadanos y a los backoffices, que hagan uso de PLATINO, la firma de documentos en formato XMLSignature en su propio navegador.

En este proceso de firma el usuario debe descargarse un ActiveX o un Applet de Java según utilice Internet Explorer o Mozilla respectivamente. Una vez hecho esto, la interfaz web sólo muestra los certificados del usuario que estén autorizados para el proceso de firma.

Una vez obtenida la firma del documento o formulario, el ciudadano podría guardarla en su equipo.

#### Precondiciones:

Ha de haber un documento que firmar y tener un certificado digital válido para llevar a cabo la firma.

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 16 de 69

### Interfaz:

Hay que tener en cuenta que el proveedor sobre el que se monta la fachada cliente, en este caso *TB-Solutions*, al cargar los certificados, los enumerará en orden ascendente y consecutivo.

### Entrada al servicio:

Los parámetros de entrada al servicio serán por lo tanto la posición en la que se encuentra el certificado con el que deseamos llevar a cabo la firma y el contenido de lo que deseamos firmar.

Nombre del parámetro	Descripción
certificatePos	Posición del certificado con el que deseamos firmar en el array de certificados cargados por el applet/ActiveX
document	Url donde encontraremos el contenido de lo que deseamos firmar.

### Salida del servicio:

A continuación se muestra una tabla con los valores devueltos por el servicio .

Resultado	Descripción
sSignedData	String con el contenido de los datos firmados en formato XMLSignature.

## 3.2 CU-FST-02: OBTENER INFORMACIÓN DE UN CERTIFICADO

Esta funcionalidad permite a los ciudadanos obtener la información almacenada en un determinado certificado que se encuentre instalado en el navegador del usuario.

### Precondiciones:

Para que la ejecución del caso de uso se lleve a cabo con un resultado satisfactorio, el consumidor de este caso de uso ha de tener instalado en su navegador web algún certificado válido.

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 17 de 69

### Interfaz:

Hay que tener en cuenta que el proveedor sobre el que se monta la fachada cliente, en este caso *TB-Solutions*, al cargar los certificados, los enumerará en orden ascendente y consecutivo.

### Entrada al servicio:

Los parámetros de entrada al servicio serán por lo tanto los siguientes:

Nombre del parámetro	Descripción
certificatePos	Posición del certificado en el array de certificados cargados por el applet/ActiveX del cual deseamos obtener información

### Salida del servicio:

A continuación se muestra una tabla con los valores devueltos por el Servicio en respuesta a una invocación con éxito de esta operación.

Resultado	Descripción
sCertInfo	Array con la información recuperada del certificado deseado. El array devuelto contiene la siguiente información (por este orden): <ul style="list-style-type: none"> <li>● Emisor del certificado</li> <li>● Asunto del certificado</li> <li>● Número de serie del certificado</li> <li>● Fecha de inicio de validez del certificado</li> <li>● Fecha de fin de validez del certificado</li> <li>● Certificado codificado en base64</li> <li>● Booleano indicando si el certificado incluye una clave privada.</li> </ul>

### 3.3 CU-FST-03: VALIDAR FIRMA XML SIGNATURE

Esta funcionalidad permite a los consumidores del servicio, la verificación en su propio navegador de las firmas realizadas sobre documentos firmados localmente.

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 18 de 69

A alto nivel, los servicios más importantes ofrecidos por este caso de uso son:

- Verificación de firma.
- Verificación de que los datos firmados se corresponden con los deseados y no fueron modificados después de llevar a cabo la firma.

Un ejemplo de carga del applet se encuentra disponible en la aplicación de ejemplo PlatinoWebSignerTest.

### Precondiciones:

Para poder validar una firma es necesario disponer del documento y de la firma a validar en formato XMLSignature.

La ejecución de esta funcionalidad se ha desarrollado en un Applet que se instala en el navegador cliente. Este applet incorpora una interfaz que permite al usuario seleccionar el documento y la firma para proceder a su validación.

Interfaz:

### Entrada al servicio:

Los parámetros de entrada al servicio serán por lo tanto los siguientes:

Nombre del parámetro	Descripción
pathDocument	Path del documento
PathSignature	Path donde está almacenada la firma del documento a validar

Salida del servicio:

A continuación se muestra una tabla con los valores devueltos por el Servicio en respuesta a una invocación con éxito de esta operación.

Resultado	Descripción
boolean	Booleano que indica si la firma es válida o no

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 19 de 69

### 3.4 CU-FST-04: FIRMA PKCS#7

Este caso de uso permite a los ciudadanos y a los backoffices, que hagan uso de PLATINO, la firma de texto en formato PKCS#7 en su propio navegador.

En este proceso de firma el usuario debe descargarse un ActiveX o un Applet de Java según utilice Internet Explorer o Mozilla respectivamente. Una vez hecho esto, la interfaz web sólo muestra los certificados del usuario que estén autorizados para el proceso de firma.

Una vez obtenida la firma del texto, el ciudadano podría guardarlo en su equipo.

#### Precondiciones:

Ha de haber un texto que firmar y poseer un certificado digital válido para llevar a cabo la firma.

#### Interfaz:

Hay que tener en cuenta que el proveedor sobre el que se monta la fachada cliente, en este caso TB-Solutions, al cargar los certificados, los enumerará en orden ascendente y consecutivo.

#### Entrada del Servicio:

Los parámetros de entrada al servicio serán por lo tanto la posición en la que se encuentra el certificado con el que deseamos llevar a cabo la firma y el contenido de lo que deseamos firmar.

Nombre del parámetro	Descripción
certificatePos	Posición del certificado con el que deseamos firmar en el array de certificados cargados por el applet/ActiveX
textToSign	Texto que deseamos firmar en formato PKCS#7

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 20 de 69

### Salida del Servicio:

A continuación se muestra una tabla con los valores devueltos por el servicio .

Resultado	Descripción
sSignedData	String con el resultado de la firma en formato PKCS#7

### 3.5 CU-FST-05: VALIDAR FIRMA PKCS#7

Esta funcionalidad permite a los consumidores del servicio, la verificación en su propio navegador de las firmas realizadas en formato PKCS#7.

A alto nivel, los servicios más importantes ofrecidos por este caso de uso son:

- Verificación de firma y obtención de los datos de los firmantes.
- Verificación de que los datos firmados se corresponden con los deseados y no fueron modificados después de llevar a cabo la firma.

### Precondiciones:

Para poder validar una firma es necesario tener el resultado de haber firmado un texto en formato PKCS#7.

### Interfaz:

#### Entrada del Servicio:

Los parámetros de entrada al servicio serán por lo tanto los siguientes:

Nombre del parámetro	Descripción
originalText	Texto original sobre el que se efectuó la firma.
signature	String que contiene la firma en formato PKCS#7 que deseamos validar.

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 21 de 69

### Salida del Servicio:

A continuación se muestra una tabla con los valores devueltos por el Servicio en respuesta a una invocación con éxito de esta operación.

Resultado	Descripción
ArrResult	Array conteniendo el resultado de la verificación y los datos del firmante. En caso de error de validación también se incluye la descripción del error que provocó el fallo en la validación.

### 3.6 CU-FST-20: FIRMA XML SIGNATURE SECUENCIAL

Este caso de uso permite a los ciudadanos y a los backoffices, que hagan uso de PLATINO, la realización de firmas secuenciales en formato XMLSignature en su propio navegador.

En este proceso de firma el usuario debe descargarse un ActiveX o un Applet de Java según utilice Internet Explorer o Mozilla respectivamente. Una vez hecho esto, la interfaz web sólo muestra los certificados del usuario que estén autorizados para el proceso de firma.

#### Precondiciones:

Para la realización de una firma secuencial es necesario disponer de una firma XMLSignature previa, así como tener un certificado digital válido para llevar a cabo la firma secuencial.

#### Interfaz:

Hay que tener en cuenta que el proveedor sobre el que se monta la fachada cliente, en este caso *TB-Solutions*, al cargar los certificados, los enumerará en orden ascendente y consecutivo.

#### Entrada al servicio:

Los parámetros de entrada al servicio serán por lo tanto la posición en la que se encuentra el certificado con el que deseamos llevar a cabo la firma y el contenido de lo que deseamos firmar.

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 22 de 69

Nombre del parámetro	Descripción
certificatePos	Posición del certificado con el que deseamos firmar en el array de certificados cargados por el applet/ActiveX
signature	Firma existente a la que deseamos añadir una nueva firma secuencial.

### Salida del servicio:

A continuación se muestra una tabla con los valores devueltos por el servicio .

Resultado	Descripción
sSignedData	String con el contenido del resultado de la firma secuencial en formato XMLSignature.

### 3.7 CU-FST-06: FIRMA XML SIGNATURE

El caso de uso de firma de documentos en el lado del servidor permite, a cualquier servicio o backoffice integrado con Platino, realizar peticiones para que el servicio realice la firma documentos en formato XML Signature.

#### Interfaz:

sign		
input	sign	sign
output	signResponse	signResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

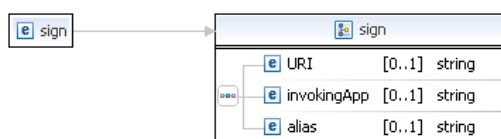
#### Precondiciones:

Para poder llevar a cabo un firma de este tipo es necesario tener un documento que firmar. Este documento a firmar debe estar accesible a través de un protocolo estándar (como por ejemplo http) o incluso, puede estar almacenado en el servicio de gestor de repositorio de documentos electrónicos; en este caso, el documento se identificará a través de la URI del gestor documental.

También es necesario estar dado de alta con un identificador de aplicación asignado, y tener un certificado válido dado de alta en la plataforma de firma, para realizar la firma.

Tanto el identificador de la aplicación como el acto de proporcionar el certificado con el que se desean realizar las firmas, se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

### Entrada al servicio:



A continuación se muestra el modelo de datos que se ha de utilizar cuando queremos invocar a la operación de firma en el servidor:

Parámetro	Descripción
URI	Uri del documento que deseamos firmar.
invokingApp	Código de la aplicación que realiza la invocación al servicio
alias	Alias del certificado, almacenado en el servidor, con el que se va a firmar el documento.

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

### Ejemplo de entrada del servicio

```

<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header />
  <soapenv:Body>
    <sfst:sign>
      <URI>http://www.mat.ucm.es/~ome2007/prueba.pdf</URI>
      <invokingApp>PLATINO</invokingApp>
      <alias>jpadron-ciber</alias>
    </sfst:sign>
  </soapenv:Body>
</soapenv:Envelope>

```

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 24 de 69

## Salida del servicio:



Valor de retorno	Descripción
result	Resultado de la firma.

El resultado de la firma dependerá del parámetro URI que se le haya pasado al método:

- En el caso de que en el parámetro URI se haya pasado un valor que indique la ubicación del documento a firmar a través de un protocolo estándar (como por ejemplo http), el resultado será una firma XML Detached tal como se muestra en el cuadro inferior “Ejemplo de salida del servicio”.
- En el caso de que en el parámetro URI se haya pasado una URI que referencia a un documento almacenado en el gestor documental de Platino, la firma resultante tendrá en cuenta las posibles firmas que pudieran existir en el metadato correspondiente que almacena la firma electrónica del documento. Si el documento ya se encontrase firmado en el gestor documental, el resultado de la firma será una firma múltiple paralela, conforme a la documentación especificada en el apartado 5.2 de este mismo documento.

NOTA: Hay que tener en cuenta que el metadato que almacena la firma electrónica en el gestor documental de Platino no será modificado por la operación de firma.

## Ejemplo de salida del servicio

```

<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <ns2:signResponse xmlns:ns2="http://platino.gobcan.es/servicios/sfst/">
      <return><![CDATA[<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010315"></ds:CanonicalizationMethod>
<ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"></ds:SignatureMethod>
<ds:Reference URI="http://www.mat.ucm.es/~ome2007/prueba.pdf">
<ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></ds:DigestMethod>
<ds:DigestValue>UlcXYDIdetAaIDRGUs7ldlSpwUs=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>
OfQp7xUGblY5Ns+kj2ak+ConxqBvLriqXTsTHuV9V1PWcrtxF3JQSx1ZYkv6eg2X8f5SEC+RrWS
N+G7bFwfJ8ucCCSNB0je8OxhL4QVrbtEKufQAOEwzIRYBCIIirzJgvuTTy9TCHK+zW2CV9X5ckA
1IYDK1i5ImxuO3wY3Ws=
</ds:SignatureValue>
      ]></return>
    </ns2:signResponse>
  </env:Body>
</env:Envelope>
  
```



```

<ds:KeyInfo>
<ds:X509Data>
<ds:X509IssuerSerial>
<ds:X509IssuerName>CN=cibercentro,OU=DGTI,O=Gobierno de
Canarias,ST=Canarias,C=ES,EMAILADDRESS=cibercentro@gobiernodecanarias.org</ds:X509IssuerName>

<ds:X509SerialNumber>294005470306486901017480</ds:X509SerialNumber>
</ds:X509IssuerSerial>
<ds:X509Certificate>
MIIEOTCCA+OgAwIBAgIKPkiRiAACAAALiDANBgkqhkiG9w0BAQUFADBlzExMC8GCCsGCSIB3DQEJ
ARYiY2liZXJjZW50cm9A229iaWVybm9kZWNhbmFyaWFzLm9yZzELMAkGA1UEBHMCRVxETAPBgNV
BAGTCENhbmFyaWFzMR0wGwYDVQQKEzRhb2JpZXJubyBkZSBzYDQ5W5hcm1hc2ENMAsGA1UECXMEREdu
STEUMBIgA1UEAxMLY2liZXJjZW50cm8wHhcNMjcwNjEzMTExMTEyMTEyMTEyMTEyMTEyMTEyMTEy
jTEuNCGUGSgSIB3DQEJARYianBhZHZJvbKbVcGVuY2FuYXJpYXMuY29tMQswCQYDVQGEwJFUzER
MA8GA1UECMBIMQ2FuYXJpYXMuHTAbBgNVBAoTFEdvYml1cm5vIGR1IENhbmFyaWFzMQ0wCwYDVQQL
EwRER1RjMRQwGwYDVQQDEwtleHQtanBhZGxvcjCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEA
rg507I0PgnBKGDHlnPmKP9pTrjwJigwuh81IKX7hLNDAIEctTPyskesVPM9KYWNpEozuD1Yolor
wv9cMX9NnrQGz8887w7nmz6IuCEBva+QeA2mfY4p4kc5kDoOHw/uaSPJqxY7xUmSkQtCenddewyG
+uS07hd7QbpR+t273I8CAwEAACAAdMwggHFFMA4GA1UdDwEB/wQEAwIE8DATBgNVHSUEDDAKBggr
BgEFBQCqDAjAdBgNVHQ4EFgQU3N3sRosdglUOUrONw4IDQEQOQzsEwgMGALUdIwSBzCyIAUcO0k
rLNBKRzd4aIbEFxWoIXlnxKhgZ2kgZowgZcxMTAvBgkqhkiG9w0BCQEWImNpYmVyY2VudHJvQGVd
Yml1cm5vZGVjYW5hcm1hc2Y5cmcxZm9kZm9kZm9kZm9kZm9kZm9kZm9kZm9kZm9kZm9kZm9kZm9k
A1UEChMUR29iaWVybm9kZWNhbmFyaWFzLm9yZzELMAkGA1UEBmAsTBERHVEkxkFDASBgNVBAMTC2NpYmVy
Y2VudHJvQGVdY29iaWVybm9kZWNhbmFyaWFzLm9yZzELMAkGA1UEEwS0wGZG9uZ29iaWVybm9kZWNhbmFya
dG9uZ29iaWVybm9kZWNhbmFyaWFzLm9yZzELMAkGA1UEEwS0wGZG9uZ29iaWVybm9kZWNhbmFya
BGFzLm9yZzELMAkGA1UEEwS0wGZG9uZ29iaWVybm9kZWNhbmFyaWFzLm9yZzELMAkGA1UEEwS0wGZG9uZ29iaWVy
VTA/ygxmLwOyL551yzSjPIaujl3bc18d3Dy76+GCCXw9OsjsNs9Dr35uNggaoLzQaa2yulGVFPZ
++k=
</ds:X509Certificate>
</ds:X509Data>
<ds:KeyValue>
<ds:RSAKeyValue>
<ds:Modulus>
rg507I0PgnBKGDHlnPmKP9pTrjwJigwuh81IKX7hLNDAIEctTPyskesVPM9KYWNpEozuD1Yolor
wv9cMX9NnrQGz8887w7nmz6IuCEBva+QeA2mfY4p4kc5kDoOHw/uaSPJqxY7xUmSkQtCenddewyG
+uS07hd7QbpR+t273I8=
</ds:Modulus>
<ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
</ds:Signature>]]</return>
</ns2:signResponse>
</env:Body>
</env:Envelope>

```

### 3.8 CU-FST-07: VALIDAR UN CERTIFICADO

Este caso de uso permite a los servicios y a los backoffices de PLATINO solicitar al servicio de firma que compruebe tanto el periodo de validez como el estado de revocación de los certificados que se le envíen.

#### Precondiciones:

Para la ejecución de este caso de uso es necesario tener un certificado que validar, y haber obtenido un identificador de aplicación válido para la plataforma de firma.

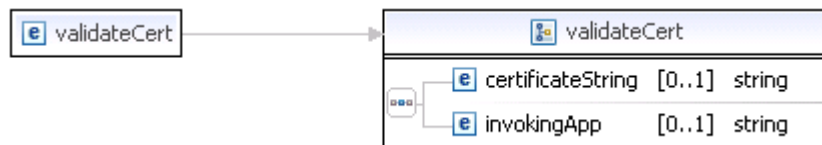
El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con platino@gobiernodecanarias.org).

#### Interfaz:



validateCert		
input	validateCert	validateCert
output	validateCertResponse	validateCertResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

### Entrada del servicio:



Parámetro	Descripción
certificateString	String que contiene el certificado a validar codificado en Base64
invokingApp	Código de la aplicación que realiza la invocación al servicio

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

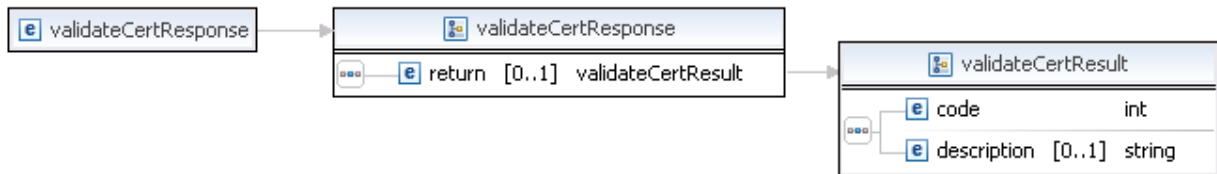
### Ejemplo de entrada al servicio.

```

<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header />
  <soapenv:Body>
    <sfst:validateCert>
      <certificateString>
        MIIEDzCCA7mgAwIBAgIKBcw2OgACAAALnTANBgkqhkiG9w0BAQUFADCB1zExMC8GCSqGSIb3DQEJ
        ARYiY2liZXJjZW50cm9AZ29 .....
      </certificateString>
      <invokingApp>PLATINO</invokingApp>
    </sfst:validateCert>
  </soapenv:Body>
</soapenv:Envelope>

```

### Salida del servicio:



Valor de retorno	Descripción														
return	<p>Resultado de la validación del certificado. Los posibles códigos de retorno son:</p> <table border="1"> <thead> <tr> <th>Código</th> <th>Descripción</th> </tr> </thead> <tbody> <tr> <td>6</td> <td>Certificado OK</td> </tr> <tr> <td>2</td> <td>Certificado no válido</td> </tr> <tr> <td>3</td> <td>El certificado no es de confianza</td> </tr> <tr> <td>4</td> <td>Certificado revocado</td> </tr> <tr> <td>5</td> <td>Certificado no verificado</td> </tr> <tr> <td>25</td> <td>Cadena de certificación no válida</td> </tr> </tbody> </table>	Código	Descripción	6	Certificado OK	2	Certificado no válido	3	El certificado no es de confianza	4	Certificado revocado	5	Certificado no verificado	25	Cadena de certificación no válida
Código	Descripción														
6	Certificado OK														
2	Certificado no válido														
3	El certificado no es de confianza														
4	Certificado revocado														
5	Certificado no verificado														
25	Cadena de certificación no válida														

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 28 de 69

### Ejemplo de salida del servicio.

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header/>
  <env:Body>
    <ns2:validateCertResponse xmlns:ns2="http://platino.gobcan.es/servicios/sfst/">
      <return>
        <code>6</code>
        <description>Certificado OK</description>
      </return>
    </ns2:validateCertResponse>
  </env:Body>
</env:Envelope>
```

### 3.9 CU-FST-08: VALIDAR FIRMA XML SIGNATURE

Esta funcionalidad permite a los servicios y backoffices que estén desplegados en la Plataforma de Interoperabilidad solicitar al servicio de firma que compruebe la validez de las firmas de documentos realizadas con formato XMLSignature obtenidas tras la invocación del caso de uso “CU-FST-06: Firma XML Signature”.

A alto nivel, los servicios más importantes ofrecidos por este caso de uso son:

- Verificación de una firma.
- Verificación de que los datos firmados se corresponden con los deseados y no fueron modificados después de llevar a cabo la firma.

#### Precondiciones:

Para la ejecución de este caso de uso, es necesario disponer de un resultado de firma previo y el código de la aplicación que se va a encargar de la verificación.

El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

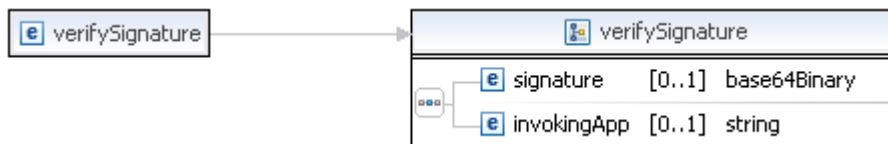
En el caso de que la firma a validar sea una firma múltiple, hay que tener en cuenta que el formato de la firma múltiple debe ser conforme a lo especificado en el apartado “5.2 Firmas Múltiples” y que todas las firmas contenidas dentro de la firma múltiple deben tener el mismo valor en el atributo URI del elemento `ds:Reference`, indicando así que hacen referencia al mismo documento. Si no fuese así, por ejemplo porque uno de los firmantes ha realizado la firma a través del CU-FST-01: Firma XMLSignature (en cliente), para validar esa firma múltiple, debemos usar el CU-FST-16: Validar Firma Contenido.

#### Interfaz:



verifySignature		
input	verifySignature	verifySignature
output	verifySignatureResponse	verifySignatureResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

### Entrada del servicio:



Parámetro	Descripción
signature	Bytes de la firma a verificar
invokingApp	Código de la aplicación que realiza la invocación al servicio

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

### Ejemplo de entrada al servicio.

```

<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:sfst="http://platino.gobcan.es/servicios/sfst/"
  <soapenv:Header />
  <soapenv:Body>
    <sfst:verifySignature>
      <signature>
        <!-- Resultado de haber firmado un documento. -->
      </signature>
      <invokingApp>PLATINO</invokingApp>
    </sfst:verifySignature>
  </soapenv:Body>
</soapenv:Envelope>

```

### Salida del servicio:

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 30 de 69



Valor de retorno	Descripción
return	Resultado de la verificación de la firma.

**Ejemplo de salida del servicio.**

```

<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header/>
  <env:Body>
    <ns2:verifySignatureResponse xmlns:ns2="http://platino.gobcan.es/servicios/sfst/">
      <return>
        true
      </return>
    </ns2:verifySignatureResponse>
  </env:Body>
</env:Envelope>
  
```

### 3.10 CU-SFT-09: TIMESTAMP

Esta funcionalidad permite a los servicios y backoffices de la plataforma solicitar sellos de tiempo para documentos, dotando a los elementos firmados de validez en el momento de la firma.

El objetivo de usar el sellado de tiempo es asegurar que un dato concreto existía antes de un determinado momento. Esto puede ser útil por ejemplo, para verificar que una firma digital que fue aplicada a un documento o formulario era válida antes de que el correspondiente certificado fuera revocado o quedase caducado, así como para que quede constancia de que algún documento se presentó en una fecha determinada.

**IMPORTANTE:** Hay que tener en cuenta que cada ejecución de este método incurre un gasto para Gobierno, por lo que se ruega que se haga un uso responsable del mismo.

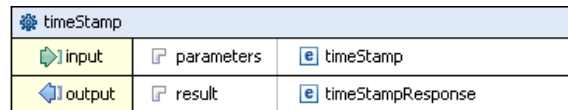
#### Precondiciones:

Debe de haber un documento al que aplicar el sellado de tiempo y estar dada de alta una aplicación en la plataforma de firma con permisos para ejecutar esta acción y un certificado asociado a la aplicación.

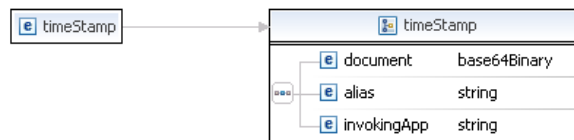
El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).



### Interfaz:



### Entrada del servicio:



Parámetro	Descripción
document	Bytes del documento a firmar.
alias	Alias del certificado con el que realizaremos la firma con sellado de tiempo
invokingApp	Código de la aplicación que realiza la invocación al servicio

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

### Ejemplo de Entrada

```
<soapenv:Envelope
  xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:sfst="http://platino.gobcan.es/servicios/sfst/"
  <soapenv:Header />
  <soapenv:Body>
    <sfst:timeStamp>
      <document><!-- Bytes del documento --></document>
      <alias>camerfirma</alias>
      <invokingApp>PLATINO</invokingApp>
    </sfst:timeStamp>
  </soapenv:Body>
</soapenv:Envelope>
```

### Salida del servicio



Parámetro	Descripción
-----------	-------------





```

<ds:RSAKeyValue>
  <ds:Modulus>
    n3J774hSvM0Iu411aXzsm2L86fQIBTp3CvBFf0fPlrbQWyn6CAExPDzWdVrMPrsue36sGCjeuwc
    vBdAc/VoFjVQF4Zm4y0cFaRN191zuCT1IRDnN3UxEi1vh4V5vzGOK0/A4JcDRkuvz00KIS7/qEU6
    Z6aU/sX6MYV578R6Eg8=
  </ds:Modulus>
  <ds:Exponent>AQAB</ds:Exponent>
</ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
<ds:Object>
  <SignatureProperties>
    <SignatureProperty Id="RFCTimeStamp1295795841" Target="#">
      <Object Encoding="base64"
        MimeType="application/timestamp-reply">
        MIIC4gYJKoZIhvcNAQcCoIIC0zCCAs8CAQMxCTAHBgUrDgMCGjCCAQkGCyqGSib3DQEJEAEEoIH5
        BIH2MIHzAgEBBgorBgEEAYRZCgMBMB8wBwYFKw4DAhoEFNuBwGwoHE+65LVSGWjv3PRGfVMAgZF
        XEtVfbEYezIwMDgxMDEzMTMxMTQxLjI2OFowBIACafSggZ2kgZowgZcxZzAJBgNVBAYTAKVTM0w
        CwYDVQQKEwRGTklUMRgwFgYDVQQLEw9GTklUIENsYXN1IDIgQ0EhEETAPBgNVBAsTCFBlYmxyY29z
        MUwwSgYDVQQDEONERNVNDUk1QQ01PTiBUU0ExIEZOTVQgQ0xBU0UgMiBDQSAtIEVVOVElEQQUgRk5N
        VCBSQ00gLSBDSUYgUTI4MjYwMDRKMUYIBsDCCAawCAQEWpjA2MQswCQYDVQQGEwJFUzENMAsGA1UE
        CmERk5NVDEYMBYGA1UECgMFRk5NVVNBZG90ZS90ZS90ZS90ZS90ZS90ZS90ZS90ZS90ZS90ZS90ZS90
        SIB3DQEJEAzENBgsqhkiG9w0BCRABBDAjBgkqhkiG9w0BCQQUxG9w0BCQQUxG9w0BCQQUxG9w0BC
        /9EwgYcGcyqGSib3DQEJEAIMMxgwdjB0MFoEFMUyEgYDVMgaaeJ2NeiuFeJSmabDOzMEIwOgQ4MDYx
        CzAJBgNVBAYTAKVTM0wCwYDVQQKEwRGTklUMRgwFgYDVQQLEw9GTklUIENsYXN1IDIgQ0EhEETAPBg
        q5EwFgYDVMgaaeJ2NeiuFeJSmabDOzMEIwOgQ4MDYx
        7JeTLNVwHuyMBJuPTP9gz+RZ7SbBA2w4Vvuhe/dpSDG4ADZG1BdxdqKINwoQkSWCbkF5BziTHgjC
        tSnD+sv5dYlMn8Iy49m0krjOD8P/29i+6PBzDWOzRHCfH9wZiaZqwtVMUjmu5FZ8rqGmIKTIcNU6
        dw==
      </Object>
    </SignatureProperty>
  </SignatureProperties>
</ds:Object>
</ds:Signature>

```

### 3.11 CU-FST-10: FIRMA PKCS#7

El caso de uso de firma de documentos en el lado del servidor permite, a cualquier servicio o backoffice integrado con Platino, realizar peticiones para que el servicio realice la firma de datos en formato PKCS#7.

#### Precondiciones:

Para poder llevar a cabo un firma de este tipo es necesario tener un texto que firmar, estar dado de alta con un identificador de aplicación asignado, y tener un certificado válido dado de alta en la plataforma de firma, para realizar la firma.

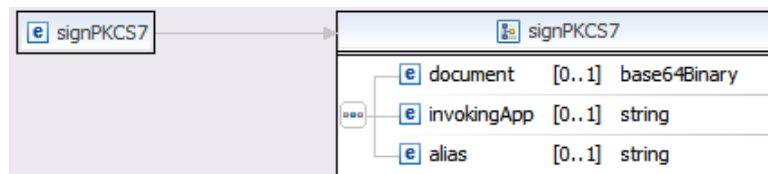
Tanto el identificador de la aplicación como el acto de proporcionar el certificado con el que se desean realizar las firmas, se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

## Interfaz:

signPKCS7		
input	signPKCS7	signPKCS7
output	signPKCS7Response	signPKCS7Response
SignatureServiceException	SignatureServiceException	SignatureServiceException

## Entrada al servicio:

A continuación se muestra el modelo de datos que se ha de utilizar cuando queremos invocar a la operación de firma en el servidor:



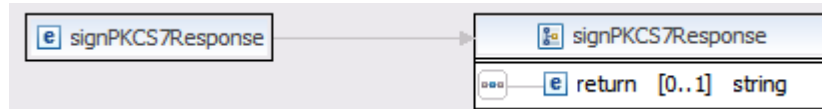
Parámetro	Descripción
document	Bytes del texto a firmar
invokingApp	Código de la aplicación que realiza la invocación al servicio
alias	Alias del certificado, almacenado en el servidor, con el que se va a firmar el documento.

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

## Ejemplo de entrada del servicio.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header/>
  <soapenv:Body>
    <sfst:signPKCS7>
      <document>Texto</document>
      <invokingApp>PLATINO</invokingApp>
      <alias>camerfirma</alias>
    </sfst:signPKCS7>
  </soapenv:Body>
</soapenv:Envelope>
```

### Salida del servicio:



Valor de retorno	Descripción
result	Resultado de la firma en formato PKCS#7.

### Ejemplo de salida del servicio

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <ns2:signPKCS7Response xmlns:ns2="http://platino.gobcan.es/servicios/sfst/"
      xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
      <return>MIIFsAYJKoZIhvcNAQcCoIIFoTCCBZ0CAQExDjAMBggqhkiG9w0CBOUAMAsGCSqSIB3DQEHAACC
      BCUwggQhMIIDy6ADAgEAgpmwKzAAIAAAw0MA0GCSqSIB3DQEBBQUAMIGXMTewLwYJKoZIhvcN
      AQkBFiJjaWJlcmNlbnRyb25Ab3B1bmlbnhbmFyaWZzLmNvbTElMAkGA1UEBHMCRVYXNl
      ETAPBgNVBAgTCENhbmFyaWZzMRUwEwYDVQQKEwxEUEVhbnR5b25Ab3B1bmlbnhbmFyaWZzLmNvbTEl
      cGFkbG9yMIGfMA0GCSqSIB3DQEBAQUAA4GNADCBiQKBgQDMcreGh4SRwRhl1KMubfYxKr8ki/Bb
      QG2lJHAXsYwUkPpDFq/nwhGgnUAzXmzIPQoC4ON8zoXyL7dzsOUXMTLkps25bEMMpFjE4YEckd4T
      L7xVbfTL22bDmO/yGfKJNNCovvFNOFHN1z44i5/MaC4mVjeAZZCFPL+J3DJ1XYbawIDAQAB04IB
      0zCCA8wDgYDVROFAQH/BAQDAgTWMBMGA1UdJQMMMAoGCCsGAQUFBwMCMCB0GA1UdDgQWBBSDuDZA
      rJOFnela7A8IycNuf8r2ZDCB0wYDVROjB1HLMIHigBRw7SSs1spHN3hohsQXFaghFwEgGBnaSB
      mjCB1zExMC8GCSqSIB3DQEJARYiY2liZXJjZW50cm9AZ29iaWVyb25Ab3B1bmlbnhbmFyaWZzLmNvbTEl
      MAKGA1UEBHMCRVYXNlETAPBgNVBAgTCENhbmFyaWZzMRUwEwYDVQQKEwxEUEVhbnR5b25Ab3B1bmlbnhbmFyaWZzLmNvbTEl
      cm1hc2ENMAsgA1UECXMEREduSTEUMBI GA1UEAxMLY2liZXJjZW50cm9AZ29iaWVyb25Ab3B1bmlbnhbmFyaWZzLmNvbTEl
      SgMwUwYDVROfEwewSjBcoEagRIZCaHR0cDovL2NvZ3N3b3J0aC5nb2JpZXJub2RlY2FuYXJpYXNlbnR5b25Ab3B1bmlbnhbmFyaWZzLmNvbTEl
      b3JnL2N1cnRlbnR5b25Ab3B1bmlbnhbmFyaWZzLmNvbTElZXJjZW50cm9AZ29iaWVyb25Ab3B1bmlbnhbmFyaWZzLmNvbTEl
      AoZCaHR0cDovL2NvZ3N3b3J0aC5nb2JpZXJub2RlY2FuYXJpYXNlbnR5b25Ab3B1bmlbnhbmFyaWZzLmNvbTElZXJjZW50cm9AZ29iaWVyb25Ab3B1bmlbnhbmFyaWZzLmNvbTEl
      ZXJjZW50cm9AZ29iaWVyb25Ab3B1bmlbnhbmFyaWZzLmNvbTElM0RwG6mj/A872LNIoc=</return>
    </ns2:signPKCS7Response>
  </soapenv:Body>
</soapenv:Envelope>
```

### 3.12 CU-FST-11: VALIDAR FIRMA PKCS#7

Esta funcionalidad permite a los servicios y backoffices que estén desplegados en la Plataforma de Interoperabilidad solicitar al servicio de firma que compruebe la validez de las firmas de documentos realizadas con formato PKCS#7.

A alto nivel, los servicios más importantes ofrecidos por este caso de uso son:

- Verificación de firma.
- Verificación de que los datos firmados se corresponden con los deseados y no fueron modificados después de llevar a cabo la firma.

### Precondiciones:

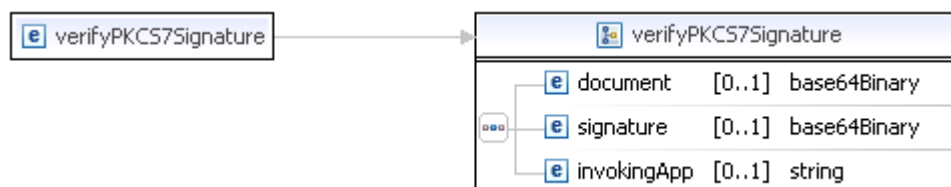
Para la ejecución de este caso de uso, es necesario disponer del resultado de firma previo y el código de la aplicación que se va a encargar de la verificación.

El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

### Interfaz:

verifyPKCS7Signature		
input	verifyPKCS7Signature	verifyPKCS7Signature
output	verifyPKCS7SignatureResponse	verifyPKCS7SignatureResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

### Entrada del servicio:



Parámetro	Descripción
document	Bytes del documento original para comprobar la firma
signature	Bytes de la firma a verificar
invokingApp	Código de la aplicación que realiza la invocación al servicio



 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 38 de 69

```
</ns2:verifyPKCS7SignatureResponse>
</soap:Body>
</soap:Envelope>
```

### 3.13 CU-SFT-12: GETTIME

Este caso de uso permite obtener el tiempo oficial obtenido por la FNMT.

**IMPORTANTE:** Hay que tener en cuenta que cada ejecución de este método incurre un gasto para Gobierno, por lo que se ruega que se haga un uso responsable del mismo.

#### Precondiciones:

Para la ejecución de este caso de uso, es necesario disponer del código de la aplicación que se va a encargar de solicitar la hora.

El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

#### Interfaz:

getTime		
input	getTime	getTime
output	getTimeResponse	getTimeResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

#### Entrada del Servicio:



Parámetro	Descripción
invokingApp	Código de la aplicación que realiza la invocación al servicio

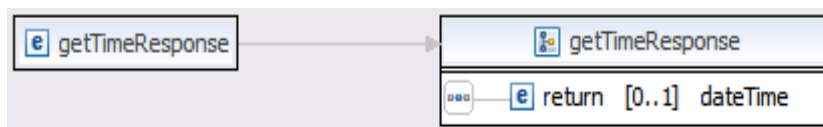
 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 39 de 69

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

### Ejemplo de entrada al servicio.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header/>
  <soapenv:Body>
    <sfst:getTime>
      <invokingApp>PLATINO</invokingApp>
    </sfst:getTime>
  </soapenv:Body>
</soapenv:Envelope>
```

### Salida del servicio:



Valor de retorno	Descripción
return	Fecha y hora obtenida del servidor de tiempo de la FNMT.

### Ejemplo de salida del servicio.

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header/>
  <soapenv:Body>
    <sfst:getTime>Fri Jun 13 17:58:04 BST 2008</sfst:getTime>
  </soapenv:Body>
</soapenv:Envelope>
```

## 3.14 CU-SFT-13: GETVERSION

Este caso de uso permite averiguar la versión en formato YYYYMMDD del servicio web desplegado.

## Interfaz:

getVersion		
input	getVersion	getVersion
output	getVersionResponse	getVersionResponse

## Entrada del servicio:

Este método no tiene parámetros de entrada.

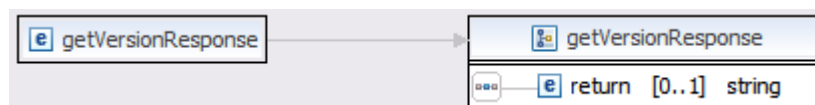


Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

## Ejemplo de Entrada

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header/>
  <soapenv:Body>
    <sfst:getVersion/>
  </soapenv:Body>
</soapenv:Envelope>
```

## Salida del servicio:



Valor de retorno	Descripción
return	String con la fecha de publicación del servicio en formato YYYYMMDD

### Ejemplo de salida del servicio.

```
<soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
    <ns2:getVersionResponse
      xmlns:ns2="http://platino.gobcan.es/servicios/sfst/"
      xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
      <return>20080613</return>
    </ns2:getVersionResponse>
  </soap:Body>
</soap:Envelope>
```

### 3.15 CU-SFT-14: OBTENER INFORMACIÓN DE UN CERTIFICADO

Esta funcionalidad obtener la información almacenada en un certificado que se encuentre instalado en el navegador del usuario.

#### Precondiciones:

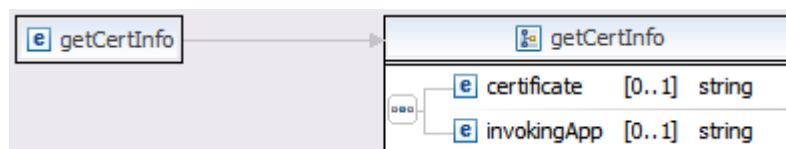
Para la ejecución de este caso de uso, es necesario disponer del código de la aplicación que se va a encargar de solicitar la información del certificado, así como la parte pública de un certificado.

El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

#### Interfaz:

getCertInfo		
input	getCertInfo	getCertInfo
output	getCertInfoResponse	getCertInfoResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

#### Entrada del Servicio:



 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 42 de 69

Parámetro	Descripción
certificate	String que contiene la clave pública del certificado al que queremos extraer la información.
invokingApp	Código de la aplicación que realiza la invocación al servicio

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

**Ejemplo de entrada al servicio.**

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header/>
  <soapenv:Body>
    <sfst:getCertInfo>
      <certificate>MIIFNTCCBJ6gAwIBAgI[...]</certificate>
      <invokingApp>PLATINO</invokingApp>
    </sfst:getCertInfo>
  </soapenv:Body>
</soapenv:Envelope>

```

**Salida del servicio:**



Valor de retorno	Descripción
return	Se retorna una estructura que empareja el campo con el valor recuperado del certificado. La descripción de cada uno de los campos por Autoridad Certificadora se describe en el apartado 5.3 INFORMACIÓN EXTRAÍDA DE LOS CERTIFICADOS

**Ejemplo de salida del servicio.**

```

<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/">
  <soapenv:Body>
    <ns2:getCertInfoResponse xmlns:ns2="http://platino.gobcan.es/servicios/sfst/"
xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
      <<return>
        <item>FullName</item>
        <item>NOMBRE XXXXXX - NIF XXXXXXXXX</item>
      </return>
      <return>
        <item>NIF</item>
        <item>XXXXXXXX</item>
      </return>
      <return>
        <item>Nombre</item>
        <item>XXXXXXXX</item>
      </return>
    </ns2:getCertInfoResponse>
  </soapenv:Body>
</soapenv:Envelope>

```



```
<item>Apellido1</item>
<item>XXXXXXXXXXXX</item>
</return>
<return>
  <item>Apellido2</item>
  <item>XXXXXXXXXX</item>
</return>
<return>
  <item>Organizacion</item>
  <item>FNMT</item>
</return>
<return>
  <item>SerialNumber</item>
  <item>00000000</item>
</return>
<return>
  <item>Issuer</item>
  <item>OU=FNMT Clase 2 CA, O=FNMT, C=ES</item>
</return>
<return>
  <item>Subject</item>
  <item>CN=XXXXXXXXXXXXXXXXXX - NIF XXXXXXXX, OU=507326001, OU=FNMT Clase 2 CA, O=FNMT, C=ES</item>
</return>
<return>
  <item>NotBefore</item>
  <item>Thu Mar 19 11:08:10 CET 2008</item>
</return>
<return>
  <item>NotAfter</item>
  <item>Sun Mar 19 11:08:10 CET 2011</item>
</return>
</ns2:getCertInfoResponse>
</soapenv:Body>
</soapenv:Envelope>
```

### 3.16 CU-FST-15: FIRMA CONTENIDO

El caso de uso de firma de contenido en el lado del servidor permite, a cualquier servicio o backoffice integrado con Platino, realizar peticiones para que el servicio realice la firma del contenido de un documento en formato XML Signature, sin que sea necesario referenciarlo a través de una URL.

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 44 de 69

## Interfaz:

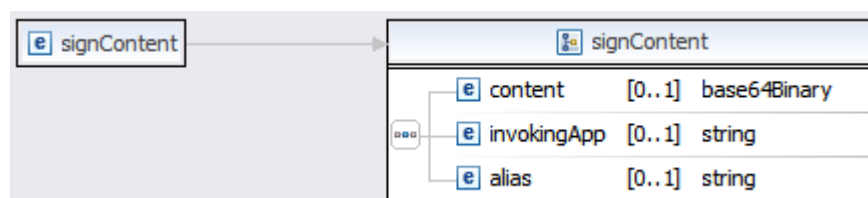
signContent		
input	signContent	signContent
output	signContentResponse	signContentResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

## Precondiciones:

Para poder llevar a cabo un firma de este tipo es necesario estar en posesión del contenido del documento que se desea firmar, estar dado de alta con un identificador de aplicación asignado, y tener un certificado válido dado de alta en la plataforma de firma, para realizar la firma.

Tanto el identificador de la aplicación como el acto de proporcionar el certificado con el que se desean realizar las firmas, se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

## Entrada al servicio:



A continuación se muestra el modelo de datos que se ha de utilizar cuando queremos invocar a la operación de firma en el servidor:

Parámetro	Descripción
content	Array de bytes que almacena el contenido que deseamos firmar.
invokingApp	Código de la aplicación que realiza la invocación al servicio
alias	Alias del certificado, almacenado en el servidor, con el que se va a firmar el documento.

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.



### Ejemplo de entrada del servicio

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header/>
  <soapenv:Body>
    <sfst:signContent>
      <content>Q29udGVuaWRvIGRlIHBydWViYSBwYXJhIGxhIGZpcmlh</content>
      <invokingApp>PLATINO</invokingApp>
      <alias>camerfirma</alias>
    </sfst:signContent>
  </soapenv:Body>
</soapenv:Envelope>
```

### Salida del servicio:



Valor de retorno	Descripción
return	Resultado de la firma.

### Ejemplo de salida del servicio

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header/>
  <env:Body>
    <ns2:signContentResponse xmlns:ns2="http://platino.gobcan.es/servicios/sfst/">
      <return><![CDATA[<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010315"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="urn:platino:firma:externa:9f67d01c-7d90-44e9-9061-ca09cec0715f">
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>oyGce041GxcZH3FjX3/jPX8iPQ=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    NuAYn5ed4moleLVsLHNETplhTQJeXo3BJE1AsdBB9Ss2MHk9VynAtmhdY/H+P94cAR3IbyUlGcNR
    baoDA303Z6nxcGo6wHcMr7v0C/onDx5MLsqSB1HxWF7b2AOY3VJD05/KjESU046HMqkL7sVZegGp
    6M1YbaXNZG5XGaG2dtY=
  </ds:SignatureValue>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509IssuerSerial>
        <ds:X509IssuerName>CN=AC Camerfirma Certificados Camerales,O=AC Camerfirma SA,SERIALNUMBER=A82743287,L=Madrid (see current
        address at www.camerfirma.com/address),EMAILADDRESS=ac_camerfirma_cc@camerfirma.com,C=ES</ds:X509IssuerName>
      <ds:X509SerialNumber>13474770085092524033</ds:X509SerialNumber>
      </ds:X509IssuerSerial>
    </ds:X509Data>
  </ds:KeyInfo>
  <ds:X509Certificate>
    MIIIDzCCBvegAwIBAgIJALsAAAAAABMA0GCSqGSIb3DQEBBQUAMIHGMQswCQYDVQQGEwJFUzEu
    MCwGCsGSIb3DQEJARYfYWVhY2F0eS5kaW8uY29udGVuaWRvIGRlIHBydWViYSBwYXJhIGxhIGZpcmlhLmNvbTFDMEEGALUEBxM6
    TWFkcmklIChzZWUgY3VycmVudCBhZGRyZXNzIGF0IHd3dy5jYXZpcmlhLmNvbS9hZGRyZXNz
    KTESMBAGALUEBRMJQTgyNzQzZjg3MRkwFwYDVQQKEwBBQYBdyW11cmZpcmlhIFNBM30wKwYDVQQD
    EyRBQYBdyW11cmZpcmlhIEN1cnRzZmljYWRvcyBdyW11cmFsZXNwHhcNMDCxMjEwMTUwMjA0WWhc
    MTIEMjA4MTUwMjA0WWhcCAAVsxCzAJBgNVBAYTAkVTMSwKgYDVQQDFDNDZj0aZWZpY2FkbyBQcnV1
    YmFzIFNvZnR3YXJlIFBhbG1kbzEiMCAGCSqGSIb3DQEJARYTAw5mb0BjYXZpcmlhLmNvbVtES
    MBAGALUEBRMJMTIzNDU2NzhaMRGwFgYDVQEF9Tb2Z0d2FyZSBW4WxpZG8xHDAaBgNVBCoTE0N1
```



 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 47 de 69

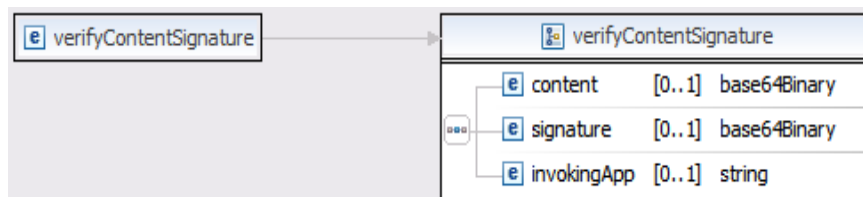
Para la ejecución de este caso de uso, es necesario disponer del resultado de una firma generada previamente tras la invocación del caso de uso Firmar Contenido, no pudiendo validar firmas que se hayan obtenido utilizando cualquier otro método de firma.

También será necesario estar en posesión del código de la aplicación que se va a encargar de la verificación.

El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

En el caso de que la firma a validar sea una firma múltiple, hay que tener en cuenta que el contenido aportado prevalecerá sobre cualquier referencia existente en las firmas contenidas en la firma múltiple, es decir, todas las firmas se validarán contra el mismo contenido.

### Entrada al servicio:



A continuación se muestra el modelo de datos que se ha de utilizar cuando queremos invocar a la operación de validación de firma de contenido:

Parámetro	Descripción
content	Array de bytes que almacena el contenido que hemos firmado.
signature	Array de bytes que contiene la firma a validar.
invokingApp	Código de la aplicación que realiza la invocación al servicio..

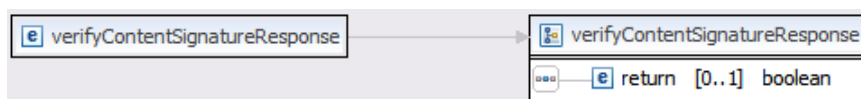
Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 48 de 69

## Ejemplo de entrada del servicio

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header/>
  <soapenv:Body>
    <sfst:verifyContentSignature>
      <content>[Bytes del contenido a validar] </content>
      <signature>[Bytes de la firma a validar]</signature>
      <invokingApp>PLATINO</invokingApp>
    </sfst:verifyContentSignature>
  </soapenv:Body>
</soapenv:Envelope>
```

## Salida del servicio:



Valor de retorno	Descripción
return	Resultado de la validación de la firma.

## Ejemplo de salida del servicio

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header/>
  <env:Body>
    <ns2:verifyContentSignatureResponse xmlns:ns2="http://platino.gobcan.es/servicios/sfst/">
      <return>true</return>
    </ns2:verifyContentSignatureResponse>
  </env:Body>
</env:Envelope>
```

### 3.18 CU-FST-17: ANALIZAR TIMESTAMP

El caso de uso llamado Analizar Timestamp permite, a cualquier servicio o backoffice integrado con Platino, realizar peticiones para que el servicio realice el análisis de de una firma con sellado de tiempo obtenida con el CU-FST-09: Timestamp

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 49 de 69

## Interfaz:

analyzeTimestamp		
input	analyzeTimestamp	analyzeTimestamp
output	analyzeTimestampResponse	analyzeTimestampResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

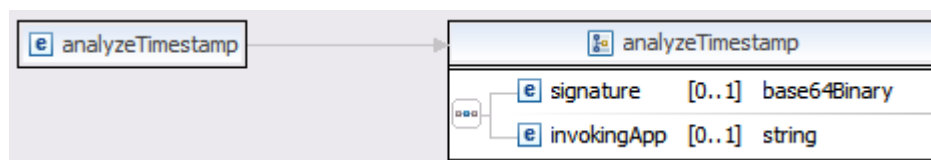
## Precondiciones:

Para la ejecución de este caso de uso, es necesario disponer del resultado de una firma con sellado de tiempo generada previamente tras la invocación del caso de uso Timestamp.

También será necesario estar en posesión del código de la aplicación que se va a encargar de la verificación.

El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

## Entrada al servicio:



A continuación se muestra el modelo de datos que se ha de utilizar cuando queremos invocar a la operación de análisis del sello de tiempo:

Parámetro	Descripción
signature	Array de bytes que almacena el resultado de una firma que incluye el sello de tiempo a analizar
invokingApp	Código de la aplicación que realiza la invocación al servicio..

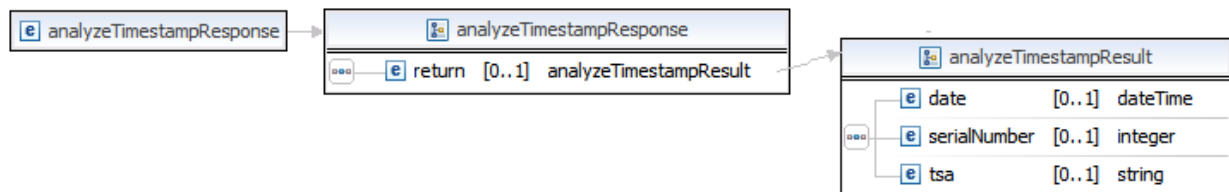
Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.



## Ejemplo de entrada del servicio

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header/>
  <soapenv:Body>
    <sfst:analyzeTimestamp>
      <signature> <!-- Bytes de la firma con sello de tiempo a analizar --> </signature>
      <invokingApp>PLATINO</invokingApp>
    </sfst:analyzeTimestamp>
  </soapenv:Body>
</soapenv:Envelope>
```

## Salida del servicio:



Valor de retorno	Descripción
analyzeTimestamResult	<p>Este objeto contiene los siguientes atributos:</p> <ul style="list-style-type: none"> <li>● date: Fecha en la que se realizó el sello de tiempo.</li> <li>● serialNumber: Número de serie del sellado de tiempo</li> <li>● tsa: Autoridad de sellado de tiempo que ha creado el sello.</li> </ul>

## Ejemplo de salida del servicio

```
<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header/>
  <env:Body>
    <ns2:analyzeTimestampResponse xmlns:ns2="http://platino.gobcan.es/servicios/sfst/">
      <return>
        <date>2008-10-15T13:29:55.326+02:00</date>
        <serialNumber>76262704907596</serialNumber>
        <tsa>4: C=ES,O=FNMT,OU=FNMT Clase 2 CA,OU=Publicos,CN=DESCRIPCION TSA1 FNMT CLASE 2 CA
- ENTIDAD FNMT RCM - CIF Q2826004J</tsa>
      </return>
    </ns2:analyzeTimestampResponse>
  </env:Body>
</env:Envelope>
```

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 51 de 69

### 3.19 CU-SFT-18: TIMESTAMP DE FIRMA

Esta funcionalidad permite a los servicios y backoffices de la plataforma solicitar sellos de tiempo para firmas, dotando a los elementos firmados de validez en el momento de la firma.

El objetivo de usar el sellado de tiempo es asegurar que un dato concreto existía antes de un determinado momento. Esto puede ser útil por ejemplo, para verificar que una firma digital que fue aplicada a un documento o formulario era válida antes de que el correspondiente certificado fuera revocado o quedase caducado, así como para que quede constancia de que algún documento se presentó en una fecha determinada.

**IMPORTANTE:** Hay que tener en cuenta que cada ejecución de este método incurre un gasto para el Gobierno de Canarias, por lo que se ruega que se haga un uso responsable del mismo.

#### Precondiciones:

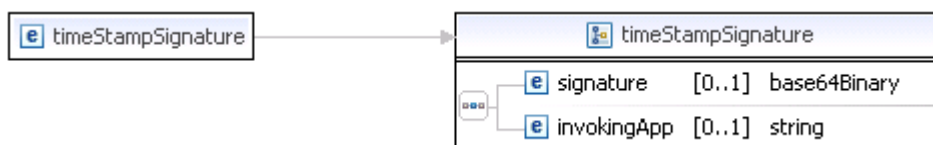
Es necesario estar en posesión de una firma a la que aplicar el sellado de tiempo y estar dada de alta una aplicación en la plataforma de firma con permisos para ejecutar esta acción y un certificado asociado a la aplicación.

El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

#### Interfaz:

timeStamp		
input	timeStamp	timeStamp
output	timeStampResponse	timeStampResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

#### Entrada del servicio:



 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 52 de 69

Parámetro	Descripción
signature	Bytes de la firma a la que añadir el sello de tiempo.
invokingApp	Código de la aplicación que realiza la invocación al servicio

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

Ejemplo de Entrada
<pre>&lt;soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"   xmlns:sfst="http://platino.gobcan.es/servicios/sfst/"&gt;   &lt;soapenv:Header/&gt;   &lt;soapenv:Body&gt;     &lt;sfst:timeStampSignature&gt;       &lt;signature&gt; &lt;!-- Bytes de la firma --&gt; &lt;/signature&gt;       &lt;invokingApp&gt;PLATINO&lt;/invokingApp&gt;     &lt;/sfst:timeStampSignature&gt;   &lt;/soapenv:Body&gt; &lt;/soapenv:Envelope&gt;</pre>

## Salida del servicio



Valor de retorno	Descripción
return	Resultado de la realización del sello de tiempo sobre la firma proporcionada.

Ejemplo de salida del servicio
<pre>&lt;ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"&gt;   &lt;ds:SignedInfo&gt;     &lt;ds:CanonicalizationMethod       Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010315" /&gt;     &lt;ds:SignatureMethod       Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" /&gt;     &lt;ds:Reference       URI="urn:platino:firma:externa:030803bd-a296-4102-8002-9391f190b33c"&gt;       &lt;ds:DigestMethod         Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" /&gt;       &lt;ds:DigestValue&gt;DsgBH+VmF53c8oT0KOzrbouclcw=&lt;/ds:DigestValue&gt;     &lt;/ds:Reference&gt;   &lt;/ds:SignedInfo&gt;   &lt;ds:SignatureValue&gt;     VSDiPAWdJUNLYFuc+4uXQhws/FQhkZTUoZiEwdm8wpTmV07hrTTurbZp7ua6QKBN108q/hAmPY0AF     bOGMSmW2kjZiMXregRACi8eZb90T71rnGgY0aiuUMhEWH2vtMbPbLDR03QpMcKjqP33ahw556us0     nS8sMe0EEKPD8DTNcQs=   &lt;/ds:SignatureValue&gt;   &lt;ds:KeyInfo&gt;     &lt;ds:X509Data&gt;       &lt;ds:X509IssuerSerial&gt;       &lt;ds:X509IssuerName&gt;         CN=AC Camerfirma Certificados Camerales,O=AC Camerfirma         SA,SERIALNUMBER=A82743287,L=Madrid (see current address         at         www.camerfirma.com/address),EMAILADDRESS=ac_camerfirma_cc@camerfirma.com,C=ES       &lt;/ds:X509IssuerName&gt;       &lt;/ds:X509Serial&gt;     &lt;/ds:X509Data&gt;   &lt;/ds:KeyInfo&gt; &lt;/ds:Signature&gt;</pre>



### 3.20 CU-SFT-19: FIRMA SECUENCIAL

Esta funcionalidad permite a los servicios y backoffices de la realización de una firma secuencial sobre otra firma de un documento existente previamente.

#### Precondiciones:

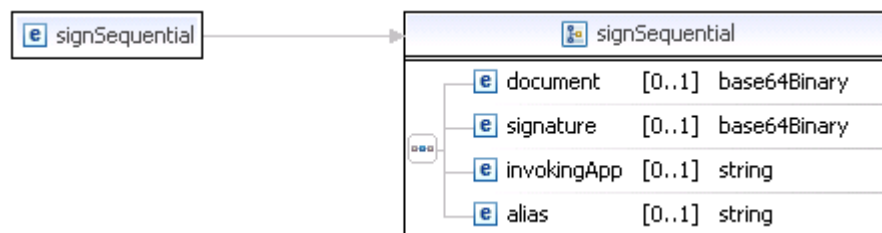
Es necesario estar en posesión de la firma previa a la que aplicar la firma secuencial. También será necesario disponer del documento que la primera firma ha firmado, así como estar dado de alta una aplicación en la plataforma de firma con permisos para ejecutar esta acción y un certificado asociado a la aplicación.

El identificador de la aplicación se proporcionará a través de la Oficina Técnica de Platino (para más información contactar con [platino@gobiernodecanarias.org](mailto:platino@gobiernodecanarias.org)).

#### Interfaz:

signSequential		
input	signSequential	signSequential
output	signSequentialResponse	signSequentialResponse
SignatureServiceException	SignatureServiceException	SignatureServiceException

#### Entrada del servicio:



Parámetro	Descripción
document	Bytes del documento firmado por la firma original
signature	Bytes de la firma a la que añadir la firma secuencial
invokingApp	Código de la aplicación que realiza la invocación al servicio
alias	Alias del certificado con el que realizar la firma secuencial

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 55 de 69

Un ejemplo típico de una invocación a esta operación es la que se muestra a continuación.

### Ejemplo de Entrada

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:sfst="http://platino.gobcan.es/servicios/sfst/">
  <soapenv:Header/>
  <soapenv:Body>
    <sfst:signSequential>
      <document> <!-- Bytes del documento firmado por la firma original --> </document>
      <signature> <!-- Bytes de la firma original --> </signature>
      <invokingApp>PLATINO</invokingApp>
      <alias>camerfirma</alias>
    </sfst:signSequential>
  </soapenv:Body>
</soapenv:Envelope>
```

### Salida del servicio



Valor de retorno	Descripción
return	String que contiene el resultado de la firma secuencial.

### Ejemplo de salida del servicio

```
<?xml version="1.0" encoding="UTF-8"?>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
Id="XMLSignature2">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod
      Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">
    </ds:CanonicalizationMethod>
    <ds:SignatureMethod
      Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1">
    </ds:SignatureMethod>
    <ds:Reference URI="#Object">
      <ds:Transforms>
        <ds:Transform
          Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
      </ds:DigestMethod>
      <ds:DigestValue>Afu/LIEflghFL6UgmGTfRGFA2Ow=</ds:DigestValue>
    </ds:Reference>
    <ds:Reference URI="#TimeStamp2">
      <ds:Transforms>
        <ds:Transform
          Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315">
        </ds:Transform>
      </ds:Transforms>
      <ds:DigestMethod
        Algorithm="http://www.w3.org/2000/09/xmldsig#sha1">
      </ds:DigestMethod>
      <ds:DigestValue>4Q/M1kgaVXz/Z/nfgXCEDjgnj40=</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    e0fJRtJXtHkxXMWTJBAeg3VDVwSgJI4By0hhbKjdv7rCn+XDjsCmTDKTLukaGkNhhkVwi0Kb64q
  </ds:SignatureValue>
</ds:Signature>
```



```

IBYqBwTERXfvG6xmNjGyB2ryYEPJxNt0f6KvRxDNORdDaSHP/DJULUO/kEYk4f1SU2sAYtATY+Op
bHkSPR7UOoaAobJAMhA=
</ds:SignatureValue>
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509IssuerSerial>
      <ds:X509IssuerName>
        CN=AC Firmaprofesional - CA1,O=Firmaprofesional S.A. NIF
        A-62634068,OU=Jerarquia de Certificacion
        Firmaprofesional,OU=Consulte
        http://www.firmaprofesional.com,L=C/ Muntaner 244
        Barcelona,EMAILADDRESS=ca1@firmaprofesional.com,C=ES
      </ds:X509IssuerName>
    <ds:X509SerialNumber>
      7819360434193339269178841547577629374
    </ds:X509SerialNumber>
  </ds:X509IssuerSerial>
  <ds:X509Certificate>
    MI IHaDCCB1CgAwIBAgIQBeH0PAGA9G9GJI19BWyavjANBgkqhkiG9w0BAQUFADCCARYxCzAJBgNV
    BAYTAkVMTSswJQYJKoZIhvcNAQkBFhhjYTFhZmlybWVwcm9mZXNpb25hbC5jb20xIjAgBgNVBAcT
    GUMvIE11bnRhbWVvYDI0NCBCYXJjZWxvbmExMTAvBgNVBAsTK0p1cmFycXVpYSBkZSBkZDZkZ0AwZmVz
    ZmlybWVwcm9mZXNpb25hbC5jb20xNDYyYmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    IEZpcmlhcHJvZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    MjYzNDQwZDEiMCAwIUEAxMzQUMgRmlhYmVwcm9mZXNpb25hbCAtIENBMTAeFw0wNzA0MTEwODQ2
    MTLAFlw0xMDA0MTEwODQ2MTEiIBGjESMBAGA1UEKHMJTk9NRU1QUONEMRgWfYyVdVQEEw9BUEVN
    UEWxIEFRUR1QTDEiXG9w0BAQUFADCCARYxCzAJBgNVBAYTAkVMTSswJQYJKoZIhvcNAQkBFhhjYTFh
    ZmlybWVwcm9mZXNpb25hbC5jb20xNDYyYmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    AQMCeW1RMDAwMDAwMEkxXjAgBgNVBAGTCUJhcnNlbG9uYU9mZXNpb25hbCAtIENBMTAeFw0wNzA0
    MTEwODQ2MTEiIBGjESMBAGA1UEKHMJTk9NRU1QUONEMRgWfYyVdVQEEw9BUEVNUEWxIEFRUR1QT
    DEiXG9w0BAQUFADCCARYxCzAJBgNVBAYTAkVMTSswJQYJKoZIhvcNAQkBFhhjYTFhZmlybWVwcm9m
    ZXNpb25hbC5jb20xNDYyYmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    ZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    c29uYmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    bS9kZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    gBSLUFdabw2SAKa35YVdw922tYaQ0jCByQYDVR0gBIHBMIG+MIG7BgsrBgEAAeZ5CgECATCBqzA3
    BggrBgEFBQcCARYraHR0cDovL3d3dy5maXJvYmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    BggrBgEFBQcCAjBkGmJfc3R1IGVzIHVvIGN1cnRmZmljYWRvIHBlcnNpb25hbC5jb20vZmVzZmVzZmVz
    IEhbnN1bHR1IGh0dHA6Ly93d3cuZmlybWVwcm9mZXNpb25hbC5jb20vZmVzZmVzZmVzZmVzZmVzZmVz
    BggrBgEFBQcCBAQRcMEAwPgYIKwYBBQUHMAKGMh0dHA6Ly93d3cuZmlybWVwcm9mZXNpb25hbC5jb2
    0vZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    MAsTA0VUVUg1BBIeBBDBGbnVHR8EPzA9MDugOaA3hjVodHRWoi8vY3JtsLmZpcmlhcHJvZmVzZmVz
    YWwU29L2ZpcmlhcHJvZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVzZmVz
    DjYc6SDBZPaAbc2cs+SxS1AibjMdc1ev/rvkxe8NzeUvJhZ3Qfe70jZNRhQuV7+KsXQP0S0cs9e3
    B9dcvnbNdezoXtQHEppQVrxtS1H7cJx87i9WHV/4LpMI1rS/dRxtGtZ/0wzZIKY9CyFuh19FUOD
    0Y7Sgz/FA7fat+LjszWdJen5IQFrusLaP44VVPqys++OR1oOW/YEYq7zgfbR1LMDVU05EiQbr700
    DFliA+Qa1uJH76u0sukooHieUO2RY6Jpbt0Kqy+kabwv0ZA213Z/jBsf0ZIT8sKVM/fuaq5WBsg
    ugb59x5F01hWv110nugm0Trpsg==
  </ds:X509Certificate>
</ds:X509Data>
<ds:KeyValue>
  <ds:RSAKeyValue>
    <ds:Modulus>
      qp3Y9gOovMI9CET/AhUW4B4qdMyYDI4AJom3Xx1FUO+AIejgSvYgsw3NRg8w++mPg4uqBrKScmQc
      NC7XH0bqvhLmPdnIBKAH4ER2YfdHadGxkWK1kLh2QbBMuWPMuxEjCea++PaC3JwZpY1Aukydbek
      gIou3wNCV7sbhOualU=
    </ds:Modulus>
    <ds:Exponent>AQAB</ds:Exponent>
  </ds:RSAKeyValue>
</ds:KeyValue>
</ds:KeyInfo>
<ds:Object Id="Object">
  <ds:Signature Id="XMLSignature">
    <ds:SignedInfo>
      <ds:CanonicalizationMethod>
        Algorithm="http://www.w3.org/TR/2001/REC-xm1-c14n-20010315"
      </ds:CanonicalizationMethod>
      <ds:SignatureMethod>
        Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"
      </ds:SignatureMethod>
      <ds:Reference>
        URI="urn:platino:firma:externa:8a1b5ca8-b303-4dd4-829b-1679809c0ef6"
        <ds:DigestMethod>
          Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"
        </ds:DigestMethod>
        <ds:DigestValue>
          fBV7J2pJLqSMqkoTpEjOmuM4rsA=
        </ds:DigestValue>
      </ds:Reference>
    </ds:SignedInfo>
  </ds:Signature>
</ds:Object>

```





```

<ds:Object>
  <SignatureProperties>
    <SignatureProperty Id="TimeStamp"
      Target="#XMLSignature">
      <timestamp>
        <date>20090116</date>
        <time>11:41:34</time>
      </timestamp>
    </SignatureProperty>
  </SignatureProperties>
</ds:Object>
</ds:Signature>
<ds:Object>
  <SignatureProperties>
    <SignatureProperty Id="TimeStamp2" Target="#XMLSignature2">
      <timestamp>
        <date>20090116</date>
        <time>11:41:43</time>
      </timestamp>
    </SignatureProperty>
  </SignatureProperties>
</ds:Object>
</ds:Signature>

```

## 4 CONTROL DE EXCEPCIONES

### 4.1 SignatureServiceException.

Todos los casos de uso descritos con anterioridad, en caso de producirse un error en su fase de ejecución, lanzarán un mismo tipo de excepción llamada SignatureServiceException. Esta excepción mostrará el código de error generado y un mensaje descriptivo del error producido.



Atributo	Descripción	Tipo
message	Mensaje descriptivo del error que se ha producido. Este incluye el código de error propio de ASF.	String

Ejemplo de excepción:

## Ejemplo de salida del servicio de consulta con la excepción.

```

<env:Envelope xmlns:env="http://schemas.xmlsoap.org/soap/envelope/">
  <env:Header />
  <env:Body>
    <env:Fault>
      <faultcode>env:Server</faultcode>
      <faultstring>
        ERROR - SUBCODE: SA_SIG_ERI - Message: Se produjo un
        error durante la invocacion.
      </faultstring>
      <detail>
        <ns2:SignatureServiceException
          xmlns:ns2="http://platino.gobcan.es/servicios/sfst/">
          <message>
            ERROR - SUBCODE: SA_SIG_ERI - Message: Se
            produjo un error durante la invocacion.
          </message>
        </ns2:SignatureServiceException>
      </detail>
    </env:Fault>
  </env:Body>
</env:Envelope>

```

## 5 INFORMACIÓN ADICIONAL DEL SERVICIO

### 5.1 TIPOS DE DATOS

#### 5.1.1 ValidateCertResult

Esta es la estructura retornada por el web service en respuesta a la solicitud de validación de un certificado:



Atributo	Descripción	Tipo
code	Código retornado por la validación del certificado	Entero
description	Descripción del código retornado por la validación del certificado	Texto

### 5.2 FIRMAS MÚLTIPLES

Las firmas múltiples que devuelve Platino mantienen el siguiente formato:

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 60 de 69

### 5.2.1 Firma Múltiple Paralela

Es un fichero XML cuya raíz es el elemento <SignatureList> e internamente almacena de forma secuencial las firmas individuales que forman la firma múltiple.

## 5.3 INFORMACIÓN EXTRAÍDA DE LOS CERTIFICADOS

### 5.3.1 Introducción

El servicio de Firma Electrónica y Sellado de Tiempo de Platino admite certificados emitidos por diferentes organizaciones denominadas Prestadores de Servicios de Certificación (PSC). Cada PSC puede emitir certificados de diferentes tipos según su finalidad.

A continuación se indican los PSC soportados por Platino así como los tipos de certificados admitidos:

- **Fábrica Nacional de Moneda y Timbre (FNMT):** <http://www.fnmt.es>

FNMT-FIS	Certificado de identidad de persona física
FNMT-JUR	Certificados de Persona jurídica para el ámbito tributario

- **Fábrica Nacional de Moneda y Timbre (FNMT-RCM):** <http://www.fnmt.es>

FNMT-SELLO	Certificado emitido para la actuación administrativa automatizada sedes electrónicas. Y generados por la AC-AP
------------	--

- **Camerfirma:** <http://www.camerfirma.com/>

CAM-PF-SW-KPSC	Certificado Cameral de persona física claves almacenadas en software y generadas por el PSC
CAM-PJ-SW-KPSC	Certificado Cameral de persona jurídica, claves almacenadas en software y generadas por el PSC
CAM-PR-SW-KPSC	Certificado Cameral de representante, claves almacenadas en software y generadas por el PSC

- **Dirección General de la Policía (DNIe):** <http://www.dnielectronico.es/>

DNIe-FIRMA	Certificado cuya finalidad es la firma de documentos
DNIe-AUTEN	Certificado para la autenticación del ciudadano

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 61 de 69

- **FirmaProfesional S.A.:** <http://www.firmaprofesional.com/>

FP-SW-JUR	Certificado de persona jurídica
FP-SW-COL	Certificado de colegiado
FP-SW-VIN	Certificado de persona vinculada a una empresa

- **ANF Autoridad de Certificación:** <http://www.anf.es>

ANF-PF	Certificado de persona física
ANF-PJ	Certificado de persona jurídica

### 5.3.2 Tipos de certificados

Según la finalidad del certificado se clasifican de la siguiente manera:

Tipo	Descripción
<b>Persona Física</b>	Certificado de identidad de persona física
<b>Persona Jurídica</b>	Certificado de identidad de persona jurídica o entidades sin personalidad jurídica
<b>Representación</b>	Persona física que representa a una persona jurídica
<b>Persona vinculada</b>	Persona física vinculada a una persona jurídica. No implica una relación de representación

Los certificados admitidos por Platino se clasifican de la siguiente manera:

	Persona Física	Persona Jurídica	Representación	Persona vinculada
<b>FNMT</b>	FNMT-FIS	FNMT-JUR FNMT-SELLO		

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 62 de 69

<b>CAMERFIRMA</b>		CAM-PJ-SW-KPSC	CAM-PR-SW-KPSC	CAM-PF-SW-KPSC
<b>DNie</b>	DNIE-FIRMA DNIE-AUTEN			
<b>Firma Profesional</b>		FP-SW-JUR		FP-SW-COL FP-SW-VIN
<b>ANF</b>	ANF-PF	ANF-PJ		

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 63 de 69

### 5.3.3 Descripción de los campos extraídos del certificado

Campo	Descripción
<b>FullName</b>	Nombre común asignado al titular del certificado según el formato proporcionado por la CA emisora
<b>NIF</b>	Código de identificación del titular o representante
<b>NombreCompleto</b>	Nombre completo con el formato "Nombre Apellido1 Apellido2"
<b>Nombre</b>	Nombre del titular del certificado o representante
<b>Apellidos</b>	Apellidos del titular del certificado o representante
<b>Apellido1</b>	Primer apellido del titular del certificado o representante
<b>Apellido2</b>	Segundo apellido del titular del certificado o representante
<b>CIF</b>	Código de identificación
<b>Entidad</b>	Razón Social de la persona jurídica o entidad sin personalidad jurídica
<b>Email</b>	Correo electrónico del titular del certificado o representante
<b>Cargo</b>	Cargo del titular del certificado o representante dentro de la organización
<b>Departamento</b>	Departamento al que pertenece el titular del certificado o representante dentro de la organización
<b>Tipo</b>	Indica el tipo de certificado. Puede contener los siguientes valores: PF: Persona física PJ: Persona jurídica PV: Persona vinculada REP: Representación
<b>Finalidad</b>	Indica si el certificado es válido para: F: Firma A: Autenticación FA: Firma y Autenticación
<b>Organizacion</b>	Entidad emisora del certificado
<b>SerialNumber*</b>	Número de serie del certificado

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 64 de 69

<b>Issuer*</b>	Autoridad emisora del certificado
<b>Subject*</b>	Asunto del certificado
<b>NotBefore*</b>	Fecha de inicio de validez del certificado
<b>NotAfter*</b>	Fecha de fin de validez del certificado

\*Campos extraídos directamente del certificado

### 5.3.4 Información extraída de cada tipo de certificado

#### Fábrica Nacional de Moneda y Timbre (FNMT)

Campo	Descripción	
	FNMT-FIS	FNMT-JUR
<b>FullName</b>	Nombre , apellidos y NIF del suscriptor	Denominación o Razón social de la persona jurídica suscriptora
<b>NombreCompleto</b>	Nombre y apellidos del suscriptor	Nombre y Apellidos del solicitante
<b>Nombre</b>	Nombre del suscriptor	Nombre del solicitante
<b>NIF</b>	NIF del suscriptor	NIF del solicitante
<b>Apellidos</b>	Apellidos del suscriptor	Apellidos del solicitante
<b>Apellido1</b>	Primer apellido del suscriptor	Primer apellido del solicitante
<b>Apellido2</b>	Segundo apellido del suscriptor	Segundo apellido del solicitante
<b>Email</b>	Email del suscriptor	Email del solicitante
<b>Entidad</b>		Denominación o Razón social de la persona jurídica suscriptora
<b>CIF</b>		CIF de la persona jurídica suscriptora
<b>Cargo</b>		
<b>Departamento</b>		
<b>Organizacion</b>	"FNMT"	
<b>Tipo</b>	"PF"	"PJ"
<b>Finalidad</b>	"FA"	

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 65 de 69

## Fábrica Nacional de Moneda y Timbre (FNMT-RCM)

Campo	Descripción
	<b>FNMT-SELLO</b>
<b>FullName</b>	Denominación o Razón social de la persona jurídica suscriptora
<b>NombreCompleto</b>	
<b>Nombre</b>	
<b>NIF</b>	
<b>Apellidos</b>	
<b>Apellido1</b>	
<b>Apellido2</b>	
<b>Email</b>	
<b>Entidad</b>	
<b>CIF</b>	CIF de la persona jurídica suscriptora
<b>Cargo</b>	
<b>Departamento</b>	Nombre del órgano de la entidad suscriptora para el que se emitió el certificado
<b>Organizacion</b>	"FNMT-RCM"
<b>Tipo</b>	"Pj"
<b>Finalidad</b>	"FA"

## Camerfirma

Campo	Descripción		
	CAM-PF-SW-KPSC	CAM-PJ-SW-KPSC	CAM-PR-SW-KPSC
<b>FullName</b>	Nombre y apellidos del titular	Organización representada	
<b>NombreCompleto</b>	Nombre y apellidos del titular	Nombre y apellidos del representante	
<b>Nombre</b>	Nombre del titular	Nombre del representante	
<b>NIF</b>	NIF del titular	NIF del representante	
<b>Apellidos</b>	Apellidos del titular	Apellidos del representante	
<b>Apellido1</b>			
<b>Apellido2</b>			
<b>Email</b>	Email del titular	Email del representante	

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 66 de 69

<b>Entidad</b>	Organización a la que pertenece el titular	Organización representada		
<b>CIF</b>	CIF de la organización	CIF de la organización representada		
<b>Cargo</b>	Cargo del titular	Cargo del representante		
<b>Departamento</b>	Departamento del titular	Departamento del representante		
<b>Organizacion</b>	"AC Camerfirma SA"			
<b>Tipo</b>	"PV"	"PJ"	"REP"	
<b>Finalidad</b>	"FA"			

### Dirección General de la Policía (DNIE)

Campo	Descripción	
	DNIE-FIRMA	DNIE-AUTEN
<b>FullName</b>	Apellido1 Apellido2, Nombre (finalidad)	
<b>NombreCompleto</b>	Nombre y apellidos del ciudadano (formato: n a1 a2)	
<b>Nombre</b>	Nombre del ciudadano	
<b>NIF</b>	NIF del ciudadano	
<b>Apellidos</b>	Apellidos del ciudadano	
<b>Apellido1</b>	Primer apellido	
<b>Apellido2</b>	Segundo apellido	
<b>Email</b>		
<b>Entidad</b>		
<b>CIF</b>		
<b>Cargo</b>		
<b>Departamento</b>		
<b>Organizacion</b>	"DIRECCION GENERAL DE LA POLICIA"	
<b>Tipo</b>	"PF"	
<b>Finalidad</b>	"F"	"A"

### FirmaProfesional S.A

Campo	Descripción
-------	-------------



	<b>FP-SW-JUR</b>	<b>FP-SW-COL</b>	<b>FP-SW-VIN</b>
<b>FullName</b>	Razón Social	Nombre, apellidos y nº de colegiado	Nombre y Apellidos
<b>NombreCompleto</b>	Nombre y apellidos del responsable	Nombre y apellidos del suscriptor	
<b>Nombre</b>	Nombre del responsable	Nombre del suscriptor	
<b>NIF</b>	NIF del responsable	NIF del suscriptor	
<b>Apellidos</b>	Apellidos del responsable	Apellidos del suscriptor	
<b>Apellido1</b>			
<b>Apellido2</b>			
<b>Email</b>	Email del solicitante	Email del suscriptor	
<b>Entidad</b>	Razón Social	Colegio Oficial que actúa como RA	Entidad a la que está vinculada
<b>CIF</b>	CIF/NIF del titular del certificado		CIF de la organización
<b>Cargo</b>		Título o especialidad	Cargo, título o rol del suscriptor
<b>Departamento</b>		Estatus colegial "Colegiado"	Departamento o tipo de vinculación
<b>Organizacion</b>	"Firmaprofesional S.A."		
<b>Tipo</b>	"PJ"	"PV"	
<b>Finalidad</b>	"FA"		

## ANF Autoridad de Certificación

<b>Campo</b>	<b>Descripción</b>	
	<b>ANF-PF</b>	<b>ANF-PJ</b>
<b>FullName</b>	Nombre y Apellidos del titular	Razón Social
<b>NombreCompleto</b>	Nombre y apellidos del titular	Nombre y apellidos del responsable
<b>Nombre</b>	Nombre del titular	Nombre del responsable
<b>NIF</b>	NIF del titular	NIF del responsable
<b>Apellidos</b>	Apellidos del titular	Apellidos del responsable
<b>Apellido1</b>	Apellidos del titular	Apellidos del responsable
<b>Apellido2</b>		

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 68 de 69

<b>Email</b>	Email del titular	Email del responsable
<b>Entidad</b>		Razón Social
<b>CIF</b>		CIF de la entidad
<b>Cargo</b>	Título profesional	Cargo del representante
<b>Departamento</b>		
<b>Organizacion</b>	" ANF Autoridad de Certificacion"	
<b>Tipo</b>	"PF"	"PJ"
<b>Finalidad</b>	"FA"	

## 6 EJEMPLO DE INTEGRACIÓN

A continuación se explica como se debe realizar la integración de una aplicación web con el cliente de firma.

Como ejemplo de integración de una aplicación web con los servicios ejecutados en el cliente del Servicio de Firma Electrónica y Sellado de Tiempo, se proporciona un WAR con las clases y librerías necesarias.

### 6.1 CONFIGURACIÓN

La configuración de la aplicación web requiere asignar valores a ciertos ficheros de propiedades:

- Fichero: config.properties
  - Ubicación: WEB-INF/classes
  - Propiedad a modificar: applicationID
  - Descripción: Identificador de la aplicación que consumirá el servicio de firma.
- Fichero: asf\_securityagent.properties
  - Ubicación: WEB-INF/classes/propertyFiles
  - Propiedad a modificar: com.tbsolutions.asf.securityagent.fileclient
  - Descripción: En esta propiedad hay que colocar la ruta absoluta donde se copiará el fichero client-config.wsdd (existente en el directorio WEB-INF).
  - Propiedad a modificar: com.tbsolutions.asf.securityagent.keystoreFile

 <b>Gobierno de Canarias</b> Consejería de Presidencia, Justicia e Igualdad	 <b>Platino</b> Plataforma de Interoperabilidad del Gobierno de Canarias
Vol. IV Manual del desarrollador Servicio de Firma Electrónica y Sellado de Tiempo	Página 69 de 69

- Descripción: En esta propiedad hay que colocar la ruta absoluta donde se copiará el fichero `firma_peticiones.jks` (existente en el directorio WEB-INF).
- Fichero: JBean.properties
  - Ubicación: WEB-INF/classes/propertyFiles
  - Propiedad a modificar: `jfactory.util.Log.nombreFicheroLog`
  - Descripción: En esta propiedad hay que colocar la ruta absoluta donde deseamos que se almacenen los ficheros de log.
  - Propiedad a modificar: `jfactory.util.Log.nombreFicheroTraza`
  - Descripción: En esta propiedad hay que colocar la ruta absoluta donde deseamos que se almacenen los ficheros de traza.
  - Propiedad a modificar: `log4j.appender.FICH.File`
  - Descripción: En esta propiedad hay que colocar la ruta absoluta donde deseamos que se almacenen los ficheros de log del PlatinoWebSigner.