7. @FIRMA

7.1 Introducción

@FIRMA es la plataforma corporativa de la Junta de Andalucía para autenticación y firma electrónica. Permite incorporar procesos de autenticación y firmado digital mediante el uso de certificados digitales, independientemente del entorno de desarrollo en que hayan sido programadas.

@FIRMA es de libre uso y sin coste adicional para cualquier Consejería, Organismo de la Junta de Andalucía o Administración pública que lo solicite. La versión usada para el desarrollo del proyecto es la versión 5.0, que respecta nuevas capacidades y funcionalidades con respecto a la versión anterior, la 4.0.

En este caso, la plataforma @firma ya se encuentra instalada en un servidor de aplicaciones de la administración para la que va dirigida el proyecto, por lo que lo único necesario será saber cómo utilizar los servicios que proporciona.

A continuación, resumiremos brevemente los servicios proporcionados por @firma y que será usados en el desarrollo de este proyecto. Todos los servicios utilizados serán habilitados como servicios web.

7.2 Servicios proporcionados

7.2.1 Validación de firmas electrónicas

Este servicio permite realizar una validación completa de la Firma Electrónica proporcionada. Como validación completa se entiende:

- Validación de la firma digital contenida en la Firma Electrónica frente a los datos proporcionados.

- Validación del certificado X.509 empleado y contenido en la Firma Electrónica. Se validará su integridad, periodo de validez y estado de revocación. Tanto el periodo de validez como el estado de revocación del certificado se comprueban frente a la fecha actual en caso que la Firma Electrónica no posea sello de tiempo o frente al mismo en caso contrario.

- Soporte del certificado. Se comprueba que el certificado y su emisor sean reconocidos y soportados por la plataforma.

Este servicio puede ser empleado para validar tanto las Firmas Electrónicas generadas por la plataforma como aquellas ajenas a @firma 5.0, siempre y cuando su formato sea soportado.

La información que se puede enviar al servicio es:

- Firma Electrónica. Puede haber sido generada de forma implícita (con los datos incrustados en la Firma Electrónica) o explícita (los datos no van incluidos). Formato de la Firma Electrónica (opcional) debe ser alguno de los soportados por la plataforma: PKCS7 v.1.5, CMS, XMLDSignature, XAdES, XAdES-BES y XAdES-T. En caso de no indicarse, se supone CMS.

- Datos (opcional). Son los datos originales sobre los cuales se calculó la Firma Electrónica. Necesarios en caso que la Firma Electrónica sea explícita.

- Hash y Algoritmo de hash (opcional). En caso que los datos sean muy grandes, o simplemente se desee optimizar la comunicación con la plataforma, se puede enviar el hash de los datos anteriores en vez de los datos en sí. En ese caso es necesario indicar el algoritmo de hash empleado para el cálculo de dicho hash.

A continuación, una imagen que ilustra la explicación anterior:

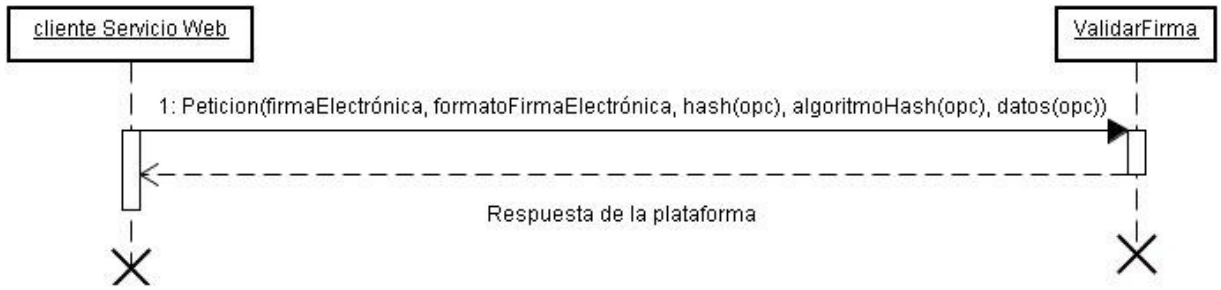

Figura 7.1. Proceso de Validación de la firma electrónica

En la ilustración anterior:

- El cliente WS envía la petición al servicio Web ValidarFirma de la plataforma @firma 5.0 con la información necesaria.

- El servicio Web devuelve el resultado de la validación.

7.2.3 Almacenar un documento

Este servicio permite a una aplicación cliente registrar un documento junto con cierta información referente a él en la plataforma @firma 5.0. Es el primer paso para llevar a cabo procesos de Firma Electrónica sobre dicho documento.

La información que recibe este servicio es la siguiente:

- Documento. Es el documento a registrar.

- Nombre del documento (opcional). Es el nombre del documento.

- Tipo de documento (opcional). Es el tipo (extensión) del documento.

Tras invocar a este servicio se obtendrá un identificador único asociado al documento registrado. Este identificador se podrá emplear tanto en subsiguientes servicios de acceso a Custodia como en servicios de Firma Electrónica de la plataforma.

7.2.4 Firma electrónica de usuario en tres fases

El diagrama que se muestra a continuación representa un proceso de Firma Electrónica de Usuario simple en el cual el documento a firmar no se encuentra registrado en la plataforma, por lo que es necesario proceder previamente a su registro.

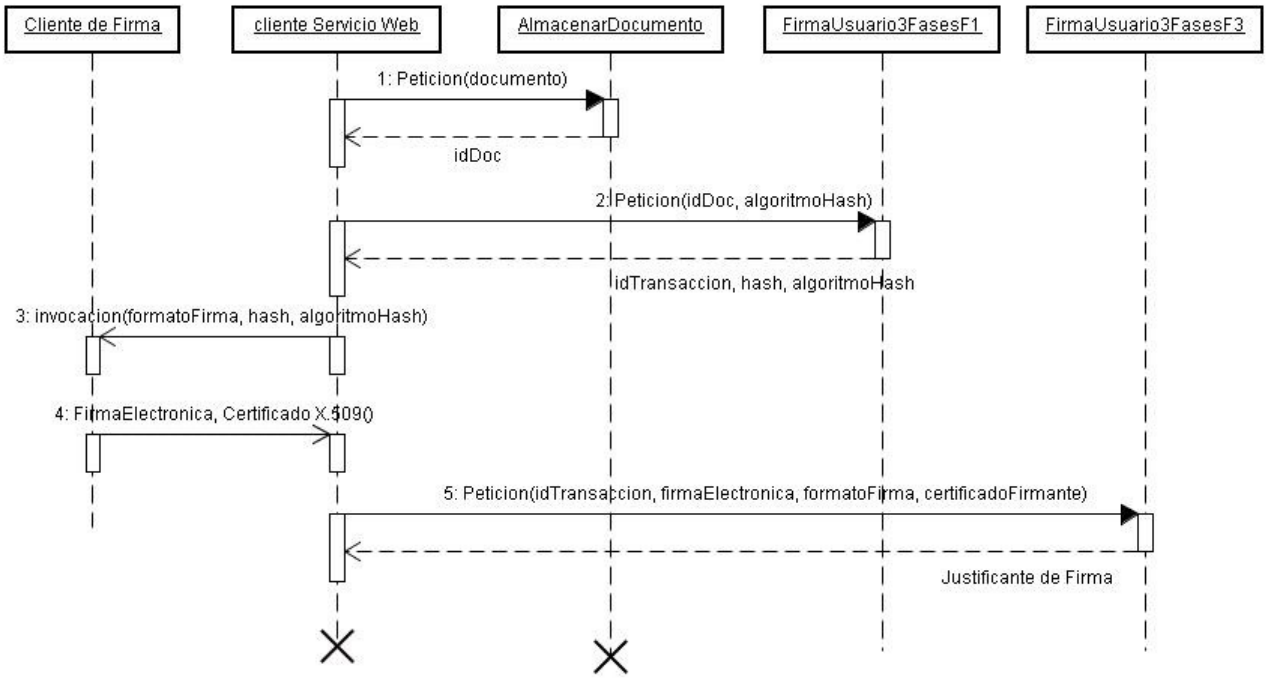

Figura 7.2. Proceso de Firma3Fases

1. El cliente WS envía la petición al servicio Web AlmacenarDocumento de la plataforma @firma 5.0, con el fin de registrar el documento a firmar.

2. El servicio Web devuelve el identificador del documento tras su registro.

3. El cliente WS envía la petición al servicio Web FirmaUsuario3FasesF1, con el identificador del documento anterior y el algoritmo de hash con el que se desea realizar la Firma Electrónica.

4. El servicio Web devuelve tanto el hash del documento indicado como el algoritmo de Hash empleado en el cálculo (se corresponde con el parámetro de entrada al servicio). Además se

obtiene el identificador de la transacción que permitirá finalizar este modo de firma en la tercera y última fase.

5. El cliente WS debe pasar al Cliente de Firma (mediante la aplicación Web propia de la aplicación cliente) la información obtenida del paso anterior así como el formato de la Firma Electrónica que se desee generar (debe ser un formato soportado por el cliente de Firma: CMS, XMLDSignature o XadES-BES).

6. Se ejecutará la lógica del Cliente de Firma.

7. La aplicación Web debe devolver al cliente WS la información generada por el Cliente de Firma, es decir, la Firma Electrónica y el Certificado X.509 empleado.

8. El Cliente WS envía la petición al servicio Web FirmaUsuario3FasesF3 con la información necesaria para poder finalizar el proceso de Firma de Usuario en 3 Fases.

9. El servicio Web devuelve el Justificante de Firma Electrónica generado por la plataforma.