Plataforma de recollida de signatures digitals per a Iniciatives Legislatives Populars

Carlos López Martínez
Enginyeria Tècnica d'Informàtica de Sistemes

Cristina Pérez Solà
15 de Juny de 2012

Vull dedicar el projecte a la meva família, en especial a la meva companya Ana i al meu fill Eidur, per el seu suport i paciència en el transcurs dels estudis.

També vull agrair a la consultora Cristina Pérez Solà la seva ajuda sempre que ho he necessitat.

RESUM

En l'actualitat existeixen pocs mètodes per a que un ciutadà pugui participar de forma directa en les tasques d'elaboració de les normes que regeixen el seu país. La Constitució ens dóna aquesta possibilitat mitjançant les Iniciatives Legislatives Populars (ILPs).
Per que una iniciativa pugui ser pressa en consideració ha de passar per infinitat de processos, però un dels més complicats al que s'han d'enfrontar les comissions promotores és la recollida de 500.000 signatures en un període limitat de nou mesos.
Per facilitar aquest procés podem aprofitar les noves tecnologies i concretament les signatures digitals.

El TFC s'encarregarà bàsicament de desenvolupar una plataforma web on les comissions promotores puguin donar-se d'alta per publicar i gestionar diferents ILPs.
La plataforma ha de oferir la possibilitat als ciutadans de signar les diferents ILPs , d'una forma intuïtiva i accessible, fent ús de certificat digitals o el DNI electrònic.
També ha de comprovar que les signatures recollides compleixin tots els requeriments de la legislació vigent per tal que tinguin validesa legal.

La plataforma utilitzarà com a servidor web (*Apache*), servidor de base de dades (*MySQL*), llenguatge de programació PHP i executarà en els clients l'applet Java de signatura Id@zki. Finalment la signatura digital tindrà un format XAdES-X-L *internally enveloped*.

PARAULES CLAU

Iniciativa Legislativa Popular, comissió promotora, plataforma, signatura digital, XML, XAdES, certificat digital,DNI electrònic, web, PHP, Apache, MySQL, JavaScript,.

ÀREA

Seguretat Informàtica

Índex de continguts

Índex de figures

Índex de taules

CAPÍTOL 1. INTRODUCCIÓ.

1.1. Justificació del TFC i context: punt de partida i aportació del TFC.

Les Iniciatives Legislatives Populars (en endavant ILPs) són un procés mitjançant el qual els ciutadans de l'Estat espanyol poden presentar proposicions de llei subscrites per un nombre mínim de persones. El principal problema que presenta elaborar una iniciativa d'aquest tipus és la recollida de les 500.000 firmes necessàries per dur-la a terme en el període màxim establert de nou mesos.

Davant d'aquest problema, farem ús de tecnologies com la signatura digital per implementar una plataforma de recollida de signatures amb la finalitat d'agilitzar aquest procés, facilitant la creació i gestió d'aquestes iniciatives. Per fer-la el més accessible possible a tots els ciutadans, s'incorporarà la funcionalitat de signar no només amb un certificat digital instal·lat en el navegador, sinó també amb el certificat digital inclòs en el DNI electrònic.

La plataforma ha de permetre tant gestionar la creació d'aquestes proposicions per part de la comissió promotora, com la signatura de les mateixes per part dels ciutadans interessats en subscriure les iniciatives.

Per tal que les ILPs creades amb la plataforma tinguin validesa legal, la plataforma haurà de contemplar el correcte compliment de la legislació vigent de les ILPs.

1.2. Objectius del TFC.

1.- Implementar una plataforma que reculli signatures digitals per a realitzar iniciatives Legislatives Populars (ILPs) .

2.- Permetre gestionar la creació de proposicions per part de la comissió promotora i la signatura de les mateixes per part dels ciutadans.

3.- Ser el més accessible possible per evitar que els usuaris desisteixin de participar en una iniciativa i així maximitzar el nombre de signatures vàlides.

4.- Comprendre el funcionament de les ILPs i de la seva legislació, de forma que les signatures recollides per la plataforma tinguin validesa legal i puguin ser utilitzades per formalitzar la iniciativa.

5.- Integrar els coneixements que he adquirit durant la carrera i utilitzar principalment els coneixements en seguretat informàtica i criptografia per implementar els mecanismes de seguretat necessaris (signatura digital, segell de temps,...) per complir amb la legislació vigent.

1.3. Enfocament i mètode seguit.

Per tenir un mínim de garanties de que qualsevol projecte pugui realitzar-se amb el termini establert i fer-ho amb el màxim de qualitat, és fonamental la definició de quina metodologia s'ha d'emprar i tenir coneixement de les eines que es poden utilitzar per portar a terme el projecte.

1.3.1. Metodologia

En principi, després d'una petita anàlisi, em vaig decidir per desenvolupar el TFC seguint les etapes previstes en un cicle de vida clàssic o en cascada, ja que els requisits de la plataforma estaven completament definits i no canviarien al llarg del termini establert per realitzar el TFC.
Les etapes d'aquest cicle de vida són:

1. Anàlisi prèvia: En aquesta fase he definit a grans trets el sistema de programari necessari per realitzar el TFC.
2. Anàlisi de requisits: He analitzat totes les necessitats de la plataforma i definit una especificació detallada dels requisits.
3. Disseny: He donat solució a totes les necessitats i requisits de l'etapa anterior (arquitectura general, estructures de dades, interfícies, ...)
4. Programació: He generat el codi que reflecteix les especificacions de la fase anterior.
5. Prova: He localitzat i corregit tots els errors de la plataforma.
6. Manteniment.

En general m'he mantingut fidel al cicle de vida clàssic, però a la part final he utilitzat una mica de programació exploratòria, és a dir, una vegada finalitzada la plataforma vaig realitzar petits canvis per millorar la usabilitat i adaptar-me a la nova normativa.

1.3.2. Eines

Per cobrir tots els objectius de la plataforma, en la anàlisi prèvia vaig pensar en utilitzar el llenguatge de programació PHP per crear les pàgines web dinàmiques, on les comissions promotores es podrien donar d'alta i gestionar les seves iniciatives i on els usuaris podrien signar-les, un servidor web (Apache) per servir-les i una base de dades (Postgres o MySql) on emmagatzemar tota l' informació rellevant .

A la vegada s'hauria de implementar un applet de signatura digital (@firma, CryptoApplet, Id@zki) que tingués una amplia compatibilitat amb diferents sistemes operatius i navegadors per tal de facilitar l'experiència a l'usuari, i així evitar que desistís de participar en una iniciativa per problemes tècnics a l'hora de signar.

Finalment, com a format de signatura electrònica s'utilitzaria XAdES-C (*XML Advanced Electronic Signatures complete*), ja que ens donaria la totalitat dels requisits per que una ILP tingués validesa legal.

1.4. Planificació del projecte.

NOM	DURADA	INICI	FINAL
PAC2	35 dies	10/03/2012	13/04/2012
Anàlisi i disseny del TFC	35 dies	10/03/2012	13/04/2012
Anàlisi de requisits	9 dies	10/03/2012	18/03/2012
Disseny d'estructures de dades	8 dies	19/03/2012	26/03/2012
Arquitectura de l'aplicació	7 dies	27/03/2012	02/04/2012
Disseny base de dades	5 dies	03/04/2012	07/04/2012
Disseny interfícies gràfiques	6 dies	08/04/2012	13/04/2012
PAC3	35 dies	14/04/2012	18/05/2012
Anàlisi i disseny del TFC	15 dies	14/04/2012	28/04/2012
Algoritmes d'alt nivell	7 dies	14/04/2012	20/04/2012
Altres (Diagrama de flux, esquema protocols, ..)	8 dies	21/04/2012	28/04/2012
Implementació	20 dies	29/04/2012	18/05/2012
PAC4	28 dies	19/05/2012	15/06/2012
Generació joc de proves	7 dies	19/05/2012	25/05/2012
Implementació del DNI electrònic	15 dies	26/05/2012	09/06/2012
Resolució d'incidències	6 dies	10/06/2012	15/06/2012
Memòria	98 dies	10/03/2012	15/06/2012
Redacció i correcció de la memòria	98 dies	10/03/2012	15/06/2012
Presentació	14 dies	09/06/2012	22/06/2012

Taula 1 - Planificació del TFC.

A la següent figura es mostra la planificació de forma gràfica:

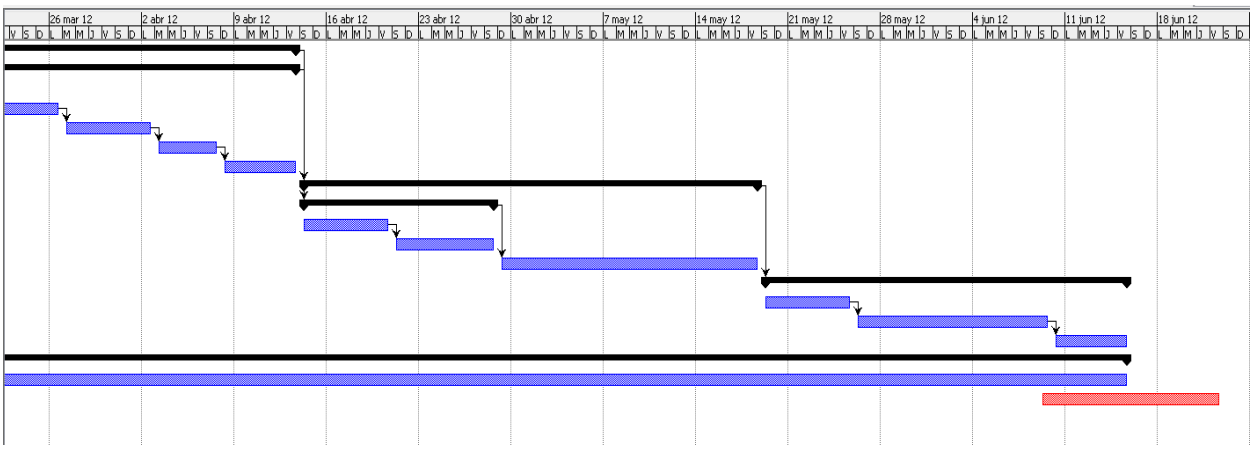

Figura 1 - Planificació del TFC.

1.5. Productes obtinguts.

El producte obtingut és una plataforma web, on les comissions poden donar-se d'alta i gestionar tant les ILPs que introdueixin, com les signatures que es recullin. També oferirà als ciutadans la possibilitat de signar aquestes ILPs de forma fàcil, i que les seves signatures tinguin validesa legal per utilitzar-se a l'hora de formalitzar la ILP.

1.6. Breu descripció dels altres capítols.

CAPÍTOL 2. MARC JURÍDIC I NORMATIU: Es resumeix el marc jurídic i normatiu utilitzat a la plataforma , és a dir, les lleis i normatives que regeixen les ILPs i les signatures digitals.

CAPÍTOL 3. ELEMENTS CRIPTOGRÀFICS: Es descriuen teòricament tots els elements criptogràfics que utilitza la plataforma.

CAPÍTOL 4. DISSENY: Es dóna solució a totes les necessitats i requisits de la plataforma, o sia, es dissenyen les estructures de dades, interfícies gràfiques; es realitzen diagrames de casos d'ús i de flux, i finalment s'estableix quin tipus i estructura han de tenir les signatures digitals.

CAPÍTOL 5. JOC DE PROVES: S'agrupen les principals proves a les quals ha estat sotmesa la plataforma.

CAPÍTOL 6. CONCLUSIONS: S'exposa com s'han assolit els objectius del TFC i totes les experiències i consideracions que s'han tingut en el transcurs del TFC.

CAPÍTOL 7. LÍNIES DE FUTUR: Es descriuen diversos aspectes de la plataforma que es podrien millorar.

CAPÍTOL 2. MARC JURÍDIC I NORMATIU.

Atès que quan es va iniciar el TFC no existia una regulació clara de l'ús de signatures digitals en les Iniciatives Legislatives Populars, la plataforma es fonamenta en el marc jurídic i normatiu present fins aleshores; és a dir:

- La Llei orgànica 3/1984, de 26 de març, reguladora de la Iniciativa Legislativa Popular.
- La Llei orgànica 4/2006, de 26 de maig, de modificació de la Llei orgànica 3/1984, de 26 de març, reguladora de la Iniciativa Legislativa Popular.
- La Llei 59/2003, de 19 de desembre, de signatura electrònica.

Amb la sortida de l'acord del 10 de maig del 2012 de la *Junta Electoral Central* (JEC) sobre el procediment per la verificació i certificació de les signatures d'una iniciativa legislativa popular, s'han adaptat petites parts de la plataforma per incloure algun dels requisits que s'expressen en l'acord.

2.1. Llei orgànica 3/1984, de 26 de març, reguladora de la Iniciativa Legislativa Popular

La Llei orgànica 3/1984, de 26 de març, reguladora de la Iniciativa Legislativa Popular ens descriu per primera vegada que és i com es regula una ILP.

Les ILPs són instruments que ofereixen als ciutadans la possibilitat d'una participació directa en la tasca d'elaboració de les normes que regeixen la seva vida i la dels seus conciutadans, i possibilita, d'altra banda, l'obertura de vies per proposar al poder legislatiu l'aprovació de normes.

A grans trets aquets són els punts principals d'aquesta llei:

- Qualsevol ciutadà espanyol major d'edat que estigui inscrit en el cens electoral pot exercir la iniciativa legislativa, d'acord amb el que disposa aquesta Llei orgànica.

- Estan excloses de la iniciativa legislativa popular les matèries següents:

    - Les que, segons la Constitució, són pròpies de lleis orgàniques
    - Les de naturalesa tributària.
    - Les de caràcter internacional.
    - Les referents a la prerrogativa de gràcia.
    - Les esmentades als articles 131 i 134.1 de la Constitució.

- La iniciativa popular s'exerceix mitjançant la presentació de proposicions de llei subscrites per les signatures d'almenys 500.000 electors autenticades en la forma que determina aquesta Llei.

- S'ha de presentar un escrit amb:

    - El text articulat de la proposició de llei, precedit d'una exposició de motius.
    - Un document en què es detallin les raons que aconsellen, segons el parer dels signants, la tramitació i aprovació per les cambres de la proposició de llei.
    - La relació dels membres que componen la Comissió Promotora de la iniciativa, amb expressió de les dades personals de tots ells.

- El procediment s'inicia mitjançant la presentació davant la Mesa del Congrés dels Diputats, a través de la seva Secretaria General, de la documentació exigida.

- La Mesa del Congrés dels Diputats ha d'examinar la documentació remesa i s'ha de pronunciar. Si no s'admet la proposició de llei, la Comissió Promotora pot interposar davant el Tribunal Constitucional un recurs d'empara.

  Si, en canvi, la proposició s'admet, la Mesa del Congrés ho ha de comunicar a la JEC, que ha de garantir la regularitat del procediment de recollida de signatures.

  Després la JEC ha de notificar-ho a la Comissió Promotora, per tal que procedeixi a la recollida de les signatures requerides.

- Rebuda la notificació d'admissió de la proposició, la Comissió Promotora ha de presentar davant la Junta Electoral Central, en paper d'ofici, els plecs necessaris per a la recollida de signatures. Aquests plecs han de reproduir el text íntegre de la proposició. Un cop la Junta Electoral Central ha rebut els plecs, aquesta, dins les quaranta-vuit hores següents, els ha de segellar, numerar i tornar a la Comissió Promotora.

- El procediment de recollida de signatures finalitza amb el lliurament a les juntes electorals provincials de les signatures recollides, en el termini de sis mesos a comptar de la notificació. Aquest termini es pot prorrogar tres mesos quan es doni una causa major apreciada per la Mesa del Congrés. Exhaurit el termini sense que s'hagi fet el lliurament de les signatures recollides, la iniciativa caduca.

- Una vegada remesos els plecs a la Junta Electoral Central, aquesta ha de procedir a la seva comprovació i recompte definitius. Les signatures que no reuneixin els requisits exigits en aquesta Llei es declaren invàlides i no es computen.

- Per autenticar les signatures,al costat de la signatura de l'elector se n'ha d'indicar el nom i cognoms, número del document nacional d'identitat i municipi en les llistes electorals del qual estigui inscrit. A més, la signatura ha de ser autenticada per un notari, per un secretari judicial o pel secretari municipal corresponent al municipi en el cens electoral del qual estigui inscrit el signant. També ha d'indicar la data i pot ser col·lectiva, plec per plec, en aquest cas, al costat de la data s'ha de consignar el nombre de signatures que conté el plec.

- Les signatures també poden ser autenticades per fedataris especials designats per la Comissió Promotora. Els fedataris són ciutadans espanyols que, en plena possessió dels seus drets civils i polítics i sense antecedents penals, jurin o prometin davant les juntes electorals provincials, donar fe de l'autenticitat de les signatures dels signataris de la proposició de llei.

- Comprovat el compliment dels requisits exigits per a la presentació vàlida de la proposició, la Junta Electoral Central ha d'elevar al Congrés dels Diputats un certificat acreditatiu del nombre de signatures vàlides i procedir a destruir els plecs de signatures que estiguin en el seu poder.

- Un cop rebuda la notificació que acrediti que s'ha reunit el nombre de signatures exigit, la Mesa ordena la publicació de la proposició, i comença la seva tramitació parlamentària.

2.2. Llei orgànica 4/2006, de 26 de maig, de modificació de la Llei orgànica 3/1984, de 26 de març, reguladora de la Iniciativa Legislativa Popular.

La Llei orgànica 4/2006, de 26 de maig introdueix principalment les següents modificacions a la Llei orgànica 3/1984, de 26 de març, reguladora de la Iniciativa Legislativa Popular:

- Es suprimeix de l'escrit de presentació el document en què es detallen les raons que aconsellen, segons el parer dels signants, la tramitació i aprovació per les cambres de la proposició de llei.
- S'amplia el termini de recollida de signatures de sis a nou mesos.
- S'estableix l'ús de la signatura electrònica, com a mètode vàlid de recollida de signatures.
- S'autoritza l'ús de les llengües cooficials conjuntament amb el castellà per als plecs de recollides de signatures.

2.3. Llei 59/2003, de 19 de desembre, de signatura electrònica

La Llei 59/2003 de 19 de desembre, de signatura electrònica, regula la signatura electrònica, la seva eficàcia jurídica i la prestació de serveis de certificació.
Dins d'aquesta llei els articles que més afecten al desenvolupament de la plataforma són:

- Article 3. Signatura electrònica i documents signats electrònicament: Aquest article ens defineix la signatura electrònica o digital, signatura electrònica avançada i signatura electrònica reconeguda. També ens diu que la signatura electrònica reconeguda té el mateix valor que la signatura manuscrita.

- Tots els articles relatius a certificats electrònics :
  - Article 6. Concepte de certificat electrònic i de signant.
  - Article 8. Extinció de la vigència dels certificats electrònics.
  - Article 9. Suspensió de la vigència dels certificats electrònics.
  - Article 10. Disposicions comunes a l'extinció i la suspensió de la vigència de certificats electrònics.

- Article 11. Concepte i contingut dels certificats reconeguts: Aquest article ens defineix els certificats reconeguts com els certificats electrònics expedits per un prestador de serveis de certificació que compleix els requisits que estableix aquesta Llei. Aquets requisits fan referència a la comprovació de la identitat i altres circumstàncies dels sol·licitants, a la fiabilitat i a les garanties dels serveis de certificació que prestin.

2.4. Acord del 10 de maig del 2012, de la Junta Electoral Central, sobre el procediment per la verificació i certificació de les signatures d'una iniciativa legislativa popular

L' acord del 10 de maig del 2012, de la Junta Electoral Central, sobre el procediment per la verificació i certificació de les signatures d'una iniciativa legislativa popular, a posat fi a les controvèrsies a l'hora de definir quins requeriments són necessaris per que un sistema digital de recollida de signatures sigui vàlid; ja que fins a aquest moment la JEC havia d' acordar el sistema ,cas a cas,amb la Comissió Promotora corresponent.
Els punts principals de l'acord són:

- Les dades obligatòries per acreditar la condició de signant són: primer cognom, segon cognom, nom, document nacional d'identitat i data de naixement i una marca de temps en les signatures digitals. No són necessàries les dades relatives al domicili, ni a la província i municipi de naixement.

- La JEC haurà d'aprovar el sistema de recollida de signatures de la Comissió Promotora i una vegada aprovat li donarà un codi identificatiu únic.

- A efectes de presentació d'una iniciativa legislativa , una signatura digital serà valida sempre que sigui avançada i que es fonamenti en un certificat vàlid al moment de signar, aquest certificat ha d'estar reconegut per les administracions públiques i publicat a la seu electrònica del INE (Instituto Nacional de Estadística).

- La JEC annexa l'esquema de l'arxiu XML amb les dades del signant que haurien de ser signades seguint la política de signatura de l'Administració General de l'Estat [POLFIRMA]. Dins d'aquesta política es recomana la signatura en format XAdES -BES *internally detached* (es pot veure detallat al capítol 3.1.3).

CAPÍTOL 3. ELEMENTS CRIPTOGRÀFICS

3.1. Signatures digitals

La signatura digital o electrònica és un conjunt de dades associades a un missatge que ens permet verificar la identitat del signant i la integritat del missatge. Es basa en la criptografia asimètrica o de clau pública.

3.1.1. Procés de signat

La signatura digital es realitza, de forma resumida, de la següent forma:

- El signant disposa d'un certificat amb les seves claus associades, una pública i una altre privada.

- El signant utilitza una funció resum (SHA,MD5,...)per obtenir el resum de les dades a signar i el xifra amb la seva clau privada (RSA,DSA,ElGammal,Diffie-Hellman,..). Tot això, dóna com a resultat una signatura digital que s'afegeix al missatge original.

- Una vegada s'han enviat les dades, el receptor desxifra la signatura adjunta amb la clau pública de l'emissor per obtenir el resum generat pel signant.

- El receptor aplica la funció resum sobre les dades originals i compara el resum obtingut amb el resum que ha rebut del signant. Si són iguals, la firma és valida garantint la integritat de les dades així com la identitat del signant. En cas contrari la signatura no és valida ja que les dades han sigut vulnerades.

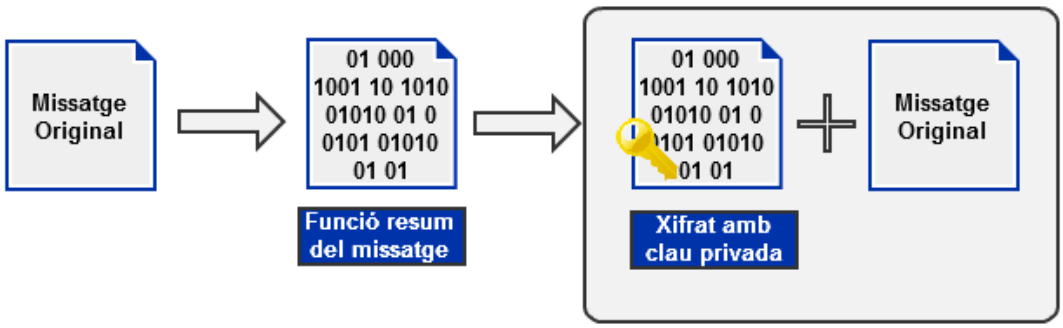

Figura 2- Signatura digital. Perspectiva de l'emissor.

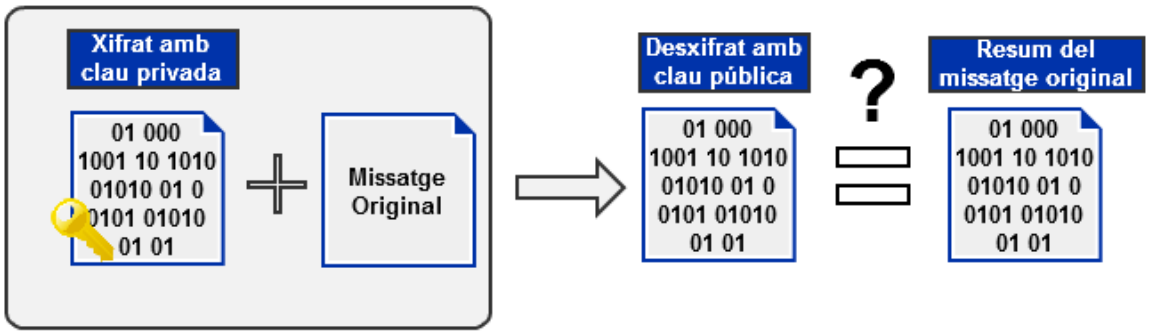

Figura 3 - Signatura digital. Perspectiva del receptor.

3.1.2. Tipus de signatures digitals

L'actual llei de signatures digitals contempla tres tipus de signatures:

- Signatura bàsica: Conté un conjunt de dades recollides de forma electrònica que identifiquen formalment a l'autor i s'afegeixen al propi document.

- Signatura avançada: Permet identificar al signant i detectar qualsevol canvi futur a les dades signades. Està vinculada de forma única al signant i a les dades. S'ha de generar a través de mitjans que el signant tingui sota el seu exclusiu control.

- Signatura reconeguda: Té les mateixes característiques que la signatura avançada però es fonamenta en un certificat reconegut i ha estat generada amb un dispositiu segur de creació de signatures. Té el mateix valor legal que la firma manuscrita.

En la pràctica també apareixen altres tipus de signatures digitals relatius a la inclusió de marques de temps o a la comprovació de la validesa dels certificats.

- Signatura amb segell temporal: Signatura digital a la que se li ha afegit un segell de temps. El segellat de temps (*timestamping*) és un mecanisme que ens permet demostrar que una sèrie de dades han existit i no han sigut alterades des d' un instant específic de temps. L'autoritat de segellat de temps (TSA, de l'anglès *Time Stamping Authority*) actua com a tercera part de confiança donant testimoni de l'existència de les dades en una data i hora concretes.

- Signatura validada o completa: Signatura digital amb segell temporal a la que se li ha afegit informació relativa a la validesa del certificat provinent d'una consulta de OCSP (*Online Certificate Status Protocol*) o CRL (*Certificate Revocation List*) realitzada a una VA (*Validation Authority*)

- Signatura longeva o de llarga durada: Es tracta d'una signatura digital validada que té validesa al llarg del temps. Això s'aconsegueix incloent a la signatura tots els certificats de la cadena de confiança i el resultat de la seva comprovació de validesa en el moment que es va realitzar la signatura. També es pot realitzar una actualització regular dels segells de temps i tornar a signar la signatura. Aquest procés s'utilitza per garantir que les dades que es van signar amb un algoritme que en el seu moment era vàlid, però actualment insegur degut a l'evolució tecnològica, no perdin el seu valor ja que s'han tornat a signar amb algoritmes criptogràfics segurs.

3.1.3. Formats de signatura digital

Existeixen diferents formats de signatura digital que ens aporten tots els elements necessaris per crear una signatura digital avançada o reconeguda.
Formats bàsics com:

- PKCS#7 (*Public –Key Cryptographic Standard #7*)/CMS (*Cryptographic Message Syntax*): Aquest format, inicialment elaborat per RSA (*Rivest, Shamir I Adleman*) i adoptat per la IETF (*Internet Engineering Task Force*), s'utilitza per signar, resumir, autenticar o xifrar electrònicament el contingut d'un missatge. CMS, com a evolució del format PKCS#7, descriu la sintaxis d'encapsulació per la protecció de les dades; els seus valors es generen utilitzant la codificació ASN.1/BER (*Abstract Syntax Notation One/Basic Encoding Rules*) i permeten incloure més d'un signant.

- Signatura XML/XML-DSig (*eXtensible Markup Language Digital Signature*): Aquest format definit com a recomanació del W3C (*World Wide Web Consortium),* és utilitzat freqüentment en aplicacions on-line. És bastant semblant al format CMS, però la codificació original de les signatures i certificats es realitza en el format Base64.

  Existeixen tres modes:

  - *enveloped*: La signatura s'afegeix al final del document XML com un element més.
  - *enveloping*: La signatura està inclosa en el document i aquest conté internament el contingut signat.
  - *detached*: La signatura i el document estan separats en dos arxius (*externally detached*) o també en el mateix arxiu però en estructures independents *(internally detached)*.

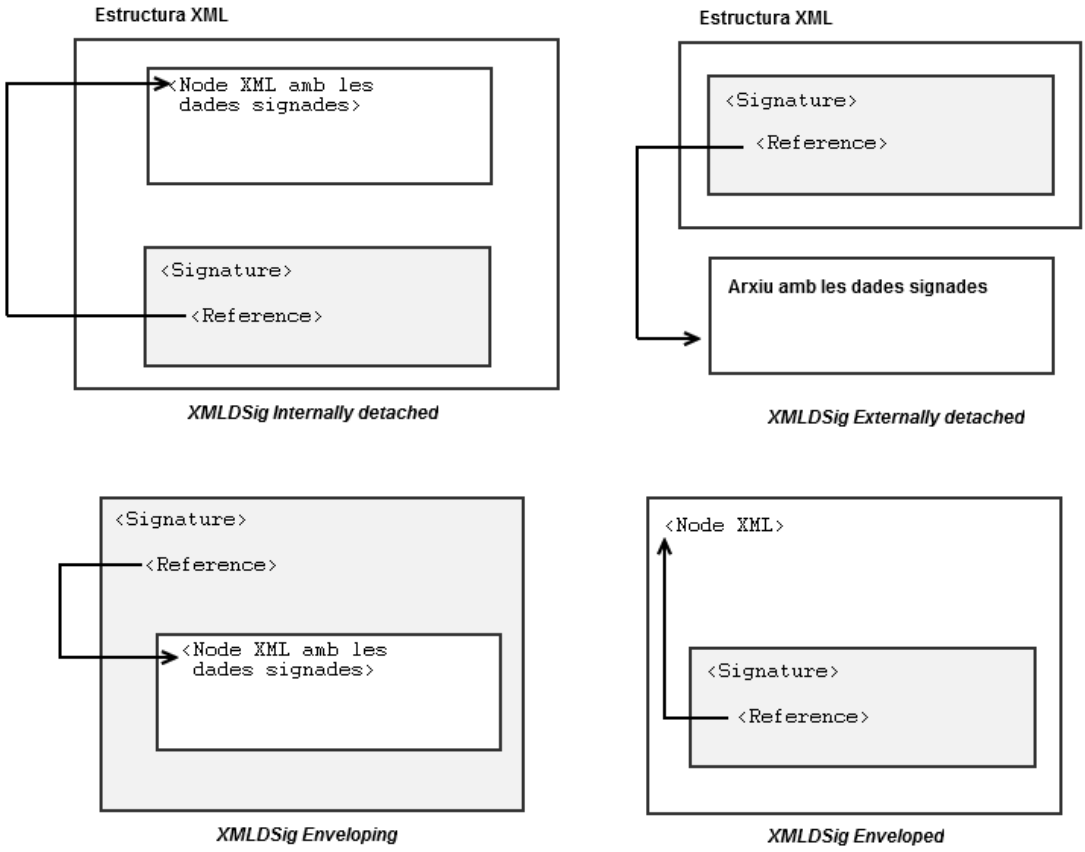

Figura 4 - Esquema modes signatura XMLDSig.

– S/MIME (*Secure/Multipurpose Internet Mail Extensions*): És un estàndard de la IETF utilitzat per criptografia de clau pública i signat de correu electrònic encapsulat en MIME. Ofereix autenticació, integritat del missatge i no repudi. Conté un objecte CMS.

També existeixen formats avançats com:

– XAdES (*XML Advanced Electronic Signature*): És un conjunt d'extensions a les recomanacions XML-DSig, fent-les adequades per la signatura electrònica avançada. També especifica perfils precisos de XML-DSig per ser utilitzats com a signatura electrònica reconeguda segons la directiva 1999/93/EC de la Unió Europea.
Existeixen 7 tipus de perfils, segons el nivell de protecció ofert.

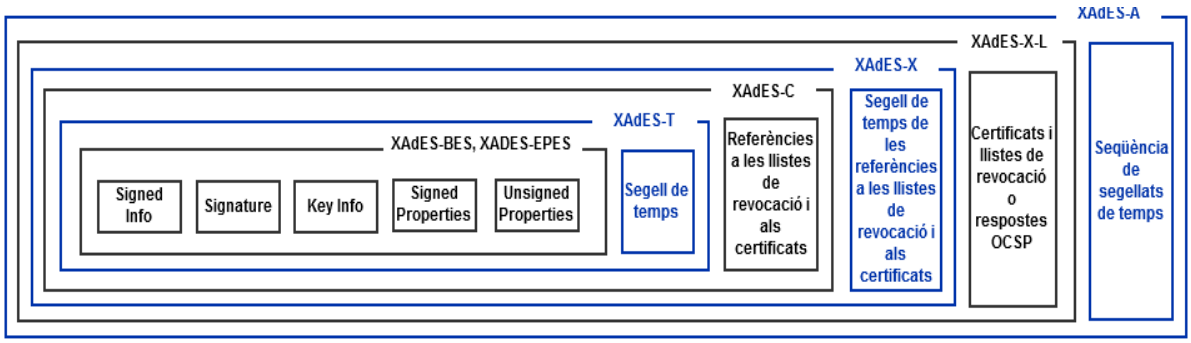

Figura 5 - Perfils XAdES.

Cadascun inclou i amplia l'anterior:

– XAdES-BES (*XAdES Basic Electronic Signature*): Forma bàsica que únicament compleix els requisits legals de la directiva 1999/93/EC de la Unió Europea per a signatures electròniques avançades. Per tal que una signatura avançada es consideri com reconeguda, s'ha de realitzar mitjançant un dispositiu segur de creació de signatures que compleixi la normativa EN-14890:1-2009.

– XAdES-EPES (*XAdES Explicit Policy based Electronic Signature*): Afegeix informació de la política utilitzada per la creació i validació de la signatura.

– XAdES-T (*XAdES with Time-stamp*): Afegeix un camp de segellat de temps (signatura amb la marca de temps de quan es va realitzar).

– XAdES-C (*XAdES Complete validation data*): Afegeix referències a les dades de verificació (respostes OCSP i CRL) dels documents signats per permetre una futura verificació i validació *off-line* (signatura validada). Les dades de verificació no estan incloses a la signatura , sinó que es troben emmagatzemades en un altre lloc.

- XAdES-X (*XAdES eXtended validation data*): S'utilitza quan és necessari implantar una mesura de seguretat davant la possibilitat de que la CA (*Certification Authority*) de la cadena de certificació es vegi compromesa en el futur. Afegeix segells de temps a les dades (la signatura electrònica, el segell de temps de la signatura i les referències introduïdes per XAdES-C) necessàries per garantir que la signatura sigui vàlida (signatura validada).

- XAdES-X-L (*XAdES eXtended Long-term validation data*): S'utilitza quan la cadena de certificació i les dades de validació no es guarden en un lloc segur en el temps. Afegeix la cadena de certificació i la informació de validació de la signatura (resposta OCSP o CRL), això permet en un futur la verificació de la signatura inclús si les fonts originals no estiguessin disponibles (signatura longeva).

- XAdES-A (*XAdES Archiving validation data*): S'utilitza per garantir la validesa de la signatura al llarg del temps, ja que en un futur els algorismes criptogràfics empleats poden ser compromesos. Aplica segells de temps periòdics a tots els elements que en un període llarg de temps poden ser compromesos (signatura longeva).

CAPÍTOL 4. DISSENY.

4.1. Arquitectura de la plataforma

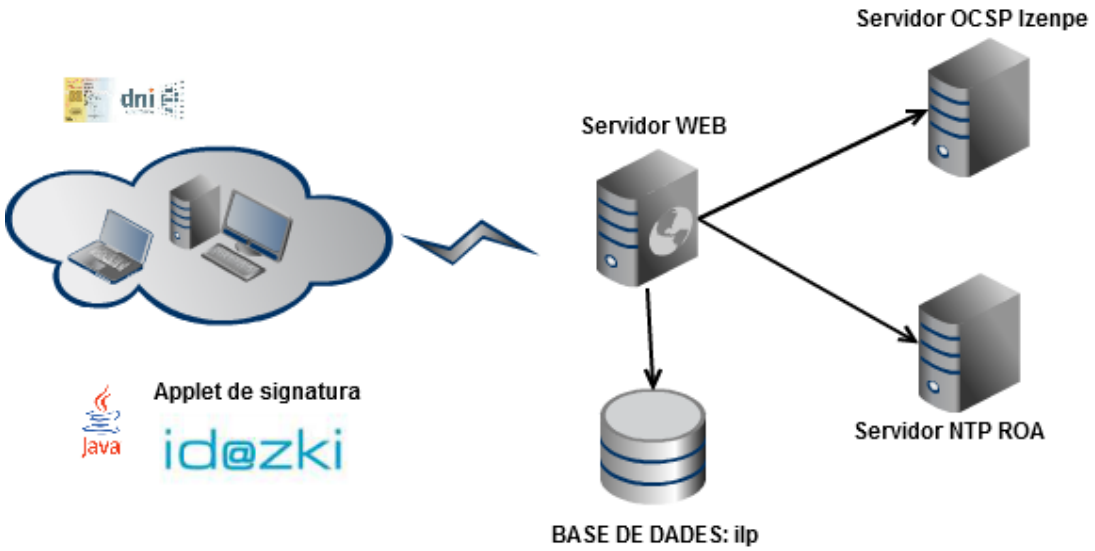

Figura 6 - Arquitectura del sistema.

L'arquitectura de la plataforma segueix l'estructura clàssica client-servidor, on el client és l'equip que gestiona les peticions d'usuari i la recepció de les pàgines provinents del servidor, també utilitza com a interfície d'usuari un navegador web .Es tracta d'un client pesat ja que part de la lògica de la plataforma es realitza en el client: applet de signatura.
Per acabar, el servidor és qui proporciona els recursos sol·licitats pel client, en el cas de la plataforma com a servidor considerem la base de dades i el servidor web, tots dos ubicats en el mateix servidor físic.

4.1.1. Servidor web

Com a servidor web, s'ha seleccionat ***Apache*** en la seva versió 2.2.14 es tracta d'un servidor web HTTP de codi obert que funciona en diverses plataformes:, com per exemple, Unix (BSD, GNU/Linux, etc...), Microsoft Windows i Macintosh. El servidor Apache es desenvolupa dins del projecte HTTP Server de la ASF (*Apache Software Foundation*) i és el servidor web més utilitzat avui en dia. És software lliure i es publica sota la llicencia *Apache License*.

4.1.2. Llenguatges de programació

Com a llenguatge de programació en el costat del servidor s'ha escollit ***PHP*** *(Hypertext Pre-processor*, inicialment *PHP Tools*, o, *Personal Home Page Tools*) en la versió 5.3.2. És un llenguatge d'alt nivell dissenyat principalment per la creació de pàgines web dinàmiques, està publicat sota la llicencia *PHP License* PHP i és software lliure. Pot ser desplegat sense cap cost a la majoria de servidors web i en la gran majoria de sistemes operatius, al mateix temps permet la connexió a diferents tipus de servidors de base de dades com poden ser, MySQL, PostgreSQL, Oracle, ODBC, DB2, Microsoft SQL Server, Firebird i SQLite. Es presenta com una alternativa lliure a tecnologies com Microsoft ASP i ASP.NET, ColdFusion de l'empresa Adobe, JSP/Java i CGI/Perl.

Com a llenguatge de programació en el costat del client s'ha triat **JavaScript**. És un llenguatge interpretat i orientat a objectes amb una sintaxi similar a Java, que ens permet interactuar amb les pàgines web fent ús del DOM (*Document Object Model*) .
El client mitjançant el navegador web descarrega el codi d'una pàgina web i si es troba amb codi JavaScript, l'interpreta i acaba executant-lo al client. Això ens permet crear webs dinàmiques, efectes visuals, etc... utilitzant pocs recursos ja que per norma s'executa en el client. Actualment tots els navegadors interpreten el codi JavaScript integrat a les pàgines web.

4.1.3. Applet

Un applet és el component d'una aplicació que s'executa d'una forma restringida en el context d'un altre programa com per exemple un navegador web.

En el cas de la plataforma s'ha provat amb diferents applets de signatura digital:

- @firma del CTT ("*Centro de Transferencia de Tecnología*"): És un *applet* de Java que es pot integrar a qualsevol web mitjançant JavaScript i té una amplia compatibilitat amb diferents sistemes operatius (Windows 2000, XP, Vista, 7, Server 2003, Server2008, Linux, Sun Solaris / OpenSolaris 10), i amb diferents navegadors (Firefox 2.0.20 o superior, Internet Explorer 6.0 o superior, Chrome 3.0 o superior, Apple Safari 5 o superior). Com a únic requisit ha de tenir JRE 1.5 update22 o superior instal·lat en el navegador. Utilitza estàndards avançats de signatura com són XAdES (màxim nivell BES), CAdES, PDF, ODF i OOXML.

- CryptoApplet: És un *applet* de Java creat per la Universitat Jaume I, és compatible amb diferents sistemes operatius (Windows, Mac OS i GNU/Linux) i amb diferents navegadors (Firefox, Internet Explorer, Chrome , Apple Safari). Com a únic requisit ha de tenir JRE 1.5 update22 o superior instal·lat en el navegador. Utilitza estàndards de signatura com són Factura-e, XAdES, XAdES-T, XAdES-X-L (Digidoc), PDF, XMLDsig, CMS/PCKS#7, ..

- Id@zki: És un *applet* de Java desenvolupat per l'autoritat de certificació IZENPE, és compatible amb diferents sistemes operatius (Windows, Mac OS i GNU/Linux) i amb diferents navegadors (Firefox, Internet Explorer, Chrome , Apple Safari, Opera). Com a únic requisit ha de tenir JRE 1.6 o superior instal·lat en el navegador i utilitza estàndards avançats de firma com són XAdES (màxim nivell XL), CAdES (màxim nivell XL), CMS/PCKS#7 i PDF.

Finalment he escollit **Id@zki,** per que després de realitzar múltiples proves és el que ha tingut un comportament més estable, a més suporta una gran varietat de formats avançats de signatura i és fàcilment configurable. El principal problema que té és la manca de documentació en comparació amb @firma, que en disposa de molta, i en menys mesura CryptoApplet. Amb aquets dos últims applets he tingut problemes amb els navegadors Firefox 12 i IE9 conjuntament amb la versió de Java 1.7.

4.2. Base de Dades.

Com a base de dades, s'ha seleccionat *MySQL Community Server* versió 5.1.61, es tracta d'un sistema de gestió de dades (*SGBD*) relacional SQL de codi obert (llicència GPL), desenvolupat en C i C++ per la companyia *MySQL AB*, actualment propietat de l'empresa *Oracle*.
És un SGBD bastant popular en aplicacions web,utilitzat conjuntament amb Apache i PHP.

4.2.1. Diagrama relacional de la Base de Dades

Amb el diagrama relacional de la base de dades es pot determinar tota la informació que emmagatzema la plataforma, així com les seves relacions.

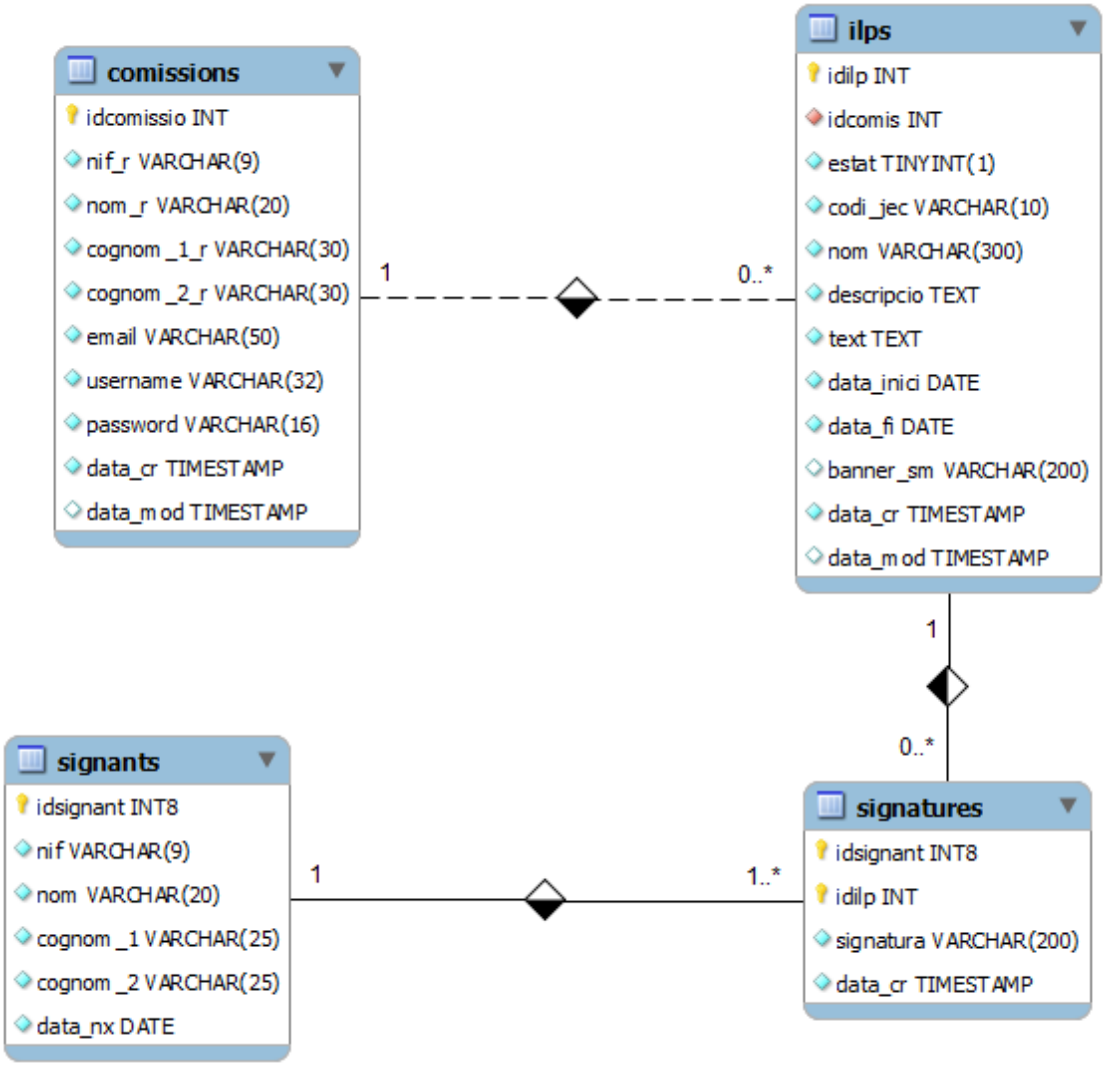

Figura 7 - Diagrama relacional de la base de dades.

4.2.2. Descripció de les taules

Taula signants

Aquesta taula emmagatzema les dades personals dels signants recollides a la doctrina de la "Junta Electoral Central" del 10 de maig de 2012.

Està formada pels següents camps :

- idsignant : Camp d'identificació del signant. Es tracta d'un camp auto incremental i obligatori (no nul). Clau primària.
- nif: NIF del signant. Camp obligatori (no nul).
- nom: Nom del signant. Camp obligatori (no nul).
- cognom_1: Primer cognom del signant. Camp obligatori (no nul).
- cognom_2: Segon cognom del signant. Camp obligatori (no nul).
- data_nx: Data de naixement del signant. Camp obligatori (no nul).

Taula comissions

Aquesta taula emmagatzema les dades de la comissió promotora, així com les dades personals del seu representant legal. També contindrà l'usuari i contrasenya per accedir a la part privada de la web on es gestionen les ILP's.
Està formada pel següents camps :

- idcomissio: Camp d'identificació d'una comissió. Es tracta d'un camp auto incremental i obligatori (no nul). Clau primària.
- nom_r: Nom del representant legal d'una comissió. Camp obligatori (no nul).
- cognom_1_r: Primer cognom del representant legal d'una comissió. Camp obligatori (no nul).
- cognom_2_r: Segon cognom del representant legal d'una comissió. Camp obligatori (no nul).
- nif_r: NIF del representant legal d'una comissió. Camp obligatori (no nul).
- username: Nom d'usuari per accedir a la gestió de les ILP's. Camp obligatori (no nul).
- password: Contrasenya de l'usuari per accedir a la gestió de les ILP's. Camp obligatori (no nul).
- email: Email de contacte d'una comissió.
- data_cr: Data de creació d'una comissió. Timestamp. Camp obligatori (no nul).
- data_mod: Data de modificació de les dades d'una comissió. Timestamp. Camp obligatori (no nul).

Taula ilps

Aquesta taula emmagatzema les dades bàsiques d'una ILP,així com imatges i dades per omplir una pàgina web personalitzada.
Està formada pel següents camps :

- idilp: Camp d'identificació d'una ILP. Es tracta d'un camp auto incremental i obligatori (no nul). Clau primària.
- idcomis: Camp d'identificació d'una comissió. Es tracta d'un camp obligatori (no nul). Clau forana (fk_comissio) que fa referència a idcomissio de la taula comissions.
- estat: Camp que ens dóna l'estat d'una ILP (0-Inactiva / 1-Activa) .Es tracta d'un camp obligatori (no nul).
- codi_jec: Codi únic que assigna la JEC a una ILP. Es tracta d'un camp obligatori (no nul).
- nom: Nom de la ILP. Camp obligatori (no nul).

- descripcio: Descripció de la ILP. Camp obligatori (no nul).
- text: Text íntegre de la ILP. Camp obligatori (no nul).
- data_inici: Data d'inici de la ILP. Camp obligatori (no nul).
- data_fi: Data de finalització de la ILP. Camp obligatori (no nul).
- banner_sm: Ubicació de la imatge que s'utilitza per omplir diferents parts de la web.
- data_cr: Data de creació d'una ILP. Timestamp. Camp obligatori (no nul).
- data_mod: Data de modificació d'una ILP. Timestamp. Camp obligatori (no nul).
-

Taula signatures

Aquesta taula emmagatzema les signatures.

Està formada pel següents camps :

- idsignant: Camp d'identificació d'un signant. Es tracta d'un camp obligatori (no nul). Clau primària. Clau forana (fk_signant) que fa referència a idsignant de la taula signants.
- idilp: Camp d'identificació d'una ILP. Es tracta d'un camp obligatori (no nul). Clau forana (fk_ilp) que fa referència a idilp de la taula ilps.
- data_cr: Data de creació d'una signatura .Timestamp. Camp obligatori (no nul).
- signatura: Ubicació de l'arxiu XML signat. Camp obligatori (no nul).

4.3. Casos d'ús

4.3.1. Diagrama dels casos d'ús

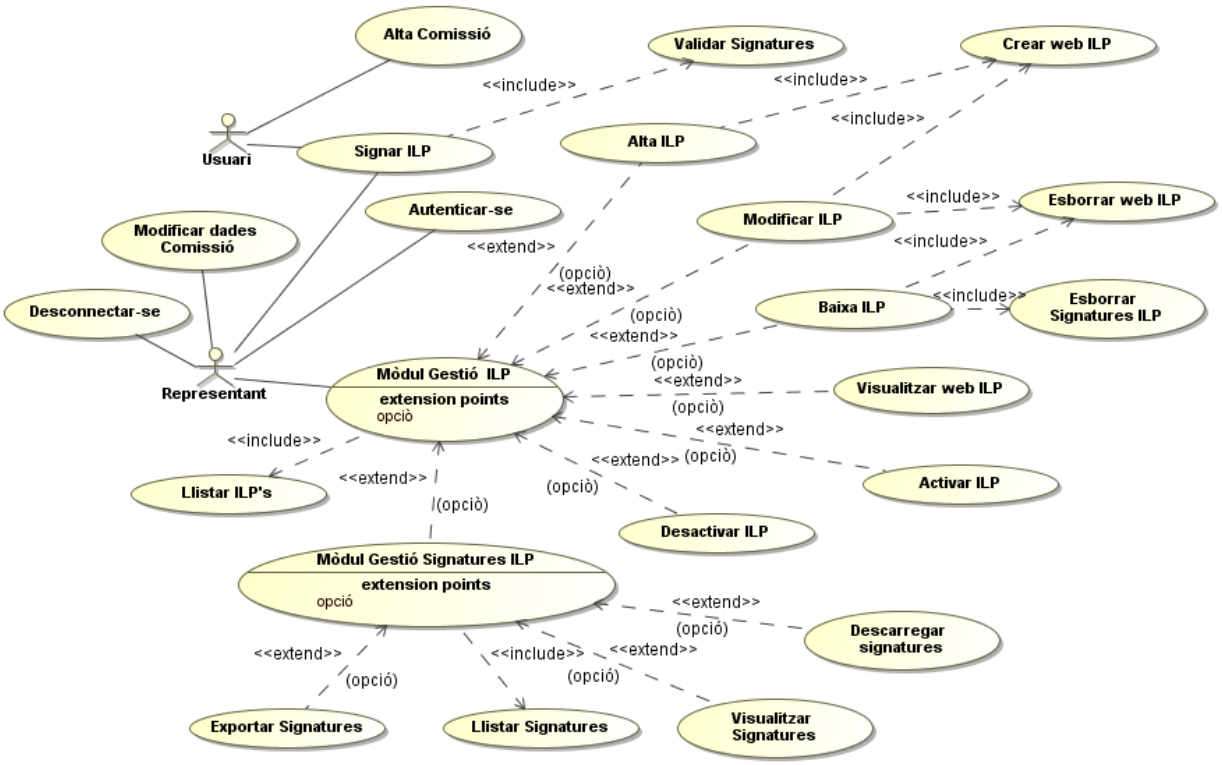

Figura 8 - Diagrama dels casos d'ús.

4.3.2. Descripció dels casos d'ús

- Cas d'ús número 1: "Autenticar-se"
  - Resum de la funcionalitat: permet l'accés del representant d'una comissió al mòdul de gestió de la plataforma.
  - Actors: **Representant**.
  - Casos d'ús relacionats: cap.
  - Precondició: hi ha una petició d'accés al mòdul de gestió de la plataforma i el **representant** no està dins.
  - Postcondició: el **representant** pot accedir al mòdul de gestió de la plataforma .
  - Procés normal principal:
    1. El sistema recull l'usuari i la contrasenya.
    2. El sistema valida que les dades siguin correctes i sigui un usuari vàlid.
    3. El sistema genera una sessió per al **representant**.
    4. El sistema dóna accés al **representant** al mòdul de gestió de la plataforma.

  - Alternatives de procés i excepcions:

    2a. No és un usuari vàlid o les dades són incorrectes.

    2a1. El sistema retorna un missatge d'error.

- Cas d'ús número 2: "Mòdul Gestió ILP"
  - Resum de la funcionalitat: mòdul que ens dóna accés a totes les opcions de gestió de la plataforma.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Alta ILP, Baixa ILP, Modificar ILP, Activar ILP, Desactivar ILP, Llistar ILP's, Mòdul Gestió Signatures ILP, Visualitzar web ILP.
  - Precondició: estar autenticat al sistema.
  - Postcondició: el **representant** pot seleccionar qualsevol opció del gestor.
  - Procés normal principal:
    1. El sistema executa el cas d'ús: Llistar ILP's.
    2. El sistema mostra totes les possibles opcions:
       -Donar d'alta una ILP.
       -Esborrar una ILP.
       -Modificar dades d'una ILP.
       -Activar una ILP.
       -Desactivar una ILP.
       -Visualitzar la web d'una ILP.
       -Accedir al mòdul de gestió de les signatures.

- Cas d'ús número 3: "LListar ILP's"
  - Resum de la funcionalitat: llista les ILP's que tenen actives o inactives una comissió.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió ILP.
  - Precondició: cap.
  - Postcondició: es mostra un llistat d' ILP's.
  - Procés normal principal:
    1. El sistema recupera informació de les ILP's d'una comissió.
    2. El sistema retorna un llistat amb les dades d'una ILP.

- Cas d'ús número 4: "Alta ILP"
  - Resum de la funcionalitat: permet crear una nova ILP per part del **representant** d'una comissió.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió ILP, Crear web ILP.
  - Precondició: el **representant** ha seleccionat l'opció de donar d'alta una ILP.
  - Postcondició: el **representant** torna al menú del mòdul de gestió.
  - Procés normal principal:
    1. L'usuari (**representant**) introdueix les dades necessàries per donar d'alta una ILP.
    2. El sistema valida que les dades siguin correctes.
    3. El sistema emmagatzema com activa la nova ILP en la base de dades.
    4. El sistema executa el cas d'ús: Crear web ILP.

  - Alternatives de procés i excepcions:
    2a. Les dades són incorrectes.
    2a1. El sistema retorna un missatge d'error.

- Cas d'ús número 5: "Crear web ILP"
  - Resum de la funcionalitat: crea una nova pàgina web personalitzada amb les dades de la ILP. Depenent de l'estat de la ILP i de la data d'inici de recollida de signatures, l'opció de signar es trobarà oculta.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Alta ILP, Modificar ILP.
  - Precondició: s'han emmagatzemat les dades de una ILP en la base de dades .
  - Postcondició: cap.
  - Procés normal principal:
    1. El sistema genera una nova pàgina web amb les dades de la ILP.

- Cas d'ús número 6: "Modificar ILP"
  - Resum de la funcionalitat: permet modificar dades d'una ILP per part del **representant** d'una comissió. Si ja ha començat el procés de recollida de signatures únicament es pot modificar la imatge.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió ILP, Esborrar web ILP,Crear web ILP.
  - Precondició: el **representant** ha seleccionat l'opció de modificar una ILP.
  - Postcondició: el **representant** torna al menú del mòdul de gestió.
  - Procés normal principal:
    1. L'usuari (**representant**) selecciona una ILP per modificar les dades.
    2. El sistema mostra les dades susceptibles de ser modificades de la ILP seleccionada.
    3. L'usuari (**representant**) modifica les dades.
    4. EL sistema valida que les dades siguin correctes.
    5. El sistema actualitza les noves dades a la base de dades.
    6. El sistema executa el cas d'ús: Esborrar web ILP.
    7. El sistema executa el cas d'ús: Crear web ILP.

  - Alternatives de procés i excepcions:
    4a. Les dades són incorrectes.
    4a1. El sistema retorna un missatge d'error.

- Cas d'ús número 7: "Esborrar web ILP"
  - Resum de la funcionalitat: esborra la pàgina web personalitzada d'una ILP.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Baixa ILP, Modificar ILP.
  - Precondició: El sistema ha actualitzat o esborrat les dades la ILP seleccionada.
  - Postcondició: cap.
  - Procés normal principal:
    1. El sistema esborra la pàgina web personalitzada de la ILP seleccionada.

- Cas d'ús número 8: "Baixa ILP"
  - Resum de la funcionalitat: permet donar de baixa una ILP per part del **representant** d'una comissió.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió ILP, Esborrar web ILP, Esborrar Signatures ILP.
  - Precondició: el **representant** ha seleccionat l'opció d'esborrar una ILP.
  - Postcondició: el **representant** torna al menú del mòdul de gestió.
  - Procés normal principal:
    1. L'usuari (**representant**) selecciona una ILP per donar de baixa.
    2. El sistema esborra la ILP en la base de dades.
    3. El sistema executa el cas d'ús: Esborrar Signatures ILP.

- Cas d'ús número 9: "Esborrar Signatures ILP"
  - Resum de la funcionalitat: Elimina totes les signatures d'una ILP.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Baixa ILP.
  - Precondició: El sistema ha esborrat les dades i la web de la ILP seleccionada.
  - Postcondició: cap.
  - Procés normal principal:
    1. El sistema esborra totes les signatures de la ILP seleccionada.

- Cas d'ús número 10: "Visualitzar web ILP"
  - Resum de la funcionalitat: s'obre una nova finestra amb la pàgina web personalitzada d'una ILP.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió ILP.
  - Precondició: el **representant** ha seleccionat l'opció de visualitzar la pàgina web personalitzada d'una ILP.
  - Postcondició: cap.
  - Procés normal principal:
    1. El sistema obre una nova finestra amb la pàgina web personalitzada de la ILP seleccionada.

- Cas d'ús número 11: "Activar ILP"
  - Resum de la funcionalitat: permet activar una ILP per part del **representant** d'una comissió.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió ILP.
  - Precondició: el **representant** ha seleccionat l'opció d'activar una ILP.
  - Postcondició: el **representant** torna al menú del mòdul de gestió.
  - Procés normal principal:
    1. El sistema activa la ILP seleccionada.

- Cas d'ús número 12: "Desactivar ILP"
  - Resum de la funcionalitat: permet desactivar una ILP per part del **representant** d'una comissió.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió ILP.
  - Precondició: el **representant** ha seleccionat l'opció de desactivar una ILP.
  - Postcondició: el **representant** torna al menú del mòdul de gestió.
  - Procés normal principal:
    1. El sistema desactiva la ILP seleccionada.

- Cas d'ús número 13: "Mòdul Gestió Signatures ILP"
  - Resum de la funcionalitat: permet consultar estadístiques d'una ILP per part del **representant** d'una comissió.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió ILP, Llistar Signatures, Visualitzar Signatures, Descarregar Signatures, Exportar Signatures.
  - Precondició: el **representant** ha seleccionat l'opció de gestionar les signatures d'una ILP.
  - Postcondició: cap.
  - Procés normal principal:
    1. L'usuari (**representant**) selecciona una ILP per gestionar les signatures .
    2. S'executa el cas d'ús: Llistar Signatures.
    3. El sistema mostra les opcions que podem realitzar amb la llista de signatures:
       - Exportar llistat signatures.
       - Visualitzar signatures.
       - Descarregar signatures.

- Cas d'ús número 14: "Llistar Signatures"
  - Resum de la funcionalitat: llista les signatures que s'han recollit per la ILP seleccionada.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió Signatures ILP.
  - Precondició: cap.
  - Postcondició: es mostra un llistat de signatures.
  - Procés normal principal:
    1. El sistema recupera informació de les signatures d'una ILP.
    2. El sistema retorna un llistat amb les dades de les signatures.

- Cas d'ús número 15: "Visualitzar Signatures"
  - Resum de la funcionalitat: visualitza les dades de la signatura seleccionada i també es pot descarregar..
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió Signatures ILP.
  - Precondició: el **representant** ha seleccionat una signatura .
  - Postcondició: s'exporta un llistat de signatures.
  - Procés normal principal:
    1. El sistema recupera informació de la signatures seleccionada.
    2. El sistema mostra les dades de la signatura.
  - Alternatives de procés i excepcions:
    2a. El sistema ofereix la possibilitat de descarregar la signatura.

- Cas d'ús número 16: "Descarregar Signatures"
  - Resum de la funcionalitat: descarrega un fitxer comprimit (zip) amb totes les signatures que s'han recollit per la ILP.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió Signatures ILP.
  - Precondició: el **representant** ha seleccionat l'opció de descarregar signatures.
  - Postcondició: es descarrega l'arxiu amb les signatures.
  - Procés normal principal:
    1. El sistema comprimeix totes les signatures d'una ILP en un únic arxiu.
    2. EL sistema descarrega el fitxer amb les signatures.

- Cas d'ús número 17: "Exportar Signatures"
  - Resum de la funcionalitat: exporta a un fitxer d'Excel (xls) una llista amb les signatures que s'han recollit per la ILP seleccionada.
  - Actors: **Representant**.
  - Casos d'ús relacionats: Mòdul Gestió Signatures ILP.
  - Precondició: cap.
  - Postcondició: s'exporta un llistat de signatures.
  - Procés normal principal:
    1. El sistema recupera informació de les signatures d'una ILP.
    2. El sistema exporta un llistat amb les dades de les signatures.

- Cas d'ús número 18: "Alta Comissió"
  - Resum de la funcionalitat: permet donar d'alta una comissió i a un representant legal d'aquesta.
  - Actors: **Usuari**.
  - Casos d'ús relacionats: cap.
  - Precondició: L' **usuari** ha seleccionat l'opció de donar d'alta una comissió.
  - Postcondició: L' **usuari** es transforma en **representant** i accedeix al mòdul de gestió de la plataforma.
  - Procés normal principal:
    1. L'**usuari** introdueix les dades requerides.
    2. EL sistema valida que les dades siguin correctes.
    3. El sistema emmagatzema les dades de la comissió i el seu representant.
    4. L'**usuari** adquireix el rol de **representant**.
    5. El **representant** accedeix al mòdul de gestió de la plataforma.
  - Alternatives de procés i excepcions:
    2a. Les dades són incorrectes.
    2a1. El sistema retorna un missatge d'error.

- Cas d'ús número 19: "Modificar dades Comissió"
  - Resum de la funcionalitat: permet modificar les dades d'una comissió i del representant legal d'aquesta.
  - Actors: **Representant**.
  - Casos d'ús relacionats: cap.
  - Precondició: El **representant** s'ha autenticat.
  - Postcondició: cap.
  - Procés normal principal:
    1 L'**usuari** introdueix les noves dades.
    2 EL sistema valida que les dades siguin correctes.
    3 El sistema emmagatzema les noves dades de la comissió i el seu representant.
  - Alternatives de procés i excepcions:
    2a. Les dades són incorrectes.
    2a1. El sistema retorna un missatge d'error.

- Cas d'ús número 20: "Signar ILP"
  - Resum de la funcionalitat: permet signar una ILP.
  - Actors: **Representant,Usuari**.
  - Casos d'ús relacionats: Validar Signatures.
  - Precondició: L' **usuari** ha seleccionat l'opció de signar una ILP.
  - Postcondició: es genera un arxiu xml amb la ILP signada per l'usuari.
  - Procés normal principal:
    1. L'**usuari** o **representant** selecciona una ILP per signar.
    2. L'**usuari** o **representant** introdueix les dades requerides.
    3. EL sistema valida que les dades siguin correctes.
    4. El sistema genera un XML amb les dades del signant.
    5. Es crida l'applet de signatura.
    6. L'**usuari** o **representant** escull un certificat .
    7. El sistema genera l'arxiu XML signat.
    8. El sistema executa el cas d'ús: Validar Signatures.
    9. El sistema emmagatzema les dades del signant i la signatura a la base de dades.
  - Alternatives de procés i excepcions:
    3a. Les dades són incorrectes.
    3a1. El sistema retorna un missatge d'error.
    6a. El certificat no és vàlid (caducat, revocat) o s'ha produït un error a l'applet de signatura.
    6a1. El sistema retorna un missatge d'error
    8a. El cas d'ús Validar Signatures, retorna un error.
    8a1. El sistema retorna un missatge d'error

- Cas d'ús número 21: "Validar Signatures"
  - Resum de la funcionalitat: valida les signatura generada pel sistema en el cas d'ús Signar ILP.
  - Actors: **Representant, Usuari**.
  - Casos d'ús relacionats: Signar ILP.
  - Precondició: s'ha generat una arxiu XML signat.
  - Postcondició: valida l'arxiu XML signat.
  - Procés normal principal:
    1. El sistema extreu les dades del certificat que s'ha utilitzat per signar ILP.
    2. El sistema comprova que el DNI del certificat sigui el mateix que el introduït en el formulari del cas d'ús: Signar ILP.
    3. El sistema comprova les dates del certificat per comprovar que estigui vigent.
    4. El sistema extreu de l'arxiu signat la resposta OCSP, codificada en ASN.1, del certificat utilitzat per signar;la descodifica i comprova que el certificat sigui vàlid.
    5. El sistema retorna el resultat de la validació de la signatura.

- Cas d'ús número 22: "Desconnectar-se"
  - Resum de la funcionalitat: permet la desconnexió del representant d'una comissió de les parts privades de la plataforma.
  - Actors: **Representant**.
  - Casos d'ús relacionats: cap.
  - Precondició: hi ha una petició de desconnexió en qualsevol lloc de la part privada de la plataforma (gestió de ILPs i gestió de signatures).
  - Postcondició: el **representant** torna a la pàgina principal de la plataforma, i es transforma en **usuari** .
  - Procés normal principal:
    1. El sistema elimina la sessió oberta.
    2. El sistema torna a la pàgina principal de la plataforma.

4.4. Diagrames de flux

Per analitzar amb més profunditat el procés de signat (cas d'ús nº20) i la validació de les signatures (cas d'ús nº21) he realitzat uns diagrames de flux , on es pot comprovar amb detall aquests processos.

4.4.1. Diagrama de flux del procés de signat

Aquest diagrama ens mostra el detall del procés de signat.

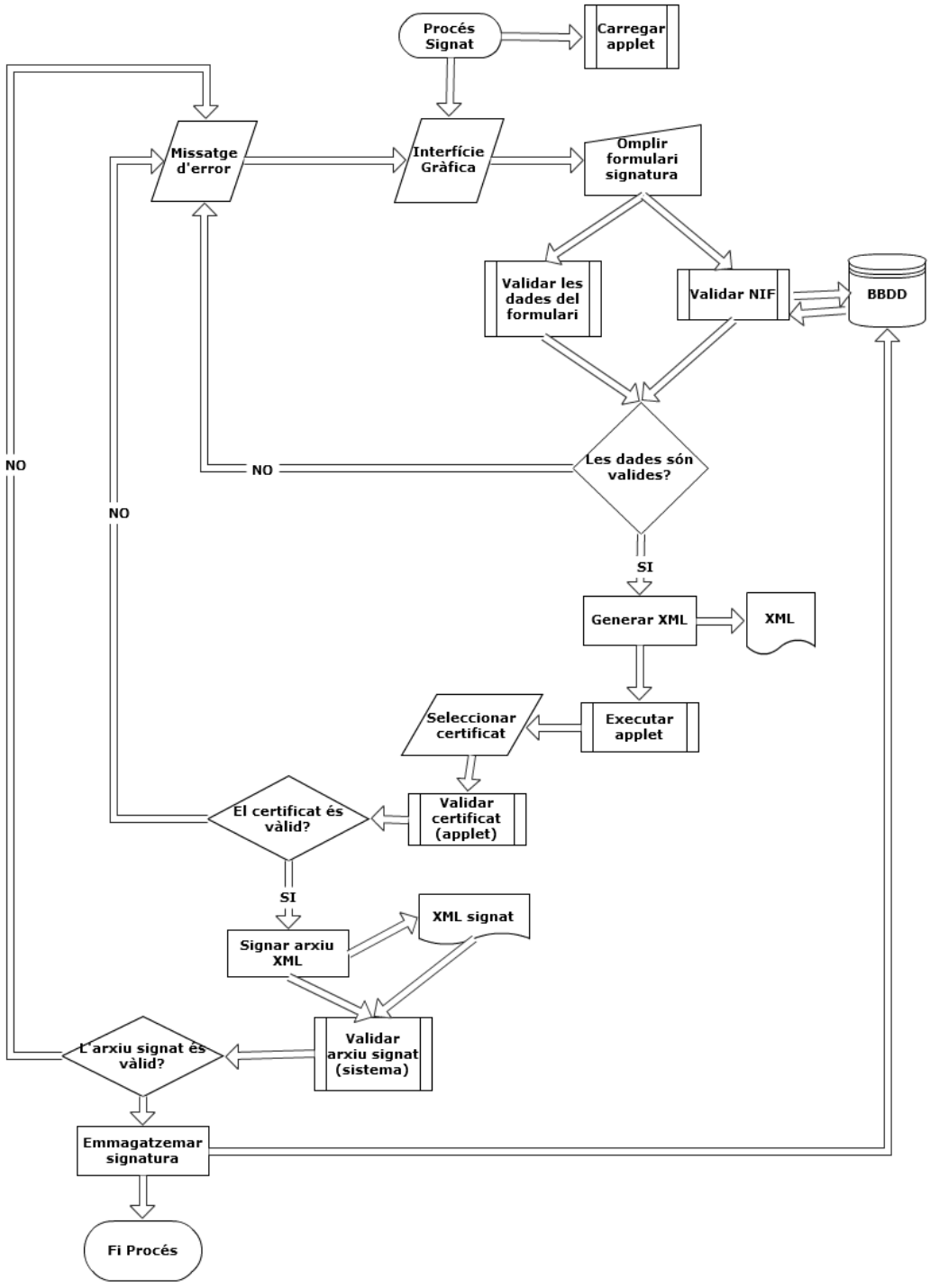

Figura 9 - Diagrama de flux del procés de signat.

L'applet únicament ens deixarà seleccionar els certificats recollits a l'annex A (Polítiques de signatura acceptades per la plataforma).

Una vegada seleccionat el certificat comença el procés de validació per part de l'applet, que a grans trets, segueix el següent procediment :

- Primer comprova l'estat del certificat mitjançant la resposta a una consulta OCSP. Si rep com resposta "*unknown*" o "*revoked*" el procés de validació finalitza amb un error.
- Si en canvi rep "good" el procés continua i es genera l'arxiu signat.

4.4.2. Diagrama de flux del procés de validació de les signatures

Aquest diagram ens descriu amb detall el procés de validació de les signatures.

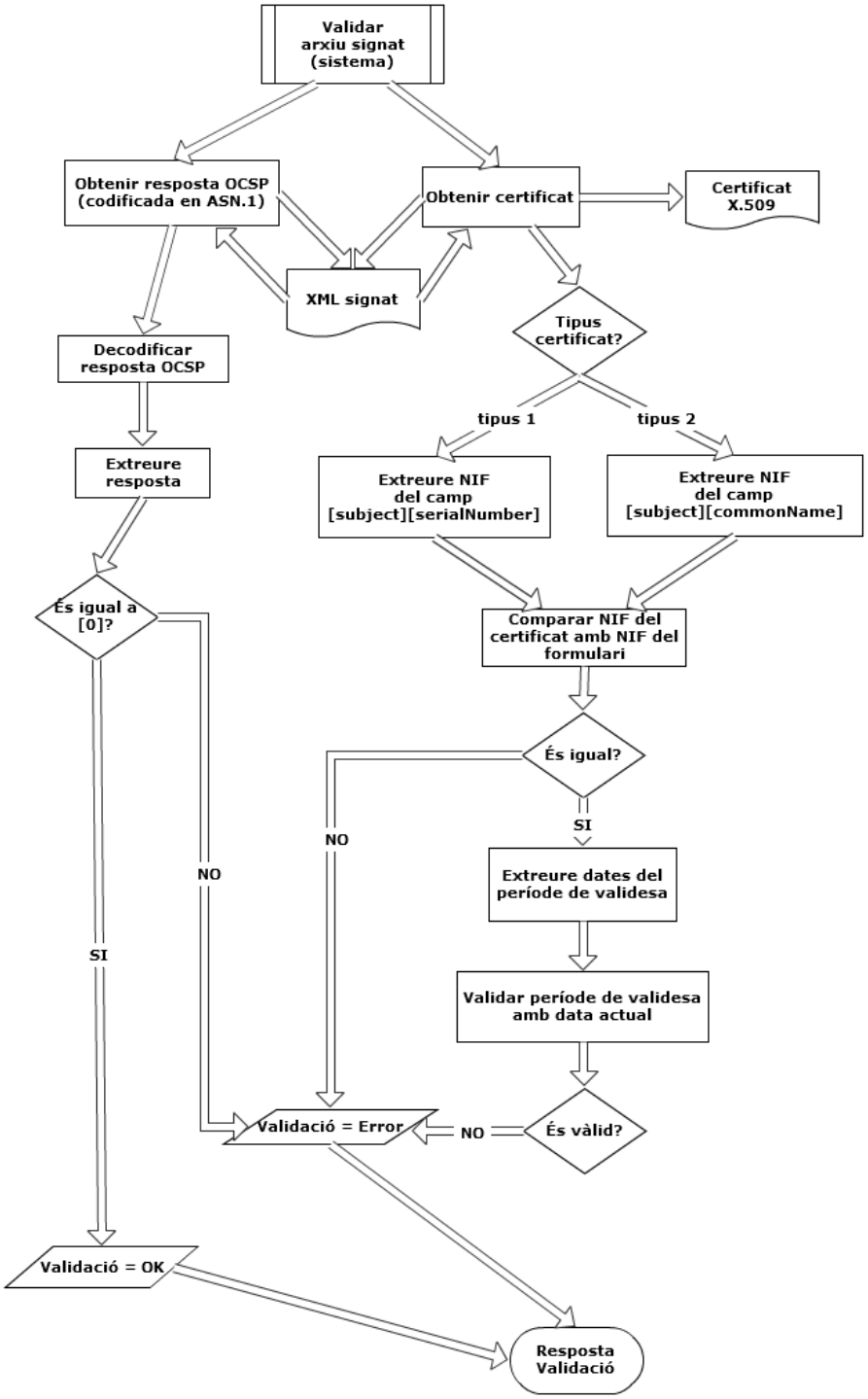

Figura 10 - Diagrama de flux del procés de validació de les signatures.

Llegint l'apartat anterior es pot deduir que el procés de validar l'arxiu signat aporta duplicitats amb la validació realitzada per l'applet a l'hora de comprovar l'estat del certificat ; però he considerat que afegeix una mica més de seguretat en el cas que l'applet no funcioni correctament, ja que la plataforma té com objectiu recollir el màxim de signatures vàlides.

S'ha omès la part de validar a cada signatura la seva estructura , considerant que es dóna per fet que l'applet sempre generarà la mateixa estructura i que primer s'ha validat una signatura segons la especificació ETSI TS 101 903 v1.3.2 (03-2006).

4.5. Disseny d'interfícies gràfiques

El disseny de les interfícies gràfiques (pàgines web) de la plataforma està orientat a facilitar el màxim possible a les comissions les gestions relacionades amb les seves ILPs, i fer que els ciutadans puguin signar les iniciatives de la manera més intuïtiva i senzilla possible.

La web consta bàsicament de 4 tipus de pàgines, la pàgina principal de la plataforma, gestió ILPs i signatures, formularis i la pàgina principal de les ILPs.

4.5.1. Pàgina principal

A la part superior (top) tenim els enllaços per accedir a la part privada de la web ("ACCÉS"), per registrar-se ("REGISTRA'T") i per tornar a la pàgina principal ("INICI").

A la part central ens trobem amb un *banner* que ens mostra de forma breu les funcionalitats bàsiques de la plataforma i enllaça amb l'opció "REGISTRA'T".

Una mica més avall hi ha les imatges amb el títol de la ILP de les iniciatives actives agrupades de tres en tres. Al posicionar el cursor sobre aquestes imatges apareix la descripció de la ILP, el nombre de signatures recollides, la data límit per signar les iniciatives i un botó per accedir a les webs personalitzades.

Si hi ha menys de 3 ILPs actives, a cada lloc lliure apareixerà una imatge fomentant el registre i que enllaça amb l'opció "REGISTRA'T". Si una ILP no té imatge emmagatzemada es mostra una estàndard.

Figura 11 – Pàgina principal de la plataforma

4.5.2. Formularis

Totes les pàgines amb formularis per introduir o modificar dades tenen la mateixa estructura, d'entrada tenim el nom del camp a omplir, el camp a omplir i en darrer lloc una llegenda explicativa del que s'ha d'introduir; una vegada comencem a escriure s'aniran fent validacions amb JavaScript i si existeix qualsevol error el text de la llegenda es substituït amb el text de l'error.

Quan s'envia el formulari es realitza una última validació JavaScript de totes les dades introduïdes, i després es realitza una validació mitjançant PHP per si tenim el JavaScript desactivat al navegador. En cas que es detecti un error en la validació PHP es mostra un missatge d'error en la part superior del formulari.

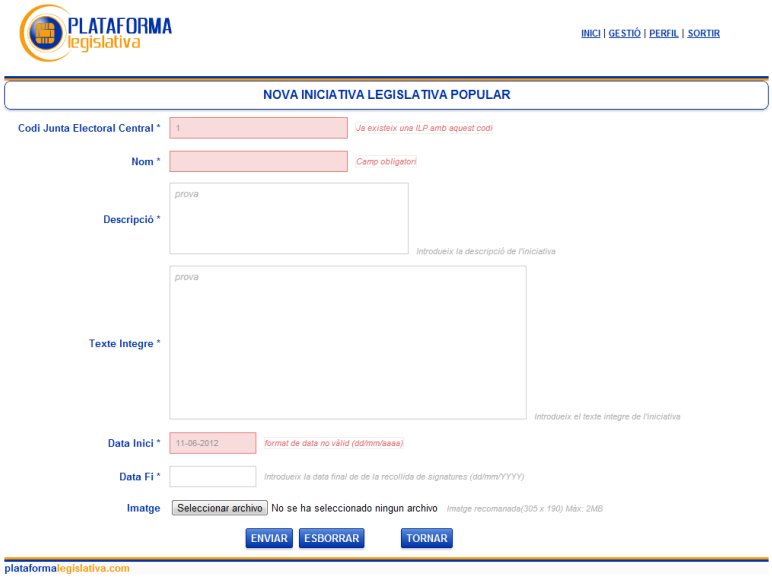

Figura 12 – Formulari

4.5.3. Pàgines de gestió (ILPs i signatures)

Per facilitar la gestió de les iniciatives i les signatures, a la part central d'aquestes pàgines es troba una taula amb les dades més representatives del que es vulgui gestionar (signatures,ILPs) i a sobre hi haurà els botons amb totes les accions que es poden realitzar amb aquets elements.

Figura 13 – Pàgina de gestió de la plataforma

4.5.4. Pàgina principal de les ILPs

La pàgina principal de les ILPs conté totes les dades que es recullen d'una ILP: imatge, nom, descripció i el text íntegre , també apareix el nombre total de signatures recollides, la data límit per signar les iniciatives i un botó per signar les iniciatives, aquest únicament apareix si la iniciativa està activa.

Figura 14 – Pàgina principal d'una ILP

4.6. Signatures

Una de les decisions més importants en l'etapa de disseny és trobar l'estructura XML òptima a fi que els ciutadans la signin, i estudiar quin format de signatura digital s'ha d'utilitzar per complir amb la legislació vigent.

4.6.1. Estructura XML

D'entrada vaig considerar una estructura que contingués totes les dades que s'extreuen de la legislació vigent i les que van ser requerides en anteriors ILPs , com per exemple la iniciativa "*Defendemos el trasvase Tajo-Segura*". Aquesta estructura consta per un costat de les dades personals del signant, com són el NIF, nom, primer cognom, segon cognom, data, província, municipi de naixement i les dades relatives al domicili censal (domicili, codi postal, província i municipi). Per l'altre costat tenim les dades pròpies de la ILP, com són el nom i el text íntegre , aquestes dades ens serveixen per comprovar la conformitat del signant amb la totalitat del proposat a la ILP.

Però al final m'he decidit a adaptar la nova normativa [JEC6/2012], perquè facilita el procés de signat per part dels ciutadans, de manera que per signar una ILP han d'omplir menys dades. Per adaptar l'estructura els canvis que he hagut de realitzar són mínims, únicament s'ha canviat el noms del elements XML, s'ha eliminat la província i municipi de naixement i les dades relatives al domicili censal. També s'ha substituït el text íntegre de la ILP pel concepte de codi de la ILP, aquest codi identifica de forma única una ILP i té un format fix ILPAAAANNN (on ILP és fix , AAAA és l'any en curs i NNN és el nombre assignat per la JEC).

Podem veure un exemple de les dos estructures:

- Estructura inicial

```
<?xml version="1.0" encoding="UTF-8"?>
<Dades id="sig">
    <DadesPersonals>
            <Nif>11111111H</Nif>
            <Nom>a</Nom>
            <PrimerCognom>1</PrimerCognom>
            <SegonCognom>1</SegonCognom>
            <DataNaixement>19/10/1977</DataNaixement>
            <ProvinciaNaixement>1</ProvinciaNaixement>
            <MunicipiNaixement>1</MunicipiNaixement>
            <Domicili>1</Domicili>
            <CodiPostal>08906</CodiPostal>
            <Provincia>1</Provincia>
            <Municipi>1</Municipi>
    </DadesPersonals>
```

```
    <DadesILP>
        <NomILP>Pr</NomILP>
        <TextILP>asdasdasdasdasdasdasdasd</TextILP>
    </DadesILP>
<ds:Signature>
……..
</ds:Signature>
</Dades>
```

– Estructura adaptada a la nova normativa

```
<?xml version="1.0" encoding="UTF-8"?>
<ilp id="sig">
    <firmante>
        <nomb>a</nomb>
        <ape1>1</ape1>
        <ape2>1</ape2>
        <fnac>19771019</fnac>
        <tipoid>1</tipoid>
        <id>11111111H</id>
    </firmante>
    <datosilp>
        <tituloilp>Pr</NomILP>
        <codigoilp> ILP2012001</codigoilp>
    </datosilp>
<ds:Signature>
……..
</ds:Signature>
</ilp>
```

4.6.2. Format de la signatura digital

En primer lloc, vaig optar per una signatura digital amb format XAdES-C per que complia tots els requisits per demostrar que una signatura és vàlida en un instant determinat de temps. Conté un segell de temps sobre la signatura que ens permet demostrar que les dades signades no s'han modificat des de la data especificada al segell (element `SignatureTimeStamp`). També afegeix referències a les dades de verificació (element `CompleteRevocationRefs`), en el cas de la plataforma utilitzem respostes OCSP, que no es troben en la signatura i ens permeten verificar que el certificat utilitzat per signar era vàlid en l'instant de la realització de la signatura.

No obstant això, vaig decidir utilitzar una signatura amb format XAdES-X-L atès que desconeixia el comportament de l'applet enfront els diferents estats dels certificats (revocats, suspesos,...), i amb aquest tipus de signatura puc tenir accés de forma directa a l'estat del certificat del signant mitjançant les respostes OCSP de la cadena de certificació, que es troben

dins de la signatura (element `RevocationValues`) i així poder fer les validacions necessàries.

Aquest format de signatura ens dóna molta seguretat davant la possibilitat que la CA de la cadena de verificació desaparegui o es vegi compromesa en un futur, tot i que són opcions força improbables. Realment no és molt eficient per que la plataforma fa validacions redundants a l'hora de comprovar la validesa dels certificats, però ens garanteix que la gran majoria de les signatures recollides siguin vàlides.

Una vegada finalitzat el TFC i després de múltiples proves he comprovat que l'applet únicament deixa signar si rep un a resposta OCSP positiva ([0]-*good*). Tot això, unit a la recomanació de la nova normativa [JEC6/2012] d'utilitzar una marca de temps conjuntament amb una signatura XAdES -BES *internally detached*, i a la poca diferència a nivell computacional entre XAdES –BES i XAdES-C (XAdES-X-L té un cost computacional més gran considerant que ha d'emmagatzemar la cadena de certificació i totes les respostes OCSP), em fa concloure que el format ideal per signar a la plataforma hauria de ser XAdES-C, sempre que realitzar segells de temps i realitzar peticions OCSP no tingui un cost econòmic.

4.6.3. Algorismes utilitzats

Dins de la signatura es fan ús de diferents algorismes:

- XML-C14N: És un algorisme de canonicalització que genera la forma canònica d'un arxiu XML o d'algun dels seus elements. La forma canònica és la representació física d'un arxiu o element XML després de les múltiples transformacions realitzades per l'algorisme de canonicalització [XMLC14N], i ens serveix per determinar si dos elements o arxius XML són idèntics tot i que tinguin diferent representació física .Es fa servir a la signatura per canonicalitzar les dades a signar abans de realitzar els càlculs de la signatura.

- SHA1 : És un algorisme de resum (*hash*) que s'utilitza per crear un resum teòricament únic d'un conjunt de dades. Dins de la signatura el fem servir a tots els llocs on es necessita un resum, per exemple als certificats. L'applet de signatura té l'opció de substituir-lo per SHA2, concretament SHA-256, avui dia és molt més segur.

- RSA amb SHA1: És un sistema criptogràfic de clau pública que utilitza com a funció resum SHA1. Ens indica quin és l'algorisme emprat per generar i validar la signatura . Tant aquest sistema com l'algorisme de canonicalització són utilitzats per la signatura i estan inclosos en l'element `SignedInfo` per evitar que puguin ésser modificats.

- Base64: És un algorisme bàsic de codificació que serveix per codificar en caràcters ASCII qualsevol tipus de dades (binaries,etc ...) .S'utilitza a tots els elements de la signatura on és necessari representar un conjunt de dades en text ASCII. Per exemple,

s'utilitza a l'element `SignatureValue` que conté el valor actual de la signatura codificada utilitzant Base64.

- DER (*Distinguished Encoding Rules*): És un dels formats de codificació que formen part de l'estàndard ASN.1, aquest ens dóna les normes per representar dades independentment del maquinari utilitzat i les seves formes de representació interna[DER]. Es fa servir a diferents parts de la signatura malgrat que no està definit en molts llocs, per exemple la majoria de dades PKI (*Public Key Infraestructure*) com ara, certificats X.509, respostes OCSP, segells de temps,etc... estan codificades seguint aquestes regles.

CAPÍTOL 5. JOC DE PROVES.

El joc de les proves té com objectiu recollir les principals proves a les quals ha estat sotmesa la plataforma.En aquestes proves s'intenta recollir la casuística més àmplia possible.
Per realitzar les proves s'ha utilitzat:

- Ordinador Intel ® Pentium ® 4 CPU 3.00 Ghz, amb 1GB de memòria RAM, 250 GB de disc dur i com a sistema operatiu: Windows 7 Ultimate 32 bits. Navegadors: Opera (versió 11.64), Firefox (versions 10,11,12 i 13), Chrome (versions 17,18 i 19), Internet Explorer (versions 8 i 9).

- Ordinador Intel ® Pentium ® 4 CPU 2.40 Ghz, amb 1GB de memòria RAM, 2 TB de disc dur i com a sistema operatiu: Linux Fedora 14. Navegadors: Firefox 11 i Chrome 18.

5.1. Proves del procés de signatura

Signar amb DNI electrònic

- Amb aquesta prova es vol comprovar la correcta implementació del DNI electrònic (DNI-e) i el procés de signat.
- Per realitzar-la, primer anem a la web personalitzada d'una ILP activa i seleccionem l'opció "SIGNAR" , omplim correctament les dades del formulari i premem el botó "SIGNAR". Després introduïm el PIN del DNI electrònic i seleccionem el certificat de signatura del DNI.
- Com a resultat observem que la signatura s'ha generat correctament.
  No existeixen diferències amb els resultats esperats.

Proves gràfiques:

Figura 15 - Seqüència de proves gràfiques de la signatura amb DNi-e.

Signar amb certificat revocat

- Amb aquesta prova es vol comprovar la correcta validació de l'estat d'un certificat per part de l'applet de signatura.
- Per realitzar-la, primer anem a la web personalitzada d'una ILP activa i seleccionem l'opció "SIGNAR" , omplim correctament les dades del formulari i premem el botó "SIGNAR". Després seleccionem un certificat revocat. Com a resultat observem que la signatura no es genera i l'applet ens torna un missatge d'error indicant-nos que el certificat està revocat.
  No existeixen diferències amb els resultats esperats.
- Per realitzar aquesta prova vaig revocar un certificat propi de la FNMT.

Proves gràfiques:

Figura 16 – Missatge d'error de l'applet de signatura

Signar amb un certificat on el DNI del certificat no es correspon amb el proporcionat

- Amb aquesta prova es vol comprovar el procés de signat quan el certificat utilitzat per signar no es correspon amb el introduït al formulari de signatura.
- Per realitzar-la, primer anem a la web personalitzada d'una ILP activa i seleccionem l'opció "SIGNAR" , omplim correctament les dades del formulari i premem el botó "SIGNAR". Després seleccionem un certificat on el DNI no es correspongui amb el introduït al formulari.
- Com a resultat observem que la signatura no es genera i la plataforma ens torna un missatge d'error indicant-nos que no hi ha coincidència entre els DNIs.
  No existeixen diferències amb els resultats esperats.

S'ha realitzat la mateixa prova amb un certificat del FNMT i amb el DNI-e, ja que cadascú té el camp DNI a llocs diferents (veure 4.4.2. Diagrames de flux de procés de validació de les signatures).

5.2. Proves de gestió de ILPs

Crear una nova ILP

- Amb aquesta prova es vol comprovar el procés de crear una nova ILP.
- Per realitzar-la, primer accedim a la gestió de ILPs i seleccionem l'opció "NOVA INICIATIVA" , omplim correctament les dades del formulari i premem el botó "ENVIAR".
- Com a resultat observem que a la base de dades s'ha creat la nova ILP i s'ha generat la seva web personalitzada.
  No existeixen diferències amb els resultats esperats.

Proves gràfiques:

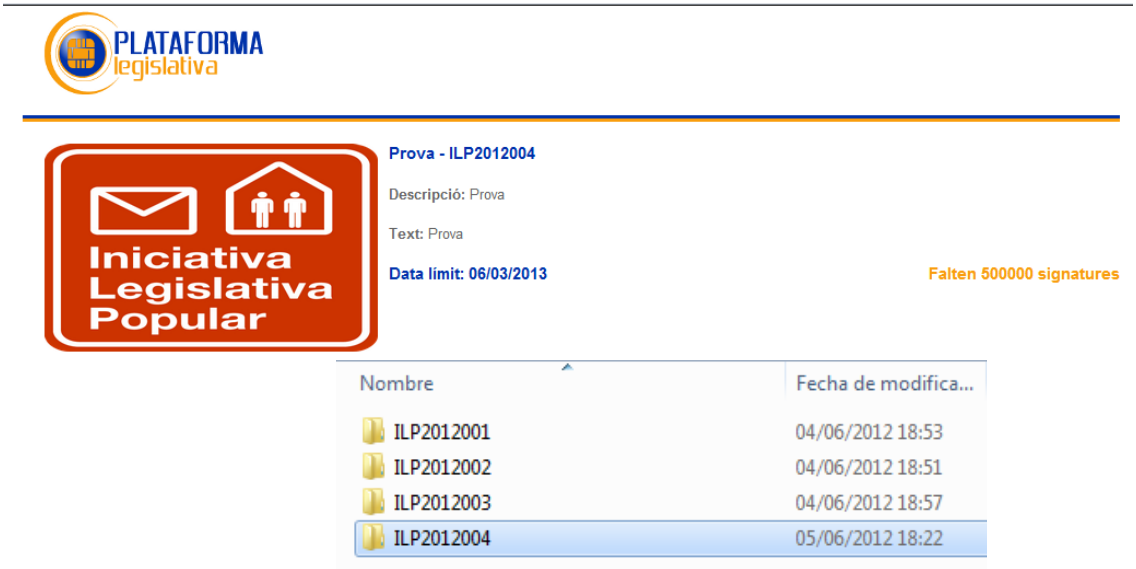

Figura 17 - Seqüència de proves gràfiques de la creació d'una nova ILP.

Modificar una ILP

- Amb aquesta prova es vol comprovar el procés de modificar una ILP. Dins d'aquesta prova també verificarem que si la ILP està activa, únicament ens deixi modificar la imatge.
- Per realitzar-la, primer accedim a la gestió de ILPs , seleccionem una ILP i premem el botó "MODIFICAR", modifiquem les dades al formulari i premem el botó "ENVIAR".
- Com a resultat observem que si la ILP està activa únicament ens deixa modificar la imatge, que a la base de dades s'han modificat les dades de la ILP i s'ha substituït l'anterior web personalitzada per una altra amb les dades actualitzades.
  No existeixen diferències amb els resultats esperats.

Activar / desactivar ILP

- Amb aquesta prova es vol comprovar el procés d'activar i desactivar una ILP. Si una ILP esta inactiva no apareixerà a la pàgina principal de la plataforma i no tindrà l'opció de signar a la seva web personalitzada.
- Per realitzar-la, primer accedim a la gestió de ILPs , seleccionem una ILP i premem el botó "ACTIVAR / DESACTIVAR", i confirmem l'acció.
- Com a resultat observem que si la ILP canvia a un estat inactiu, no apareix a la pàgina principal i tampoc es visualitzarà l'opció de signar a la seva web personalitzada.
  No existeixen diferències amb els resultats esperats.

Esborrar ILP

- Amb aquesta prova es vol comprovar el procés d'esborrar una ILP.
- Per realitzar-la, primer accedim a la gestió de ILPs , seleccionem una ILP i premem el botó "ESBORRAR", i confirmem l'acció.

- Com a resultat observem que a la base de dades s'ha eliminat la ILP seleccionada i s'ha esborrat la seva web i totes les seves signatures .
  No existeixen diferències amb els resultats esperats.

5.3. Proves de gestió de signatures

Visualitzar i descarregar una signatura

- Amb aquesta prova es vol comprovar el procés de visualitzar i descarregar una signatura.
- Per realitzar-la, primer accedim a la gestió de ILPs , seleccionem una ILP i premem el botó "GESTIÓ SIGNATURES" , una vegada dins s'ha de seleccionar una signatura i prémer el botó "DETALL SIGNATURA" , llavors visualitzarem les dades del signant i ens podrem descarregar la signatura prement el botó "DESCARREGAR".
- Com a resultat observem que les dades del signant es visualitzen correctament , que la signatura es descarrega i les seves dades corresponen a les del signant seleccionat. El nom i format de l'arxiu amb la signatura segueix les recomanacions de la nova normativa [JEC6/2012].
  No existeixen diferències amb els resultats esperats.

Exportar les signatures d'una ILP

- Amb aquesta prova es vol comprovar el procés d'exportar les signatures d'una ILP.
- Per realitzar-la, primer accedim a la gestió de ILPs , seleccionem una ILP i premem el botó "GESTIÓ SIGNATURES" , una vegada dins prémer el botó "EXPORTAR SIGNATURES" .
- Com a resultat observem que es descarrega un arxiu Excel (signatura.xls)amb les dades dels signants.
  No existeixen diferències amb els resultats esperats.

Descarregar totes les signatures d'una ILP

- Amb aquesta prova es vol comprovar el procés de descarregar totes les signatures d'una ILP.
- Per realitzar-la, primer accedim a la gestió de ILPs , seleccionem una ILP i premem el botó "GESTIÓ SIGNATURES" , una vegada dins prémer el botó "DESCARREGAR SIGNATURES" .
- Com a resultat observem que es descarrega un arxiu comprimit que conté totes les signatures d'una ILP. El nom i format de l'arxiu segueix les recomanacions de la nova normativa [JEC6/2012].
  No existeixen diferències amb els resultats esperats.

5.4. Proves de compatibilitat de l'applet.

S'ha comprovat que l'applet utilitzat funcionés correctament amb múltiples navegadors , versions de Java i sistemes operatius.
En el sistema operatiu Windows 7 s'ha provat amb les versions de Java 1.6 i 1.7 i amb els següents navegadors: Opera (versió 11.64), Firefox (versions 10,11,12 i 13), Chrome (versions 17,18 i 19), Internet Explorer (versions 8 i 9).
En el sistema operatiu Fedora 14 s'ha provat amb la versió 1.6 de Java i amb Firefox 11 i Chrome 18.
En totes aquestes proves s'han utilitzat el DNI electrònic i un certificat FNMT vàlid, i un altre de revocat .

5.5. Altres proves

Donar d'alta una comissió

- Amb aquesta prova es vol comprovar el procés de registre per part d'una comissió.
- Per realitzar-la, primer accedim a la pàgina principal de la plataforma i seleccionem l'opció "REGISTRA'T", omplim correctament les dades del formulari i premem el botó "ENVIAR".
- Com a resultat observem que a la base de dades es crea una nova comissió i s'accedeix a la part privada de la plataforma, concretament a la gestió de ILPs.
  No existeixen diferències amb els resultats esperats.

Accés a les parts privades de la plataforma.

- Amb aquesta prova es vol comprovar el procés d'accés a les parts privades de la plataforma.
- Per realitzar-la, primer accedim a la pàgina principal de la plataforma i seleccionem l'opció "ACCÉS" ", omplim l'usuari i contrasenya i premem el botó "ENTRAR".
- Com a resultat observem que amb un usuari i contrasenya correctes accedim a la part privada de la plataforma, concretament a la gestió de ILPs.
  No existeixen diferències amb els resultats esperats.

Sortir de les parts privades de la plataforma

- Amb aquesta prova es vol comprovar el procés de sortir de les parts privades de la plataforma.
- Per realitzar-la, a qualsevol lloc de la plataforma seleccionem l'opció "SORTIR".
- Com a resultat observem que es torna a la pàgina principal de la plataforma , finalitzant la sessió oberta i sortint de la part privada.
  No existeixen diferències amb els resultats esperats.

CAPÍTOL 6. CONCLUSIONS

En aquest TFC s'ha dissenyat i implementat una plataforma de recollida de signatures digitals per a ILPs.

S'han complert tots els objectius proposats al començament del TFC, ja que s'ha obtingut una plataforma que dóna la possibilitat a les comissions promotores de crear i gestionar les seves pròpies ILPs. A la vegada recull, d'una forma accessible, signatures digitals que compleixin tots els requeriments de la legislació vigent de les ILPs.

L'ús de signatures digitals i el DNI-e, unit a la possibilitat d'influir en la vida política i legislativa d'un país és una combinació que des d'un principi m'ha semblat força interessant. Així mateix, ha suposat un gran repte adaptar la plataforma per tal que les ILPs generades tinguin validesa legal considerant que no existia (fins a la sortida de la nova normativa [JEC6/2012]) un marc legal clar respecte l'ús de signatures digitals en les ILPs .

Com a conclusió, puc dir que a nivell personal aquest treball ha estat molt enriquidor gràcies a que he pogut participar en totes les fases d'un projecte informàtic i he tingut l'oportunitat de posar en pràctica i consolidar els coneixements adquirits a diferents signatures en el transcurs dels estudis, com poden ser Enginyeria del programari, Criptografia, Seguretat, Bases de dades entre d'altres. A més, he ampliat els meus coneixements en seguretat informàtica i criptografia al profunditzar en temes com, estructura de certificats, formats de signatures digitals, respostes OCSP, que no s'han tractat amb detall als estudis.

CAPÍTOL 7. LÍNIES DE FUTUR

La plataforma actual compleix amb tots els requisits però és molt bàsica, es podria millorar en molts aspectes:

- Incorporar tots els aspectes relatius a la Llei Orgànica 15/1999, del 13 de desembre , de Protecció de Dades de caràcter personal (LOPD); per tal de garantir i protegir les dades dels signants i les comissions.

- Integrar les xarxes socials (Facebook, Twitter, Google+, ...) com a mètode per ampliar la repercussió de les ILPs i així maximitzar el nombre de possibles signants.

- Adaptar el procés de signatura, tenint en compte la nova normativa [JEC6/2012].Això facilitaria que el procés fos més ràpid, ja que únicament es necessita una signatura XAdES-BES i una marca de temps en lloc de la signatura utilitzada actualment (XAdES-XL) que emmagatzema tota la cadena de certificació i la informació de validació de les signatures (respostes OCSP).

- Incorporar l'opció de fer-se fedatari, signant digitalment una declaració jurada, i afegir la gestió dels fedataris per part de les comissions. Aquesta opció augmentaria el

nombre total de signatures recollides ja que a Espanya encara hi ha un baix índex d'utilització de certificats digitals per part de la ciutadania .

- Utilitzar la plataforma per recollir signatures per Iniciatives Legislatives Autonòmiques, Iniciatives Ciutadanes Europees, Iniciatives Legislatives Locals i avals per eleccions.

- Millorar la interfície web per fer-la el més clara, atractiva i accessible a l'usuari.

- Implementar ajudes per millorar la interacció amb la plataforma i facilitar la se va comprensió.

En conclusió, podem dir que qualsevol projecte sempre és pot anar millorant al llarg del temps reben feedbacks per part dels usuaris i observant noves necessitats.

GLOSSARI

CA (*Certification Authority)*: Autoritat encarregada d'emetre i revocar certificats, i donar legitimitat a la relació d'una clau pública amb la identitat de l'usuari.

CRL (*Certificate Revocation List)*: Llista on s'inclouen tots els certificats que han deixat de ser vàlids abans de la data establerta dins del mateix certificat. S'utilitza per comprovar la validesa dels certificats digitals i té com avantatge, respecte altres mètodes (OCSP), que no requereix de connexió a la xarxa però la informació que aporta pot estar desactualitzada.

DOM (*Document Object Model)*: Interfície de programació d'aplicacions (API) que proporciona un conjunt d'objectes per representar documents HTML i XML, un model que ens diu com poden combinar-se els objectes i una interfície per accedir i manipular els objectes. Mitjançant aquest model els programes poden accedir i modificar el contingut, estructura i estil de qualsevol document HTML i XML.

JEC (*Junta Electoral Central)*: Òrgan superior de l'administració electoral a Espanya que té com funció principal garantir la transparència del procés electoral i supervisar l'actuació de l'Oficina del Cens Electoral.

Marca de temps: Assignació per mitjans electrònics de data i hora a un document electrònic.

Mesa del Congrés: Òrgan rector i de representació col·legiada del partits polítics que formen part del Congrés dels Diputats. Està integrada per el President del Congrés i la resta de vicepresidents.

OCSP (*Online Certificate Status Protocol)*: Protocol que ens permet comprovar la validesa dels certificats digitals de forma *online*, aconseguint una informació més encertada i actual que altres mètodes (CRL). Els missatges OCSP es codifiquen en ASN.1 i es transmeten per sobre del protocol HTTP.

PKI (*Public Key Infraestructure)*: Infraestructura que recull tot allò que permet la creació i gestió dels certificats digitals fonamentats en la criptografia asimètrica o de clau pública (software, components de hardware, usuaris, polítiques, procediments,...). Té com objectiu principal gestionar de forma eficient i confiable les claus criptogràfiques i els certificats per que puguin ser utilitzats en propòsits d'autenticació, integritat, confidencialitat i no repudi.

RA (*Registration Authority)*: Autoritat responsable de verificar l'enllaç entre els certificats, concretament la clau pública, i la identitat d'un usuari.

Segell de temps *(Timestamp):* Assignació per mitjans electrònics de la data i hora a un document electrònic amb la intervenció d'un prestador de serveis de certificació que ens assegura la integritat i exactitud de la marca de temps del document.

TSA (*Time Stamping Authority)*: Prestador de serveis de certificació que ens assegura la preexistència de determinats documents en una data i hora especifiques.

VA (*Validation Authority)*: Autoritat encarregada de subministrar informació sobre la vigència dels certificats digitals que han estat registrats per una autoritat de registre (RA) i certificats per l'autoritat de certificació (CA).

X.509 (*Document Object Model)*: Estàndard per infraestructures de clau pública (PKI).

XML (*eXtensible Markup Language)*: Llenguatge de representació de dades.

BIBLIOGRAFIA

[@FIRMA] **CTT (Centro de Transferencia Tecnológica).** *Cliente de firma electrónica de @firma*. <http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=clienteafirma>

[BASE64] **The Internet Society** (2006). *The Base16, Base32, and Base64 Data Encodings*. RFC 4648.
<http://tools.ietf.org/html/rfc4648>

[CRAPPLET] **Universitat Jaume I.** *CryptoApplet*.
<http://proyectostic.uji.es/pr/cryptoapplet/>

[DER] **ITU – International Telecommunication Union** (2002, febrer). *ITU-T Recommendation X.690 - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER),Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.
<http://www.itu.int/ITU-T/studygroups/com17/languages/X.690-0207.pdf>

[ETSI132] **ETSI – European Telecommunications Standards Institute** (2006, març). *ETSI TS 101 903 V1.3.2 (2006-03) Technical Specification - XML Advanced Electronic Signatures (XAdES)*.
<http://uri.etsi.org/01903/v1.3.2/ts_101903v010302p.pdf>

[ID@ZKI] **IZENPE.** Id@zki - *Applet de firma y cifrado de Izenpe*.
<http://www.izenpe.com/s1512020/es/contenidos/informacion/idazki/es_idazki/adjuntos/id@zki_COMPLETO_V.1.5.4.pdf>

[JEC6/2012] **Junta Electoral Central** (2012, 10 de maig). *Acord del 10 de maig del 2012, de la Junta Electoral Central, sobre el procediment per la verificació i certificació de les signatures d'una iniciativa legislativa popular*.
<http://www.juntaelectoralcentral.es/jec/htdocs/web/documentos/AJEC_400-101_10-05-2012.pdf>

[LO3/1984] **Espanya** (1984, 26 de març). *Llei* orgànica 3/1984, de 26 de març, reguladora de la Iniciativa Legislativa Popular.
< http://www.boe.es/boe_catalan/dias/1984/12/31/pdfs/A00011-00013.pdf>

[LO4/2006] **Espanya** (2006, 26 de maig). *Llei orgànica 4/2006, de 26 de maig, de modificació de la Llei orgànica 3/1984, de 26 de març, reguladora de la Iniciativa Legislativa Popular*.
<http://www.boe.es/boe_catalan/dias/2006/06/01/pdfs/A01693-01695.pdf>

[PKCS] **RSA Laboratories**. *Public-Key Cryptography Standards (PKCS)*.
<http://www.rsa.com/rsalabs/node.asp?id=2124>

[POLFIRMA] **Consejo Superior de Administración Electrónica** (2010, 11 de octubre). *Política de firma electrónica basada en certificados v 1.8 – OID : 2.16.724.1.3.1.1.2.1.8.*
<http://administracionelectronica.gob.es/recursos/PAE_13234313958311571.pdf?iniciativa=239>

[SHS] **NIST – National Institute of Standards and Technology** (2008, octubre). *FIPS (FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION) PUB 180-3 -Secure Hash Standard (SHS)*.
<http://csrc.nist.gov/publications/fips/fips180-3/fips180-3_final.pdf>

[USTSA] **Consejo Superior de Administración Electrónica** (2011, 29 d'abril). *Guía de uso del sello de tiempo y marca de tiempo. Uso de la TS@ (Time Stamping Authority)*.
<http://administracionelectronica.gob.es/recursos/pae_020000456.pdf/>

[X509] **D. Cooper** (2008, maig). *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*
<http://tools.ietf.org/html/rfc5280>

[XADES] **Juan Carlos Cruellas, Gregor Karlinger, Denis Pinkas, John Ross** (2003, 20 de febrer). *XML Advanced Electronic Signatures (XAdES)*.
<http://www.w3.org/TR/XAdES/>

[XMLC14N] **John Boyer, PureEdge Solutions Inc** (2001, 15 de març). *Canonical XML Version 1.0 W3C Recommendation*.
<http://www.w3.org/TR/xml-c14n>

[ZTIC1] *Criptografía y esquemas de clave pública*.
<https://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos/196-criptografia-y-esquemas-de-clave-publica.html>

[ZTIC2] *La PKI del DNI electrónico*.
<https://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos/197-la-pki-del-dni-electronico.html>

[ZTIC3] *Los certificados de autenticación y firma del DNIe*.
<https://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos/207-los-certificados-de-autenticacion-y-firma-del-dnie.html>

[ZTIC4] *Validez de Certificados*.
<https://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos/329-validez-de-certificados.html>

[ZTIC5] *Sistemas actuales de autenticación y firma*.
<https://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos/208-sistemas-actuales-de-autenticacion-y-firma.html>

[ZTIC6] *Autenticación y firma con el DNI electrónico*.
<https://zonatic.usatudni.es/es/aprendizaje/aprende-sobre-el-dnie/57-aspectos-tecnicos/198-autenticacion-y-firma-com-el-dni-electronico.html>

ANNEXOS

A. POLÍTIQUES DE SIGNATURA ACCEPTADES PER LA PLATAFORMA

S'adjunten totes les politiques de certificats acceptades per la plataforma, on tots els certificats son reconeguts per les administracions públiques i publicats a la seu electrònica del INE. Es segueix l'estructura:
Prestador de serveis de certificació.

- Nom certificat (Política del certificat)

ACA- "*Autoridad de Certificación de la Abogacía*"

- ACA PF *Administrativo* (1.3.6.1.4.1.16533.10.3.1)
- ACA PF *Colegiado* (1.3.6.1.4.1.16533.10.2.1)

ACCV - Autoritat de Certificació de la Comunitat Valenciana

- *GVA ACCV-CA2 PF Dispositivo Seguro (1.3.6.1.4.1.8149.3.6.5.0)*
- *GVA ACCV-CA2 PF Soporte Software (1.3.6.1.4.1.8149.3.7.4.0)*
- *GVA APE EMPLEADO PÚBLICO MEDIO HW (1.3.6.1.4.1.8149.3.13.3.0)*
- *GVA APE EMPLEADO PÚBLICO MEDIO SW (1.3.6.1.4.1.8149.3.18.1.0)*

ANCERT - "*Agencia Notarial de Certificación*"

- *ANCERT PF Notarial Personal (1.3.6.1.4.1.18920.1.1.1.1)*
- *ANCERT PF Notarial Personal de Representación Personal (1.3.6.1.4.1.18920.1.1.2.1)*
- *ANCERT PF Notarial Corporativo de Representación Firma 2010 (1.3.6.1.4.1.18920.1.3.2.2.1)*
- *ANCERT PF Notarial Personal Firma 2010 (1.3.6.1.4.1.18920.1.1.1.2.1)*
- *ANCERT PF Notarial Personal de Representación Personal Firma 2010 (1.3.6.1.4.1.18920.1.1.2.2.1)*
- *ANCERT PF FEREN (1.3.6.1.4.1.18920.4.1.1.1)*
- *ANCERT PF Empleado (1.3.6.1.4.1.18920.4.2.1.1)*
- *ANCERT PF FEREN Firma 2010 (1.3.6.1.4.1.18920.4.1.1.2.1)*
- *ANCERT PF Empleado Firma 2010 (1.3.6.1.4.1.18920.4.2.1.2.1)*

ANF AC - "*Asociación Nacional de Fabricantes Autoridad de Certificación*"

- *ANF PF Nuevo (1.3.6.1.4.1.18332.3.4)*
- *ANF APE EMPLEADO PÚBLICO Firma (1.3.6.1.4.1.18332.4.4)*

BANESTO

- BANESTO PF (Persona Física) (1.3.6.1.4.1.11076.1.2)

CAMERFIRMA

- *CAMERFIRMA APE EMPLEADO PUBLICO Medio (1.3.6.1.4.1.17326.1.3.4.4)*
- *CAMERFIRMA PF Apoderado HW Clave usuario (1.3.6.1.4.1.17326.10.9.5.2.2)*
- *CAMERFIRMA PF Apoderado SW Clave PSC (1.3.6.1.4.1.17326.10.9.5.1.1)*
- *CAMERFIRMA PF Apoderado SW Clave usuario (1.3.6.1.4.1.17326.10.9.5.1.2)*
- *CAMERFIRMA PF EFactura HW Clave PSC (1.3.6.1.4.1.17326.10.9.7.2.1)*
- *CAMERFIRMA PF EFactura HW Clave usuario (1.3.6.1.4.1.17326.10.9.7.2.2)*
- *CAMERFIRMA PF EFactura SW Clave PSC (1.3.6.1.4.1.17326.10.9.7.1.1)*
- *CAMERFIRMA PF EFactura SW Clave usuario (1.3.6.1.4.1.17326.10.9.7.1.2)*
- *CAMERFIRMA PF HW Clave PSC (1.3.6.1.4.1.17326.10.9.2.2.1)*
- *CAMERFIRMA PF HW Clave usuario (1.3.6.1.4.1.17326.10.9.2.2.2)*
- *CAMERFIRMA PF Representante HW Clave PSC (1.3.6.1.4.1.17326.10.9.3.2.1)*
- *CAMERFIRMA PF Representante HW Clave usuario (1.3.6.1.4.1.17326.10.9.3.2.2)*
- *CAMERFIRMA PF Representante SW Clave PSC (1.3.6.1.4.1.17326.10.9.3.1.1)*
- *CAMERFIRMA PF Representante SW Clave usuario (1.3.6.1.4.1.17326.10.9.3.1.2)*
- *CAMERFIRMA PF SW Clave PSC (1.3.6.1.4.1.17326.10.9.2.1.1)*
- *CAMERFIRMA PF SW Clave usuario (1.3.6.1.4.1.17326.10.9.2.1.2)*
- *CAMERFIRMA RACER PF Ciudadano SW Clave PSC (1.3.6.1.4.1.17326.10.8.6.1.1)*
- *CAMERFIRMA PF Apoderado HW Clave PSC (1.3.6.1.4.1.17326.10.9.5.2.1)*

CATCERT

- *CATCERT EC-IDCat PF con cifrado (1.3.6.1.4.1.15096.1.3.1.86.1)*
- *CATCERT AL PF Iden. Firma Recon. Cargo Uso Concreto Clase 1 (1.3.6.1.4.1.15096.1.3.1.81.3.2)*

- *CATCERT AL PF Identidad y Firma Reconocida Cargo de Clase 1 (1.3.6.1.4.1.15096.1.3.1.81.2.5)*
- *CATCERT AL PF Identidad y Firma Reconocida Cargo de Clase 2 (1.3.6.1.4.1.15096.1.3.1.82.3.5)*
- *CATCERT GENCAT SAFP PF Identidad y Firma Recon. de Clase 1 (1.3.6.1.4.1.15096.1.3.1.81)*
- *CATCERT SAFP PF Iden. Firma Reco. Cargo Uso Concreto Clase 1 (1.3.6.1.4.1.15096.1.3.1.81.3.4)*
- *CATCERT SAFP PF Iden. Firma Recon. Cargo de Clase 2 (1.3.6.1.4.1.15096.1.3.1.82.3.2)*
- *CATCERT SAFP PF Iden. Firma Reconocida con Cargo de Clase 1 (1.3.6.1.4.1.15096.1.3.1.81.2.4)*
- *CATCERT PARL PF Iden. Firma Recon. con Cargo de Clase 2 (1.3.6.1.4.1.15096.1.3.1.82.3.2)*
- *CATCERT PARL PF Iden. Firma Recon. Cargo Uso Concreto Clase 1 (1.3.6.1.4.1.15096.1.3.1.81.3.4)*
- *CATCERT PARL PF Iden. y Firma Recon. con Cargo de Clase 1 (1.3.6.1.4.1.15096.1.3.1.81.2.2)*
- *CATCERT URV PF Iden. Firma Rec. Cargo Clase 1 (1.3.6.1.4.1.15096.1.3.1.81.2.3)*
- *CATCERT URV PF Iden. Firma Rec. Cargo Clase 2 (1.3.6.1.4.1.15096.1.3.1.82.3.3)*
- *CATCERT URV PF Iden. Firma Rec. Cargo Estu. Extr. Clase 2 (1.3.6.1.4.1.15096.1.3.1.82.2.4)*
- *CATCERT URV PF Iden. Firma Rec. Cargo Estudiante Clase 2 (1.3.6.1.4.1.15096.1.3.1.82.2.2)*
- *CATCERT UR PF Iden. Firma Rec. Cargo Clase 2 (1.3.6.1.4.1.15096.1.3.1.82.3.1)*
- *CATCERT UR PF Iden. Firma Rec. Cargo Uso Concreto (1.3.6.1.4.1.15096.1.3.1.81.3.3)*
- *CATCERT UR PF Iden. Firma Rec. Estudiante Clase 2 (1.3.6.1.4.1.15096.1.3.1.82.2.1)*
- *CATCERT UR PF Ident. Firma Reco. Cargo Clase 1 (1.3.6.1.4.1.15096.1.3.1.81.2.1)*
- *CATCERT URV PF Iden. Firma Rec. Cargo Uso Concreto Clase 1 (1.3.6.1.4.1.15096.1.3.1.81.3.5)*

DNIe

- *Firma de Ciudadano (SHA 1) (2.16.724.1.2.2.2.3)*

FIRMAPROFESIONAL

- *FP PF Colegiado Común (1.3.6.1.4.1.13177.10.1.1.2)*
- *FP PF Colegiado con DSCF (1.3.6.1.4.1.13177.10.1.1.1)*
- *FP PF Persona Vinculada Común (1.3.6.1.4.1.13177.10.1.2.2)*
- *FP PF Persona Vinculada con DSCF (1.3.6.1.4.1.13177.10.1.2.1)*
- *FIRMAPROFESIONAL APE EMPLEADO PÚBLICO Firma (1.3.6.1.4.1.13177.10.1.22.1)*
- *FIRMAPROFESIONAL APE EMPLEADO PÚBLICO Medio (1.3.6.1.4.1.13177.10.1.22.2)*

FNMT-Ceres

- *FNMT PF (Persona Física) (1.3.6.1.4.1.5734.3.5)*
- *FNMT APE EMPLEADO PÚBLICO Medio (1.3.6.1.4.1.5734.3.14)*

- *FNMT APE EMPLEADO PÚBLICO Medio SW NEW (1.3.6.1.4.1.5734.3.3.4.4.2)*
- *FNMT APE EMPLEADO PÚBLICO Medio HW NEW (1.3.6.1.4.1.5734.3.3.4.4.1)*

IZENPE

- *IZENPE AAPP PF Personal (1.3.6.1.4.1.14777.4.1)*
- *IZENPE PF (1.3.6.1.4.1.14777.2.6)*
- *IZENPE AAPP PF Personal (2009) (1.3.6.1.4.1.14777.4.1)*
- *IZENPE PF Personal Gobierno Vasco (2009) (1.3.6.1.4.1.14777.7.1)*
- *IZENPE PF (2009) (1.3.6.1.4.1.14777.2.6)*

SCR – "*Servicio de Certificación de los Registradores*"

- *SCR SL EXTERNOS PF Administración Local (1.3.6.1.4.1.17276.0.2.4.1)*
- *SCR SL EXTERNOS PF Cargo Administrativo (1.3.6.1.4.1.17276.0.2.3.1)*
- *SCR SL EXTERNOS PF Personal (1.3.6.1.4.1.17276.0.2.1.1)*
- *SCR SL EXTERNOS PF Profesional (1.3.6.1.4.1.17276.0.2.5.1)*
- *SCR SL INTERNOS PF Registrador (1.3.6.1.4.1.17276.0.1.1.1)*

B. SCRIPT DE CREACIÓ I CONFIGURACIÓ DE LA BASE DE DADES

S'adjunta el *script* de comandes SQL per a la:

- Creació de la base de dades.
- Creació del model de dades
- Creació de l'usuari de connexió
- Assignació de permisos a l'usuari de connexió

```
SET @OLD_UNIQUE_CHECKS=@@UNIQUE_CHECKS, UNIQUE_CHECKS=0;
SET @OLD_FOREIGN_KEY_CHECKS=@@FOREIGN_KEY_CHECKS, FOREIGN_KEY_CHECKS=0;
SET @OLD_SQL_MODE=@@SQL_MODE, SQL_MODE='TRADITIONAL';

CREATE SCHEMA IF NOT EXISTS `ilp` DEFAULT CHARACTER SET utf8 COLLATE
utf8_spanish_ci ;
USE `ilp` ;

-- -----------------------------------------------------
-- Table `ilp`.`signants`
-- -----------------------------------------------------
CREATE  TABLE IF NOT EXISTS `ilp`.`signants` (
  `idsignant` BIGINT(20) NOT NULL AUTO_INCREMENT ,
  `nif` VARCHAR(9) NOT NULL ,
  `nom` VARCHAR(20) NOT NULL ,
  `cognom_1` VARCHAR(25) NOT NULL ,
  `cognom_2` VARCHAR(25) NOT NULL ,
  `data_nx` DATE NOT NULL ,
  PRIMARY KEY (`idsignant`) )
ENGINE = InnoDB;
```

```
-- -----------------------------------------------------
-- Table `ilp`.`comissions`
-- -----------------------------------------------------
CREATE  TABLE IF NOT EXISTS `ilp`.`comissions` (
  `idcomissio` INT NOT NULL AUTO_INCREMENT ,
  `nif_r` VARCHAR(9) NOT NULL ,
  `nom_r` VARCHAR(20) NOT NULL ,
  `cognom_1_r` VARCHAR(30) NOT NULL ,
  `cognom_2_r` VARCHAR(30) NOT NULL ,
  `email` VARCHAR(50) NOT NULL ,
  `username` VARCHAR(32) NOT NULL ,
  `password` VARCHAR(16) NOT NULL ,
  `data_cr` TIMESTAMP NOT NULL ,
  `data_mod` TIMESTAMP NULL ,
  PRIMARY KEY (`idcomissio`) )
ENGINE = InnoDB;

-- -----------------------------------------------------
-- Table `ilp`.`ilps`
-- -----------------------------------------------------
CREATE  TABLE IF NOT EXISTS `ilp`.`ilps` (
  `idilp` INT NOT NULL AUTO_INCREMENT ,
  `idcomis` INT NOT NULL ,
  `estat` TINYINT(1) NOT NULL ,
  `codi_jec` VARCHAR(10) NOT NULL ,
  `nom` VARCHAR(300) NOT NULL ,
  `descripcio` TEXT NOT NULL ,
  `text` TEXT NOT NULL ,
  `data_inici` DATE NOT NULL ,
  `data_fi` DATE NOT NULL ,
  `banner_sm` VARCHAR(200) NULL ,
  `data_cr` TIMESTAMP NOT NULL ,
  `data_mod` TIMESTAMP NULL ,
  PRIMARY KEY (`idilp`) ,
  INDEX `fk_comissio` (`idcomis` ASC) ,
  CONSTRAINT `fk_comissio`
    FOREIGN KEY (`idcomis` )
    REFERENCES `ilp`.`comissions` (`idcomissio` )
    ON DELETE NO ACTION
    ON UPDATE NO ACTION)
ENGINE = InnoDB;

-- -----------------------------------------------------
-- Table `ilp`.`signatures`
-- -----------------------------------------------------
CREATE  TABLE IF NOT EXISTS `ilp`.`signatures` (
  `idsignant` BIGINT(20) NOT NULL ,
  `idilp` INT NOT NULL ,
  `signatura` VARCHAR(200) NOT NULL ,
  `data_cr` TIMESTAMP NOT NULL ,
  INDEX `fk_signant` (`idsignant` ASC) ,
  INDEX `fk_ilp` (`idilp` ASC) ,
  PRIMARY KEY (`idsignant`, `idilp`) ,
  CONSTRAINT `fk_signant`
    FOREIGN KEY (`idsignant` )
    REFERENCES `ilp`.`signants` (`idsignant` )
    ON DELETE NO ACTION
    ON UPDATE NO ACTION,
```

```
  CONSTRAINT `fk_ilp`
    FOREIGN KEY (`idilp` )
    REFERENCES `ilp`.`ilps` (`idilp` )
    ON DELETE CASCADE
    ON UPDATE NO ACTION)
ENGINE = InnoDB;

CREATE USER `ilp` IDENTIFIED BY 'ilp1977';

grant DELETE on TABLE `ilp`.`signants` to ilp;
grant INSERT on TABLE `ilp`.`signants` to ilp;
grant SELECT on TABLE `ilp`.`signants` to ilp;
grant UPDATE on TABLE `ilp`.`signants` to ilp;
grant INSERT on TABLE `ilp`.`comissions` to ilp;
grant SELECT on TABLE `ilp`.`comissions` to ilp;
grant UPDATE on TABLE `ilp`.`comissions` to ilp;
grant DELETE on TABLE `ilp`.`comissions` to ilp;
grant DELETE on TABLE `ilp`.`ilps` to ilp;
grant INSERT on TABLE `ilp`.`ilps` to ilp;
grant SELECT on TABLE `ilp`.`ilps` to ilp;
grant UPDATE on TABLE `ilp`.`ilps` to ilp;
grant DELETE on TABLE `ilp`.`signatures` to ilp;
grant INSERT on TABLE `ilp`.`signatures` to ilp;
grant SELECT on TABLE `ilp`.`signatures` to ilp;
grant UPDATE on TABLE `ilp`.`signatures` to ilp;

SET SQL_MODE=@OLD_SQL_MODE;
SET FOREIGN_KEY_CHECKS=@OLD_FOREIGN_KEY_CHECKS;
SET UNIQUE_CHECKS=@OLD_UNIQUE_CHECKS;
```

C. INSTALACIÓ I CONFIGURACIÓ DE LA PLATAFORMA

Els requisits necessaris per instal·lar la plataforma són:

- Servidor web amb suport per PHP 5 i MySQL (recomanació: Apache 2.2).
- MySQL *Community Server* (recomanació: versió 5.1 o superior).
- PHP amb els següents mòduls actius: openssl, mysql, SimpleXML, zip, mcrypt, session.

1.- Per instal·lar la plataforma s'ha de copiar l'estructura de la plataforma a la carpeta corresponent del servidor web i comprovar que el usuari del servidor web tingui permisos d'escriptura, principalment a les carpetes imatges/ilp, signatures i web.

2.- Utilitzar el *script* de creació i configuració de la base de dades (crear_plataforma.sql) per generar l'estructura de dades de la plataforma, abans d'executar-lo es pot configurar la informació relativa als usuaris (nom usuari i contrasenya) modificant la següent línea del *script*:
`CREATE USER `nomusuari` IDENTIFIED BY 'contrasenya';`

Si es modifica el nom d'usuari, també s'haurien de modificar els permisos d'aquest.
Ex: `grant DELETE on TABLE `nomusuari`.`signants` to ilp;`

3.- Per configurar la plataforma s'ha de modificar l'arxiu de configuració (app_config.php), que es troba a la carpeta *scripts*.

En aquest arxiu trobem diverses constats susceptibles d'ésser modificades :

- "DEBUG_MODE": Pot prendre els valors *true*, si volem que PHP notifiqui tots els errors o *false* si volem desactivar la notificació d'errors.
- "SITE_ROOT": directori local on es troba la web. Ex: "/var/www/plataformalegislativa.com/"
- "DATABASE_HOST": Nom del host on es troba la base de dades. Ex: "localhost".
- "DATABASE_USERNAME": Nom d'usuari per conectar-se a la base de dades. Ex: "userilp".
- "DATABASE_PASSWORD": Contrasenya d'accés a la base de dades. Ex: "passilp".
- "DATABASE_NAME": Nom de la base de dades. Ex: "ilp".