Treball final de carrera:

Disseny i implementació d'una plataforma per a la recollida i signatura d'iniciatives legislatives populars.

Yago Luling Gimeno

Enginyeria tècnica en informàtica de sistemes (ETIS)

Cristina Pérez Solà

Professora Consultora

05.121 – TFC-Seguretat informàtica

Curs 2011/12, Q2

Dedicatòria i agraïments.

Vull dedicar aquest treball a la meva dona Mei i al meu fill Nick que han patit gairebé quatre mesos la meva absència i que m'han recolzat en els moments que ho he necessitat.

Vull agrair especialment a la meva parella el haver-se fet càrrec de tot per que jo pogués portar a terme aquest projecte i que ha estat sempre al meu costat.

També, vull donar les gràcies a la Cristina Pérez Solà que com a consultora m'ha ajudat moltíssim a aclarir com enfocar i desenvolupar el projecte. Gràcies per la excepcionalment ràpida resposta davant els dubtes que m'han anat sorgit en el transcurs del projecte.

Per acabar, també vull agrair a totes aquelles persones i companyies compromeses amb el programari lliure; especialment, a la comunitat GNU/Linux que ha contribuït en el meu aprenentatge i que contribueix dia a dia el l'aprenentatge de milions de persones arreu del món.

Resum

Amb aquest projecte es pretén implementar una plataforma web que permeti la creació de noves iniciatives legislatives populars i la seva posterior signatura.

Aquesta plataforma contempla els requisits de seguretat propis d'una iniciativa d'aquest tipus com l'autenticació dels usuaris, la protecció de dades, la verificació del dret a signar i la no duplicitat de signatures entre d'altres.

La solució es basa en l'autenticació dels usuaris mitjançant tècniques criptogràfiques de clau pública. En concret aquesta plataforma permet l'autenticació, no només mitjançant un certificat digital instal·lat en el navegador, sinó també amb el certificat digital inclòs en el DNI electrònic.

A més dels requisits de seguretat esmentats i del sistema d'autenticació establert, la plataforma també contempla el correcte compliment dels requisits legals per tal que les signatures recollides siguin vàlides davant la Junta Electoral Central.

La present memòria es presenta en compliment parcial dels requisits del Treball Final de Carrera per l'Enginyeria Tècnica en Informàtica de Sistemes, ubicat dins de l'àrea de seguretat informàtica.

Paraules clau: ***certificat digital, signatura digital, x509, HTTPS, SSL, TLS, DNI-e, ILP, Iniciativa legislativa popular, Autenticació*****, @firma.**

Índex

Índex de figures.

1. Introducció

1.1. Justificació del TFC i context en el qual es desenvolupa.

Avui en dia, el règim polític espanyol és constituït com a una monarquia parlamentària que es reflexa com a una democràcia representativa.

La participació popular en el govern de l'estat es basa en l'elecció de representants populars als òrgans del govern mitjançant les eleccions legislatives en les que el poble designa als seus representats a les Corts Generals.

Així, seguint la tendència d'altres països democràtics moderns i amb la intenció d'intensificar la participació ciutadana en la vida pública, la constitució espanyola preveu la participació directa dels ciutadans mitjançant les Iniciatives legislatives Populars (ILP).

Les Iniciatives Legislatives Populars (ILP) són un procés mitjançant el qual els ciutadans de l'Estat espanyol poden presentar proposicions de llei al poder legislatiu subscrites per gran part de l'electorat però que no es veuen esmentades per cap formació política amb representació parlamentaria.

El principal inconvenient que presenta elaborar una Iniciativa Legislativa Popular és la recollida de les 500,000 firmes i la comprovació de la seva validesa per tal de que aquestes siguin totalment vàlides davant la Junta Electoral Central(JEC).

Aquest treball es desenvolupa per a la simplificació del procés de recollida de firmes evitant així els desplaçaments necessaris propis d'una recollida de firmes tradicional, amb la intenció de intensificar encara més la participació ciutadana en la vida pública.

1.2. Objectius del TFC.

El principal objectiu d'aquest projecte és:

Elaboració d'una plataforma web que ajudi a la tramitació d'ILP des de la que es puguin fer proposicions de llei i recollida de signatures mitjançant certificat digital o DNI electrònic, tot tenint en compte els requisits establerts per a que aquestes siguin vàlides davant la Junta Electoral Central.

L'objectiu d'aquest projecte ha de contemplar els següents requisits:

- ***Protecció de dades del signant.***

  Els usuaris han de poder veure el nombre de signatures fins al moment però mai els noms o d'altres dades dels que han signat anteriorment. Només la comissió promotora i el propi administrador del lloc web han de poder veure les dades dels signants.

- ***Creació propostes.***

  Els usuaris podran crear noves propostes, essent l'usuari que dóna d'alta la nova proposta la comissió promotora d'aquesta.

- ***Control signants.***

  Només els usuaris censats poden signar les propostes.

- ***Control duplicitat signatures.***

  Cada usuari només pot signar un sol cop per a cada iniciativa.

- ***Autenticació signants.***

  Possibilitat d'autenticació amb certificat digital o DNI-e.

- ***Facilitat d'ús per part de l'usuari***

1.3. Enfocament i mètode seguit.

Se seguirà una metodologia basada en sis fases.

Fase d'anàlisi:

Durant aquesta primera etapa es pretén comprendre i assimilar la feina a realitzar, identificar els objectius, els requisits funcionals, els casos d'ús i els usuaris als qui va destinada la plataforma.

Fase de planificació:

Durant aquesta fase es definiran els requeriments tècnics.

Es definiran els requeriments del software que es farà servir per a la implementació de la aplicació, és a dir, sistema operatiu, software per al servidor, editor disseny web i llenguatges programació.

També es definiran els requeriments a nivell de hardware com equip servidor i requeriments de xarxa si l'aplicació ha de ser accessible des de internet o des de la intranet.

Fase de disseny:

En aquesta fase es portarà a terme el disseny de la web i BBDD però no únicament des de la vesant gràfica, sinó que es tindran en compte aspectes com la usabilitat o l'accessibilitat.

La usabilitat per tal de crear una web intuïtiva i de fàcil ús.

L'accessibilitat per tal de que el contingut sigui visible per al major nombre d'usuaris possible, tenint en compte diferents equips, navegadors o idiomes.

Per part de la BBDD es portarà a terme el disseny de l'estructura de les dades

En aquesta fase també es definiran els mòduls i les seves especificacions.

Fase de programació:

Durant aquesta fase es portarà a terme la implementació de la web.

Creació de la interfície gràfica, creació de la BBDD i la implementació del codi

Fase de proves:

Durant aquesta fase es realitzaran proves exhaustives per a comprovar el bon funcionament de la web.

Es realitzaran proves amb diferents navegadors per a comprovar la seva accessibilitat.

Per altra banda es faran proves tot intentant signar iniciatives amb certificats no vàlids o en nom de menors, així com intentar signar múltiples vegades una iniciativa entre d'altres.

Fase de documentació:

Durant aquesta ultima etapa, es farà un recull de manuals, informes i guies per tal de comprendre el procés de creació del nostre projecte.

1.4. Planificació del projecte.

1.4.1. Desglossat de tasques del projecte

Tasca 1: Estudi de l'entorn legal que envolta a les ILP.

Descripció de la tasca:

Recopilar la informació disponible sobre ILP a nivell de requisits legals i de seguretat.

Objectius de la tasca:

Adquirir els coneixements necessaris, per a poder implementar la seguretat pertinent a la nostra plataforma de manera que les propostes i signatures siguin vàlides davant la Junta Electoral.

Tasca 2 : Estudi de l'estat de l'art:

Descripció de la tasca:

Recopilar informació sobre altres plataformes per a la recollida i signatura de ILP, així com d'altres que facin ús del vot electrònic amb certificat digital o DNI electrònic.

Objectius de la tasca:

Adquirir el coneixement necessari per a comprendre l'estat actual de l'art.

Tasca 3: Anàlisi dels requisits de l'aplicació

Descripció de la tasca:

Fer un anàlisi dels objectius, requisits funcionals i de seguretat de la web.

Objectius de la tasca:

Determinar les funcions i requisits a implementar.

Tasca 4: Descripció dels casos d'ús.

Descripció de la tasca

Descriure tots els possibles casos d'ús que es poden donar.

Objectius de la tasca:

Determinar tots els possibles usuaris i les accions que poden prendre prèviament a l'inici de la implementació.

Tasca 5: Descripció requisits a nivell de hardware.

Descripció de la tasca

Descriure el hardware necessari per a la implementació de la nostra plataforma web.

Objectius de la tasca:

Determinar equip servidor i equipament de xarxa necessari per a la implementació del projecte.

Tasca 6: Descripció requisits a nivell de software.

Descripció de la tasca:

Definir els requeriments del software que es farà servir per a la implementació de la aplicació; és a dir, sistema operatiu, software per al servidor, editor disseny web i llenguatges de programació.

Objectius de la tasca:

Determinar el software necessari per a la complerta implementació del projecte.

Tasca 7: Disseny de la base de dades

Descripció de la tasca:

Disseny de l'estructura de dades que farem servir per a la gestió dels usuaris, propostes i signatures entre d'altres.

Objectius de la tasca:

Determinar la estructura de dades necessària per a la gestió del projecte.

Tasca 8: Disseny de les interfícies gràfiques.

Descripció de la tasca

Disseny del entorn gràfic que tindrà la nostra web.

Objectius de la tasca:

Definir l'estil de la nostra web.

Tasca 9: Disseny del flux de l'aplicació.

Descripció de la tasca

Dissenyar el flux de l'aplicació.

Objectius de la tasca:

Determinar les validacions que es faran quan un usuari enviï una signatura, o quan una comissió creï una proposta, etc.

Tasca 10: Creació de la pàgina web.

Descripció de la tasca

Implementació d'una pàgina web segura seguint els requisits funcionals i de disseny prèviament definits.

Objectius de la tasca:

Obtenir una pàgina web segura seguint les especificacions esmentades.

Tasca 11: Creació de la base de dades.

Descripció de la tasca

Implementació i integració de la base de dades prèviament dissenyada a la nostra web.

Objectius de la tasca:

Obtenir una base de dades totalment funcional integrada amb la web.

Tasca 12: Implementació algorismes criptogràfics.

Descripció de la tasca:

Implementar els algorismes per a la signatura amb certificat digital o amb DNI electrònic.

Objectius de la tasca:

Obtenir la funcionalitat criptogràfica requerida.

Tasca13: Banc de proves

Descripció de la tasca:

Comprovar el bon funcionament de la plataforma.

Objectius de la tasca:

Avaluar el bon rendiment del servei davant de possibles errors tant si són intencionats com si no.

Tasca 14: Correcció de "*bugs*"

Descripció de la tasca:

Corregir possibles errors en el funcionament de l'aplicació.

Objectius de la tasca:

Obtenir una aplicació sense errors.

Tasca 15: Recollida de documentació

Descripció de la tasca:

Recopilar tota la informació i redactar el procés de implementació del projecte.

Objectius de la tasca:

Obtenir una memòria del projecta detallada en la que es vegi reflectida tot el procés de creació del projecte

1.4.2. Planificació temporal.

Cronograma:

TASCA	DESCRIPCIÓ	INICI	FI	DEDICACIÓ (dies)
TASCA 1	Estudi de l'entorn legal que envolta a les ILP.	22-mar	25-mar	4
PAC 1	Preparació entrega PAC 1	26-mar	29-mar	4
TASCA 2	Estudi de l'estat de l'art	30-mar	31-mar	2
TASCA 3	Anàlisi de requisits de l'aplicació	1-abr	2-abr	2
TASCA 4	Descripció dels casos d'us	3-abr	4-abr	2
TASCA 5	Descripció requisits a nivell de hardware.	5-abr	5-abr	1
TASCA 6	Descripció requisits a nivell de software.	6-abr	8-abr	3
TASCA 7	Disseny de la base de dades	9-abr	10-abr	2
PAC 2	Preparació Entrega PAC 2	11-abr	13-abr	3
TASCA 8	Disseny de les interfícies gràfiques.	14-abr	16-abr	3
TASCA 9	Disseny del flux de l'aplicació.	17-abr	19-abr	3
TASCA 10	Creació de la pàgina web.	20-abr	29-abr	10
TASCA 11	Creació de la base de dades.	30-abr	2-may	5
TASCA 12	Implementació algorismes criptogràfics.	3-may	11-may	9
TASCA 13	Banc de proves	12-may	15-may	4
PAC 3	Preparació Entrega PAC 3	16-may	18-may	3
TASCA 14	Correcció de "bugs"	19-may	27-may	9
TASCA 15	Recollida de informació	28-may	5-jun	9
PAC 4	Preparació Entrega PAC 4	6-jun	8-jun	3
REPÀS	Revisió memòria	9-jun	12-jun	4
Lliurament producte	Preparació Lliurament memòria i producte resultant	13-jun	15-jun	3
Presentació	Elaboració presentació virtual	16-jun	21-jun	6
Lliurament presentació	Lliurament de la presentació virtual	22-jun	22-jun	1

Figura 1.

Diagrama de Gannt:

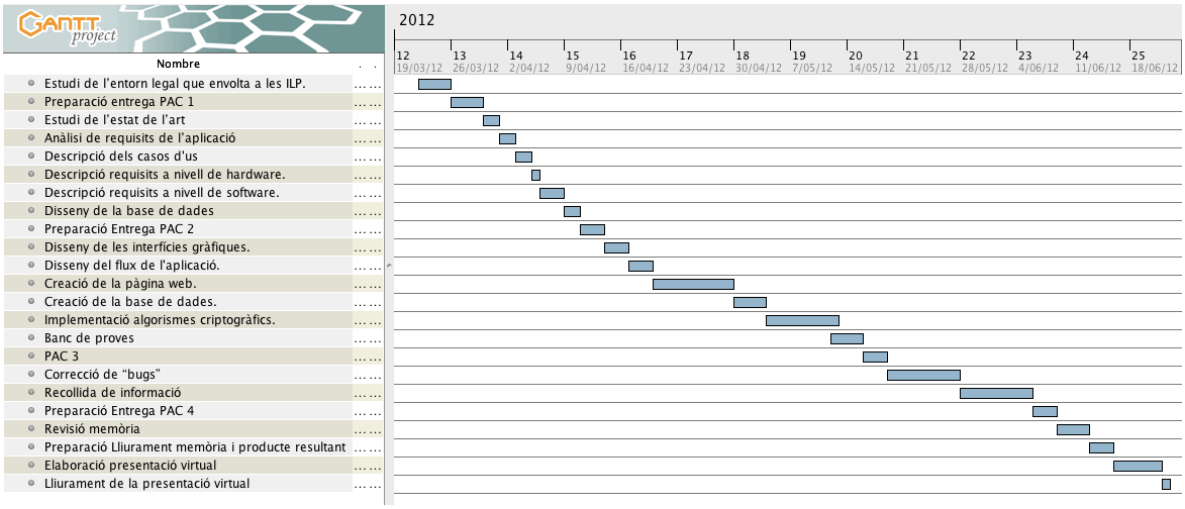

Figura 2.

1.5. Producte obtingut.

El producte resultant d'aquest treball final de carrera és una plataforma web per a la gestió d'iniciatives legislatives populars.

Aquesta plataforma a banda de visualitzar les iniciatives en curs i el nombre de signatures fins al moment, permet 3 accions ben diferenciades:

Crear iniciativa:

Abans d'admetre la inserció d'una nova iniciativa, aquesta plataforma farà les comprovacions següents:

- Autenticació amb dnie o certificat digital de la FNMT Clase 2
- Comprovació de majoria d'edat.
- Comprovació codi iniciativa tingui el format adient.
- Comprovació de camps buits.
- Comprovació de data fi recollida signatures. Aquesta no pot ser anterior a la data del moment de creació ni superior a 9 mesos des de la data actual.
- Comprovació de no duplicitat de codi o títol.

Signar iniciativa:

Per a admetre una signatura, la plataforma farà les comprovacions següents.

- Autenticació amb dnie o certificat digital de la FNMT Clase 2
- Comprovació de majoria d'edat.
- Comprovació de que termini de recollida de signatures no s'hagi exhaurit
- Comprovació de que l'usuari no hagi signat anteriorment aquella iniciativa.

Un cop fetes aquestes comprovacions, la plataforma fa les següents accions:

- Es crea fitxer xml amb les dades de la iniciativa i del usuari seguint el format exigit per la Junta Electoral Central.
- Es signa en format XADES i l'algorisme SHA256withRSA.
- Es permet a l'usuari guardar una còpia de la signatura.
- S'insereix la signatura a la BBDD en format text.
- Es crea i emmagatzema fitxer xml amb la signatura amb el nom: ILPAAAANNN.DDDDDDDDD.XML, on:
  - ILPAAAANNN és el codi de la iniciativa
  - DDDDDDDDD és el DNI de l'usuari que signant.
- Es mostra missatge de finalització del procés.

Obtenir Signatures:

Aquesta és una tasca exclusiva del promotor de la iniciativa en qüestió. Així doncs les comprovacions a fer en aquest cas són les següents:

- Autenticació amb dnie o certificat digital de la FNMT Clase 2,
- Comprovació de que l'usuari autenticat es correspon amb l'usuari promotor que va crear la iniciativa.

Un cop fetes aquestes comprovacions es potent a terme les següents accions:

- Es crea fitxer zip amb nom: ILPAAAANNN.001.ZIP on :
  - ILPAAAANNN és el codi de la iniciativa.
  - 001 número de fitxer d'entrega. (Només es contempla 1 fitxer)
- S'inicia la descarrea del fitxer ILPAAAANNN.001.ZIP.

1.6. Breu descripció dels altres capítols de la memòria.

Capítol 2. Fase d'anàlisi:

En aquest capítol s'estudia l'entorn legal que envolta a les iniciatives legislatives populars i la recollida de signatures en format digital juntament amb l'estat de l'art per tal de determinar els requisits funcionals i casos d'ús necessaris per a la implementació de la nostra aplicació.

Capítol 3. Fase de planificació.

En aquest capítol establim els requisits a nivell de software i hardware necessaris per al desenvolupament de la nostre aplicació donats els requisits funcionals determinats a la fase d'anàlisi.

Capítol 4. Fase de disseny.

En aquest capítol ja definim amb detall quin serà el funcionament i estructura de la nostra aplicació. Definirem doncs la estructura conceptual i lògica de la base de dades, la interfície d'usuari i el flux de la nostra aplicació.

Capítol 5. Fase de programació.

En aquest capítol veurem amb detall com s'ha portat a terme el desenvolupament de la nostra aplicació per al que fa la preparació de l'entorn de treball, l'establiment de comunicació segura amb el servidor mitjançant el protocol HTTPS, l'autenticació amb dnie i certificat digital i la implantació de l'applet de @firma per a la signatura amb certificat digital.

Capítol 6. Fase de proves.

En aquest capítol veurem les proves que s'han fet per tal de validar el nostre producte tals com la creació de noves iniciatives, signatura de iniciatives, accés a les signatures per part del promotor, accessos restringits i gestió d'errors.

2. Fase d'anàlisi

2.1 Entorn legal que envolta les ILP.

Per a comprendre les necessitats de l'aplicació que es vol desenvolupar, primerament hem de conèixer més a fons tot el procés des de que es fa una proposta fins que aquesta és aprovada o rebutjada per la Junta Electoral Central.

2.1.1 Presentació proposició de llei.

Tots els ciutadans inscrits al cens electoral poden exercir la iniciativa legislativa popular.

El procediment s'inicia amb la presentació davant la Mesa del Congrés dels diputats de la següent documentació:

- Text articulat de la proposició de llei precedida per una exposició de motius.
- Relació dels membres de la comissió promotora de la iniciativa.

Estan excloses de la iniciativa legislativa popular les següents matèries:

- Lleis orgàniques
- Les de caràcter tributari
- Les de caràcter internacional
- Les referents a la prerrogativa de gràcia
- Les referents als pressupostos de l'estat

Un cop la Mesa del congrés dels diputats rep la documentació requerida l'examina i en un termini de quinze dies es pronuncia per a determinar si ha sigut admesa. En cas de no admissió, la comissió promotora si ho considera pot recórrer al Tribunal Constitucional.

2.1.2 Recollida de firmes electròniques.

Un cop admesa la iniciativa, la Mesa del Congrés ho notificarà a la Junta Electoral Central que serà l'encarregada de garantir la regularitat del procés de recollida de firmes. La Junta Electoral Central comunicarà l'admissió de la proposició a la comissió promotora per a que aquesta iniciï el procés de recollida de firmes.

El procés de recollida de firmes finalitza amb l'entrega per part de la comissió promotora de les firmes recollides a la Junta Electoral Central. Si en el termini màxim de 9 mesos no es fan entrega de les firmes, la iniciativa caducarà. Només si s'acredita causa major, la Mesa del Congrés pot prorrogar en tres mesos addicionals la recollida de firmes.

2.1.3 Recompte de firmes i tramitació.

Un cop entregades les signatures a la Junta Electoral, aquesta les ha de validar i procedir a fer el recompte.

Les firmes que no compleixin amb els requisits establerts seran invalidades.

Un cop finalitzat el recompte, si el nombre de firmes vàlides supera el mínim exigit, la Junta Electoral enviarà certificació acreditativa amb el nombre total de firmes al Congrés dels diputats.

Un cop rebuda la notificació, la Mesa del congrés ordenarà la publicació de la proposició que haurà de ser inclosa a l'ordre del dia en el termini de sis mesos per a la seva consideració.

2.2 Estat de l'art.

L'ús de mecanismes d'autenticació electrònica, és una tendència que creix a gran velocitat al món.

A Espanya, el 26 de maig del 2006 va sortir publicada la llei orgànica 4/2006 de modificació de la llei orgànica 3/1984 reguladora de les iniciatives legislatives populars. Des d'aleshores, gràcies a aquesta modificació, s'accepten les firmes electròniques com a vàlides dintre del procés de recollida de firmes propi d'una iniciativa popular.

Dintre de la mateixa iniciativa que va impulsar aquesta modificació, apareix al març del 2007 el primer DNI electrònic, essent des del 2008 l'únic DNI que es fa.

Tot i així, no és fins a l'any del 2010 que no apareix la iniciativa a favor del transvasament del Tajo-Segura, que amb l'ajuda de la universitat de Múrcia (UMU), va ser la primera Iniciativa popular en implementar un sistema de recollida de firmes electròniques mitjançant DNI electrònic.

Des d'aleshores han anat apareixent comptades plataformes que fan ús d'aquesta tecnologia per a la recollida de firmes d'iniciatives legislatives populars com per exemple:

Plataforma per a la defensa de la festa dels toros:

http://www.openilp.org/tau4/

Plataformes per a la creació de ILP i la seva signatura

http://www.mifirma.com/

http://www.iniciativalegislativapopular.es/

Actualment encara que es disposen mecanismes i plataformes per a la signatura electrònica d'iniciatives legislatives populars i ja s'han expedit més de 28 milions de DNI electrònics, la dificultat d'adquirir i usar un certificat digital i per altre banda la necessitat de lectors addicionals per l'ús del DNI electrònic fa que molts dels usuaris descartin aquesta tecnologia.

2.3 Anàlisi requisits aplicació.

2.3.1 Identificació dels usuaris.

Aquesta aplicació està dirigida a dos tipus d'usuari, encara que en podem distingir tres tipus diferent d'usuari sense comptar amb l'administrador.

Usuari observador:

Aquest és l'usuari que entra a la web simplement per a obtenir informació de les propostes vigents com les firmes recollides fins el moment.

Usuari signant:

Aquest és l'usuari que ha de poder triar i signar una iniciativa.

Usuari comissió promotora:

Aquest tipus d'usuari és el que ha de fer servir l'aplicació per a crear una nova iniciativa. De fet tot usuari ha de poder crear una nova iniciativa, i en el moment de fer-ho passarà automàticament a ser integrant de la comissió promotora de la iniciativa que ha creat. També és l'usuari encarregat de recollir les signatures per a entregar-les a la Junta Electoral Central un cop finalitzat el procés de recollida.

Tant l'usuari creador de propostes com l'usuari signant han de complir el requisit de ser major d'edat i estar inscrits al cens electoral.

2.3.2 Requisits funcionals.

A continuació veiem els requisits funcionals de l'aplicació per a cada usuari.

Usuari observador:

Visualitzar llistat de les propostes vigents.

Obtenir informació detalla d'una proposta en concret.

- Text articulat de la proposició de llei precedida per una exposició de motius.
- Relació dels membres de la comissió promotora de la iniciativa.
- Nombre total de firmes recollides fins al moment.
- Data inici recollida.
- Data termini per a la recollida.

Usuari signant

L'usuari signant ha de poder accedir a les mateixes funcions que l'usuari observador més d'altres de pròpies.

Firmar una iniciativa

- Firma amb DNI electrònic.
- Firma amb certificat digital.

Creació nova proposta

- Al crear una nova proposta, automàticament l'usuari passarà a ser Usuari comissió promotora de la iniciativa que ha creat però seguirà exercint com a usuari signant per a la resta de iniciatives

Usuari comissió promotora

L'usuari comissió promotora ha de poder accedir a les mateixes funcions que l'usuari signant més d'altres de pròpies.

Obtenir llistat de firmes de la iniciativa que ha creat per a entregar-les a la Junta Electoral Central.

2.3.3 Requisits de seguretat.

Algunes de les funcions esmentades anteriorment requereixen d'algunes comprovacions de seguretat per a poder garantir l'admissibilitat de les firmes recollides.

Autenticació dels usuaris.

Per aquelles funcions pròpies d'un usuari signant o d'un usuari comissió promotora cal autenticar els usuaris. Els usuaris poden autenticar-se mitjançant:

- DNI electrònic.
- Certificat digital instal·lat al navegador.

En el cas d'autenticació mitjançant certificat digital instal·lat al navegador, el certificat haurà d'estar entre els reconeguts per la "Administarción". Podem obtenir la llista d'aquests certificats de la seu electrònica de la INE *https://sede.ine.gob.es*

Addicionalment, el servidor haurà de comprovar la vigència del certificat, és a dir comprovar que no estigui ni caducat ni revocat.

Control usuaris.

A banda de que l'autenticació tingui èxit, el sistema haurà de comprovar addicionalment que l'usuari és major de edat i que està censat per a acceptar una petició de creació d'una nova iniciativa o signatura.

Control duplicitat signatures.

Durant el procés de signatura d'una iniciativa, després l'autenticació i control haurem de comprovar que l'usuari autenticat no havia signat prèviament. En el cas de trobar una signatura prèvia del mateix signant aquesta es desestimarà.

Segell de temps

A banda de tancar el procés de recollida de signatures un cop transcorregut el termini, s'haurà d'incorporar a la firma un segell de temps per tal de garantir el moment en que aquesta s'ha produït.

2.4 Casos d'ús.

El diagrama de casos d'ús ens serveix per a mostrar les funcions del sistema des del punt de vista de les seves interaccions.

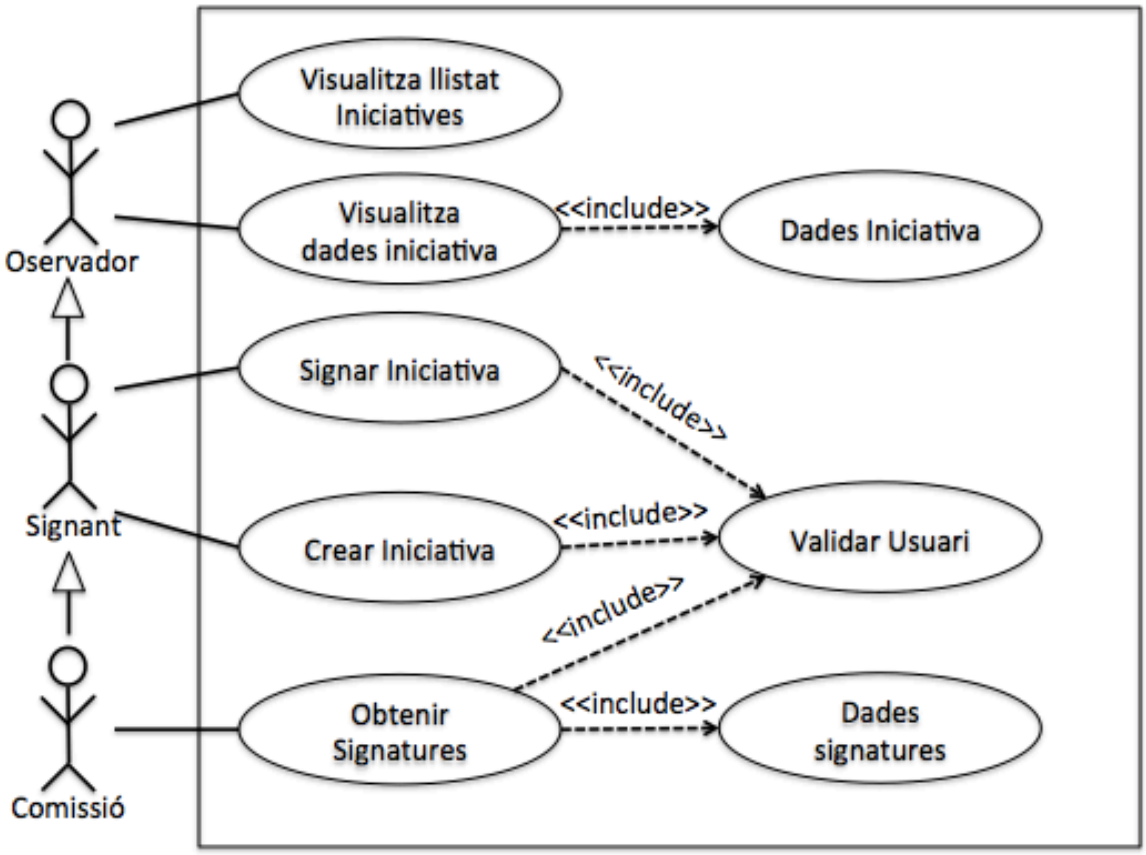

Figura 3.

Els usuaris ***observador*** només poden intervenir en els casos d'ús "***Visualitza llistat iniciatives***" i "***Visualitza dades iniciativa***". El cas d'ús "***Dades iniciativa***" representa l'accés a les dades no protegides d'una iniciativa; com que no es un cas d'ús que es pugui dur a terme de manera directa, sinó que es una funció dintre del cas d'ús "***Visualitza dades iniciativa***" la relació es d'inclusió.

Els usuaris ***signan***t són un cas d'especialització dels usuaris observador, el que vol dir que poden intervenir en els mateixos casos però també amb d'altres propis com són "***Signar iniciativa***" i "***Crear iniciativa***".

Els usuaris ***comissió*** són un cas d'especialització dels usuaris ***signan***t amb el cas d'us propi "***Obtenir Signatures***". El cas d'ús "***Dades signatura***" representa l'accés a les dades de les signatures.

El cas d'ús "***Validar Usuari***" representa l'autenticació i control dels usuaris de dins els casos d'ús "***Signar iniciativa***", "***Crear iniciativa***" i "***Obtenir Signatures***".

3. Fase de planificació

3.1 Requisits a nivell de hardware.

Encara que seria possible implementar la plataforma amb equips amb prestacions inferiors es recomana com a mínim l'equipament següent:

- Servidor Web.
    - Procesador Intel Dual Core 1.8 Ghz, AMD Dual Core 1.8 Ghz o superior.
    - Memòria RAM de 1 GB (800 Mhz).
    - Disco Dur amb 8 GB de memoria disponible.
        - Hem de tenir en compte que aquests són els mínims recomanats per al bon funcionament de la web.
        - Depenent del nombre de iniciatives i signatures , les necessitats d'espai poden variar molt.

- Router
    - IP fixe per a la connexió al nostre sistema des de l'exterior
    - Apertura dels ports 80(HTTP) i 443 (HTTPS) i redireccionament cap a la nostra web.
    - Implementació sistema tallafocs.
        - Addicionalment, si es tenen altres equips dins de la xarxa és recomanable implementar un segon tallafocs ja sigui a nivell de software o de hardware per tal de implementar una DMZ on situar la web.

Per a la implementació i proves del projecte es farà servir el següent equipament a nivell de hardware:

- Ordinador portàtil MacBook
    - Processador Intel Core 2 duo a 2,26 GHz
    - 4 GB 1067MHz DDR3
    - Sistema operatiu MAC OSX 10.7.3 Lion

- Router Linksys WRT54GS
    - IP fixe per a la connexió al nostre sistema des de l'exterior
    - Apertura dels ports 80(HTTP) i 443 (HTTPS) i redireccionament cap a la nostra web

- Ordinador portàtil Sony VAIO (Client)
    - Processador Intel Core duo a 2,20 GHz
    - 2 GB RAM
    - Sistema operatiu Windows Vista Home Premium

3.2 Requisits a nivell de software.

Per a la elecció del software s'ha donat especial importància a l'ús de software lliure pels motius següents:

- Software totalment gratuït.
- Llibertat d'ús i redistribució.
- Independència tecnològica.
- Sistemes sense portes de darrera i més segurs.
- Correcció mes ràpida i eficient d'errades.
- Mètodes simples i unificats de gestió del software.

En concret el software que es farà servir és el següent:

- Oracle VM Virtual box per a la virtualització del servidor web.
- Sistema operatiu xubuntu 11.10.
- Servidor web Apache2.
- Gestor base de dades MySQL.
- PHP5.
- Phpmyadmin.
- Bluefish per a l'edició HTML, CSS, SQL, PHP i JavaScript.
- GanttProject per a la creació de diagrames de Gantt.
- OpenOffice per a l'edició de la memòria.

4. Fase de disseny

4.1 Disseny de la base de dades

4.1.1 Disseny conceptual

Per al disseny conceptual hem adoptat l'enfocament del model entitat-interrelació (Entity-Relationship), que abreviarem amb la sigla ER.

Esquema ER:

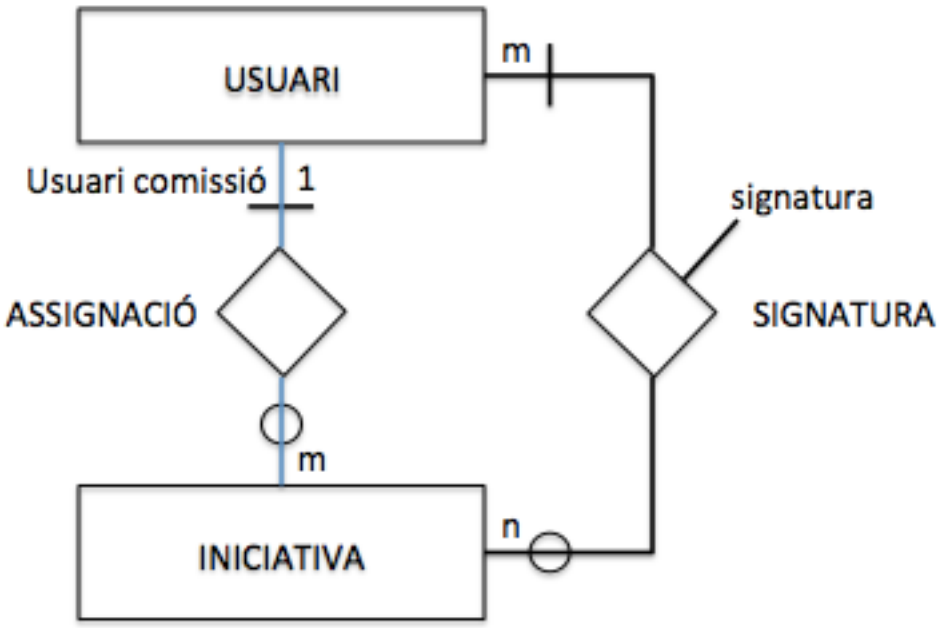

Figura 4.

Entre les entitats **USUARI** i l**NICIATIVA** hi ha la interrelació **ASSIGNACIÓ** per a indicar l'usuari comissió promotora que ha creat la iniciativa.

Per altra banda, entre aquestes mateixes entitats també tenim la interrelació **SIGNATURA** per a indicar quines iniciatives han signat els usuaris. Aquesta interrelació té l'atribut signatura que fa referencia a la signatura digital.

4.1.2 Disseny lògic

Per al disseny lògic partirem del disseny conceptual expressat mitjançant el model ER per a transformar-lo en una estructura de dades del model relacional.

La transformació de l'esquema ER es transforma en:

USUARI (DNI, nom, cognom1, cognom2, data_naixement, email)

INICIATIVA (codi_iniciativa, títol, descripció, data_inici, data_fi, DNI_comissio, nombre_signatures)

On DNI_comissio es clau forana de **USUARI.**

SIGNATURA (DNI,_usuari, codi_iniciativa, signatura)

On DNI_usuari es clau forana de **USUARI**

i codi_iniciativa es clau forana de **INICIATIVA.**

4.2 Disseny de la interfície gràfica.

Per al disseny de la interfície gràfica ens centrarem en dos aspectes fonamentals com són la usabilitat i l'accessibilitat.

Usabilitat:

Volem una web intuïtiva i de fàcil ús. Per a aconseguir-ho farem servir els següents criteris:

- Evitar tot allò que no sigui imprescindible per al bon funcionament d'aquesta i que no suposi una ajuda al usuari.
    - No mostrar informació que l'usuari no necessita saber.

- Evitar possibles errors al ingressar dades.
    - Facilitar la metodologia per a l'ingrés de dades susceptibles a errors de format. Un bon exemple d'això pot ser l'ingrés de dates. Per a aconseguir-ho podem fer servir desplegables amb les opcions de dia, mes i any.
    - Gestionar els errors de manera que proporcionin als usuaris la informació necessària per a solventar-los alhora que evitem l'entrada de dades errònies al sistema. Un bon exemple d'això pot ser el control i avís davant l'enviament de formularis amb camps obligatoris buits com per exemple el títol de una proposta durant la seva creació.

Accessibilitat:

Per al disseny de la interfície gràfica, dedicarem un interès especial a que aquesta sigui accessible i còmode de visualitzar des de un ventall el més ampli possible de navegadors, sistemes operatius i tipus de dispositiu tals com ordinadors personals, tablets i smartphones. Per a aconseguir-ho farem servir els següents criteris:

- Dimensionar la amplada del contingut gràfic
    - Garantir que al carregar la pàgina des dels diferents dispositius tot el contingut hi cap dintre de la seva amplada per a evitar desplaçaments laterals innecessaris i sovint molestos.

- Creació d'un menú principal accessible des d'arreu.
    - Facilitar la navegació per tal de trobar el que busquem ràpidament.
    - Hem definit un menú principal amb tres opcions:
        - INICI.
            - Pantalla inicial informativa

        - VEURE INICIATIVES.
            - Pantalla d'accés a les iniciatives actives per a la seva visualització, signatura o obtenció de signatures per part del promotor.

        - CREA NOVA INICIATIVA
            - Pantalla per a la creació d'una nova iniciativa

- Evitar finestres emergents.
    - Facilitar la navegació sobretot des de smartphones on la navegació amb varies finestres és més complicada.
    - Evitar diferències en el format d'aquestes finestres davant diferents navegadors, SO i dispositius.

- Evitar en mida del possible l'ingrés de dades des de teclat.
    - Tenir en compte les dificultats per a escriure text des de alguns dispositius com tablets o sobretot smartphones.
    - Optar per desplegables a l'hora d'entrar dades amb un ventall reduït de possibilitats com per exemple els camps d'ingrés de dates.

- Definir tipus de lletra Standard gran.
    - Facilitar la lectura per part del ventall més ampli d'usuari i des de qualsevol dispositiu.

El disseny a nivell estètic queda fora l'abast d'aquest projecte.

4.3 Disseny del flux de l'aplicació.

Per al disseny del flux de l'aplicació, ens centrarem en els diferents usuaris i en els possibles casos d'ús prèviament definits.

L'objectiu és el de definir per a cadascuna de les funcionalitats que la aplicació ha de oferir quins són els passos que l'usuari haurà de seguir i quin és el ordre d'execució.

Una eina molt útil per a visualitzar el flux de l'aplicació són els diagrames de seqüència. Així doncs farem els diagrames de seqüencia per a les funcions "Crear nova iniciativa", "Signar" i "Obtenir signatures" les quals engloben totes les funcions.

Crea nova iniciativa:

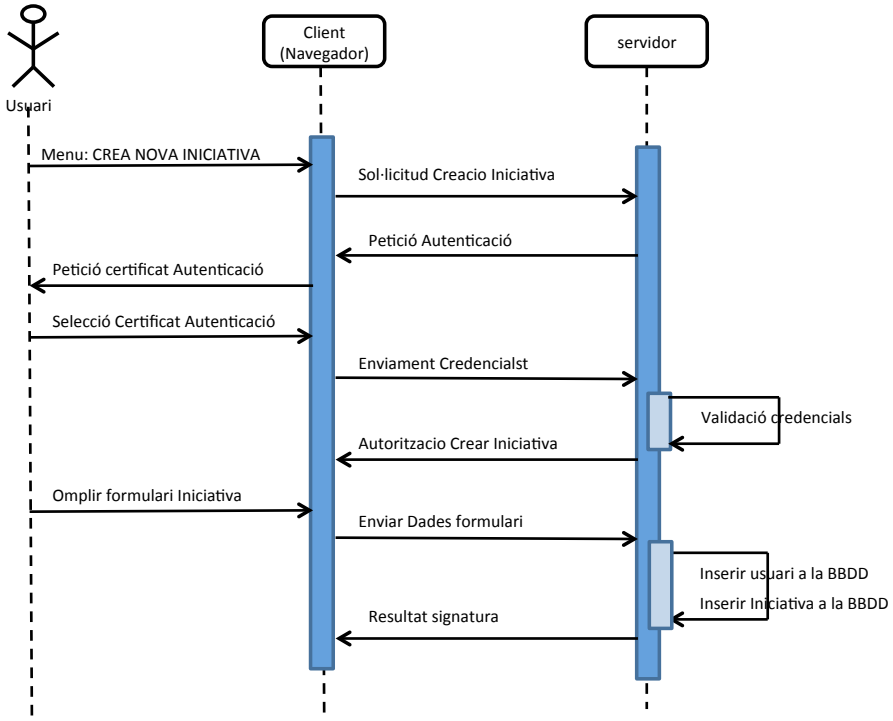

Figura 5.

Signar:

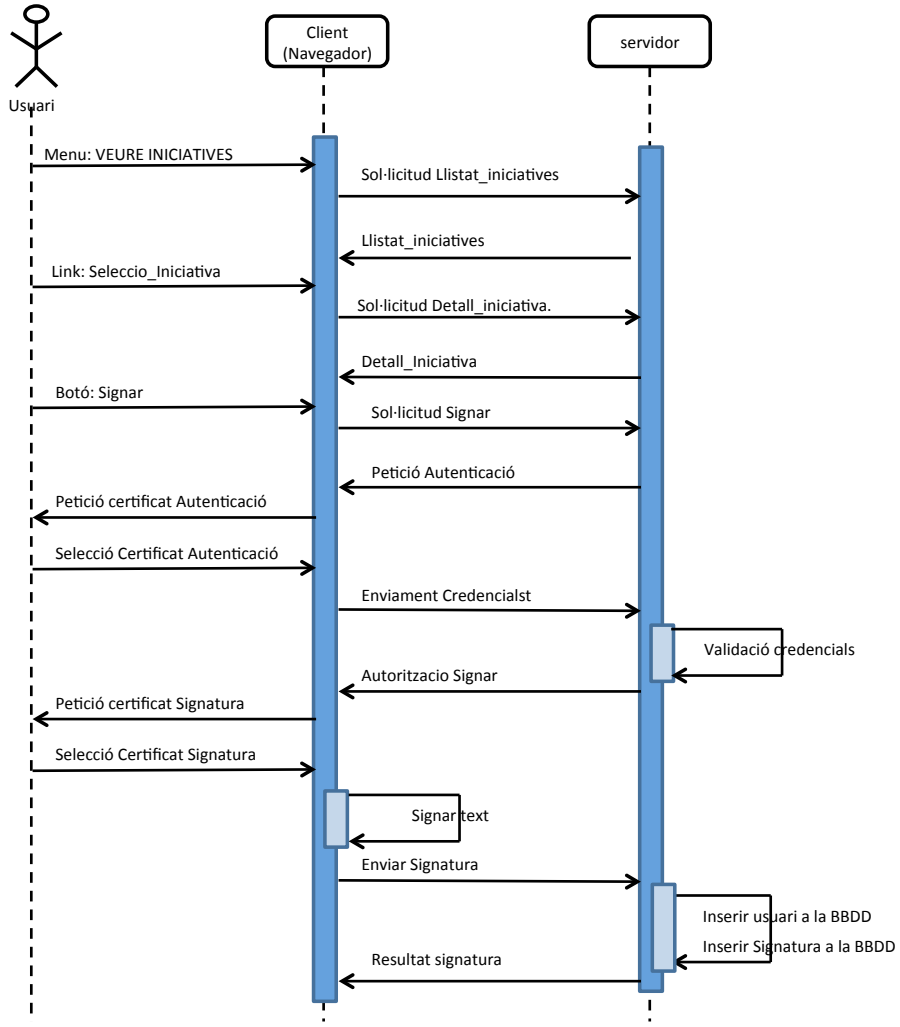

Figura 6.

Obtenir signatures:

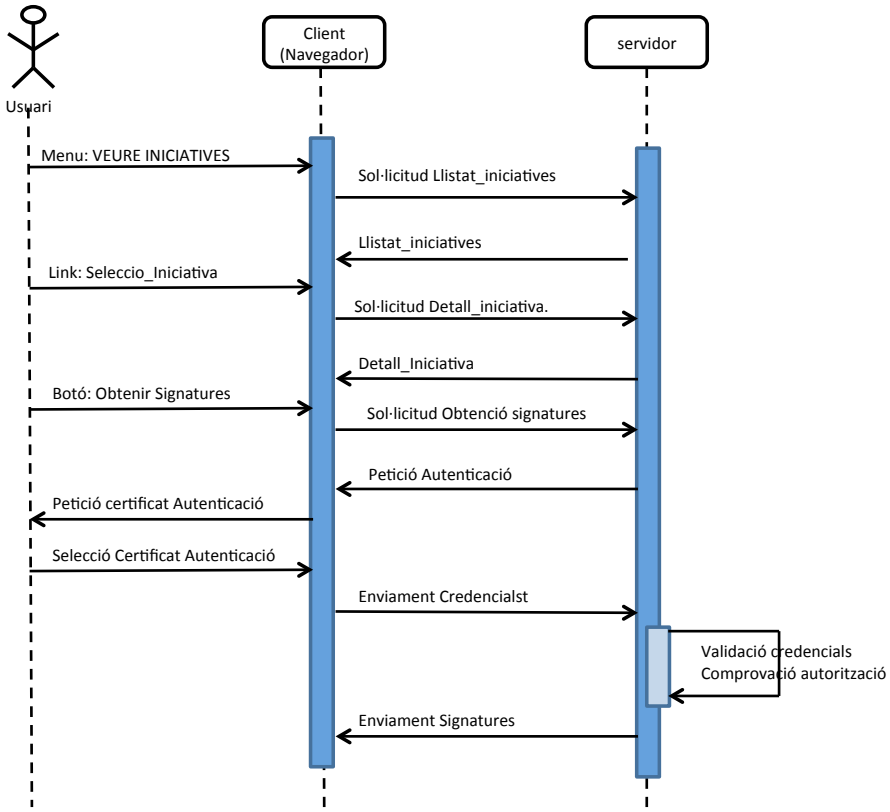

Figura 7.

5. Fase de programació

5.1. Preparació de l'entorn de treball.

Per a la implementació del nostre servidor hem triat una solució lliure coneguda com a LAMP, que fa referència a les primeres lletres de:

Linux (Sistema Operatiu)
Apache (Servidor HTTP)
MySQL (Base de dades)
PHP (Llenguatge de programació).

Instal·lació sistema operatiu:

Com a sistema operatiu hem triat la distribució xubuntu 11.10; la qual instal·larem en una màquina virtual que hem creat amb VirualBox de Oracle.

A aquest màquina redirigim totes les peticions a la adreça ip pública 80.64.39.210 per tal de fer-la visible des de l'exterior.

Per a la instal·lació dels diferents components haurem d'executar des d'un terminal les comandes següents:

Instal·lació servidor i client MySQL:

$sudo apt-get install mysql-server mysql-client

Instal·lació Apache2

$sudo apt-get install apache2

Instal·lació PHP:

$sudo apt-get install php5 libapache2-mod-php5

Instal·lació mòdul php5-mysql:

El mòdul php5-mysql ens serveix per obtenir support mysql des de php.

$sudo aptget install php5-mysql

Instal·lació phpmyadmin:

Phpmyadmin és una interfície web que ens permetrà gestionar la nostra base de dades MySQL.

$sudo apt-get install phpmyadmin

Un cop fet això, per tal que els canvi sorgeixin efecte reiniciem el nostre servidor apache amb la comanda:

$/etc/init.d/apache2 restart

Instal·lació Bluefish:

Bluefish és un editor de text de programari lliure que suporta el desenvolupament en HTML, PHP, CSS, JAVASCRIPT, SQL, XML, ... el qual ens servirà com a editor universal per tot el que hem de implementar en aquest projecte.

$sudo apt-get install Bluefish

Finalment, per a comprovar la correcta instal·lació del php5 i per a obtenir detalls sobre aquesta instal·lació, crearem amb l'ajuda del editor Bluefish un fitxer que anomenarem info.php.

Creació fitxer info.php:

Obrim editor Bluefish.

$sudo bluefish

Creem nou fitxer info.php a la carpeta /var/www amb el contingut següent:

```
<?php
        phpinfo();
?>
```

Un cop fet això, accedim des de qualsevol navegador a l'arxiu que acabem de crear i podrem visualitzar la informació relativa al php que acabem d'instal·lar com ara la versió o els mòduls instal·lats.

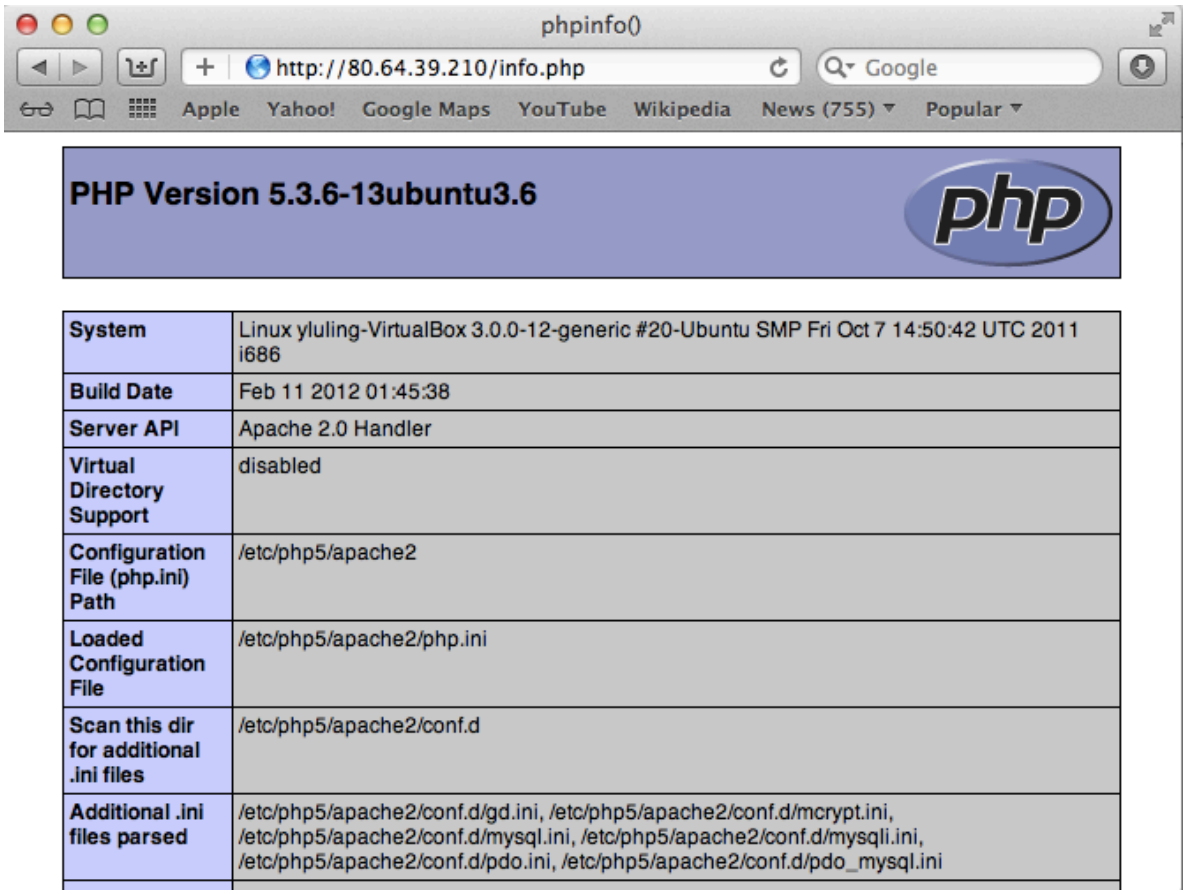

Figura 8.

5.2. Creació base de dades.

Un cop instal·lada la interfície phpmyadmin, la utilitzarem per crear la nostra base de dades sense haver de programar amb sql.

Així doncs, creem la base de dades que anomenarem "ilp" i, dintre d'aquesta, crearem les tres taules següents:

Iniciativa:

Estructura de la taula iniciativa.

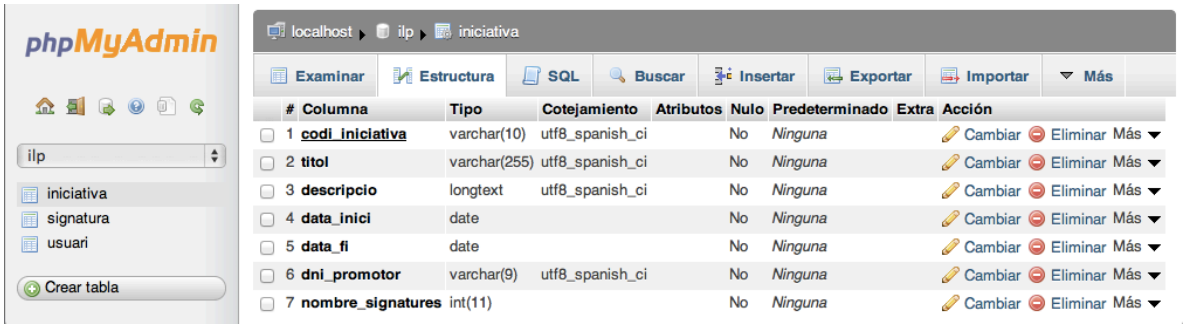

Figura 9.

Usuari:

Estructura de la taula usuari.

Figura 10.

Signatura:

Estructura de la taula signatura.

Figura 11.

Observem que l'atribut data_naixement de la taula usuari és l'únic atribut en el que permetem un valor nul. Això és així degut a que no tots els certificats contenen aquesta informació.

Per tal de mantenir actualitzat l'atribut nombre_signatures de la taula iniciativa hem creat un disparador que en el moment d'inserir una signatura a la base de dades, ens incrementi en 1 el nombre de signatures. D'aquesta manera podrem obtenir el nombre de signatures duna iniciativa sense necessitat de rastrejar tota la base de dades.

```
CREATE TRIGGER suma_signatura
AFTER INSERT ON signatura
For each row
BEGIN
UPDATE 'iniciativa' SET 'nombre_signatures' = nombre_signatures +1
WHERE codi_iniciativa = NEW.codi_iniciativa;
END;
```

5.3. Implementació servidor segur HTTPS

5.3.1. Creació certificat Autoritat de certificació (CA)

Per a la configuració del servidor Apache en mode segur, primer, necessitem disposar d'un certificat per al servidor.
En el nostre cas, com que inicialment no disposem de cap certificat digital i degut a que els únics que ens poden atorgar un certificat digital és una autoritat de certificació (CA), es decideix per a la elaboració del present projecte crear una autoritat de certificació pròpia i auto signar els nostres propis certificats.

El procés de creació de una autoritat de certificació pròpia consta de tres passos:

1- **Creació de la clau privada de la CA**

$openssl genrsa –des3 –out clau_privada_CA.key 2048

A l'executar la comanda anterior es crea el fitxer clau_privada_CA.key amb la clau privada de la nostra CA. El procés d'execució ens demanarà establir un passphrase. Farem servir el passphrase "nick6810".

2- **Creació de la sol·licitud de certificat de CA**

$openssl req –new –key clau_privada_CA.key –out solicitud_CA.csr

A continuació, omplim les dades de la CA que se'ns va demanant. Finalment, es crearà el fitxer sol·licitud_CA.csr

3- **Emissió del certificat auto signat per a la CA**

$openssl x509 –days 3650 –signkey clau_privada_CA.key –in sol·licitud_CA.csr –req –out certificat_CA.crt

A l'executar aquesta comanda el que fem és emetre el certificat certificat_CA.crt amb format x509 i validesa per 10 anys. En aquest cas el que hem fet és auto signar la nostra pròpia sol·licitud.

5.3.2. Creació certificat Servidor Web.

Un cop ja tenim un certificat per a la nostre CA, el que farem ara és crear un certificat per al nostre servidor signat per la CA que acabem de crear. Els passos a seguir per a la elaboració d'aquest certificat són molt similars als de creació del certificat de la CA. Els passos a seguir són:

1- **Creació de la clau privada del servidor**

$openssl genrsa –out clau_privada_servidor.key 2048

Es crea el fitxer clau_privada_servidor.key.

2- **Creació de la sol·licitud de certificat per al servidor**

$openssl req –new –key clau_privada_servidor.key –out solicitud_servidor.csr

A continuació omplim les dades del servidor com hem fet anteriorment amb la CA. Finalment es crearà el fitxer sol·licitud_servidor.csr.

3- **Emissió del certificat per al servidor.**

$openssl x509 –days 3650 –CA certificat_CA.crt –Cakey clau_privada_CA.key –set_serial 01 –in sol·licitud_servidor.csr –req –out certificat_servidor.crt

A l'executar aquesta comanda el que fem és emetre el certificat certificat_servidor.crt amb format x509 i validesa per 10 anys. En aquest cas el que hem fet és signar amb el certificat i clau de la CA que hem creat anteriorment la sol·licitud emesa en el punt anterior per el servidor.

Val a dir que en una situació normal el que faríem és enviar la nostre sol·licitud a una CA la qual ens tornaria la mateixa signada amb el seu certificat i clau privada prèvia confirmació de que som qui diem ser.

5.3.3. Configuració servidor Apache.

Un cop ja tenim un certificat per al servidor ja podem començar a configurar el nostre servidor per a establir connexions segures mitjançant HTTPS.
El primer que farem serà crear un directori dintre el directori www amb el nom zona_segura el qual li donarem drets de lectura i escriptura. Acte seguit, el que farem serà habilitar el mòdul ssl al nostre servidor amb la comanda:

$sudo a2enmod ssl

Un cop fet això, haurem de modificar el fitxer /etc/apache2/sites-enabled/000-default i afegir al final de tot el següent:

```
<Directory "/var/www/zona_segura">
        SSLRequireSSL
</Directory>


NameVirtualHost *:443


<VirtualHost *:443>
        SSLEngine On
        SSLOptions +StdEnvVars +ExportCertData
        SSLCertificateFile /etc/apache2/ssl/certificat_servidor.crt
        SSLCertificateKeyFile /etc/apache2/ssl/clau_privada_servidor.key
        DocumentRoot /var/www/zona_segura
        ErrorLog /var/log/apache2/error.log
        LogLevel warn
</VirtualHost>
```

Amb les instruccions contingudes entre les etiquetes <Directory> el que fem es establir el mode segur SSL com l'únic mode d'accés al directori zona_segura que hem creat anteriorment.

La instrucció: ***NameVirtualHost *:443*** ens serveix per a dir al nostre servidor que accepti qualsevol ip que faci peticions per el port 443 que és el port reservat per a connexions segures HTTPS.

Les instruccions contingudes entre les etiquetes <VirtualHost> són les que s'aplicaran al VirtualHost per a peticions sobre el port 443.

- ***SSLEngine On***
  Habilitem el motor SSL del servidor.

- ***SSLOptions + StdEnvVars + ExportCertData.***
  Habilitem les opcions StdEnvVars i ExportCertData amb les quals ens permetran accedir des de php més endavant a la informació continguda a les variables d'entorn del servidor i en els certificats tant del client com del propi servidor.

- ***SSLCertificateFile /etc/apache2/ssl/certificat_servidor.crt***
  Especifiquem la ruta absoluta fins on hem desat el certificat del servidor.

- ***SSLCertificateKeyFile /etc/apache2/ssl/clau_privada_servidor.key***
  Especifiquem la ruta absoluta fins on hem desat la clau privada del servidor

- ***DocumentRoot /var/www/zona_segura***
  Especifiquem la ruta absoluta del que considerarem l'arrel d'aquest servidor virtual en mode segur.

- ***ErrorLog /var/log/apache2/error.log***
  Especifiquem ruta absoluta fins l'arxiu on desarem els informes dels errors que es puguin produir.

- ***LogLevel warn***
  Establim les advertències com a errades mínimes a enregistrar en el nostre arxiu d'errors.

Un cop desats els canvis, reiniciem apache per a que els canvis tinguin efecte amb la comanda:

$/etc/init.d/apache2 restart

Fins ara el que hem fet és configurar el nostre servidor per a que treballi en mode segur. Això vol dir que disposem d'un certificat que ens identifica com a servidor i que la informació entre client i servidor circula encriptada mitjançant una clau simètrica.
Aquesta configuració ens permet evitar que algú altre suplanti la nostre identitat.

5.4. Implementació servidor segur amb certificat de client.

Ara farem un pas més i configurarem el nostre servidor per a que exigeixi als clients que disposin d'un certificat de client per a accedir a un directori determinat.

Els certificats de client que acceptarem seran els certificats inclosos al DNI electrònic signats per la DIRECCION GENERAL DE POLICIA, els certificats FNMT Clase 2 signats per la FNMT (Fábrica Nacional de Moneda y Timbre) i els certificats signats per la nostre CA que hem creat anteriorment.

5.4.1. Obtenció certificats arrel

El primer que hem de fer és obtenir els certificats arrel del DNIe i FNMT. Per a fer-ho els descarreguem dels enllaços següents:

ACRAIZ-SHA1.crt

http://www.dnielectronico.es/seccion_integradores/certs.html

FNMTClase2CA.cer

http://www.cert.fnmt.es/content/pages_std/certificados/FNMTClase2CA.cer

Els certificats que acabem de descarregar estan en format DER i el servidor Apache requereix que els certificats arrel estiguin en format PEM.
Transformem de format DER a format PEM amb les instruccions següents:

$sudo openssl x509 -in ACRAIZ-SHA1.crt -inform DER -out ArrelDNIe.crt -outform PEM

$sudo openssl x509 -in FNMTClase2CA.cer -inform DER -out ArrelFNMT.crt -outform PEM

Ara ja tenim els tres certificats arrels que volíem en format PEM. A continuació haurem de ajuntar aquests certificats en un únic fitxer.

Executem la comanda:

$sudo cat ArrelDNIe ArrelFNMT certificat_CA > certificats.crt

5.4.2. Configuració servidor Apache

Un cop ja tenim tots tres certificats concatenats en un únic fitxer, haurem de modificar el fitxer /etc/apache2/sites-enabled/000-default i afegir el següent: (marcat en blau)

```
<VirtualHost *:443>
        SSLEngine On
        SSLOptions +StdEnvVars +ExportCertData
        SSLCertificateFile /etc/apache2/ssl/certificat_servidor.crt
        SSLCertificateKeyFile /etc/apache2/ssl/clau_privada_servidor.key
        SSLCACertificateFile "/etc/apache2/ssl/certificats.crt"
        DocumentRoot /var/www/zona_segura
        ErrorLog /var/log/apache2/error.log
        LogLevel warn

        <Directory "/var/www/zona_segura/autenticat">
                SSLVerifyClient require
                SSLVerifyDepth 2
                 SSLRequire (%{SSL_CLIENT_V_REMAIN} >= "0")
        </Directory>
</VirtualHost>
```

Les instruccions contingudes entre les etiquetes <VirtualHost> són les que s'aplicaran al VirtualHost per a peticions sobre el port 443.

- ***SSLCACertificateFile "/etc/apache2/ssl/certificats.crt"***
  Especifiquem la ruta absoluta fins on hem desat els certificats arrel de les CA autoritzades.

Les instruccions contingudes entre les etiquetes <Directory> especifiquen el directori restringit i les condicions d'accés.

- ***SSLVerifyClient require***
  Especifiquem a apache que s'ha d'exigir un dels certificats admesos per a accedir a aquest directori.

- ***SSLVerifyDepth 2***
  Especifiquem que per a validar el certificat d'usuari farem servir si cal un segon nivell de CA subordinada. Aquesta instrucció és imprescindible per als certificats inclosos al DNI-e.

- ***SSLRequire (%{SSL_CLIENT_V_REMAIN} >= "0")***
  Especifiquem que no s'accepten certificats caducats.

5.5. Implementació autenticació amb PHP.

A banda de validar el certificat de client, necessitarem conèixer algunes dades addicionals dels usuaris per tal de garantir els requisits funcionals i de seguretat que hem establert anteriorment.

En concret volem conèixer les dades dels clients següent:

NIF, Nom, primer cognom, segon cognom i data naixement.

Així doncs, creem un fitxer que hem anomenat autenticació.php al qual cridarem sempre que es vulgui prendre alguna acció en el que sigui necessària fer algun tipus de comprovació de les dades del usuari.

Aquest fitxer únicament té com a finalitat extreure la informació del certificat de client per a més endavant aquesta pugui ser analitzada.

Analitzem el contingut del fitxer "autenticacio.php:

```
<?php

$dades = openssl_x509_parse($_SERVER['SSL_CLIENT_CERT']);

if ($dades['issuer']['O']=="FNMT"){

      $z=explode('=',str_replace
      ("/",'=',$dades['extensions']['subjectAltName']));

      $nom = $z[8];

      $cognom1 = $z[6];

      $cognom2 = $z[4];

      $dni = $z[2];
```

```
        $menor_edat = false;

        echo "<p class='titol'>Autenticació satisfactòria amb certificat
        FNMT clase 2</p>";

        echo "<p class='autenticacio'>Nom: ".$nom."<br />Cognoms:
        ".$cognom1." ".$cognom2."<br />DNI: ".$dni."<br /></p>";

    }


    if ($dades['issuer']['OU']=="DNIE"){

        $nom = $dades['subject']['GN'];

        $cognom1 = $dades ['subject']['SN'];

        $cognoms =explode(',',str_replace
        ("(AUTENTICACIÓN)",'',$dades['subject']['CN']));

        $cognom2 = str_replace($cognom1." ",'',$cognoms[0]);
        $dni = $dades['subject']['serialNumber'];

        $data_naixement=substr($dades['extensions']
        ['subjectDirectoryAttributes'],-15,8);

        $any_naixement = substr($data_naixement,0,4);

        $mes_naixement = substr($data_naixement,4,2);

        $dia_naixement = substr($data_naixement,6,2);

        $data_naixement = date($any_naixement."-".$mes_naixement."-
        ".$dia_naixement);

        echo "<p class='titol'>Autenticació satisfactòria amb DNI-e</p>";


        echo "<p class='autenticacio'>Nom: ".$nom."<br />Cognoms:
        ".$cognom1." ".$cognom2."<br />Data Naixement:
        ".$dia_naixement."/".$mes_naixement."/".$any_naixement."<br />DNI:
        ".$dni."<br /></p>";

        $data_actual = date("d-m-Y");

        $any_naixement = $any_naixement +18;

        $data_major_edad = date($dia_naixement.'-'.$mes_naixement.'-
        '.$any_naixement);

        $menor_edat =    strtotime($data_major_edad) >
        strtotime($data_actual);

    }
```

```
if ($dades['issuer']['O']=="TFC"){
      $info =explode(' ',$dades['subject']['CN']);

      $nom = $info[0];

      $cognom1 = $info[1];

      $cognom2 = $info[2];

      $dni = $info[3];

      $menor_edat = false;

      echo "<p class='titol'>Autenticació satisfactòria amb certificat
      autosignat</p>";

      echo "<p class='autenticacio'>Nom: ".$nom."<br />Cognoms:
      ".$cognom1." ".$cognom2."<br />DNI: ".$dni."<br /></p>";

}

?>
```

Observem la primera instrucció.

```
$dades =openssl_x509_parse($_SERVER['SSL_CLIENT_CERT']);
```

Aquesta instrucció és la instrucció clau que ens permet obtenir dintre de la variable que hem anomenat `$dades` el contingut del certificat del client en forma de Array.

Un cop fet això, i degut a que cada certificat ordena les dades de forma diferent, analitzem si el certificat en qüestió és un certificat atorgat per la FNMT, un certificat auto signat o és un DNI-e. Així doncs, depenent de l'emissor del certificat ja podrem extreure les dades que necessitem tot i tenint en compte la seva ordenació.

5.5.1. Restriccions d'accés

Signatura de una ILP

Per a que una signatura sigui vàlida per la JEC cal, a més a més del certificat digital, que el signant sigui major d'edat.

Així doncs, per tal de assegurar al màxim que les signatures recollides seran vàlides farem una comprovació de majoria d'edat abans de iniciar el procés de signatura i no permetrem l'accés a menors d'edat tot mostrant un avís per pantalla.
Aquesta comprovació serà només possible si el client utilitza el DNI-e, ja que els certificat de la FNMT no disposa d'aquesta dada. Aquest fet no ens suposa cap problema ja que per a sol·licitar un certificat a la FNMT cal ser major d'edat o en tot cas estar emancipat.

Creació d'una nova ILP

Encara que no hi ha establert cap requisit alhora de qui crea la nova iniciativa. En el nostre cas hem considerat adient el comprovar la majoria d'edat de la mateixa manera com ho hem fet en el procés de signatura.

Accés promotor.

L'accés al promotor permet descarregar les signatures fetes fins el moment comprimides en un únic fitxer .zip per a la seva posterior entrega a la JEC.
Per a accedir a aquesta àrea comprovarem addicionalment a la majoria d'edat que l'usuari que està fent la petició d'accés a aquesta àrea és el mateix que va crear la iniciativa

5.6. Implementació procés de signatura amb @firma.

Per a la implementació del procés de signatura es decideix utilitzar el MiniApplet de @firma desenvolupat pel "Ministerio de Hacienda y Administraciones Públicas" ja que ha sigut desenvolupat per a la administració pública i es programari lliure sota llicència GNU.
Aquesta eina de signatura electrònica funciona en forma d'applet de Java integrat a la nostra web mitjançant Javascript.
El MiniApplet fa ús dels certificats digitals X.509v3 i de les seves claus que es trobin instal·lats en el magatzem de claus i certificats del sistema operatiu o del navegador Web, així com dels que estiguin en altres dispositius configurats a tal efecte com és el cas dels lectors de DNIe.
El MiniApplet és una aplicació que s'executa a la màquina del client. Això és així per a evitar que la clau privada associada a un certificat circuli per la xarxa. De fet el que circula per la xarxa és el text a signar que envia el servidor al client, i el text signat de tornada del client al servidor.

5.6.1. Integració MiniApplet @firma a la nostre web

Per a la integració del MiniApplet de @firma, primerament necessitarem descarregar l'applet en format jar miniapplet-full.jar i el Javascript miniapplet-full.js des de la web de forja-ctt:

http://forja-ctt.administracionelectronica.gob.es/web/clienteafirma

Un cop fet això els passos a seguir per a integrar el miniapplet @firma a la nostra web són els següents:

1- publiquem els fitxers miniapplet-full.jar i miniapplet-full.js via web situant-los al directori …/www/zona_segura/autenticat.

2- Creem fitxer miniapplet-full.php des de el que s'iniciarà el procés de signatura.

3- Dintre de miniapplet-full.php haurem de importar les biblioteques següents:
   a. Biblioteca JavaScript Oracle Java Deployment Toolkit (deployjava.js) situada a http://www.java.com/js/deployJava.js
   b. Biblioteca JavaScript del MiniApplet (miniapplet-full.js) situada al directori . .../www/zona_segura/autenticat del nostre servidor.
   c. Biblioteca file_exists per a comprovar l'existència del fitxer a signar i així poder gestionar possibles errors.
   d. Biblioteca file_get_contents que ens serà útil a l'hora de recollir les dades en forma de text del fitxer a signar.

4- Es crea funció JavaScript doSign() dintre de miniapplet-full.php que serà la encarregada de llegir el fitxer a signar, capturar el text, fer conversió de dades, cridar a la funció sign de miniapplet.js per a iniciar el procés de signatura i recollir signatura per a juntament amb les dades del usuari enviar-les a un altre fitxer signar2.php que serà l'encarregat de inserir les dades a la nostra BBDD.

5- Es crea funció JavaScript showLog(error) que serà l'encarregada de mostrar els errors durant el procés de signatura per pantalla.

6- Es crea formulari amb dades usuari i es crida la funció doSign()

A continuació veiem el contingut de la funció doSign().:

```
function doSign() {
     try {

            var not_exist = " No s'ha trobat el fitxer a signar";
            var exist = file_exists('xml/text_xml.xml');

            if (exist == true){
                  var text = file_get_contents ('xml/text_xml.xml');
                  var text = "<pre>" + text + "</pre>";
                  var dataB64 = getBase64FromText(text);

      var signaturaB64 = sign( dataB64, "SHA256withRSA", "XAdES", null);

      saveDataToFile(signaturaB64,"Desar Signatura", null, null, null);

      signatura = getTextFromBase64(signaturaB64, charset = "utf-8");

                  document.forms[0].signatura.value = signatura;
                  document.formulario.submit();

            } else {
                  document.write(not_exist);
            }

      } catch(e) {

            showLog(getErrorMessage());

      }

}
```

6. Fase de proves

6.1. Preparació entorn de proves.

Per a la preparació de l'entorn de proves farem servir un ordinador Sony Vaio amb Windows Vista Home Premium.

6.1.1. Instal·lació DNI-e.

Seguint les especificacions del fabricant del lector del DNI-e, inserim el CD de instal·lació i executem fitxer instal·lació.

Automàticament s'instal·len els divers del lector del DNI-e i el servei Criptogràfic CSP(Cryphtographic Service Provider).

6.1.2. Certificat digital

Per a preparar el client amb un certificat digital, primerament haurem de crear un certificat vàlid seguint els passos següents:

1- **Creació de la clau privada del client**

   $openssl genrsa –out yago_privada.key 2048

   Es crea el fitxer yago_privada.key.

2- **Creació de la sol·licitud de certificat per al client**

   $openssl req –new –key yago_privada.key –out yago_solicitud.csr

   A continuació introduïm les dades personals. Finalment es crearà el fitxer yago_solicitud.csr.

3- Emissió del certificat per al client.

$openssl x509 –days 3650 –CA certificat_CA.crt –Cakey clau_privada_CA.key –CAcreateserial –sha1 –in yago_solicitud.csr –req –out certificat_yago.pem

A l'executar aquesta comanda el que fem és emetre el certificat certificat_yago.pem amb format x509 i validesa per 10 anys. En aquest cas el que hem fet és signar amb el certificat i clau de la CA que hem creat anteriorment la sol·licitud emesa en el punt anterior.

4- Fem conversió certificat a format pkcs12

$openssl pkcs12 –export –in certificat_yago.pem –inkey yago_privada.key –out pkcs12_cert_yago.pfx

5- Importem certificat al navegador Explorer

Anem a Opciones de Internet > Contenido > Certificados > Importar
S'engegarà assistent que ens guia en el process de importació.

6.2. Proves amb DNI-e

6.2.1. Crear nova iniciativa amb DNI-e.

Seguim els passos següents:

1- Des de un navegador ens adrecem a la URL 80.64.39.210.
- L'aplicació ens redirecciona a https://80.64.39.210/index.php

2- Cliquem sobre la pestanya "CREA NOVA INICIATIVA"
- L'aplicació ens demanarà un certificat.
- Triem el certificat d'autenticació del DNI-e.
- Entrem el password.
- La aplicació ens mostrarà per pantalla les nostres dades(Nom, cognoms, data naixement i DNI).
- Verifiquem que les dades són correctes.

3- Cliquem el botó "següent".

4- Omplim el codi de la iniciativa.
- Triem any des de desplegable (Ex. 2012)
- Entrem codi (Ex. 123)

5- Entrem Títol Iniciativa

6- Entrem Descripció Iniciativa (Text articulat)

7- Entrem Data fi recollida signatures.
- Triem dia des de desplegable (Ex. 21).
- Triem mes des de desplegable (Ex. Agost).
- Triem any des de desplegable (Ex. 2012).

8- Cliquem botó "Enviar".
- L'aplicació ens ha de mostrar el missatge "S'ha afegit la iniciativa amb èxit".

9- Cliquem a la pestanya "VEURE INICIATIVES"
   - Comprovem que la iniciativa que hem creat es visualitza.

10- Cliquem sobre la iniciativa.
   - Comprovem que les dades són les que hem entrat.

6.2.2. Signar Iniciativa amb DNI-e

Per a provar el funcionament de signatura d'una iniciativa, seguim els passos següents:

1- Des de un navegador ens adrecem a la URL 80.64.39.210.
   - L'aplicació ens redirecciona a https://80.64.39.210/index.php

2- Cliquem sobre la pestanya "VEURE INICIATIVES".

3- Cliquem sobre la iniciativa que volem signar.
   - L'aplicació ens ha de mostrar les dades de la iniciativa.

4- Cliquem el botó "Signar".
   - L'aplicació ens demanarà un certificat.
   - Triem el certificat d'autenticació del DNIe.
   - Entrem el password.
   - La aplicació ens mostrarà per pantalla les nostres dades(Nom, cognoms, data naixement i DNI).
   - Verifiquem que les dades són correctes

5- Cliquem botó "Següent"
   - El navegador ens mostra missatge d'advertència preguntant si estem segurs d'executar l'aplicació".

6- Cliquem "Executar acceptant els riscos".
   - L'aplicació ens demanarà un certificat per a signar el text.
   - Triem el certificat de signatura del DNI-e.
   - L'aplicació ens demana confirmació abans de signar.

7- Donem consentiment clicant "Sí".
   - Se'ns obrirà explorador arxius per a seleccionar on volem desar una còpia de la signatura.

8- Seleccionem la ubicació i cliquem "Guardar"
   - Comprovar aparició missatge "Procés de signatura en curs. Espereu uns instants."
   - Comprovar aparició missatge "La seva signatura ha sigut afegida correctament."

9- Cliquem sobre la pestanya "VEURE INICIATIVES".
   - Comprovem que el nombre de signatures s'ha incrementat en una unitat.

10- Obrim fitxer on hem desat la còpia de la signatura.
   - Comprovem que el fitxer conté la signatura.

6.2.3. Obtenir signatures amb DNI-e.

Per a comprovar el bon funcionament del procés d'obtenció de signatures fem el següent:

1- Des de un navegador ens adrecem a la URL 80.64.39.210.

- L'aplicació ens redirecciona a https://80.64.39.210/index.php

2- Cliquem sobre la pestanya "VEURE INICIATIVES".

3- Cliquem sobre la iniciativa que volem signar.
- L'aplicació ens ha de mostrar les dades de la iniciativa.

4- Cliquem el botó "Accés promotor".
- L'aplicació ens demanarà un certificat
- Triem el certificat d'autenticació del DNIe.
- Entrem el password.
- La aplicació ens mostrarà per pantalla les nostres dades(Nom, cognoms, data naixement i DNI) i el missatge "Has accedit a l'àrea promotor satisfactòriament.
- Verifiquem que les dades són correctes

5- Cliquem botó "Obtenir signatures"
- Se'ns obrirà explorador arxius per a seleccionar on volem desar el fitxer comprimit amb nom codi_iniciativa.001.zip

6- Seleccionem la ubicació i cliquem "Guardar"
- Comprovar la correcte descàrrega del fitxer.

7- Obrim fitxer on hem desat el fitxer amb les signatures.
- Comprovem que el fitxer conté totes les signatures cadascuna amb nom codi_iniciativa.DNI.xml

6.3. Proves amb Certificat digital.

6.3.1. Crear nova iniciativa amb Certificat digital.

Seguim els passos següents:

1- Des de un navegador ens adrecem a la URL 80.64.39.210.
- L'aplicació ens redirecciona a https://80.64.39.210/index.php

2- Cliquem sobre la pestanya "CREA NOVA INICIATIVA"
- L'aplicació ens demanarà un certificat.
- Triem el certificat digital auto signat.
- La aplicació ens mostrarà per pantalla les nostres dades(Nom, cognoms i DNI).
- Verifiquem que les dades són correctes.

3- Cliquem el botó "següent".

4- Omplim el codi de la iniciativa
- Triem any des de desplegable (Ex. 2012)
- Entrem codi (Ex. 123)

5- Entrem Títol Iniciativa

6- Entrem Descripció Iniciativa (Text articulat)

7- Entrem Data fi recollida signatures
- Triem dia des de desplegable (Ex. 21).
- Triem mes des de desplegable (Ex. Agost).
- Triem any des de desplegable (Ex. 2012).

8- Cliquem botó "Enviar"
   - L'aplicació ens ha de mostrar el missatge "S'ha afegit la iniciativa amb èxit".

9- Cliquem a la pestanya "VEURE INICIATIVES"
   - Comprovem que la iniciativa que hem creat es visualitza.

10- Cliquem sobre la iniciativa.
   - Comprovem que les dades són les que hem entrat.

6.3.2. Signar Iniciativa amb Certificat digital.

Per a provar el funcionament de signatura d'una iniciativa, seguim els passos següents:

1- Des de un navegador ens adrecem a la URL 80.64.39.210.
   - L'aplicació ens redirecciona a https://80.64.39.210/index.php

2- Cliquem sobre la pestanya "VEURE INICIATIVES".

3- Cliquem sobre la iniciativa que volem signar.
   - L'aplicació ens ha de mostrar les dades de la iniciativa.

4- Cliquem el botó "Signar".
   - L'aplicació ens demanarà un certificat.
   - Triem el certificat digital auto signat.
   - La aplicació ens mostrarà per pantalla les nostres dades(Nom, cognoms i DNI).
   - Verifiquem que les dades són correctes.

5- Cliquem botó "Següent".
   - El navegador ens mostra missatge d'advertència preguntant si estem segurs d'executar l'aplicació".

6- Cliquem "Executar acceptant els riscos"
   - L'aplicació ens demanarà un certificat per a signar el text
   - Triem el certificat digital auto signat.
   - L'aplicació ens demana confirmació abans de signar.

7- Donem consentiment clicant "Sí".
   - Se'ns obrirà explorador arxius per a seleccionar on volem desar una còpia de la signatura.

8- Seleccionem la ubicació i cliquem "Guardar".
   - Comprovar aparició missatge "Procés de signatura en curs. Espereu uns instants."
   - Comprovar aparició missatge "La seva signatura ha sigut afegida correctament."

9- Cliquem sobre la pestanya "VEURE INICIATIVES".
   - Comprovem que el nombre de signatures s'ha incrementat en una unitat.

10- Obrim fitxer on hem desat la còpia de la signatura.
   - Comprovem que el fitxer conté la signatura.

6.3.3. Obtenir signatures amb Certificat digital.

Per a comprovar el bon funcionament del procés d'obtenció de signatures fem el següent:

8- Des de un navegador ens adrecem a la URL 80.64.39.210.
   - L'aplicació ens redirecciona a https://80.64.39.210/index.php

9- Cliquem sobre la pestanya "VEURE INICIATIVES".

10- Cliquem sobre la iniciativa que volem signar.
   - L'aplicació ens ha de mostrar les dades de la iniciativa.

11- Cliquem el botó "Accés promotor".
   - L'aplicació ens demanarà un certificat
   - Triem el certificat digital auto signat.
   - La aplicació ens mostrarà per pantalla les nostres dades(Nom, cognoms i DNI) i el missatge "Has accedit a l'àrea promotor satisfactòriament.
   - Verifiquem que les dades són correctes

12- Cliquem botó "Obtenir signatures"
   - Se'ns obrirà explorador arxius per a seleccionar on volem desar el fitxer comprimit amb nom codi_iniciativa.001.zip

13- Seleccionem la ubicació i cliquem "Guardar"
   - Comprovar la correcte descàrrega del fitxer.

14- Obrim fitxer on hem desat el fitxer amb les signatures.
   - Comprovem que el fitxer conté totes les signatures cadascuna amb nom codi_iniciativa.DNI.xml

6.4. Control de requisits.

6.4.1. Control creació iniciativa.

Per a acabar de validar el procés de creació comprovarem la no inserció d'una nova iniciativa davant d'errors a l'hora de inserir les dades i els missatges d'advertència per tal de reconèixer els errors. Les comprovacions a fer són:

1- Enviar formulari amb any codi iniciativa buit.
   - Comprovar aparició missatge "L'any del codi d'una ILP s'ha d'omplir obligatòriament i no pot ser posterior a l'any actual"

2- Comprovem que només s'accepten números al inserir codi iniciativa.

3- Enviar formulari amb codi iniciativa amb menys de tres dígits.
   - Comprovar aparició missatge " El codi de una ILP ha de ser de la forma ILPAAAAXXX. On AAAA és l'any i XXX és el codi que ha de ser forçosament de tres dígits"

4- Enviar formulari amb títol iniciativa buit.
   - Comprovar aparició missatge " El camp Títol s'ha d'omplir obligatòriament"

5- Enviar formulari amb descripció iniciativa buit.
   - Comprovar aparició missatge " El camp Descripció s'ha d'omplir obligatòriament"

6- Enviar formulari amb dia, mes o any buit.
    - Comprovar aparició missatge "Els camps dia, mes i any s'han d'omplir obligatòriament."

7- Enviar formulari amb data fi recollida anterior a la data actual.
    - Comprovar aparició missatge " La data fí a de ser posterior a la data actual".

8- Enviar formulari amb data fi superior a 9 mesos des de data actual.
    - Comprovar aparició missatge " El termini màxim per a la recollida de signatures és de 9 mesos".

9- Enviar formulari amb codi iniciativa o títol iniciativa igual a iniciativa existent.
    - Comprovar aparició missatge "Duplicate entry ILPAAAAXXX for key PRIMARY".

També comprovem que si autentiquem amb un DNI-e d'un menor d'edat la aplicació no ens deixa continuar i ens mostra el missatge "Aquesta és un àrea restringida per a menors d'edat"

6.4.2. Control signatura iniciativa

Per a acabar de validar el procés de signatura comprovarem la no inserció d'una signatura de una ILP que ja hem signat o que el termini de recollida de signatures s'ha exhaurit. Així com els respectius missatges que la aplicació donarà davant aquestes situacions. Les comprovacions a fer són:

1- Signar iniciativa amb termini recollida signatures exhaurit.
    - Comprovar aparició missatge "El termini per a la recollida de signatures a finalitzat"
    - Comprovar la no aparició del botó "Signar".

2- Signar iniciativa que ja havíem signat prèviament.
    - Comprovar aparició missatge " La seva signatura NO s'ha pogut afegir correctament".

També comprovem que si autentiquem amb un DNI-e d'un menor d'edat la aplicació no ens deixa continuar i ens mostra el missatge "Aquesta és un àrea restringida per a menors d'edat"

6.4.3. Control obtenció signatures

Comprovem que davant l'intent d'accés a l'àrea promotor d'un usuari que no és el que ha creat la iniciativa apareix el missatge "Accés restringit. Aquesta és un àrea exclusiva per al promotor de la iniciativa" i no apareix el botó "Obtenir signatures".

7. Conclusions.

Aquest treball ens ha fet veure les aplicacions possibles que ens pot oferir la autenticació amb certificat digital i signatura digital de documents.

Per a una persona com jo que no havia programat una pàgina web i que desconeixia totalment aquest món ha sigut una experiència molt enriquidora el veure com de manera força senzilla es pot arribar a crear una plataforma completament segura.

Avui en dia que la gent comença a aclamar una gestió política amb una participació més activa per part dels ciutadans, es molt gratificant veure com realment existeixen eines prou potents per a realment poder iniciar un procés d'aquest tipus amb garanties. Entenc que aquesta podria ser una de les línies de treball futur més interessants

També he de dir que m'ha sorprès molt negativament com en depèn quins sistemes operatius i/o navegadors és extremadament complex el preparar l'entorn de client; o fins i tot impossible. Potser aquesta és la línia de treball més important a dur a terme per a les diferents empreses distribuïdores de software, ja que per a que la tecnologia tingui èxit és indispensable simplificar el procés de preparació de l'entorn i estandarditzar els certificats.

8. Glossari.

Apache

Servidor web HTTP de codi obert per a plataformes Unix (BSD, GNU/Linux, ...)

Applet

Component d'una aplicació que s'executa en el context d'un altre programa, per exemple un navegador web.

BBDD

Base de dades

Bluefish

Programari lliure per a la edició d'HTML, CSS, PHP, SQL ,JavaScript, ...

CA

Autoritat de certificació

Certificat Digital

Document signat per una CA que garanteix la vinculació entre la identitat del titular amb la seva clau pública

CSS

De l'anglès "Cascading Style Sheets", és un llenguatge usat per a definir la presentació de un document escrit en html o XML.

DNI-e

Document Nacional de Identitat electrònic

FNMT

Fábrica Nacional de Moneda y Timbre

GNU

Projecte que té per objectiu la creació de un sistema operatiu completament lliure.

HTML

De l'anglès "HyperText Markup Language", és un llenguatge de marcatge per a la elaboració de pàgines web.

HTTP

De l'anglès "HyperText Transfer Protocol", és el protocol usat per les transaccions de la World Wide Web.

HTTPS

De l'anglès "Hyper Text Transfer Protocol Secure", és un protocol per a la transferència de hipertexte segur basat en SSL/TLS.

ILP

Iniciativa Legislativa Popular

JEC

Junta Electoral Central

MySQL

MySQL és un sistema de gestió de bases de dades.

PHP

Llenguatge de programació dissenyat per a la creació de pàgines web dinàmiques.

SSL/TLS

De l'anglès "Secure Sockets Layer"/"Transport Layer Security", són protocols criptogràfics que proporcionen comunicacions segures .

Ubuntu

Sistema Operatiu amb nucli Linux basat en Debian.

X509

Estàndard per a infraestructures de clau pública.

XadES

De l'anglès "XML Advanced Electronic Signatures", és un format de signatura electrònica basat en XML.

XML

De l'anglès "eXtensible Markup Language", és un llenguatge de marques desenvolupat pel World Wide Web Consortium (W3C).

9. Bibliografia.

Base de dades Lleis Legislació ILP:

http://noticias.juridicas.com/base_datos/Admin/lo3-1984.html

http://noticias.juridicas.com/base_datos/Admin/lo4-2006.html

http://noticias.juridicas.com/base_datos/Admin/l59-2003.html

Altres plataformes recollida signatures per a ILPs.

http://www.openilp.org/

http://www.iniciativalegislativapopular.es/

Instal·lació LAMP

http://www.howtoforge.com/installing-apache2-with-php5-and-mysql-support-on-ubuntu-10.10-lamp

Configuració Apache com a servidor segur HTTPS

http://www.rinconastur.com/php/php21.php

MiniApplet @firma

http://forja-ctt.administracionelectronica.gob.es/web/clienteafirma

Portal oficial dni electrònic.

http://www.dnielectronico.es/

Programació amb PHP

http://www.php.net/

Programació HTML, CSS, PHP

http://www.w3schools.com/