Universitat Oberta de Catalunya

Proyecto Final

Creación de una plataforma para firmar una ILP en línea

Autor:
Marçal Machado Chaiben

Supervisor:
Cristina Pérez Solà

Memoria enviada para el cumplimento de los requerimientos para la obtención del
Posgrado en Seguridad en servicios y aplicaciones

en el

Departamento Informática, Multimedia y Telecomunicación

19 de junio de 2015

UNIVERSITAT OBERTA DE CATALUNYA

Abstract

Departamento Informática, Multimedia y Telecomunicación

Posgrado en Seguridad en servicios y aplicaciones

Creación de una plataforma para firmar una ILP en línea

by Marçal Machado Chaiben

This work shows how to create an ILP platform to obtain valid digital signatures that can be used to support Popular Legislative Initiative.

Agradecimientos

Gracias a Qustodio por permitirme realizar este Posgrado, Josep Gaspar, Josh Gabel y Eduardo Cruz.

Gracias a mi orientadora Cristina Pérez Solà y su paciencia infinita.

Gracias a Rosa Gisbert Díaz por ayudarme con la revisión de esta memoria.

Abreviaciones

BOE	**B**oletín **O**ficial del **E**stado
CE	**C**onstitución **Española**
CP	**C**omisión **P**romotora
DNIe	**D**ocumento **N**acional de **I**dentidad **e**lectrónico
DNI	**D**ocumento **N**acional de **I**dentidad
GA	**G**oogle **A**nalytics
HTML	**H**yper**T**ext **M**arkup **L**anguage
ILP	**I**niciativa **L**esgislativa **P**opular
JS	**J**ava**S**cript
PHP	Hypertext Preprocessor
XAdES	**X**ML **Ad**vanced **E**lectronic **S**ignatures
XAdES-BES	XAdES básico que cumple la Directiva para firma electrónica avanzada
XAdES-EPES	XAdES-BES añadido información sobre la política de firma
XAdES-T	XAdES-EPES con **T**imestamp para evitar repudio
ZF	**Z**end**F**ramework

A mi Rosa por animarme a seguir adelante en todo momento.

Capítulo 1

Introducción

Nuestra democracia representativa tiene su principal herramienta de participación en el voto, mediante el cual el ciudadano designa a quienes lo representarán en las Cortes Generales y en los Parlamentos Autonómicos. Estos representantes son quienes tienen la potestad para proponer leyes y, tras su aprobación, legislar. Así lo establece el art. 87 de la Constitución Española (CE) cuando asegura que la "iniciativa legislativa corresponde al Gobierno, al Congreso y al Senado". Este sistema implica que el ciudadano tiene voz propia solamente una vez cada cuatro años, cuando elige a quien en su nombre detectará los problemas que tiene la sociedad, les dará solución bajo la forma de norma y presentará una propuesta de Ley que, posteriormente, será aprobada o no. De esta forma, parece, que el ciudadano queda muy alejado de la creación de las normas.

La Constitución pretende arreglar esto en el punto 3 del mismo artículo introduciendo el concepto de iniciativa legislativa popular (ILP). El texto establece que una Ley Orgánica regulará la iniciativa popular para la presentación de proposiciones de ley y que serán necesarias al menos 500.000 firmas para dar curso a la petición. La Ley Orgánica 3/1984 de 26 de Marzo es el texto que regula los requisitos y el procedimiento a seguir para presentar una ILP.

El texto normativo establece que para iniciar el proceso se deberá presentar un escrito ante la Mesa del Congreso de los Diputados que incluya: el texto articulado de la Ley que se pretende proponer y un listado de las personas responsables de promover la firma del texto con sus datos personales. A este grupo, la ley le da el nombre de Comisión Promotora (CP). Una vez la Mesa admite la propuesta, se lo comunica a la Junta Electoral Central que es el órgano que supervisará la recogida de firmas. La Junta es quien comunica la aceptación a la CP y a partir de ese momento se abre un plazo de 9 meses para reunir las 500 000 firmas y entregarlas. Cuando se da una causa de fuerza

mayor existe la posibilidad de prorrogar el plazo tres meses más, pero una vez agotado, la iniciativa simplemente caduca.

Medio millar de españoles suponen alrededor del 1 % de la población, cifra que puede parecernos pequeña. No lo es tanto si pensamos que esas personas llenarían más de cinco veces el estadio del Camp Nou y que hemos de llegar a todas ellas en un período de tiempo limitado. Tal vez por eso en 2012, treinta años después de aprobada la Constitución, tan sólo se han presentado un centenar de iniciativas de las que 66 han sido admitidas a trámite y de las cuales solamente 9 llegaron a recabar las firmas dentro del plazo estipulado. De estas, la única que acabó siendo aprobada fue una ILP sobre deudas comunitarias.

Lo que en principio parece una buena herramienta de participación cívica, acaba siendo poco útil debido a las diferentes trabas con las que se encuentra, que van desde la restricción temática que impone la CE hasta la dificultad de admisión a trámite. Pero estas no son objeto del trabajo, que se centra en solventar otro problema: el de la recolección de firmas.

Viendo el número de Iniciativas legislativas presentadas en los últimos años, resulta evidente que estas están proliferando. Durante la década de los ochenta y noventa se presentaba una anualmente o cada dos años y desde la introducción de Internet se presentan a admisión de cuatro a cinco por año. Está claro que la red supone un caldo de cultivo de movimientos e ideas y un excelente canal para difundir una causa. Pero, aun así, el número de firmas no ha sido todavía suficiente como para que la propuesta pasara a ser debatida por la cámara. ¿Por qué?

En España se empezó a implantar el DNI electrónico en 2006 y en la actualidad la gran mayoría de españoles tienen este tipo de identificación. En ese mismo año una Ley Orgánica modificó el preámbulo y el artículo 7 de la LO 3/1964 de 26 de marzo, Reguladora de la Iniciativa Legislativa Popular para que esta incluyera la posibilidad de firmar una ILP por vía telemática. El preámbulo modificado dice que “también se podrán recoger las firmas por vía electrónica siempre que se garantice la voluntad auténtica del ciudadano que suscribe la iniciativa legislativa popular” y el artículo 7 establece que se recogerán “como firma electrónica conforme a lo que establezca la legislación correspondiente”.

Parecería que la posibilidad de la vía telemática facilitaría que los ciudadanos firmasen estas peticiones pero, de momento, no está siendo así. Hay que tener en cuenta la reticencia al cambio y la desconfianza de gran parte de la sociedad española. Por otro lado, el ciudadano debe contar con un certificado digital o bien con un lector de DNIe (en caso de firmar con DNIe), cosa que no siempre se tiene. Con cada vez más promoción de

la administración para que las personas utilicen la vía telemática para realizar trámites, es previsible que cada vez más personas se acostumbren a este instrumento.

Pero existe otro problema, y es el de cómo la CP recoge esas firmas electrónicas. En la actualidad existen algunas plataformas en las que se pueden firmar peticiones, como puede ser Change.org. El problema con estas webs es que la recoleta de esos datos (normalmente nombre y número de identificación) no supone realmente una firma y no tendrían validez a la hora de presentarlas ante la Junta Electoral.

Existe una plataforma en España llamada Mifirma.com que es la única a través de la cual se pueden recoger firmas electrónicas válidas. En ella las Comisiones Promotoras pueden colgar su petición y es Mifirma.com quien recoge las firmas y los datos y una vez se llega al número necesario los presenta ante la Junta Electoral. El grupo que creó y gestiona la página de forma gratuita lo conforman una serie de voluntarios ingenieros informáticos y juristas. Aun siendo una buena y loable iniciativa, se queda corta. Por un lado es la única que existe y por otro, hace necesario que la CP dependa de una serie de personas externas.

Este proyecto tiene como objetivo principal diseñar e implementar una plataforma que permita recoger firmas digitales para una ILP de manera sencilla, garantizando que las firmas cumplen los requisitos necesarios. Esta podrá ser utilizada por cualquiera que desee promover una petición de este tipo, pudiéndola incluir de forma sencilla en su propia web. ¿Qué ventaja tiene sobre la plataforma ya existente? Que se crea una herramienta que permite recolectar de forma independiente firmas válidas sin necesidad de depender de servidores y base de datos, de un grupo externo y permitiendo la completa incorporación de la plataforma al sistema de la organización a cual pertenece la CP.

Esta memoria está dividida en otros tres (3) capítulos: El Capítulo 2 presenta la definición del proyecto. Allí se verá los requerimientos para realizar la recolecta de firmas electrónicas para una ILP, la definición de la base de datos, los pasos para realizar la firma electrónica de la ILP, la configuración requerida para el servidor así como los lenguajes y técnicas de programación utilizados. El Capítulo 3 presenta el proyecto que se consiguió realizar y el Capitulo 4 una breve conclusión con los próximos pasos a seguir y comentarios finales.

Capítulo 2

Definición del proyecto

Este capítulo engloba los requerimientos del sistema para la firma de la ILP. También veremos la estructura de base de datos, los pasos para realizar la firma electrónica de la ILP, la configuración del servidor así como los lenguajes y técnicas de programación utilizados.

2.1. Requerimientos

En esta sección detallaremos los requerimientos para una ILP, los datos requeridos a la CP, los elementos necesarios para la firma y el elemento que será firmado, en nuestro caso, el XML a ser firmado.

2.1.1. Para una ILP:

El Boletín Oficial del Estado (BOE) [1] especifica los requerimientos para una ILP:

- Una ILP debe cursarse mediante la presentación de una proposición de Ley suscrita por firmas de al menos, 500 mil electores, si la ILP es a nivel nacional. A nivel regional ese numero cambia.
- La CP deberá solicitar a la Junta Electoral Central la aprobación del sistema electrónico de recogida de firmas que desee utilizar, indicando la dirección electrónica de acceso así como la descripción del sistema de firma y de verificación de firma electrónica. Los datos del firmante tienen que tener el formato del archivo XML presentado en la sección 2.1.4.

- La ILP tendrá un código con el formato ILPAAAANNN donde "ILP" es fijo, AAAA es el año y NNN un número asignado por la Junta Electoral.
- Las páginas deben estar escritas en castellano o pueden ser también redactadas en las lenguas cooficiales correspondientes al ámbito de la ILP.
- La firma electrónica tiene que ser una firma del tipo avanzada basada en un certificado reconocido por las administraciones públicas.
- La CP deberá comunicar a la Junta Electoral Central la fecha prevista para el envío de las firmas y el número total de firmas.
- La CP entregará los ficheros que contienen las firmas recogidas electrónicamente en soportes físicos o mediante un sistema de transmisión telemática previamente acordado con la Oficina del Censo Electoral.
- Las firmas deberán ser recogidas en un plazo de nueve meses desde el día en el que la proposición ha sido aceptada, pudiendo prorrogarse este plazo tres meses más si la Mesa de la Cámara lo considerase oportuno.

2.1.2. Para la Comisión Promotora:

La CP, para efecto de recoger las firmas electrónicas, deberá introducir los siguientes datos de sus integrantes:

- Nombre y apellidos
- Correo electrónico de contacto
- Teléfono de contacto
- Cargo dentro de la CP
- Contraseña
- Si tiene permiso de administrador de esta CP.

2.1.3. Para la firma electrónica:

Para la firma se necesitan los siguientes datos del firmante:

- Nombre
- Primero apellido

- Segundo apellido
- Fecha de nacimiento
- Documento de identificación - DNI en el caso de la firma electrónica.
- Código de la ILP que se está firmando
- *Timestamp* de la firma.
- XML de la firma

2.1.4. XML a ser firmado

El formato de la XML que será firmado está está definido en el BOE [1] y representado abajo.

```
<?xml version="1.0" encoding="UTF-8"?>
<ilp>
    <firmante>
        <nomb />
        <ape1 />
        <ape2 />
        <fnac />
        <tipoid />
        <id />
    </firmante>
    <datosilp>
        <tituloilp />
        <codigoilp />
    </datosilp>
</ilp>
```

En el BOE [1] también se define la estructura y restricciones del contenido del XML, el cuadro 2.1.

Observaciones: La validación de los cambios se realiza en la parte del cliente por *JavaScript* y en el servidor por el PHP.

2.2. Definición de la base de datos

Tomando como base la información de la sección 2.1 se definió la estructura de base de datos representada en la figura 2.1. En esta sección veremos las tablas creadas.

Cuadro 2.1: Descripción de los campos del XML que será firmado.

Campo	Descripción	Restricción
nomb	Nombre firmante	tamaño máximo: 20 caracteres
ape1	Primer apellido	tamaño máximo: 25 caracteres
ape2	Segundo apellido	tamaño máximo: 25 caracteres
fnac	Fecha nacimiento	Formato: AAAAMMDD
tipoid	Número del documento nacional de identidad, incluida la letra final	Tamaño 9 caracteres, formato [0-9]+[a-zA-Z]1
tituloilp	Título de la ILP	Tamaño máximo 300 caracteres.
codigoilp	Código ILP	Formato ILPAAAANNN, donde AAAA es el año y NNN es el número asignado.

2.2.1. Tabla Miembro Comisión Promotora

En esta tabla encontramos los datos relativos a los miembros que componen la CP. Los miembros de la CP son los usuarios que podrán cambiar los datos relativos a la ILP. Entre los datos guardados están: Nombre, apellidos, correo-electrónico, dos teléfonos de contacto, una contraseña de acceso con un campo de "salt" que sirve como seguridad para evitar que se puedan romper todas las contraseñas en el caso que se consiga romper una de ella (se podrá ver en el código fuente como es calculado y utilizado el "salt".).

2.2.2. Tabla ILP

En la tabla ILP se guarda toda la información relativa a la ILP. Entre ellas encontramos: el código de la ILP (formato ILPAAAANNN), título, una descripción corta, una descripción más larga, la ILP entera, las fechas de inicio y fin, cuándo fue creada y cuándo fue alterada.

2.2.3. Tabla Comisión Promotora

Es la tabla que une cada Miembro de la CP con la ILP. También en ella se guarda las informaciones relativas de cada Miembro con la ILP que se está firmando. Entre los datos están: el rango que tiene el miembro dentro de la CP, si el mismo tiene permiso de administrador y un campo de descripción que puede guardar cualquier información que el administrador crea pertinente.

2.2.4. Tabla Firma

En esta tabla se guarda toda la información sobre la firma realizada. Los datos obligatorios del firmante como: nombre, apellidos, fecha de nacimiento, número del DNI y el

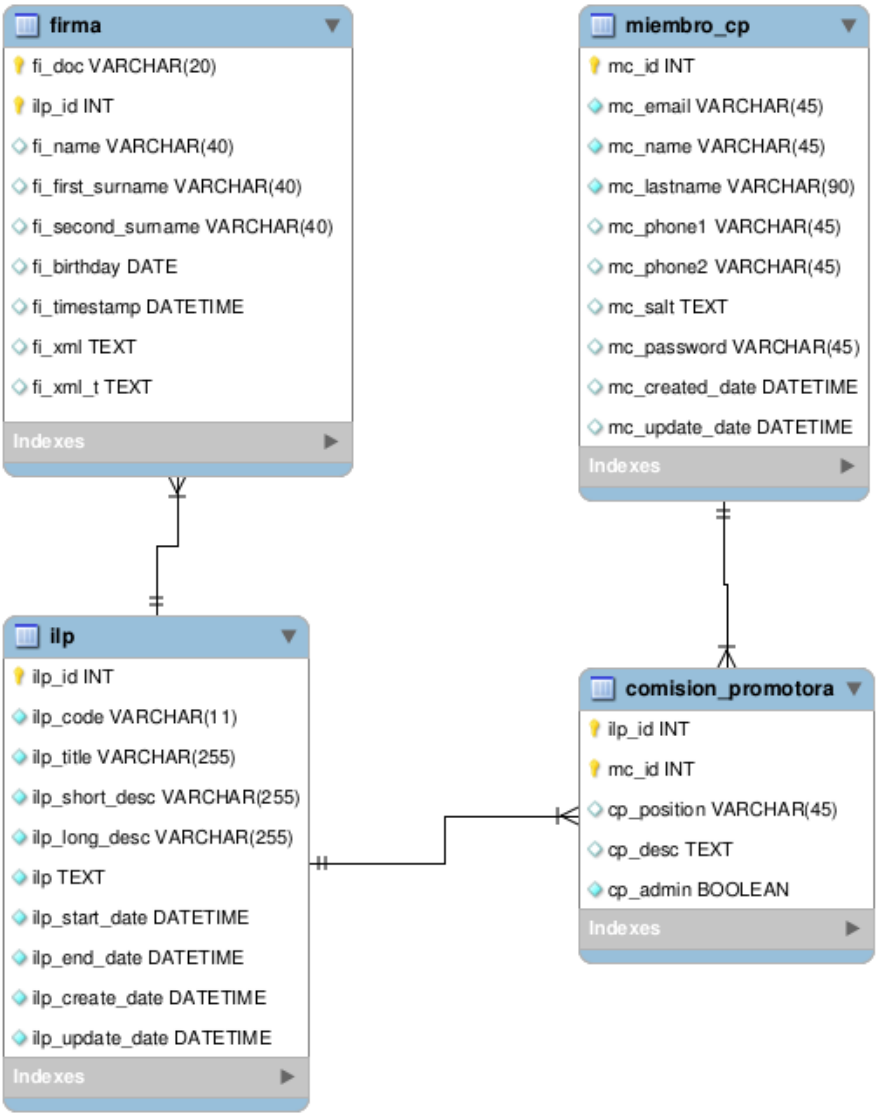


FIGURA 2.1: Base de datos de la plataforma ILP

XML firmado. En el campo fi_xml se guarda el XML firmado en formato XAdES sin la firma de tiempo. El campo de *timestamp* sirve para que sepamos cuándo el firmante envió la firma pero no es el *timestamp* de la firma XAdES-T.

La firma de tiempo sirve para asegurar que el documento fue firmado durante el período correcto de validez de la colecta de firmas, pero para este proceso se necesita la conexión a un tercer servidor que realizará la firma de tiempo. Para evitar retrasos y posibles desistencias durante el proceso de firma, la firma de tiempo será realizada utilizando un servicio de "cron". La idea aquí es que este servicio se ejecute cada cierto tiempo para poner el sello de tiempo en todas las nuevas firmas. Otra ventaja de este método en diferido es que solamente se lleva a cabo en el lado del servidor y en el caso de error el administrador puede solucionar la incidencia sin que se pierda ninguna firma. Una vez realizada la firma de tiempo - XAdES-T esta será guardada en el campo fi_xml_t.

2.3. Firma

En esta sección veremos los pasos necesarios para la realización de la firma y cómo asegurar la integridad de la misma.

2.3.0.1. Realización de la firma digital

En la figura 2.2 se representa el diagrama de los principales pasos realizados para la firma del XML de la ILP.

1. El firmante accede a la página de la ILP donde se carga el contenido de la ILP y el formulario para la firma de la misma.
2. El firmante lee el contenido de la ILP y rellena el formulario y hace clic en "firmar".
3. Verifica si los datos del formulario están correctamente firmados.
4. Si en los datos del formulario no hay errores se verifica si el usuario no ha firmado antes esta ILP.
5. Si está todo correcto, el servidor genera el XML a ser firmado y un *hash* que sirve para controlar la integridad del XML firmado por el usuario (ver diagrama de generar *hash* de la figura 2.3 de la sección 2.3.0.2).
6. Se solicita que el firmante firme el documento XML con su certificado digital o DNIe.
7. Verifica si el XML recibido está firmado correctamente y verifica si el contenido del mismo corresponde con el *hash* de verificación enviado (ver validar *hash* de la figura 2.3 de la sección 2.3.0.2).
8. Si todo está correcto se guarda el XML firmado en la base de datos y se agradece la firma.

2.3.0.2. Generar y Validar *Hash*

La figura 2.3 describe el proceso de generar y validar el *hash*.

Generar el *hash*

1. El servidor genera el XML que será enviado al firmante

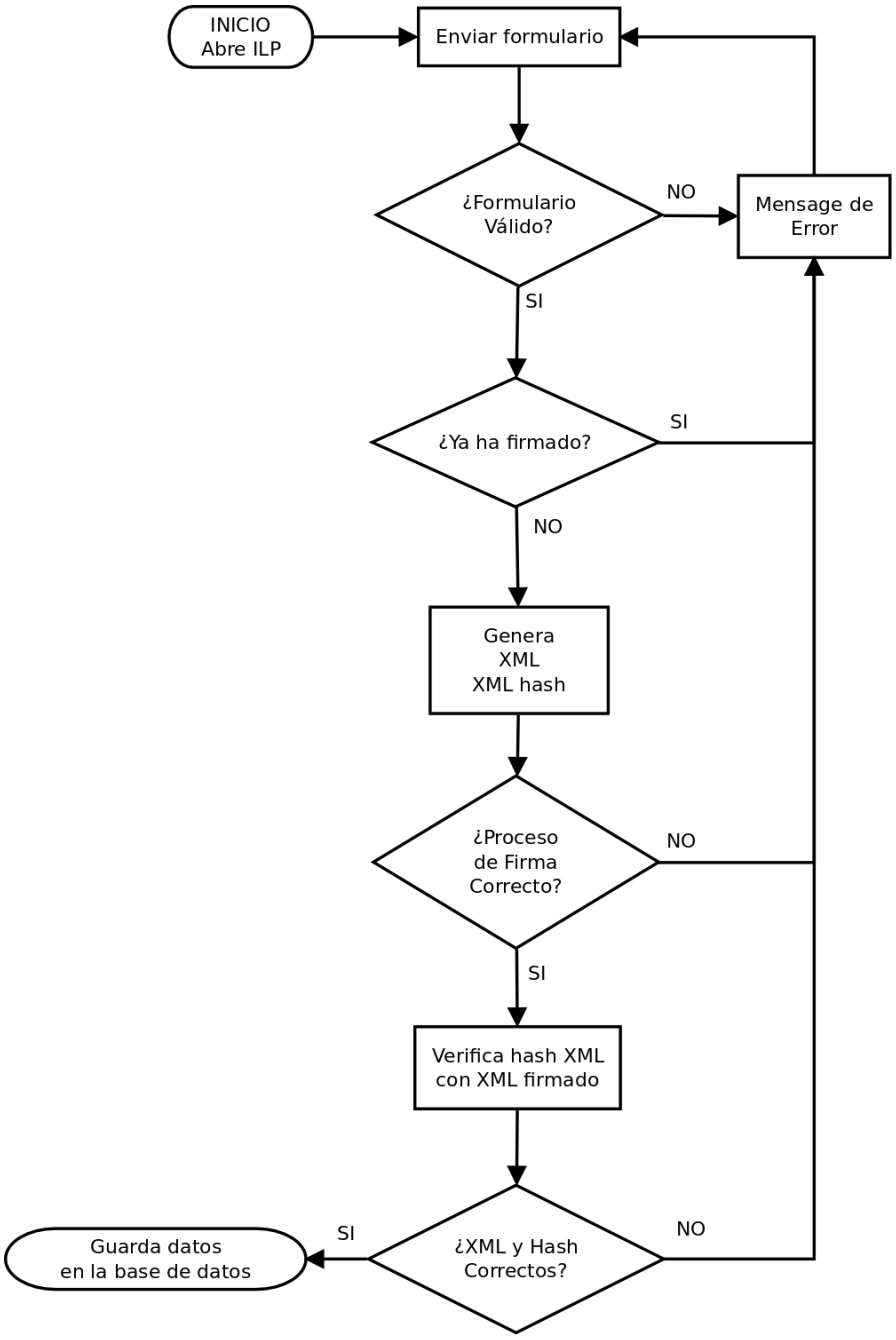


FIGURA 2.2: Diagrama de flujo simplificado para la firma del XML representado en la sección 2.1.4

2. Utilizando una variable auxiliar, se concatena una clave secreta que solamente conoce el servidor que genera el XML.

3. Se elige un número N al azar entre 1 y 100.

4. Se realiza N veces el proceso SHA-1 de la variable auxiliar.

5. Se envía al firmante el *hash* resultante y el número N.

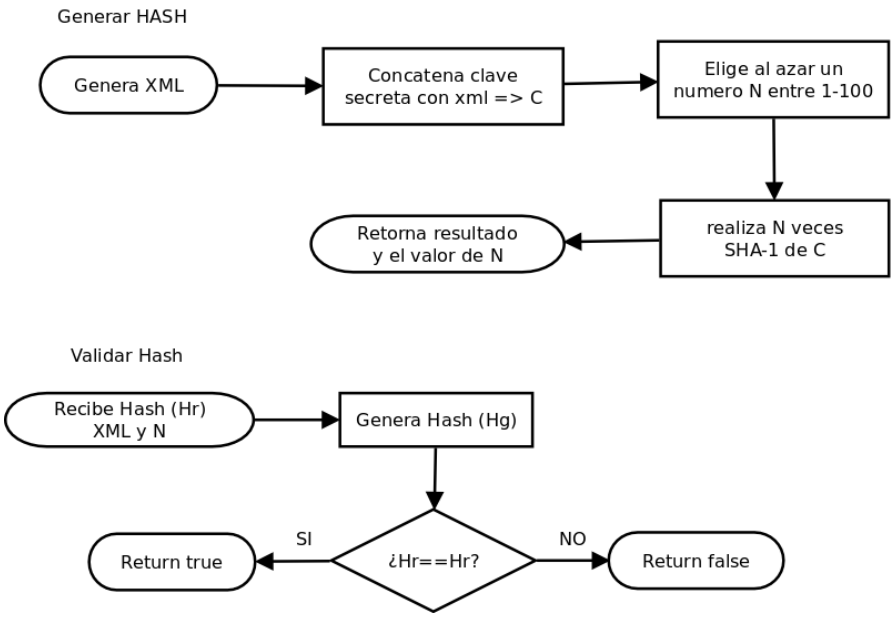


FIGURA 2.3: Hash de seguridad para evitar el cambio de contenido del XML al ser firmado. En la figura se puede ver el diagrama de generación y el de validación.

Validar Hash

1. El servidor recibe del firmante el XML firmado, el *hash* que se le había enviado, y el número N.

2. Del XML firmando se extrae el XML que fue enviado anteriormente y se calcula el *hash* con el proceso de Generar Hash presentado anteriormente.

3. Se compara el valor del *hash* calculado con el valor del *hash* recibido. Si son iguales retorna "Verdadero", si no "Falso".

2.4. Configuración del servidor

En esta sección veremos la configuración del servidor y las técnicas utilizadas.

2.4.1. Base de datos

La base de datos utilizada fue la MySQL v5.5.43, ver referencia [2]. Esta base fue la seleccionada por ser una base de datos gratuita y con muy buen rendimiento. Hemos utilizado el motor InnoDB y el juego de caracteres UTF-8.

El esquema representado se puede ver en la figura 2.1 de la sección 2.2.

2.4.2. Sevidor web

El servidor web utilizado fue el Apache 2 [3] con PHP 5.5 [4]. Para conectar al servidor se utiliza el puerto 80.

Como servidor web Java fue utilizado Apache Tomcat [5]. Esta parte es necesaria para la realización de la firma XAdES-EPES necesaria para cumplir los requerimientos de de la ILP. La mayor parte de los programas para servidor relacionados con firma digital están implementados en el lenguaje JAVA o .NET. Para facilitar la realización de esas firmas fue elegido implementar también este servidor. En [6] se puede ver las herramientas distribuidas por el Gobierno Español.

2.4.3. Git

Para la gestión de versión de los archivos programados se está utilizando Git [7]. Git aquí se encaja a la perfección con la filosofía del proyecto, ya que cualquier programador de una CP que quiera utilizar el código base lo puede modificar y si quiere aportar su grano al proyecto lo puede hacer utilizando *pull-requests*. La idea aquí es que el núcleo del programa se mantenga lo más neutral y sencillo posible, pero que crezca para acompañar los cambios de tecnología y tendencias. En la fecha de publicación de este documento, ya se ha publicado una versión inicial de la firma en el repositorio de GitHub [7] chaiben/FIRMA-ILP [8].

2.4.4. Vagrant

Todavía pensando en facilitar el trabajo de desarrollo, el proyecto utiliza Vagrant [9] para poder exportar el servidor de desarrollo ya pre-configurado. Por ahora se está exportando el archivo *box* pero debido a su gran tamaño esta parte requiere mejoras. La solución que estoy planteando sería la utilización de puppet [10] porque sus *scripts* permiten levantar máquinas enteras y pre-configuradas, y claro, se puede guardar en Git. Pero por ahora se está utilizando Vagrant y compartiendo el “box” con toda la configuración necesaria.

2.5. Lenguaje de programación

Esta sección está dividida en dos partes principales, el lenguaje de programación en el lado del servidor y en el lado del cliente (el firmante).

2.5.1. Programación lado Servidor

2.5.1.1. PHP / ZendFramework

Fue elegido el PHP [4] como lenguaje de programación en el lado del servidor. Para facilitar la organización del proyecto fue elegido utilizar *ZendFramework* (ZF) [11] como *Framework* PHP. El ZF permite el desarrollo ágil [12] y elimina el desarrollo de componentes genéricos, además permite que se trabaje sobre una estructura unificada y ampliamente documentada lo que facilita la incorporación futura de otros programadores al proyecto.

2.5.1.2. PHPUnit test

Como en este proyecto hay problemas con la cantidad de recursos humanos disponibles y el control de calidad también será hecho por el programador, fue elegido utilizar una herramienta automatizada de pruebas: PHPUnit [13]. Como mínimo en toda la parte de los modelos de datos y herramientas auxiliares fueron implementados los tests automatizados. Lo que se busca aquí es evitar que cualquier cambio en el núcleo del programa cause daños a otras partes del programa sin que el programador se dé cuenta.

2.5.2. Programación lado Cliente

En la parte del cliente se utiliza HTML, hojas de estilo CSS, *JavaScript* (JS) y Applet Java.

2.5.2.1. Biblioteca CSS Skeleton

Para las hojas de estilo se ha utilizado la biblioteca *Skeleton* [14] con el objetivo de facilitar el desarrollo y la compatibilidad con dispositivos móviles.

2.5.2.2. Biblioteca JS - jQuery

Con JS se está utilizando la biblioteca jQuery [15] que posé muchas herramientas útiles para la manipulación de eventos, animaciones, funciones útiles y facilita el desarrollo para las diversas versiones de los navegadores. También se esta utilizando jQueryUI [16] para mejora la interfaz del usuario.

2.5.2.3. Google Analytics

Otro punto que vale resaltar es que del lado del servidor tiene la ventaja que se puede guardar en archivos de log todos los errores y problemas que pasan. Pero en el lado del cliente los errores de JS se acaban perdiendo y así podríamos estar perdiendo muchas firmas porque determinada parte del programa no funciona como se espera. Para solucionar este problema y poder analizar el comportamiento de los firmantes se ha instalado un código JS de Google Analytics (GA). Con esta herramienta podemos:

- Visualizar el comportamiento del usuario dentro del sistema.
- Conocer en que paso hay un mayor número de desistencias
- Verificar cuales son los errores más comunes
- Saber cuales con los navegadores más utilizados por nuestros visitantes
- Identificar que tipos de dispositivos son los más utilizados.
- Saber de qué región provienen la mayor parte de las firmas
- Conocer que sistemas operativos son los más utilizados
- etc.

Toda esta información es muy útil tanto para los programadores como para la CP. Los programadores podrán identificar en que tipo de dispositivos o navegadores los firmantes están teniendo más problemas y en el caso que hubiere muchos problemas, se puede priorizar la solución de los problemas en aquellos tipos de dispositivos o navegadores que sean más utilizados.

2.5.2.4. La aplicación de firma: MiniApplet @firma

MiniApplet @firma es una herramienta de firma electrónica que funciona en forma de *applet* de Java integrado en una página Web mediante JS. Este cliente se ejecuta en el lado del Firmante y no en el servidor Web. Esto es así para evitar que la clave privada asociada a un certificado tenga que salir del dispositivo del firmante. El servidor envía los datos a firmar y él lo devuelve firmado. En *clientE @firma* [6] se puede obtener el programa. La versión utilizada es la MiniApplet v1.2.

2.5.2.5. Selenium

Para la parte del cliente fue pensado, pero no se ha implementado todavía, la automatización de los test utilizando Selenium [17]. Pero infelizmente no se ha podido desarrollar esta parte hasta la presente fecha. Esta parte está pensada para que sea posible automatizar las pruebas en el servidor y ahorrar en los gastos de control de calidad.

Capítulo 3

Proyecto implementado

Este capítulo demostrará el programa implementado para la recoger firmas. Para esta parte solamente se ha utilizado el navegador Firefox que soporta *Applets*. Hasta el momento en que este documento se ha escrito no ha sido posible terminar la implementación para los demás navegadores y otros dispositivos.

3.1. Interfaz

En la figura 3.1 se puede ver la interfaz implementada para la firma de la ILP. El objetivo aquí es mantener la sencillez y el menor número de pasos necesarios para la firma.

3.1.1. Avisos de seguridad de Firefox

Al acceder a la página el navegador pide al firmante que autorice ejecutar una aplicación JAVA, figura 3.2.

Una vez autorizado puede aparecer otra ventana donde el usuario puede permitir que no se solicite otra vez este permiso para este dominio, figura 3.3.

Una vez autorizada la ejecución de la aplicación JAVA empieza la carga del *Applet* de MiniApplet, sección 2.5.2.4. Este generará otro aviso de seguridad, figura 3.4. Una vez aceptado este aviso la ILP ya puede ser firmada.

3.1.2. Datos de la ILP

Una vez superados los avisos de seguridad llega la hora de que el firmante revise los datos de la ILP. Los datos han sido organizados en 3 secciones.

FIGURA 3.1: Página para la firma de la ILP

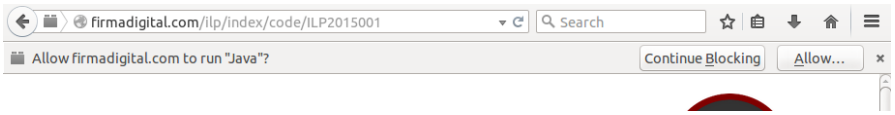


FIGURA 3.2: Solicitud del navegador Firefox para ejecutar la aplicación JAVA

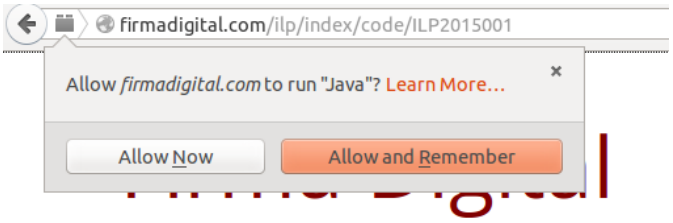


FIGURA 3.3: Solicitud del navegador Firefox para recordar la autorización a la aplicación JAVA

1. **Datos de la ILP**: Aquí se puede ver el título de la ILP, su código, las fechas de inicio y fin y una descripción corta de que trata la ILP, figura 3.5.

2. **Resumen**: Aquí el usuario puede encontrar una descripción más detallada del documento que está firmando. Pero bastante más reducida que la descripción detallada

3. **Descripción detallada**: Sería la copia integral del texto de la ILP, figura 3.6.

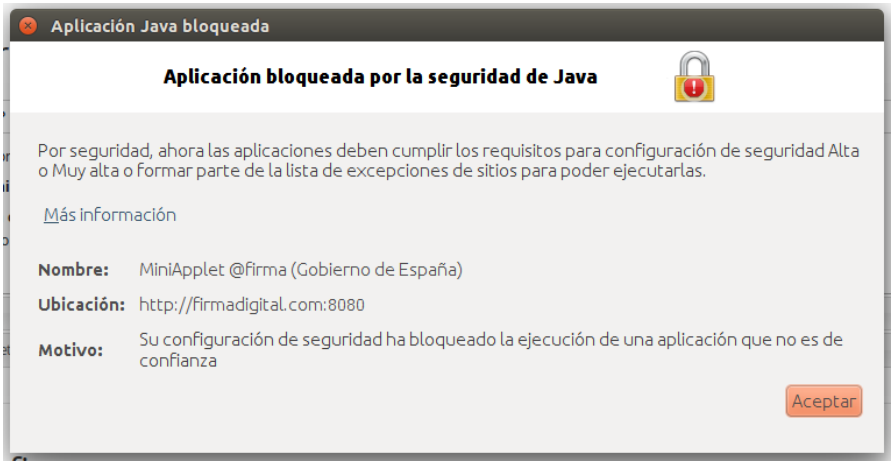


FIGURA 3.4: Aviso de seguridad del navegador Firefox

FIGURA 3.5: Datos de la ILP

3.1.3. Formulario para la firma ILP

El formulario de la ILP está compuesto de solamente 5 campos, todos obligatorios. Nombre, primer y segundo apellido, fecha de nacimiento del firmante y su DNI, ver figura 3.7. Aquí vale recordar que solamente se acepta como documento para firmar una ILP el DNI del firmante, Pasaporte o NIE no son documentos permitidos. Como el programador es inmigrante y solamente poseé NIE se ha permitido la utilización de este tipo de documento en el entorno de desarrollo.

Si el firmante no rellena algún campo o lo rellena con un dato invalido se le avisará con un mensaje de error, figura 3.8.

Una vez rellenado correctamente el formulario y presionando el botón de "Firmar", el sistema empezará a verificar si este formulario ya está firmado, si lo está aparecerá un mensaje de error : "Ya has firmado esta ILP", si no lo está se generará el XML a ser firmado en el servidor y se envirá un hash descrito en la sección 2.3.0.2. También en este paso se crea un filtro en formato RFC 2254 [18]. Este filtro evita que el firmante pueda firmar el XML de la ILP con un certificado que tenga datos distintos a los del formulario rellenado. Este filtro se pasa a la miniApplet por JS, lo que significa que un usuario con conocimientos avanzados podría intentar saltarse este filtro. Así que hay que

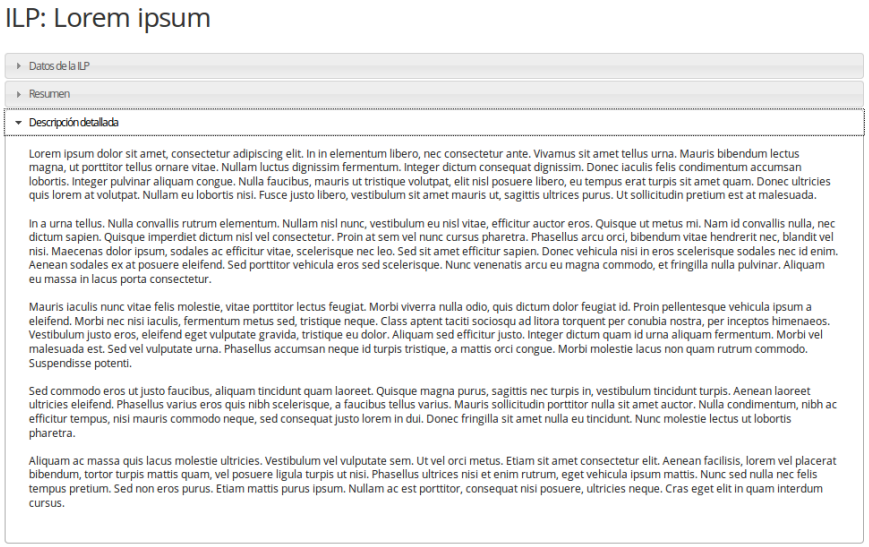


FIGURA 3.6: Descripción detallada de la ILP

FIGURA 3.7: Formulario de la ILP

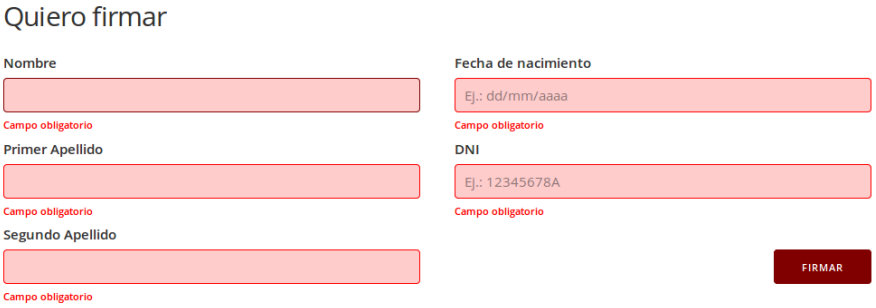


FIGURA 3.8: Ejemplo de errores del formulario de la ILP

implementar más soluciones para evitar que esta situación ocurra. Pero igualmente este filtro ya evitaría un gran número de errores por parte de firmantes honestos.

Con toda esta información el navegador mostrará otro mensaje de seguridad al firmante, figura 3.9. Si este no da su permiso, no se podrá seguir con la firma.

Una vez permitido el acceso del servidor al applet, este busca un certificado válido. Si no se encuentra un certificado digital con datos válidos, el firmante recibirá un mensaje de error de la Applet: "*El almacen no contenia entradas validas*". Este y los demás mensajes

FIGURA 3.9: Aviso de permitir acceso a la aplicación desde la web de firma

de error provenientes del miniApplet tienen que ser formateados para que el firmante pueda entenderlos. Si encuentra un certificado válido (o varios) pedirá al usuario que seleccione el certificado que quiere utilizar, figura 3.10.

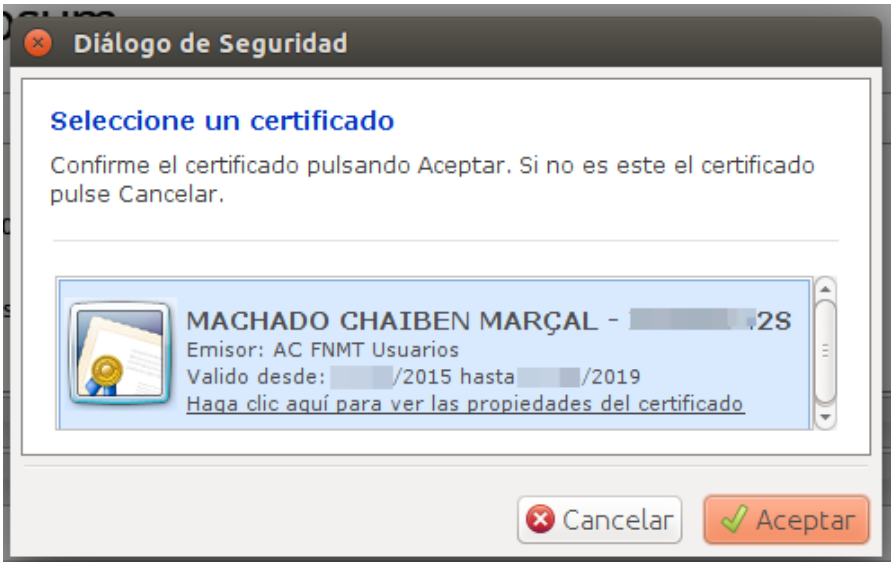
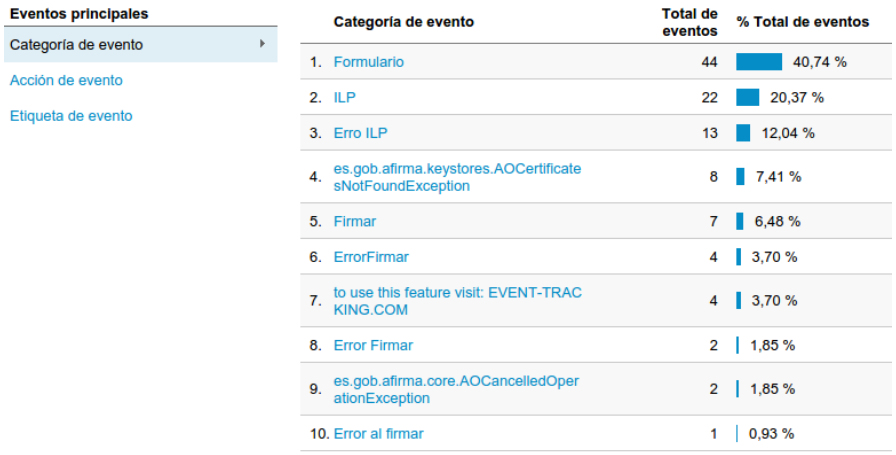


FIGURA 3.10: Selecciones un certificado

Una vez seleccionado el certificado el firmante hará clic en "Aceptar", enviando el formulario al servidor. Este verifica si el formulario firmado es válido y lo guarda en la base de datos. Hasta este momento tenemos una firma XAdES-BES implementada. A nivel de firma todavía quedan dos pasos por implementar. El primero es convertir la firma XAdES-BES en XAdES-EPES. El segundo es convertir de XAdES-EPES a XAdES-T. Una vez realizado eses pasos, tendremos la firma necesaria para la ILP.

3.1.4. Registro de los eventos - Google Analytics

Cualquier evento que realiza el firmante se registra en GA. La figura 3.11 y 3.12 muestran ejemplos de categorías y acciones recibidas. En la etiqueta "label" se guardan los datos relativos al proceso que el firmante está realizando, por ejemplo, si está realizando un envío del formulario, allí se encontraran los datos que utilizó para rellenar el formulario. Si está realizando una firma, se encontraran los datos del XML a ser firmado. El campo de value fue alimentado utilizando una secuencia basada en la secuencia de Fibonacci (1, 2, 3, 5, 8,...). Los valores representan que tan lejos llegó un usuario en el proceso de firma, ver cuadro 3.1.



Eventos principales

Categoría de evento

Acción de evento

Etiqueta de evento

	Categoría de evento	Total de eventos	% Total de eventos
1.	Formulario	44	40,74 %
2.	ILP	22	20,37 %
3.	Erro ILP	13	12,04 %
4.	es.gob.afirma.keystores.AOCertificatesNotFoundException	8	7,41 %
5.	Firmar	7	6,48 %
6.	ErrorFirmar	4	3,70 %
7.	to use this feature visit: EVENT-TRACKING.COM	4	3,70 %
8.	Error Firmar	2	1,85 %
9.	es.gob.afirma.core.AOCancelledOperationException	2	1,85 %
10.	Error al firmar	1	0,93 %

FIGURA 3.11: Ejemplo de categorías guardadas en GA

Eventos principales

Categoría de evento

Acción de evento

Etiqueta de evento

	Acción de evento	Total de eventos	% Total de eventos
1.	Validado	39	36,11 %
2.	Recibido	22	20,37 %
3.	Ya has firmado esta ILP.	19	17,59 %
4.	El almacen no contenia entradas validas	8	7,41 %
5.	ILP guardada en la base de datos	7	6,48 %
6.	to use this feature visit: EVENT-TRACKING.COM	4	3,70 %
7.	Erro de validación	3	2,78 %
8.	Error validación	2	1,85 %
9.	Operacion de seleccion de certificado cancelada	2	1,85 %
10.	sucess	1	0,93 %

FIGURA 3.12: Ejemplo de acciones guardadas en GA

Este método ayuda a identificar en que paso los firmante están teniendo más problemas y se puede buscar soluciones para evitarlos.

Cuadro 3.1: Valores básicos enviados a GA

Valor	**Descripción**
1	Error al validar el formulario
2	Formulario validado correctamente
3	Usuario ya ha firmado la ILP o hay un error de validación del formulario detectado en el servidor
5	Error al firmar el XML
8	ILP firmada correctamente

Capítulo 4

Conclusión

4.1. Próximos pasos

Hay muchos requerimientos para que este proyecto pueda seguir adelante, hago una lista de los principales:

- Implementar la firma XAdES-ESEP
- Implementar la firma XAdES-T
- Implementar la firma para dispositivos que no puedan utilizar Applets.
- Implementar la página donde el firmante pueda ver más información sobre la CP.
- Implementar la descarga de las firmas XML generadas para enviarlas al gobierno.
- Planear y implementar la página de administración de la CP.
- Implementar la página de informes para la CP.
- Validar el sistema con el Gobierno para que se pueda realizar una ILP.
- Realizar una ILP verdadera con este sistema.

Con estos puntos mínimos cumplidos y validados ya se podría empezar a distribuir este proyecto como la versión 1.0 de la plataforma.

4.2. Comentarios

Con este proyecto he podido realizar la base de una plataforma de firma ILP. Trabajar en un caso práctico de firma digital y las dificultades técnicas que están relacionadas con las mismas.

También he podido trabajar por primera vez con una herramienta de tests automatizados, PHPUnit y montar mi primer proyecto en Zend. Ya tenía conocimiento del framework pero no había montado nunca un proyecto desde cero.

He tenido muchos problemas con el programa de miniApplet v1.3 y no conseguí hacerlo funcionar correctamente. Al volver a la versión v1.2 sí que lo he conseguido. Otro problema con esta parte es que la documentación del gobierno es muy limitada y en los foros no se encuentra mucha ayuda sobre estos programas, faltan más ejemplos y manuales sobre el tema de firmas.

El proyecto realizado no ha cumplido con todos los requerimientos para la firma de las ILPs y todavía se necesitan muchos pasos para llegar al objetivo inicial de construir una plataforma completa de firmas que pueda ser utilizada de modo fácil por otros desarrolladores y las CP. Espero seguir desarrollando y contar la ayuda de otros programadores para conseguir la solución completa y hacer con que en el futuro esta sea una herramienta más de democracia al alcance de todos.

Bibliografía

[1] Junta Electoral Central. Boletín oficial del estado. Sec. III Pag.36601, Mayo 2012.

[2] MySQL. The world's most popular open source database. https://www.mysql.com/.

[3] Apache. http://httpd.apache.org/.

[4] PHP. Hypertext preprocessor. http://php.net/.

[5] Apache Tomcat. http://tomcat.apache.org/.

[6] clientE @firma. http://forja-ctt.administracionelectronica.gob.es/web/clienteafirma.

[7] Git. https://git-scm.com/.

[8] Marçal Machado Chaiben. Firma ilp. https://github.com/chaiben/FIRMA-ILP.

[9] Vagrant. https://www.vagrantup.com/.

[10] Puppet Labs. https://puppetlabs.com/.

[11] Zend Framework. http://framework.zend.com/.

[12] Desarrollo ágil de software. https://es.wikipedia.org/wiki/Desarrollo_ágil_de_software.

[13] PHPUnit. The php testing framework. https://phpunit.de/.

[14] Skeleton. Responsive css boilerplate. http://getskeleton.com/.

[15] jQuery. Write less, do more. https://jquery.com/.

[16] jQuery UI. User interface. https://jqueryui.com/.

[17] Selenium. Web browser automation. http://www.seleniumhq.org/.

[18] RFC 2254. The string representation of ldap search filters. http://www.faqs.org/rfcs/rfc2254.html.