Recogida de firmas para una ILP

Diseño e implementación

Índice de contenidos

1. Introducción

La Ley Orgánica 3/1984, de 26 de marzo, reguladora de la iniciativa legislativa popular [BOE1984], modificada por la Ley Orgánica 4/2006, de 26 de mayo [BOE2006], regula la participación directa de los ciudadanos en el proceso de producción normativa, derecho reconocido a su vez por la Constitución Española [BOE1978]. Este proceso, denominado como Iniciativa Legislativa Popular (ILP), permite a los ciudadanos presentar proposiciones de ley, apoyadas por un número mínimo de firmantes.

La modificación de la Ley Orgánica de 2006 [BOE2006] incorpora la mención explícita de la posibilidad de recoger las declaraciones de apoyo como firma electrónica, siempre que se garantice la voluntad auténtica del ciudadano que suscribe la iniciativa legislativa popular y conforme a lo que establezca la legislación correspondiente.

El Acuerdo de 10 de mayo de 2012, de la Junta Electoral Central, sobre el procedimiento para la verificación y certificación de las firmas de una iniciativa legislativa popular [BOE2012], precisa los aspectos más importantes del procedimiento para la recogida de firmas, especificando, entre otros, los requisitos técnicos recomendados para la recogida de firmas digitales para una ILP.

Este documento recoge el proceso de diseño, implementación, despliegue y test de una aplicación web mínima que permita recoger firmas digitales para iniciativas legislativas populares. El despliegue y test de la aplicación se realiza en el servidor de la Fundación para la Ciudadanía Global.

2. Análisis de requisitos

A continuación, se detallan los requisitos de la aplicación de recogida de firmas digitales para una ILP extraídos de las normativas vigentes ([BOE1984], [BOE2006] y [BOE2012]).

La Tabla 1 detalla los requisitos funcionales de la aplicación.

ID	Requisito	Origen
RF.1	El sistema debe permitir a los usuarios visualizar el título y la totalidad del texto de la proposición de ley (los pliegos para la recogida de firmas reproducirán el texto íntegro de la proposición).	[BOE1984] Art. 8
RF.2	El sistema debe permitir a los usuarios consultar el Acuerdo de aprobación de la JEC conforme se aprueba el sistema electrónico de recogida de firmas.	[BOE2012] Art. 3.2
RF.3	El sistema debe recoger los siguientes datos de los firmantes: primer apellido, segundo apellido, nombre, número del documento nacional de identidad o pasaporte y fecha de nacimiento, además de la marca de tiempo en las firmas electrónicas.	[BOE2012] Art. 1.1
RF.4	El sistema debe permitir a un elector ofrecer una declaración de apoyo a una ILP a través de una firma digital.	[BOE2006] [BOE2012]

Tabla 1. Requisitos funcionales

La Tabla 2 detalla los requisitos no funcionales de la

aplicación.

ID	Requisito	Origen
RNF.1	El sistema se desplegará en el servidor de la Fundación para la Ciudadanía Global.	FCG
RNF.1	El sistema debe permitir generar firmas digitales accediendo con los navegadores Chrome y Firefox en Windows y Linux desde entornos de escritorio.	FCG

Tabla 2. Requisitos no funcionales

La Tabla 3 detalla los requisitos relativos a las firmas digitales.

ID	Requisito	Origen
RS.1	Los datos del firmante deben almacenarse en un fichero XML con el formato indicado en el anexo [BOE2012].	[BOE2012] Art. 3.1
RS.2	Las firmas deben almacenarse en un fichero XML con el formato indicado en el anexo [BOE2012].	[BOE2012] Art. 3.1
RS.3	Los ficheros deben tener la nomenclatura especificada en el anexo [BOE2012].	[BOE2012] Art. 3.1
RS.4	El firmante debe de ser mayor de edad.	[BOE1984] Art. 1
RS.5	La firma electrónica será una firma electrónica avanzada.	[BOE2012] Art. 3.4
RS.6	El certificado electrónico de firma tiene que ser válido a la fecha de la firma.	[BOE2012] Art. 3.4
RS.7	El fichero firmado debe contener el código y título de la iniciativa legislativa popular.	[BOE2012] Art. 3.5 y Art. 5.1
RS.8	No serán válidas las firmas electrónicas recogidas con anterioridad al acuerdo favorable de la JEC.	[BOE2012] Art. 5.2
RS.9	El Documento Nacional de Identidad del firmante debe coincidir con el Documento Nacional de Identidad del certificado electrónico utilizado para la firma.	[BOE2012] Art. 5.3
RS.10	El certificado electrónico de firma tiene que estar reconocido por la sede electrónica del Instituto Nacional de Estadística.	[BOE2012] Art. 3.4 y Art. 5.4
RS.11	El certificado electrónico de firma no puede estar revocado.	[BOE2012] Art 5.4
RS.12	La firma tiene que ser válida (los datos firmados no pueden haber sido alterados después de la firma).	[BOE2012] Art 5.4
RS.13	En la medida en que sea indubitada la acreditación del firmante, se considerarán válidas las firmas electrónicas realizadas con un certificado caducado.	[BOE2012] Art 5.5

RS.14	Las firmas deben realizarse siguiendo la política de firma de la Administración General del Estado definida en (OID: 2.16.724.1.3.1.1.2.1.8).	[BOE2012] Anexo
RS.15	Dentro de esta política se recomienda la firma en formato XADES, clase básica, internally detached.	[BOE2012] Anexo

Tabla 3. Requisitos relativos a las firmas digitales

3. Diseño

En este apartado se recoge el diseño básico de la aplicación, detallando las pantallas que la conforman y el flujo de ejecución de la misma.

3.1 Pantallas básicas

La aplicación web de recogida de firmas digitales para una ILP consta de cinco pantallas básicas:

1. Texto de la ILP
2. Formulario datos personales
3. Firma correcta
4. Error en la firma
5. Error falta AutoFirma

Las tres primeras pantallas representan el flujo correcto de la realización de una firma digital por parte de un ciudadano. En primer lugar, se presenta el título y el texto completo de la ILP, junto con un enlace de descarga del Acuerdo de aprobación de la JEC conforme se aprueba el sistema de recogida de firmas digitales. Si el ciudadano procede a firmar la ILP, se muestra un formulario de recogida de los datos mínimos necesarios para registrar la firma correctamente.

Una vez introducidos los datos personales (y siempre que el formato de los mismos sea válido) el ciudadano puede proceder a la firma de la ILP. La firma digital es gestionada por la aplicación de firma digital del Ministerio de Asuntos Económicos y Transformación Digital, AutoFirma, que es lanzada automáticamente al pulsar el botón de firma de la pantalla. Si la firma se ha realizado correctamente, se muestra la pantalla que confirma al ciudadano que se ha recibido la firma correctamente.

El proceso de firma generará un error si el usuario no dispone del software AutoFirma instalado en su sistema. En este caso, se mostrará una pantalla informando al usuario de la situación, con enlaces e indicaciones para su instalación.

El proceso de firma puede generar errores en otras situaciones, por ejemplo, si el DNI introducido por el usuario en el formulario no se corresponde con el DNI especificado en el certificado, si el certificado ha sido emitido por una autoridad de certificación no reconocida, etc. (la especificación de las casuísticas que generan un error en el proceso de firma se detalla más adelante). En estos casos, se mostrará una pantalla de error informando al usuario de que la firma no se ha podido completar con éxito.

3.2 Flujo de la aplicación

La Figura 1 detalla el diagrama de flujo de la aplicación, donde se pueden observar las transiciones entre las diferentes pantallas mencionadas en el apartado anterior, así como las casuísticas que pueden generar que se rechace una firma.

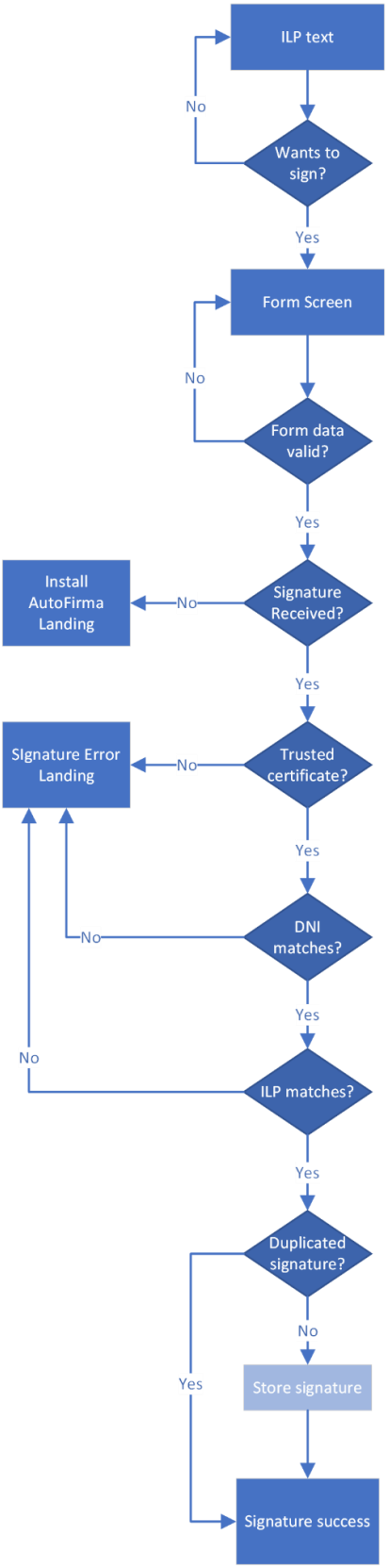

Figura 1. Diagrama de flujo de la aplicación.

4. Implementación

4.1. Tecnologías

La aplicación de recogida de firmas digitales para una ILP se ha implementado como una aplicación web con el framework de PHP Symfony 5.4 (la LTS vigente actualmente), usando una base de datos MariaDB 10.3.

La aplicación de recogida de firmas digitales delega en la aplicación del Ministerio AutoFirma [AF2022] la generación de las firmas electrónicas. Para ello, se utiliza el plugin de javascript AutoScript versión 1.7.0 (y la versión de AutoFirma que tenga el cliente instalada en su máquina localmente).

4.2. Formato del documento a firmar

Tal como se indica en el Acuerdo de 10 de mayo de 2012 sobre el procedimiento para la verificación y certificación de las firmas de una iniciativa legislativa popular [BOE2012], el formato del fichero XML[1] antes de ser firmado es el siguiente:

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

[1] La estructura y restricciones de contenido del fichero anterior quedan definidas también en el Anexo de [BOE2012] (y no se reproducen de nuevo en este documento).

4.3. Formato de las firmas

La aplicación de recogida de firmas digitales para ILPs delega en la aplicación del Ministerio AutoFirma [AF2022] la generación de las firmas electrónicas. Con el objetivo de cumplir con los requisitos y recomendaciones especificadas para las firmas digitales detalladas en el Acuerdo sobre el procedimiento para la verificación y certificación de las firmas de una iniciativa legislativa popular [BOE2012], se procede a configurar AutoFirma para usar la política de firma electrónica basada en certificados de la Administración General del Estado v1.8 [PF2010], con los siguientes parámetros:

```
 expPolicy=FirmaAGE18
policyIdentifier=urn:oid:2.16.724.1.3.1.1.2.1.8
policyIdentifierHash=V8lVVNGDCPen6VELRD1Ja8HARFk=
 policyIdentifierHashAlgorithm=http://www.w3.org/2000/09/xmldsig#sha1
policyQualifier=https://administracionelectronica.gob.es/es/ctt/politicafirma/politica_firma_AGE_v1_8.pdf
 format=XAdES Detached
mode=implicit
```

El fichero XML que contiene los datos firmados y la firma XAdES se almacena con el nombre ILPAAAANNN.DDDDDDDDD.XML, donde ILPAAAANNN es el código de la ILP y DDDDDDDDD es el documento nacional de identidad de la persona que firma.

4.4. Requisitos cubiertos por la implementación

A continuación se detalla el comportamiento de la aplicación con relación a los requisitos especificados en la Sección 2.

Todos los requisitos especificados en la Sección 2 se cumplen totalmente, a excepción de las consideraciones mencionadas a continuación:

- Para la comprobación de la mayoría de edad del firmante [RS.4], se asume la veracidad de los datos introducidos por el firmante en el formulario (dado que esta información no está incluída en el certificado digital que presenta el firmante y que no se accede a datos externos).
- En relación a la caducidad del certificado electrónico usado para firmar ([RS.6] y [RS.13]), se delega en la configuración de AutoFirma la aceptación o no de certificados caducados.
- La aplicación no comprueba el estado de revocación del certificado usado para firmar [RS.11], dado que la aplicación del Ministerio para dicha validación requiere de

la intervención manual de un humano (por el uso de Captchas y la falta de una API pública).

- La aplicación valida que el XML con la firma enviado por AutoFirma contiene los datos correctos de la ILP [RS.7] pero asume que la firma realizada por AutoFirma es válida [RS.12] (es decir, no hace una comprobación adicional de la validez de la firma electrónica enviada), dadas las limitaciones del software instalado en el servidor de la Fundación.
- El sistema solo acepta la identificación del firmante mediante DNI (siguiendo el formato especificado para el XML con los datos del firmante [RS.1]), por lo que la identificación del firmante con pasaporte [RF.3] no se contempla.

5. Batería de pruebas

A continuación se detallan las pruebas realizadas de la aplicación de firmas digitales para ILPs.

Se han realizado pruebas con cuatro configuraciones distintas:

- Sistema Operativo Linux Ubuntu 20.04.4 con navegador Chrome 99.0.4844.84
- Sistema Operativo Linux Ubuntu 20.04.4 con navegador Firefox 98.0.2
- Sistema Operativo Windows 7 Professional con navegador Chrome 100.0.4896.75
- Sistema Operativo Windows 7 Professional con navegador Firefox 99.0

todas ellas con la última versión de AutoFirma instalada (a excepción de la prueba E.6, que consiste en el intento de firma sin tener el software previamente instalado).

Las pruebas realizadas consisten en seguir el procedimiento de firma correctamente (C.1), interrumpir el proceso de firma por parte del usuario (C.2) o bien en intentar forzar un proceso erróneo (pruebas E.X). En el caso de los errores, un tratamiento correcto implica que no se permite continuar con el procedimiento y, si procede, se informa al usuario del error detectado.

La Tabla[2] siguiente recoge los resultados de las pruebas realizadas.

ID	Sistema Operativo	Linux		Windows	
	Navegador	Chrome	Firefox	Chrome	Firefox
C.1	Proceso de firma correcto	✓	✓	✓	✓
C.2	Proceso de firma interrumpido por el usuario	✓	✓	✓	✓
E.1	Formulario incompleto	✓	✓	✓	✓
E.2	Fecha de nacimiento formato inválido	✓	✓	✓	✓
E.3	Fecha de nacimiento en el futuro	✓	✓	✓	✓

[2] Los iconos usados en la tabla tienen una licencia libre y han sido descargados de Vecteezy.

E.4	Fecha de nacimiento menor de edad	✓	✓	✓	✓
E.5	Formato DNI inválido	✓	✓	✓	✓
E.6	AutoFirma no instalado	✓	✓	✓	✓
E.7	Certificado personal ausente	✓	✓	✓	✓
E.8	Certificado personal de autoridad no reconocida	✓	✓	✓	✓
E.9	DNI formulario no coincidente con certificado	✓	✓	✓	✓
E.10	Código ILP inválido en la firma	✓	✓	✓	✓
E.11	Firma duplicada	✓	✓	✓	✓
E.12	Firma sin ver el texto de la proposición	✓	✓	✓	✓

6. Bibliografía

[AF2022] Portal Administración Electrónica - Firma Electrónica - Descargas, Ministerio de Asuntos Económicos y Transformación Digital · Secretaría General de Administración Digital https://firmaelectronica.gob.es/Home/Descargas.html

[BOE1978] Constitución Española. Cortes Generales «BOE» núm. 311, de 29 de diciembre de 1978, páginas 29313 a 29424 (Referencia: BOE-A-1978-31229) https://www.boe.es/eli/es/c/1978/12/27/(1)

[BOE1984] Ley Orgánica 3/1984, de 26 de marzo, reguladora de la iniciativa legislativa popular. Jefatura del Estado «BOE» núm. 74, de 27 de marzo de 1984 (Referencia: BOE-A-1984-7249), actualizada el 31 de marzo de 2015. https://www.boe.es/eli/es/lo/1984/03/26/3/con

[BOE2006] Ley Orgánica 4/2006, de 26 de mayo, de modificación de la Ley Orgánica 3/1984, de 26 de marzo, reguladora de la Iniciativa Legislativa Popular. Jefatura del Estado «BOE» núm. 126, de 27 de mayo de 2006, páginas 19944 a 19946 (Referencia: BOE-A-2006-9290) https://www.boe.es/eli/es/lo/2006/05/26/4

[BOE2012] Acuerdo de 10 de mayo de 2012, de la Junta Electoral Central, sobre el procedimiento para la verificación y certificación de las firmas de una iniciativa legislativa popular. Jefatura del Estado «BOE» núm. 120 (Referencia: BOE-A-2012-6675), de 19 de mayo de 2012, páginas 36601 a 36607 (7 págs.). https://www.boe.es/eli/es/a/2012/05/10/(1)

[PF2010] Política de firma electrónica basada en certificados, Consejo Superior de Administración Electrónica, v 1.8 (OID: 2.16.724.1.3.1.1.2.1.8), de 11 de octubre de 2010.