1148

PROTOCOL DE COMERÇ ELECTRÒNIC BASAT EN SERVEIS WEB

Memòria del Projecte Fi de Carrera
d'Enginyeria en Informàtica
realitzat per
Guillem Llop Vilaltella
i dirigit per
Helena Rifà Pous
Bellaterra, 18 de Juny de 2009

Índex

1.Definició i estudi del problema....3
1.1.Motivació....3
1.2.Plantejament del projecte....3
1.3.Problemàtica existent....4
1.3.1.LSSI....4
1.3.2.LOPD....5
1.3.3.Sistema d'identificació....6
1.3.4.Comunicació....6
1.3.5.Mantenir la privacitat de l'usuari....7
1.4.Objectius generals del projecte....7
1.5.Despeses inicials obligatòries....8
2.Estat de l'art....10
2.1.Exemples reals....10
2.2.Estudi de tecnologies....12
2.2.1.Sistema d'autenticació....13
2.2.2.Llenguatge per a la creació de pàgines web dinàmiques....14
2.2.3.Servidor web....15
2.2.4.Sistema gestor de BBDD....16
2.2.5.Comunicació mitjançant servies web....17
2.2.6.Estàndards d'autenticació basats amb missatges XML....24
2.3.Camí a seguir i estudi d'alternatives i viabilitat....28
2.3.1.Quin és el paper del proveïdor d'identitats?....28
2.4.Planificació....32
3.Anàlisi del sistema....34
3.1.Objectius del sistema....34
3.2.Requeriments d'emmagatzemar informació....37
3.3.Requeriments funcionals....39
3.3.1.Definició dels actors....39
3.3.2.Requeriments funcionals....41
3.4.Requeriments no funcionals....54
4.Disseny del sistema....55
4.1.Model estàtic....55
4.1.1.Model de dades conceptual (Model E-R)....56
4.1.2.Diagrama de classes....57
4.1.3.Model de dades físic....59
4.1.4.Diagrama de casos d'ús....62
4.2.Model dinàmic....65
4.2.1.Diagrames de seqüència dels RF (interacció)....65
4.2.2.Diagrames de seqüència del protocol (interacció)....73
5.Desenvolupament....75
5.1.Eines de desenvolupament software....75
5.2.Eines de desenvolupament hardware....77
5.3.Justificacions a la implementació i solucions a problemes....77
5.4.Funcionalitat (captures)....89
6.Conclusions....103
6.1.Objectius complerts....103

6.2.Possibles millores.....104
6.3.Valoració.....107
7.Bibliografia.....108

1. Definició i estudi del problema

Tot projecte esdevé d'una necessita que s'intenta cobrir. És durant aquest primer apartat on s'explica què és el que mou aquest projecte, com es planteja i donats uns sèrie de problemes que s'han de tenir en compte quins són els grans objectius que s'han d'assolir.
Donada aquesta problemàtica inicial sorgeixen unes despeses inicials obligatòries tant de software com de hardware amb les que s'han de comptar.

1.1. Motivació

Cada cop més apareixen en Internet diferents webs oferint serveis de tot tipus. És possible comprar entrades pel teatre, roba, tecnologia, informació, etc.

Un dels principals atractius de sol·licitar aquests serveis per Internet és que la persona sol·licitant pot conservar el seu anonimat. Un exemple és el sistema usual amb login i contrasenya que no revela l'autèntica identitat de la persona. De totes maneres aquest sistema d'autenticació de persones basat en quelcom conegut (la contrasenya) no és suficient per guanyar la confiança de molts webs que ofereixen serveis. Els interessa un mètode d'autenticació que garanteixi que les persones amb qui tracten siguin qui diuen ser i que siguin de confiança. Mentre que les persones voldran seguir preservant la seva veritable identitat.

1.2. Plantejament del projecte

Es demana buscar una solució al problema plantejat anteriorment que permeti, per una part, mantenir l'anonimat a una persona que sol·licita un servei a un web i garantir, per un altre part, al web que ofereix el servei, que la persona amb qui tracta és qui diu ser i és de confiança.

Per tant s'ha d'implementar un sistema de validació d'usuaris en un entorn web per oferir a

altres webs que ho demanin l'autenticitat i una reputació de les persones sol·licitants dels seus serveis. El sistema que autentiqui a les persones ha de tenir la confiança tant de les persones autenticades com dels web oferidors de serveis. El procediment haurà de ser de manera segura, transparent i que respecti la privacitat les dades personals d'aquestes persones.

A la definició inicial del projecte es demana que la comunicació entre el sistema de validació d'usuaris i els webs que ofereixen els serveis i desitgen autenticar a les persones es faci mitjançant un servei web. També es parla del nou DNI-E com a instrument per acreditar la identitat de les persones i per tant comprovar l'autenticitat d'aquestes.

1.3. Problemàtica existent

Un dels grans problemes d'aquest projecte al tractar amb informació personal, com pot ser el contingut del DNI-E i altres dades que volem gestionar com el de la reputació de l'usuari autenticat, és el de preservar de manera segura aquestes dades. I no és un caprici fer-ho ja que hi ha dos lleis que regulen aquest fet; la LSSI i la LOPD.

1.3.1. LSSI

La LSSI avarca quatre aspectes importants: drets d'autor, marques registrades, transaccions i propietat intel·lectual. També regula que no hi hagi un codi o disseny extret d'altres webs o fonts.

S'ha de fer un repàs exhaustiu de les dades mostrades al web. En cas d'errada s'haurà d'assumir les conseqüències. Passa el mateix amb la publicitat enganyosa i si es treu beneficis directes o indirectes d'aquests mateixos.

Han d'haver clàusules pels usuaris en els formularis indicant que les seves dades es tractaran i manipularan de manera automatitzada però sempre respectant la LOPD. També hauran d'autoritzar l'enviament de propaganda als seus mails. Les condicions del acord han de quedar clares (no ambigües) així com els casos i excepcions a desistiment.

S'ha de fer acceptar una clàusula a l'usuari on s'explica la legislació aplicable corresponent al

nostre país.

Ha de quedar clara, en un comerç electrònic, una secció o plana de forma "quí som" indicant a què es dedica, que fa, la raó social del web, el NIF i contactes (mails, direccions físiques, telèfons, etc per tal de que qualsevol pugui contactar amb ells).

1.3.2. LOPD

És un organisme que protegeix dades de caràcter personal d'informació, numèrica, alfabètica, gràfica, fotogràfica, acústica, susceptible de registre, tractament o transmissió concernent a persones físiques identificades o identificables.

Les dades especialment protegides són corresponents a l'àmbit de la intimitat personal i familiar, i no de la professional. Dades de caràcter personal que revelen:

- Ideologia
- Afiliació sindical
- Religió, creences
- Origen racial
- Salut
- Orientació sexual
- Infraccions penals o administratives

Les dades ofertes han de seguir els principis de qualitat, finalitat, d'exactitud, d'informació i de consentiment.

Es pretén afegir la funcionalitat d'indicar-li al web que interacciona amb el client la reputació de la que disposa. Pensem en un moment què passaria si sortissin a la llum les la informació sobre les diferents reputacions.

Per tant tal com indica la LOPD i la LSSI s'haurà de tenir en compte en que les dades que es manegaran no siguin modificades ni voluntàriament ni involuntàriament, o el que s'anomena preservar la **autenticitat** o bé **integritat** de les dades personals. Per altre banda tampoc es podrà divulgar aquesta informació ja que ha de ser totalment confidencial o com també es

coneix per la **privacitat** de les dades.

1.3.3. Sistema d'identificació

Necessitem un sistema per identificar-se únic i que acrediti la identitat de la persona. En necessitem un que estigui prou divulgat per a que el màxim d'usuaris puguin identificar-se amb ell i ha de ser de prou confiança per a totes les parts. La seguretat i el fet que ens asseguri que l'usuari és qui diu ser i que les dades no siguin alterades també serà un punt igual o més important. El DNI-E, plantejat a la definició inicial del projecte, sembla cobrir aquest problema. Tot i que encara no el té tota la gent, al ser un document d'identitat obligatori, tothom acabarà tenint-ne un.

1.3.4. Comunicació

Hem de pensar a gran escala on moltes webs voldran identificar a persones mitjançant aquest sistema. Cada una d'aquestes webs farà servir una tecnologia de servlet diferent i per sol·licitar l'autenticitat o la reputació d'una persona s'haurà de comunicar amb el web encarregat d'autenticar a persones. Aquest projecte, com a oferidor d'aquest servei d'autenticar a persones, farà servir una tecnologia que no ha de per què ser la mateixa que la dels webs sol·licitants.

El problema està en establir una comunicació comú entre les diferents webs interessades i el web que autentica persones. Aquesta comunicació ha de el més senzilla i segura possible.

La solució a aquest problema és la comunicació a través d'arxius XML mitjançant serveis web com s'explicarà en el següent apartat.

1.3.5. Mantenir la privacitat de l'usuari

Uns dels èxits d'Internet ha estat la privacitat dels usuaris envers els diferents proveïdors de serveis. Podem tenir una identitat però no cal que sigui totalment descriptiva amb la realitat. Podem identificar-nos per diferents portals registrant-nos amb un login i password diferent.

El problema sorgeix quan volem un sistema d'autenticació únic com el que es planteja a l'inici del projecte com és el DNI-E en que hi ha dades personals dels usuaris. Això viola d'alguna manera la filosofia que hi ha fins ara d'Internet. Per lo tant, s'ha de buscar una solució per tal de que l'usuari pugui autenticar-se a un web, mitjançant el DNI-E, i que pugui mantenir la seva privacitat en tot moment.

Així que el resum dels objectius a les problemàtiques existents seran :

- Protecció i seguretat de les dades privades
- Facilitar el comerç a través d'Internet
- Creació d'un sistema accessible a tothom

1.4. Objectius generals del projecte

A grans trets els objectius generals del projecte són:

- Dissenyar i implementar un sistema que permeti a una persona obtenir un producte o servei d'un portal web sempre i quan aquesta persona tingui la reputació suficient.
  - Aquest portal web no haurà de conèixer la identitat del seu client.
  - El portal haurà de verificar l'autenticitat i la reputació del client mitjançant una petició a un servei web d'un proveïdor d'identitats.
- Dissenyar i implementar un proveïdor d'identitats en entorn web que permeti a una persona autenticar-se amb el nou DNI-E.

- Aquest portal haurà de gestionar la reputació acumulada de cada persona.
- Aquest portal haurà d'oferir mitjançant un servei web, l'autenticitat i reputació de les persones als web oferidors de serveis que ho sol·licitin.
- La reputació de les persones haurà d'actualitzar-se en funció dels vots rebuts dels webs que ofereixen serveis mitjançant peticions al servei web.

- Donat que hi ha dades personals pel mig, la seguretat d'aquestes no s'ha de veure compromesa.
- Complir amb la legislació vigent que regula la privacitat de les dades personals en Internet.

1.5. Despeses inicials obligatòries

El projecte necessita una sèrie de materials o suports tecnològics. Aquests són:

- 1x lector de DNI-e
- SW de validació
- 1x equip informàtic
- Allotjament Web
- Servidor Web
- Sistema gestor de BBDD

Aquests són a grans trets les despeses en material que ens farà falta en un futur. Així que aquesta llista pot veure's ampliada més endavant.

Ja es disposa d'un equip informàtic i pel que fa la resta dels elements d'aquesta llista es poden aconseguir de manera fàcil (econòmica) o bé gratuïta. Així que treien del que ja es disposa, un càlcul estimat seria:

- 1x DNI-e 10€
- 1x lector de DNI-e 20€

- SW de validació 0€
- Allotjament Web 0€ - 40€/anuals
- Servidor Web 0€ - 50€
- Sistema gestor de BBDD 0€ - 5.000$

Les variacions de preu són una estimació depenent de la versió i llicència escollida per a cada cas. Però d'això ja se'n parlarà més endavant en els punts d'estudis de productes existents i en el d'estudis d'alternatives i viabilitat.

2. Estat de l'art

Cal fer un estudi de quines són les tecnologies existents, tant a nivell d'implementacions ja funcionant en casos reals i quotidians com de tecnologies software per implementar aquests casos.

La finalitat d'aquest apartat no és més que aquest i de prendre una primera decisió de quin ha de ser el camí a seguir amb una breu justificació. També explicar quins són els objectius a grans trets que crec que es poden assolir amb el temps de que es disposa amb possibles alternatives. L'apartat acaba amb la que serà la planificació per endavant de les dates d'entrega dels diferents objectius.

2.1. Exemples reals

Prenent com a bo el DNI-E com a sistema d'autenticació d'usuaris plantejat a l'inici del projecte s'observa que les aplicacions que utilitzen aquest sistema no són masses degut a la novetat i a la no total distribució del DNI-E. Degut a això aquest tipus d'autenticació corre paral·lelament amb altres sistemes per evitar una baixa accessibilitat al web.

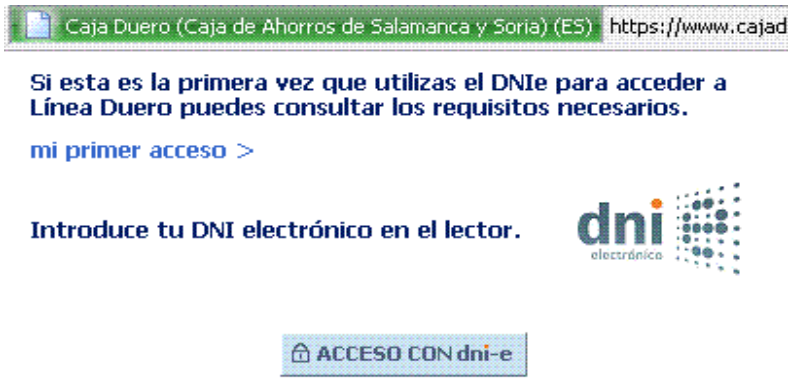
Les primeres implementacions es veuen sobretot en les planes web d'entitats financeres que ofereixen com a possibilitat autenticar-se als seus portals mitjançant el certificat digital que ofereix el nou DNI-E. De totes maneres no s'ha trobat cap aplicació similar amb la funcionalitat de reputació que es pretén implementar per aquest projecte.

Quasi tots els portals que ofereixen la possibilitat funcionen d'una manera molt similar; indiquen de manera molt clara els passos d'inserció del DNI-E al lector i la introducció del pin de la targeta després d'haver premut un botó d'acceptació. Tot això és clar, que amb una comunicació SSL.

El funcionament és bastant fiable i ràpid d'executar i per no deixar amb cap dubte als usuaris s'inclouen molt links d'informació del DNI-E, dels lectors i/o d'exemples de funcionament.

És de suposar que en un futur no molt llunyà aquest mètode d'autenticar s'implantarà més enllà de les entitats financeres degut a la comoditat i a la distribució total del DNI-E.

Unes captures d'exemple:



Imatge 1: exemple real

Faciliten molt la informació a l'usuari per disminuir l'aversió que pot crear el sistema d'autenticació donat a que encara és desconegut per a la major part dels usuaris.

Imatge 2: exemple real

Imatge 3: exemple real

Els formularis d'accés o estan reduïts a la menor expressió demandant per molts casos que només s'introdueixi la tarja al lector.

2.2. Estudi de tecnologies

Tenint en compte l'objectiu general del projecte que es proposa es fa a continuació un petit estudi de les tecnologies, tècniques web de comunicació o el DNI-E com a sistema d'autenticació que han de servir per assolir el projecte.

2.2.1. Sistema d'autenticació

DNI-E

Per a la identificació d'usuaris s'ha optat per mantenir el de la idea inicial de fer-la amb el DNI-E degut a que resol tots els problemes abans plantejats. Com a document d'identitat és obligatori a tota persona amb nacionalitat espanyola, dóna confiança a l'usuari ja que és un document oficial totalment conegut per a tothom i que la acreditació de la identitat de l'usuari està garantida per una Autoritat Certificadora com és la 'Fábrica Nacional de Moneda y Timbre'.

Per tal d'identificar i d'autenticar a un usuari, el nou DNI-E conté un certificat digital en el seu interior que és el que realment l'usuari, de manera transparent a ell, enviarà quan així se li requereixi en algun web.

Certificat digital

És un document digital certificat per una Autoritat Certificadora, pel nostre cas la 'La Fabrica Nacional de Moneda y Timbre' que ens assegura l'autenticitat de l'emissor del certificat.

Aquesta autenticitat es basa amb un sistema criptogràfic de clau asimètrica. On cada una de les parts té un parell de claus; la pública i la privada. La pública la pot conèixer tothom mentre que la privada es manté en privat. La idea és que si una de les parts vol enviar un missatge, xifra aquest missatge amb la clau pública de l'altre. De manera que quan l'altre rebi el missatge, només podrà desxifrar-lo amb la seva clau privada.

La composició del certificat digital és la següent:

$$Cd = A, Pk_A, T, Dsk_A(A, Pk_A, T)$$

A = identificador de l'usuari.

Pk_A = clau pública de l'usuari A.

T = time-stamp únic

Dsk_A = signat digital (associa el document a la identitat de l'usuari) amb la clau privada de la Autoritat Certificadora.

Com veiem en la composició del certificat digital, en aquest es desxifra un duplicat del contingut amb la clau privada de l'emissor. Així que quan l'altre part rebi el certificat, agafarà la clau pública del emissor que hi ha en el certificat i aplicarà un xifrat amb aquesta clau a la part que estava desxifrada. Com que les claus tenen una propietat commutativa, el resultat obtingut serà l'esperat i es comprova la vinculació entre la persona emissora i la seva clau pública.

La tasca de validar el certificat digital així de com el de comprovar de que no estigui en un dels repositoris on es guarda la informació sobre els certificats revocats (CRL), pertany a l'Autoritat Certificadora (autoritat de confiança que assegura l'autenticitat del certificat) i és un servei ofert durant tot l'any.

Aquesta validació es realitzarà mitjançant 'Online Certificate Status Protocol' (OCSP) que un cop feta aquesta petició OCSP sobre l'estat d'un certificat a la Autoritat Certificadora, aquesta consultarà en la seva base de dades per tal de tornar una resposta també OCSP via HTTP sobre l'estat d'aquest certificat. Cal doncs una connexió a Internet per realitzar aquesta comunicació.

2.2.2. Llenguatge per a la creació de pàgines web dinàmiques

Són llenguatges de programació interpretats que s'executen a un servidor web per a la generació de pàgines web dinàmiques en HTML.

PHP

- Està amb llicència GNU i molt extès en el món del desenvolupament web.
- Permet múltiples extensions per generar tot tipus d'arxius, permet connexions a diferents sistemes gestors de bases de dades com: MySQL, Oracle, SQLServer, SQLite i un llarg etc.
- Pot ser executat en Sistemes Operatius com Linux, MacOS o Windows.

ASP

- Ús sota llicència.
- És capaç d'accedir, gràcies al estàndard d'accés a base de dades ODBC, a qualsevol sistema gestor de base de dades.
- Al estar desenvolupat per Windows, ASP corre sobre servidors amb SO Windows amb IIS tot i que existeixen mòduls per a servidors Apache.

JSP

- Desenvolupat per Sun Microsystems i basada en Java.
- Software lliure.
- Té una connexió amb base de dades més eficient per a un nombre alt de peticions gràcies a la seva persistència.
- És multiplataforma degut a la utilització de la màquina virtual Java.

2.2.3. Servidor web

Programa que s'executa contínuament en un servidor que rep peticions de clients sol·licitant respostes en forma de planes web per ser visualitzades als navegadors.

Apache

- Molt utilitzat en el desenvolupament web.
- Ofereix molt de suport amb el mòdul de PHP.
- És software lliure i per tant gratuït
- És multiplataforma.

Tomcat

- Dóna suport de servlets i JSP.
- Desenvolupat per Apache
- És software lliure.
- És multiplataforma.

IIS

- Desenvolupat per Windows.
- Composat per serveis que s'integren al SO Windows per que puguin fer de servidors web.
- Suporta llenguatges per a la generació de planes web com ASP, ASP.NET o PHP
- No és software lliure.
- No és multiplataforma.

2.2.4. Sistema gestor de BBDD

Tots els sistemes gestors de base de dades plantejats treballen amb SQL com a llenguatge tot i que sintàcticament poden haver petites diferències.

MySQL

- És software lliure però pot oferir serveis addicionals a partir de llicència.

- És multiplataforma.

PostgreSQL

- És software lliure i gratuït
- És multiplataforma

SQLServer

- Desenvolupat per Windows.
- És necessària una llicència.
- No és multiplataforma

Oracle

- És necessària una llicència.
- És multiplataforma
- Considerat el més potent.

2.2.5. Comunicació mitjançant servies web

Un servei web és un conjunt de protocols i estàndards necessari per la comunicació i compartiment de dades entre les diferents aplicacions. Com a conjunt de protocols, els serveis web, utilitzen HTTP per enviar missatges XML de manera que aquesta comunicació pugui ser entre aplicacions amb diferents tecnologies i executades en plataformes diferents. Les característiques principals dels serveis web són:

- No estan associats a cap protocol de transport ja que mentre es pugui enviar arxius XML ja els hi val.
- Aprofiten els estàndards existents al mercat i no n'inventa cap de nou. Poden aprofitar el

protocol HTTP.

- La implementació de la API per fer-los servir l'especifica el propi llenguatge amb el que s'estigui treballant i no hi ha un de propi del servei web.

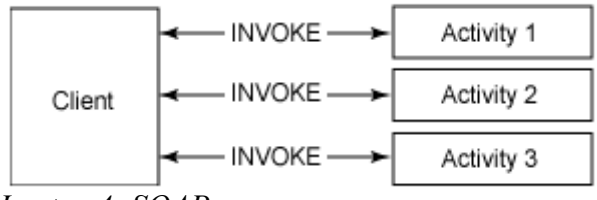
Protocols per comunicar serveis web hi ha uns quants però considerem els més coneguts:

SOAP (Simple Object Access Protocol)

SOAP és un dels primers protocols de comunicació per serveis web en sortir i dels més utilitzats. És una millora del XML-RPC però a l'hora més complex. L'èxit de la seva difusió ha estat que moltes empreses que normalment no col·laboren plegades, com IBM, SUN, Microsystems, Google o Microsoft, donin suport a aquest protocol.

Característiques:

- Pot aprofitar també el protocol SMTP (mitjançant correus) per l'enviament dels documents XML. És a dir, que no està lligat al protocol HTTP
- Més complexe però amb més especificacions (WSDL, UDDI,..)
- Està basat en crides directes a procediments des dels arxius XML
- Gràcies a la seva popularitat i anys en els sector s'ha convertit en un estàndard
- Tota la comunicació es realitza utilitzant POST. Tots els detalls de la petició es troben en el missatge XML.



Imatge 4: SOAP

És un protocol utilitzat en serveis web orientat a “accions” o “activitats” on tenim una operació per a cada activitat. Cada activitat contindrà dintre els recursos automatitzats per la pròpia activitat de manera transparent al client un cop faci la crida a aquesta activitat. Imaginem com a exemple un servei d'un banc per fer una transferència bancària en que un client fa una crida amb SOAP a una funció *transferenciaBancari* que cridarà a una activitat que farà el seguit de crides als diversos intermediaris i recursos (els diners, el banc, etc) que calen per fer aquesta transferència bancària. Per tant, l'usuari no haurà de preocupar-se de tots aquests elements.

Seguretat

En quan a la seguretat dir que SOAP utilitza WS-Security, un protocol desenvolupat per IBM, Microsoft i VeriSign que permet subministrar seguretat a la comunicació en serveis web. WS-Security és una sèrie d'extensions per SOAP situades en la capçalera del missatge XML que permeten l'intercanvi entre client - servidor d'identificadors en forma de 'Tokens' de seguretat. Això, junt amb xifrats i signatures, permet assegurar una autenticació, confidencialitat i integritat respectivament de les operacions realitzades.

Servei de seguretat	Tecnologia	
Integritat	Signatura XML	
Confidencialitat	Xifrat XML	
Autenticitat del emissor SOAP (client)	Tokens	Login i password
		Certificats X509
		Kerberos
		SAML

En WS-Security es poden implementar diferents tipus de seguretat com sistema de clau pública, Kerberos (clau privada) i complementat amb SSL, de manera que depenent de les

necessitats del desenvolupador s'implementarà una o l'altre. Per això es diu que SOAP obliga al programador a controlar la majoria dels aspectes de la seguretat.

Recordem que el protocol SSL procura també integritat, confidencialitat i autenticitat del servidor (poden fer també de part del client).

XML-RPC

XML-RPC va ser el primer mecanisme per invocar procediments remots via XML. És una tecnologia precedent a SOAP. És molt simple i fàcil de fer servir. Això és un punt favorable ja que no requereix de cap enteniment per part del client però a l'hora no hi ha tantes especificacions i ja es considera una tecnologia substituïda per SOAP, que és més robusta.

Aquesta consideració es per diferents raons, però les resumiré en dues:

La primer es deu a que XML-RPC al contrari de SOAP no conté WSDL, un XML específic que descriu les funcionalitats, així com els formats del missatges necessaris per interaccionar amb el servei web. XML-RPC necessita, donada aquesta mancança, conèixer amb anterioritat les funcions residents al servidor, a més de conèixer el llenguatge amb el que està fet; cosa que amb WSDL s'aïlla aquest fet.

La segona raó és l'absència de UDDI. UDDI tracta un catàleg de negocis en Internet ("e-Business") per concentrar i publicar serveis web en un directori centralitzat. Per lo tant, si es disposa d'un servei web, és possible la seva publicació en un director UDDI per tal de que el servei web sigui descobert en aquest directori centralitzat conegut.

Per lo tant, l'absència d'aquestes especificacions li resta flexibilitat i escalabilitat respecte a SOAP.

Per aquest fet es desestima fer servir XML-RPC.

Rest (Representational State Transfer)

Rest és diferencia amb SOAP en que és un protocol en que el principal són els recursos i no els procediments en que cada recurs està identificat amb una URI. Aquests recursos estan en una interfície comú on estaran els procediments per un conjunt de tipus per a la

comunicació entre client - servidor.

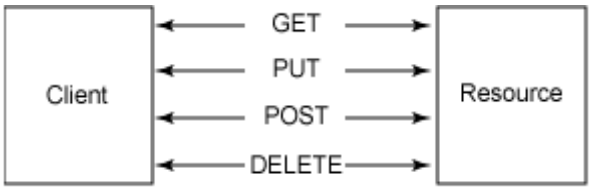
És utilitzat per empreses com Google o especialment Yahoo, Amazon, eBay o Flikr i està de moda en Webs 2.0 per la seva facilitat per la comunicació.

Rest està lligat al protocol HTTP i les operacions que es poden fer servir són les definides per l'especificació HTTP:

- GET: per a fer consultes.
- PUT: per crear un recurs.
- POST: per a modificacions o també per la creació de recursos. També es podran fer consultes amb aquesta operació.
- DELETE: per eliminar els recursos.

Característiques:

- Comença a ser molt popular ja que facilita la programació al cient ideal per aplicacions lleugeres que s'executen al navegador
- És més simple i flexible
- No és un estàndard
- Funciona només pel protocol HTTP



Imatge 5: Rest

S'ha de pensar a un equivalent al funcionament de SQL per accedir a una base de dades; un client fa diferents peticions a un sistema gestor de base de dades i rep les conseqüents respostes. Per això es diu que REST dóna al servei web una orientació a "recursos" en que el client interacciona amb un recurs amb diferents operacions. Un exemple són les peticions en sistemes de blogs on els usuaris demanen certes informacions, modifiquen, esborren sobre un mateix recurs.

Seguretat

La seguretat en REST pot ser tan segura com li permeti el protocol HTTP degut a que es basa en les seves especificacions. Per tant la seva seguretat seran les típiques de HTTP: Basic, Digest, NTLM, Certificats SSL, SSL, etc.

Apart s'ha de dir que amb REST els recursos queden mapejats en un espai comú per lo que es poden aplicar polítiques d'accés amb llistes de control d'accés (ACLs) on guardar els privilegis segons els recursos a on es vulgui accedir. També es pot restringir a nivell de mètodes que es poden utilitzar (GET, POST, etc).

L'administrador també pot observar els diferents accessos als logs del servidor web o bé la podrà utilitzar firewalls.

No es fan servir ni cookies ni variables de sessió per lo que s'elimina tota la problemàtica de robatoris de sessions. Per suplantar però la carència de gestió d'usuaris, alguns opten per la implantació d'un sistema amb tokens però fent vulnerable el sistema per la raó anterior.

Les vulnerabilitats de REST són les típiques d'HTTP:

- Injecció HTML (XSS)
- Injecció SQL
- Autenticació dèbil
- Cross Site Request Forgery (CSRF) (XSRF)

Pel que fa a l'autenticació la millor opció és la d'utilitzar certificats SSL que a més aporten integritat i xifrat a les dades. El problema és que autenticarà als usuaris però no als processos per el que es pot ser fàcilment víctima de CSRF, que és el principal problema de seguretat que té REST. Per evitar això s'ha de tornar a mirar un sistema d'identificadors amb tokens negociats amb el client per cada operació sensible de manera que el token no pugui ser obtingut per terceres persones. Es pot arribar a xifrar o signar el token per a millorar la seguretat.

Com es pot observar es pot obtenir una seguretat amb major control per part de l'administrador i del programador. Tot i així estem parlant de mesures addicionals que cal tenir en compte. Aquestes són mesures que milloren la seguretat de REST per fer-la tant segura com permeti HTTP. El problema es que ningú a dedicat temps a estandarditzar aquestes mesures a REST i per tant és feina que cal fer per arribar a aquesta seguretat teòrica.

2.2.6. Estàndards d'autenticació basats amb missatges XML

SAML

SAML (*Security Assertion Markup Language*) és un estàndard que es basa en XML per l'intercanvi de dades d'autenticació, mitjançant missatges SOAP sobre HTTP entre entitats no relacionades com un proveïdor d'identitat i un altre de servei. Proveeix un protocol d'emissió d'assercions (documents XML que contenen informació relativa a l'usuari com, de quina manera ha estat autenticat i opcionalment atributs sobre la seva identitat) entre autoritat i tercers i defineix un conjunt de perfils que simplifiquen SSO (autenticat un sol cop) a través d'Internet.

D'aquesta manera el protocol aporta amb les seves assercions:

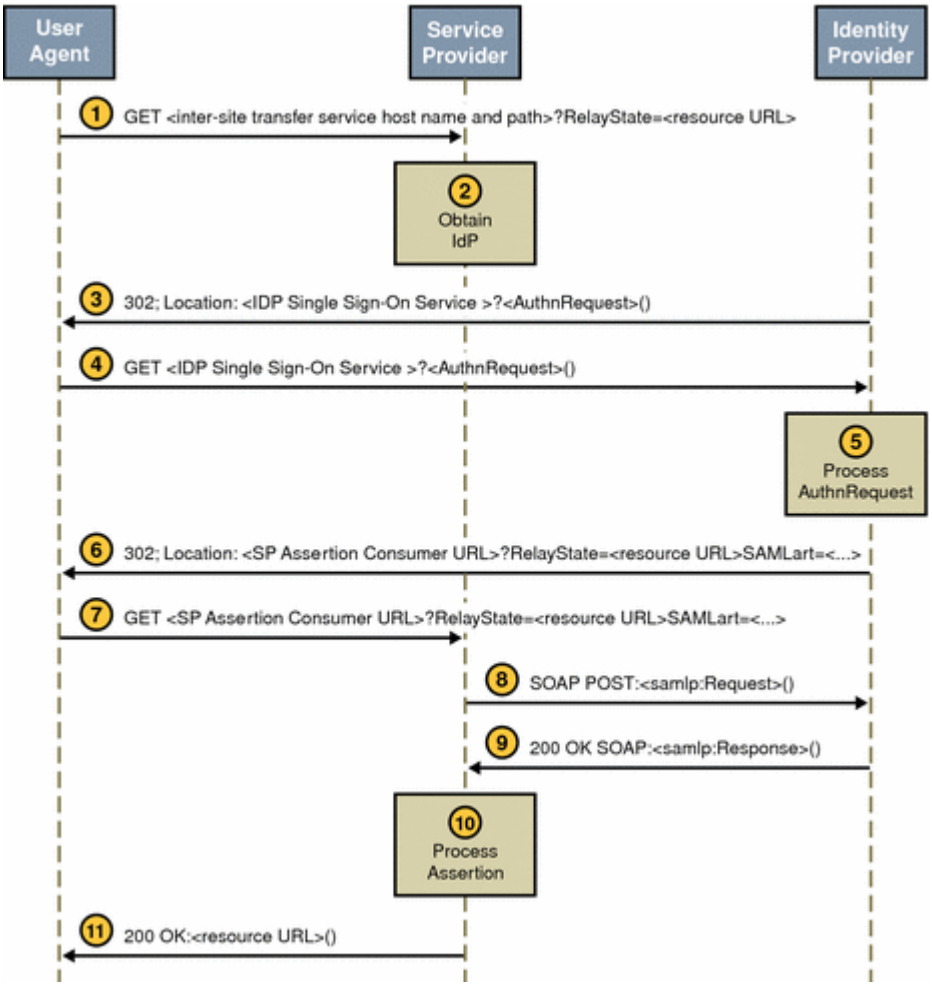
- Autenticació: indica si el usuari a estat autenticat i de quina manera.
- Autorització: procés amb el qual s'autoritza a un usuari a accedir a un servei determinat.
- Atribució: associa a un usuari determinats atributs (privilegis, categories, etc).

Aquestes característiques vindran representades en les assercions mitjançant diferents etiquetes XML específiques per l'autenticació, autorització i atribució integrades en missatges SOAP (Imatge 8: integració de SAML amb SOAP).
Hi ha dos possibles perfils per SAML que defineixen de quina manera s'incrusten i s'extreuen aquestes assercions durant el protocol:

- Perfil “Browser artifact”
- Perfil “Browser POST”

Els dos es fan via HTTP i suporten SSO (“Single sign-on”) (amb un sol cop que s'autentiqui ja li valdrà per a tots els proveïdors de servei) però cada un d'ells té els seus avantatges i inconvenients.

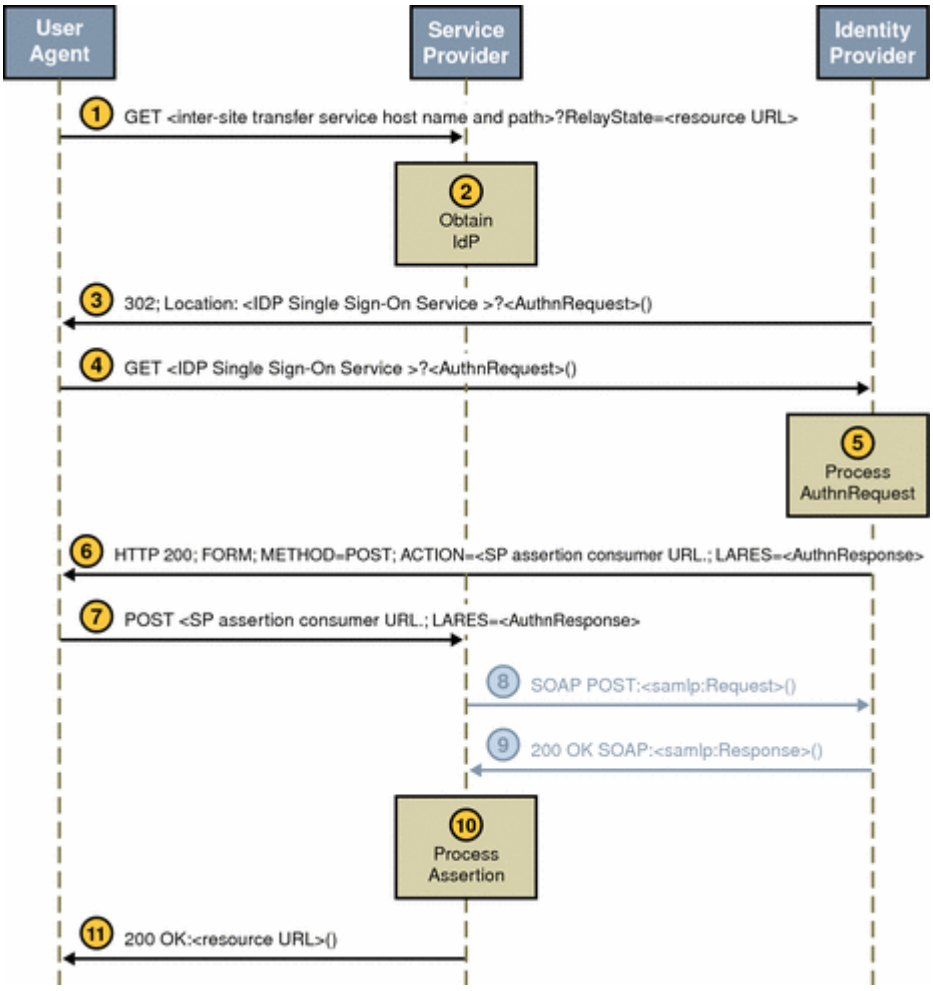
Per una banda el perfil "Browser artifact" insereix un "artefacte" o identificador associat a una asserció en el navegador (URL) de la persona un cop autenticada de manera que cada vegada que la persona entri en un proveïdor de servei, aquest agafarà l'identificador i preguntarà per la asserció al proveïdor d'identitats.



El proveïdor d'identitats és el que realitza l'autenticació de la persona i la que genera el identificador de l'asserció SAML que guardarà en el seu servidor. Com veiem un cop el proveïdor de serveis agafi l'identificador farà una petició SOAP al proveïdor d'identitats (amb autenticació bàsica o mitjançant autenticació amb certificat tot per SSL per autenticar a l'hora al proveïdor de servei). Aquesta petició sol·licitarà mitjançant l'identificador la asserció de la persona en concret.

Pel que fa el perfil "Browser POST" les assercions són carregades directament al navegador

de la persona i aprofita la seguretat amb POST amb SSL amb l'asserció signada per enviar la asserció a cada proveïdor de servei.



Imatge 7: diagrama de seqüència del perfil "Browser POST"

Aquí el proveïdor d'identitats també autentica a la persona i crea la asserció corresponent però posa la asserció al navegador de la persona. Per aquest perfil com veiem no és necessària la petició per SOAP de la asserció ja que la persona ja la porta al “damunt”.

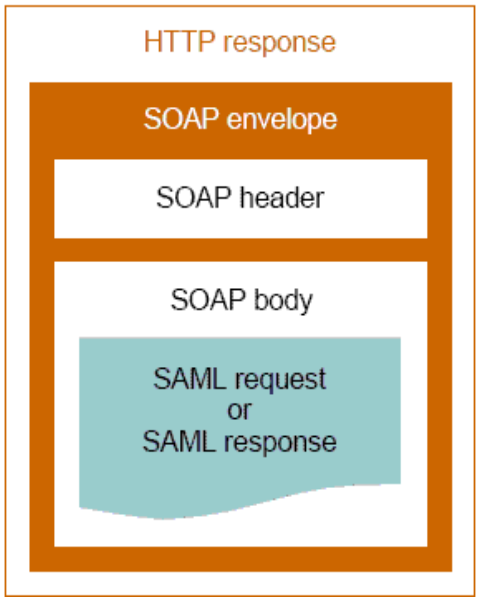
Pels dos casos serà el proveïdor de servei el que un cop rebuda la asserció o bé per part del proveïdor d'identitat o bé pel navegador de la persona qui decidirà si accepta o no l'usuari en funció del seu criteri de seguretat. Ha de ser ell que ha de confiar amb el sistema d'autenticació que s'ha fet servir (que explica l'asserció) i amb les dades relacionades associades a la persona (autoritzacions i atribucions).

També cal dir que la privacitat de la persona sempre preval ja que tant l'identificador del primer perfil com les dades de l'asserció no coincideixen amb les dades reals de la persona fent servir tokens aleatoris o pseudònims. Així la persona pot demostrar que és qui diu ser sense donar-se realment a conèixer qui és.

El perfil "Browser artifact" està considerat més segur que el "Browser artifact" apart de tenir un processament menor degut a que no hi ha signat en les assercions i funciona per navegadors amb el JavaScript desactivat. El perfil "Browser artifact" té l'avantatge de tenir menys problemes amb els "firewalls", s'assoleix amb menys passes i sobrecarrega menys al servidor del proveïdor d'identitats degut a que no hi ha peticions SOAP.

Amb SAML 2.0, la última versió, ja no només depenem de fer servir SOAP com a protocol d'enviament però sí que és un molt bon complement per aprofitar tota la lògica de SAOP. En les imatges Imatge 9: capçalera WSS i Imatge 8: integració de SAML amb SOAP veiem un resum dels XML de SAML integrats a SOAP.

Imatge 9: capçalera WSS



Imatge 8: integració de SAML amb SOAP

2.3. Camí a seguir i estudi d'alternatives i viabilitat

Un projecte amb tants aspectes, solucions possibles, plantejaments diferents pot portar-se a terme de moltes maneres. Crec preferible plantejar-lo bé i amb un estat funcional que pugui ser ampliat en un futur.

És important entendre tots els problemes que van sorgint i trobar quina és la millor manera de solucionar-los degut a que la naturalesa del problema implica treballar amb diferents fronts i les solucions podran ser distintes. Per això trobo necessari fer un estudi i poder definir la viabilitat de cadascuna de les solucions.

2.3.1. Quin és el paper del proveïdor d'identitats?

Per què un proveïdor de servies com per exemple un comerç electrònic qualsevol decidirà comunicar-se amb un proveïdor d'identitats com a intermediari per autenticar a un usuari i no fer-ho directament?

En primer lloc perquè no haurà d'implementar la lògica de comunicació si ja hi ha algú que proporciona de manera fàcil i especialitzada la funcionalitat d'autenticar usuaris. El proveïdor d'identitats podrà rebre tot tipus de peticions de tot tipus de webs (programats en diferents llenguatges) demanant que autentifiquem als seus usuaris.

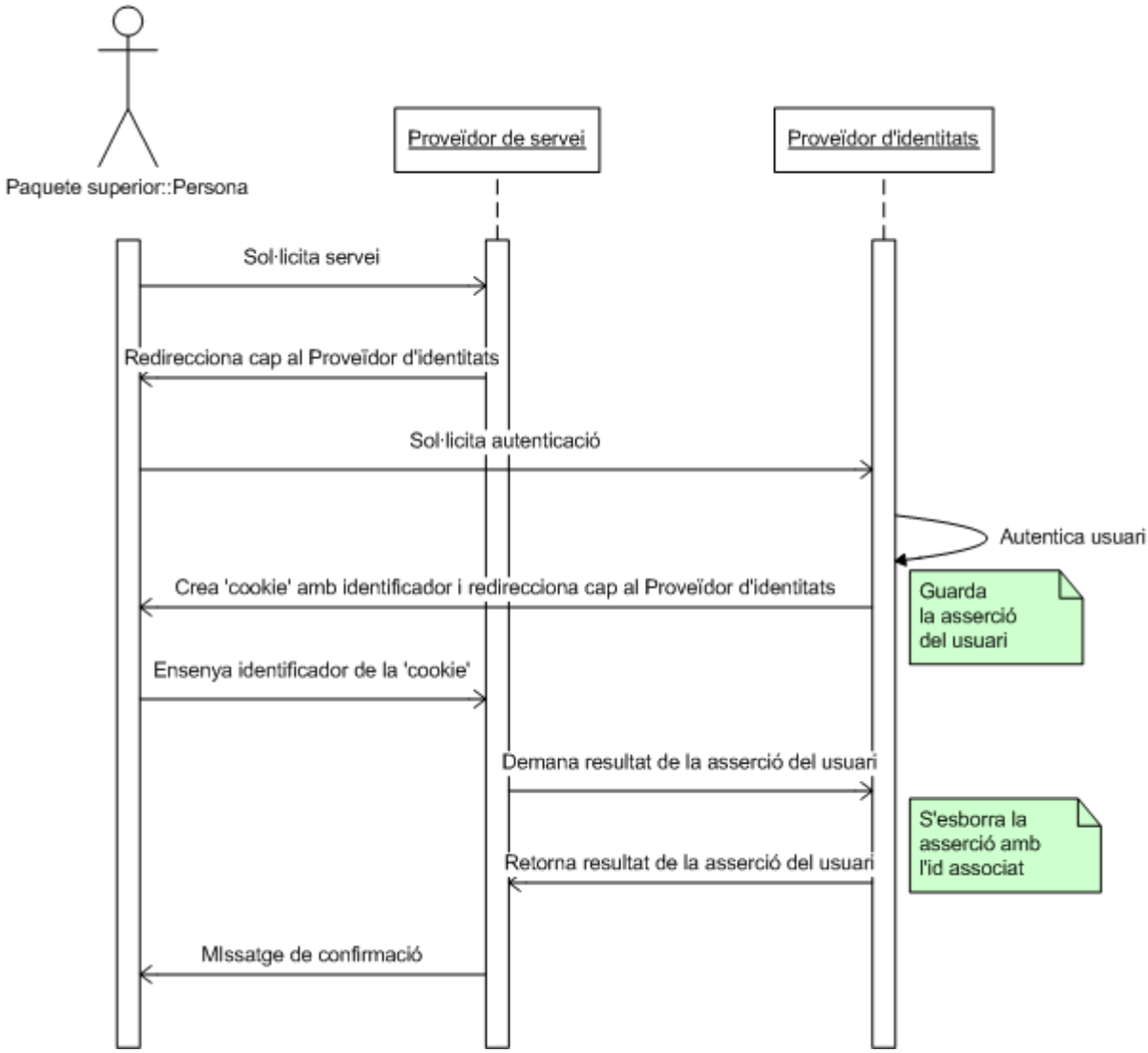
En segon lloc perquè dóna uns valors afegits com a proveïdors d'identitat. Aquest valor es basen en que el proveïdor d'identitats tindrà una base de dades prou potent amb el pas del temps que permetrà mesurar d'alguna manera la reputació acumulada d'un usuari (equivalent al que seria les atribucions en SAML).

El proveïdor d'identitats té un compromís tant explícit com implícit de que no farà ús fraudulent i sense permís de les dades personals de cada persona autenticada (LSSI i LOPD). La figura pròpia del proveïdor d'identitats ha de proporcionar serietat ja que és la seva principal imatge de marca.

Per altre banda i potser més important, és el fet que en Internet, una persona pugui autenticar-se però no cal que la seva veritable identitat sigui descoberta. Això amb una autenticació amb el DNI-E no es pot donar, ja que al ser un document oficial hi ha dades d'identitat personals. Aquest fet pot donar aversió a un usuari a l'hora d'autenticar-se per exemple a un comerç electrònic. I és aquí on el paper del proveïdor d'identitats, com a intermediari, dóna un valor afegit donat que serà el que tracti amb les dades de la persona a autenticar i no el proveïdor de servei. Aquesta no és més que la filosofia que predica SAML.

Seguint aquestes premisses, aquest projecte pretén seguir la filosofia que predica SAML (S'ha produït un error: No s'ha trobat la font de referència i Imatge 6: diagrama de seqüència del perfil "Browser artifact") aplicant d'una manera similar el protocol i l'ordre de comunicació entre el proveïdor de serveis i el d'identitats. La raó per implementar un sistema similar com el perfil “Browser artifact” de SAML és perquè compleix exactament amb el que es proposa al projecte des d'un principi; preservar la veritable identitat de les persones però garantir als proveïdors de serveis la autenticitat d'aquestes. A part de donar més seguretat que l'altre perfil proposat per SAML, el “Browser POST”.

Hi ha molts models a seguir per la implementació d'una comunicació que compleixi els trets descrits anteriorment. La lògica a seguir després de varis models s'ha inspirat com es deia amb el perfil “Browser artifact” de SAML i l'ordre de comunicació serà la següent:



Imatge 10: seqüència de camí a seguir

La idea és que el proveïdor de servei mai manegui les dades d'autenticitat de la persona ja que en una primera versió (i al contrari de lo que indica SAML) el proveïdor de servei era el que adquiria el certificat de la persona i l'enviava al proveïdor d'identitats. Aquesta idea no va tirar endavant ja que qui ens asseguraria que el proveïdor de servei no arribaria mai a esbrinar les dades personals que es troben al certificat? Per això s'ha proposat que sigui el proveïdor d'identitats l'únic que agafi directament el certificat d'autenticació i es guardi la resposta d'autenticat (asserció) tornant com a resposta lo mínim necessari per confirmar al proveïdor de servei que la persona és qui diu ser i la reputació.

Un cop feta l'autenticació per part de la persona interessada, el proveïdor de servei li ha de donar mitjançant una 'cookie' amb caducitat un identificador únic amb el qual es pugui presentar als diferents proveïdors de serveis que han contractat a aquest proveïdor d'identitats .

S'ha pensat d'aquesta manera perquè a la persona autenticada no li calgui cada vegada sol·licitar que l'autentiquin. La 'cookie' ja contindrà un identificador amb el que cada proveïdor de servei podrà comprovar, un cop agafat, l'autenticitat de la persona mitjançant una petició via servei web al proveïdor d'identitats. El proveïdor d'identitats haurà de guardar una relació de les assercions amb l'identificador associat.

D'aquesta manera la persona interessada en ser autenticada mantindrà el seu anonimat front al proveïdor de servei al haver un proveïdor d'identitats que fa d'intermediari. El proveïdor de servei també es beneficia d'aquests sistema degut a que una persona confiarà més amb un portal que es dedica de manera especialitzada a aquest tipus de tasca (autenticar a persones compromesa a no divulgar cap dada persona com indica la LOPD).

Cal fer aquestes altres consideracions:

- Les tecnologies per a la implementació dels portals es faran amb PHP, MySQL i Apache degut a que s'entenen molt bé entre elles, són gratuïts (http://www.php.net/license/), hi ha molt de suport al darrera i el rendiment dels tres plegats ha estat més que contrastat al ser la principal tecnologia aplicada a entorns web.
- L'autenticació es farà mitjançant al certificat emès pel DNI-E degut a que és un document comú a tothom, oficial i obligatori en l'estat espanyol. Estalvia d'aquesta manera molts problemes de falta d'adquirir un certificat per part de la persona a autenticar-se.
- La comunicació entre ambdós es produirà mitjançant missatges XML (servei web) i la seva corresponent seguretat. Aquesta comunicació es farà amb SOAP afegint capçaleres WS – Security i si cal SSL. La raó degut a que és estàndard, permet afegir de manera modular seguretat (integritat, confidencialitat i autenticitat i és pot llançar tranquil·lament per una comunicació SSL per complementar) i tot i que és més complexe que altres tecnologies, permet més especificacions com WSDL (descriu una interfície pública pels Serveis Web i

facilitaria la implementació als proveïdors de serveis).

- A més el proveïdor d'identitats gestionarà un sistema de reputacions de les persones autenticades al portal per oferir més informació als diferents proveïdors de serveis que ho sol·licitin. Aquests últims hauran de poder actualitzar aquesta reputació segons ho creguin convenient establin un altre comunicació mitjançant servei web amb el proveïdor d'identitats. De moment s'ha pensat en un comptador que s'incrementi per cada vot positiu i es decrementi per cada negatiu.

2.4. Planificació

A grans trets el que es vol aconseguir és resoldre la problemàtica inicial existent que es planteja en el apartat anterior cobrint els Objectius generals del projecte. A partir d'aquest punt és poden implementar millores escalables a la solució inicial.

Per tant, plantejo fer en primer lloc la implementació estàtica dels dos portals web: el proveïdor de servei i el proveïdor d'identitats. Tot seguit pretenc dedicar-me al que és el DNI-E i al certificat digital que conté dins per autenticar via el lector de targetes. Un cop autentiqui a persones vull establir una comunicació SOAP amb un servei web entre les dues parts. Després afegiré dinamisme als portals, inserint, modificant, eliminant, etc en la base de dades allà on calgui i afegiré tota la lògica i funcionalitat a la part d'administració del proveïdor d'identitats i a la comunicació entre els portals web. Arribat a aquest punt cal implementar seguretat al protocol de comunicació i si hi ha temps afegiré millores allà a on es cregui convenient.

Proposo les següents dades de planificació per a la implementació del projecte:

1. **Del 20-12-2008 al 5-01-2009** Implementar un petit portal simulant un proveïdor de servei.

2. **Del 5-01-2009 al 10-02-2009** Implementar un petit portal corresponent al proveïdor d'identitats. Dissenyar el que serà el 'backoffice' per gestionar les futures persones autenticades amb les corresponents reputacions.

3. **Del 10-02-2009 al 16-02-2009** Instal·lació del 'firmware' del lector de targetes de DNI-e com dels 'drivers' pel SO utilitzat per accedir a les dades d'autenticació.

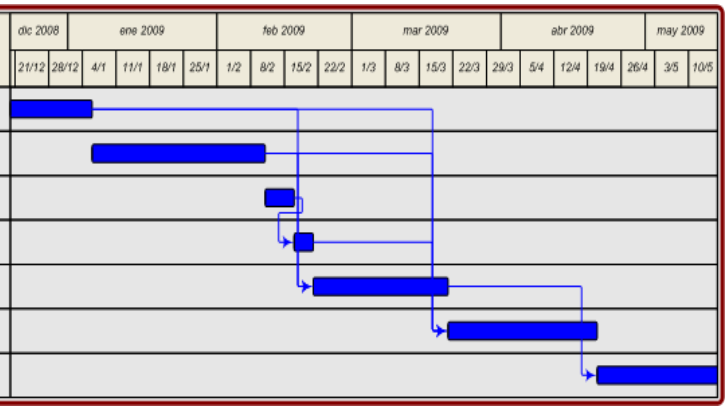
4. **Del 16-02-2009 al 20-02-2009** **A**utenticar-me amb el lector de targetes i el DNI-e amb una petició a la fàbrica de moneda i timbre.

5. **Del 20-02-2009 al 20-03-2009** Comunicació i servei web entre el proveïdor d'identitats i el proveïdor de serveis.

6. **Del 20-03-2009 al 20-04-2009** Crear lògica amb base de dades inclosa al proveïdor de servei, al proveïdor d'identitats i a la comunicació apart de les funcionalitats del 'bakoffice' per fer seleccions, modificacions i eliminacions d'entrades de la base de dades.

7. **Del 20-04-2009 al 15-05-2009** Implementació de seguretat a la comunicació del servei web.

Id.	Nombre de tarea	Comienzo	Fin	Duración
1	Implementar proveïdor de servei	20/12/2008	05/01/2009	17d
2	Implementar proveïdor d'identitats i disseny del backoffice	06/01/2009	10/02/2009	36d
3	Instal·lació drivers del DNI-E i accedir al certificat	11/02/2009	16/02/2009	6d
4	Proves d'autenticació amb el DNI-E	17/02/2009	20/02/2009	4d
5	Comunicació i servei web entre el PS i PI	21/02/2009	20/03/2009	28d
6	Dinamisme als portals i lògica del backoffice del PI	21/03/2009	20/04/2009	31d
7	Seguretat en les comunicacions i servei web	21/04/2009	15/05/2009	25d



3. Anàlisi del sistema

Després de fer l'estudi sobre les tecnologies existents i definits uns objectius desitjats de que es volen assolir, estructuraré i nombraré en taules ja d'una manera precisa tots i cadascun dels objectius del sistema. A partir d'aquests objectius i dels actors que interaccionaran amb el sistema esdevenen la resta d'apartats com són els requeriment d'emmagatzemar informació o els requeriments funcionals. Al final i de manera breu també es llisten els requeriments no funcionals.

3.1. Objectius del sistema

OBJ - 01	**Autenticar a persones amb el DNI - E**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com
Descripció	Mitjançant un lector de targetes, l'entorn a de ser capaç de validar i autenticar el certificat que conté el DNI – E.
Importància	Vital
Urgència	Immediata
Comentaris	L'objectiu inclou la petició OCSP, instal·lació de drivers pel lector, autenticació mútua amb SSL i gestió de les respostes (assercions).

OBJ - 02	**Gestionar les persones autenticades**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com
Descripció	Les persones que ja s'han autenticat al portal quedaran enregistrades de manera anònima.
Importància	Important
Urgència	Immediata
Comentaris	S'inclou la lògica de reputació vigent d'una persona.

OBJ - 03	**Gestionar els proveïdors de serveis**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com
Descripció	Es tindran un seguit de dades per autenticar i per altres funcions als serveis que vulguin contactar amb el providentitats.com
Importància	Important
Urgència	Immediata
Comentaris	Cap

OBJ - 04	**Implementació / Comunicació Servei Web**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com / restaurant.com
Descripció	Servei Web que donarà la reputació de les persones demanades i actualitzarà les reputacions a petició dels proveïdors de serveis.
Importància	Vital
Urgència	Immediata
Comentaris	S'inclou la descripció de la comunicació (núm. de paràmetres, funcions, etc) amb WSDL i la seguretat de les dades amb la comunicació.

OBJ - 05	**Oferir servei**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	restaurant.com
Descripció	Pel cas del restaurant oferir un formulari de reserva de taula. L'usuari haurà estat autenticat i haurà de tenir una reputació suficient.
Importància	Important
Urgència	Immediata
Comentaris	Cada proveïdor de servei ofereix un servei diferent.

OBJ - 06	**Gestió d'usuaris**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com / restaurant.com
Descripció	Tant pel providentitats.com com pel restaurant.com caldran tenir un formulari per poder accedir a una zona d'administració.
Importància	Important
Urgència	Immediata
Comentaris	Cap.

3.2. Requeriments d'emmagatzemar informació

RI - 01	**Informació sobre les persones**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com
Objectius associats	OBJ - 02 Gestionar les persones autenticades
Descripció	El sistema haurà d'emmagatzemar la informació corresponent a les persones autenticades en providentitats.com. En concret:
Dades específiques	• Número de sèrie del DNI-E xifrat amb “sha1” • Data en la que s'ha donat d'alta • Reputació acumulada
Interval temporal	Passat i present
Importància	Important
Urgència	Immediata
Comentaris	Remarcar que no es guarda el nom de la persona ni cap altre dada privada.

RI - 02	**Informació sobre els proveïdors de identitat**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com
Objectius associats	OBJ - 03 Gestionar els proveïdors de serveis
Descripció	El sistema haurà d'emmagatzemar la informació corresponent als proveïdors d'identitats que han contractat providentitats.com. En concret:
Dades específiques	• Nom del proveïdor de servei • Data en el que s'ha donat d'alta • Indicador de si el proveïdor de servei està actiu o no • IP del servidor d'on està allotjat el proveïdor se servei • Domini del proveïdor de servei • Contrasenya que l'autentica
Interval temporal	Passat i present

Importància	Important
Urgència	Immediata
Comentaris	Les contrasenyes estaran generades per el providentitats.com.

RI - 03	**Informació sobre els usuaris**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com / restaurant.com
Objectius associats	OBJ - 06 Gestió d'usuaris
Descripció	El sistema haurà d'emmagatzemar la informació corresponent als usuaris que es vulguin identificar en la zona d'administració. En concret:
Dades específiques	• Login d'usuari • Contrasenya d'accés • Indicador de si el proveïdor de servei està actiu o no • Nivell d'administrador • Data de creació
Interval temporal	Passat i present
Importància	Important
Urgència	Immediata
Comentaris	Cap.

3.3. Requeriments funcionals

3.3.1. Definició dels actors

ACT - 01	**Persona**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	restaurant.com / providentitats.com
Descripció	Persona interessada en el servei ofert pel proveïdor se servei que ha d'autenticar-se amb el DNI - E
Comentaris	Navegant d'Internet interessat amb un servei ofert d'un portal.

ACT - 02	**Administrador restaurant.com**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	restaurant.com
Descripció	Administrador encarregat de gestionar la part administrativa del portal restaurant.com.
Comentaris	Com a tal haurà de tenir l'usuari i password corresponent.

ACT - 03	**Administrador providentitats.com**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com
Descripció	Administrador encarregat de gestionar la part administrativa del portal providentitats.com.
Comentaris	Com a tal haurà de tenir l'usuari i password corresponent.

ACT - 04	**Superadministrador providentitats.com**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	providentitats.com
Descripció	Superadministrador encarregat de gestionar la part administrativa del portal restaurant.com a part de funcionalitats addicionals reservades pel Superadministrador.
Comentaris	Com a tal haurà de tenir l'usuari i password corresponent.

3.3.2. Requeriments funcionals

Hi ha requeriments funcionals que no s'han afegit en el llistat de requeriments funcionals degut a que considero que no són tant importants ni vitals per a la consecució del projecte. Aquests són els requeriments que sorgeixen dels objectius associats a gestió d'usuaris. Tot així sí que estan implementats i es mostren en l'apartat Funcionalitat (captures).

RF - 01	**Autenticar persona**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com	
Objectius associats	OBJ - 01 Autenticar a persones amb el DNI - E	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan la persona s'autentica.	
Precondició	La persona haurà de tenir un lector de targetes, els drivers corresponents instal·lats i un DNI – E.	
Seqüència normal	**Pas**	**Acció**
	1	La persona sol·licita al sistema començar el procés d'autenticar-se.
	2	El sistema sol·licita el pin del DNI - E per iniciar l'autenticació.
	3	La persona proporciona el pin del DNI - E al sistema.
	4	El sistema sol·licita escollir entre el certificat d'autenticació o el de signat.
	5	La persona escull el certificat d'autenticació.
	6	El sistema autentica a la persona.
	7	El sistema insereix la persona a la base de dades si no existeix.
Postcondició	La persona ha estat autenticada.	
Excepcions	**Pas**	**Acció**
	1	El sistema no detecta cap certificat de part de la persona.
	3	El sistema no dóna com a bo el pin proporcionat per la persona.

	4	El sistema només reconeix un certificat.
	6	El sistema no dóna com a bona l'autenticació.
	7	El sistema no insereix a la persona a la base de dades degut a una mala autenticació.
Rendiment	**Pas**	**Quota de temps**
	2	0,5 - 2 segons
	6	2 - 5 segons
	7	0,5 - 1 segons
Freqüència esperada	50 vegades / hora	
Importància	Vital	
Urgència	Immediata	
Comentaris	La quota de temps en el pas 6 dependrà molt de l'estat de la línia en aquell moment així com les peticions concurrents.	

RF - 02	**Llistar persones autenticades**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com	
Objectius associats	OBJ - 02 Gestionar les persones autenticades	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan l'administrador o el superadministrador de providentitats.com ho creguin convenient.	
Precondició	Les persones hauran d'estar donades d'alta al sistema.	
Seqüència normal	**Pas**	**Acció**
	1	L'administrador o el superadministrador realitza el cas d'ús RF – 12 (s'identifica com a tal).
	2	El administrador o el superadministrador de providentitats.com sol·licita al sistema començar el procés de llistar persones.
	3	El sistema llista a les persones autenticades que es troben en la base de dades.
Postcondició	Les persones han estat llistades.	
Excepcions	**Pas**	**Acció**
	3	No hi ha persones en la base de dades.
Rendiment	**Pas**	**Quota de temps**
	3	0,5 - 1 segons
Freqüència esperada	5 vegades / dia	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 03	**Modificar persona autenticada**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com	
Objectius associats	OBJ - 02 Gestionar les persones autenticades	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan el superadministrador de providentitats.com ho creguin convenient.	
Precondició	La persona haurà d'estar donada d'alta al sistema.	
Seqüència normal	**Pas**	**Acció**
	1	El superadministrador realitza el cas d'ús RF – 12 (s'identifica com a tal).
	2	El superadministrador de providentitats.com sol·licita al sistema començar el procés de modificar persones.
	3	El sistema sol·licita les noves dades de la persona seleccionada: reputació.
	4	El superadministrador de providentitats.com proporciona les dades requerides al sistema.
	5	El sistema modifica les dades de la persona de la base de dades.
Postcondició	La persona ha estat modificada.	
Excepcions	**Pas**	**Acció**
	4	El sistema detecta que les dades inserides no són correctes.
Rendiment	**Pas**	**Quota de temps**
	5	0,5 - 1 segons
Freqüència esperada	1 vegada / dia	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 04	**Eliminar persona autenticada**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com	
Objectius associats	OBJ - 02 Gestionar les persones autenticades	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan el superadministrador de providentitats.com ho cregui convenient.	
Precondició	La persona haurà d'estar donada d'alta al sistema.	
Seqüència normal	**Pas**	**Acció**
	1	El superadministrador realitza el cas d'ús RF – 12 (s'identifica com a tal).
	2	El superadministrador de providentitats.com sol·licita al sistema començar el procés de eliminar la persona.
	3	El sistema demana confirmació per a procedir en la eliminació de la persona seleccionada.
	4	El superadministrador accepta la confirmació d'eliminació.
	5	El sistema elimina a la persona de la base de dades.
Postcondició	La persona ha estat eliminada.	
Excepcions	**Pas**	**Acció**
	4	El superadministrador no accepta la confirmació d'eliminació.
Rendiment	**Pas**	**Quota de temps**
	5	0,5 - 1 segons
Freqüència esperada	1 vegada / dia	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 05	**Llistar proveïdors de serveis**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com	
Objectius associats	OBJ - 03 Gestionar els proveïdors de serveis	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan l'administrador o el superadministrador de providentitats.com ho creguin convenient.	
Precondició	Els proveïdors de serveis hauran d'estar donats d'alta al sistema.	
Seqüència normal	**Pas**	**Acció**
	1	L'administrador o el superadministrador realitza el cas d'ús RF – 12 (s'identifica com a tal).
	2	El administrador o el superadministrador de providentitats.com sol·licita començar el procés de llistar els proveïdors se serveis.
	3	El sistema llista a els proveïdors de serveis que es troben en la base de dades.
Postcondició	Els proveïdors de serveis han estat llistats.	
Excepcions	**Pas**	**Acció**
	3	No hi ha proveïdors de serveis en la base de dades.
Rendiment	**Pas**	**Quota de temps**
	3	0,5 - 1 segons
Freqüència esperada	5 vegades / dia	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 06	**Inserir proveïdor de servei**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com	
Objectius associats	OBJ - 03 Gestionar els proveïdors de serveis	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan l'administrador o el superadministrador de providentitats.com ho creguin convenient.	
Precondició	Cap.	
Seqüència normal	**Pas**	**Acció**
	1	L'administrador o el superadministrador realitza el cas d'ús RF – 12 (s'identifica com a tal).
	2	El administrador o superadministrador de providentitats.com sol·licita al sistema començar el procés d'inserir proveïdors de servei.
	3	El sistema sol·licita les següents dades per inserir el nou proveïdor de servei: reputació: nom, flag d'actiu, IP, domini i contrasenya.
	4	El administrador o superadministrador de providentitats.com proporciona les dades requerides al sistema.
	5	El sistema insereix el proveïdor de servei en la base de dades.
Postcondició	El proveïdor de servei ha estat inserit en la base de dades.	
Excepcions	**Pas**	**Acció**
	4	El sistema detecta que les dades inserides no són correctes.
Rendiment	**Pas**	**Quota de temps**
	5	0,5 - 1 segons
Freqüència esperada	1 vegada / setmana	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 07	**Modificar proveïdor de servei**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com	
Objectius associats	OBJ - 03 Gestionar els proveïdors de serveis	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan l'administrador o el superadministrador de providentitats.com ho creguin convenient.	
Precondició	El proveïdor de servei haurà d'estar donada d'alta al sistema.	
Seqüència normal	**Pas**	**Acció**
	1	L'administrador o el superadministrador realitza el cas d'ús RF – 12 (s'identifica com a tal).
	2	El administrador o superadministrador de providentitats.com sol·licita al sistema començar el procés de modificar proveïdor de servei.
	3	El sistema sol·licita les noves dades del proveïdor de servei seleccionat: nom, data de creació, flag d'actiu, IP, domini i contrasenya.
	4	El superadministrador de providentitats.com proporciona les dades requerides al sistema.
	5	El sistema modifica les dades del proveïdor de servei de la base de dades.
Postcondició	El proveïdor de servei ha estat modificat de la base de dades.	
Excepcions	**Pas**	**Acció**
	4	El sistema detecta que les dades inserides no són correctes.
Rendiment	**Pas**	**Quota de temps**
	5	0,5 - 1 segons
Freqüència esperada	1 vegades / mes	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 08	**Eliminar proveïdor de servei**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com	
Objectius associats	OBJ - 03 Gestionar els proveïdors de serveis	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan l'administrador o el superadministrador de providentitats.com ho creguin convenient.	
Precondició	El proveïdor de servei haurà d'estar donada d'alta al sistema.	
Seqüència normal	**Pas**	**Acció**
	1	L'administrador o el superadministrador realitza el cas d'ús RF – 12 (s'identifica com a tal).
	2	El administrador o superadministrador de providentitats.com sol·licita al sistema començar el procés de eliminar el proveïdor de servei.
	3	El sistema demana confirmació per a procedir en la eliminació del proveïdor de servei seleccionat.
	4	El superadministrador accepta la confirmació d'eliminació.
	5	El sistema elimina al proveïdor de servei de la base de dades.
Postcondició	El proveïdor de servei ha estat eliminat de la base de dades.	
Excepcions	**Pas**	**Acció**
	4	El superadministrador no accepta la confirmació d'eliminació.
Rendiment	**Pas**	**Quota de temps**
	5	0,5 - 1 segons
Freqüència esperada	1 vegades / mes	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 09	**Demanar reputació de persona**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com / restaurant.com	
Objectius associats	OBJ - 04 Implementació / Comunicació Servei Web	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan l'administrador del proveïdor de servei ho cregui convenient.	
Precondició	El proveïdor de servei haurà d'estar donat d'alta al sistema. La persona haurà d'estar donada d'alta al sistema.	
Seqüència normal	**Pas**	**Acció**
	1	L'administrador realitza el cas d'ús RF – 12 (s'identifica com a tal).
	2	L'administrador del restaurant.com sol·licita la reputació d'una persona.
	3	El sistema autentica al proveïdor de servei.
	4	El sistema retorna la reputació de la persona demanada.
Postcondició	La reputació de la persona ha estat retornada.	
Excepcions	**Pas**	**Acció**
	2	El sistema detecta que les dades enviades no són correctes.
	3	El sistema no autentica al proveïdor de servei.
	4	El sistema no troba a la persona inserida en la base de dades.
Rendiment	**Pas**	**Quota de temps**
	4	1 – 3 segons
Freqüència esperada	50 vegades / hora	
Importància	Vital	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 10	**Actualitzar reputació de persona**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	providentitats.com / restaurant.com	
Objectius associats	OBJ - 04 Implementació / Comunicació Servei Web	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan l'administrador del proveïdor de servei ho cregui convenient.	
Precondició	El proveïdor de servei haurà d'estar donat d'alta al sistema. La persona haurà d'estar donada d'alta al sistema.	
Seqüència normal	**Pas**	**Acció**
	1	L'administrador realitza el cas d'ús RF – 12 (s'identifica com a tal).
	2	L'administrador del restaurant.com sol·licita actualitzar la reputació d'una persona.
	3	El sistema autentica al proveïdor de servei.
	4	El sistema modifica la reputació de la persona.
Postcondició	La reputació de la persona ha estat actualitzada de la base de dades.	
Excepcions	**Pas**	**Acció**
	2	El sistema detecta que les dades enviades no són correctes.
	3	El sistema no autentica al proveïdor de servei.
	4	El sistema no troba a la persona inserida en la base de dades.
Rendiment	**Pas**	**Quota de temps**
	4	1 – 3 segons
Freqüència esperada	50 vegades / hora	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 11	**Reservar taula**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	restaurant.com	
Objectius associats	OBJ - 05 Oferir servei	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan la persona ho cregui convenient.	
Precondició	La persona haurà d'estar autenticada.	
Seqüència normal	**Pas**	**Acció**
	1	La persona sol·licita al sistema començar el procés de fer una reserva.
	2	El sistema sol·licita les següents dades per efectuar la reserva: dia i hora, nom de la reserva i nombre de persones.
	3	La persona proporciona les dades requerides al sistema.
	4	El sistema insereix la persona a la base de dades.
Postcondició	La persona ha efectuat una reserva.	
Excepcions	**Pas**	**Acció**
	3	El sistema detecta que les dades inserides no són correctes.
Rendiment	**Pas**	**Quota de temps**
	4	0,5 – 1 segons
Freqüència esperada	2 vegades / hora	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

RF - 12	**Identificar usuari**	
Versió	V 1.0	
Autors	Guillem Llop Vilaltella	
Fonts	restaurant.com / restaurant.com	
Objectius associats	OBJ - 06 Gestió d'usuaris	
Descripció	El sistema haurà de comportar-se tal com es descriu en el següent cas d'ús concret quan l'usuari ho cregui convenient.	
Precondició	L'usuari haurà d'estar registrada en la base de dades.	
Seqüència normal	**Pas**	**Acció**
	1	L'usuari sol·licita al sistema començar el procés d'identificar-se.
	2	El sistema sol·licita les següents dades per efectuar la identificació: Login i password.
	3	L'usuari proporciona les dades requerides al sistema.
	4	El sistema identifica al usuari segons les entrades que hi ha en la base de dades.
Postcondició	L'usuari ha estat identificada.	
Excepcions	**Pas**	**Acció**
	3	El sistema detecta que les dades inserides no són correctes.
Rendiment	**Pas**	**Quota de temps**
	4	0,5 – 1 segons
Freqüència esperada	2 vegades / hora	
Importància	Important	
Urgència	Immediata	
Comentaris	La quota de temps dependrà molt de l'estat de la línia en aquell moment.	

3.4. Requeriments no funcionals

RNF – 01	**Entorn de treball**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	restaurant.com / providentitats.com
Objectius associats	--
Descripció	El sistema funcionarà en un entorn d'un PC Pentium Core 2 Quad 2,5 Ghz amb 4 GB de RAM i 300 GB de disc dur amb sistema operatiu Windows XP. Haurà de tenir connexió a Internet per tal de poder fer les comunicacions OCSP.
Importància	Vital
Urgència	Immediata
Comentaris	Com entorn de treball s'entén l'entorn de desenvolupament amb servidor local per a desenvolupar més ràpidament.

RNF – 02	**Còpies de seguretat**
Versió	V 1.0
Autors	Guillem Llop Vilaltella
Fonts	restaurant.com / providentitats.com
Objectius associats	--
Descripció	El sistema haurà d'incorporar algun mecanisme que permeti realitzar còpies de seguretat de les dades emmagatzemades.
Importància	Vital
Urgència	Immediata
Comentaris	Com entorn de treball s'entén l'entorn de desenvolupament amb servidor local per a desenvolupar més ràpidament.

4. Disseny del sistema

Un cop tenim tots els requeriments i llistats d'actors desitjats comencem amb el disseny, que com veurem per alguns apartats del disseny s'hereta del que s'ha definit durant l'anàlisi.

S'ha separat l'apartat en dos grans subapartats: el model estàtic i el model dinàmic.

Pel que fa el estàtic i degut que s'ha de tenir dos portals (recordem que són el proveïdor de servei i el proveïdor d'identitats) es mostra el model de dades conceptual, el diagrama de classes i el model físic per cada un dels dos webs. No s'ha fet una separació tant explícita pels diagrames de casos d'ús degut a que es llisten en funció dels objectius del sistema proposats en l'apartat d'anàlisi del sistema. Recordo que cada requeriment funcional apunta a un objectiu i és amb els diagrames de casos d'ús a on es veuen els diferents actors interaccionant amb aquest conjunt de requeriments funcionals amb el mateix objectiu com a propòsit.

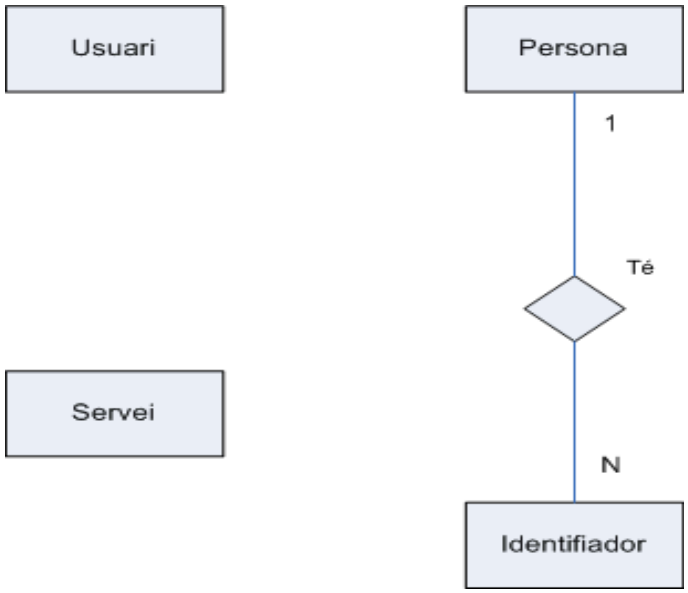
I pel que respecta al model dinàmic es llisten els diagrames de seqüència on podem veure quin és l'ordre dels missatges i accions d'una manera més tècnica que als requeriments funcionals als quals cada diagrama de seqüència fa referència.

4.1. Model estàtic

Degut a que no es un projecte de gestió, tant el model de dades conceptual, el diagrama de classes i el model físic es mostren tant senzills. No ha calgut emmagatzemar més informació ni fer-ho, per aquests requeriments, més complexe.

4.1.1. Model de dades conceptual (Model E-R)

providentitats.com

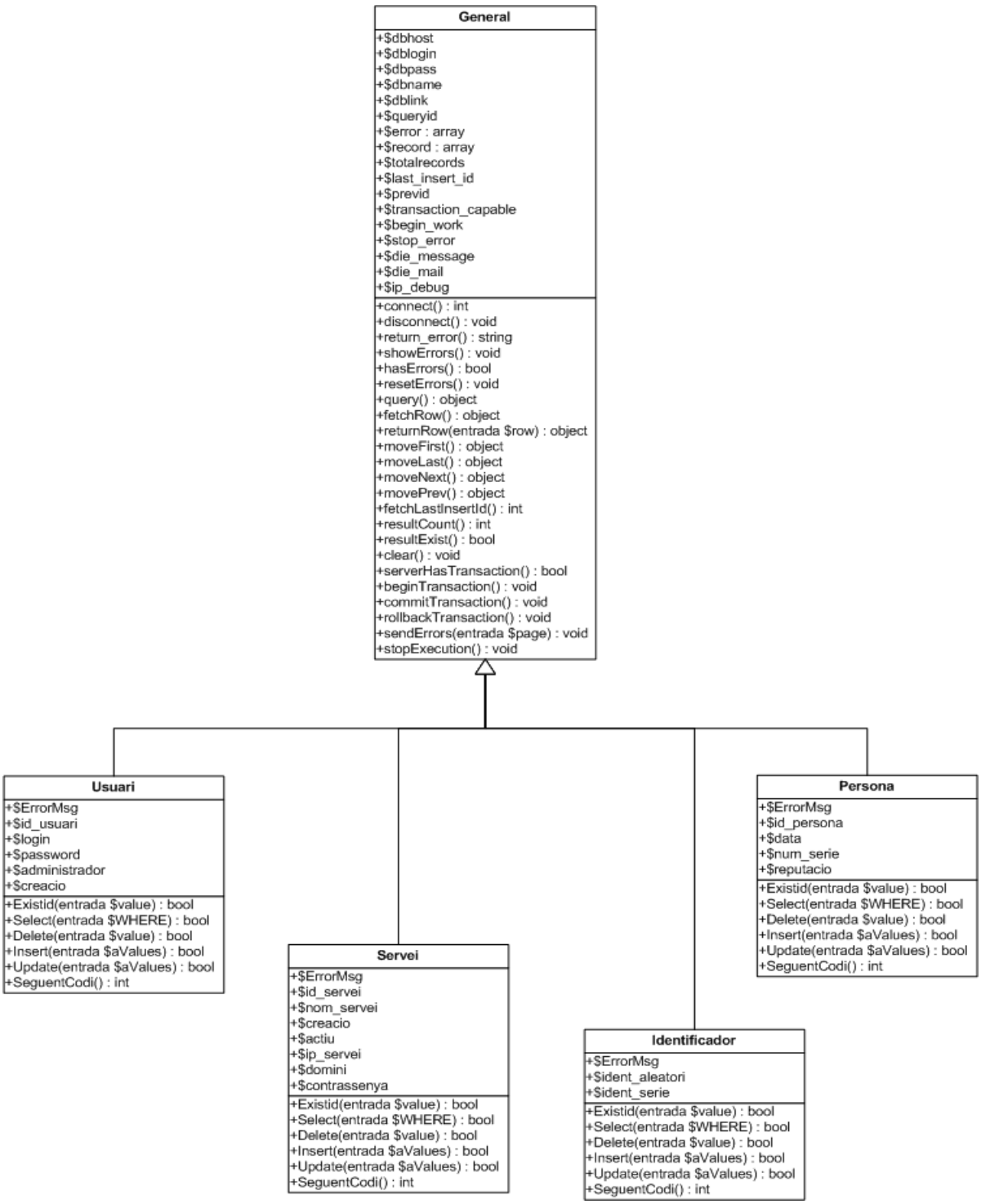


restaurant.com

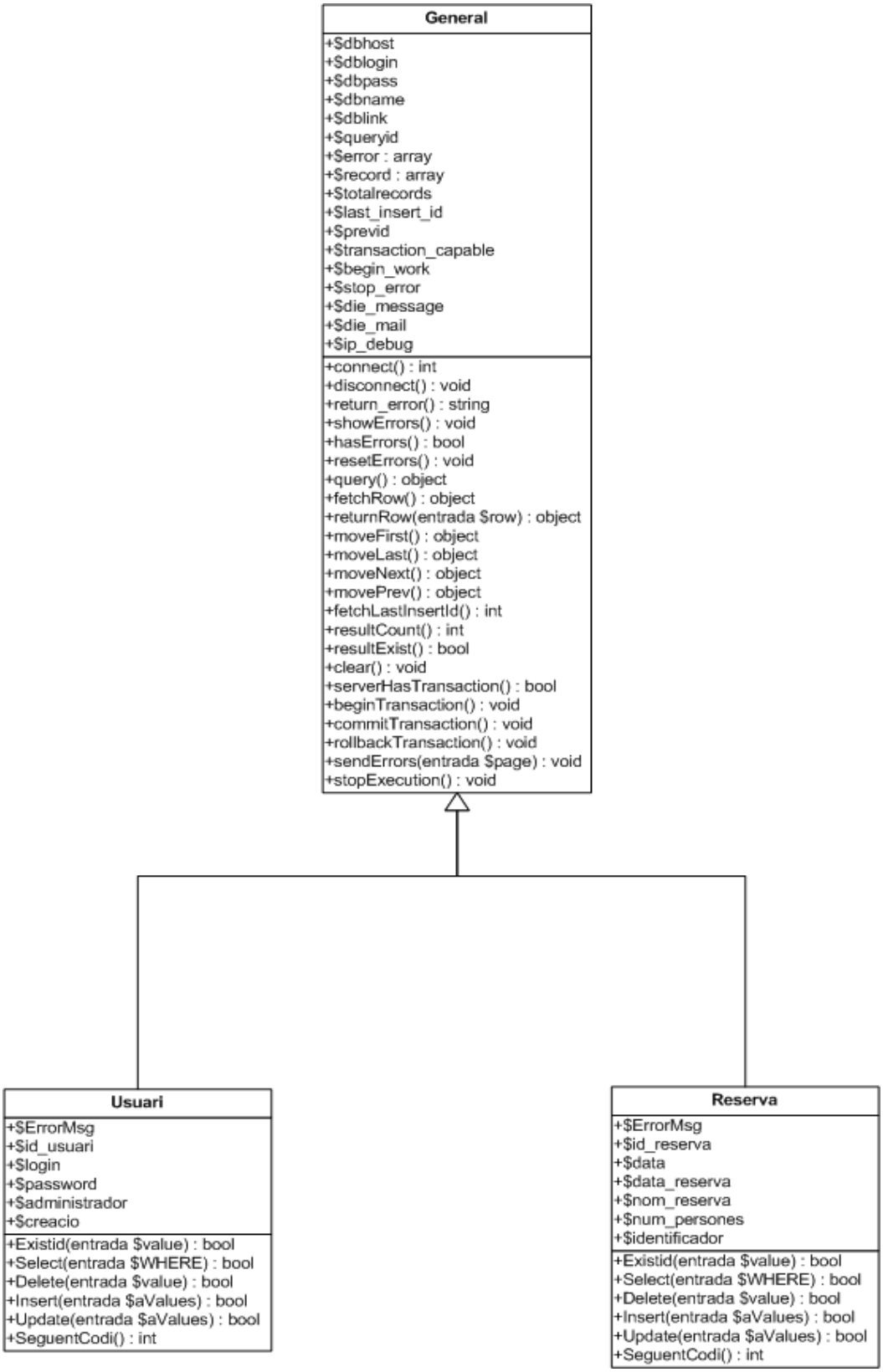
Imatge 13: Model de dades conceptual del proveïdor de servei

4.1.2. Diagrama de classes

providentitats.com



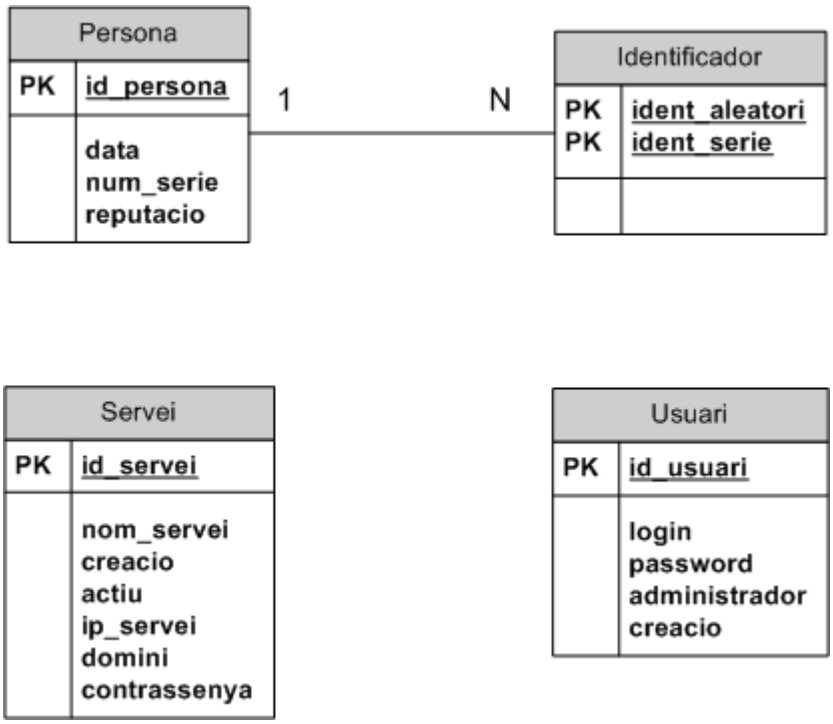
restaurant.com



Imatge 15: diagrama de classes del proveïdor de servei

4.1.3. Model de dades físic

providentitats.com



El que relaciona la taula Persona amb la taula Identificador (Imatge 16: model de dades físic del proveïdor d'identitats) és el num_serie que en la taula Identificador correspon a ident_serie. És una relació de 1 a N. Aquest identificador no és més que el nombre de serie del DNI-E de la persona un cop aplicat un SHA1.

La finalitat de la taula Identificador no és més que tenir un mapeig d'aquest nombre de serie amb un identificador aleatori que se li dóna a una persona autenticada.

Persona

Camp	Tipus	Nul	Extra
id_persona	int(11)	no	auto_increment
data	date	no	
num_serie	varchar(100)	no	
reputacio	int(10)	no	

Identificador

Camp	Tipus	Nul	Extra
ident_aleatori	varchar(100)	no	
ident_serie	varchar(100)	no	

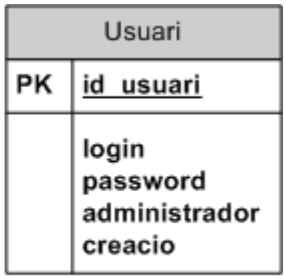
Servei

Camp	Tipus	Nul	Extra
id_servei	int(11)	no	auto_increment
nom_servei	varchar(50)	no	
creacio	date	no	
actiu	int(11)	no	
ip_servei	varchar(20)	no	
domini	varchar(200)	no	
reputacio	varchar(200)	no	

Usuari

Camp	Tipus	Nul	Extra
id_usuari	int(11)	no	auto_increment
login	varchar(50)	no	
password	varchar(200)	no	
admnistrador	tinyint(11)	no	
creacio	date	no	

restaurant.com



Reserva

Camp	Tipus	Nul	Extra
id_reserva	int(11)	no	auto_increment
data	datetime	no	
data_reserva	varchar(150)	no	
nom_reserva	varchar(50)	no	
num_persones	int(2)	no	
identificador	varchar(150)	no	

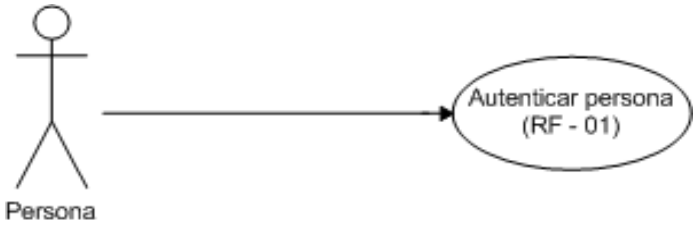
Usuari

Camp	Tipus	Nul	Extra
id_usuari	int(11)	no	auto_increment
login	varchar(50)	no	
password	varchar(200)	no	
admnistrador	tinyint(11)	no	
creacio	date	no	

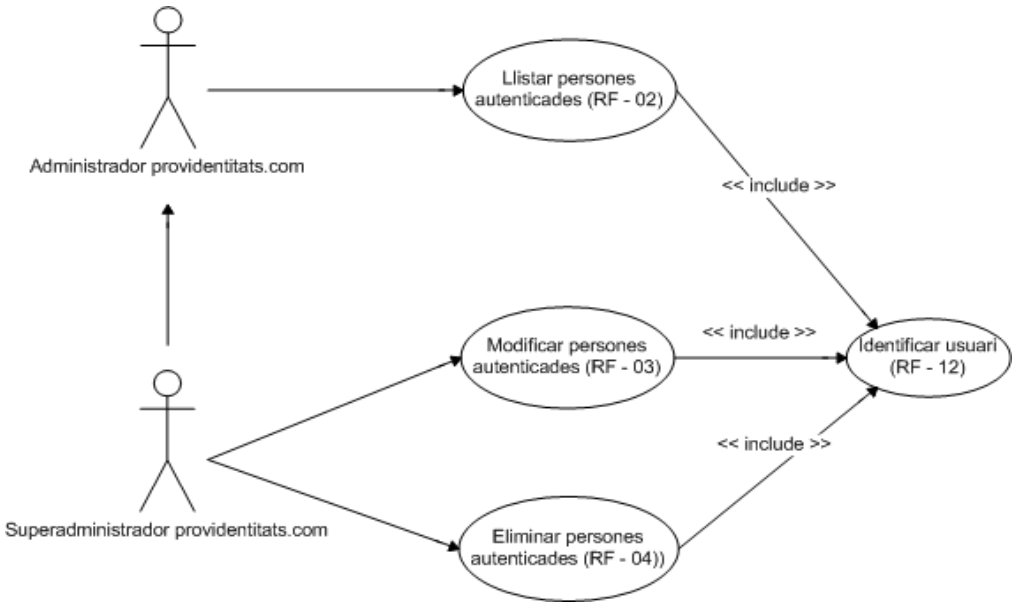
4.1.4. Diagrama de casos d'ús

A continuació es mostren els casos d'ús associats als actors anteriorment presentats interaccionant amb els diferents requeriments funcionals.

Casos d'us del paquet autenticar a persones amb el DNI – E



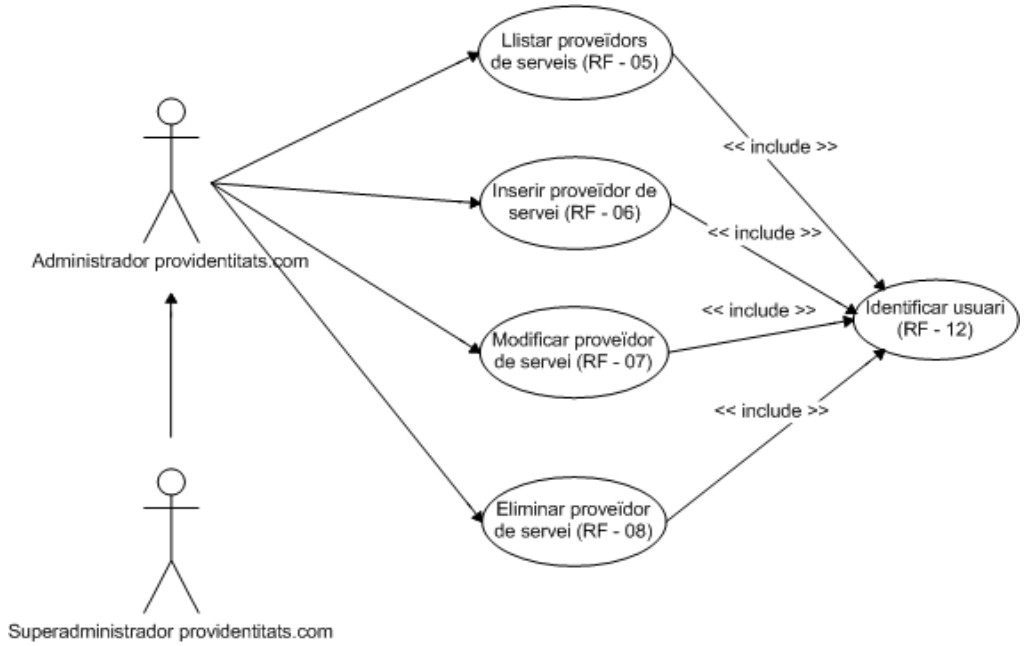
Casos d'us del paquet gestionar les persones autenticades



Imatge 19: cas d'ús de l'objectiu gestionar les persones autenticades

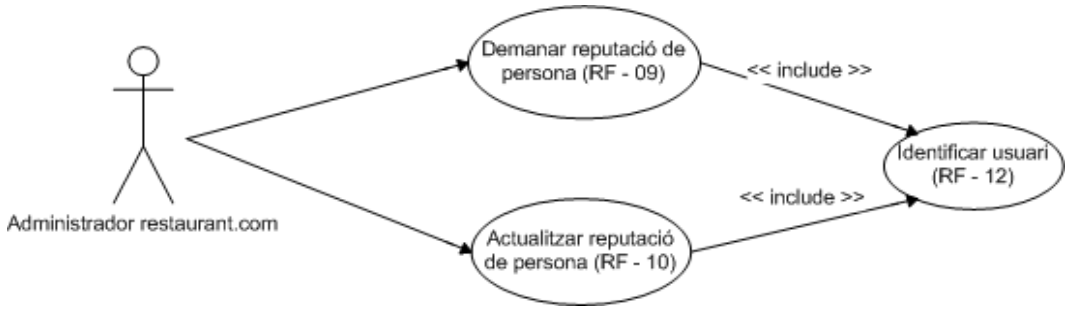
Segons el grau d'administració de que es disposi es podran fer segons quines funcionalitats.

Casos d'us del paquet gestionar els proveïdors de servei



Pel que respecta al paquet de gestionar els proveïdors de servis totes les graduacions d'administració del portal providentitats.com podrà fer totes les funcionalitats.

Casos d'us del paquet implementació / comunicació Servei Web

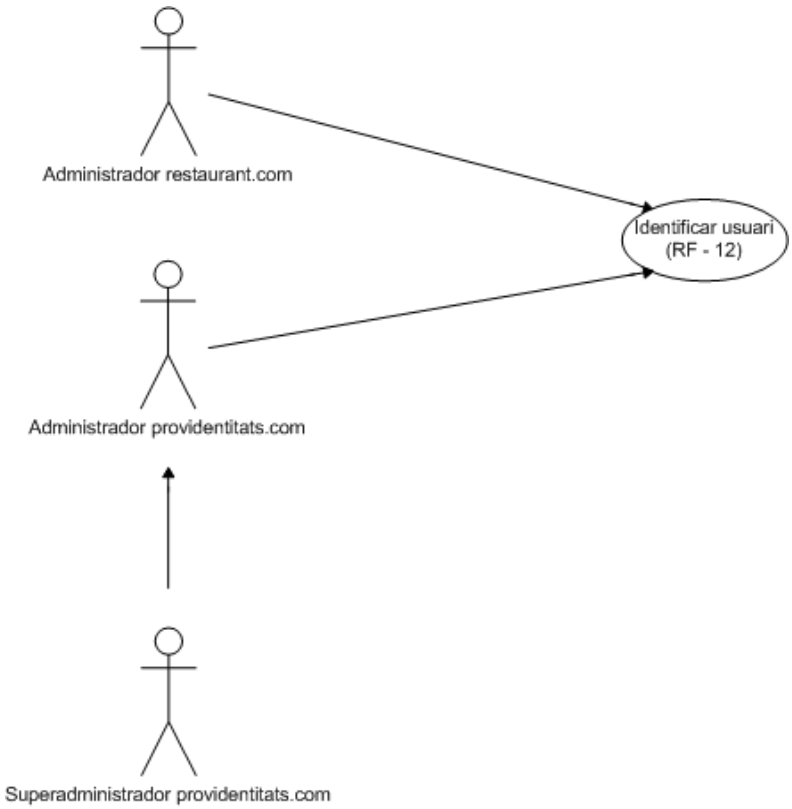


Imatge 21: cas d'ús de l'objectiu implementació / comunicació servei web

Casos d'us del paquet oferir servei

Per poder arribar a sol·licitat definitivament el servei caldrà haver estat autenticat pel proveïdor d'identitats i tenir suficient reputació pel proveïdor de servei.

Casos d'us del paquet gestió d'usuaris



Imatge 23: cas d'ús de l'objectiu gestió d'usuaris

Com veiem pel cas del portal providentitats.com és capaç de distingir entre diferents graus d'administració.

4.2. Model dinàmic

4.2.1. Diagrames de seqüència dels RF (interacció)

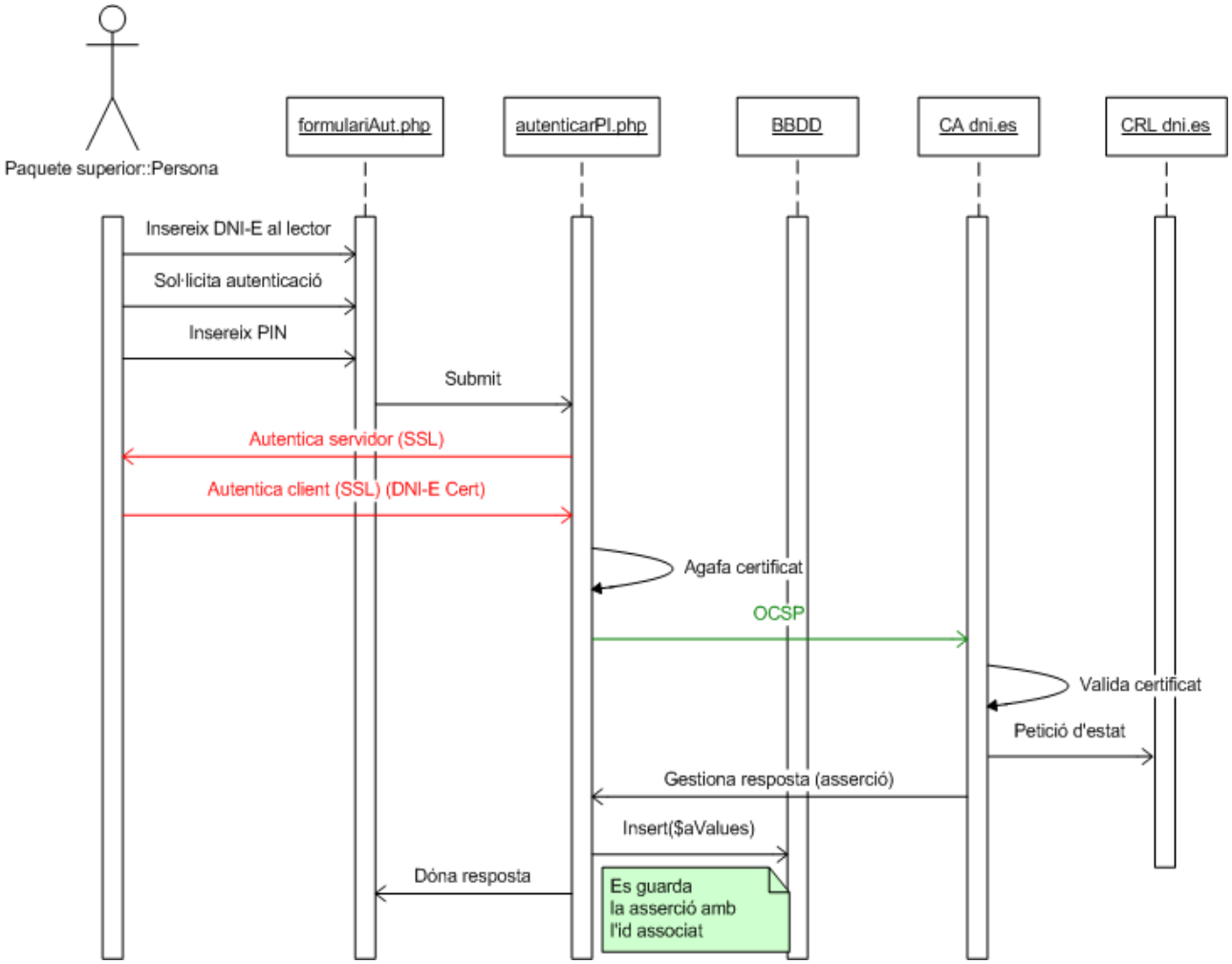
Es mostren els diagrames de seqüència on podem veure l'ordre de seqüència dels missatges i accions dels diferents actors amb el proveïdor de servei i el d'identitats.

Cada diagrama de seqüència correspon a un requeriment funcional especificat durant l'anàlisi del sistema a excepció de l'últim que és un resum, amb varis dels diagrames, de quin és el protocol de missatges aplicat per tota la seqüència en la autenticació de les persones i comunicacions posteriors entre el proveïdor de servei i el d'identitats.

Aclariments:

- Amb vermell es troben les comunicacions SSL, amb verd les relacionades amb peticions OCSP o gestió de certificats i en blau les comunicacions amb SOAP (Servei Web).
- Les planes que apareixen com a *.php són els noms reals fets servir al projecte.
- L'acció “Submit” és pròpia dels formularis XHTML al realitzar enviaments tant per POST com per GET. L'acció “Header” és una redirecció en el llenguatge PHP.

RF – 01 Autenticar persona

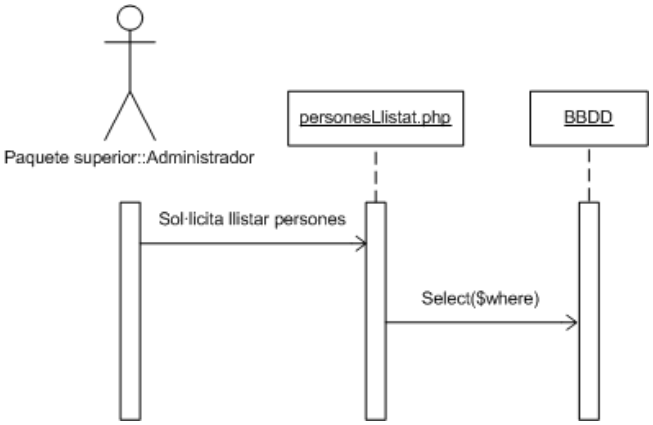


En aquest diagrama de seqüència es mostra el procés d'autenticar a la persona pel proveïdor d'identitats i no com el proveïdor de servei autentica a la persona en funció de la sol·licitud que li fa aquest al proveïdor d'identitats.

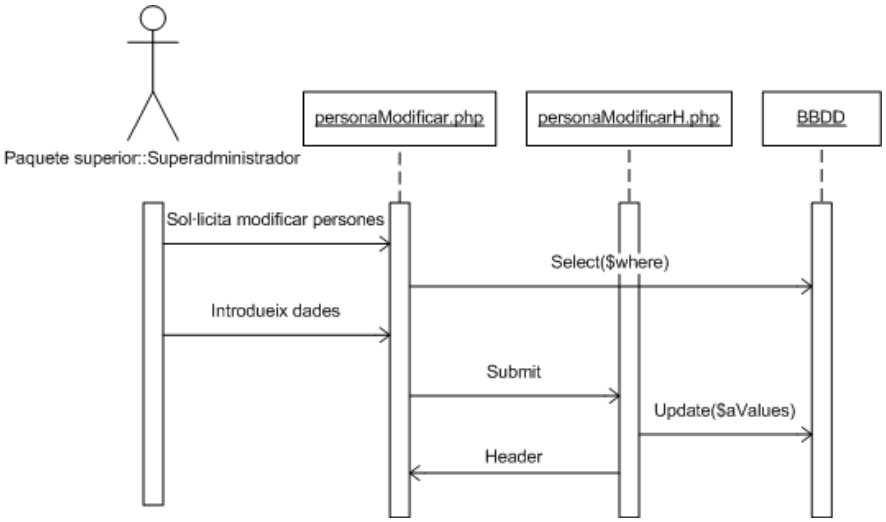
La comunicació es fa mitjançant un canal segur (SSL en vermell) amb una autenticació mútua perquè el proveïdor d'identitats pugui realment autenticar a la persona pel certificat del seu DNI-E apart de garantir integritat i confidencialitat durant la comunicació. Un cop agafat, la petició d'estat del certificat del DNI-E es fa mitjançant una petició OCSP per HTTP al servidor OCSP http://ocsp.dnie.es/ . La resposta OCSP (asserció) es guardarà al servidor del proveïdor d'identitats.

En la Imatge 37: diagrama de seqüència resum del procés d'autenticar persona i comunicacions posteriors amb servei web, sí que es mostra tota la seqüència d'autenticació d'una persona començant des del proveïdor de servei i altres.

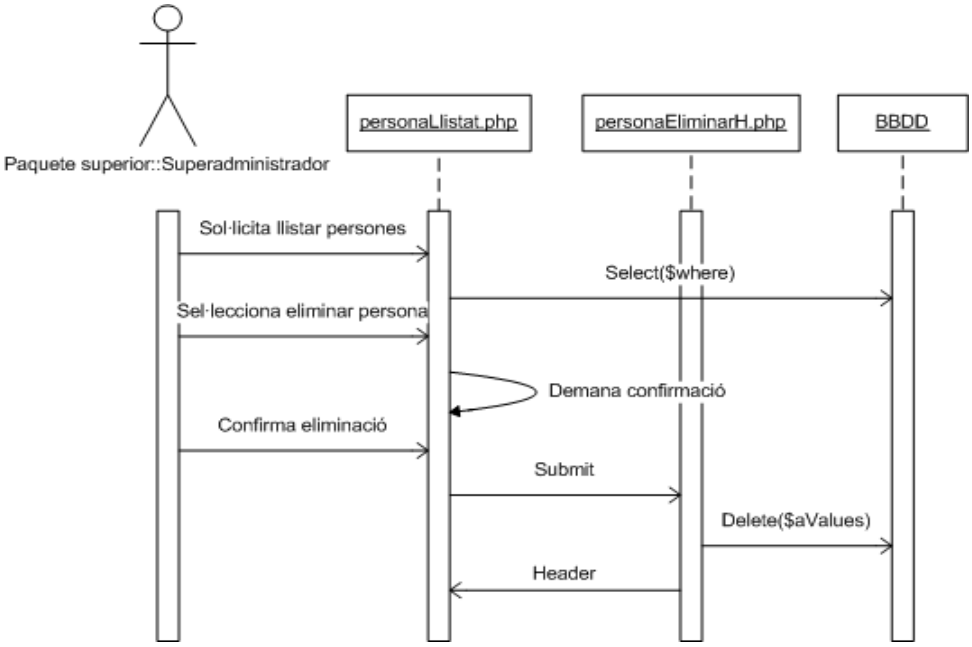
RF – 02 Llistar persones autenticades



RF – 03 Modificar persona autenticada

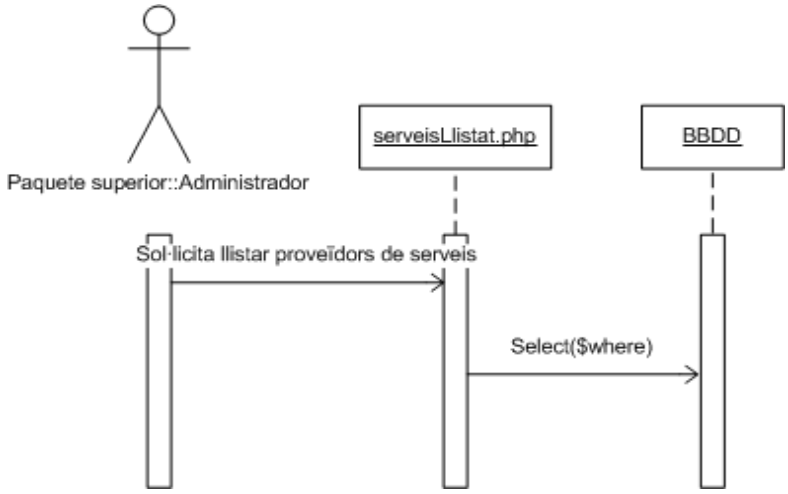


RF – 04 Eliminar persona autenticada



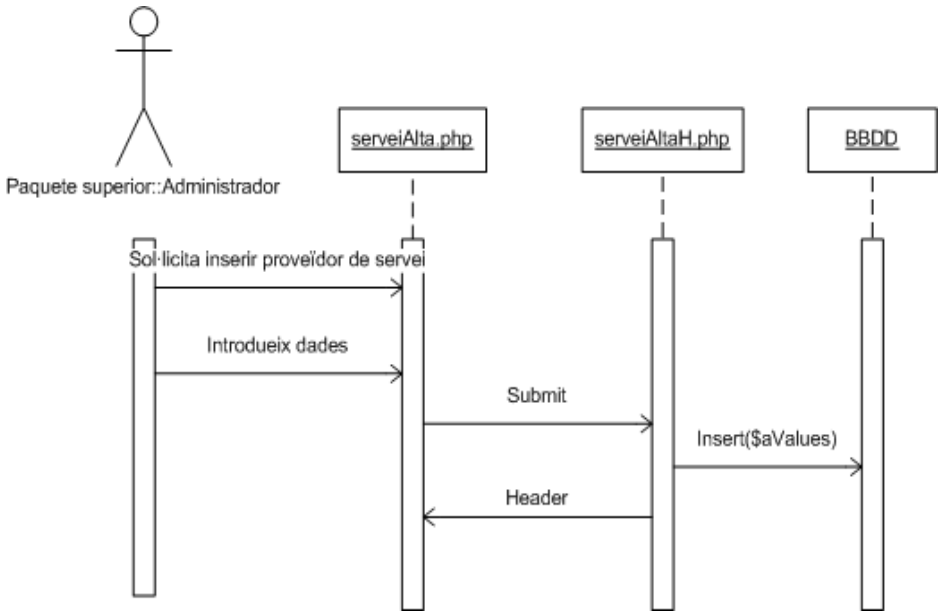
S'haurà d'eliminar en cascada totes les possibles entrades que hi hagin en la taula identificador que facin referència a la persona eliminada.

RF – 05 Llistar proveïdors de serveis

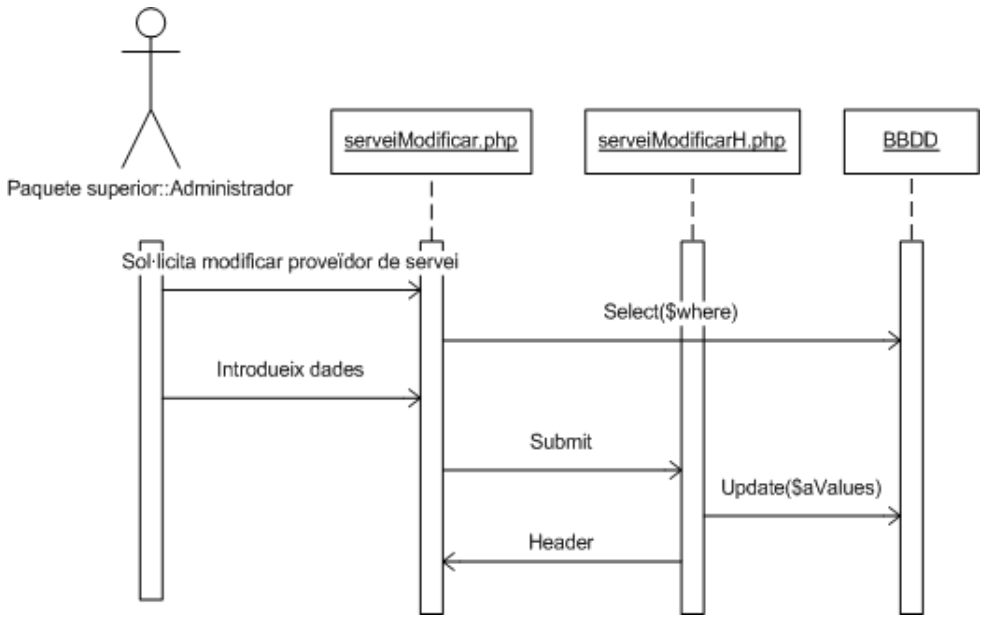


Imatge 28: diagrama de seqüència del requeriment funcional llistar proveïdors de serveis

RF – 06 Inserir proveïdor de servei

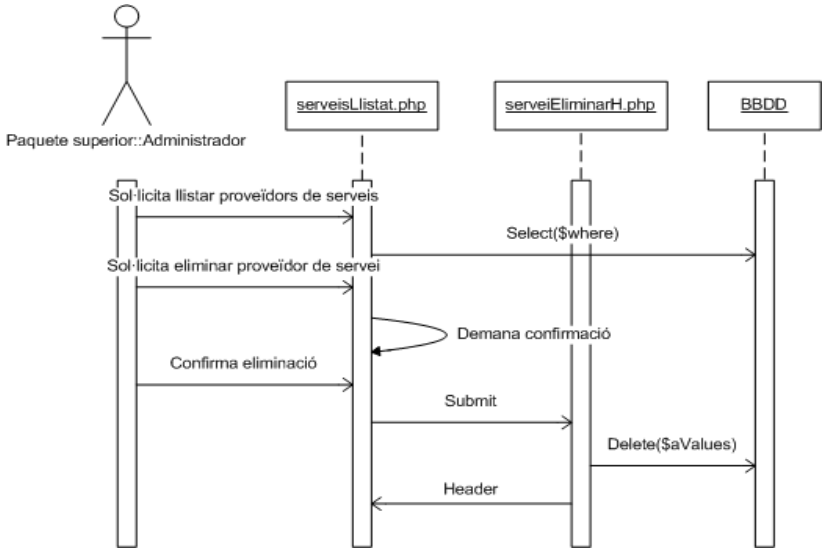


RF – 07 Modificar proveïdor de servei

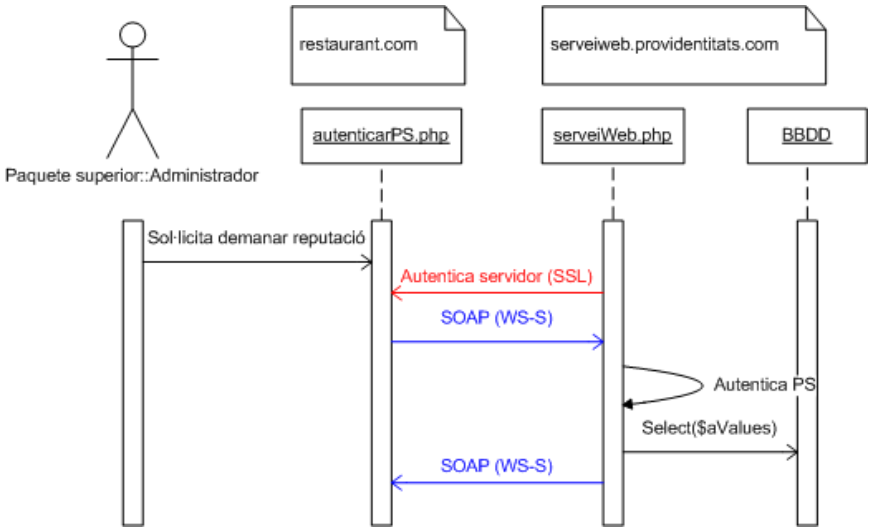


Imatge 30: diagrama de seqüència del requeriment funcional modificar proveïdor de servei

RF – 08 Eliminar proveïdor de servei



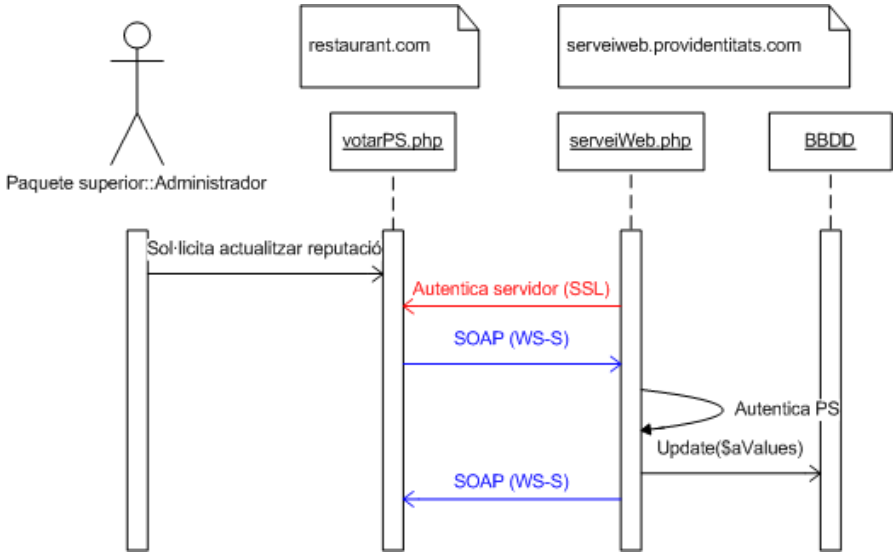
RF – 09 Demanar reputació de persona



Imatge 32: diagrama de seqüència del requeriment funcional demanar reputació de persona

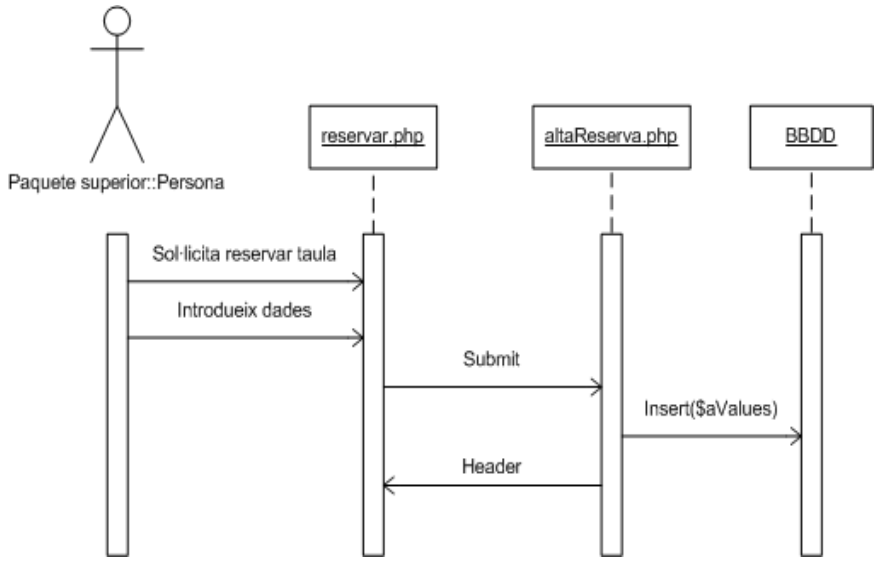
Durant l'enviament de la petició al servei web per SOAP s'utilitzen capçaleres WS-Security per autenticar al restaurant.com. A més a més s'afegeix una comunicació segura (SSL) per dotar d'integritat i confidencialitat a la petició.

RF – 10 Actualitza reputació de persona



Utilització de les mateixes capçaleres WS-Security que feia referència en la Imatge 32: diagrama de seqüència del requeriment funcional demanar reputació de persona

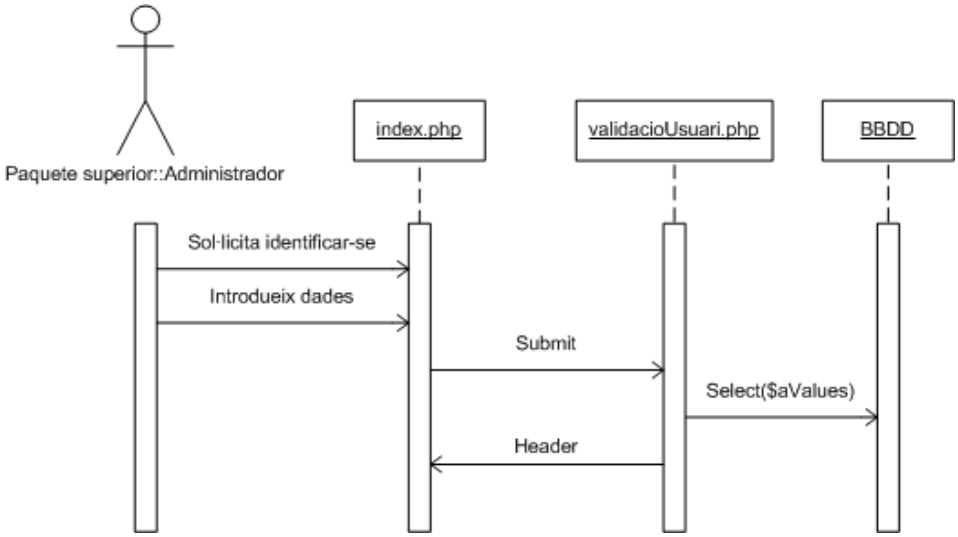
RF – 11 Reservar taula



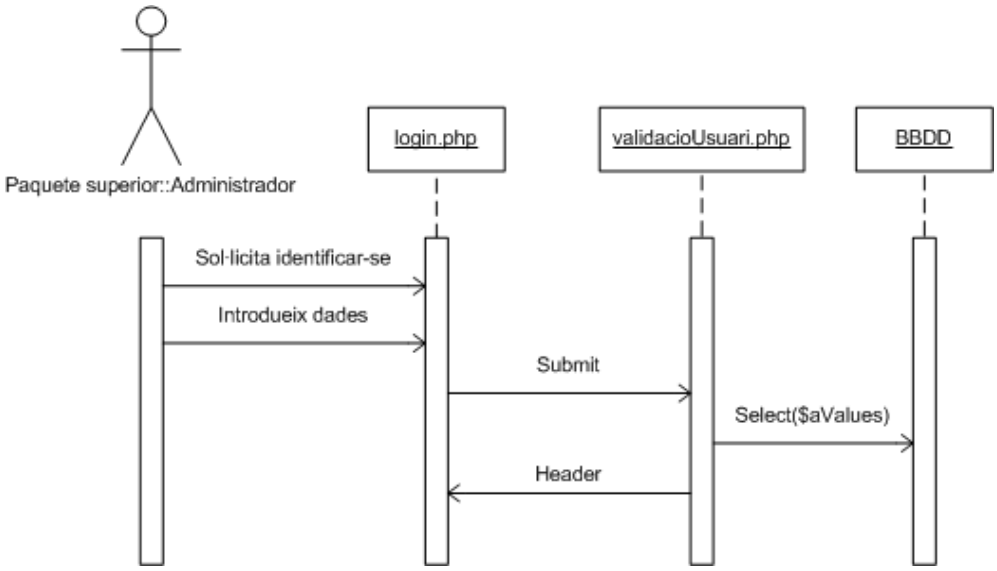
Imatge 34: diagrama de seqüència del requeriment funcional reservar taula

RF – 12 Identificar usuari

restaurant.com



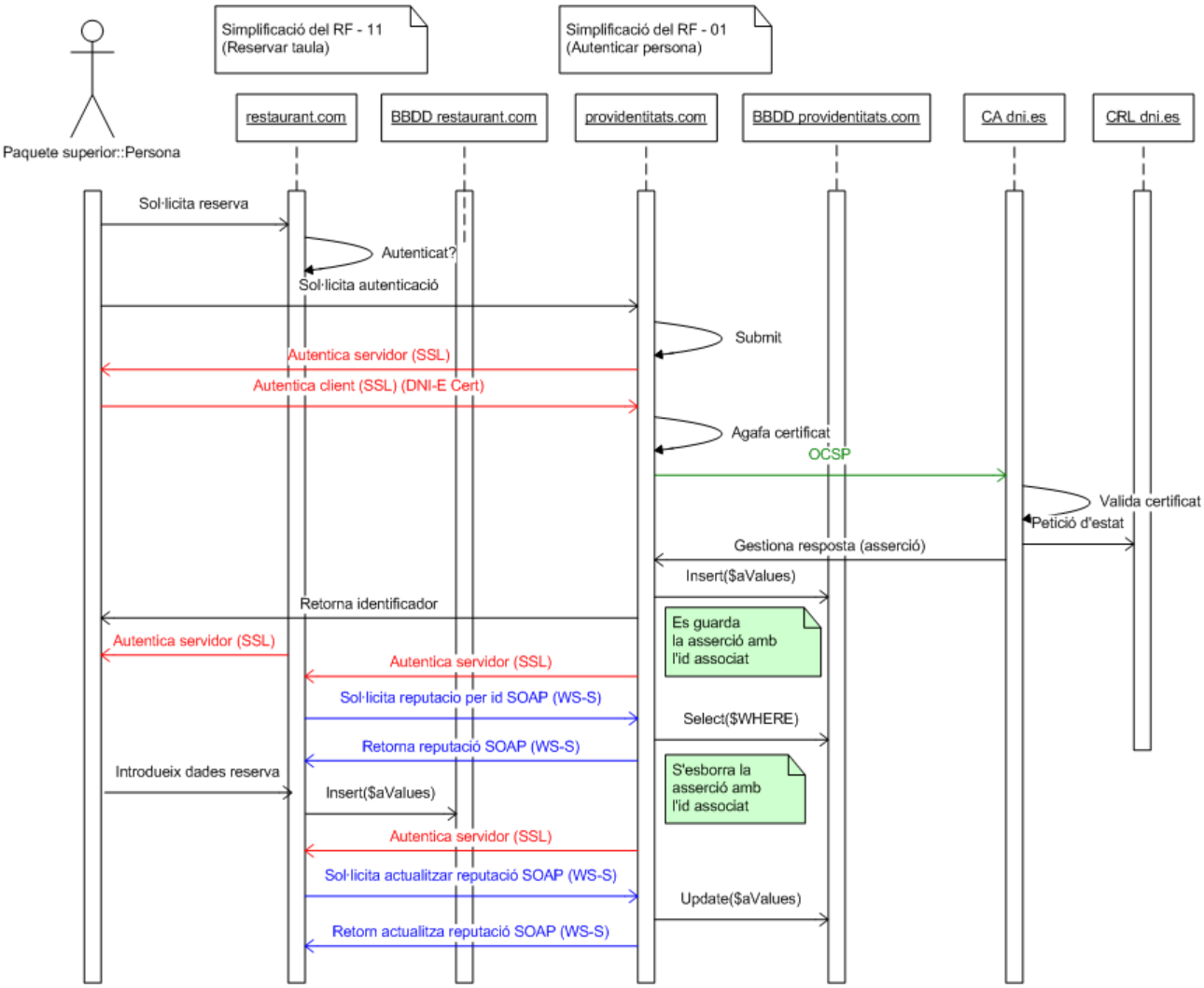
providentitats.com



Imatge 36: diagrama de seqüència del requeriment funcional identificar usuari del proveïdor d'identitats

4.2.2. Diagrames de seqüència del protocol (interacció)

Resum del diagrama de seqüència resultant del procés d'autenticat d'una persona. Per a més detall cal consultar els diagrames de la part corresponent del procés que es troben més amunt (Imatge 24: diagrama de seqüència del requeriment funcional autenticar persona).



Totes les comunicacions que es realitzen durant el procés d'autenticació d'una persona, en que viatgen dades compromeses, es fan mitjançant SSL per oferir un canal segur amb integritat

(que el contingut prevalgui inalterat) i confidencialitat (només coneguda per persones autoritzades) durant l'enviament. I particularment de manera mútua, autenticar al client, quan el proveïdor d'identitats demana la autenticitat d'aquest mitjançant el DNI-E.

Com veiem en la seqüència un cop rebuda la resposta OCSP se li dóna a la persona un identificador únic associat a la asserció (equivalent al "artefacte" en el perfil "Browser artifact" de SAML) que presentarà al proveïdor de servei (restaurant.com). Aquest últim farà una petició al servei web que un cop verificada la seva autenticació (la del restaurant.com gràcies a les capçaleres WS-Security) rebrà una resposta amb l'estat del certificat i la reputació de la persona (associat al identificador donat).

Un cop donada la resposta el proveïdor d'identitats esborrarà la asserció que s'està guardant. Més endavant, quan el restaurant.com ho cregui convenient, farà un vot a la persona mitjançant de nou amb una petició al servei web i el proveïdor d'identitats actualitzarà la seva reputació.

Com veiem el disseny implementat coincideix en l'ordre dels missatges i funcionalitat amb el que es va plantejar durant l'anàlisi del projecte (Imatge 10: seqüència de camí a seguir). Es manté la idea inicial de no donar en cap cas al proveïdor de servei, cap informació privada sobre les persones però a l'hora garantir que aquesta persona és qui diu ser. La principal causa és que el proveïdor d'identitats fa d'intermediari entre la persona i el proveïdor de servei i és l'únic que manega el contingut del certificat que hi ha al DNI-E. La idea inicial en quan a filosofia, seguretat i seqüència de missatges prové del que planteja SAML pel perfil "Browser artifact" però ha estat aplicat manualment sense fer ús d'aquest estàndard. La lògica d'insercions a base de dades o gestió de les respostes OCSP ha estat pensat en principi per autenticar a persones amb el DNI-E.

5. Desenvolupament

Deixant enrere l'anàlisi i el disseny entro a comentar a nivell més específic les eines, tant de software com de hardware, que he emprat i per què han servit.

No tot ha sortit tal com m'esperava en un principi i he hagut de buscar solucions alternatives i això és el que explicaré tot seguit. Tracto de justificar el per què de les meves decisions d'una manera tècnica i de com s'ha portat a terme.

Acabant l'apartat hi ha una mostra en captures de la funcionalitat del projecte.

5.1. Eines de desenvolupament software

- **XHTML + CSS:** evolució de l'HTML clàssic pensat per w3c (World Wide Web consortium) per complir un nou estàndard pels navegadors web. Procura que hi hagi una major semàntica en el contingut separant-lo de la forma donada per un arxiu extern .css.

  Apart que d'aquesta manera és més fàcil treballar degut a que els dissenys dels web queden separats del codi XHTML i un dissenyador sempre podrà tocar més ràpidament el disseny, els nous tags XHTML es visualitzen d'una manera més uniforme pels diferents navegadors; Firefox, Explirer, Opera, Chrome, etc. A més els diferents robots d'indexació dels navegadors agraeixen els nous tags premiant amb un bon posicionament del web.

  És per això que tant el proveïdor d'identitats com el de servei estan fets amb aquests dos llenguatges en quan a forma i contingut.

- **PHP orientat a objectes:** per donar dinamisme a les planes XHTML s'ha optat pel llenguatge **PHP 5.2.7** . He muntat una classe per cada taula de la respectiva base de dades que gestiona les entrades, modificacions, eliminacions o consultes entre altres. Cada una d'aquestes classes es hereva d'una classe superior que té mètodes més genèrics com la de connexió, desconnexió o gestió d'errors.

  D'aquesta manera queda tot molt més encapsulat, estalviant línies de codi, trobant els errors

molt més ràpidament i amb una semàntica molt major del codi. Per fer les instàncies pertinents des de cada plana haurà d'haver una cosa similar a:

```
include ("../classes/class_general.php") ;
include ("../classes/class_persona.php") ;

$clsPersona = new Persona(DB_USER, DB_PASS, DB_NAME, DB_SERVER);
$clsPersona->Select('ORDER BY nom asc');

...
```

El sistema gestor de base de dades serà **MySQL 5.1.30** i el llenguatge d'accés a ell SQL. Tot corre sota un servidor **Apache 2.2.10.**

- **javaScript:** llenguatge interpretat que s'executa a la banda del client molt utilitzat en la creació de planes web. L'utilitzo per al control de camps en els diferents formularis d'inserció, modificació, etc per agilitzar l'execució de la aplicació.
- **nusoap:** llibreria escrita en PHP per desenvolupar Serveis Web d'una manera més còmoda. Està basat en SOAP 1.1, WSDL 1.1 i HTTP 1.0/1.1 . Cal afegir les llibreries en el servidor i des de cada plana que es vulguin fer instàncies de les classes s'haurà d'incloure les llibreries:

```
require_once('.\nusoap.php');
$server = new soap_server();
...
```

- **openssl:** paquet d'administració i llibreries que proporcionen funcions criptogràfiques. Ha calgut per generar el certificat i les claus corresponents del servidor per establir la comunicació SSL.

  També es fa servir per fer la petició OCSP del certificat de les persones:

```
$output = shell_exec('openssl ocsp -CAfile '.$RootCA.' -issuer '.$dir.
      $a.'cert_i.pem  -cert  '.$dir.$a.'cert_c.pem  -url  '.$OCSPUrl.'
      -resp_text -out '.$dir.$a.'validacio.txt');
```

5.2. Eines de desenvolupament hardware

- **CPU:** Pentium Intel Core 2 Quad 2,5 Ghz amb 4 GB de RAM que farà tant de servidor com de client degut a que treballo en servidor local.
- **Lector de targetes:** Lector LTC31 de C3PO. S'instal·la de manera Plug and Play per USB. Cal instal·lar els drivers i firmwares adequats per a que pugui llegir els DNI-E.

5.3. Justificacions a la implementació i solucions a problemes

Els canvis sobre la marxa han estat nombrosos per motius diferents. De vegades el plantejament inicial no era el correcte, d'altres el resultat no era l'òptim i d'altres simplement que degut a no trobar solució s'ha optat per una via alternativa. Tot seguit tracto d'esmentar els problemes més importants que m'he trobat i de quina manera i per què s'han arreglat de la manera descrita.

Tot comença creant diferents dominis pels dos webs que s'hauran d'implementar configurant el fitxer hosts de Windows i el httpd-vhosts de l'Apache:

```
(hosts.txt)

127.0.0.1       providentitats.com
127.0.0.1       serveiweb.providentitats.com
127.0.0.1       restaurant.com
127.0.0.1       localhost
```

El domini providentitats.com correspon al proveïdor d'identitats mentre que el restaurant.com al de servei. El domini serveiweb.proveidentitats.com associat al que serà el servei web té un domini propi per que sigui més fàcil de recordar pels proveïdors d'identitats a l'hora d'establir comunicació.

Un cop configurats els dominis que faran falta vaig fer els dissenys estàtics dels dos webs com indico en l'apartat eines de desenvolupament software amb XHTML pel contingut i CSS per la forma.

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional

...

<link href="estils/style.css" rel="stylesheet" type="text/css" />
```

La idea és separar el contingut de la forma per una gestió molt millor del que és el disseny dels webs i poder maquetar amb molta més facilitat. Validar els webs en w3c ha de premiar, en teoria ,amb un millor posicionament del web pels motors de cerca en Internet i una millor visualització per diferents navegadors ja que s'utilitza un estàndard.

Imatge 39: validació XHTML

Imatge 40: validació CSS

Després del disseny dels dos portals encara sense funcionalitat em vaig disposar a començar amb la part de configurar l'arxiu httpd-ssl i de nou el httpd-vhosts per crear comunicacions SSL i va ser aquí on em vaig trobar amb un dels primers problemes.

El problema va ser de com generar el certificat i les claus del servidor per tal d'establir una comunicació SSL que en un futur necessitaria. La solució la vaig trobar amb el programa openssl en que, prèvia instal·lació, a través de consola (cmd en Windows) i les comandes pertinents consultades en manuals vaig generar el certificat autosignat i les claus corresponents de manera fàcil que em servirien per autenticar al servidor un cop configurada la comunicació SSL.

Seguint amb l'ordre de la planificació vaig instal·lar el lector de targetes e instal·lar els 'firmwares' i 'drivers' per Windows i vaig comprovar el seu bon funcionament autenticant-me en diverses pàgines bancaries que ofereixen l'opció d'autenticar-se amb el DNI-E.

Tot seguit quan em vaig plantejar aconseguir que el servidor es fes amb el certificat del DNI-E del lector de targetes, vaig tenir problemes. Vaig començar malament degut a que feia una comunicació SSL en que només el servidor s'autenticava de cara al client. I és clar, faltava que el client també hagués d'autenticar-se cara al servidor perquè aquest segon pogués fer-se amb el certificat del DNI-E emès pel client.

Entès això el problema va continuar amb la configuració del servidor local (Apache) per tal de que fes aquesta autenticació mútua amb SSL.

```
SSLEngine On

SSLCipherSuite HIGH:MEDIUM:-SSLV2
SSLCertificateFile "conf/ssl.crt/server.crt"
SSLCertificateKeyFile "conf/ssl.key/server.key"
SSLCACertificateFile "conf/cadni/acraiz-sha1-2.crt"
SSLVerifyClient require
SSLVerifyDepth 2
```

Tot semblava correcte però a l'hora de provar-ho mai obtenia l'autenticació mútua desitjada. El navegador em mostrava un missatge dient-me que era necessària una autenticació mútua però no es podia autenticar al client.

Arribat en aquest punt vaig mirar els .log corresponents a la comunicació SSL i vaig determinar que no es podia obtenir correctament la AC Arrel (certificat autosignat per una AC, per aquest cas per la Direcció General de la Policia) que havia baixat de http://www.dnielectronico.es/. I és que la AC Arrel que distribueixen està en format DER mentre que Apache només admet PEM. La conversió també la vaig fer via openssl:

```
openssl x509 -in ACRAIZ-SHA2.crt -inform DER -out ACRAIZ-SHA2-2.crt
-outform PEM
```

Un cop solucionada l'autenticació mútua i ja poden agafar el certificat del client amb PHP, havia de fer la petició OCSP per comprovar l'estat del certificat de la persona. Vaig comprovar que es podia fer novament amb OpenSSL només que havia de ser llançat dinàmicament des de la plana web. Vaig trobar una funció PHP "`shell_exec`" que em permetia llançar una instrucció a la consola des de la plana .php. Primer de tot llançava un .bat degut a que no em trobava en el directori on estava el executable d'OpenSSL:

```
$output = shell_exec("arrelopen.bat $RootCA $dir $a $OCSPUrl");
```

i el arrelopen.bat:

```
cd c:\
cd wamp
cd bin
cd apache
cd Apache2.2.10
```

cd bin

openssl ocsp -CAfile %1 -issuer %2%3cert_i.pem -cert %2%3cert_c.pem -url %4 -resp_text -out %2%3validacio.txt

Finalment el .bat va ser canviat per aquesta altre instrucció degut a que vaig copiar l'instal·lable a la mateixa plana que feia la crida:

```
$output = shell_exec('openssl ocsp -CAfile '.$RootCA.' -issuer '.
      $dir.$a.'cert_i.pem -cert '.$dir.$a.'cert_c.pem -url '.
      $OCSPUrl.' -resp_text -out '.$dir.$a.'validacio.txt');
```

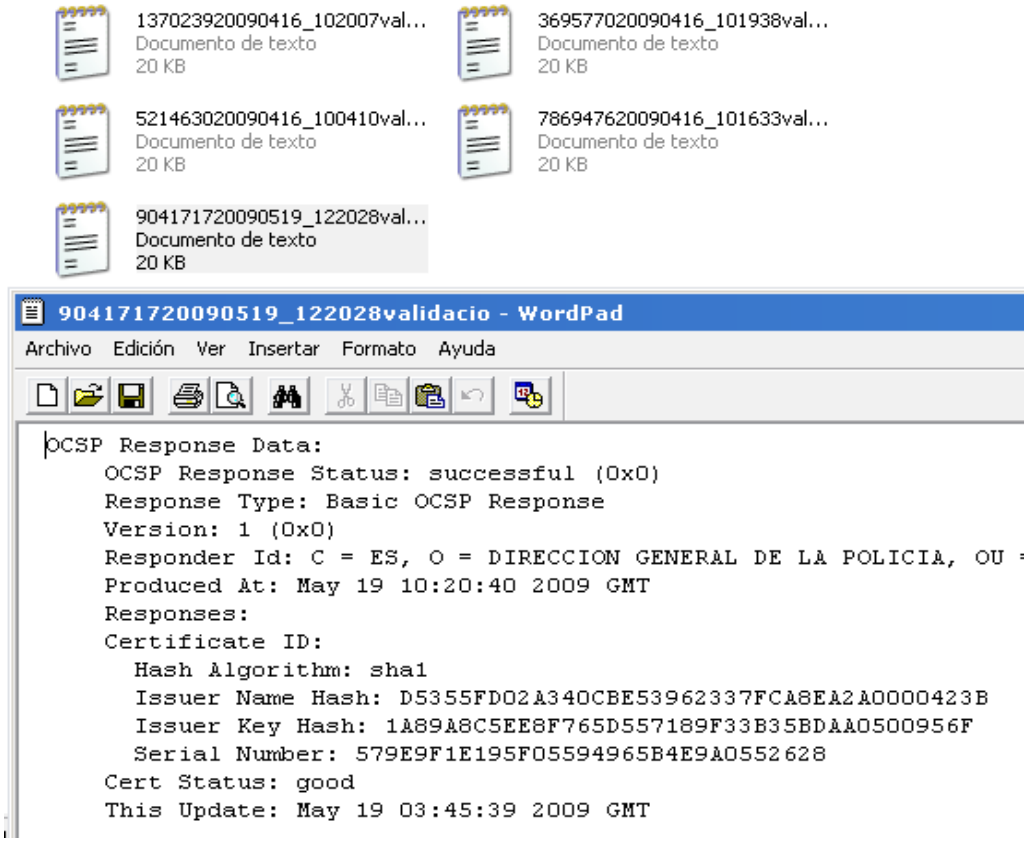
Fixem-nos que al final, la resposta (-resp_text que correspon a l'asserció) es guarda (-out) en el servidor concatenant un directori constant amb una variable $a. Aquesta variable al principi no la vaig posar fins que vaig veure que si volia fer peticions concurrents havia d'anar guardant les respostes amb diferents noms:

```
$a = rand(1000000,9999999) . trim(date("Ymd_His"));
```

Vaig triar aquest criteri de concatenar la data i hora a un nombre aleatori per tal de que no s'anessin repetint els noms de les assercions o certificats de les persones que anessin concurrentment demanant autenticacions.

Per altra banda i donat que les assercions es guarden amb aquesta variable $a, el nombre aleatori que se li dóna a la persona (veure Imatge 37: diagrama de seqüència resum del procés d'autenticar persona i comunicacions posteriors amb servei web) per tal de que ho pugui presentar al proveïdor de servei, és precisament aquest mateix nombre. Així la resposta (asserció) associada a l'identificador donat a una persona és fàcil de recuperar.

Degut a que ja no serà necessari el certificat de la persona (client) i del emissor (servidor), s'esborren. La resposta (asserció) encara no l'esborrem ja que la necessitarem per més endavant per donar resposta cada petició dels diferents proveïdors de serveis.



Imatge 41: assercions guardades en el servidor amb $a com a nom de fitxer

Arribat aquí, i seguint amb l'idea inicial de donar-li a la persona l'identificador, com esmentava durant etapes anteriors, amb una 'cookie' amb temps de caducitat perquè pogués navegar tranquil·lament presentant aquesta 'cookie' als diferents proveïdors de serveis i no haver-se d'autenticar cada vegada, vaig trobar un problema amb la funció de PHP "setcookie" treballant amb servidor local. La funció "setcookie" té els següents paràmetres:

```
setcookie("identificadorUsuari", $a, time() + 86400, '/',
'restaurant.com');
```

on el primer paràmetre és el nom de la variable, el segon és el valor que tindrà la variable (que com deia és el mateix valor amb que es guardarà l'asserció al servidor del proveïdor d'identitats), el tercer paràmetre correspon al temps de caducitat, el quart el directori en que la

'cookie' serà visible dins del servidor i l'últim paràmetre per quin domini serà visible. Doncs bé, treballant amb servidor local (localhost) el quart paràmetre sempre es substitueix per 'localhost' de manera que si es té un 'virtualhost' amb diferents dominis (com és el cas) aquesta 'cookie' no es fa visible pels nous dominis del 'virtualhost'. Veient que no trobava la solució vaig optar per redireccionar a la persona cap al proveïdor de servei del que prové (observant des d'on venia) i passant el identificador ($a) per GET per SSL i a una plana del proveïdor de servei no visible per la persona (per que quedi més elegant) que gestiona la validesa d'aquest identificador.

No hi ha perill de passar l'identificador per GET gràcies a que és fa mitjançant SSL que dóna integritat i confidencialitat a la comunicació. Recordem que la idea inicial de fer servir 'cookies', que està implementada alternativament (comentada al codi), té l'avantatge de que pot donar resposta a l'autenticitat de la persona fins que duri la 'cookie' que anirà agafant cada proveïdor de servei per fer la petició. Això fa que la asserció no s'hagi d'esborrar fins que per lo menys caduqui la 'cookie' de la persona (degut a que és el temps amb el que podrà presentar l'identificador) o bé passat un temps prudencial ja que l'estat de la asserció (de la resposta OCSP) pot canviar passat un temp. Com que el nom de les assercions es guarden, entre altres coses, amb l'hora de creació, s'esborraran de manera automatitzada del servidor les assercions que 'caduquin'. Ara bé, com la implementació a servidor local, s'ha fet amb la redirecció cap al proveïdor d'identitat abans comentat i no es guarda l'identificador en cap 'cookie', la persona haurà de sol·licitar autenticar-se per cada proveïdor de servei diferent. I és per això que cada asserció s'esborra un cop feta la petició d'autenticació del proveïdor de servei corresponent. Per altra banda, aquesta manera té l'avantatge de que funcionarà tot i que la persona tingui desactivat les 'cookies' al seu navegador.

Aquesta redirecció cap el proveïdor de servei amb l'identificador passat per GET és la segona comunicació SSL que s'estableix en servidor local (veure Imatge 47: autenticació realitzada i redirecció). La primera recordem que era autenticació mútua mentre que aquesta és només per part del servidor. Doncs bé, un cop feta aquesta comunicació SSL no funcionava. Després d'un temps sense entendre que és el que passava, vaig descobrir que cada comunicació SSL pel mateix servidor requereix d'un port diferent. La primera ja ocupava el 443 (que és el per defecte), de tal manera que vaig habilitar el 444 per fer aquesta segona comunicació SSL

aquest cop no mútua si no només per part del servidor (aprofitant el mateix certificat autosignat de la primera comunicació SSL).

```
Listen 443
Listen 444
Listen 446
```

ex: `https://restaurant.com:444`

El port 446 està obert per una tercera comunicació SSL explicada més abaix. No es fa servir el 445 ja que està reservat per un altre protocol.

Un cop rebut l'identificador per SSL, el proveïdor de servei estableix una comunicació via servei web amb SOAP amb el proveïdor d'identitats per obtenir l'autenticitat i la reputació de la persona amb aquest identificador. Per dotar de seguretat als missatges XML per SOAP es va optar per afegir capçaleres WS-Security amb un login i un password que autentica a cada proveïdor de serveis. Aquests logins i passwords es troben a la base de dades xifrats pel cas dels passwords amb SHA1. S'hagués pogut enviar un certificat per autenticar d'una manera més fiable als proveïdors de serveis però s'ha deixat com una de les millores possibles. Per complementar l'autenticitat també es comprova que la petició provingui d'un domini conegut guardat a la base de dades corresponent al proveïdor de servei.

Degut a que no s'ha fet servir ni signatures ni xifrats XML propis de WS-Security que són els que donen integritat i confidencialitat a la comunicació s'ha optat per complementar aquesta comunicació amb SSL que atorga integritat, confidencialitat i autenticitat del costat del servidor. No caldrà establir una autenticitat mútua per SSL i autenticar també el costat del client degut a que sí s'ha fet servir, com explicava anteriorment, en les capçaleres WS-Security els 'UsernameToken' que autentiquen el costat del client.

```
$headers = ('<wsse:Security soap:mustUnderstand="1"
xmlns:wsse="http://restaurant.com">
```

```
<wsu:Timestamp    wsu:Id="Timestamp-c95dbad2-6625-
            451b-ae80-  774aff3d0b3f" xmlns:wsu="restaurant.com">

       <wsu:Created>'. $created . '</wsu:Created>
       <wsu:Expires>'. $expires . '</wsu:Expires>

</wsu:Timestamp>
<wsse:UsernameToken wsu:Id="User">

       <wsse:Username>RestaurantETSE</wsse:Username>
       <wsse:Password>XXXXXXXXXXXXXX</wsse:Password>
       <wsse:Nonce>XXXXXXXXXXXXXXXX</wsse:Nonce>

 </wsse:UsernameToken>
 </wsse:Security>');


$oSoap->setHeaders($headers);
```

D'aquesta manera amb SSL suplim a nivell de capa de transport el que no hi és a la capa de missatgeria.

El port utilitzat per aquesta comunicació SSL amb la petició SOAP amb WS-Security ha estat el 446:

```
$oSoap  =  new  soapclient('https://serveiweb.providentitats.com:446?
         wdsl');
```

Al afegir SSL un cop es tenien les capçaleres WS-Security no es realitzava la comunicació correctament. Faltava afegir a l'arxiu php.ini la següent línia:

extension=php_curl.dll (http://es2.php.net/manual/es/intro.curl.php)

Llibreria que permet molts protocols de comunicació necessària per enviar les capçaleres de seguretat per HTTPS.

Un cop rebuda la petició al servidor es fa una comprovació del nom d'usuari i del password com deia, de si la petició es fa des d'un domini conegut associat al proveïdor de servei que consta en la base de dades i si aquest està actiu o no per complementar l'autenticitat.

Ja feta l'autenticació del proveïdor de servei el proveïdor d'identitats dintre del servei web comprova la asserció (veure Imatge 41: assercions guardades en el servidor amb $a com a nom de fitxer) de la persona amb l'identificador rebut. Si aquesta persona no li consta en la base de dades la insereix per guardar a partir d'ara la seva reputació acumulada. Es guarda entre altres coses el nombre de sèrie del DNI-E un cop aplicat un SHA1. S'ha fet d'aquesta manera degut a que és necessari un identificador únic que relacioni les assercions del DNI-E amb la persona de la base de dades, però a l'hora com s'aplica un 'hash' ja que com és 'unidireccional' molt difícilment es podrà obtenir el nombre de sèrie original. Així es protegeixen més les dades personals o possibles filtracions de la base de dades.

No s'ha guardat abans les dades de la persona per estalviar espai pel cas en que una persona decideixi a l'últim moment no sol·licitar el servei. La resposta d'estat de la petició OCSP no es guarda en la base de dades ja que aquesta resposta pot canviar en un termini relativament curt de temps i per això convé fer cada cop la petició d'estat.

El proveïdor d'identitats dóna resposta a l'autenticitat i reputació corresponent a la persona que el proveïdor de servei sol·licita i és aquest qui decideix si accepta o no a aquesta persona (veure Imatge 48: autenticació en el proveïdor de servei realitzada) en funció si la reputació és o no és suficient per confiar amb ella (el restaurant.com accepta reputacions de zero o més. Si és el cas, obre una variable de sessió perquè la persona pugui navegar pel web sense haver de tornar a autenticar-se cada vegada). A part el proveïdor de servei afegeix en la seva base de dades l'identificador de la persona per a un futur fer una votació per aquest identificador.

Però just abans de donar resposta al proveïdor de servei, s'esborra la asserció de la persona del servidor per estalviar espai. Es guarda però una relació en una taula de la base de dades (taula identificador Imatge 16: model de dades físic del proveïdor d'identitats) d'aquest nombre de serie amb SHA1 amb l'identificador amb el que ens han fet la petició (i a l'hora també nom del fitxer asserció). La raó, ha estat evitar utilitzar com a identificador un nombre no aleatori, ja que si no, per cas del restaurant per exemple, un empleat del local pogués identificar i relacionar a la llarga a un dels seus client amb un identificador únic i sempre igual per aquella persona. A l'hora també va molt bé per portar el control de les vegades que un proveïdor de servei ha demanat l'autenticitat d'aquesta persona en concret, ja que cada entrada a aquesta taula representa una petició i quan el proveïdor d'identitats vulgui fer més endavant una votació sobre aquest usuari no ho pugui fer indiscriminadament amb moltes peticions. S'ha de

dir que la petició de vot es fa amb l'identificador aleatori que se li va atorgar anteriorment a la persona i que el proveïdor de servei guarda a la base de dades junt amb la reserva (pel cas del restaurant.com) (veure Imatge 51: plana de llistat de reserves i vots de clients en l'administració del proveïdor de servei). Un cop feta la votació s'esborrarà pertinentment l'entrada de la taula identificador i s'incrementarà o decrementarà la reputació correctament en la taula persona degut a la relació que hi ha entre aquestes dues taules (el nombre de serie amb SHA1 com a clau externa) (veure Imatge 52: actualitzada la reputació en la plana de llistat de persones autenticades de l'administració del proveïdor d'identitats).

Com que en el seu moment el proveïdor de servei guarda l'identificador de la persona, podrà quan ho cregui convenient fer una votació per aquest identificador. En una primera implementació el proveïdor de servei podia arribar a fer votacions massives prement F5 per exemple o amb un bucle malintencionadament. Per evitar això com explicava anteriorment la taula de la base de dades del proveïdor d'identitats guarda aquest identificador amb la persona que correspon. Així quan li arribi la petició de vot, esborrarà aquesta entrada i no es podrà fer un altre votació per aquella persona amb aquell identificador.

Cal dir que un cop es tenien moltes entrades de reserves (pel cas del restaurant.com) era una mica avorrit anar votant un per un que és com es feia abans. Es va introduir una millora amb un petit selector al costat de cada reserva i un únic botó de vot positiu i negatiu per poder fer votacions de manera massiva (veure Imatge 51: plana de llistat de reserves i vots de clients en l'administració del proveïdor de servei).

Per finalitzar, dir que per facilitar les coses als proveïdors de serveis que vulguin interaccionar amb el servei web i donat que SOAP ho permet, s'ha fet ús de WSDL (veure Imatge 62: WSDL del servei web del proveïdor d'identitats) per descriure els requisits i formats dels missatges per poder fer peticions als diferents mètodes que es llistaran. Així no només se'ls informa de com han de ser les peticions si no que també es pot veure què és el que es retornarà per a cada un del mètodes que hi ha en el servei web. SOAP ho permet i les llibreries utilitzades nusoap també:

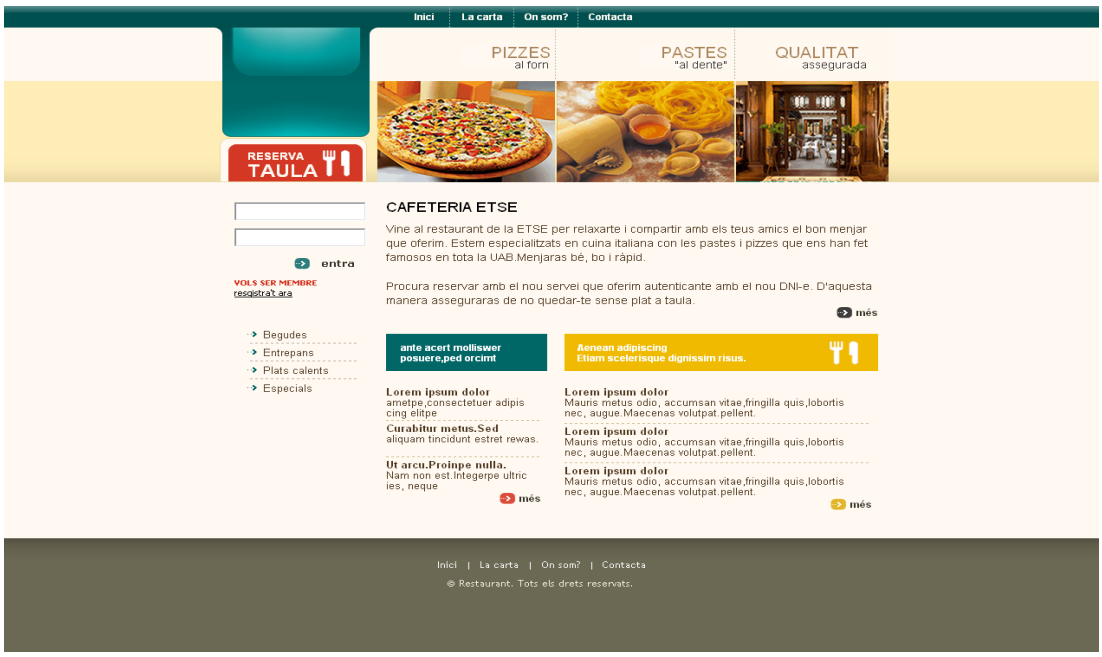
```
$server = new soap_server();
```

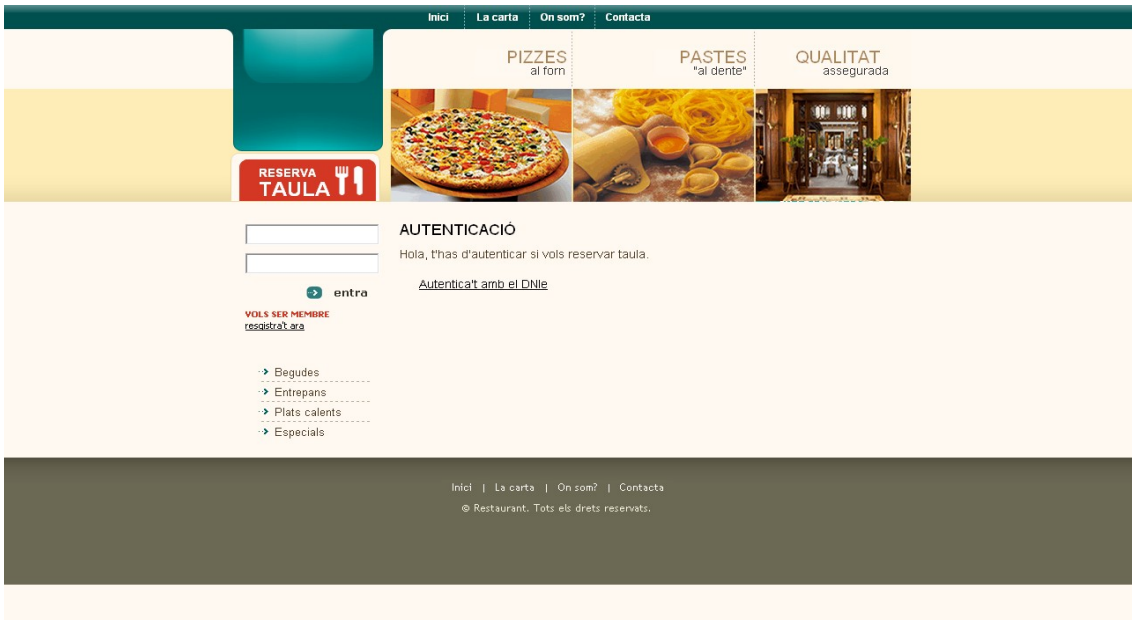
```
$ns="https://serveiweb.providentitats.com:446";
$server->configurewsdl("Servei Web PFC Proveïdor d'identitats",$ns);
$server->wsdl->schemaTargetNamespace = $ns;

// registrem el metode HolaMon
$server->register('HolaMon', array('nom' => 'xsd:string'),
      array('return' => 'xsd:string'), $ns, $ns . '#' . 'HolaMon',
      'rpc', 'encoded', "Mètode de prova i testeig del Servei Web en
      que li passem un nom i ens retorna una salutació.");
```

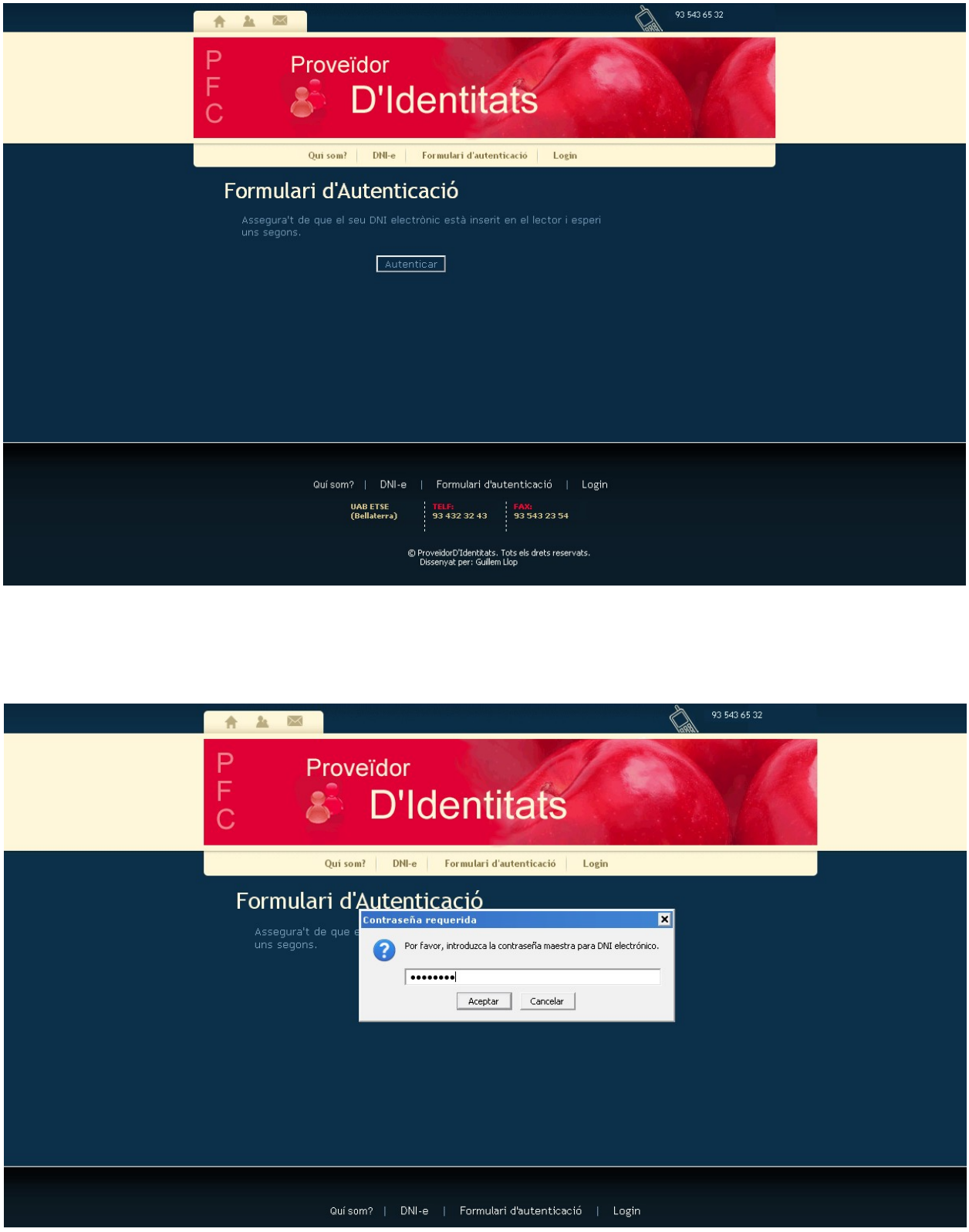
5.4. Funcionalitat (captures)

En aquestes captures és a on les persones entren per primer cop en el proveïdor de servei que en aquest cas és un restaurant i sol·licitaran reservar una taula per menjar.

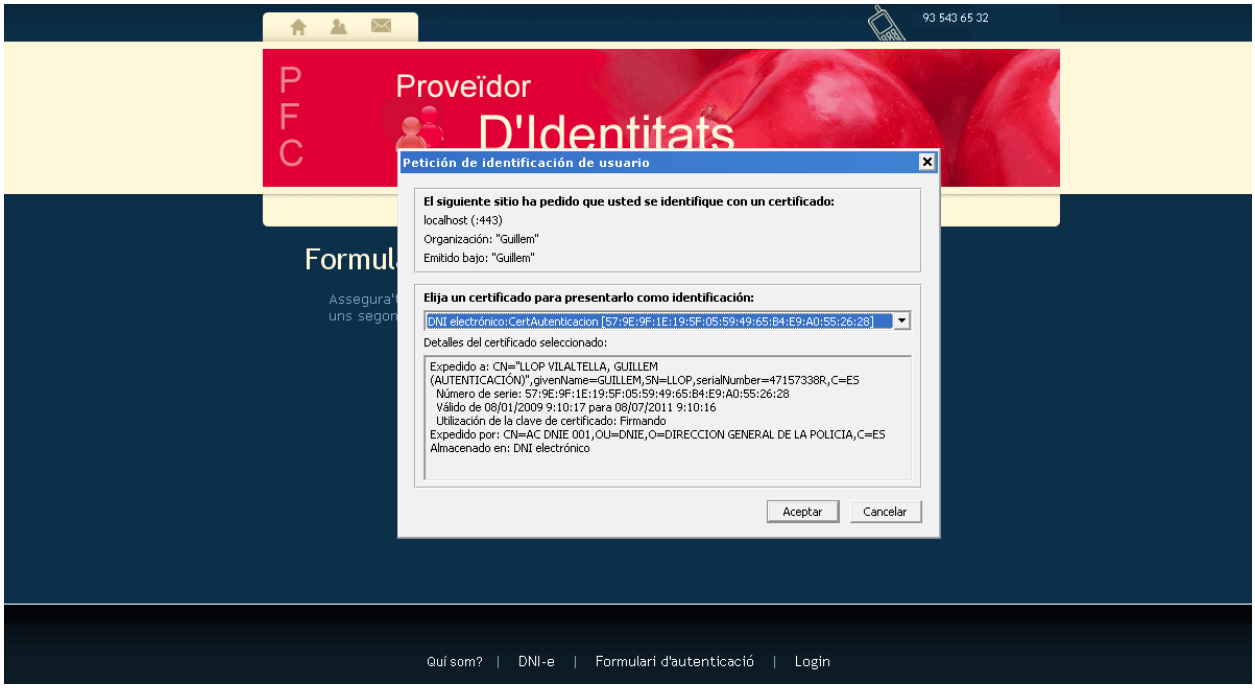




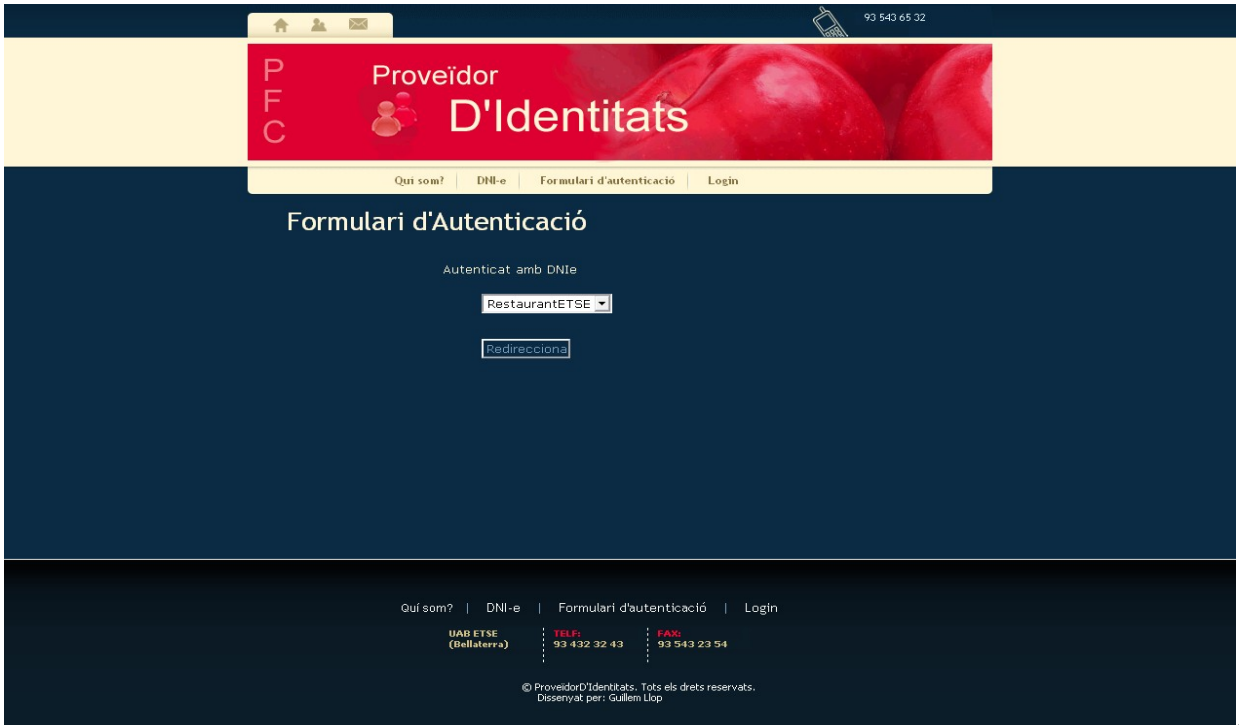
Degut a que el restaurant demana una autenticació, redirigeix a la persona cap al proveïdor d'identitats. La persona s'autenticarà mitjançant la inserció del el DNI-E en un lector.



Imatge 45: sol·licitud del PIN del DNI-E

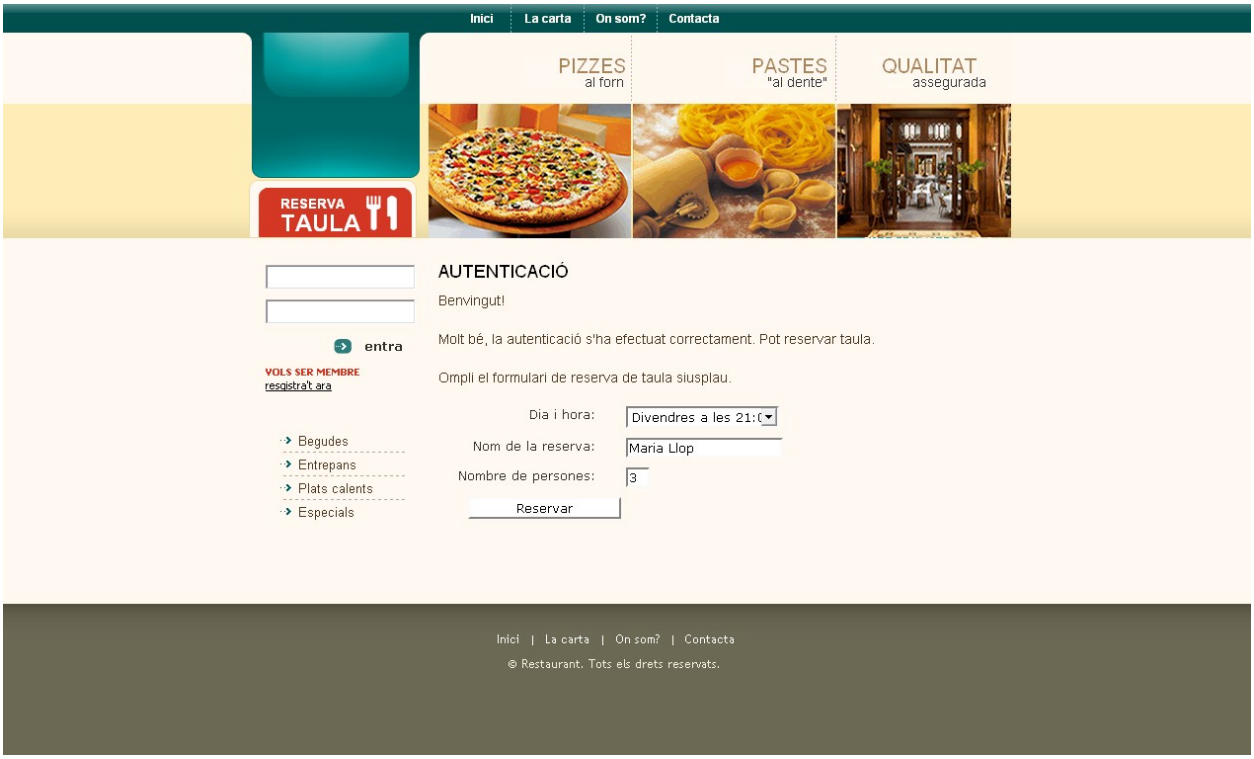


Un cop la persona s'hagi autenticat, el proveïdor d'identitats l'ofereix tornar al restaurant.



Captura de quan la persona torna al restaurant amb un identificador que li ha donat el

proveïdor d'identitats. El restaurant agafa l'identificador i sol·licita al servei web del proveïdor d'identitats l'autenticació i reputació de la persona. Si està d'acord amb la reputació rebuda permet a la persona reservar taula. Si no l'informa de manera educada de que la reserva no és possible.

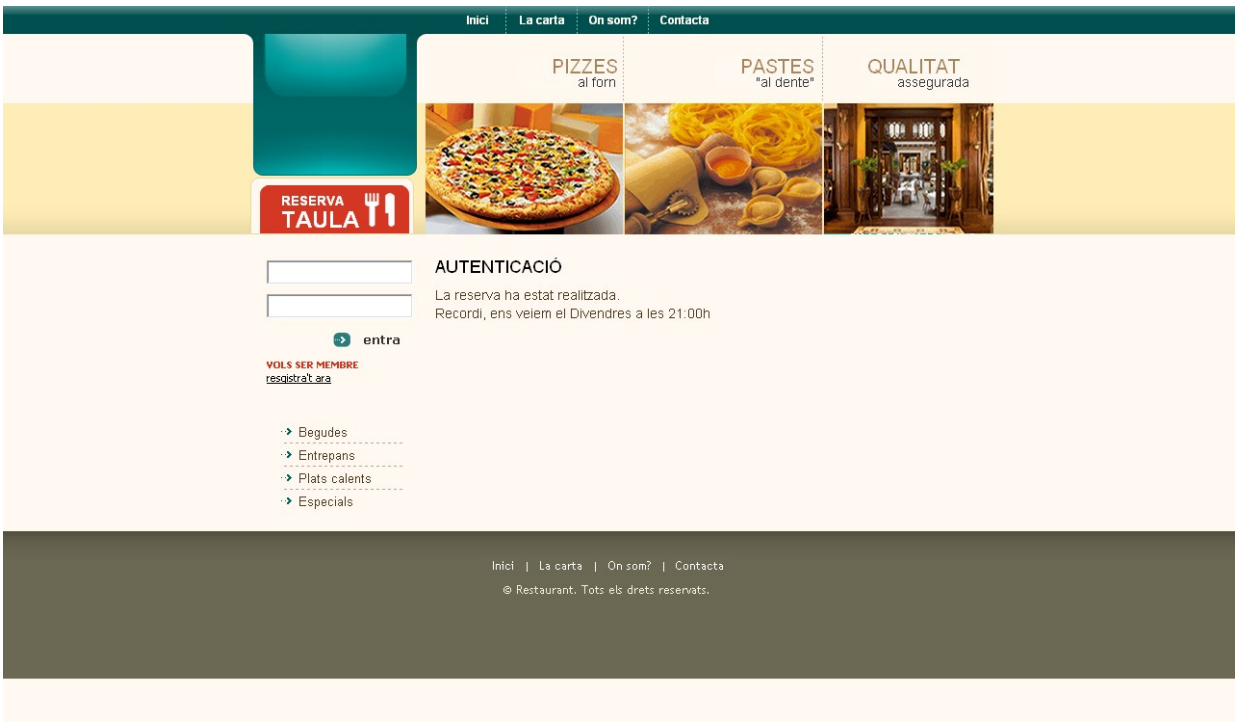


Imatge 48: autenticació en el proveïdor de servei realitzada

A l'hora, en el proveïdor d'identitats, si aquesta persona mai havia estat autenticada abans en el sistema, s'insereix en la base de dades. Veiem en la Imatge 49: nova entrada en la plana de llistat de persones autenticades de l'administració del proveïdor d'identitats com la nova persona ha estat inserida amb una reputació inicial de zero.

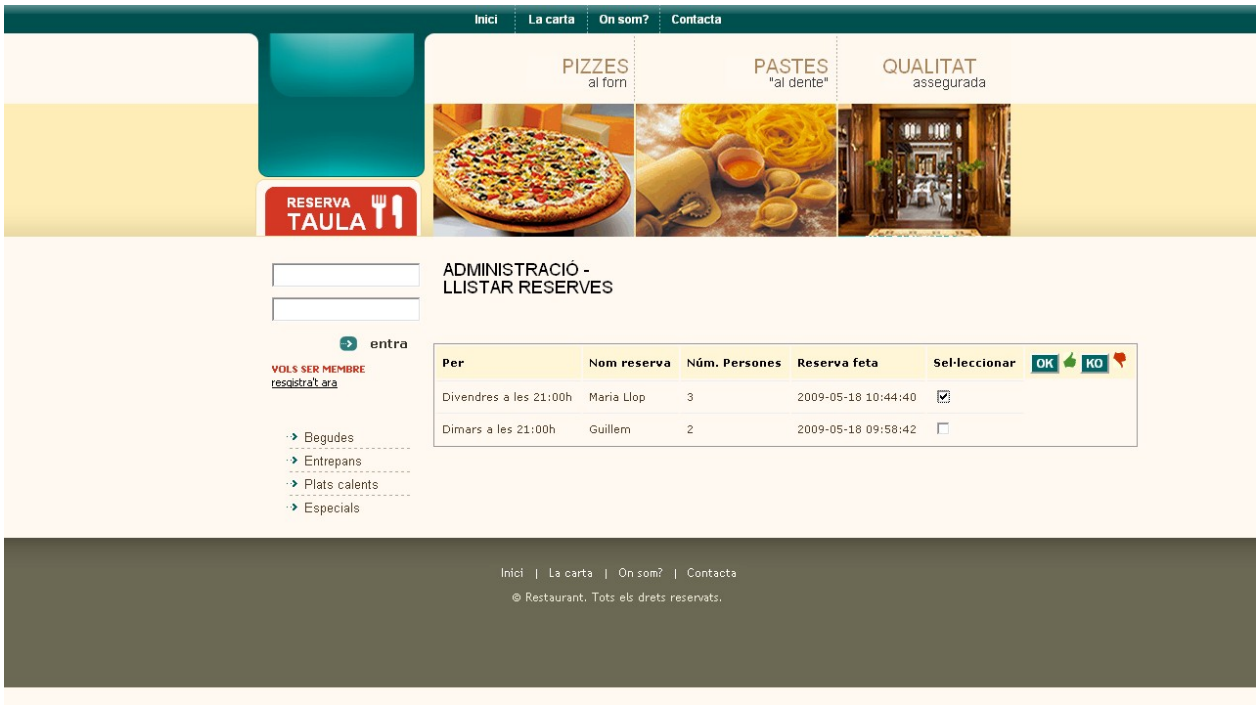
Imatge 49: nova entrada en la plana de llistat de persones autenticades de l'administració del proveïdor d'identitats

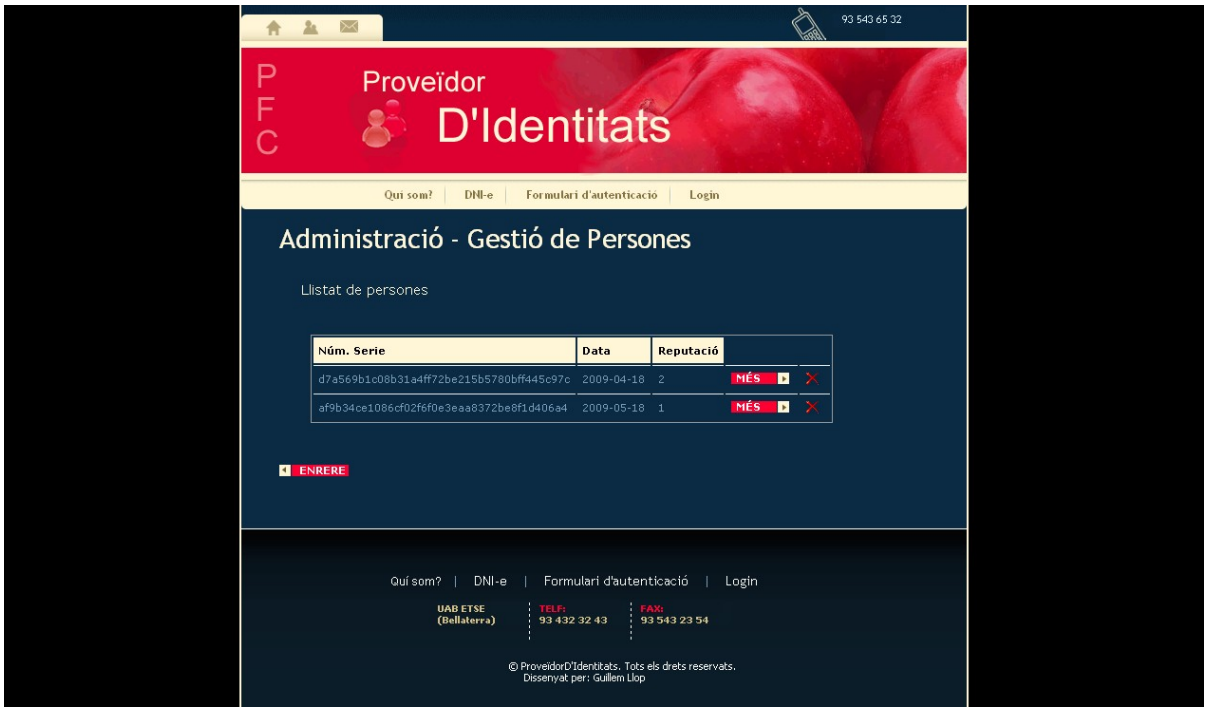
Al final la sol·licitat de la reserva de taula ha estat realitzada correctament per la persona autenticada.



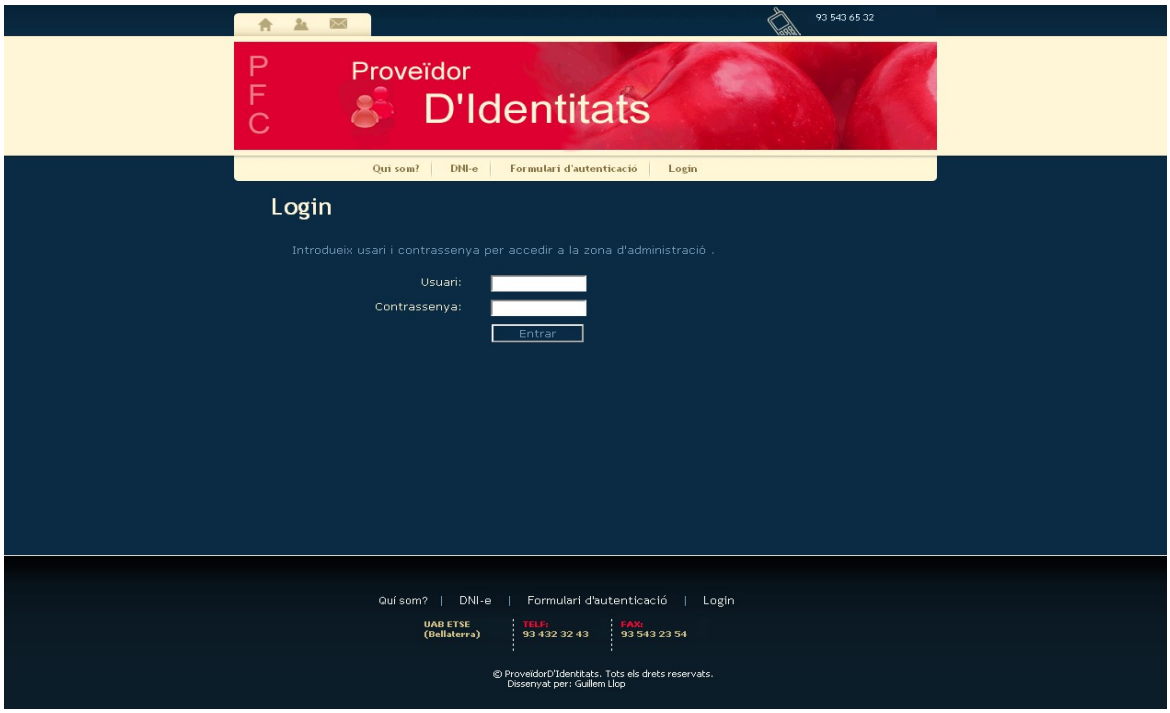
Imatge 50: servei realitzat

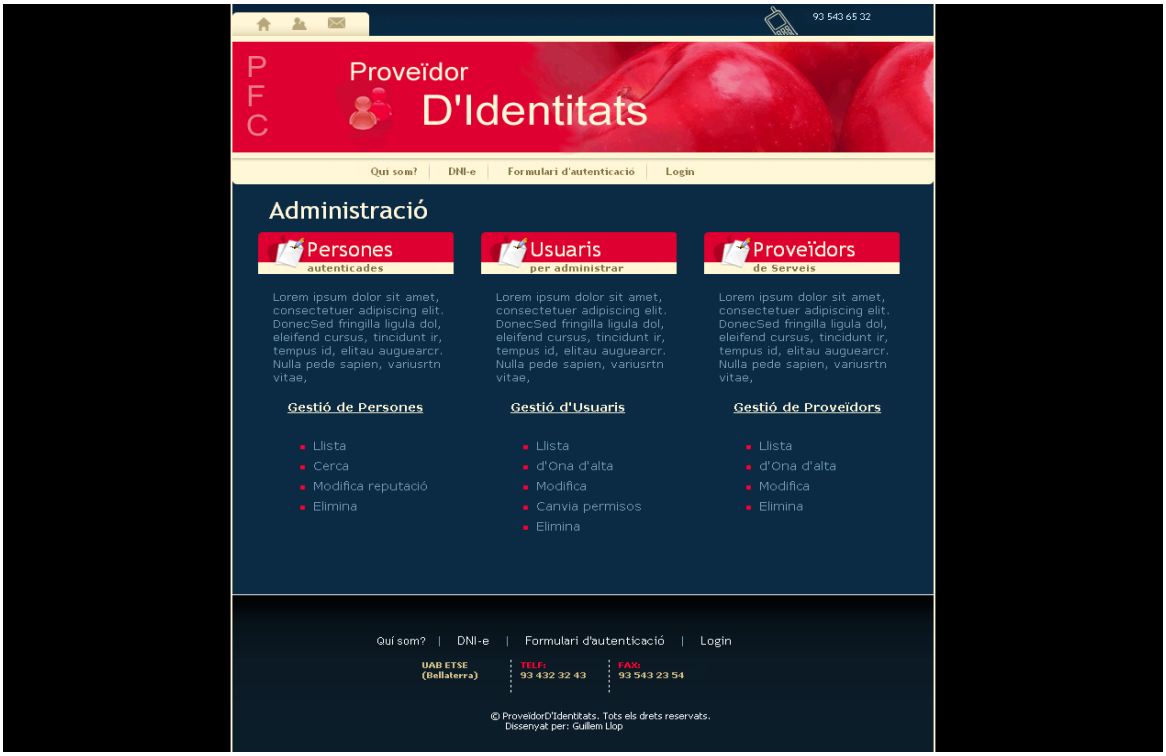
El restaurant podrà votar per actualitzar la reputació de les persones en funció del comportament d'aquestes i la reputació s'actualitzarà en la en la base de dades del proveïdor d'identitats.

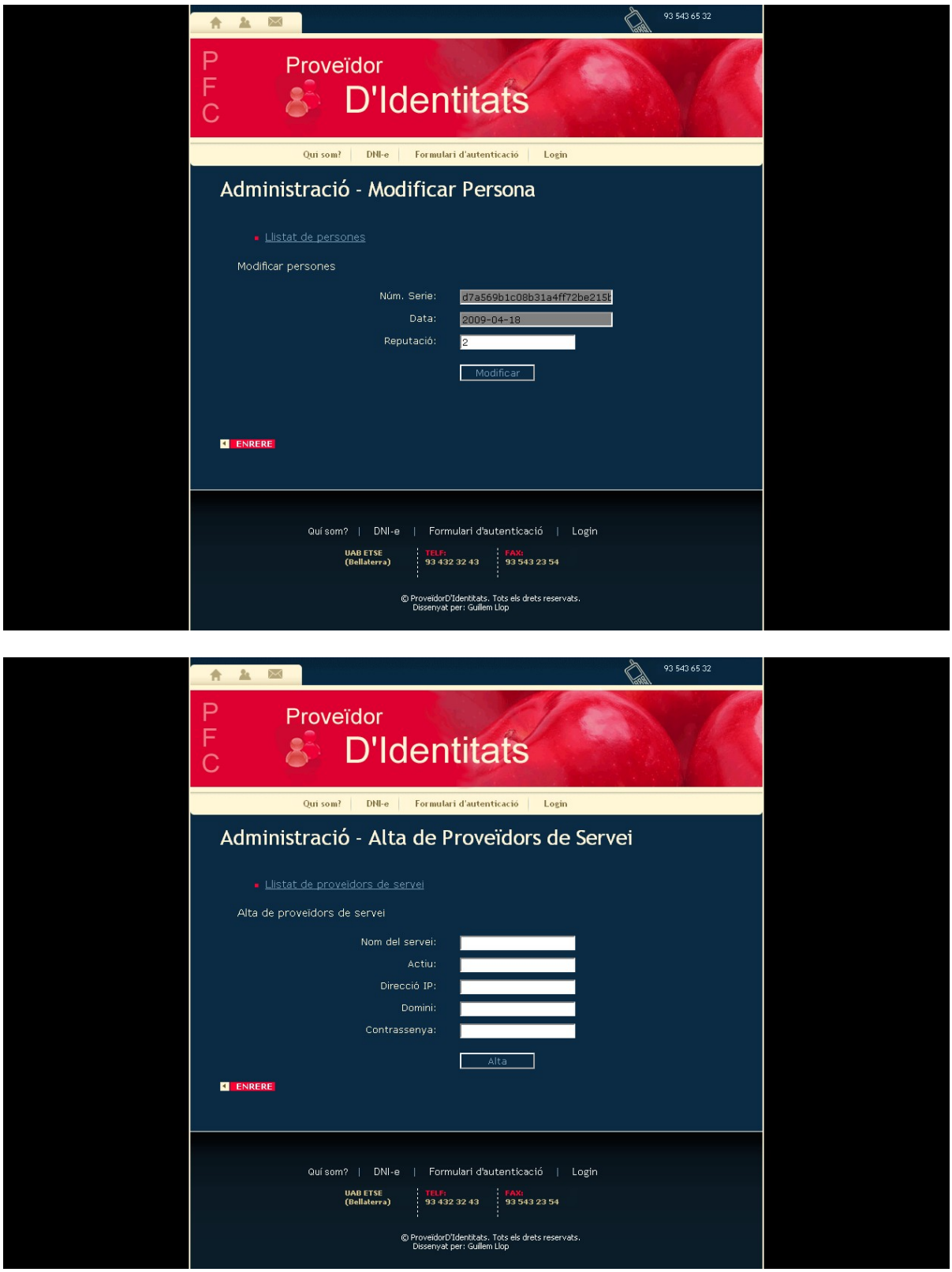




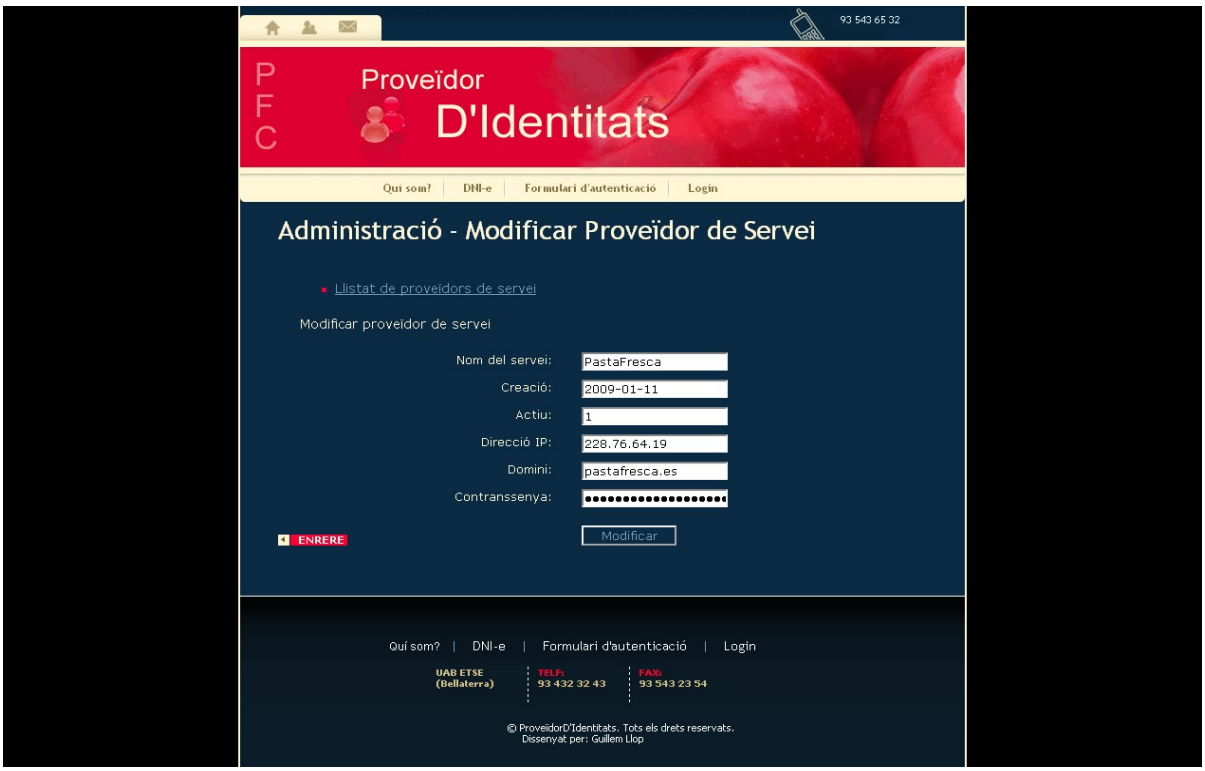
Plana d'entrada a la part d'administració del proveïdor d'identitats i les respectives funcionalitats que presenta.







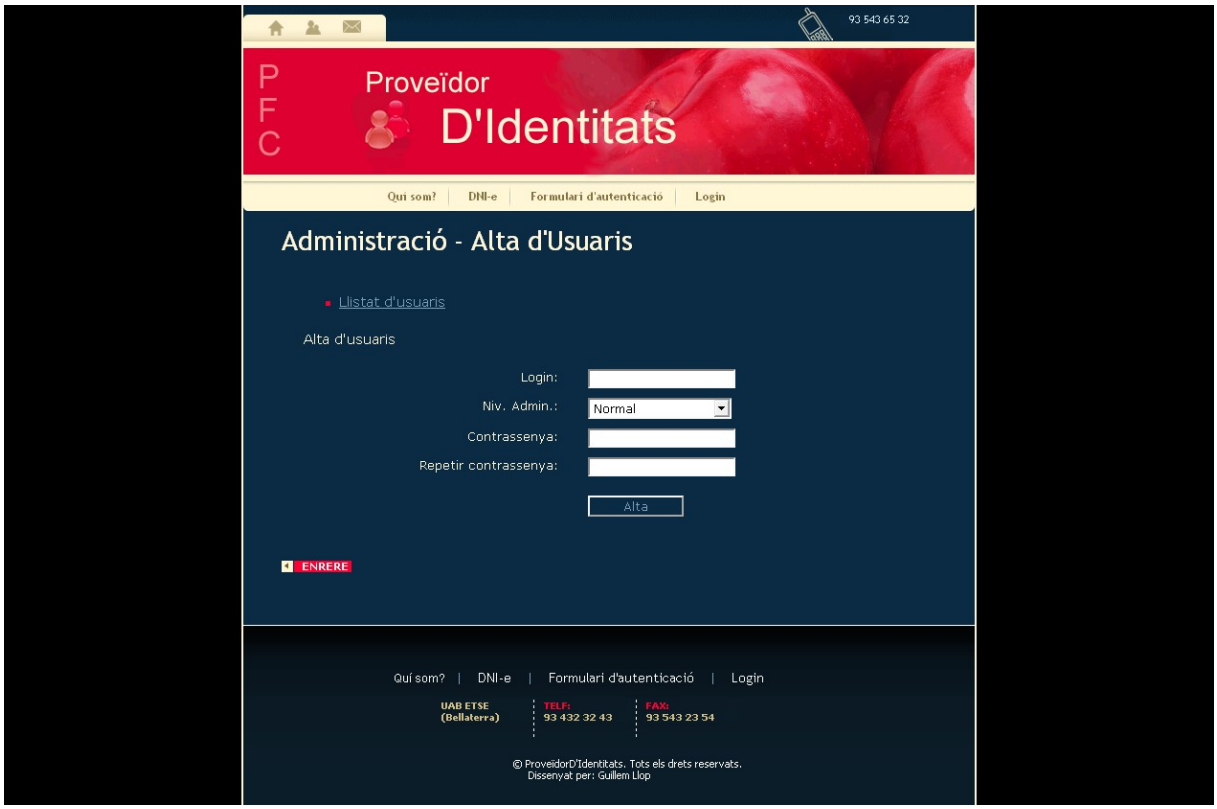
Imatge 56: plana d'inserció de proveïdor de servei

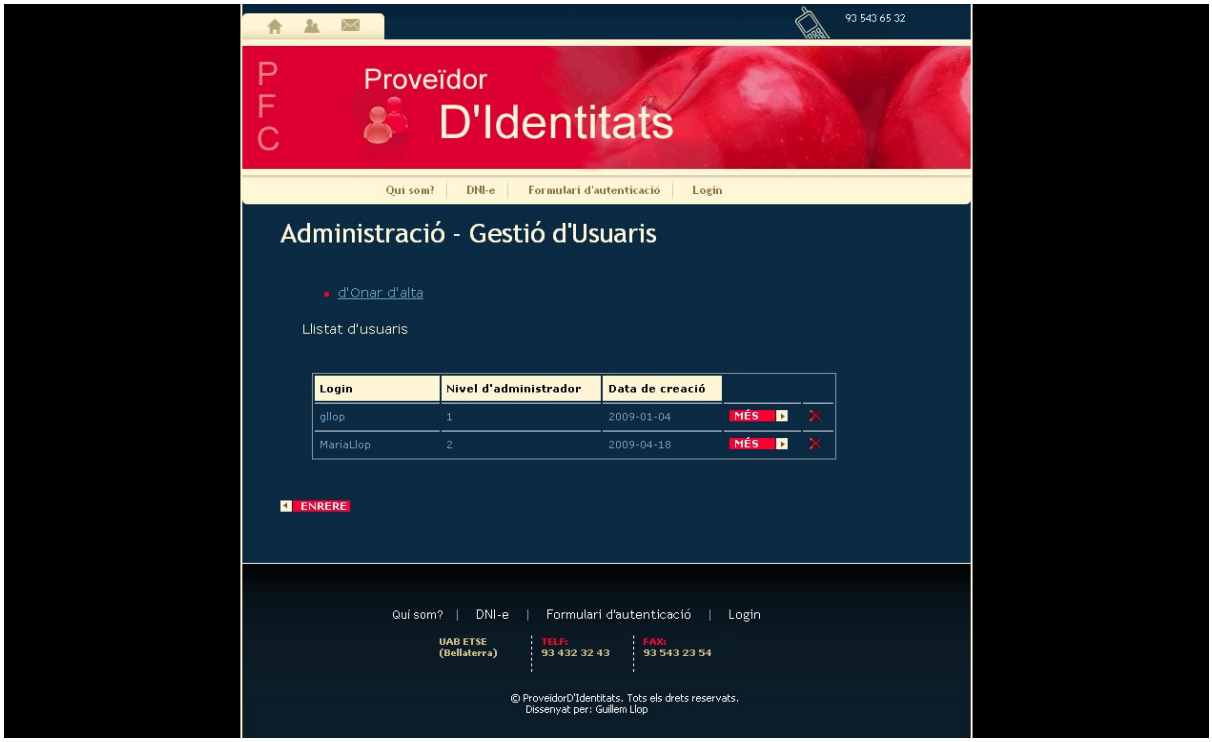


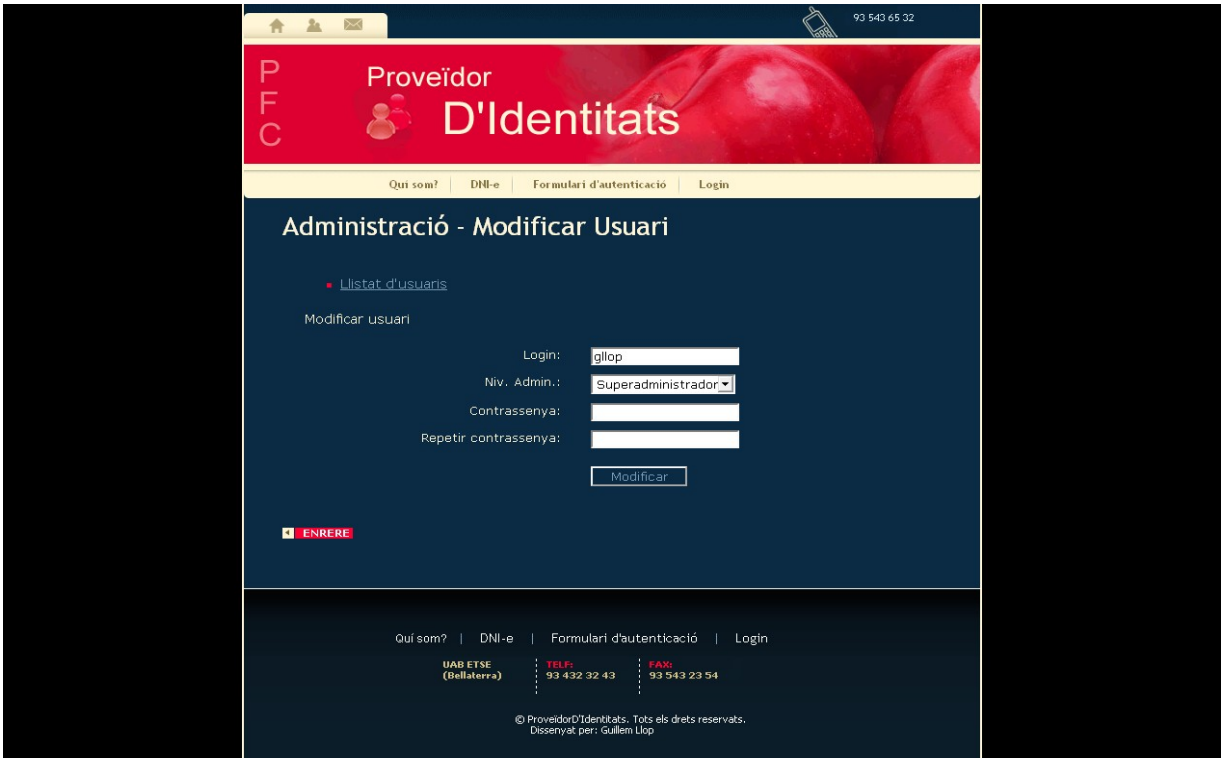
Imatge 58: plana de modificació de proveïdor de servei

A continuació es mostren les planes de gestió d'usuaris administradors del portal providentitats.com. No han estat inclosos en els requeriments funcionals, els casos d'ús ni els diagrames de seqüència corresponents degut a que no són tant rellevant pel projecte com la resta de funcionalitats.

Existeixen dos nivells possibles d'administració: administrador i superadministrador. I depenent del nivell del que es disposi serà possible realitzar segons quines funcionalitats.







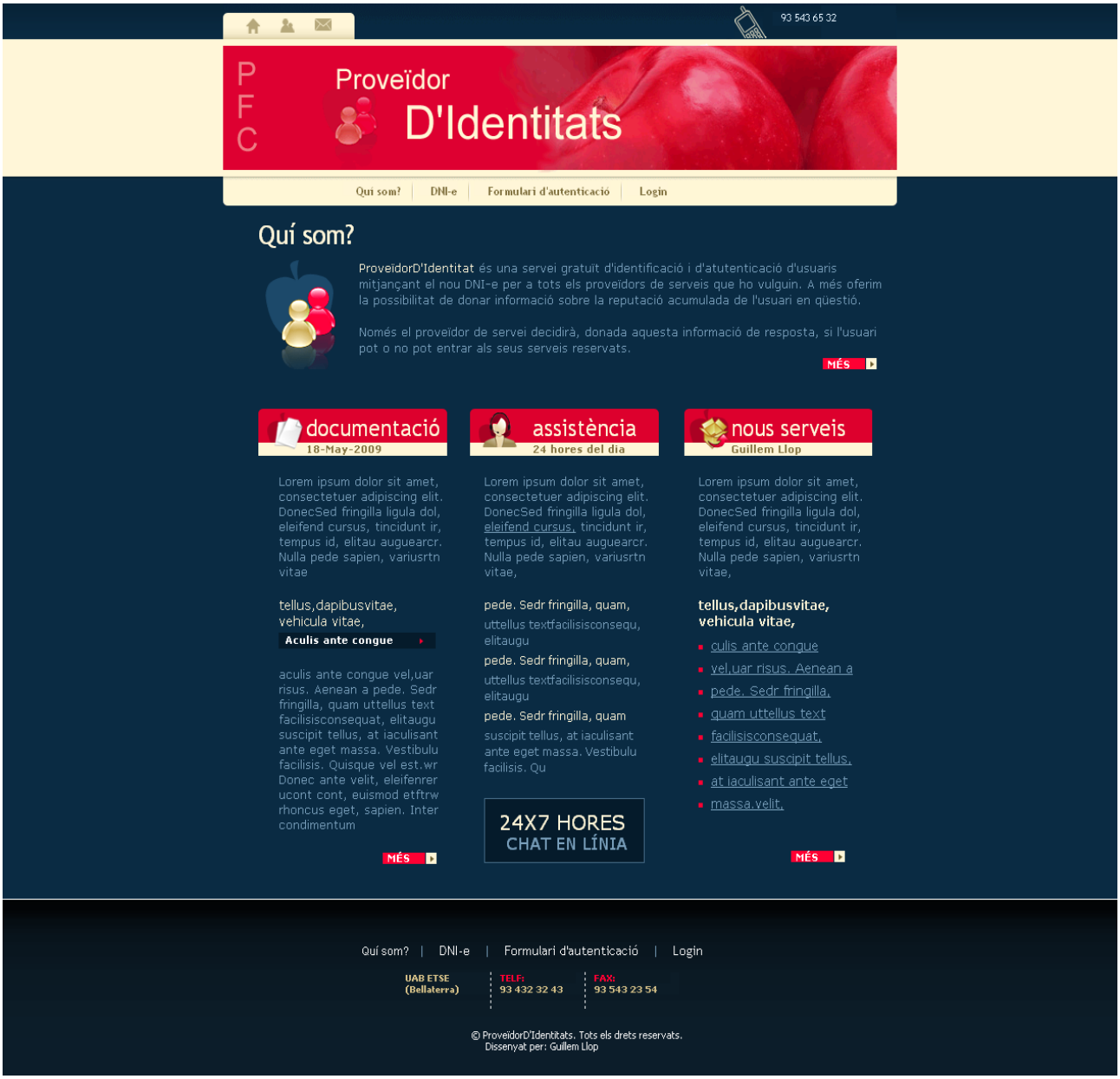
Imatge 61: plana de modificació dels usuaris administradors del proveïdor d'identitats

Mostro les planes del WSDL del servei web mostrant les diferents entrades, sortides o explicacions sobre els diferents mètodes existents.

Imatge 63: WSDL del servei web del proveïdor d'identitats 2

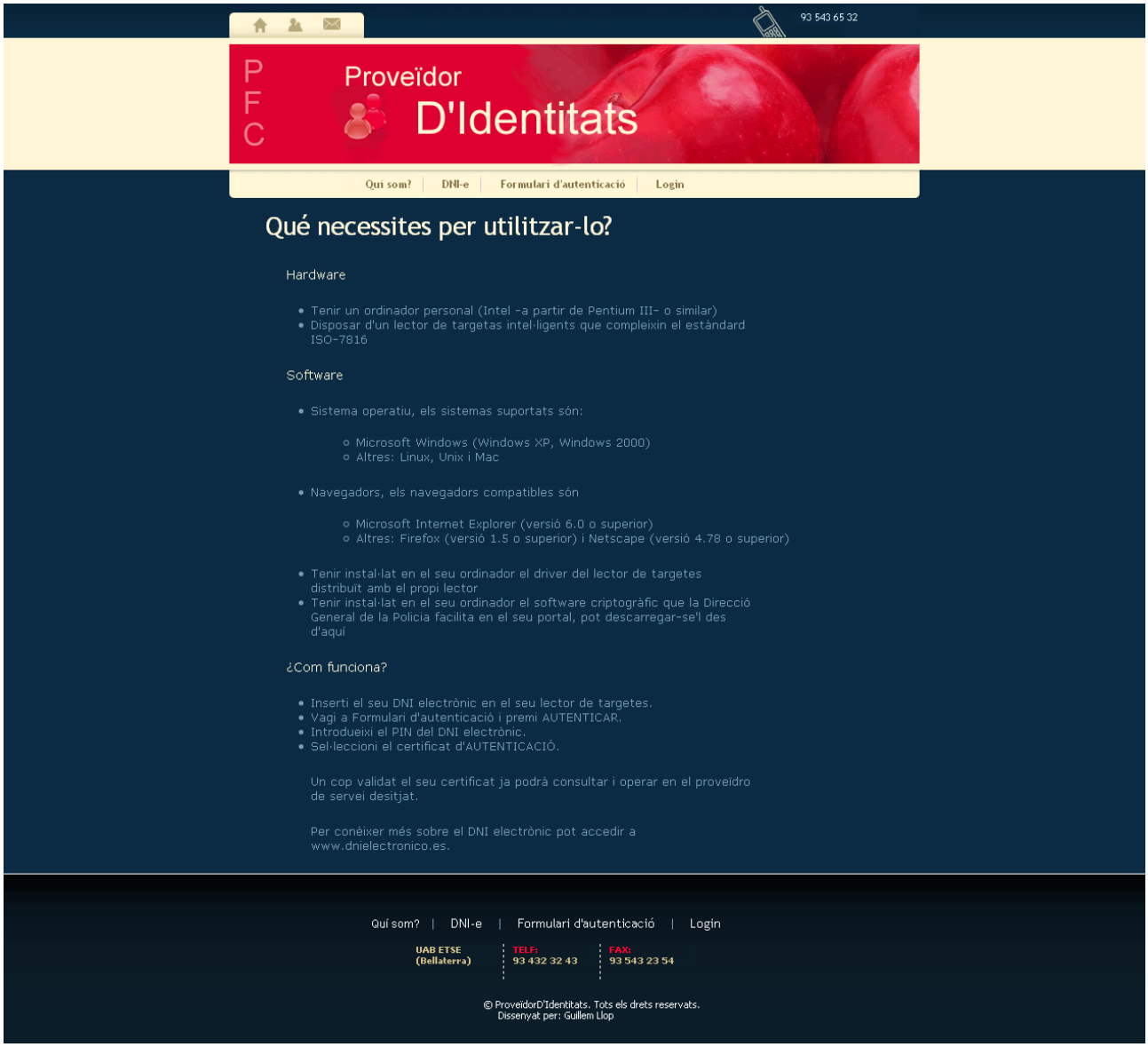
Plana corresponent a la plana inicial del proveïdor d'identitats a on les persones troben un breu resum del que es poden trobar. Hi ha els telèfons i e-mails de contacte i assistència tal com especifica la LSSI que hi ha d'haver.

En els diferents links podran descarregar els drivers o firmwares necessaris pel bon funcionament de l'autenticació.



Imatge 64: plana d'inici del proveïdor d'identitats

Plana d'explicació en la part pública del web del proveïdor d'identitats informant de quins són els requisits a complir per a l'autenticació.



Imatge 65: plana d'explicació per poder autenticar-se amb el DNI-E

6. Conclusions

Per acabar plantejo les raons per les que crec que he assolit els objectius inicials i les que podrien ser unes bones millores pel futur o les que amb temps hauria implementat al projecte. Tot seguit una valoració del que ha estat fer el projecte, quines han estat les coses que més m'han satisfet i del que crec que m'ha aportat.

6.1. Objectius complerts

Donats els Objectius generals del projecte (Definició i estudi del problema) i el protocol de comunicació que establia en la Imatge 10: seqüència de camí a seguir (Camí a seguir i estudi d'alternatives i viabilitat) he anat complint tots els objectius amb el temps establert per cada objectiu (Planificació).

En quan al resultat del disseny dels portals del proveïdor de servei (restaurant.com) com el del proveïdor d'identitats (providentitats.com) així com de les seves diferents funcionalitats es mostren durant l'apartat de Funcionalitat (captures). S'han seguit els models, les passes i lògica definides durant l'Anàlisi del sistema i el Disseny del sistema.

Era tant important seguir amb la filosofia que predicava SAML i adaptada al que seria el meu protocol de comunicació i seqüència d'accions dissenyada per cobrir els objectius (Diagrames de seqüència del protocol (interacció)). La idea era protegir la privacitat de les persones autenticades cara als proveïdors de serveis però a l'hora poder assegurar que eren qui deien ser. També s'havia d'oferir un sistema de reputacions que s'aniria actualitzant en funció de vots. Tot això mitjançant una comunicació entre el proveïdor de servei i el d'identitats amb un servei web. Això s'ha portat a terme tal i com es descriu durant el Desenvolupament.

Aquestes comunicacions amb el servei web s'han dotat de seguretat com requerien els objectius inicials. Per alguns casos amb SSL per dotar d'integritat, confidencialitat o autenticació i/o amb capçaleres WS-Security per autenticar als diferents proveïdors de serveis per a cada petició que feien al servei web.

Crec també haver cobert les demandes de la LSSI i LOPD al crear apartats explicatius i de contacte per oferir transparència a les persones que s'han d'autenticar. Les dades personals de cada persona mai es distribueixen i si en tot cas el nombre de sèrie del DNI-E sí que es guarda en una base de dades, es fa un cop aplicada una funció 'hash'.

Haig de dir també que les dates d'entrega s'han respectat totes i donat que per algunes vaig acabar una mica abans vaig implementar altres aspectes que no es tenien en compte en un principi. Parlo de l'especificació WSDL o de la gestió de les persones administradores del portal providentitats.com.

6.2. Possibles millores

Arribat a una fase estable del projecte en que tot funciona per unes proves bàsiques de funcionament en un servidor local tracto d'explicar quines són al meu entendre les millores que amb temps aplicaria per millorar la versió actual. I tenint en compte que les millores d'un projecte informàtic mai acaben degut a que el factor humà deixa molts errors en la implementació i sempre apareixeran "bugs" i més quan les proves les fa el mateix programador que amb tota seguretat prova coses que una persona aliena al projecte provaria de diferent manera. Trobo tres grans tipus de millores diferents que s'haurien de tenir en compte: les de usabilitat dels portals web, les de funcionalitat i les de rendiment.

En quant les millores de usabilitat, que és la ciència que estudia de quina manera un usuari entén el mapa de navegació del portal i a on trobar o entendre el que se li demana correctament, hi ha unes quantes coses que crec que es podria millorar.

Per una banda el formulari de Login pels administradors del portal restaurant.com (veure Imatge 42: plana d'inici del proveïdor de servei) queda just per sota del link de reservar taula per les persones no administradores. Pot portar confusions a una persona que vulgui reservar taula i acabi omplint el formulari per entrar a la zona d'administració del portal. Crec que caldria fer un petit link en la part superior dreta, que és a on s'acostuma a posar, on portés al formulari d'entrada. Per altra banda pel link de reservar taula caldria remarcar que

efectivament és un link ja que sembla més bé una imatge i prou.

Continuant amb el portal restaurant.com, un cop s'està efectuant la reserva de taula hi ha un selector per triar dia i hora (veure Imatge 48: autenticació en el proveïdor de servei realitzada). Però aquest selector proposa unes dates i hores estàtiques. Hi ha llibreries per Internet que un cop integrades al teu portal ofereixen d'una manera molt còmoda un calendari dinàmic. Donaria més possibilitats de tria a la persona per fer la reserva.

Pel portal providentitats.com, per altra banda, crec que el link de formulari d'autenticació se li dóna la mateixa importància que a la resta de links quan hauria d'haver un formulari ben vistós des de la plana principal (veure Imatge 64: plana d'inici del proveïdor d'identitats) ja que és principal funcionalitat del web.

De la navegabilitat de la part administrativa del providentitats.com tampoc n'estic del tot satisfet ja que si bé és cert que el menú principal, del que parlaré més endavant, està ben distribuït, un cop entres en cada una de les parts a administrar apareix per defecte el llistat de la taula corresponent quan potser hauria de preguntar primer què es vol fer (veure S'ha produït un error: No s'ha trobat la font de referència); si inserir o bé llistar o el que sigui.

Pel que fa al menú principal de la part administrativa del providentitats.com (veure Imatge 55: plana de modificació de la reputació de les persones autenticades) trobo que el disseny es massa igual al de la resta del web. Només canvia els marges del portal que es tornen negres. Crec que quedaria millor i més entenedor si el contrast en el disseny fos més important. Potser canviant els colors i fent una capçalera específica.

En quant a les funcionalitats es podrien millorara moltes coses degut a que els requeriments funcionals poden ser tants com es vulguin, oferint sempre més i més coses.

Del que m'he quedat més insatisfet ha estat la manera d'autenticar als proveïdors de serveis des del servei web. Tot i que s'utilitza una capçalera WS-Security amb login i password i a més es comprova el domini des d'on ve la petició, no deixa de ser un autenticat amb clau simètrica tot i que s'ha de dir que s'ha afegit comunicació SSL per resoldre aquesta mancança. S'hagués pogut enviar un certificat digital per la capçalera per autenticar d'una manera encara més fiable a cada proveïdor d'identitats, o bé afegir integritat i confidencialitat a nivell de missatge amb signats i xifrats XML i aprofitar d'aquesta manera més el potencial de WS-

Security. Estava pensat però pel temps no ha estat possible.

El sistema de votacions el considero molt bàsic degut a que només és un nombre que va creixent o decreixent en funció de les votacions (veure Imatge 52: actualitzada la reputació en la plana de llistat de persones autenticades de l'administració del proveïdor d'identitats). Hi ha altres indicadors de reputació vistos en altres web en que hi ha dos nombres; el de vots positius i el de negatius. D'aquesta segona manera es pot contar el nombre total de vots i per tant calcular un percentatge de confiança. A favor té que aquesta millora no portaria massa temps portar-la a terme.

Es podria trobar una solució al problema actual de no poder utilitzar cookies en servidor local per diferents dominis en comptes de la redirecció utilitzada passant el identificador de la persona per GET que es fa actualment. Tot i que s'ha de dir que en servidor real sí que funciona i s'ha deixat el codi comentat.

Actualment un cop la persona queda autenticada en providentitats.com se li mostra una selecció de proveïdors de serveis amb el proveïdor de servei del qual ve marcat per defecte (veure Imatge 47: autenticació realitzada i redirecció). Es podria fer una redirecció automàtica per estalviar-se aquest pas potser innecessari.

En un futur quan hi haguessin moltes persones autenticades amb la seva reputació respectiva al sistema hauria de ser bastant molest haver de cercar a una persona concreta amb la actual funcionalitat de llistar persones (veure Imatge 49: nova entrada en la plana de llistat de persones autenticades de l'administració del proveïdor d'identitats). Una millora seria implementar un petit cercador per cercar persones concretes o filtres per reputació o altres.

Per la millora del rendiment és difícil proposar millores degut a que només s'han fet proves de tot el muntatge en servidor local on les peticions que es poden realitzar i la sobrecàrrega del servidor no té res a veure amb un àmbit de proves real.

Les peticions que es fan a la base de dades són bastant simples i no han de portar molta demora en la resposta encara que hi hagi moltes entrades. De totes maneres seria bo implementar un sistema de neteja automatitzat de persones autenticades de la base de dades per evitar entrades innecessàries.

6.3. Valoració

Després de finalitzar el PFC i tornant la vista enrere penso que ha estat un treball abans que res portat al dia i en que la constància a estat clau per la seva consecució. Trobo molt important veure un projecte com la suma de moltes parts i etapes diferenciades en que cal abordar pas per pas amb la filosofia de divideix i conqueriràs per no agafar vertigen un cop es comença. Cada fase del projecte cal però portar-la de la millor manera possible dintre del plaç; tot és millorable amb temps i recursos però en molts casos cal ser humil i no voler anar més enllà i dedicar-se a cobrir els objectius bàsics en cas de que la data d'entrega d'una fase ens vingui justa.

Començant amb un petit estudi de viabilitat i anàlisi finalitzat a finals de novembre i retocats al principis de desembre es va començar la implementació a finals d'any. Crec haver complert amb totes les dates d'entrega que vaig programar i negociar amb la tutora de projecte sempre assolint els objectius proposats. Tant és així que en un principi no estava previst la petita part administrativa de cada portal i que es va finalment afegir que permet la gestió de les persones autenticades, dels proveïdors de serveis i dels usuaris administradors del portal providentitats.com i de la gestió de reserves pel que fa al restaurant.com.

Vull remarcar també que he volgut fer les coses de millor manera que he considerat. A l'hora d'implementar ho he fet orientat a objectes pensant amb el l'encapsulament del codi i a la gestió d'errors o fent servir especificacions com WSDL (veure Imatge 62: WSDL del servei web del proveïdor d'identitats) per arrodonir una mica més la feina. A l'hora de dissenyar he pensat amb els estàndards de w3c separant forma de contingut i utilització de XHTML, he procurat que el disseny dels portals fossin el més corporatius i reals possibles. Per a la documentació he fet servir modelats UML apresos en enginyeria del software, etc.

Res ha estat fàcil però crec que per això penso haver aprés força amb el PFC. Els aspectes tècnics crec que són importants però el que més valoro és el fet de portar a terme un procés llarg d'anàlisi d'un problema, el seu disseny i implementació amb unes dates, formalismes i negociacions a complir en el PFC. Crec que aquesta experiència és la diferència amb la resta d'assignatures.

7. Bibliografia

- Plana oficial del DNI-E [onlie][ref. 15 de Novembre] http://www.dnielectronico.es/
- Article de les diferències entre Rest i SOAP per IBM [online][ref. 17 de Novembre] http://www.ibm.com/developerworks/webservices/library/ws-restvsoap/index.html
- Presentació de seguretat en serveis web [online][ref. 18 de Novembre] http://www.slideshare.net/jselman/seguridad-para-servicios-web-presentation
- Article sobre serveis web [online][ref. 19 de Novembre] http://webservices.xml.com/pub/a/ws/2003/09/30/soa.html
- Desenvolupador de SAML [online][ref.20 de Novembre] http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
- Article en PDF sobre la seguretat en serveis web [online][20 de Novembre] http://www.samelan.com/oscargonzalez/doc/ws_security.pdf
- Presentació en PDF per S21sec sobre Rest i la seva seguretat [online][ref. 22 de Novembre] http://www.fistconference.org/files/ramonpinuagas21secrest1.pdf
- Article de SUN sobre el funcionament de SAML2.0 [online][ref. 23 de Novembre] http://developers.sun.com/identity/reference/techart/lightbulb.html
- Article sobre les avantatges i signatura única en SAML (SSO) [online][ref. 24 de Novembre] https://www.idg.es/comunicaciones/articulo.asp?id=151152
- Explicació de funcionament de SAML en Google Apps [online][ref.24 de Novembre] http://code.google.com/intl/es-ES/apis/apps/sso/saml_reference_implementation.html
- Framework de SAMP SimpleSAMLPHP [online][ref.27 de Novembre] http://rnd.feide.no/simplesamlphp
- Presentació sobre la seguretat en SSO en PDF [online][ref. 28 de Novembre] http://www.esi.uem.es/~jmgomez/eventos/jornada.seguridad.050222/Liberty.pdf
- Article dels elements de SAML per SUN[online][29 de Novembre] http://docs.sun.com/app/docs/doc/819-2142/6n4evuvvk?a=view#admen

- Article sobre estàndards sobre la gestió d'identitats [online][ref. 4 de Desembre] http://www.borrmart.es/articulo_redseguridad.php?id=816&numero=20
- Documentació sobre SAML 2.0 per OASIS en PDF [online][10 de Desembre] http://www.oasis-open.org/committees/download.php/22553/sstc-saml-tech-overview-2%200-draft-13.pdf
- Documentació per XHTML, CSS i JavaScript [online][ref.15 de Decembre] http://www.w3schools.com/
- Plana oficial del servidor web Apache [online][ref. 15 de Desembre] http://www.apache.org/
- Guia d'XHTML per w3c [online][ref. 16 de Desembre] http://www.w3c.es/Divulgacion/Guiasbreves/XHTML
- Guia de CSS per w3c [online][ref. 16 de Desembre] http://www.w3c.es/divulgacion/guiasbreves/HojasEstilo
- Plana oficial del sistema gestor de base de dades MySQL [online][ref. 25 de Desembre] http://www.mysql.com/
- Guia d'istalació de PHP, MySQL, Apache amb SSL en PDF [online][ref. 27 de Desembre] http://www.adcommcepts.com/install-wamp-ssl.pdf
- Documentació oficial de PHP [online][ref.28 de Desembre] http://www.php.net/
- Plana web del software OpenSSL [online][ref. 7 de Febrer] http://www.openssl.org/
- Llistat de funcions OpenSLL amb PHP [online][ref. 8 de Febrer] http://es2.php.net/openssl
- Plana oficial del lector de targetes [online][ref. 10 de Febrer] http://www.c3po.es/
- Guía de configuració d'Apache i funcions PHP per autenticar amb DNI-E en PDF [online] [15 de Febrer] https://1enise.inteco.es/ponencias/ENISE-T21_Isaac_Amezaga_i_Saumell.pdf
- Composició de les capçaleres WS-Security [online][ref. 22 d'Abril] http://www.onjava.com/pub/a/onjava/2005/03/30/wssecurity2.html?page=2

Resum

Protocol per autenticar a persones que sol·liciten un servei o producte en un web mitjançant un proveïdor d'identitats amb el DNI-E. El proveïdor d'identitats garanteix als proveïdors de serveis que les persones amb qui tracten són qui diuen ser i proporciona a més una reputació associada a cada persona. Aquesta comunicació es fa amb un servei web que prèvia autenticació del proveïdor de servei podrà realitzar les diferents peticions d'autenticitat i de reputació dels seus clients. Donat que es tracten amb dades personals, durant el protocol es protegeix en tot moment l'autèntica identitat de cada persona per tal de que pugui mantenir el seu anonimat.

Resumen

Protocolo para autenticar a personas que solicitan un servicio o producto en una web mediante un proveedor de identidades con el DNI-E. El proveedor de identidades garantiza a los proveedores de servicios que las personas con las que tratan son quienes dicen ser y proporciona además una reputación asociada a cada persona. Esta comunicación se hace con un servicio web que, previa autenticación del proveedor de servicio, podrá realizar las diferentes peticiones de autenticidad y de reputación de sus clientes. Dado que se trata con datos personales, durante el protocolo se protege en todo momento la auténtica identidad de cada persona para que pueda mantener su anonimato.

Abstract

Protocol to authenticate people requesting a service or a product in a website through an identity provider using “DNI-E”. The identity provider guarantees the services providers that their clients are who they really seem and also provides an associated reputation to each person. The services provider will be able to make different demands of authenticity and reputation of its customers, but previously he has to authenticate himself with the Web Service. Due to the use of personal data, the protocol protects in every moment, the truth identity and the anonymity of each person.