Securització en la comunicació d'associacions

Enginyeria Tècnica en Informàtica de Sistemes

Projecte de Fi de Carrera

Autor : Pere Ramon Erro Mas

Professor consultor: Cristina Pérez Solà
Universitat Oberta de Catalunya (UOC)
11 de Gener de 2013

Llicència

Índex

Dedicatòria i agraïments

Primer de tot vull agrair la tasca de seguiment de la professora consultora Cristina Pérez Solà que m'ha acompanyat en aquest treball amb consells i apunts molt valuosos.

Vull nombrar al professor d'informàtica de la UPC i expert en OpenERP en Jordi Esteve per la seva tasca de difusió a tots els nivells, també el tècnic, del programari lliure en general i de l'OpenERP en particular.

Agraeixo emotivament la comunitat de codi obert pel seu esforç sempre amb la component de l'aprofitament màxim comú i de la qualitat contrastada de la tasca feta pública. Foros, howtos, wikis, repos i tota la infraestructura necessària com eines de desenvolupament, de compartició, de formació, etc...

Un agraïment especial es mereixen els grups de particulars, organitzats o no en empreses, que donen suport al macroprojecte de DNI electrònic. Sense poder arribar al nivell personal m'he trobat amb els següents:

- ViaFirma : http://www.viafirma.com

  Oferiment de un entorn de proves molt complert que permet comprovar el funcionament de tot el cicle complert de signatura i verificació.

- Sinadura : http://www.sinadura.net/es/

  Ofereix un programari de signatura i verificació amb DNIe que pot córrer sobre els diferents sistemes operatius.

Cal un reconeixement just, llàstima que amb les dues accepcions, cap a les administracions públiques per la tasca de fer extensiva a tots els ciutadans aquesta tecnologia d'autenticació i signatura. Trobo a faltar un seguiment dels objectius o bé l'aplicació de les mesures correctores de les insuficiències que clarament sorgeixen de qualsevol simple anàlisis.

Per finalitzar aquest capítol, vull dedicar aquest treball a la meva família que m'han donat suport, ànims, temps (!) i prou estimació per poder omplir amb convicció aquest apartat tant humà del treball. Moltes gràcies a tots, i, molt en especial, a tu, Claudina, esposa meva.

Resum

Securització en la comunicació d'associacions és un projecte que posa focus sobre les zones fosques que el programari lliure té perquè es pugui dur a terme unes comunicacions telemàtiques segures (autenticació, no repudi, privadesa) entre un usuari-soci i una entitat de tipus associativa, no tant pel tracte de seguretat dels documents com dels casos d'us contemplats.

Incloem, com formant part de la comunicació d'una associació l'accés a la difusió de informació, la recepció de documents de l'associació i la conformitat o no conformitat d'un document (generat per l'associació o per un formulari omplert per l'usuari) per part de l'usuari-soci que es requereix per part de l'entitat.

En aquesta solució de principi a fi, per poder aconseguir l'autenticació, no repudi i privadesa es fan servir tècniques fonamentalment obertes i amb estàndards reconeguts que garantir la durabilitat tant del contingut del projecte com dels desenvolupaments de projectes derivats.

L'altra característica que m'agrada destacar és la importància que se li ha donat a la simplicitat. Aquesta s'ha imposat al projecte de tal forma que si en algun punt s'observa un indici de complexitat, o bé es descarta o bé s'hi treballa en la simplificació.

Índex de taules i contingut gràfic

Cos de la memòria

1 Introducció

En aquest capítol s'incorporen els continguts que serveixen de introducció al projecte.

1.1 Context

Fins ara, tots els documents en paper intercanviats en molts processos de les associacions es basaven en un model més o menys personalitzat i una signatura de conformitat amb el text que conté el paper un cop emplenat si calia.

Aquest treball va en la tendència de fer una equivalència electrònica d'aquest model. Aquest paper passa a ser un PDF que s'elabora amb la informació continguda en les bases de dades o recollint les dades que aporta l'usuari mitjançant formulari. Aquest PDF passa a ser un document legal quan queda signat amb el DNI electrònic. Com a tal document legal, ha de tenir una gestió adequada de privacitat i d'emmagatzemament.

Molts dels serveis que s'ofereixen per Internet encara funcionen amb el sistema base d'usuari i contrasenya. És cert que darrerament les grans plataformes de serveis Google, Yahoo, Microsoft permeten a tercers usar la seva plataforma d'autenticació, però la facilitat d'obrir comptes d'usuari -per la gran competència per captar futurs clients per a les respectives empreses anunciadores- , fa que la usurpació d'identitats es converteixi en quelcom gairebé accidental, sense que calgui intencionalitat de fer mal.

Amb el model sobre el que s'ha treballat, la tercera persona que garanteix la correcció de la relació és un organisme públic i, d'aquesta forma s'ha de poder garantir una resolució justa d'un conflicte que, a més, vagi en benefici de tots, estiguin implicats o no.

En l'àmbit del programari lliure, una de les mancances que s'observen és sobre la gestió de la seguretat, tot i tenir programari suficient per possibilitar un entorn segur de funcionament.

De tant en tant apareixen notícies que Facebook, Twitter, i altres xarxes socials, augmenten els controls, de moment no per autentificar amb certificats d'usuari -on tindríem un tercer aliè de confiança comuna-, sinó, continuant amb el model majoritari actual, amb millors formularis de denúncia quan s'hagi detectat suplantació o problemes d'autenticació (veure notes de premsa en annexes).

D'altra banda, els certificats digitals que faciliten les administracions per a les gestions telemàtiques no tenen gaire ús fora dels respectius entorns. Aquest TFC encararà aquesta circumstància i buscarà possibles aprofitaments per les entitats associatives.

1.2 Objectius

La finalitat d'aquest TFC és exposar un sistema segur per les comunicacions d'una associació sense ànim de lucre amb els seus socis.

Entenem com associació un conjunt, en principi nombrós, de persones, la majoria de les quals amb una activitat principal diferent amb la de l'associació. Això marcarà la forma de buscar la interactuació i la necessitat que les operacions de configuració en els clients siguin mínimes.

Per aconseguir-ho, definim els següents objectius:

- Apuntar detalls o enllaços útils de les eines existents.
- Generar noves eines quan no n'hi hagi o estiguin en solucions que impossibiliten la

incorporació en una solució senzilla de principi a fi.

- La simplicitat ha de ser extrema tant per als usuaris com per als administradors.
- Ha de ser un sistema segur i reconegut públicament.
- La solució s'ha de basar en codi obert.

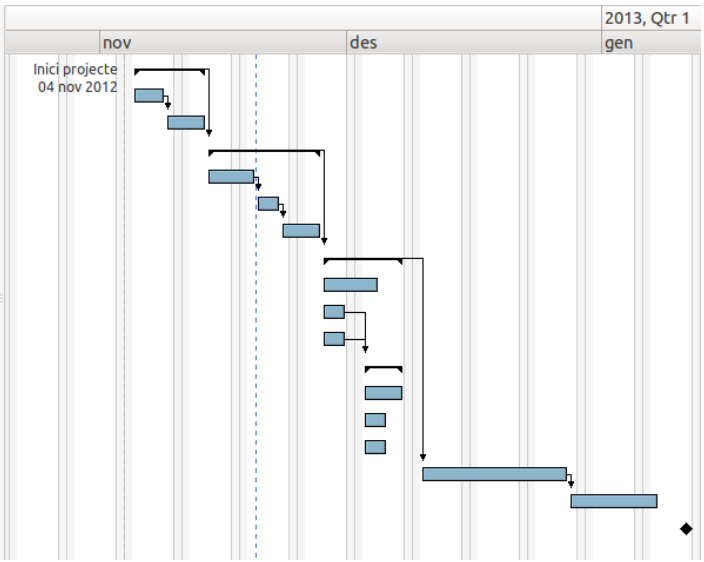
El TFC té un cas ambé serà una memòria de com es posa en pràctica en un cas particular: l'Associació de Mares i Pares d'Alumnes de l'Institut Lluís de Peguera de Manresa.

1.3 Planificació

1.3.1 APLICACIÓ DE PLANIFICACIÓ

Per planificar el projecte he fet servir l'aplicació Planner que corre sobre Gnome de Linux.

WBS	Nom	Feina
1	**Anàlisis de Interactuacions**	**7d**
1.1	Estudi programari existent	4d
1.2	Connexió amb administracions	3d
2	**Disseny Programari**	**10d**
2.1	Processos E/S de les aplicacions	4d
2.2	Disseny comunicació per capes	3d
2.3	Entitats i protocols	3d
3	**Codificació Programari**	**22d**
3.1	Mòdul accés Joomla amb certificat	5d
3.2	Vendes amb docs signats requerits	3d
3.3	Factura amb annexes	3d
3.4	**Connexió Joomla-OpenERP**	**11d**
3.4.1	Coixí de comunicació	5d
3.4.2	Comanda de venda amb docs requerits	3d
3.4.3	Factures amb descàrrega del document signat	3d
4	Elaboració i execució de tests	14d
5	Completar Documentació	7d
6	Presentació TFC	N/D



Il·lustració 1: Gràfic de la planificació del projecte

1.3.2 TASQUES PLANIFICADES

1. Elaboració del mapa d'aplicacions i requeriments d'interactuacions entre elles. (1 setmana)
    1. Estudi del programari existent
    2. Estudi del marc de col·laboració amb administracions a nivell informàtic
2. Disseny del programari director de interactuacions. (1 setmana)
    1. Estudi de processos (comportament, entrada i sortida, ...) de les aplicacions per separat
    2. Disseny de la comunicació per capes
    3. Concreció de les entitats i els protocols a utilitzar
3. Codificació del programari. (1 setmanes)
    1. Nou mòdul d'accés Joomla amb interrogació de certificat i comprovació per part d'una entitat autoritzada.
    2. Preparació del mòdul OpenERP de traspàs de socis al Joomla com usuaris amb el DNI com a nom d'usuari.
    3. Connexió del portal amb les dades de soci de dins el programa de gestió interna.

1. Preparació de la capa de comunicació
2. Enregistrament de document de comanda de venda del portal a l'OpenERP
3. Document legal de venda o factura on s'incorporen els documents relacionats amb el producte o execució dels servei.

4. Elaboració i execució de tests (2 setmanes)
5. Completar documentació (1 setmana)

1.4 Productes Obtinguts

Com que l'objectiu era fer una connexió entre programari lliure per poder fer una línia de funcionalitat determinada, s'ha hagut de treballar en varis projectes diferents aportant aquests productes que es troben en dos dipòsit de codi lliura a la xarxa:

- Branca en Launchpad emmarcada en el projecte OpenERP-School on es troben tots els productes excepte un:

  https://code.launchpad.net/~school-dev-team/school-base-openerp-module/school-ampa-openerp-module

- Branca en GitHub on es troba el producte validatePDFSignedByDNIe.jar :

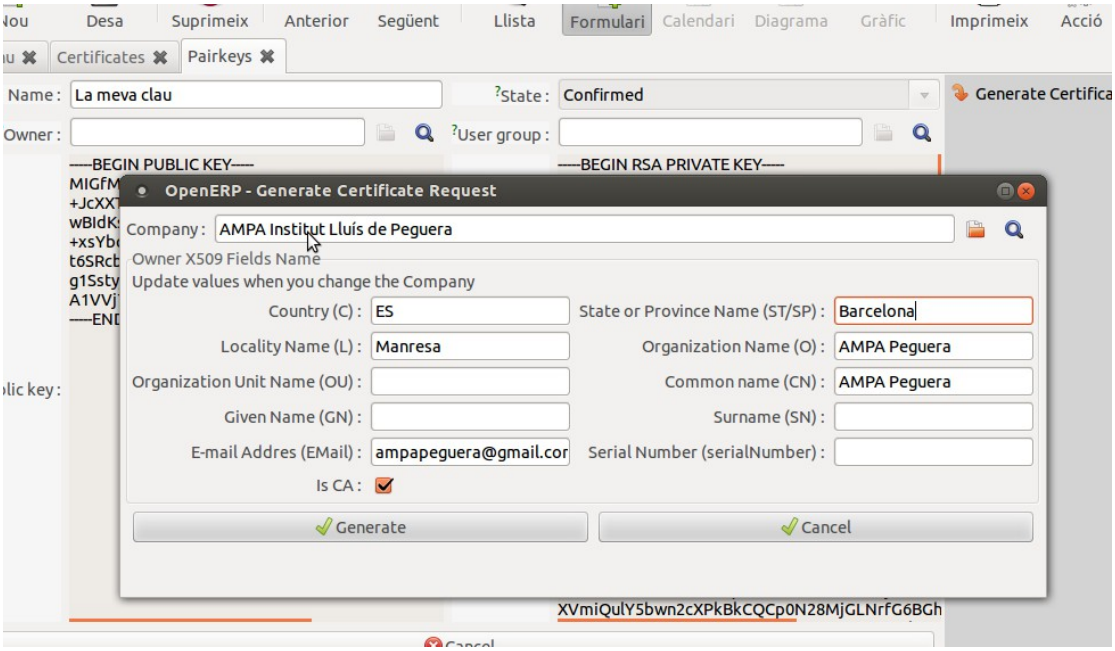
  https://github.com/pereerro/validatePDFSignedByDNIe.git

1.4.1 Modificació de Plugin i mòdul de Joomla per l'autentificació amb DNIe : mod_viafirma, plg_viafirma

No és un producte totalment propi ni totalment acabat. S'han fet les modificacions necessàries perquè en la configuració de Joomla actual funcioni. No s'ha publicat perquè la generalització no es troba suficientment provada. És a dir, en cada instal·lació caldrà provar el funcionament.

1.4.2 Millora del mòdul de dipòsit de claus per OpenERP : openerp_crypto

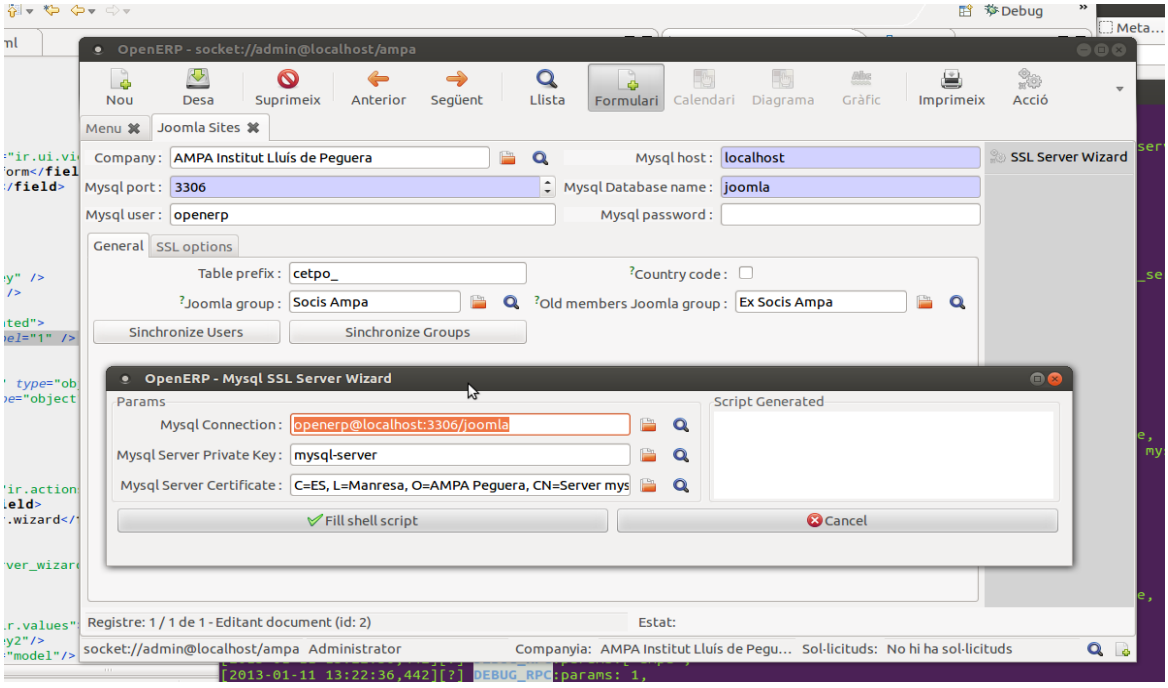
Al mòdul existent de criptografia per OpenERP se li amplia la funcionalitat per gestionar autoritats de certificació i poder generar certificats signats i així poder crear una PKI X509. En no tenir un nom de mòdul acord amb els estàndards, s'opta per no posar-lo com a dependència.



Il·lustració 2: openerp_crypto : Generació de petició de certificat

1.4.3 SOCI-USUARI OPENERP EN JOOMLA : MEMBERSHIP_JOOMLA

Per crear usuaris i dotar-los de un grup especial en Joomla mentre són socis en OpenERP. Té com a dependència el mòdul anterior.



Il·lustració 3: Detall de l'assistent de securització de la connexió OpenERP-Joomla

1.4.4 EXECUTABLE VALIDANT DE SIGNATURA DNIE : VALIDATEPDFSIGNEDBYDNIE.JAR

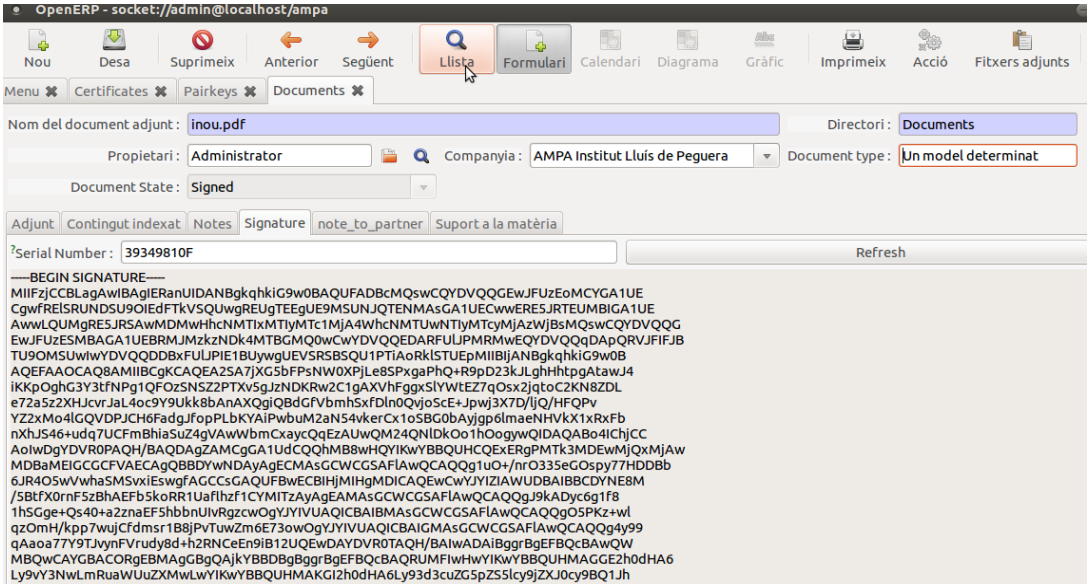
Tot i que és una funcionalitat central i molt específica per al mòdul següent, s'ha ideat com un

producte a part per la inexistència de llibreries per fer aquesta funció en el llenguatge de programació Python.

1.4.5 CREACIÓ D'UN MÒDUL OPENERP DE GESTIÓ DE SIGNATURES EN PDF : CONTACT_DOCUMENT

Basat en el gestor documental del ERP, comprova la correcció de la signatura realitzada amb un DNIe. Fa ús del executable JAVA anomenat en el producte anterior.

També es troba integrat en el projecte OpenERP-School en la branca contact_document .



Il·lustració 4: Extracció de signatura en PDF

1.4.6 COMPONENT JOOMLA DE CONNECTOR AMB OPENERP : COM_ERP

Per la presentació dels documents PDF per cada usuari dins del servidor OpenERP

Ens permet la interactuació de l'usuari en un entorn familiar i totalment personalitzable segons la imatge i tarannà de les diferents

Encara no té un projecte propi en els dipòsits de software per a aquest CMS i s'ha desat en una carpeta dins de la branca de Launchpad.

Il·lustració 5: Pantalla del component en Joomla

1.5 Capítols específics

Breu descripció dels capítols del cos de la memòria.

1 Introducció

En aquest capítol s'incorporen els continguts que serveixen de introducció al projecte.

2 Programari base i usat

En aquest capítol s'enumera el programari que s'ha usat en aquest treball.

3 Requeriments i casos d'ús

En aquest capítol enumerarem i explicarem els requeriments i els casos d'ús que s'han contemplat.

4 Desenvolupament del programari

En aquest capítol s'explica amb cert detall com ha estat el desenvolupament del programari.

5 Proves i tests efectuats

Aquí es detallen les proves i els test que s'han efectuat. Es tracta de verificar si el resultat del projecte compleix els requisits per assolir els objectius proposats.

6 Conclusió i apunts de millora

Es passa a donar una opinió tècnica i a apuntar línies de millora.

7 Glossari

Breu definició de les paraules que poden no ser comunes amb el lector.

8 Bibliografia i llocs WEB d'interès

Llibres i llocs WEB contrastats que apareixen en el treball o que s'han usat com a documentació.

9 Referències de premsa

Referències a les notícies de premsa que s'inclouen en el text del treball.

2 Programari base i usat

En aquest capítol s'enumera el programari que s'ha usat en aquest treball.

El programari sobre el quin es basa el treball és:

- CMS Joomla

  Per la gestió de continguts WEB. Tot i que actualment no és el millor CMS que es pot triar per fer programari lliure, sí que és el CMS obert més veterà.

  D'altra banda, es considera el CMS com una passarel·la de l'usuari cap a les dades que es manipulen i s'enregistren en el programari de gestió d'empresa. D'aquesta forma, la complexitat del disseny i la quantitat de codi queda molt reduït de cara a plantejar passarel·les en altres CMS com Drupal.

  Està codificat en PHP.

- Apache WEB server

  Per a servir les pàgines que genera el Joomla. És el servidor WEB per excel·lència mantenint una bona relació entre pes i prestacions. És fàcil d'instal·lar i apareix com a programari recomanat en els sistemes operatius Linux.

- Mysql Server

  Servidor de base de dades de codi obert de la casa Oracle sobre el que córrer el Joomla.

- OpenERP

  Per la gestió interna dels documents i integrarà la lògica dels processos. Ens servirem del mòdul Membership per la gestió d'associacions. Està programat en Python.

- PostgresSQL Server

  Servidor de base de dades lliure.

- OpenSSL

  Programari obert per al tractament de claus, certificats, signatures... amb tot d'algoritmes, estàndards, protocols,

- iText

  Com a única llibreria lliure trobada per la manipulació dels PDF a nivell de certificats i signatures. Està en Java.

Eines de programació utilitzades:

- Eclipse per desenvolupament en Python i Java. S'ha utilitzat el plugins PyDev per programar en Python.
- Geany per generar les pàgines PHP com a editor lleuger i que disposa, entre altre, de coloració de sintaxis i assistent en etiquetes HTML.
- Oracle Java JDK per compilar i aprofitar llibreries en llenguatge JAVA.

Els llenguatges de programació que s'han tocat són:

- Java
- Perl
- Shell Unix
- Python
- Php
- XML (pseudo llenguatge)

3 Requeriments i casos d'ús

En aquest capítol enumerarem i explicarem els requeriments i els casos d'ús que s'han contemplat.

3.1 Requeriments

El sistema ha de satisfer l'execució dels processos següents:

1. Quan es dóna d'alta un soci en el programa de gestió interna, el soci rep un email d'invitació a utilitzar el portal WEB.
2. El usuari del portal s'ha de poder identificar amb un certificat de les administracions públiques que ofereixin una comprovació d'autentificat.
3. L'usuari un cop autentificat com a soci, podrà accedir als documents de l'associació personals signats per l'associació.
4. També podrà signar els formularis requerits per l'associació.
5. El procés ha de ser molt simple i s'ha de poder replicar en format paper en cas que el soci no disposi de certificat d'administració pública.

3.2 Casos d'ús i processos activats

3.2.1 ALTA DE SOCI

1. El procés s'activarà en canviar l'estat d'un contacte a soci. Fins aquí el procés el gestiona el vertical Membership de l'OpenERP.
2. Es crea un usuari en Joomla amb el DNI com a nom d'usuari. S'incorpora al grup de CMS especial de socis a on podrem configurar els permisos de la resta de continguts.
3. S'envia un correu electrònic de benvinguda.

3.2.2 DESACTIVACIÓ D'USUARI

1. El procés s'activarà que el soci canvia l'estat a un de no associat.
2. Es treu l'usuari del grup especial de socis en el CMS. No es preveu eliminar-lo del tot per poder utilitzar el portal com un dipòsit d'informació relacionada amb els socis i ex-socis.

3.2.3 ELIMINACIÓ TOTAL DE LA INFORMACIÓ D'USUARI

1. El procés s'activa manualment. S'esborra l'usuari en el CMS però es manté en l'OpenERP, amb tots els documents relacionats, fins que sigui legalment necessari.

3.2.4 SIGNATURA DE DOCUMENT

1. L'usuari s'identifica en Joomla i accedeix al ítem de menú que presenta la llista de documents per signar.
2. En la llista apareix un enllaç per cada document que requereix a la pàgina PHP enllaçada la càrrega del PDF cap a la plataforma de signatura.

3. Acabada la càrrega, redirigeix el navegador del client cap a la plataforma on tenim el document apunt per signar.
4. La plataforma de signatura gestiona amb l'usuari (i directament amb el sistema operatiu, navegador inclòs) el certificat que l'usuari farà servir.
5. L'usuari ha de poder signar el document amb un dels seus certificats electrònics.
6. Quan s'ha finalitzat la signatura la plataforma retorna al servidor WEB que fa córrer el Joomla el document signat.
7. El script PHP que s'executa, amb l'identificador de sessió per mantenir la informació de l'autentificació sobre quin usuari actua, passa aquest document al servidor OpenERP.
8. Com a mesura addicional, abans de guardar la signatura en el camp dedicat es verifica que la signatura sigui correcta sobre el document, que el signant ho ha fet amb un certificat DNIe i que el NIF correspon amb el que s'apunta en el camp signador "signer".
9. Quan hi ha signatura s'actualitza l'estat del document i desapareix de la llista de documents per signar que l'usuari torna a visualitzar.

3.2.5 CONSULTA AL DIPÒSIT DE DOCUMENTACIÓ

1. El usuari tindrà accés als documents signats per la persona de l'associació que correspongui que hagin estat requerits o confeccionats per l'associació.
2. En la llista apareixerà un enllaç que servirà per anar a la plataforma de signatura digital per poder verificar la persona que signa el document.
3. Quan l'usuari demana aquesta URL, la pàgina PHP envia el document a la plataforma de signatura digital i, després redirigeix el navegador de l'usuari cap a la pàgina de verificació amb els paràmetres que identifiquen el document enviat.
4. En la pàgina de la plataforma de signatura reconeguda i de confiança generalitzada, amb la seguretat que dóna l'autenticitat del lloc WEB destacat en el navegador del client, es pot comprovar la validesa de la signatura.
5. Per a assegurar una confiança absoluta en aquell document, s'ofereix l'opció a l'usuari de verificar aquell document en altres plataformes de validació ja que s'està signant amb un certificat públic.

4 Desenvolupament del programari

En aquest capítol s'explica amb cert detall com ha estat el desenvolupament del programari.

Es consideren 5 blocs de treball:

4.1 Autentificació d'identitat per certificat d'administracions públiques en Joomla

Com a plataforma d'autentificació s'usa la de ViaFirma (www.viafirma.com). Els motius de tal decisió han estat:

1. Es delega la compatibilitat amb els dispositius dels usuaris per una autenticació sense problemes.
2. Es delega la gestió de l'autenticitat amb les entitats certificadores. Cal destacar que aquest és un punt crític i convé confirmar la signatura de l'autenticació de l'entitat certificadora (TODO explain)
3. Treballa amb l'estàndard obert OpenID en el protocol de comunicació.
4. Mòdul preparat per la versió 1.5 de Joomla

El software ofert per la plataforma d'autentificació per la integració a les versions modernes del CMS Joomla no va resultar del tot compatible i es va haver d'adaptar. Veure annex 2.

4.2 Connexions entre Joomla i openERP

1. Mòdul OpenERP interceptador del canvi d'estat del soci per disparar creació d'usuari en Joomla en cas que no estigui creat i afegir-lo al grup de socis, o bé treure'l del grup de socis.
    1. Creat el mòdul que sincronitza els socis de OpenERP amb els usuaris de Joomla.
    2. Utilitza connexions xifrades entre el servidor OpenERP i el servidor Mysql del que beu Joomla. S'annexa un correu d'exemple cap a l'administrador Joomla on s'explica com preparar el MySQL per acceptar connexions xifrades per SSL.
    3. Dins de OpenERP, el formulari d'alta de servidor Joomla per sincronitzar facilita el certificat de la CA i del servidor a més de la clau RSA.
2. Ampliar el component Joomla que presenta la documentació que es demana al usuari.

4.3 Enllaç de signatura de documents amb la plataforma de signatura ViaFirma

1. Perquè la decisió de PDFs http://itextpdf.com/book/digitalsignatures20120823.pdf
2. Mòdul OpenERP que amplia el gestor de documentació del OpenERP per guardar les signatures digitals incorporant la validació.
3. Preparació de l'enllaç amb el facilitador de signatura d'aquests arxius.

4.4 Verificació de signatura

Tot que l'arxiu PDF es pot validar a la plataforma que utilitzem per facilitar la signatura a l'usuari (http://services.viafirma.com/viafirma/test/verification/check-sign/), per evitar atacs tipus man-in-

the-middle es decideix implementar l'opció de validar directament la signatura en un OSCP públic i gratuït. Per extreure el certificat amb el que s'ha signat el PDF utilitzem la llibreria itext de java.

1. Problemes: http://itextpdf.sourceforge.net/howtosign.html#howtoverify
2. Solució: http://permalink.gmane.org/gmane.comp.encryption.bouncy-castle.devel/10679
3. Verificar signatura : http://av-dnie.cert.fnmt.es/validayfirma/verificar_firma.jsp

4.5 Signatura digital dels documents de l'associació per als associats

És convenient la programació en Java perquè cal accés al hardware del dispositiu que allotja la smartCard del DNI (es descarta doncs la WEB) i també perquè és el llenguatge de la llibreria iText per poder incorporar la signatura en els PDF.

Però, un cop avançat l'estudi del disseny, es comprova que cal un projecte de pes per arribar a completar aquest requeriment. Això faria que es sobrepassés les limitacions autoimposades i es torna a fer un anàlisis de les alternatives.

Queda clar que el més pràctic per un usuari que ha de signar digitalment un munt de documents és treballar amb programari executant-se en local i amb els documents més “propers” possibles per fer una càrrega i descàrrega ràpida.

Com que el servidor OpenERP disposa de l'accés documental en WEBDAV, es planteja l'aprofitament d'aquest servei per als usuaris del OpenERP preparant una carpeta específica per als documents per signar. Un cop tenen signatures comprovades passen a la carpeta de documents signats.

5 Proves i tests efectuats

Aquí es detallen les proves i els test que s'han efectuat. Es tracta de verificar si el resultat del projecte compleix els requisits per assolir els objectius proposats.

5.1 Accés al lector de smart card

El lector de targetes intel·ligents utilitzat per les proves ha estat el LTC31 USB de la casa C3PO, SL.

En els 2 sistemes operatius Windows provats, ha calgut instal·lar la plataforma java però, en acabat, els applets ha funcionat amb normalitat en tots els navegadors provats: Iexplorer, Firefox, Chrome.

No passa el mateix amb els aplicatius de signatura digital d'escriptori que necessiten un treball de configuració addicional per ser compatibles amb un o altre model de lector de smart card.

En el sistema operatiu Linux no s'ha arribat a configurar correctament els drivers d'accés a la smart card i no s'han pogut fer proves. Tot i això, les característiques que s'hi documenten asseguren que el funcionament és possible.

5.2 Autenticació de l'usuari-soci en la WEB

Es verifica que un nou usuari-soci apareix com a usuari Joomla i que els que deixen de ser-ho passen al grup que es marca (en els paràmetres de la connexió) com ex-socis. Es posa o treu una data de suspensió per provocar el canvi d'estat del soci.

Sempre tenint present la implementació de la solució de la incompatibilitat (veure annex 2) , es comprova que l'usuari autentifica amb el DNIe passant per la plataforma d'autenticació i retornant a la WEB de l'associació amb un usuari autentificat.

5.3 Signatura de document per part de l'usuari

Es verifica que l'usuari registrat pot accedir a la llista de documents per signar.

Es realitza l'enllaç correctament cap a la plataforma de signatura i es descarrega el mateix document que s'espera segons el llistat.

Un cop realitzada la signatura en la plataforma, retornem al la pàgina del Joomla sense perdre la identificació i amb l'avís de conformitat en l'operació de signatura.

El document deixa d'aparèixer en la llista de pendents i apareix en la llista o bé de pendents de verificació o en la de documents signats.

5.4 Signatura de document per part d'un responsable de l'associació

Es comprova que els programes d'escriptori dedicats a signar PDF poden llegir els documents bé en la carpeta WEBDAV integrada en un sistema de fitxers Linux.

Tot i que no ha estat possible una prova de signatura directament des de l'aplicació signadora per problemes de compatibilitat amb el hardware utilitzat per les proves, s'ha fet una emulació de sobreescriptura de fitxers amb les eines del sistema operatiu.

Amb el client WebDAV integrat en el programari d'escriptori del Linux Nautilus, no hi ha hagut inconvenients en sobreescriure. En canvi no he estat capaç de configurar el muntador cap el sistema

de fitxers perquè passes aquesta prova bàsica de modificació d'arxiu: en esborrar i crear un nou arxiu el gestor documental crea una nova fitxa perden les dades de l'anterior.

Aquest inconvenient s'ha donat al final de les proves sense temps material per resoldre'l.

El programari d'escriptori per signar PDF que s'ha intentat fer funcionar en Windows i Linux (Ubuntu 10.04) sense èxit ha estat :

- Sinadura Desktop
- Firma OnLine PDF de la Generalitat Valenciana

6 Conclusió i apunts de millora

Es passa a donar una opinió tècnica i a apuntar línies de millora.

6.1 Conclusió

En les properes línies passem a valorar el resultat de les proves i tests en el sentit de consecució dels objectius previstos mitjançant l'acompliment dels requisits.

Tot i que s'ha aconseguit complir amb els requeriments, l'objectiu de muntar un sistema de forma simple no ha estat possible dins de l'àmbit d'aquest treball.

Hi ha varis motius que poden explicar aquesta tèbia valoració :

Segons les proves fetes, no hi ha una seguretat que l'accés al hardware lector de la smart card estigui garantit en tots els casos. Sembla que els esforços que s'hi han dedicat en l'àmbit del codi obert, s'hagin dirigit a solucions concretes sense que s'hagi pogut establir un estàndard.

En l'apartat dels certificats software com pot ser el de la FMNT, hi ha restriccions via taxes per una verificació dels certificats que s'extreuen de les signatures. Això impedeix un ús públic.

La tasca de facilitar la seguretat de tots els passos requereix de nous assistents de tal dimensió que cadascú d'ells ja seria un projecte com aquest. Un exemple de com voldria que fossin els assistents seria el creat per poder tenir la connexió entre l'OpenERP i el Mysql del Joomla per SSL .

6.2 Millores

- Fer compatible el contact_document amb les versions 6.1 i 7.0 de OpenERP.
- Millorar el membership_joomla perquè doni més opcions per facilitar la connexió segura.
- Dotar al contact_document de suport per a la signatura múltiple d'un document per varis socis.
- Reaprofitar els programaris de signatura d'escriptori per una connexió directa als WebDav .
- Facilitar d'assistents al openerp_crypto perquè configuri el servidor OpenERP i el client WebDav amb connexions SSL , o bé per configurar Apaches de Joomla amb certificats i CA guardades.
- I naturalment, generalitzar aquesta línia de treball en altres configuracions informàtiques : iOS, Android, Mac, ...

7 Glossari

Breu definició de les paraules que poden no ser comunes amb el lector.

Android : Sistema Operatiu dels productes portables que no són Apple.

Apache : Apache Software Foundation és una fundació que dóna, entre altres facilitats, un entorn legal al software de codi obert.

Bug : Petit error de codi.

CMS : Content Manager System . Programari que serveix per gestionar els continguts d'un lloc WEB.

DNI : En aquest treball és les sigles del Document Nacional d'Identitat Espanyol.

DNIe : El DNI en format de smart card i amb dos certificats de PKI activats: un per autentificar-se i l'altre per signar.

FNMT : Fabrica Nacional de Moneda i Timbre, encarregada dels certificats d'usuari de per l'operativa amb el Ministeri d'Hisenda i altres.

Hardware : La part dura de la informàtica, és a dir, l'electrònica i tot allò per protegir-la i accedir-hi.

iOS : Sistema Operatiu dels productes d'Apple.

Java : Llenguatge de programació de tipus interpretat molt proper al hardware i molt usat en codi obert.

Joomla : Programari veterà de codi obert que serveix de CMS per un lloc WEB. Està fet en llenguatge PHP i diposita les dades en un servidor MySQL . Tot i que disposa de molts mòduls, altres competidors li han arrabassat el lideratge dels CMS en tenir majors facilitats per oferir el servei hostatjat, com el Wordpress o Drupal.

Linux : Sistema operatiu lliure.

Llibreria : Programari dissenyat per a la reutilització.

Mac : El PC de Apple (el Mac va ser anterior)

Man-in-the-middle : Problema de seguretat que consisteix en que hi ha un sistema que es posa enmig d'una comunicació de forma transparent amb l'objectiu de capturar dades i codis d'encriptació.

Mòdul : Programari que complementa a un de principal.

MySQL : Servidor de base de dades. Un Microsoft Access en incrustat a l'internet.

OCSP : Online Certificate Status Protocol .

OpenERP : RAD d'aplicacions per a empreses de software lliure.

OpenSource : Denominació en anglès del programari lliure. Actualment abasta a la documentació d'aquest programari.

OpenSSL : Programari de codi lliure que manté bona part de la responsabilitat de la gestió dels esquemes de seguretat de clau pública d'arreu.

PDF : Portable Document Format (http://ca.wikipedia.org/wiki/PDF)

Plugin : Petita aplicació que ofereix més funcionalitat a una altra sense canviar-la massa.

Python : Llenguatge de programació amb característiques divertides.

Servidor : Software que serveix dades, normalment per la xarxa.

Signatura digital : Manipulació informàtica amb la que obtenim la seguretat que un document ha estat validat per un posseïdor d'un certificat.

Smart Card : Targeta que té la possibilitat de manipular dades mitjançant un xip.

Software : Les intruccions que segueix el hardware.

SSL : Secure Socket Layer, protocol per establir una capa de connexions segures.

URL : Unificate Resource Locator.

WebDav : Programari que permet accés als fitxers mitjançant el protocol HTTP.

Windows : Sistema operatiu propietari de Microsoft.

XML : eXtended Markup Language, pseudo llenguatge d'estructura de dades mitjançant etiquetes.

8 Bibliografia i llocs WEB d'interès

Llibres i llocs WEB contrastats que apareixen en el treball o que s'han usat com a documentació.

Viafirma : http://developers.viafirma.com , empresa que es dedica a gestionar els certificats digitals i DNI electrònic. (http://services.viafirma.com/viafirma/ demostració de la plataforma)

Agència de Tecnologia i Certificació Electrònica de la Generalitat Valenciana (signatura i validació de DNIe on line) : http://www.accv.es/ciudadanos/firma-on-line-pdf

DNI electrònic : http://www.dnielectronico.es/seccion_integradores/certificaciones.html , pàgina oficial amb informació sobre les certificacions relacionades amb el DNI electrònic

Argumentari Joomla-OpenERP : http://www.slideshare.net/raimonesteve/openerp-y-cms-radiotv

Comandes del OpenSSL : http://www.sslshopper.com/article-most-common-openssl-commands.html

Infraestructura de clau pública en Java : http://docs.oracle.com/javase/1.5.0/docs/guide/security/pki-tiger.html

Sinadura OpenSource : http://www.sinadura.net/es/ . Productes i serveis per a la identitat digital i signatura electrònica. Ofereix eines de software (sinaduraDesktop), serveis i suport a la comunitat.

Explicació de verificació de certificat per OSCP :http://www.rinconastur.com/php/php24.php

Article de seguretat en Joomla : http://docs.joomla.org/How_to_add_CSRF_anti-spoofing_to_forms

Manual del carregador de webdav en el sistema de fitxers de Linux : http://linux.die.net/man/5/davfs2.conf

OpenERP-Crypto, Cryptology addon for OpenERP : https://launchpad.net/openerp-crypto

Document del Ministeri de l'Interior d'Espanya per a la signatura electrònica : http://www.dnielectronico.es/oficina_prensa/Documentos/060216/doc_firma_dgp.pdf

Llei de protecció de dades a Espanya : http://www.boe.es/boe_catalan/dias/1999/12/30/pdfs/A01399-01411.pdf (articulat en WEB : http://noticias.juridicas.com/base_datos/Admin/lo15-1999.html)

WEB d'ajuda al seguiment de la llei : http://www.ayudaleyprotecciondatos.es/

9 Referències de premsa

Referències a les notícies de premsa que s'inclouen en el text del treball.

9.1 Cal més seguretat

- *La Vanguardia, 8/11/2012*: **Twitter podría haber recibido un ataque hacker masivo**, http://www.lavanguardia.com/internet/20121108/54354967624/twitter-ataque-hacker-masivo.html
- *La Vanguardia*, 8/11/2012: **Twitter niega que el reseteo de miles de contraseñas se deba a un ataque hacker,** http://www.lavanguardia.com/internet/20121108/54354977817/twitter.html
- *Ministerio de Educación, Cultura y Deporte*, 19/11/2012: Privacidad y seguridad en Redes Sociales, http://recursostic.educacion.es/observatorio/web/es/internet/recursos-online/1015-daniel-ortega-carrasco

Annexes

1 Instal·lació de programari

1.1 Instal·lació de programari OpenERP

Hi ha diferents versions del servidor i en cada versió hi ha canvis substancials que fa evolucionar molt ràpid el ERP en la vessant de interacció amb l'usuari però, per contra, afecta, encara que mínimament, al programari base del servidor.

Els mòduls que s'han dissenyat en aquest treball estan pensats per la versió 6.0 del servidor OpenERP. Les posteriors versions afecten al mòdul contact_document pel diferent tracte que se li dóna a l'entitat contacte d'empresa.

Un tutorial d'instal·lació de l'OpenERP es pot trobar a

http://www.howtoforge.com/how-to-install-openerp-6-on-ubuntu-10.04-lts-server

Tant el servidor com el client, com els paquets que són necessaris, es poden trobar en els repositoris de les versions Linux més esteses.

1.2 Instal·lació de Joomla

Tot i que actualment no és el millor CMS que es pot triar per fer programari lliure, sí que és el CMS obert més veterà.

D'altra banda, es considera el CMS com una passarel·la de l'usuari cap a les dades que es manipulen i s'enregistren en el programari de gestió d'empresa. D'aquesta forma, la complexitat del disseny i la quantitat de codi queda molt reduït de cara a plantejar passarel·les en altres CMS com Drupal.

Un tutorial de instal·lació que es pot oferir

1.3 Instal·lació del mòdul/plugin ViaFirma en Joomla

Podem seguir els passos de la instal·lació aquí : http://developers.viafirma.com/instalacion

No podem utilitzar aquests enllaços directes per carregar tant el plugin com el mòdul fent servir els quins hi ha en aquesta pàgina: http://code.google.com/p/viafirma-joomla-client/downloads/list perquè es troben mal empaquetats. Cal descomprimir-los en local i tornar a comprimir la primera subcarpeta que contingui un arxiu XML que és el de configuració.

El plugin i el mòdul d'autenticació de la plataforma de signatura digital escollida no va funcionar a la primera en la versió de Joomla actual

2.1 Funcionament plataforma ViaFirma per integració en Joomla

La integració de la plataforma ViaFirma en Joomla es fa efectiva amb dos extensions:

Mòdul que presenta el butó que redirecciona a la pàgina de ViaFirma.

Plugin que prepara la comunicació amb el servidor OpenID tot direccionant-hi el client, i, un cop la plataforma finalitza el procés d'autentificació, allotjant la informació amb les credencials que envia l'autentificador.

2.2 Tasques a fer

1. Adaptar mòdul i plugin plataforma del Joomla 1.5 (versió antiga) al Joomla 3.0.

   A data del 16 de desembre he aconseguit que el Joomla reculli l'usuari que ViaFirma li retorna després de l'autenticació en la plataforma.

2. En les distribucions de Joomla per sobre de la 1.7 cal dir-li al Joomla que també agafi el comprovador dels paràmetres que reben per Url amb aquesta modificació:

   ```
   diff -r joomla_3.0_modificat/components/com_users/controllers/user.php joomla_3.0_original/components/com_users/controllers/user.php
   30c30
   < JSession::checkToken('post') or JSession::checkToken('get') or jexit(JText::_('JInvalid_Token'));
   ---
   > JSession::checkToken('post') or jexit(JText::_('JInvalid_Token'));
   ```

3. Per les darreres versions no hi ha cap mòdul d'autenticació OpenID que n'aporti les llibreries. He inclòs aquesta llibreria en el plugin de Joomla i ha hagut de canviar aquesta línia del Auth/OpenID/Consumer.php:

   ```
   926,927c924
   < # the parameter return is added anywhere inside the code and avoid the correct authentify process
   < if ($key!="return" && Auth_OpenID::arrayGet($q, $key) != $value) {
   ---
   > if (Auth_OpenID::arrayGet($q, $key) != $value) {
   ```

   D'aquesta forma no dóna error quan es troba aquest paràmetre en les dades que rep de l'autenticació.

Aquest seria un exemple de correu per l'administrador Joomla:

Com que el tema dels usuaris en un servidor és crític, per augmentar la seguretat, millor forçar l'usuari joomla a fer servir SSL . T'he preparat el tema...

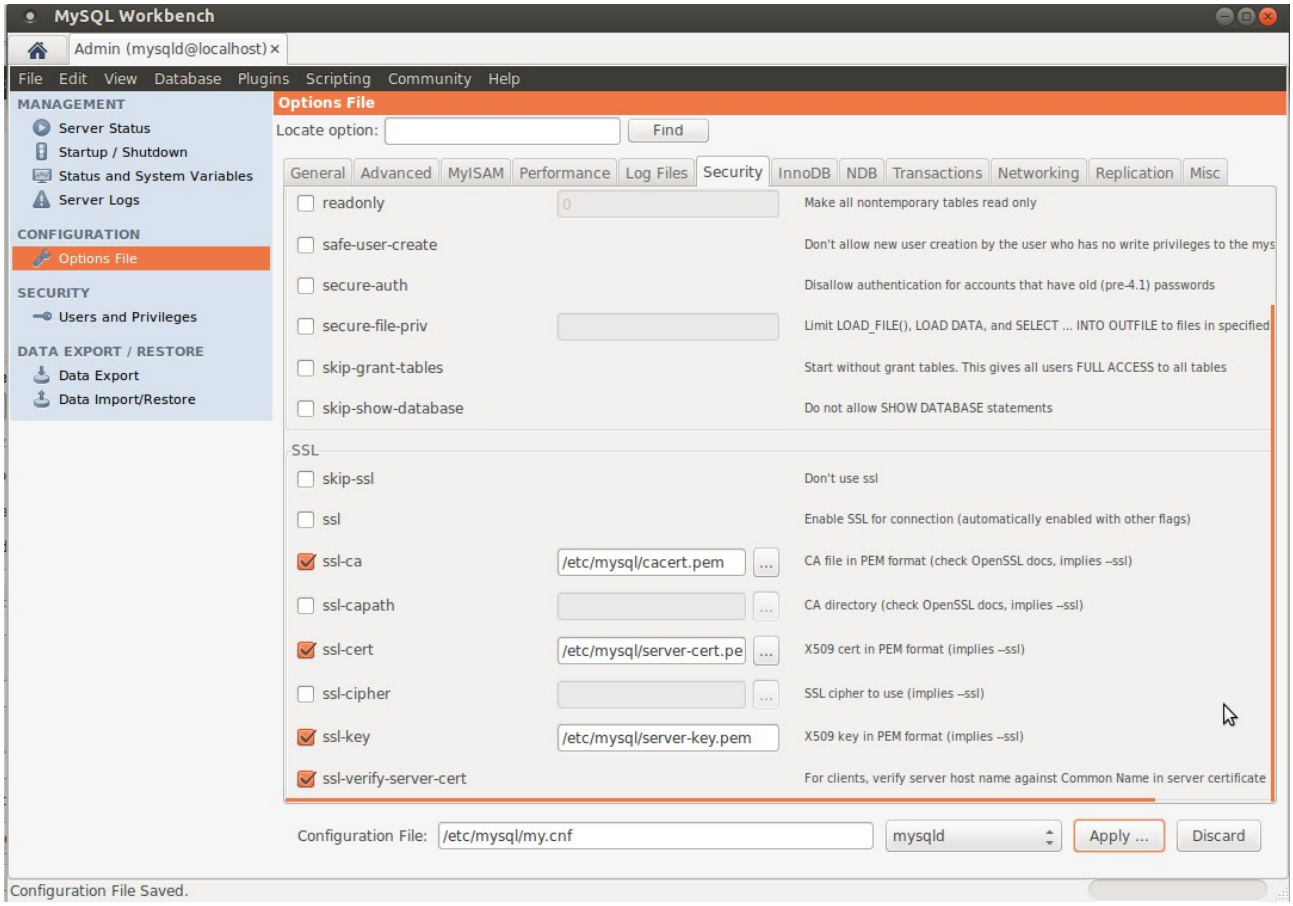
Com veus no li poso password perquè ja autentifico amb el certificat requerit.

```
GRANT ALL PRIVILEGES ON joomla.* TO 'openerp'@'%' IDENTIFIED BY '' REQUIRE SUBJECT '/C=ES/ST=Barcelona/L=Manresa/O=Insti/CN=openerp';
```

Alerta que amb això dones tots els permisos sobre la base de dades joomla.

Et passo els certificats de la CA i del servidor i la clau privada del servidor per si les vols fer servir. Aquestes claus s'han de desar en la carpeta de configuració del MySQL que normalment és la /etc/mysql. Per si vols generar les pròpies et passo un request.

Et passo la pantalla de configuració del servidor en el Mysql-Workbench.



Il·lustració 6: Pantalla de configuració per una connexió segura a un servidor MySQL

El servidor Mysql usa OpenSSL, i per donar com a vàlid el certificat generat per la CA, hem de validar CA en aquest context.

Ens situem en el directori on es guarden els certificats en aquest entorn. En linux normalment es troben en /etc/ssl/certs .

Des d'allí s'ha de fer una comanda per copiar el certificat de la CA amb el nom que corresponent

amb el hash que deriva de la comanda :

```
ln -s /etc/mysql/cacert.pem `openssl x509 -hash -noout -in /etc/mysql/cacert.pem`.0
```

Per confirmar que tenim l'entorn openssl bé podem fer un verify:

```
openssl verify server-cert.pem
```

Naturalment, com a dipositari de la clau privada de la CA estic a disposar per signar els request que m'arribin per canals de confiança.

Una observació més sobre la seguretat d'aquest correu: com que aquests certificats han de treballar en una intranet relativament tancada i controlada, podem passar aquestes claus privades per email.

4 Bug del paquet python mysqldb (en Ubuntu) que no realitza connexions SSL

A l'hora de fer les connexions SSL des del python del OpenERP em vaig trobar amb que no s'establia la connexió.

El detall de l'error resava que la llibreria C no estava compilada amb l'opció SSL. La solució la vaig trobar en la pàgina del bug corresponent allotjat en el repositori oficial:

https://bugs.launchpad.net/ubuntu/+source/python-mysqldb/+bug/1027075

4.1 Compilació de python-mysqdb

Cal seguir les instruccions que es troben en el README del codi font instal·lant les dependències que s'hi detallen o, alternativament, que ens marquen els errors de compilació.

error que no troba mysql-config: solució instal·lar libmysqlclient-dev :

http://stackoverflow.com/questions/7475223/mysql-config-not-found-when-installing-mysqldb-python-interface

error que falta arxiu Python.h : solució instal·lar python-dev :

http://snippets.aktagon.com/snippets/211-How-to-install-and-use-the-mysql-python-library

5 Bug de WEBDAV en el mòdul d'OpenERP

Quan volem fer servir el mount.davfs amb el WEBDAV del mòdul OpenERP ens trobem que dóna l'error següent:

```
XML parse error at line 1: undeclared namespace prefix
```

Amb un capturador de paquets WireShark, solució dràstica perquè no veia la sortida de les opcions de debug, vaig veure que l'XML que envia el servidor WEBDAV de Python era incorrecte perquè apareixia un nom de domini que no es declarava.

La solució que vaig adoptar va ser la d'eliminar aquesta referència al nom de domini inexistent després de comprovar que altres clients WEBDAV no necessitaven aquesta referència.