Firma Electrónica en Dispositivos Móviles

Trabajo Final de Máster

Máster Interuniversitario de Seguridad de las Tecnologías de la Información y de las Comunicaciones

David Alcaraz Pérez

ÍNDICE

1. OBJETIVOS

El objetivo del presente trabajo es el estudio de las distintas opciones disponibles en el mercado para la creación de firma electrónica en dispositivos móviles, así como la implementación de software capaz de generar firma electrónica cualificada de acuerdo con lo establecido en el Reglamento Europeo por el cual se definen y regulan los aspectos básicos de la firma electrónica para los estados miembros.

2. INTRODUCCIÓN A LA FIRMA ELECTRÓNICA

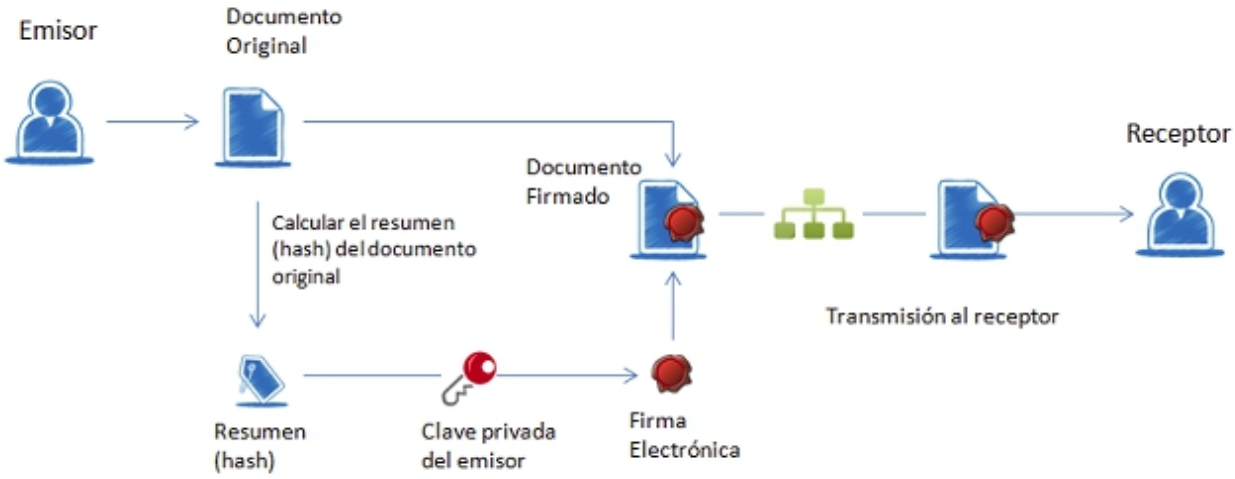
La firma electrónica es **un conjunto de datos electrónicos** que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

• Identificar al firmante de manera inequívoca

• Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación

• **Asegurar la integridad del documento firmado.** Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento.

Para firmar un documento es necesario disponer de un certificado digital o de un DNI electrónico como sucede en España. El certificado electrónico o el DNI electrónico contiene unas claves criptográficas que son los elementos necesarios para firmar. Los certificados electrónicos tienen el objetivo de identificar inequívocamente a su poseedor y son emitidos por Proveedores de Servicios de Certificación.



El proceso básico que se sigue para la firma electrónica es el siguiente:

• El usuario dispone de un documento electrónico (una hoja de cálculo, un pdf, una imagen, incluso un formulario en una página web) y de un certificado que le pertenece y le identifica.

• La aplicación o dispositivo digital utilizados para la firma realiza un resumen del documento. El resumen de un documento de gran tamaño puede llegar a ser tan solo de unas líneas. Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.

• La aplicación utiliza la clave contenida en el certificado para codificar el resumen.

• La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este nuevo documento es la firma electrónica.

El resultado de todo este proceso es un documento electrónico obtenido a partir del documento original y de las claves del firmante. La firma electrónica, por tanto, es el mismo documento electrónico resultante.

3. FIRMA ELECTRÓNICA EN ESPAÑA

La base legal de la Firma electrónica en el ámbito español está recogida en la *Ley 59/2003 de Firma Electrónica,* donde se recoge, por ejemplo que:

Art. 3.1) La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Art. 3.2) La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

(Art. 3.3) Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

En ocasiones, esta firma se denomina Cualificada por traducción del término *Qualified* de la Directiva Europea de Firma Electrónica. Según la ley, la **firma electrónica reconocida** es la única que puede ser considerada equivalente a la firma manuscrita:

(Art. 3.4) La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor que la firma manuscrita en relación con los consignados en papel.

FIRMA ELECTRÓNICA RECONOCIDA

Una firma electrónica reconocida debe cumplir las siguientes propiedades o requisitos:

• Identificar al firmante.

• Verificar la integridad del documento firmado.

• Garantizar el no repudio en el origen.

• Contar con la participación de un tercero de confianza.

• Estar basada en un certificado electrónico reconocido.

• Debe de ser generada con un dispositivo seguro de creación de firma.

Los 4 primeros puntos son posibles gracias al uso de las claves criptográficas contenidas en el certificado y a la existencia de una estructura de Autoridades de Certificación que ofrecen confianza en la entrega de los certificados. Pero según la Ley 59/2003, esos 4 puntos sólo nos ofrecen una firma avanzada.

Para que la firma electrónica sea equivalente a la manuscrita, es decir, que una Firma electrónica sea reconocida, debe además:

Estar basada en un Certificado Reconocido

El certificado debe haber sido reconocido por el Ministerio de Industria y Comercio como habilitado para crear firmas reconocidas y debe estar listado en su página web como tal.

Se pueden ver todos los certificados reconocidos por el MITyC en la dirección https://sedeaplicaciones2.minetur.gob.es/prestadores/

Son certificados reconocidos porque tanto el prestador que los emite como el contenido mismo del certificado, cumplen con los requisitos declarados en el Capítulo II de la Ley 59/2003 de firma electrónica sobre Certificados reconocidos.

Ser generada con un dispositivo seguro de creación de firma

Las características de un dispositivo seguro de creación de firma están recogidas en el artículo 24 de la Ley 59/2003 de Firma Electrónica.

Principalmente, el dispositivo seguro debe garantizar que las claves sean únicas y secretas, que la clave privada no se puede deducir de la pública y viceversa, que el firmante pueda proteger de forma fiable las claves, que no se altere el contenido del documento original y que el firmante pueda ver qué es lo que va a firmar.

Desde un punto de vista técnico, según el artículo 27 de la Ley 59/2003, un dispositivo seguro de firma debe ser certificado como que cumple las características anteriores según las normas técnicas publicadas en la Decisión 2003/511/CE, de 14 de julio de 2003 de la Comisión Europea.

El DNI Electrónico es considerado un dispositivo seguro de firma y por tanto, las firmas generadas con él, son reconocidas y tienen la misma validez que la firma manuscrita.

4. FIRMA ELECTRÓNICA EN EUROPA

El Reglamento Europeo de Firma Electrónica (eIDAS) tiene un gran impacto en la actividad de Firma profesional y los servicios de confianza que presta. Es un reglamento de aplicación inmediata en los estados miembros que pasa a sustituir y ampliar la antigua Directiva de Firma Electrónica.

El citado reglamento es el **REGLAMENTO (UE) No 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior** y por la que se deroga la Directiva 1999/93/CE.

El objetivo del Reglamento es el establecimiento de un marco jurídico claro que garantice el reconocimiento transfronterizo de identidades electrónicas, la interoperabilidad de la firma electrónica y otros servicios de confianza tales como los sellos electrónicos o los sellos de tiempo, posibilitando las comunicaciones electrónicas entre ciudadanos, empresas y Administraciones públicas y potenciando el comercio y la administración electrónica.

El nuevo reglamento se divide en dos grandes bloques:

I.- IDENTIFICACIÓN ELECTRÓNICA Sistemas (nacionales) de identificación electrónica: notificación; publicación de la lista en el Diario Oficial de la UE; interoperabilidad; cooperación entre Estados miembros. Medios de identificación electrónica expedidos por los sistemas de identificación electrónica notificados: niveles de seguridad **(bajo, sustancial y alto)**; reconocimiento mutuo por los servicios prestados en línea por los organismos públicos (a efectos de la autenticación transfronteriza).

II.- SERVICIOS DE CONFIANZA. El servicio electrónico prestado (por un prestador de servicios de confianza) habitualmente a cambio de una remuneración, consistente en:

–> la creación, verificación y validación de **firmas electrónicas, sellos electrónicos** o **sellos de**

tiempo electrónicos, **servicios de entrega** electrónica certificada y **certificados** relativos a estos servicios, o

> –> **la creación, verificación y validación de certificados** para la autenticación de sitios web, o
>
> –> la **preservación de firmas**, sellos o certificados electrónicos relativos a estos servicios.

Servicios de confianza cualificados (prestados por prestadores cualificados de servicios de confianza): aspectos internacionales (reconocimiento en la UE de servicios originarios de un tercer país en virtud de un acuerdo); supervisión (por un organismo de supervisión nacional, que los certifica como cualificados); auditorias (por un organismo de evaluación de conformidad nacional); publicación en listas de confianza nacionales (TSL); obtiene una etiqueta de confianza «UE».

Firmas electrónicas: firmante (una persona física); firma electrónica avanzada (se cambia el requisito "haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo").

Firmas electrónicas cualificadas: definición (firmas electrónicas avanzadas que se crean mediante un dispositivo cualificado de creación de firmas electrónicas y que se basan en un certificado cualificado de firma electrónica); efectos jurídicos (equivalentes a las firmas manuscritas; reconocimiento en todos los Estados miembros); requisitos de los certificados cualificados de firma electrónica; requisitos de la validación; servicio de validación cualificado; servicio cualificado de conservación.

Dispositivos cualificados de creación de firmas electrónicas: requisitos; certificación (por organismos públicos o privados nacionales); publicación en una lista (por la Comisión); servicios de firma electrónica cualificada a distancia.

Sellos electrónicos: creador de un sello (una persona jurídica); sello electrónico avanzado (mismos requisitos que firma electrónica avanzada).

Sellos electrónicos cualificados: definición (igual que firmas electrónicas cualificadas); efectos jurídicos (presunción de integridad de los datos vinculados y de certeza de su origen; reconocimiento en todos los Estados miembros); requisitos de los certificados cualificados de sello electrónico (iguales a los requisitos de los certificados cualificados de firma electrónica); validación y conservación (igual que en firmas electrónicas cualificadas); dispositivos cualificados de creación de sello electrónico (iguales que dispositivos cualificados de creación de firmas electrónicas).

Sellos cualificados de tiempo electrónicos: efectos jurídicos (presunción de exactitud de la fecha y hora y de la integridad de los datos vinculados).

Servicios cualificados de entrega electrónica certificada: efectos jurídicos de los datos enviados y recibidos (presunción de la integridad, el envío por el remitente identificado, la recepción por el

destinatario identificado y la exactitud de la fecha y hora de envío y recepción).

Requisitos de los certificados cualificados de autenticación de sitios web: iguales a los requisitos de los certificados cualificados de firma electrónica.

5. FORMATOS DE FIRMA ELECTRÓNICA

El formato de firma es la forma como se genera el documento de firma y como se guarda o estructura la información de firma en el documento generado.

La existencia de múltiples formatos de firma se debe a razones históricas, a cómo se ha ido introduciendo la firma en formatos de documentos ya existentes y a cómo se han ido añadiendo funcionalidades a lo largo del tiempo.

Un fichero de firma tiene un formato que viene determinado por estos aspectos:

- Estructura del fichero: formatos CAdES, XAdES, PAdES, OOXML, ODF…
- ¿Dónde se guarda el documento original?
- Firmas con múltiples usuarios.
- Longevidad de la firma y sello de tiempo

Estructura de la firma: CAdES, XAdES, PAdES, OOXML, ODF…

Una firma electrónica es un fichero que contiene información sobre el documento original, el firmante, la fecha de la firma, algoritmos utilizados y posible caducidad de la firma.

Cómo se estructura esta información (el orden de esa información dentro del fichero, las etiquetas que indican cuando empieza un campo y cuando termina, la opcionalidad de esos campos, etc.) viene determinado por distintos formatos:

- CAdES (CMS Avanzado).
  Es la evolución del primer formato de firma estandarizado. Es apropiado para firmar ficheros grandes, especialmente si la firma contiene el documento original porque optimiza el espacio de la información. Tras firmar, no podrás ver la información firmada, porque la información se guarda de forma binaria.

- XAdES (XML Avanzado).
  El resultado es un fichero de texto XML, un formato de texto muy similar al HTML que

utiliza etiquetas. Los documentos obtenidos suelen ser más grandes que en el caso de CAdES, por eso no es adecuado cuando el fichero original es muy grande. Aplicaciones como eCoFirma del Ministerio de Industria y Comercio, sólo firman en XadES.

- PAdES (PDF Avanzado).
  Este es el formato más adecuado cuando el documento original es un pdf. El destinatario de la firma puede comprobar fácilmente la firma y el documento firmado. Con los formatos anteriores esto no es posible si no se utilizan herramientas externas.

- OOXML y ODF.
  Son los formatos de firma que utilizan Microsoft Office y Open Office, respectivamente.
  Algunas aplicaciones de firma dejan elegir el formato a utilizar (@Firma). Otras imponen siempre el mismo formato (eCoFirma) y otras deciden automáticamente el formato en función del formato original del documento a firmar (@FirmaFácil).

Según cómo se referencie o dónde se guarde el documento original en el fichero de firma, podemos tener dos casos:

El documento original se incluye **en el fichero de firma.**

Ventaja: No es necesario guardar siempre el documento original y el documento de firma porque aquél ya está incluido en éste. Es, por tanto, un formato cómodo de almacenar.

Desventaja: Si el tamaño del fichero es elevado, se consume más espacio de almacenamiento, porque al final se acaba teniendo por un lado el documento original, que siempre habrá que guardarlo, y por otro, la firma.

En el caso de CAdES estas firmas se llaman firmas implícitas.

En el caso de firmas **XAdES XML**, lo habitual es que el documento esté incluido en el fichero de firma. Hablamos de firmas **despegadas (detached), envolventes (enveloping) y envueltas (enveloped)** según en qué sitio del propio fichero de firma se guarde el documento original.

En la práctica, se suele utilizar el caso 1, que es la forma de funcionar por defecto de las aplicaciones de firma. Se obtienen ficheros de firma más grandes pero, como contrapartida, no requiere almacenar el fichero original como otro documento aparte junto al de firma.

El documento no se incluye **en la firma**.

En este caso, el documento no se incluye en el resultado de firma o solamente se **incluye una referencia al lugar** en el que se encuentra para que el documento pueda ser localizado.Por tanto, se obtienen **ficheros de tamaño más reducido**, pero, por el contrario, el **documento original siempre hay que guardarlo junto a la firma.**

En el caso de CAdES estas firmas se llaman **firmas explícitas.**

En el caso de firmas XAdES XML, sólo para las **firmas despegadas (detached)**, el documento puede estar fuera.

6. VERIFICACIÓN DE FIRMA

Para verificar una firma es necesario:

- Comprobar la integridad de los datos firmados asegurando que éstos no hayan sufrido ninguna modificación.

- Comprobar que el estado del certificado con el que se firmó era el correcto, es decir, era vigente en el momento de la operación.

En el caso de la firma electrónica básica, si el certificado está caducado automáticamente se da la firma como no válida.

Entonces, ¿cómo sabemos que el certificado estaba vigente o no en la fecha en la que se firmó? Y ¿qué debe hacerse para que cuando se quiera validar o verificar una firma en el futuro la validación sea posible aunque esté caducado el certificado?

Para dar respuesta a estas preguntas, los formatos AdES (forma genérica de llamar a los formatos CAdES, XAdES y PAdES) contemplan la posibilidad de incorporar a las firmas electrónicas información adicional que garantiza la validez de una firma a largo plazo, una vez vencido el periodo de validez del certificado.

Estos formatos añaden a la firma evidencias de terceros (de autoridades de certificación) y certificaciones de tiempo,que realmente certifican cuál era el estado del certificado en el momento de la firma.

Concretamente, existen distintos formatos de firma que van incrementando la calidad de la misma hasta conseguir una firma que pueda ser verificada a largo plazo (de forma indefinida) con plenas

garantías jurídicas:

- Firma Básica (AdES - BES), es el formato básico para satisfacer los requisitos de la firma electrónica avanzada.
- AdES T, se añade un sellado de tiempo (T de TimeStamp) con el fin de situar en el tiempo el instante en que se firma un documento.
- AdES C, añade un conjunto de referencias a los certificados de la cadena de certificación y su estado, como base para una verificación longeva (C de Cadena).
- AdES X, añade sellos de tiempo a las referencias creadas en el paso anterior (X de eXtendida).
- AdES XL, añade los certificados y la información de revocación de los mismos, para su validación a largo plazo (XL de eXtendido Largo plazo).
- AdES A, permite la adición de sellos de tiempo periódicos para garantizar la integridad de la firma archivada o guardada para futuras verificaciones (A de Archivo).

7. FIRMA ELECTRÓNICA EN DISPOSITIVOS MÓVILES

La posesión de un certificado digital que permita realizar firma electrónica reconocida permite a su titular disfrutar de multitud de funcionalidades y servicios on-line. Con la firma electrónica móvil, el objetivo es llevar la firma electrónica al campo de la movilidad.

Los equipos portátiles cada vez son más pequeños y la línea entre un ordenador personal portátil y una PDA es cada vez más difusa. En este último caso las capacidades de estos dispositivos se parecen mucho a las que podríamos tener en un ordenador portátil y por lo tanto, la ejecución de aplicativos en una u otra plataforma no se diferencian. En una PDA podemos encontrarnos con versiones reducidas pero funcionales de los clientes de correo y aplicaciones ofimáticas que tenemos en nuestro ordenador de sobremesa.

En estos casos, los procesos de firma apenas se distinguen excepto por la limitación de la pantalla y por la dificultad de conexión con elementos externos como lectores de tarjetas criptográficas.

Claves criptográficas en SIM

Para la realización de firma electrónica con teléfonos móviles clásicos, los operadores de telefonía móvil han desarrollado una plataforma de firma que utilizan tarjetas SIM con capacidades criptográficas, pudiendo generar y almacenar en ellas claves y certificados de propiedad de dichas claves, es decir los certificados digitales. Todo esto permite la realización de firmas electrónicas de documentos y transacciones utilizando nuestro teléfono móvil como dispositivo de firma.

Para realizar firmas electrónicas de documentos y transacciones desde un teléfono móvil es necesario tener:

- Una tarjeta SIM criptográfica de al menos 128K, ya que las tarjetas convencionales de 64K no soportan firma electrónica. Para verificar si se tiene o no una tarjeta compatible el usuario deberá extraer la misma del terminal y comprobar la información referente a la capacidad de la misma. En caso de no tener la tarjeta SIM adecuada, deberá ponerse en contacto con su operador telefónico
- Un certificado emitido por una autoridad de certificación que tenga conexión con la plataforma del operador de telefonía móvil del cliente.

Los actores en el proceso de generación y uso de la firma digital en el móvil son:

- **El operador telefónico**, que es quien dispone de la infraestructura de comunicaciones necesaria y ofrece a los clientes una solución de firma móvil así como la adquisición de las tarjetas SIM criptográficas. Actualmente, algunos operadores de telefonía ya disponen de

soluciones de firma electrónica móvil.

- **La autoridad de certificación**, que es quien genera las claves pública y privada asociadas al certificado digital que permite realizar firma electrónica reconocida, conforme a los requerimientos legales establecidos por la LFE. Además, la autoridad certificadora deberá validar las consultas acerca del estado de vigencia de los certificados.
- **El usuario final**, que posee el dispositivo móvil y es titular de la clave privada integrada en la tarjeta SIM criptográfica.
- **Proveedores de servicios** que disponen de aplicaciones de firma móvil que dialogan con la solución del operador telefónico y presentan solicitudes a los usuarios finales del servicio

Claves criptográficas en microSD

Diversas empresas han desarrollado tarjetas de memoria que permiten disponer de completa funcionalidad smartcard en base a hardware en estandard micro SD o MMC, que utilizan ya todos los dispositivos móviles y teléfonos *(excepto Apple)*. Los formatos aceptados incluyen micro SD, y adaptadores para soportar formato SD o miniSD o USB. Tambien estan disponibles MultiMedia Card (MMC) o MultiMedia Card (RSMMC) de tamaño reducido.

Las funciones de Firma Digital y cifrado seguras basadas en tarjeta inteligente son posibles en dispositivos móviles, PDAs, Smartphones y teléfonos, esta solución proporciona una forma eficiente de permitir disponer de seguridad de datos para el sector financiero, tecnología, e infraestructuras PKI en toda clase de dispositivos portátiles incluyendo portátiles, PDAs y smartphones.

La memoria flash y el controlador criptográfico pueden ser accedidos independientemente del terminal en que se usen. Las claves criptográicas pueden ser generadas direcatamente en la tarjeta micro SD sin que nunca tengan que dejar el sistema original, y por tanto nunca son expuestas a riesgo alguno de intercepción o manipulación.

La empresa alemana **G & D** desarrolló la tarjeta *StarSign Mobile Security Card* con las siguientes características:

Technical key features

Chip
- Smart Card Controller
- Common Criteria EAL 5+ certified

Chip operating system
- G&D Sm@rtCafé® Expert 3.2

Memory
- 67 kB free EEPROM

Mass storage capability
- Min. 1 GB flash memory

SD specifications
- SDA Physical Layer Specification 1.10
- SDA Supplementary Notes for Version 1.10 1.0
- SDA microSD Addendum 1.10
- SDA Mobile Commerce Extension 1.10

Java Card specifications
- Java Card™ 2.2.1
- GlobalPlatform 2.1.1

Security
- DPA/SPA and physical attack secured
- Hash algorithms: SHA-1, SHA256, MD5, RIPE-MD160
- Symmetric encryption: DES, 3-DES, AES up to 256 bit, Seed 128 bit
- Asymmetric encryption: RSA® up to 2048 bit (RSA® and RSA®-CRT) DSA up to 1024 bit
- Digital signatures with symmetric / asymmetric encryption
- Enhanced high security memory management

Supported platforms
- Windows® PC
- Windows Mobile™
- Symbian OS
- Linux®

Via PC/SC or similar interface

Available adapters
- microSD™ to miniSD™
- microSD™ to SD

Compatible middleware
- StarSign®

Available smart card tools
- Sm@rtCafé® Professional Toolkit for Application Development
- Sm@rtCafé® Customizer and JLoad for Lifecycle Management

Lector de Tarjetas Criptográficas

Es posible la creación de una firma reconocida en dispositivos móviles de la misma forma que se haría en un PC portátil o sobremesa, haciendo uso de un software específico y de un lector de tarjetas criptográficas, como puede ser el **dnie,** adaptado a este tipo de dispositivos como el que distribuye la empresa española **ViaFirma.**

Firma en el lado del servidor

Dadas las características del nuevo Reglamento Europeo, el cual propicia la creación de firma mediante el uso de claves centralizadas alojadas en **"la nube"**, en contraposición al modelo de claves alojadas en dispositivos *(Tarjeta criptográfica, SIM, sdCard etc.),* es posible desarrollar software para dispositivos móviles capaz de generar firma cualificada sin necesidad de disponer de un dispositivo criptográfico.

El Reglamento Europeo define la firma electrónica cualificada como:

"una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica;"

Siendo una firma electrónica avanzada:

"Una firma que cumple con los siguientes requisitos:

a) estar vinculada al firmante de manera única;

b) permitir la identificación del firmante;

c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y

d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable. "

Por tanto, para poder llevar a cabo una firma electrónica cualificada, podemos alojar en servidor las claves correspondientes a un certificado cualificado de firma electrónica, y realizar la firma con un dispositivo cualificado de creación de firmas electrónicas, el cual debe cumplir los siguientes requisitos:

"1. Los dispositivos cualificados de creación de firma electrónica garantizarán como mínimo, por medios técnicos y de procedimiento adecuados, que:

> ***a) esté garantizada razonablemente la confidencialidad de los datos de creación de firma electrónica utilizados para la creación de firmas electrónicas;***
>
> ***b) los datos de creación de firma electrónica utilizados para la creación de firma electrónica solo puedan aparecer una vez en la práctica;***
>
> ***c) exista la seguridad razonable de que los datos de creación de firma electrónica utilizados para la creación de firma electrónica no pueden ser hallados por deducción y de que la firma está protegida con seguridad contra la falsificación mediante la tecnología disponible en el momento;***
>
> ***d) los datos de creación de la firma electrónica utilizados para la creación de firma electrónica puedan ser protegidos por el firmante legítimo de forma fiable frente a su utilización por otros.***

2. Los dispositivos cualificados de creación de firmas electrónicas no alterarán los datos que deben firmarse ni impedirán que dichos datos se muestren al firmante antes de firmar.

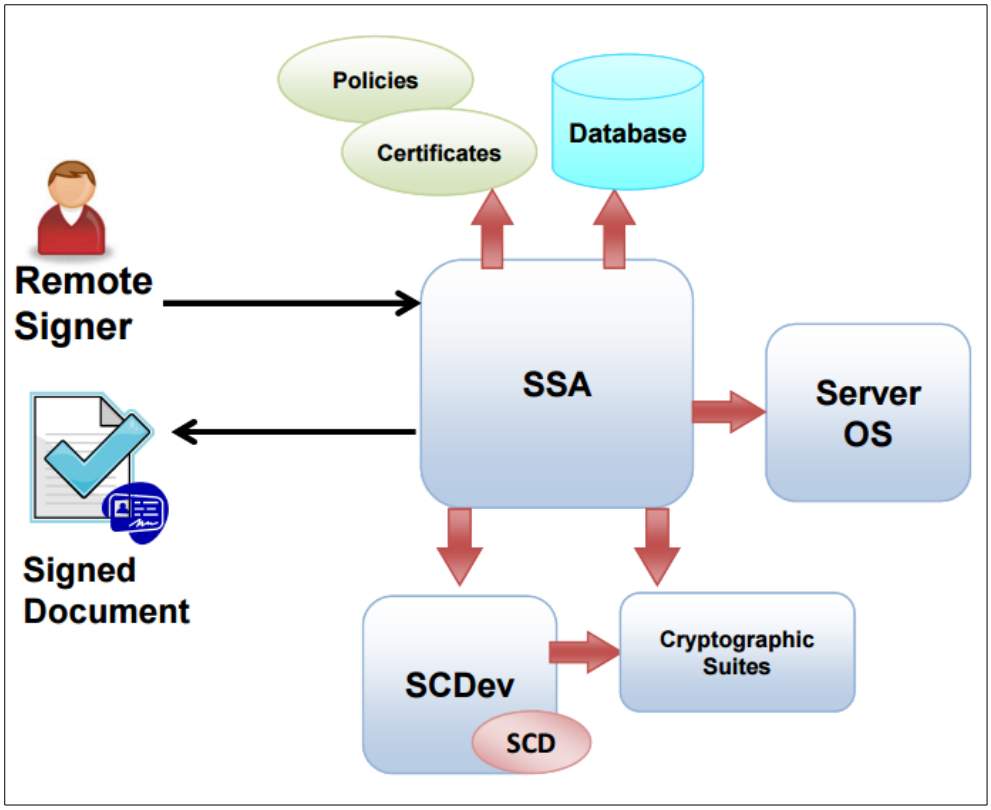
3. La generación o la gestión de los datos de creación de la firma electrónica en nombre del firmante solo podrán correr a cargo de un prestador cualificado de servicios de confianza.

4. Sin perjuicio de la letra d) del punto 1, los prestadores cualificados de servicios de confianza que gestionen los datos de creación de firma electrónica en nombre del firmante podrán duplicar los datos de creación de firma únicamente con objeto de efectuar una copia de seguridad de los citados datos siempre que se cumplan los siguientes requisitos:

> ***a) la seguridad de los conjuntos de datos duplicados es del mismo nivel que para los conjuntos de datos originales;***
>
> ***b) el número de conjuntos de datos duplicados no supera el mínimo necesario para garantizar la continuidad del servicio."***

Siendo, por esto, recomendable utilizar un **Módulo de Segurdad Hardware (HSM)**, para el almacenaje de las claves y/o la generación de las firmas, ya que estos dispositivos pueden tener conectividad SCSI / IP u otras y aportar funcionalidad criptográfica de clave pública (PKI) de alto rendimiento que se efectúa dentro del propio hardware.

Una arquitectura que implemente este modelo, podría ser la siguiente:

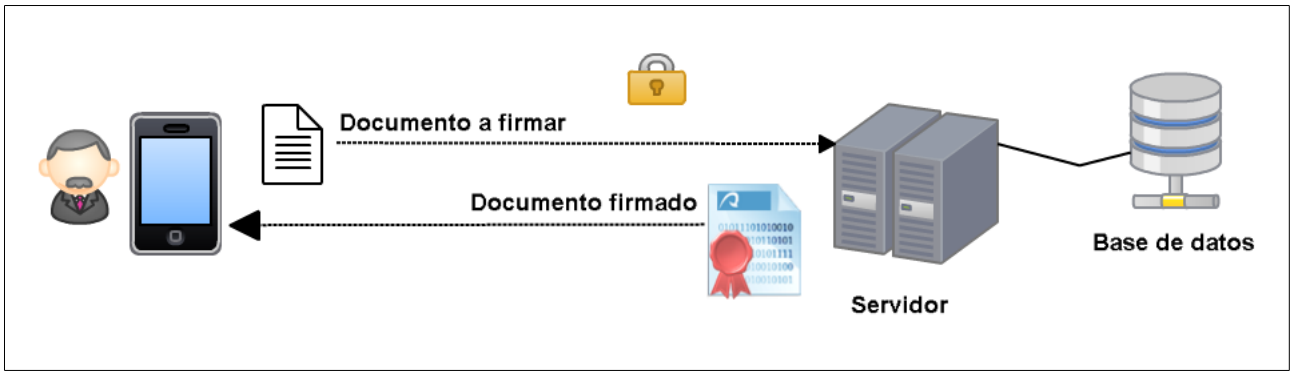


Donde:

- Cliente y servidor **(SSA)** intercambian información a través de un canal seguro.
- Cliente debe autenticarse contra el servidor e implementar algún factor extra de autenticación **(PIN, OTP etc.)** para garantizar la autenticidad con un alto nivel de confianza.
- Se obtiene clave del usuario
- Se genera la firma electrónica mediante el dispositivo de creación de firma **(SCD)**
- Se devuelve documento firmado al firmante

8. SOFTWARE DESARROLLADO

Para el cumplimiento de los objetivos de este trabajo, se ha procedido la implementación de la arquitectura descrita en el apartado anterior, resultando en una aplicación **PHP & MySQL** para la lógica del lado del servidor y una aplicación cliente para dispositivos **Android**.



APLICACIÓN SERVIDOR

La aplicación servidor se encarga de las siguientes tareas:

- Registro de usuarios (Datos personales, credenciales y claves criptográficas)
- Gestión de tokens de acceso mediante **Oauth 2.0**
- Gestión de OTP's (One Time Password)
- Generación de firma electrónica de documentos haciendo uso de la clave privada del usuario almacenada en base de datos.
- Verificación de firma electrónica de documentos.

Para el desarrollo de esta parte se ha utilizado:

- **phpseclib 1.0.** Librería criptográfica PHP interoperable con OpenSSL
- **Slim framework.** Framework PHP para la creación de API REST.
- **Oauth2 Server PHP.** Librería PHP que implementa Oauth 2.0

Despliegue e instalación

Para el despliegue de la aplicación servidor se ha utilizado un servidor **Apache** con **PHP 5.6.16**, en concreto, se ha alojado la aplicación en el hosting gratuito **alwaysdata.net,** quedando la aplicación accesible en la url **https://tfm.alwaysdata.net/tfm,** de esta forma se facilita el acceso desde la aplicación cliente, pudiendo ser probada tanto desde dispositivos físico como desde emulador.

Para la instalación de la aplicación, necesitamos crear una base de datos vacía, a continuación editamos el fichero **include/config.php** con los datos de conexión**:**

```
class Config {
    static $DB_SERVER    = 'mysql-tfm.alwaysdata.net';
    static $DB_NAME      = 'tfm_uoc';
    static $DB_USERNAME  = 'tfm';
    static $DB_PASSWORD  = 'tfm';
}
```

Finalmente se debe acceder a través del navegador a **db/install.php**, donde se vuelca el script **.sql** del directorio en la base de datos. Después de terminar el proceso de instalación puede eliminarse el directorio db del servidor.

Modelo de datos

El modelo de base de datos se compone de las siguientes tablas:

Users

Name	Type
id	int(11)
first_name	varchar(255)
last_name	varchar(255)
telephone	varchar(12)
encypted_privatekey	longtext
privatekey_salt	varchar(32)
public_key	longtext
created	date

Esta tabla almacena los datos personales de los usuarios, así como la *clave publica* y la *clave privada* cifrada con **AES** mediante una clave **(PIN)** escogida por el usuario y el salt disponible en el campo *privatekey_salt*.

oauth_clients

Name	Type
client_id	varchar(80)
client_secret	varchar(80)
redirect_uri	varchar(2000)
grant_types	varchar(80)
scope	varchar(100)
user_id	int(11)

Esta tabla contiene las credenciales del usuario, siendo **client_id** el *email* del usuario y **client_secret** su *contraseña,* el campo *user_id* es una clave ajena al campo id de la tabla users.

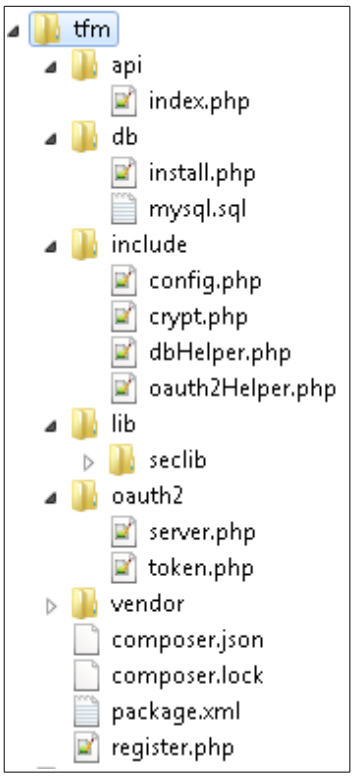
otp

Name	Type
user_id	int(11)
otp	varchar(16)
exp_date	datetime

Esta tabla contiene los OTP (One Time Password) generados para un usuario, además de la fecha de expiración del mismo.

Estructura

El código se encuentra estructurado de la siguente forma:



API

Aquí encontramos el fichero **index.php,** mediante el cual, haciendo uso del framework *Slim,* se crea un API utilizado para gestionar las llamadas al servidor solicitando operaciones tales como: Generación de OTP, Firma y Verificación. Las distintas llamas que se pueden realizar al API son:

- OTP

  Mediante una petición GET a **/api/otp** solicitamos la generación de un código OTP asociado al usuario autenticado, el OTP generado será enviado en la respuesta.

```php
/**
 * Generates an OTP associated to the logged user
 *
 * @return        Generated OTP
 */
$app->get('/otp', function($request, $response, $args) use ($app)
{

    $user_id = getUserIdFromToken();

    try {
        $response->write(generateOTP($user_id));
    }
    catch (Exception $e) {
        return $response->withStatus(500, 'Error generating OTP');
    }

    return $response;
});
```

- SIGN

  Para la creación de una firma, se debe llamar a **/api/sign** con una petición POST, enviando en formato JSON la información necesaria:

```json
{
    "data": "aG9sYQ==",
    "pin": "david",
    "otp": "qkhrb9z0"
}
```

Siendo **data,** el fichero a firmar codificado en Base64, **pin,** PIN para desbloquear la clave privada de usuario y **otp,** el OTP recibido tras la llamada a /api/otp

El proceso de firma sigue los siguentes pasos:

1. Obtención de parámetros

```
$json = $request->getParsedBody();

$data = base64_decode($json['data']);
$pin  = $json['pin'];
$otp  = $json['otp'];
$id   = getUserIdFromToken();
```

2. Validación de otp

Se comprueba que el otp pasado exista y no haya caducado

```
if (isValidOTP($id, $otp)) {
```

3. Obtención de clave privada

```
$pinSalt     = getPinSalt($id);
$encryptedPk = getEncryptedPk($id);
$privateKey  = decrypt_AES256($encryptedPk, $pin, $pinSalt);
```

4. Generación de firma

```
if (!empty($privateKey)) {

    sign($data, $signature, $privateKey);
```

5. Validación de firma

```
$public_key = getPublicKey($id);
$res        = verifySignature($data, $signature, $public_key);
```

6. Codificación de firma en Base64

```
if ($res == "OK") {
    return $response->write(base64_encode($signature));
} else {
    //Signature verification failed
    return $response->withStatus(400, 'Error in signature creation');
}
```

- VERIFY

  Para la verificación de una firma, se debe llamar a **/api/verify** con una petición POST, enviando en formato JSON la información necesaria:

```
{
    "data": "aG9sYQ==",
    "signature": "s87wQ7eACm90a9J
}
```

Siendo **data,** el fichero a firmado codificado en Base64 y **signature,** la firma a validar

```
$public_key = getPublicKey($id);
$res        = verifySignature($data, $signature, $public_key);

if ($res == "ERR") {
    return $response->withStatus(500, 'Error verifiying signature');
} else if ($res == "KO") {
    return $response->withStatus(400, 'Not valid signature');
} else if ($res == "OK") {
    $response->write('Signature verified!!');
    return $response;
}
```

INCLUDE

En este directorio aparecen distintos fichero que contienes clases o funciones que son llamadas desde otros puntos de la aplicación.

- Config.php

  Este fichero contiene los datos de conexión con base de datos

- crypt.php

  Aquí se han creado todas las funciones necesarias para el cifrado de claves, firma y verificación, haciendo uso de la librería phpseclib, entre las cuales se encuentran:

```php
function encrypt_AES256($data, $key, $iv)
{

    $cipher = new Crypt_AES(CRYPT_AES_MODE_CBC); // could use
    $cipher->setPassword($key, 'pbkdf2', 'sha256', 'phpseclib/salt', 1000, 256 / 8);
    $cipher->setIV($iv); // defaults to all-NULLs if not explicitely defined

    return $cipher->encrypt($data);
}
```

```php
function sign($data, &$signature, $private_key)
{

     $rsa = new Crypt_RSA();
     $rsa->loadKey($private_key); // private key
     $rsa->setSignatureMode(CRYPT_RSA_SIGNATURE_PKCS1);
     $rsa->setHash('sha512');
     $signature = $rsa->sign($data);

}
```

```php
function verifySignature($data, $signature, $public_key)
{
    $res = openssl_verify($data, $signature, $public_key, "sha512WithRSAEncryption");

    switch ($res) {
        case 1:
            return 'OK';
        case 0:
            return 'KO';
        default:
            return 'ERR';
    }

}
```

- dbHelper.php

  Este fichero contiene todas las funciones que interactúan con base de datos, necesarias para el registro de usuarios, gestión de OTP

- oauth2Helper.php

  Aquí contamos con dos funciones, una para la verificación de tokens para el acceso a recursos y otra para la obtención del id de usuario del usuario autenticado.

```php
/**
 * This function verifies the token used to access to a resource
 * If the token is not valid or is not present a 401 HHTP code will be sent
 */
function verifyToken()
{
    global $server;

    // Handle a request to a resource and authenticate the access token
    if (!$server->verifyResourceRequest(OAuth2\Request::createFromGlobals())) {
        $server->getResponse()->send();
        die;
    }
}
```

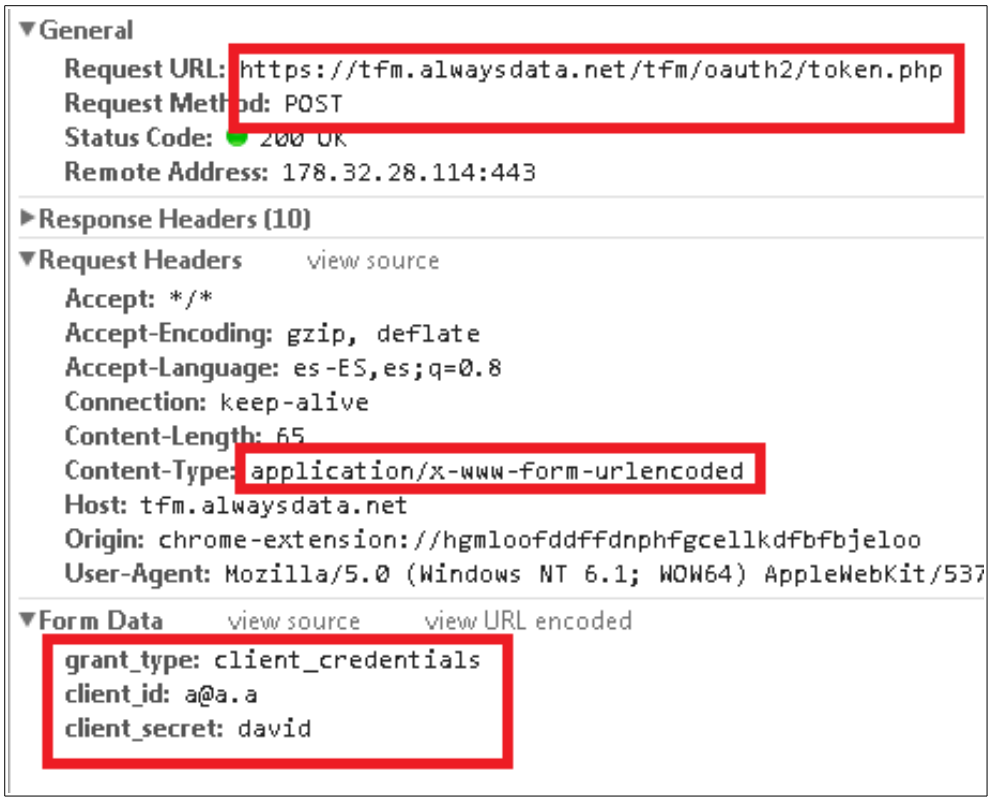
```php
/**
 * This function gets the user id related to the used token
 *
 * @return       User id
 */
function getUserIdFromToken()
{
    global $server;

    $token = $server->getAccessTokenData(OAuth2\Request::createFromGlobals());
    return $token['user_id'];
}
```

LIB

Este directorio contiene la librería criptográfica phpseclib, utilizada en las funciones creadas en crypt.php.

OAUTH2

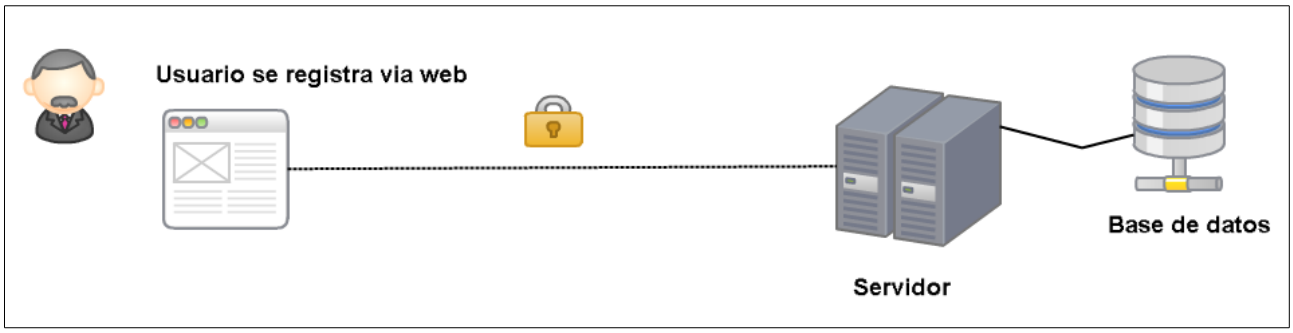
Aquí residen los ficheros **server.php,** encargado de cargar la librería para Oauth2 y de crear los objectos necesarios para la utilización de la misma y el fichero **token.php,** al cual debe llamarse mediante petición POST para obtener un access_token válido, un ejemplo de petición para la obtención de un access token sería el siguiente:



VENDOR

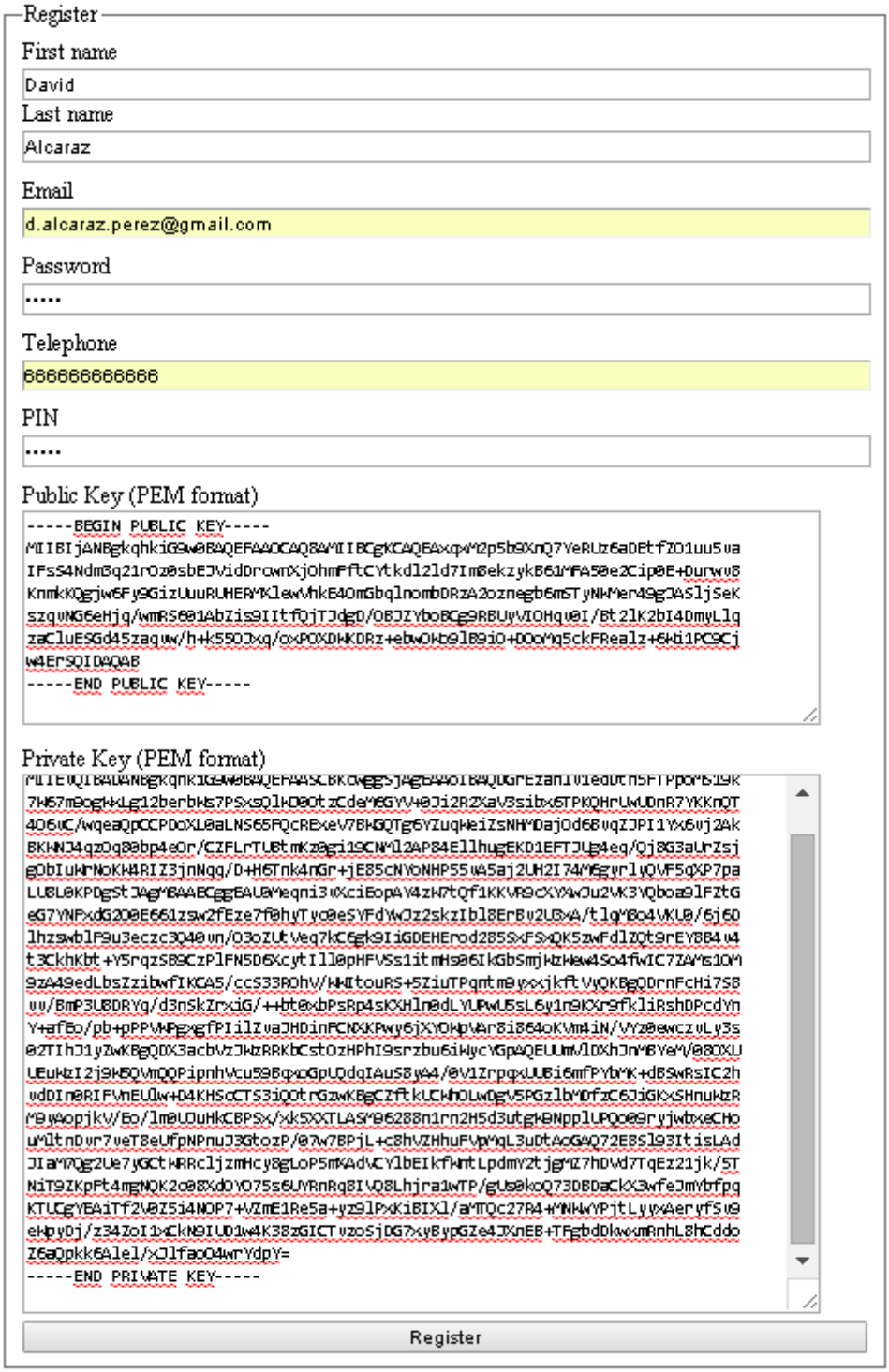
Esta carpeta ha sido creada automáticamente por composer y en ella reside el código correspondiente al framework Slim y a la librería Oauth2.

Registro de usuarios (register.php)



Los usuarios firmantes deben registrarse vía web a través de HTTPS, mediante un formulario donde adjuntarán sus datos personales y sus claves criptográficas. Los campos que debe introducir el usuario son:

- **First name:** Nombre del usuario
- **Last name:** Apellidos del usuario
- **Email:** Dirección de correo electrónico del usuario utilizada posteriormente para la autenticación.
- **Password:** Contraseña de autenticación
- **Telephone:** Teléfono del usuario donde se recibirán los OTP
- **PIN:** Contraseña utilizada junto con un salt para cifrar la clave privada aportada por el usuario.
- **Public Key:** Clave pública RSA del usuario en formato PEM
- **Private Key:** Clave privada RSA del usuario en formato PEM


Register
First name
David
Last name
Alcaraz
Email
d.alcaraz.perez@gmail.com
Password
•••••
Telephone
666666666666
PIN
•••••
Public Key (PEM format)
-----BEGIN PUBLIC KEY-----
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAxqvM2p5b9XnQ7YeRUz6aDEtfZO1uu5va
IFsS4NdmSq21rOz0sbEJVidDrcwnXjOhmFftCYtkdl2ld7Im8ekzykB61MFA50e2Cip0E+Durwv8
KnmkKQgjw6FyGGizUuuRUHERMKlewVhkE4OmGbqlnombDRzA2oznegb6m5TyNkMer49gJASljSeK
szqvNG6eHjq/wmRS601AbZis9IItfOjTJdgD/OBJZYboBCg9RBUyVIOHqu0I/Bt2lK2bI4DmyLlq
zaCluESGd45zaquw/h+k55OJxg/oxPOXDWKDRz+ebwOkb0lB9iO+DOoMq5ckFRealz+6Ki1PC9Cj
w4ErSQIDAQAB
-----END PUBLIC KEY-----
Private Key (PEM format)
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQDGrEzanI0IedDtn5FTPpoM6l9K
7W57m0ogkkLg12berbWs7PSxsQlkD8OtzCdeM6GYV+0Ji2RZXaV3sibx6TPKQHrUwUDnR7YKKnQT
4Q6uC/wqeaQpCCPDoXL0aLNS65FQcRExeV7BKGQTg6YZuqWeiZsNHMDajOd68vqZJPI1Yx6vj2Ak
BKkNJ4qzOq80bp4eOr/CZFLrTUBtmKz0gi19CNMl2AP84EllhugEKD1EFTJUg4eq/Qj8G3aUrZsj
gObIuHrNoKk4RIZ3jnNqq/D+H6Tnk4nGr+jE85cNYoNHP55wA5aj2UH2I74M6gyrlyQVF5qXP7pa
LU8L0KPDgStJAgMBAAECggEAU0Meqni3UXciEopAY4zW7tQf1KKVR9cXYXwOu2VK3YQboa9lFZtG
eG7YNPxdG2O0E661zsw2fEze7f0hyTyc0eSYFdWwOz2skzIbl8ErBv2UBxA/tlqM8o4VKU0/6j6D
lhzswblP9u3eczc3Q40un/O3oZUtVeq7kC6gk9IiGDEHErod285SxFSxQK5zwFdlZQt9rEY8B4u4
t3CkhKbt+Y5rqzSB3CzPlFN5D6XcytIll0pHFVSs1itmHs06IkGbSmjkzHew4So4fwIC7ZAMs1OM
9zA49edLbsZzibwfIKCA5/ccS33ROhV/MMItouRS+5ZiuTPqntm0yxxjkftVyQKBgQDrnFcHi7S8
uu/BmP3U8DRYq/d3nSkIrxiG/++bt0xbPsRp4sKXHln0dLYUPwU5sL6y1n0KXrSfkliRshDPcdYn
Y+afEo/pb+pPPVMPgxgfPIilIuaJHDinPCNXKPwy6jXYOHpVAr8i864oKVm4iN/VYz0ewczvLy3s
02TIhJ1yZwKBgQDX3acbVzJHzRRKbCstOzHPhI9srzbu6iHycYGpAQEUUmVlDXhJnMBYeYV08OXU
UEuHzI2j9kEQVmQQPipnhVcu59BqxoGpUQdqIAuS8yA4/0V1IrpqxUUBi6mfPYbMK+dBSwRsIC2h
vdDIn0RIFVnELUw+D4KHScCTS3iQOtrGzwKBgCZftkLCKhOLwDgV5PGzlbMDfzC6JiGKxSHnuHzR
M8yAopjkV/Eo/lm0LOuHkCBPSx/xk5XXTLASY06288n1rn2H5d3utgkBNpplUPQo09ryjwbxeCHo
uMltnDvr7weT8eUfpNPnuJ3GtozP/07w7BPjL+c8hVZHhuFVpMqL3uDtAoGAQ72E8Sl93ItisLAd
JIaM7Qg2Ue7yGCtHRRcljzmHcy8gLoP5mKAdVCYlbEIkfWntLpdmY2tjgMZ7hDVd7TqEz21jk/5T
NiT9ZKpPt4mgNQK2o08XdOYO75s6UYRnRq8IVQ8LhjraiwTP/gUs0koQ73DBDaCkX3wfeJmYbfpq
KTLCgYEAiTf2\0Z5i4NOP7+VZmE1Re5a+yz9lPxKiBIXl/aMTQc27P4+MNWvYPjtLyy+AeryfSu9
ekpyDj/z34ZoI1xCkN9IUD1w4K38zGICTvzoSjDG7xyBypGIe4JXnEB+TFgbdDkwxmRnhL8hCddo
Z6aQpkk6Alel/xJlfaoO4wrYdpY=
-----END PRIVATE KEY-----
Register

Una vez completado el registro, podremos observar que se han utilizado dos tablas en base de datos para el mismo:

Users

id	first_name	last_name	telephone	encypted_privatekey	privatekey_salt	public_key	created
21	David	Alcaraz	666666666666	†°¤í KÛÚ#as0÷UsUaØÈà6;::T>=›l÷æ°eKÝ›Sop¼VòÙp...	°¬û'ÉSDJÂZ?6Ú	-----BEGIN PUBLIC KEY----- MIIBIjANBgkqhkiG9w0BAQ...	2016-01-05

En esta tabla se almacenan todos los datos relativos a los firmantes excepto email y password, como se puede observar, la clave privada se encuentra cifrada, el cifrado se lleva a cabo utilizando el algoritmo AES junto con el salt disponible en el campo **privatekey_salt** y una derivación del PIN escogido por el usuario, derivado con **pbkdf2**, dicho PIN no se almacena en base de datos, es una información que debe conocer únicamente el firmante.

```
/**
 * This function encrypts the passed data with AES256
 * using the key parameter and the inicialization vector
 *
 * @param $data     Data to be encrypted
 * @param $key      Key used to encrypt/decrypt
 * @param $iv       Inicialization vector
 *
 * @return          AES256 encrypted data
 */
function encrypt_AES256($data, $key, $iv)
{

    $cipher = new Crypt_AES(CRYPT_AES_MODE_CBC); // could use
    $cipher->setPassword($key, 'pbkdf2', 'sha256', 'phpseclib/salt', 1000, 256 / 8);
    $cipher->setIV($iv); // defaults to all-NULLs if not explicitely defined

    return $cipher->encrypt($data);
}
```

Oauth_clients

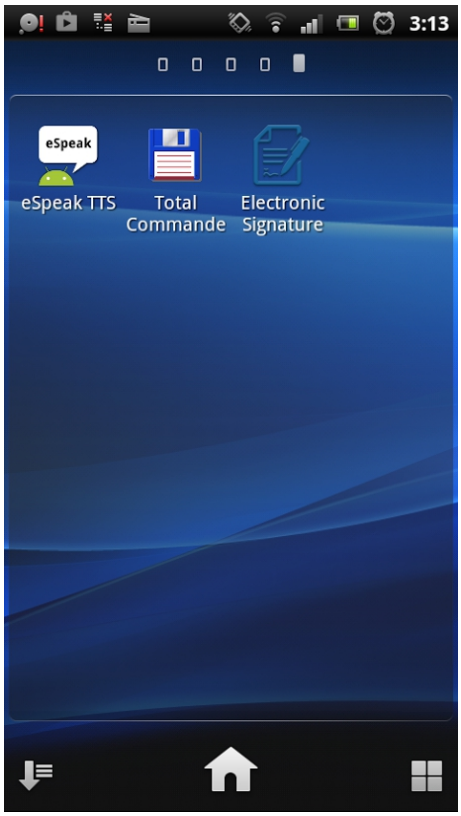
client_id	client_secret	redirect_uri	grant_types	scope	user_id
a@a.a	david		*NULL*	*NULL*	21

En esta tabla se almacenan las credenciales de los usuarios (email y password), además de una referencia al **id** del usuario en la tabla **users.** Estas credenciales, serán utilizadas desde la aplicación cliente para solicitar un **access_token** que nos permita interactuar con el servidor a través de **Oauh2.**

APLICACIÓN CLIENTE

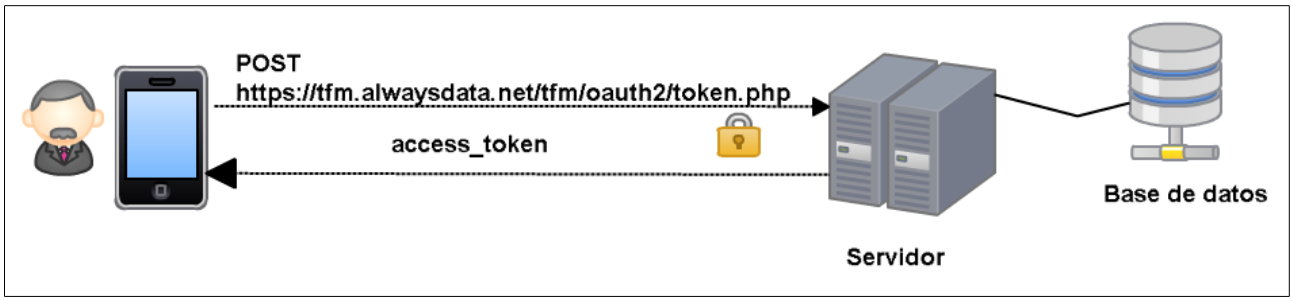
La aplicación cliente se ha desarrollado para dispositivos móviles Android, en concreto móviles desde la versión 10 (Android 2.3) hasta la 23 (Android 6.0).

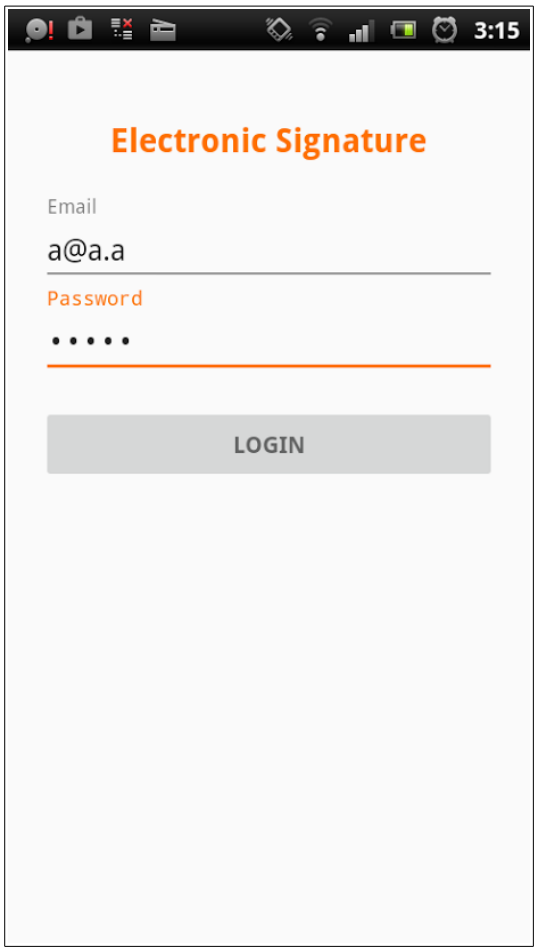
Una vez que un usuario ha completado el registro, puede proceder, a través de la aplicación Android, a la generación de una firma electrónica, enviando un fichero al servidor, el cual será firmado con la clave privada alojada en base de datos. Una vez instalada la aplicación, podremos acceder desde el menú del teléfono:



Login

Tras abrir la aplicación se nos mostrará la pantalla de **login**, donde introducir las credenciales del usuario (email y contraseña), el proceso de login consiste en la petición de un **access_token** cuya duración es de **1 hora** y que tendrá que ser empleado para realizar las operaciones posteriores de firma y verificación.

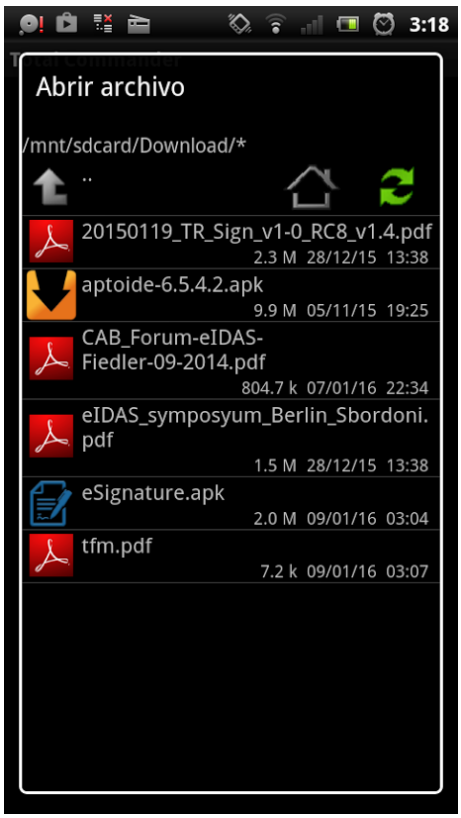




Selección de documento

Una vez se ha hecho login, se mostrará la pantalla donde seleccionar el documento a firmar:

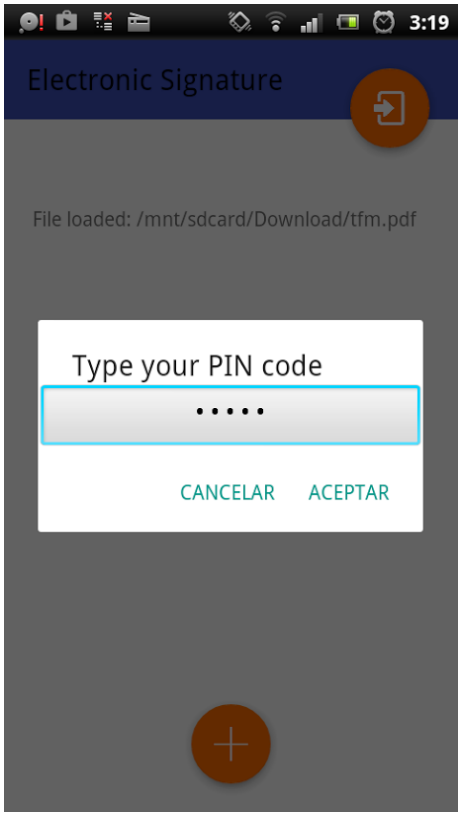
Pulsando el botón de la parte de abajo, podremos elegir el programa para seleccionar el documento a firmar, en este caso vamos a seleccionar un documento pdf que contiene el texto **HOLA TFM.**



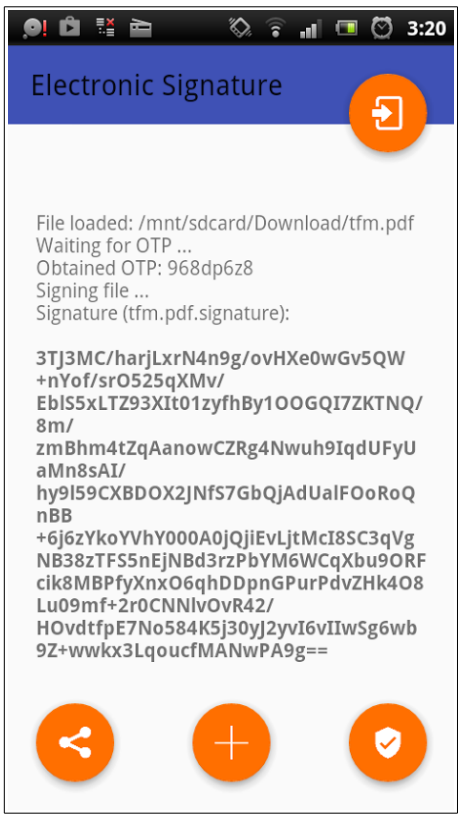
Tras seleccionar el fichero, comprobaremos que tanto en el log de la pantalla como en la parte inferiror se nos informa del fichero cargado, este fichero será leido y codificado en Base64, para ser posteriormente enviado al servidor para ser firmado.

Firma

Para proceder a la firma del documento, debemos pulsar el botón **SIGN,** tras esto se nos pedirá que introduzcamos el PIN establecido en el registro para ser usado como clave para el cifrado de la clave privada.



Después de introducir el PIN, se realizarán una serie de acciones que podemos ir viendo en el log de la pantalla hasta recibir la firma desde el servidor.



Antes de recibir la firma se realiza una petición al API (**api/otp**) para solicitar un OTP, este OTP se genera en el servidor mediante sofware asociado al usuario con una validez de cinco minutos, el OTP tendría que ser recibido por SMS y ser detectado por la aplicación al ser recibido, debido a que para llevar esto a cabo se tendría que contratar algún servicio de pago con un proveedor, se ha simulado la recepción del OTP, ya que simplemente se recibe como respuesta en la llamada al API.

Finalmente para generar la firma se hace una última llamada al API, en concreto a **api/sign,** enviando el OTP, el PIN y el documento a firmar, la respuesta de esta petición es la firma codificada en Base64 y que se muestra en la pantalla, además de estar contenida en un fichero creado en tarjeta SD del mismo nombre que el fichero firmado con extensión **.signature**.


3:38
Total Commander
0/1
/mnt/sdcard/Download/ElectronicSignature
..
tfm.pdf.signature
344 09/01/16 03:32
Sel

Verificación de firma

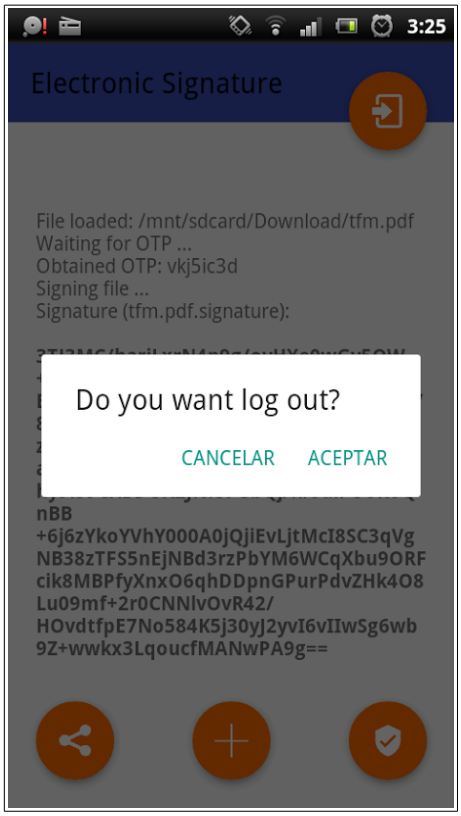
Una vez recibida la firma podemos verificarla, realizando una llamada al API **(api/verify)**, enviando en la petición la firma y el documento original.

Compartición de la firma

Tras recibir la firma, podemos proceder a compartirla mediante el software disponible en el teléfono : Bluetooth, Gmail, WhatsApp, Hangouts etc.

Logout

Al pulsar el botón de logout, se nos pedirá confirmación y finalmente se redirigirá a la pantalla de login.



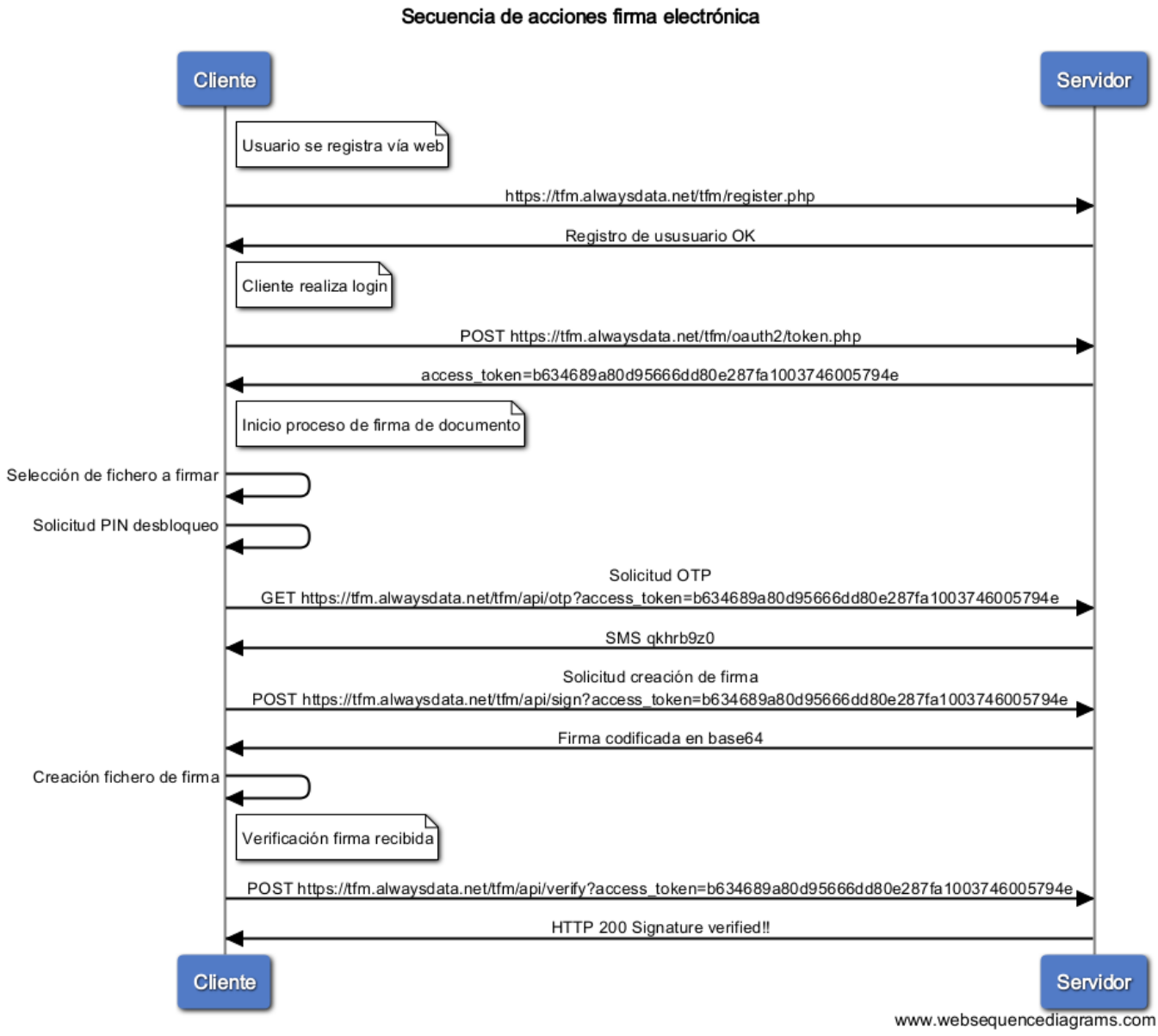
OPORTUNIDADES DE MEJORA

Como mejoras de la aplicación desarrollada se proponen las siguientes:

- Utilizar dispositivo HSM para la creación de firma
- Utilizar dispositivo hardware para la generación de OTP
- Modificar código servidor para que los OTP se envíen por SMS
- Generar la firma en formato AdES
- Corregir problema en aplicación android al abrir ficheros de varios megas
- Permitir subir claves en registro en otros formatos

SECUENCIA COMPLETA DE ACCIONES

La secuencia completa de acciones entre la aplicación cliente y servidor, desde que se realiza la autenticación hasta que se verifica la firma es la que se muestra en el siguiente diagrama:



9. BIBLIOGRAFÍA

- **Portal Administración electrónica**
  http://firmaelectronica.gob.es/

- **Sede electrónica Real Casa de la Moneda**
  https://www.sede.fnmt.gob.es/normativa/firma-electronica

- **Giesecke & Devrient**
  http://www.gi-de.com/en/index.jsp

- **REGLAMENTO (UE) Nº 910/2014 DEL PARLAMENTO EUROPEO Y DEL CONSEJO**
  https://www.boe.es/doue/2014/257/L00073-00114.pdf

- **DIRECTIVA 1999/93/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO**
  http://www.boe.es/doue/2000/013/L00012-00020.pdf

- **Ministerio de Industria, Energía y Turismo**
  http://www.minetur.gob.es/telecomunicaciones/es-ES/Servicios/FirmaElectronica/Paginas/NormasTecnicas.aspx

- **Normativa de la Unión Europea**
  http://www.agenciatributaria.es/AEAT.internet/Inicio/La_Agencia_Tributaria/Normativa/Otra_normativa_de_interes/Administracion_electronica/Normativa_de_la_Union_Europea/Normativa_de_la_Union_Europea.shtml