Escenari Client - Servidor Segur

Memòria

Andreu Sans Fons

Juny 2008

Enginyeria Tècnica Informàtica de Sistemes

Consultor: Carlos Ares Angulo

UOC
Universitat Oberta de Catalunya
www.uoc.edu

A Encarna i Maria, sense la seva font d'energia
i comprensió no hauria estat possible aquest treball.

1. Agraïments

En primer lloc agrair al consultor pel seu suport en el desenvolupament d'aquest treball i en general a la Universitat Oberta de Catalunya que permet retrobar la il·lusió pel coneixement i l'aprenentatge, al marge d'edat, feina i situació social. Poder compaginar de manera efectiva els estudis amb la situació laboral i familiar de cadascú estic segur que ha estat molt positiu per a moltes persones que com en el meu cas, hem trobat un camí que en temps passats estava tancat a partir de certa edat. Gràcies per obrir les possibilitats d'aprendre a tanta gent.

Agrair als meus pares el seu esforç i afany de superació en circumstàncies molt adverses que ens han ensenyat a mirar endavant i no donar-se per vençut. Al meu germà pel seu esforç del dia a dia i a la meva germana pel seu recent doctorat. Gràcies a tots, tots teniu el vostre percentatge d'esforç en aquest treball.

Per últim, si hi ha algú que ha compartit l'esforç d'aquesta carrera és la Encarna, sense el seu ajut ens moments baixos i en els grans moments que he tingut en aquests anys no hauria estat possible arribar fins aquest punt. Gràcies per compartir amb mi les PACS (paraula que ja forma part de la nostra vida), els treballs, exàmens i facilitar-me el camí per disposar del temps necessari per poder tirar endavant, gràcies per estar al meu costat i compartir tantes coses que omplen les nostres vides.

I com dir-ho, la Maria, que va néixer al començar aquests estudis i ha anat creixent al meu costat. Gràcies per la teva font d'energia, per poder compartir el teu aprenentatge i permetre que a vegades no hagi pogut jugar amb tu com hauria desitjat. Gràcies per ser qui ets.

2. Resum

El present document descriu el treball de fi de carrera de *Enginyeria Tècnica Informàtica de Sistemes* en *l'àrea de seguretat informàtica* que d'acord amb l'enunciat planteja la implementació d'un escenari segur *client-servidor* amb un proveïdor d'identitat i control d'accés extern.

En concret, s'han implementat tres components diferenciats:

- Proveïdor de Servei
- Petició de Client
- Proveïdor d'identitat

El *Proveïdor de Servei* és una aplicació web que dóna accés de manera controlada a un nombre determinat de recursos al que s'hi connecten els clients mitjançant un canal segur, la *Petició de Client* és un component que envia les dades facilitades pel proveïdor de servei al *Proveïdor d'identitat* i torna la resposta obtinguda per tal que el proveïdor de servei apliqui el control d'accés corresponent i deixi accedir als recursos en funció del resultat obtingut.

Pel que fa al Proveïdor d'identitat disposa de dos funcionalitats clarament diferenciades, una és la aplicació web de gestió administrativa de permisos i l'altra el servei web on hi connecten els clients, un cop feta la sol·licitud de servei, per sol·licitar la resposta a la petició d'accés a un recurs.

Tots els processos que formen part de la solució han estat securitzats mitjançant diferents mecanismes de seguretat com són l'establiment de canals segurs, la utilització d'autenticació amb certificat digital i la utilització de signatures digitals. Cal destacar la utilització del *DNI Electrònic* com a mitjà d'autenticació i signatura de client.

3. Índex de Continguts

4. Índex de Figures

5. Memòria Tècnica

En aquest apartat és descriuen els diferents punts propis de la memòria tècnica començant per una introducció dels aspectes genèrics de la solució per passar a continuació a detallar els fonaments, disseny, implementació, instal·lació i funcionament del producte obtingut.

5.1 Introducció

D'acord amb el pla docent, el treball fi de carrera consisteix en la implementació d'un escenari segur client - servidor amb un proveïdor d'identitat i un control d'accés extern. En concret, s'han d'implementar principalment dos components web, el proveïdor de servei i el proveïdor d'identitat amb els següents requeriments:

Proveïdor de Servei:

El proveïdor de servei ha de disposar dels següents components i funcionalitats:

- Els clients és connecten al proveïdor de servei a través d'un canal segur.

- El proveïdor de servei disposa d'una aplicació Web convencional que s'executa en el servidor. Aquesta aplicació ha de poder establir connexions segures sense autenticar al client, ja que serà el proveïdor d'identitat qui s'encarregarà d'aquesta funció. Serà necessari que el servidor web disposi d'un certificat digital per establir la connexió segura i que utilitzarà també per signar les dades de petició del client.

- El proveïdor de servei disposarà de control d'accés als recursos en funció del resultat de la autenticació realitzada per una tercera entitat de confiança, el proveïdor d'identitat.

- El proveïdor de servei ha de poder validar les signatures rebudes del client signades del proveïdor d'identitat.

Proveïdor d'identitat:

El proveïdor d'identitat ha de disposar dels següents components i funcionalitats:

- Aplicació web de gestió administrativa de permisos. Aquest component del Proveïdor d'identitat té com a funció gestionar la informació dels clients, recursos i proveïdors de serveis. L'accés a la administració de permisos ha de ser autenticat i mitjançant un canal segur. Serà necessari que el servidor web disposi d'un certificat digital per establir la connexió segura i que utilitzarà també per signar la resposta a la petició.

- Servei web on hi contacten els clients un cop feta la sol·licitud al proveïdor de servei. Aquest servei ha de poder enviar els missatges SOAP corresponents a la resposta de la petició del client (signada pel proveïdor de servei). Aquest servei també haurà de ser capaç de validar la signatura tant del client com del proveïdor de servei.

Clients:

Els clients contactaran mitjançant navegador web tant al proveïdor de servei com el proveïdor d'identitat i disposaran d'un certificat digital emès per una entitat certificadora de confiança pel proveïdor d'identitat, aquest certificat és utilitzat per signar les dades de petició de servei amb l'objectiu que el proveïdor d'identitat els autentiqui. El navegador utilitzat pel client ha de poder enviar missatges SOAP i executar els components web necessaris per realitzar les signatures.

5.1.1 Objectius

5.1.1.1 Objectiu General

L'objectiu del projecte és la implementació d'un escenari segur client-servidor amb un proveïdor d'identitat i un control d'accés extern que funcionarà de la següent manera:

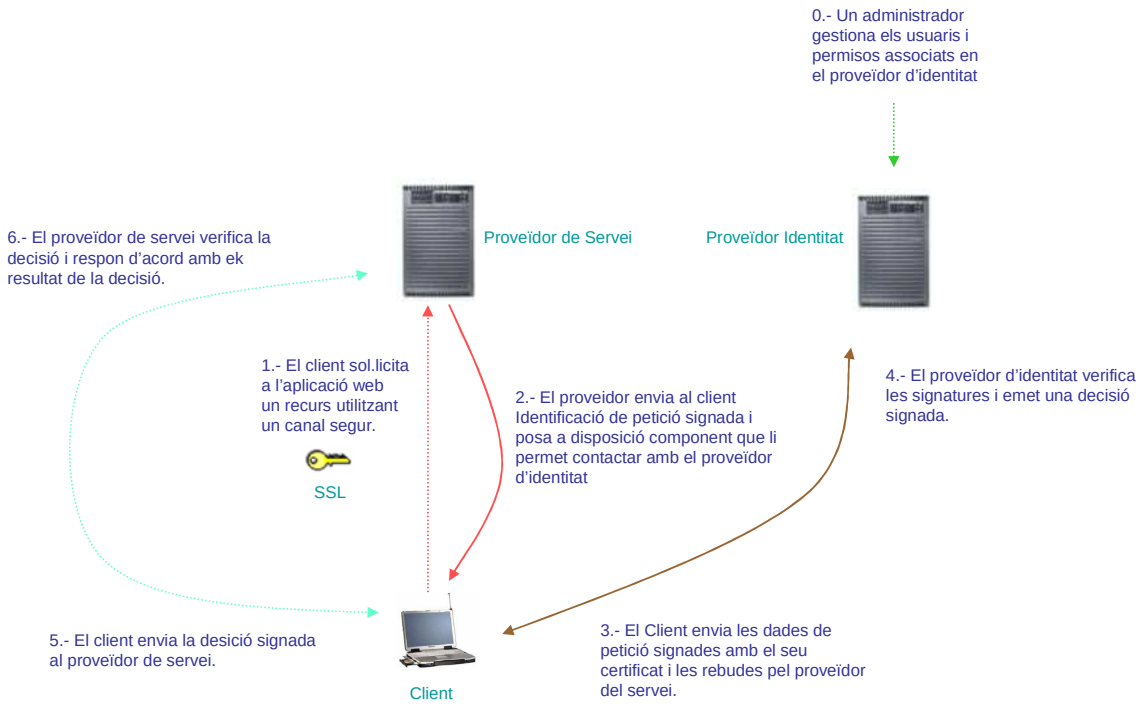


Figura 1

D'acord amb el flux descrit anteriorment la solució ha de permetre d'una banda la comunicació segura amb l'aplicació i d'altra banda ha de proporcionar el control d'accés dels recursos de l'aplicació assegurant la identitat del client mitjançant l'autenticació basada en la utilització de certificats i que la portarà a terme una entitat de confiança tant pel client com pel proveïdor.

Aquest escenari ens permet disposar d'una autenticació robusta sense necessitat que el proveïdor del servei disposi de mecanismes d'autenticació complexes com poden ser autenticació de doble factor, etc. Amb la utilització d'una entitat de confiança i mitjançant la utilització de signatures digitals i certificat d'usuari reconegut és pretén assegurar la identitat del client que accedeix al servei i els permisos associats sense que hi hagi una comunicació directa entre el proveïdor del servei i el proveïdor d'identitat.

5.1.1.2 Objectius Personals

Partint de coneixements previs en comunicacions, criptografia i programació Java, els objectius personals d'aquest projecte son els d'aprofundir en la programació de aplicacions mitjançant el llenguatge Java i aprofundir en els coneixements i la utilització de certificats digitals.

També és un objectiu el planificar i executar un projecte de programació d'aplicacions en la que s'utilitzen tecnologies de xifrat ja que la meva experiència professional està vinculada a projectes de seguretat en les comunicacions en les que també intervenen tecnologies de xifrat però no el desenvolupament d'aplicacions.

5.1.2 Planificació

Per tal de portar a terme el treball de fi de carrera s'han executat les següents fases:

1. Elaboració del Pla de Treball Inicial.
2. Elaboració del Pla de Treball detallat.
3. Disseny de la Solució.
4. Desenvolupament de la aplicació.
5. Correccions.
6. Elaboració de la memòria tècnica.
7. Elaboració de la presentació i entrega del treball.

Entrant en detall, un cop realitzat el pla de treball inicial la següent tasca es la de definició de la arquitectura de la solució i la elaboració d'un pla de treball detallat d'acord amb aquesta definició.

En la fase de disseny de la solució és realitzarà una definició formal del producte en la que s'inclourà el diagrama de casos d'ús, el funcionament del producte, comunicació, dades i interfícies gràfiques.

Pel que fa al desenvolupament de la aplicació s'ha desglossat en les següents tasques a realitzar:

1. Preparació de l'entorn de desenvolupament.
    a. Instal·lació de Programari.
    b. Creació de Certificats auto-signats per als servidors web.
    c. Proves prèvies.

2. Proveïdor de Servei
    a. Aplicatiu web de servei.
    b. Applet de Identificació de Petició.

3. Proveïdor d'identitat
    a. Disseny de la Base de Dades.
    b. Aplicació web d'administració d'usuaris i proveïdor de serveis.
    c. Aplicació de validació d'identitat.

4. Integració

5. Entrega Parcial

En detall, en el primer punt s'instal·larà el programari necessari per al desenvolupament del producte, és prepararan els serveis web i és faran les proves prèvies necessàries per tal de validar el funcionament de servlets així com l'accés amb Java a la base de dades. L'apartat de proves prèvies és important ja que no tinc massa experiència en la programació de servlets i pretén estalviar temps alhora de programar els aspectes importants del desenvolupament del producte. En les proves prèvies també és definiran els aspectes formals (Interfícies, etc) que seran necessaris en la fase de disseny.

En el segon punt és desenvoluparà tot el que fa referència a un proveïdor de servei i el applet de identificació de petició. Pel que fa al servei la idea inicial és de disposar d'un llistat de recursos (directoris) que siguin accessibles en funció del resultat de la autenticació.

El tercer punt estarà dedicat al desenvolupament del proveïdor d'identitat, sent necessari tenir desenvolupat l'apartat de administrador de usuaris (clients) i proveïdors de servei abans del de validació d'identitat.

En el quart punt és desenvoluparà i verificarà la integració entre les diferents aplicacions fent les proves necessàries per fer la entrega parcial que serà l'últim punt de l'apartat de desenvolupament de l'aplicació.

L'objectiu és tenir el producte amb totes les funcionalitats bàsiques implementades per a la entrega parcial, quedant les possibles correccions, temes pendents i bateria de proves finals.

Les últimes fases del treball de fi de carrera seran les correccions dels aspectes a millorar respecte la entrega parcial, la elaboració de la memòria tècnica, presentació i finalment la entrega del treball.

La planificació de les diferents fases descrites anteriorment ha estat la següent:

	Nombre de tarea	Duración	Comienzo	Fin	Predecesoras
1	Pla de Treball (Pac 1)	5,88 días?	jue 28/02/08	jue 06/03/08	
2	Pla de Treball Detallat - Definició i Arquitectura (Pac 2)	9,88 días	vie 07/03/08	jue 20/03/08	1
3	Disseny de la Solució (Pac 3)	16 días	vie 21/03/08	vie 11/04/08	2
4	**Desenvolupament de l'Aplicació**	**48,88 días?**	**lun 10/03/08**	**jue 15/05/08**	**1**
5	**Preparació Entorn Desenvolupament**	**15 días**	**lun 10/03/08**	**lun 31/03/08**	**1**
6	Instal.lació de Programari	2 días	lun 10/03/08	mié 12/03/08	
7	Creació de Certificats	2 días	lun 10/03/08	mié 12/03/08	
8	Proves Prèvies	13 días	mié 12/03/08	lun 31/03/08	6;7
9	**Proveïdor de Servei**	**20 días**	**lun 31/03/08**	**lun 28/04/08**	**5**
10	Aplicatiu web de servei	10 días	lun 31/03/08	lun 14/04/08	
11	Applet de Identificació de Petició	10 días	lun 14/04/08	lun 28/04/08	10;3
12	**Proveïdor d'Identitat**	**20 días**	**lun 31/03/08**	**lun 28/04/08**	**5**
13	Disseny de la Base de Dades	5 días	lun 31/03/08	lun 07/04/08	
14	Aplicació web d'administració d'usuaris i proveïdor de serveis	10 días	lun 31/03/08	lun 14/04/08	
15	Aplicació de validació d'identitat	10 días	lun 14/04/08	lun 28/04/08	14;13;3
16	Integració	10 días	lun 28/04/08	lun 12/05/08	9;12
17	Entrega Parcial (Pac 4)	1 día?	jue 15/05/08	jue 15/05/08	16
18	Correccions	10 días	vie 16/05/08	jue 29/05/08	17
19	Elaboració Memòria Tècnica	10 días	vie 30/05/08	vie 13/06/08	18;4
20	Elaboració Presentació	13 días	vie 30/05/08	mar 17/06/08	18;4
21	Entrega Treball Fi de Carrera	1 día?	jue 19/06/08	jue 19/06/08	19;20

Figura 2

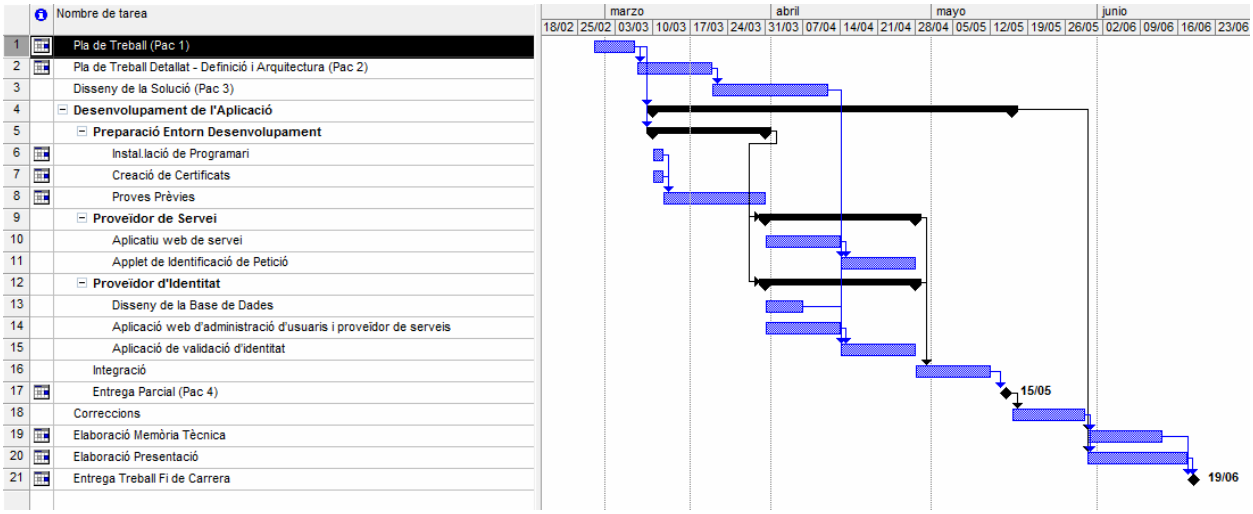


Figura 3

5.1.3 Producte Obtingut

D'acord amb el plantejament del treball de fi de carrera i com és detalla en els punts posteriors s'ha obtingut una solució que permet l'accés als recursos d'un proveïdor de servei utilitzant tant els certificats emesos per una autoritat certificadora específica per al desenvolupament d'aquest treball com utilitzant el DNI electrònic.

5.2 Fonaments i Estat de l'Art

Per al desenvolupament del producte s'ha utilitzat programari de lliure de distribució que compleix amb els requeriments del producte.

Les tecnologies utilitzades han estat en primer lloc la plataforma de programació J2EE (Java Platform, Enterprise Edition) que ens permet desenvolupar software amb arquitectura distribuïda de manera que puguem executar els mòduls necessaris en el servidor. El servidor J2EE utilitzat ha estat Tomcat.

Per una altra banda, per a l'enviament dels missatges entre el client i el proveïdor d'identitat s'ha utilitzat el protocol SOAP (Simple Object Access Protocol). Aquest protocol és un estàndard basat en el intercanvi de dades en format XML que conjuntament amb la utilització de certificats que ens asseguren la identitat de l'emissor i les signatures que ens asseguren la integritat del missatge compleixen amb els requisits plantejats per al desenvolupament d'aquest producte.

La utilització del DNI electrònic per a la autenticació del client, la utilització del protocol OCSP per a la validació del certificat de DNI y el seguiment de les especificacions del consorci World Wide Web per a les signatures digitals XML han estat utilitzades també en el desenvolupament de la solució.

En el cas de la base de dades, malgrat que en el desenvolupament del producte utilitza una base de dades Informix, el producte tindrà la possibilitat de fer servir els drivers adequats per que es pugui utilitzar qualsevol altra base de dades.

La utilització de JDK ens ha permès utilitzar totes les tecnologies descrites anteriorment per al desenvolupament del producte.

5.3 Especificació i Disseny

En aquest apartat és documenten els aspectes propis del disseny de la solució que seran descrits en detall en l'apartat posterior d'implementació.

5.3.1 Interfícies Gràfiques

- Plana principal del Proveïdor de Servei

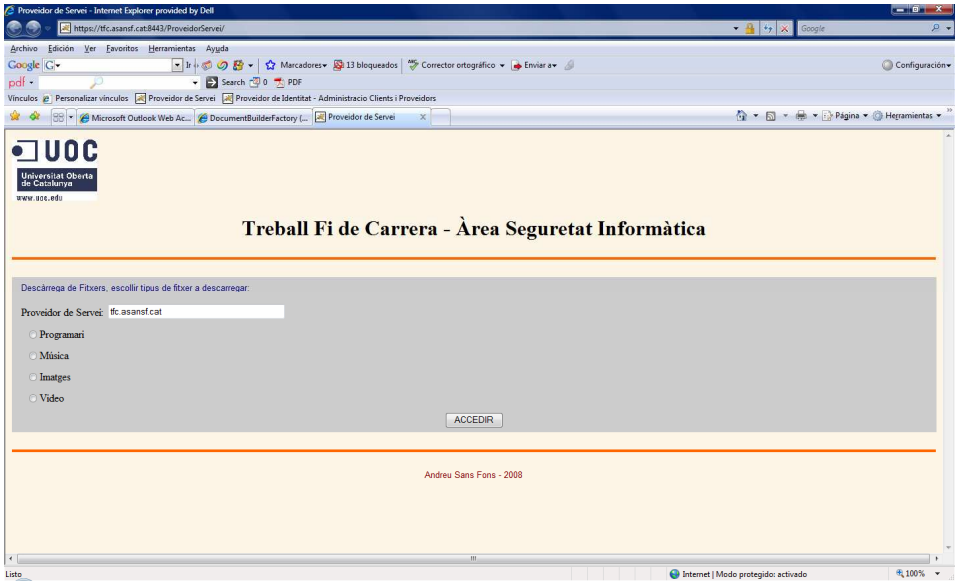


Figura 4

- Plana principal del Proveïdor de Identitat

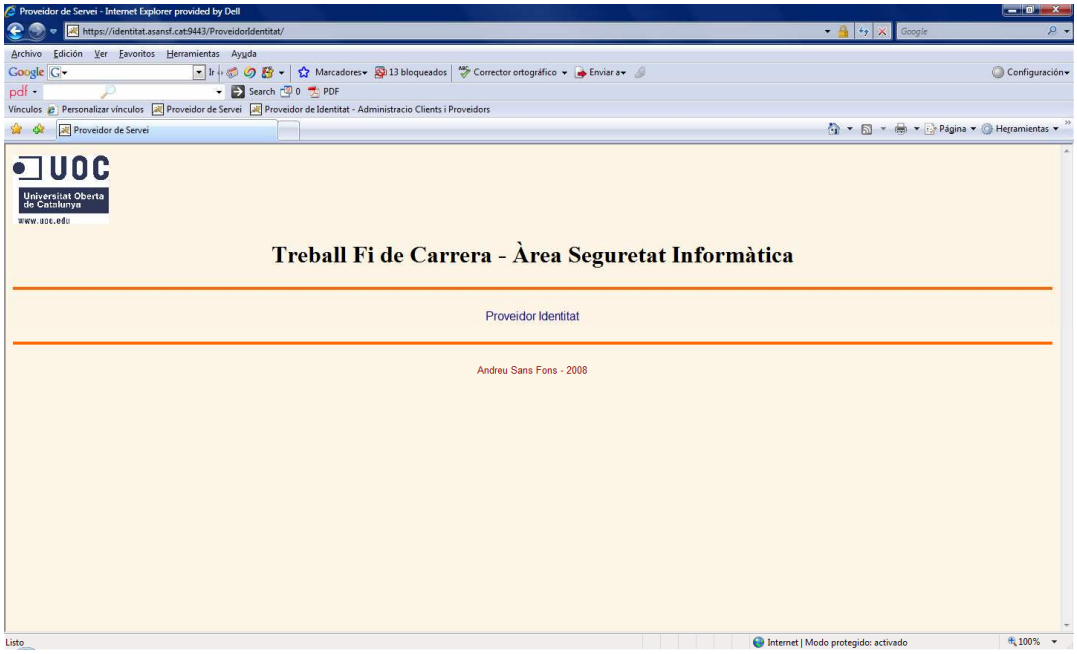


Figura 5

- Plana Administració d'Usuaris i Proveïdors

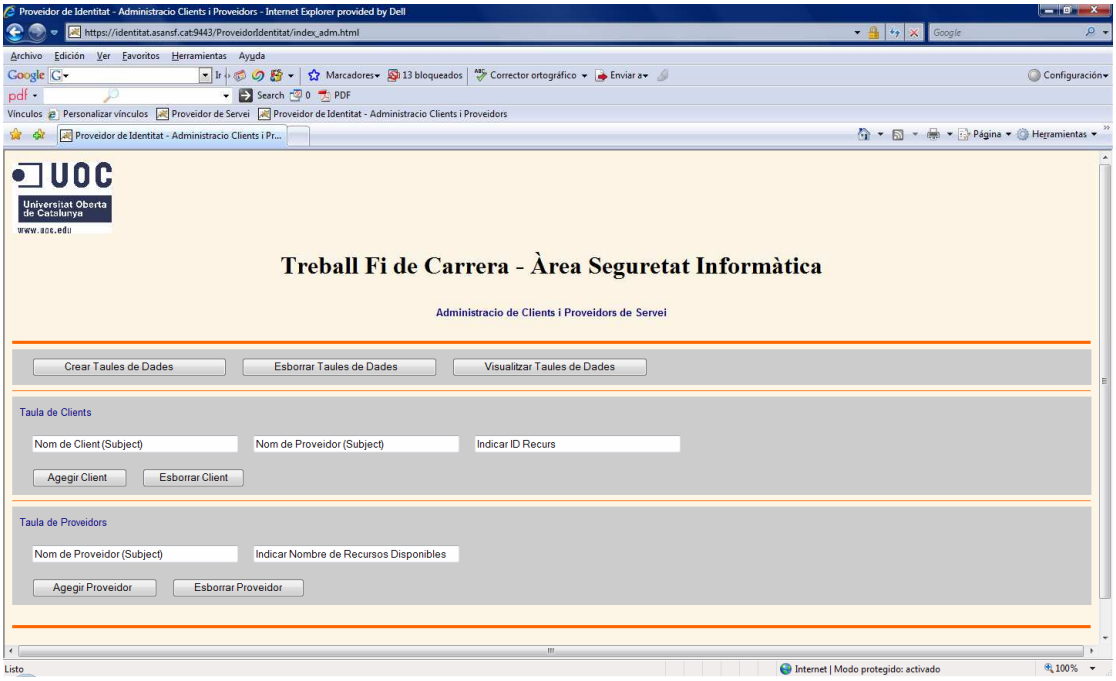


Figura 6

- Applet Petició de Client

Figura 7

- Plana d'accés al recurs del proveïdor de servei

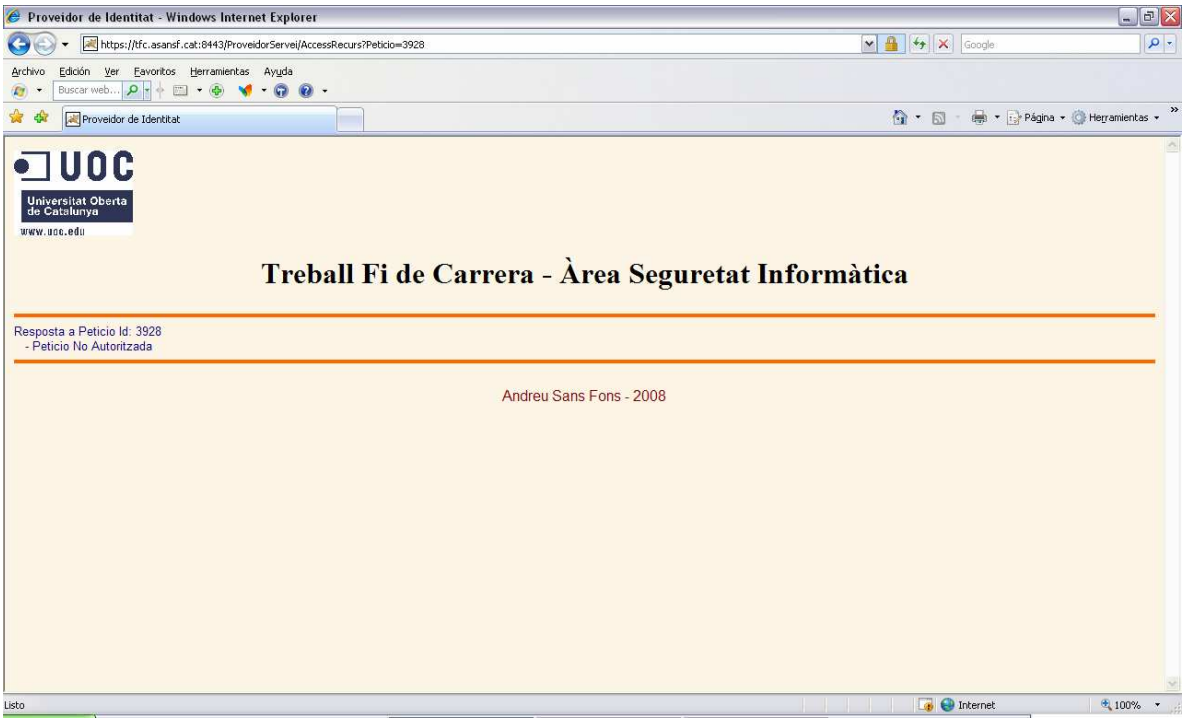


Figura 8

5.3.2 Diagrama de Casos d'Ús

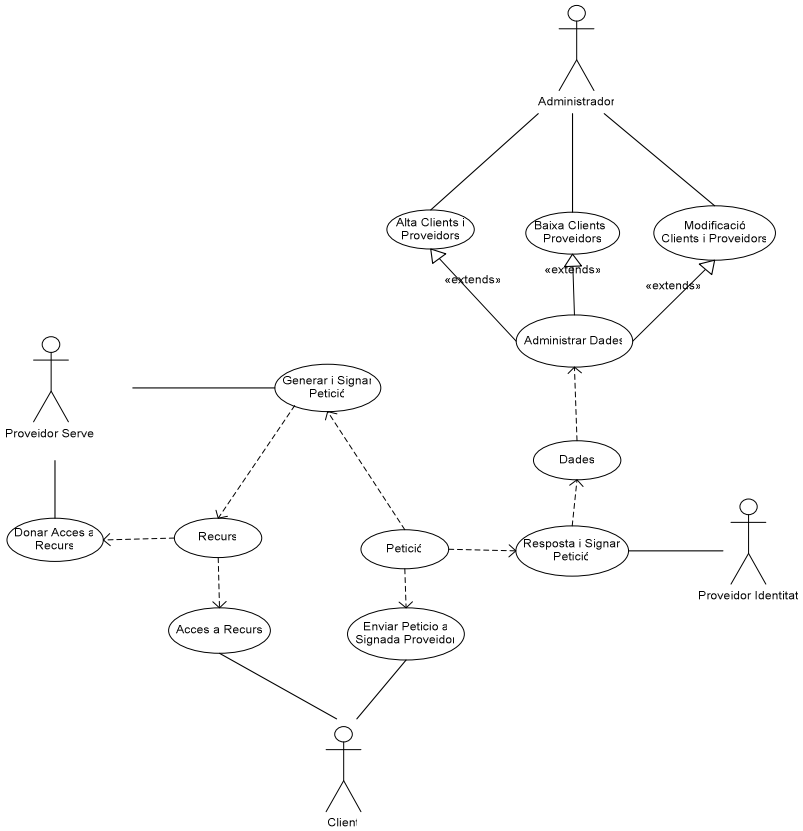


Figura 9

5.3.3 Base de dades

La base de dades conté dues taules: la taula de clients (usuaris) i la taula de proveïdors. Els camps de la primera taula corresponen al *subject* del client, el proveïdor i el identificador del recurs del proveïdor de servei al que té accés. La taula de proveïdors disposa de dos camps, el *subject* del proveïdor i el nombre de recursos disponibles.

5.3.4 Diagrama de Classes

- Proveïdor de Servei

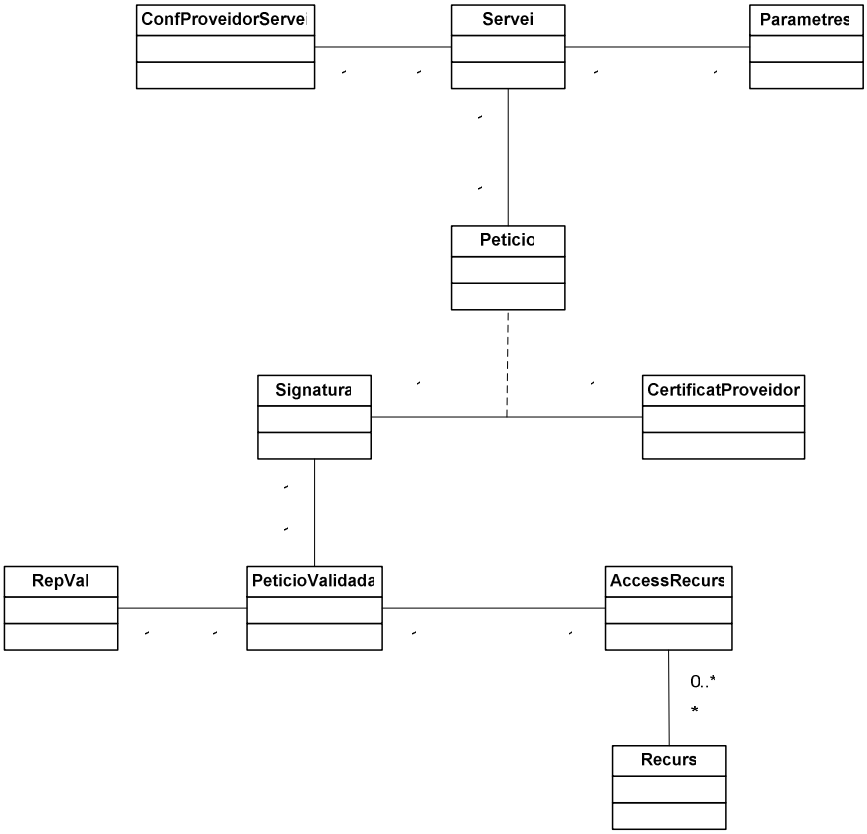


Figura 10

- Applet de Petició de Client

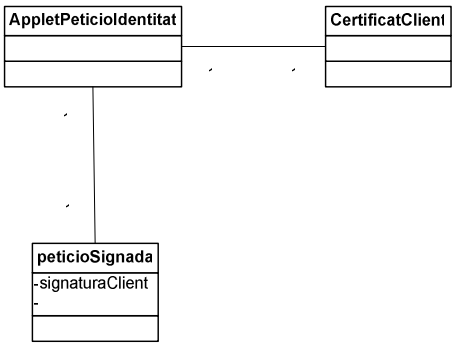


Figura 11

- Proveïdor de Identitat

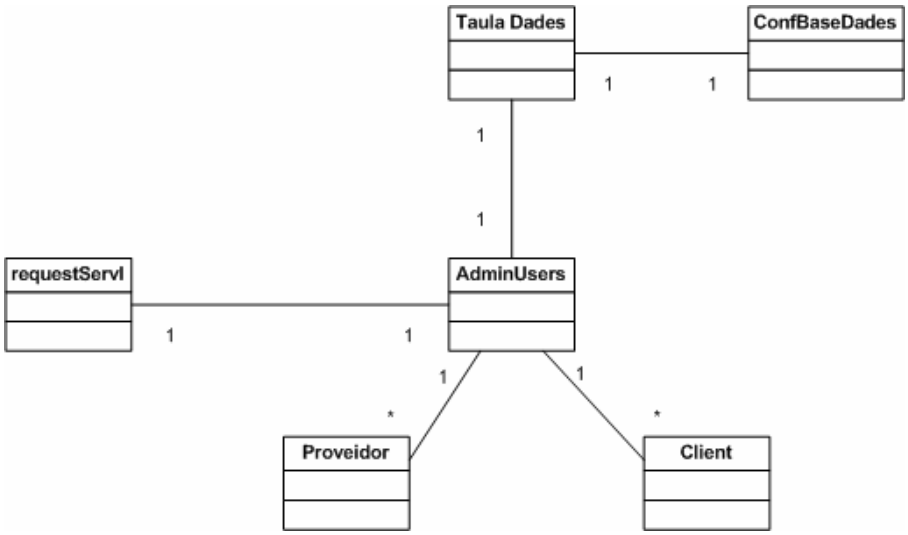


Figura 12

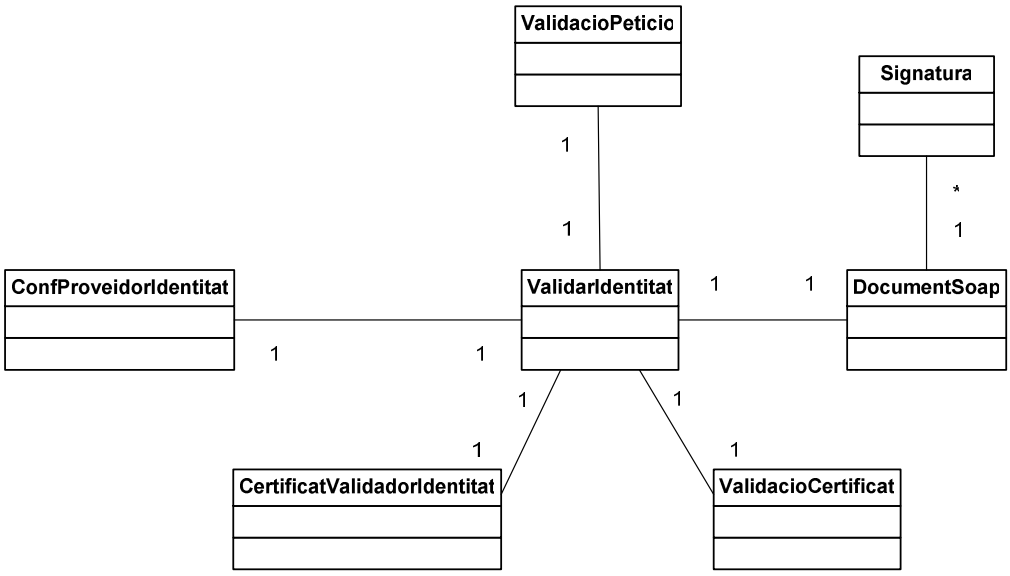


Figura 13

5.3.5 Format Documents XML i SOAP

- Petició Signada pel Proveïdor de Servei

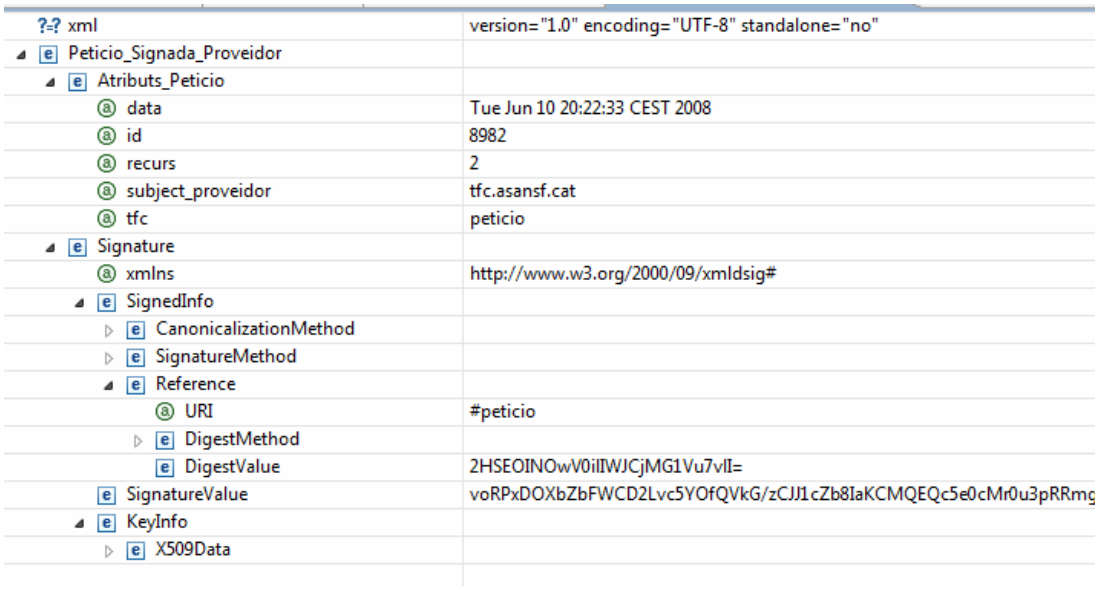


Figura 14

- Petició Signada pel Client

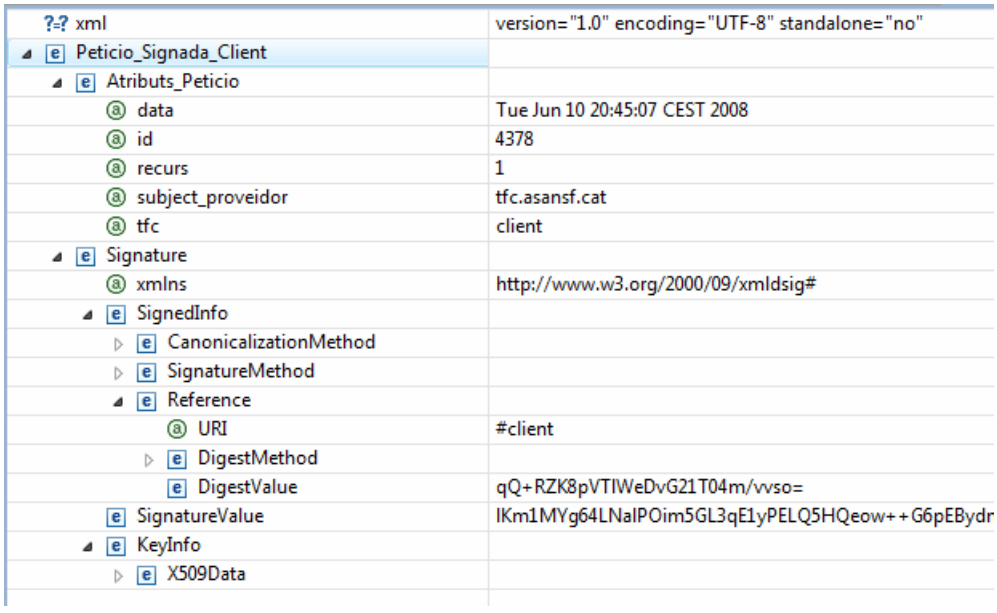


Figura 15

- Document SOAP enviat pel Applet

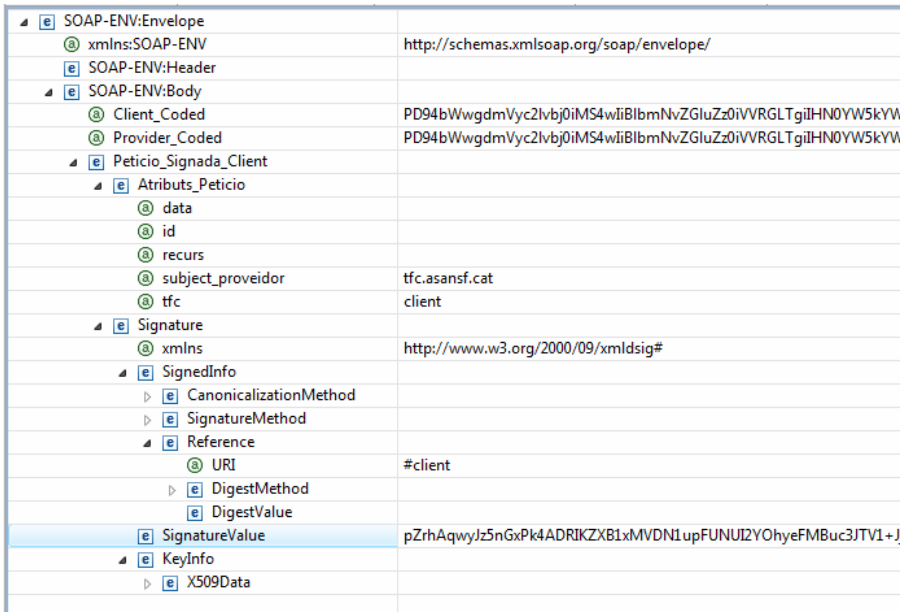


Figura 16

- Document Contrafirma

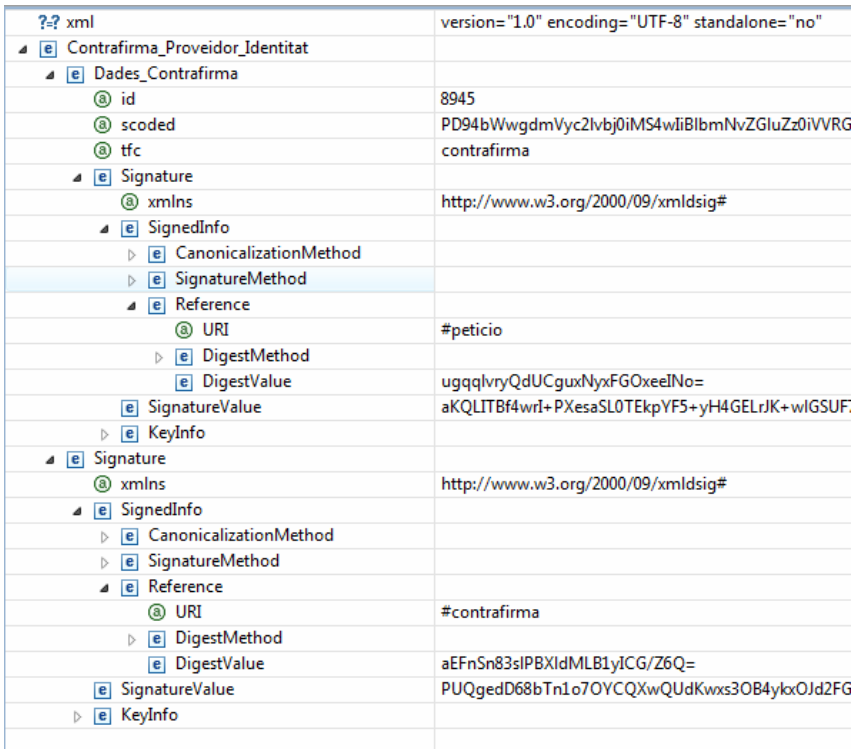


Figura 17

- Document Resposta Proveïdor Identitat

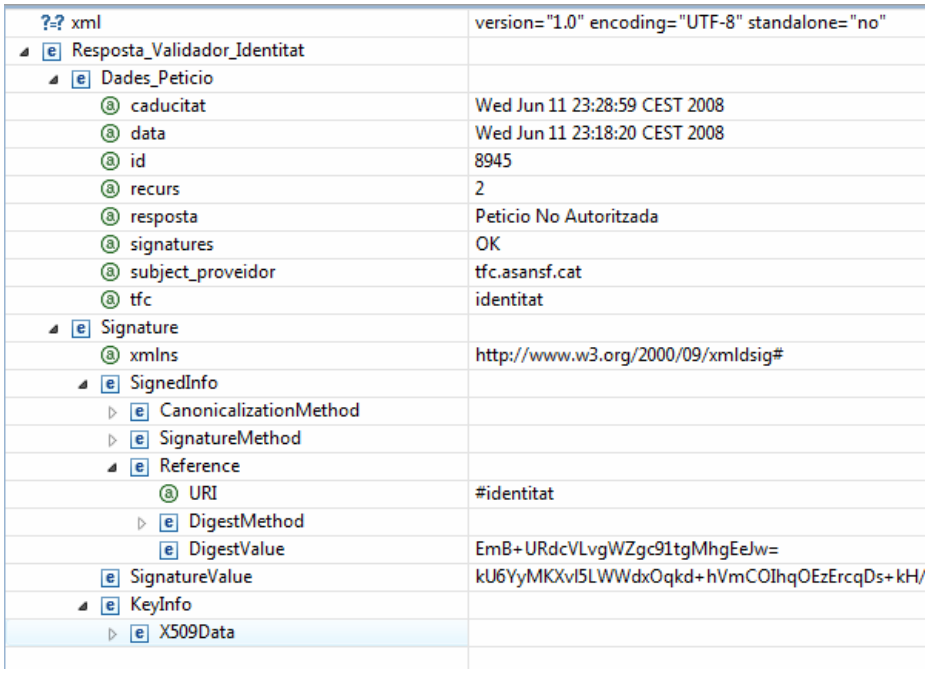


Figura 18

- Document SOAP resposta Proveïdor Identitat

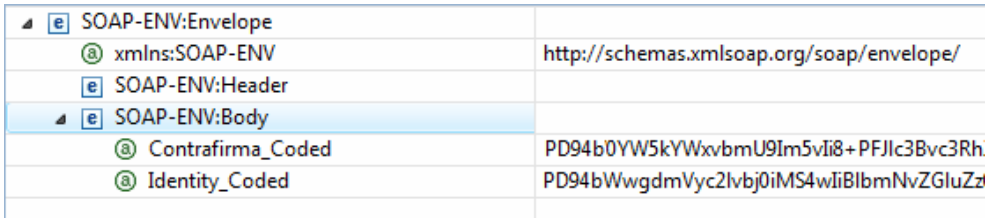


Figura 19

5.4 Implementació

A continuació és detalla la implementació del producte a partir del fluxe des de que el client sol·licita l'accés al recurs fins que rep la resposta de la validació i l'accés al recurs o no, en funció de la mateixa. També és descriuen les decisions preses en cada punt de la implementació i com han afectat al pla de treball presentat inicialment.

5.4.1 Proveïdor de Servei – Accés al Servei

La classe principal del proveïdor de Servei es la classe *servei* que té per funcionalitat bàsica la de generar el document XML de petició d'accés a un recurs. Al marge de generar la plana web d'accés al recurs, aquesta classe crea el document XML, llegeix el certificat de proveïdor (c:\tfc_asansf\certificats\prSRV_s.pfx) i signa el document. La classe *Signatura* simbolitza una signatura i disposa dels mètodes tant per signar un document com per fer la validació. La classe *CertificatProveidor* simbolitza el certificat del proveïdor de servei.

Addicionalment abans de cridar el applet de petició és verifica la signatura deixant en un fitxer de registre el resultat de la validació (log_signatura_proveidor.txt):

```
Clau: Sun RSA public key, 1024 bits
  modulus:
142970412922154848503801337885802807063138282143887288873258374878271436904303328935065591242523111305024213874392670643141743691079223824249666054284773852865545183855267040108798539438559799150479594691861063878588562034337007395161732503071785701240452849850092190551920938351021395781080925718112496277871
  public exponent: 65537
Validacio: true
signature validation status: true
Signature passed core validation
```

Figura 20

5.4.2 Applet Petició Identitat

Cridat pel proveïdor de servei, el applet de petició te com a classe principal la classe *AppletPeticioIdentitat*. Aquesta classe al marge de presentar la finestra gràfica on el client te la opció d'escollir el certificat de DNI electrònic o el certificat específic creat per aquest producte, te com a funció generar el missatge SOAP que s'enviarà al proveïdor d'identitat per fer les validacions corresponents d'acord amb els requeriments.

La classe *PeticioSignada* representa la petició rebuda pel proveïdor de servei i que és signarà amb el certificat de client escollit. Durant el desenvolupament del producte és va optar per generar totes les signatures del tipus “detached” i codificar en base64 la petició per tal que les modificacions que és realitzen al incorporar un document XML en el cos d’un missatge SOAP fossin un impediment per a la validació correcta de la signatura. La classe CertificatClient representa el certificat de client generat específicament per aquest producte i emès per una Autoritat Certificadora creada per aquest fi (veure apartat de certificats utilitzats). Pel que fa a la lectura del certificat de DNIe, s’ha utilitzat un lector de smartcard del fabricant Omnikey (Model cardman 2020) i s’ha implementat mitjançant la lectura del keystore de windows, fent un recorregut i cercant els certificats emesos per la organització “DIRECCION GENERAL DE POLICIA”.

5.4.3 Proveïdor de Identitat

El proveïdor d’identitat té com a classe principal la classe *ValidarIdentitat* que rep el document SOAP del Applet (veure format en l’apartat d’especificació i disseny). Un cop descodificats els missatges signats pel client i pel proveïdor, es validen les dues signatures, es valida el certificat de client, es comprova que tingui autorització per accedir al recurs, es fa una contrafirma de la signatura original del proveïdor de servei, es genera la caducitat de la petició, es signa i tot plegat es retorna com a resposta del missatge SOAP del applet.

En el cas del DNIe la validació del certificat s’ha realitzat utilitzant un client OCSP basat en *Bouncycastle* que verifica accedint a la url http://ocsp.dnie.es que el certificat és vàlid i està emès per la autoritat certificadora corresponent. Pel que fa al certificat específic creat per aquest producte només és verifica la seva validesa, no s’ha implementat cap consulta a llista de revocació local.

La classe signatura simbolitza una signatura i és utilitzada tant per signar com per validar una signatura. Com s’ha indicat anteriorment les signatures generades son del tipus “detached” i es codifiquen en base64 per tal de garantir de manera addicional a la signatura, la integritat dels documents.

Com en el cas del proveïdor de servei és generen diferents fitxers de registre i documents per tal de validar el funcionament del producte.

5.4.4 Proveïdor de Servei – Accés al Recurs

Un cop rebuda la resposta per l'applet de petició, aquest envia amb dos missatges SOAP diferenciats, el document amb la contrafirma y el document amb la resposta del proveïdor d'identitat signada convenientment.

Un cop rebuts aquests missatges, el client és redirigit a la *url* de l'accés al recurs que en funció del resultat de la validació del proveïdor d'Identitat, la validesa de les signatures (contrafirma i resposta del proveïdor d'identitat), la validesa de la signatura original de la petició, la comprovació que ha estat realitzada pel proveïdor de servei i la petició correspon a la sessió en curs.

Si la validació de tots aquests aspectes és correcta, es dona accés a la visualització de les dades del recurs, en cas contrari, es mostra el resultat de la validació.

Exemple Petició no autoritzada:

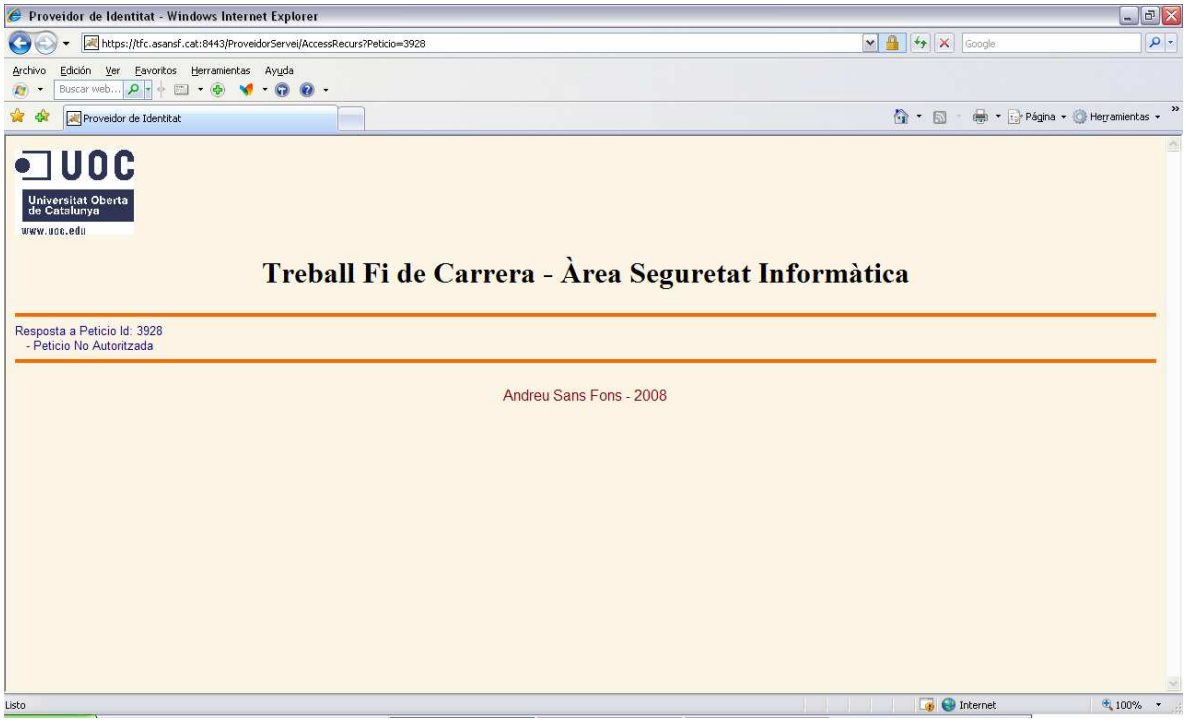


Figura 21

Exemple Petició autoritzada:

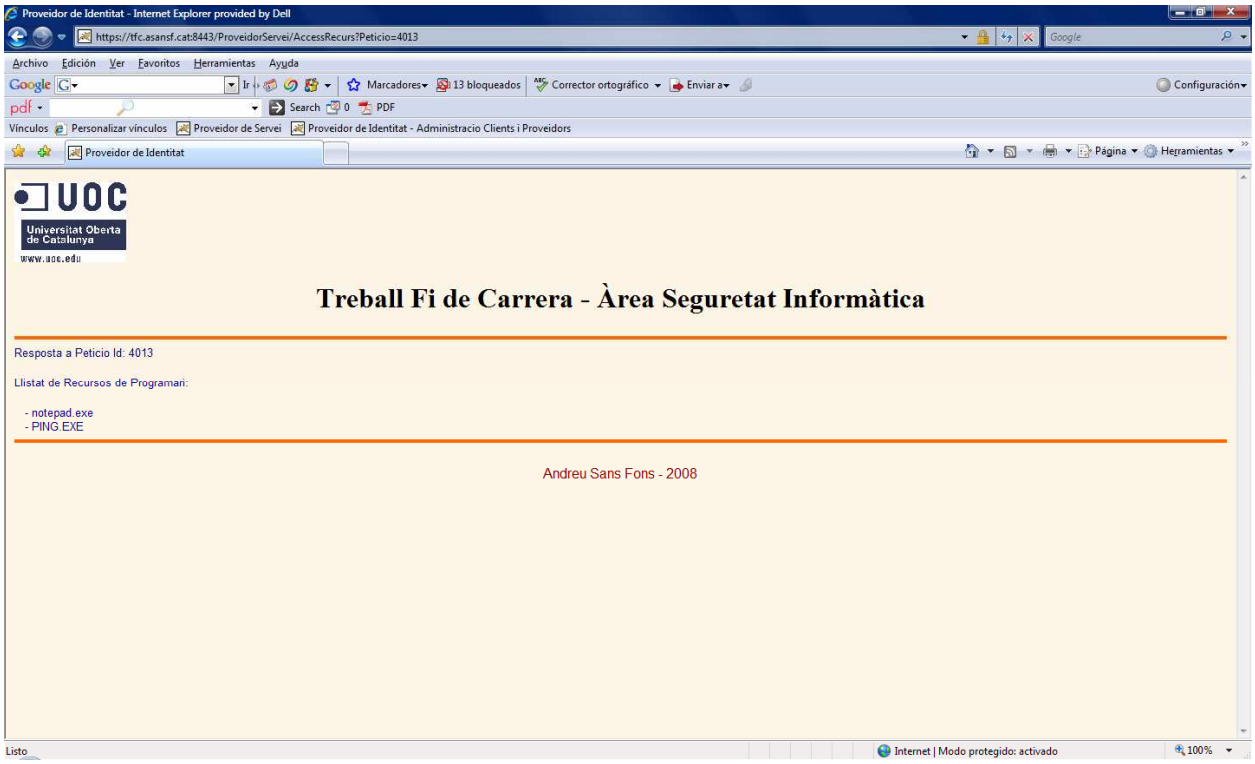


Figura 22

5.4.5 Signatura i Validació de Signatura

De manera resumida, el procés de signatura i validació de la signatura ha estat el que es descriu a continuació:

Signatura:

- Tal com s'ha indicat anteriorment les signatures XML utilitzades son del tipus "detached". Això vol dir que l'element que conté la signatura està separada de les dades signades.
- El primer pas per crear una signatura és la creació d'una instància XMLSignatureFactory.
- Posteriorment s'escull el mètode de signatura i la referència a l'element que es vol signar.
- S'indica també el mètode de canocalització.

- A continuació és crea l'objecte SignedInfo amb els paràmetres anteriors.
- El següent pas és crear un DOMSignContext que te com a paràmetre la clau privada que s'utilitzarà per fer la signatura i la ubicació de l'element corresponent a la signatura dintre del document.
- És crea també l'element KeyInfo que conte el certificat utilitzat per signar i que ens permetrà fer les validacions posteriors, obtenint el certificat i la clau pública.
- Finalment és realitza la signatura.

Validació:

- S'agafa l'element que conte la signatura.
- És crea un objecte DOMValidateContext (Context de validació)
- S'obté la clau pública.
- S'obté el resultat de la validació.
- Prèviament s'indica que guardi els elements referenciats per poder obtenir la causa d'una validació incorrecte. Funcionalment no és necessària per validar una signatura, en aquest cas s'ha implementat per verificar el procés de signatura i validació.

5.4.6 Fitxers de configuració

En el proveïdor de identitat i de servei estan disponibles els fitxers *tfc_conf.txt* en els que s'hi poden indicar diferents paràmetres de l'aplicació com poden ser si és fa log o no, i en quin directori és deixen els fitxers per tal de validar el funcionament del producte.

5.4.7 Fitxers de descripció de directoris

El els directoris que s'ha considerat oportú s'ha deixat un fitxer de text, anomenat *TFCinfo.txt* que descriu el contingut del directori.

5.4.8 Fitxers de Registre (log)

En el directori c:\tfc_asansf\log s'han ubicat els diferents fitxers de registre que permeten registrar les diferents validacions de les signatures i events remarcables. També en el mateix directori és deixen els diferents documents XML i SOAP utilitzats. També és deixen diferents missatges per consola per validar els diferents passos de la solució.

5.4.9 Documentació Javadoc

En el subdirectori c:\tfc_asansf\javadoc s'ha generat la documentació de les classes utilitzades en aquest producte.

5.4.10 Altres aspectes i millores del producte.

Malgrat que el producte compleix amb els requeriments i funcionalitats plantejades són millorables o s'han de considerar els següents aspectes:

- En aquesta versió del producte el proveïdor de servei només mostra el llistat de fitxers de cada un dels recursos. Les funcionalitats del producte permeten extrapolar la solució a qualsevol tipus d'accés a un recurs malgrat no s'hagi implementat en aquest cas un servei complert.
- La utilització dels certificats creats específicament per aquest producte han estat creats per al desenvolupament de la solució, no tenen per que ser una opció en una versió comercial. La possibilitat d'utilitzar un certificat públic com el DNIe compleix amb els requeriments plantejats.
- En aquest producte s'ha implementat una solució simple de la base de dades y la administració de la mateixa. És millorable tant l'aplicació d'administració com el disseny de la base de dades.
- S'ha modificat el fitxer hosts (c:\windows\systems32\drivers\etc\hosts) per tal de resoldre tant *tfc.asansf.cat* com *identitat.asansf.cat* i poder verificar la solució simulant un entorn real.

5.5 Instal·lació

Per a la instal·lació del producte cal descomprimir el fitxer entregat i seguir les consideracions descrites a continuació.

5.5.1 Directoris i Fitxers

La totalitat dels fitxers utilitzats s'entrega en document comprimit que s'ha de descomprimir en el directori c:\tfc_asansf on hi ha referenciats en el producte els certificats i d'altres documents.

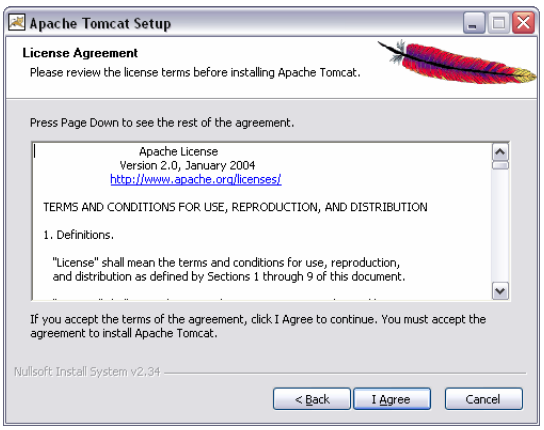
En aquest directori hi tenim els subdirectoris següents:

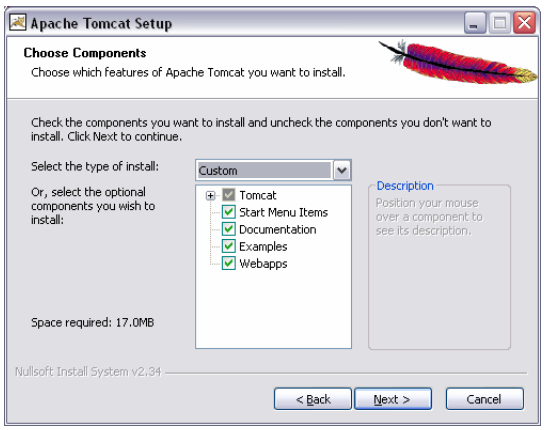
- AppletPeticioIdentitat -> Classes del Applet de Petició d'identitat
- Certificats -> Certificats utilitzats
- Htdocs -> Documents HTML
- Programari -> Tomcat i fitxers de configuració
- ProveidorIdentitat -> Classes del Proveïdor Identitat
- ProveidorServei -> Classes del Proveïdor de Servei
- Log -> Registre i fitxers de proves
- Recursos -> Directori on estan ubicats els recursos del proveïdor de servei
- Javadoc -> Documentació de les classes de java generades.

5.5.2 Tomcat

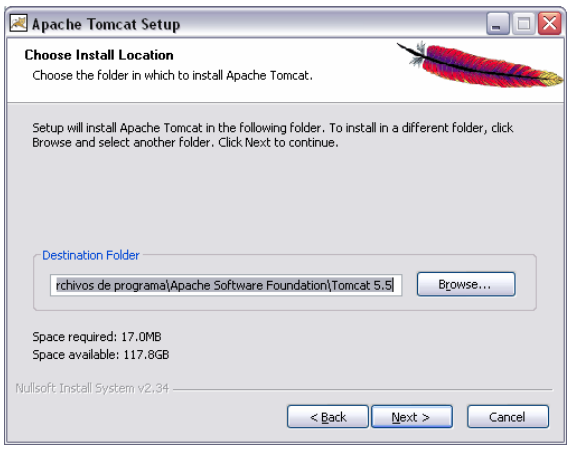
Un cop descomprimits els fitxers cal instal·lar Tomcat seguint el següent procediment:

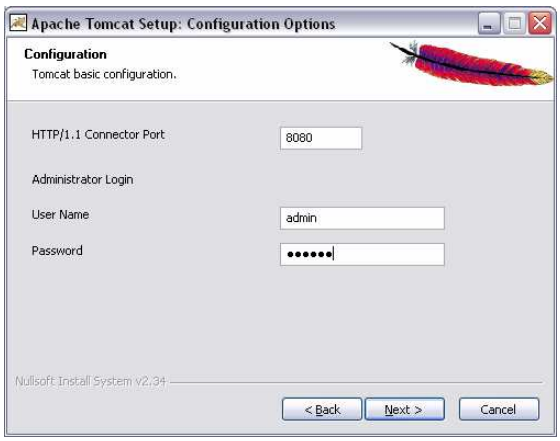
- Executar *apache-tomcat-5.5.26.exe* del subdirectori *Programari* i seguir els passos descrits a continuació.



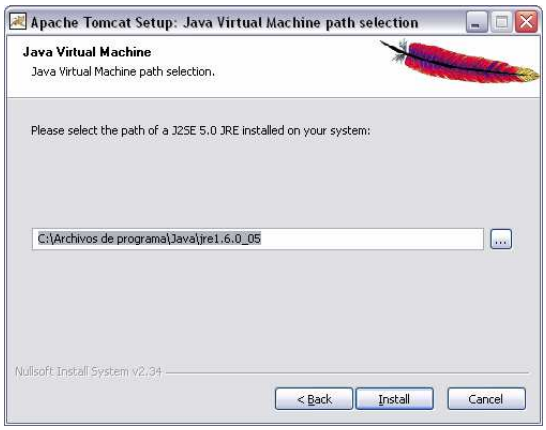


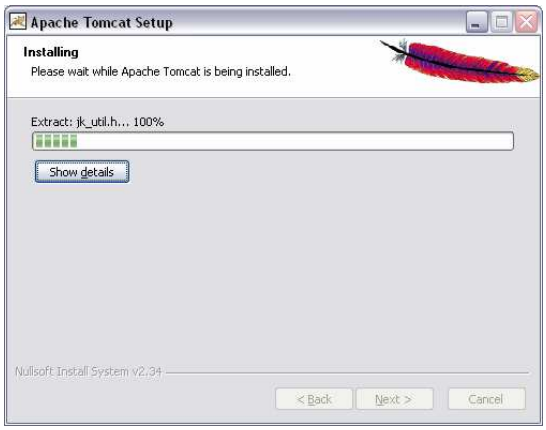
- Indicar Directori on instal.lar Tomcat i Credencials d'accés.





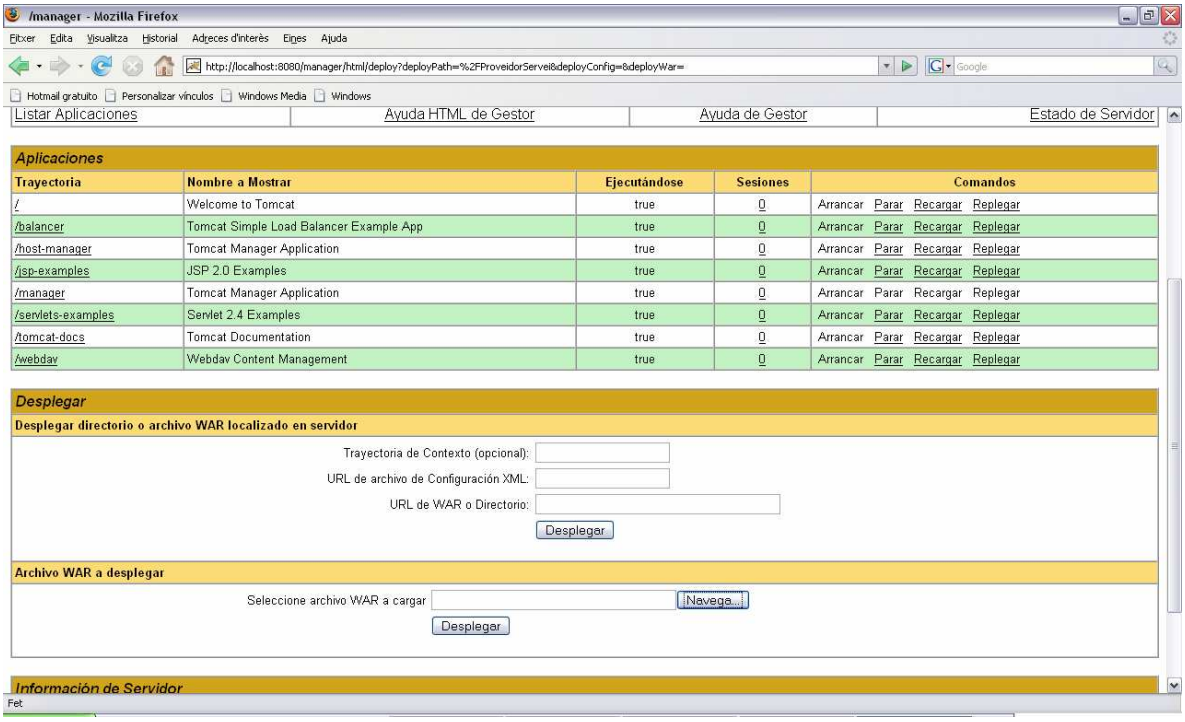
- Indicar Directori on està ubicat Java





- Abans d'iniciar el servei, copiar en el directori *C:\Program Files\Apache Software Foundation\Tomcat 5.5\conf* els fitxers *server.xml* i *tomcat-users.xml* Subministrats en el subdirectori *Programari*.

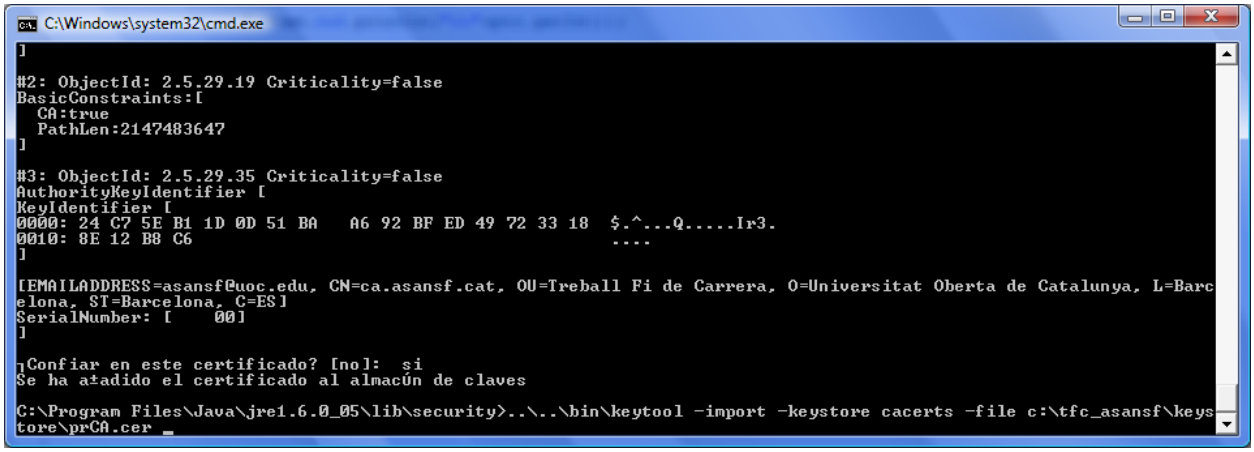
- Un cop iniciat el servei cal accedir a la administració de Tomcat (http://tfc.asansf.cat:8080) i desplegar l'aplicació tal com és descriu a continuació.



- Copiant els subdirectoris *ProveidorIdentitat* i *ProveidorServei* a el directori *C:\Archivos de programa\Apache Software Foundation\Tomcat 5.5\webapps*, les aplicacions ja seran accessibles.

5.5.3 Instal.lació Certificats Keystore de Java

Per tal d'instal·lar en el keystore de java el certificat de CA utilitzat s'ha utilitzat la comanda *keytool* de la següent manera:



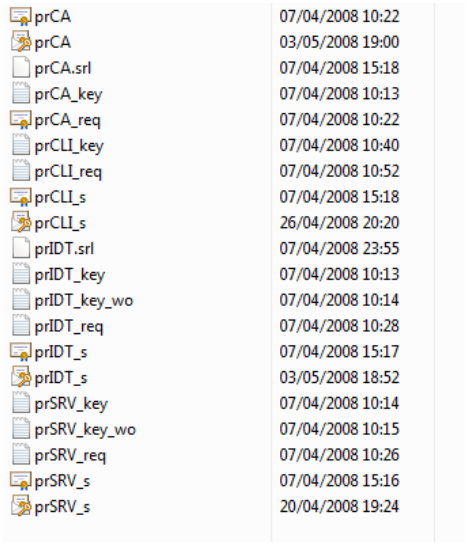
5.5.4 Base Dades

El driver JDBC utilitzat en el desenvolupament del producte es el ODBC de manera que és puguin utilitzar bases de dades d'altres fabricants diferents l'utilitza't. Les dades del connector amb la base de dades també és podran modificar, accedint e indicant els paràmetres adequats al fitxer de text subministrat en el directori *c:\tfc_asansf\ProveidorIdentitat* anomenat *odbc_conf.txt* i que te la sintaxi
d'exemple següent:

 # Connector Driver JDBC
url:Usuaris
userID:informix
password:1234

5.5.5 Certificats Utilitzats

En el directori c:\tfc_asansf\Certificats podem trobar els certificats utilitzats:



Per a cada certificat tenim els següents fitxers:

- .cer -> Cerfificat
- .pfx -> Cerfificat i clau privada en format PKCS12
- .srl -> Nº de Serie del Certificat
- _key.txt -> Clau privada
- _req.txt -> Petició de Certificat

La descripció de cada un dels certificats es la següent:

- prCA -> Certificat de CA
- prCLI_s -> Certificat de Client (client.asansf.cat)
- prSRV_s -> Certificat de Proveïdor de Servei (tfc.asansf.cat)
- prIDT_z -> Certificat del Proveïdor de Identitat (identitat.asansf.cat)

En el mateix directori està ubicat el certificat de la CA emissora dels certificats de DNI electrònic.

5.6 Funcionament del Producte

En aquesta apartat descriu el funcionament del producte per tal de mostrar que les funcionalitats del producte assolides d'acord amb el plantejament inicial. A nivell global, en el següent diagrama d'estats podem veure el funcionament de la solució:

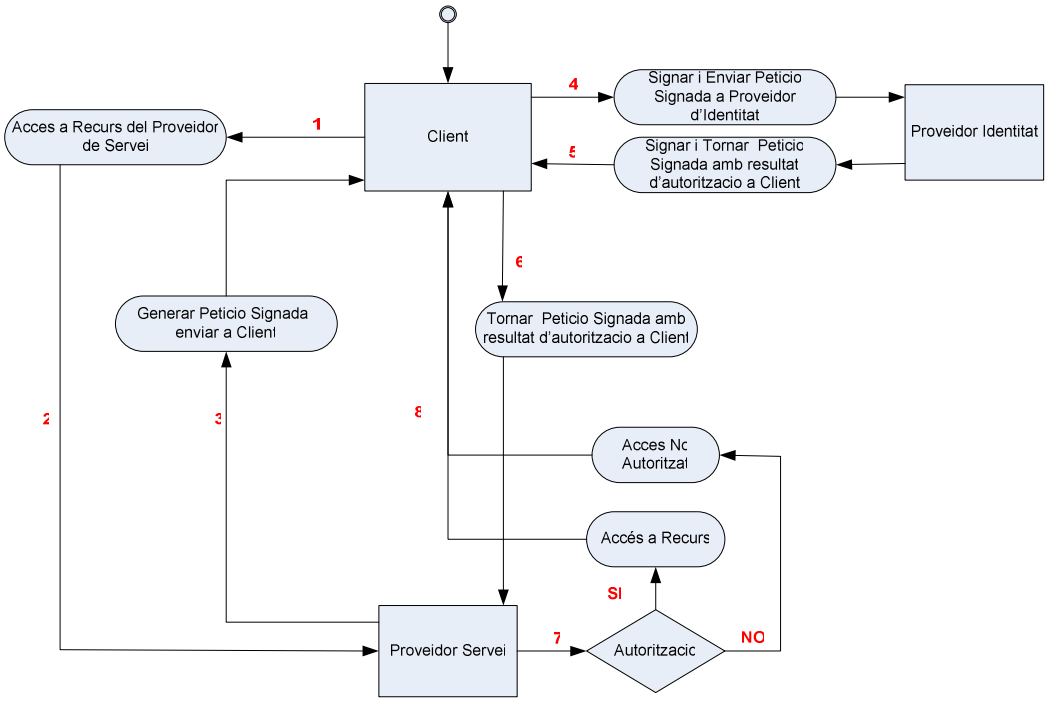


Figura 23

5.6.1 Accés al Proveïdor de Servei

Per accedir a l'aplicació del proveïdor de servei , cal accedir a la url següent:
https://tfc.asansf.cat:8443/ProveidorServei/

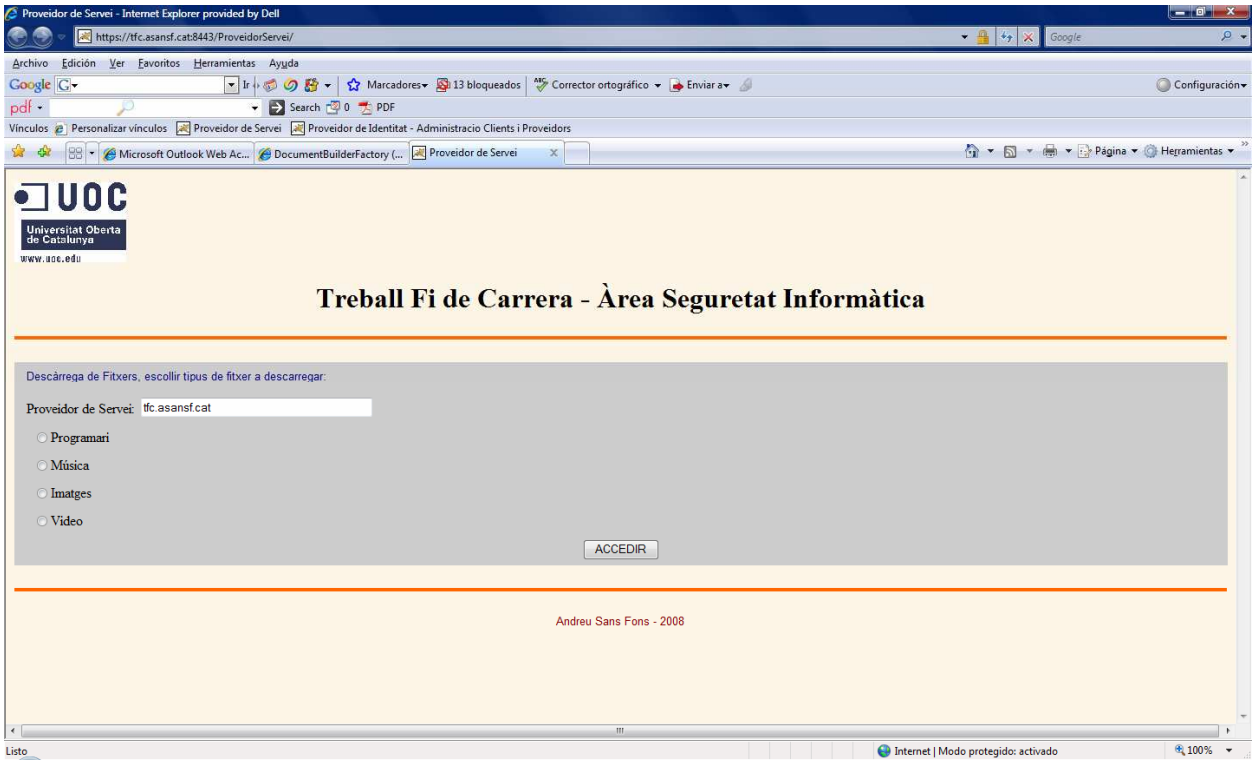


Figura 24

Aquest proveïdor de servei disposa de quatre recursos disponibles. Per tal d'accedir al recurs desitjat cal seleccionar el recurs i pressionar el botó "accedir". Un cop pressionat aquest botó és genera la petició d'accés al recurs signada amb el certificat del proveïdor de servei destinat a aquest fi. Previ a la execució del applet de petició de client, de manera addicional, és valida la signatura.

(Veure document XML signat pel proveïdor en l'apartat de especificació i disseny)

5.6.2 Applet de Petició de Client

El proveïdor de servei crida a l'applet de petició que s'executa en el client i que ens dona la opció de signar la petició de dues maneres, utilitzant els certificats creats específicament per al desenvolupament d'aquest producte o utilitzant el certificat de DNI electrònic.

El applet de petició ens mostra l'identificador de la petició, el proveïdor de servei, el recurs al que volem accedir, la data i les opcions de llegir DNI electrònic, llegir fitxer PKCS12 amb el certificat específic per aquest producte i sortir de l'applet.

Figura 25

En la part final de la finestra de l'applet disposem d'un camp de text que ens mostra els missatges dels passos a seguir. La opció d'enviar la petició al proveïdor d'identitat no s'activa fins que s'ha llegit el certificat de DNIe o s'ha llegit del fitxer.

Si escollim la opció de llegir de fitxer ens apareixerà un quadre de diàleg on escollirem el fitxer PKCS12 on està ubicat el certificat i posteriorment haurem d'introduir la contrasenya de protecció del certificat.

Figura 26

Posteriorment tindrem habilitat el boto d'enviar la petició al proveïdor d'identitat.

Figura 27

Si escollim la opció de llegir el DNI Electrònic, cal introduir el DNI en el lector i pressionar el botó "Llegir DNIe". Després d'uns segons ens demanarà la contrasenya del certificat del DNI per duplicat i un cop llegit ens donarà la opció d'enviar la petició al proveïdor d'identitat.

Figura 28

Un cop pressionat el botó d'enviar ens demanarà la conformitat per utilitzar el certificat del DNI per signar un document:

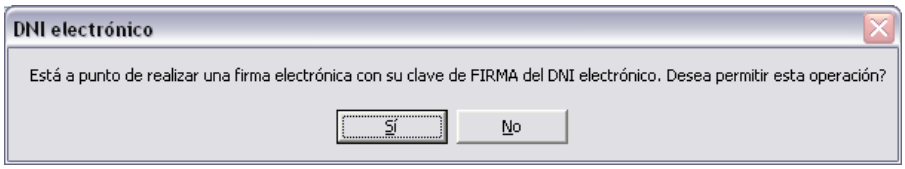


Figura 29

Un cop enviada la petició, tant en el cas del DNI com en el cas de fitxer ens redirigeix a una plana web amb el resultat de la validació o directament a la plana del recurs en cas que el resultat hagi estat positiu.

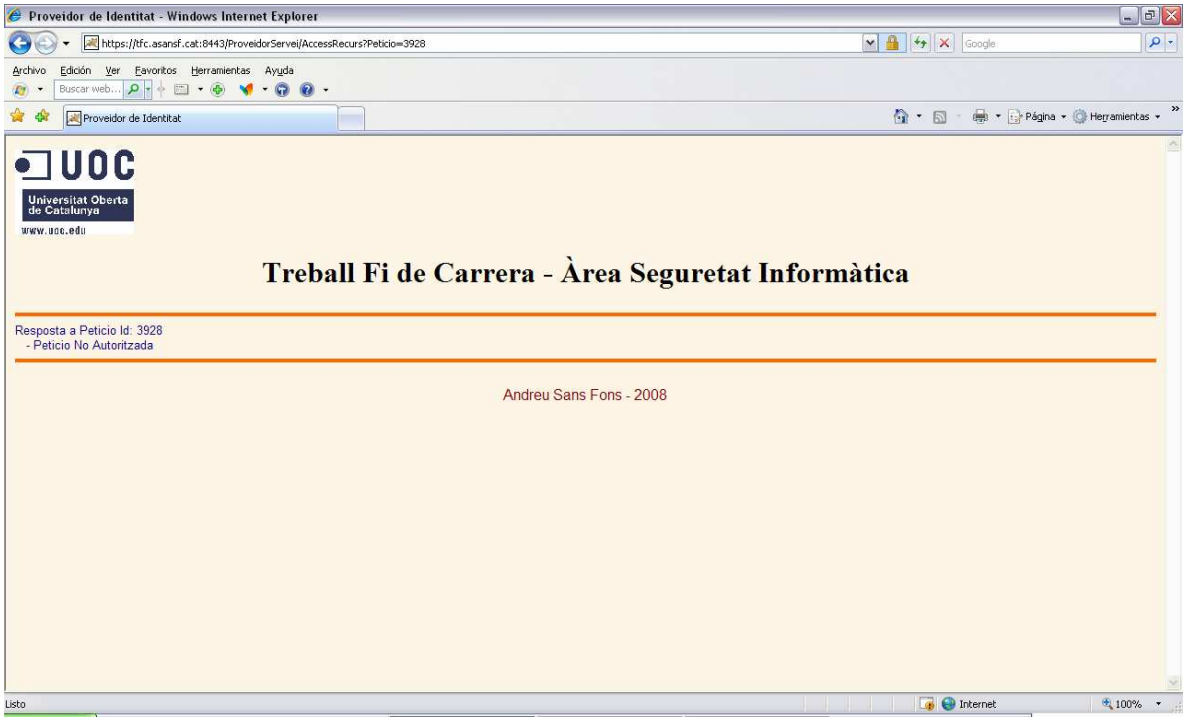


Figura 30

5.6.3 Proveïdor d'Identitat

Malgrat no ser directament visible per l'usuari, el proveïdor d'identitat rep el missatge SOAP *(veure apartat de especificació i disseny)* del applet de petició de client. Aquest missatge conté el document amb la petició signada pel proveïdor de servei, signat pel client.

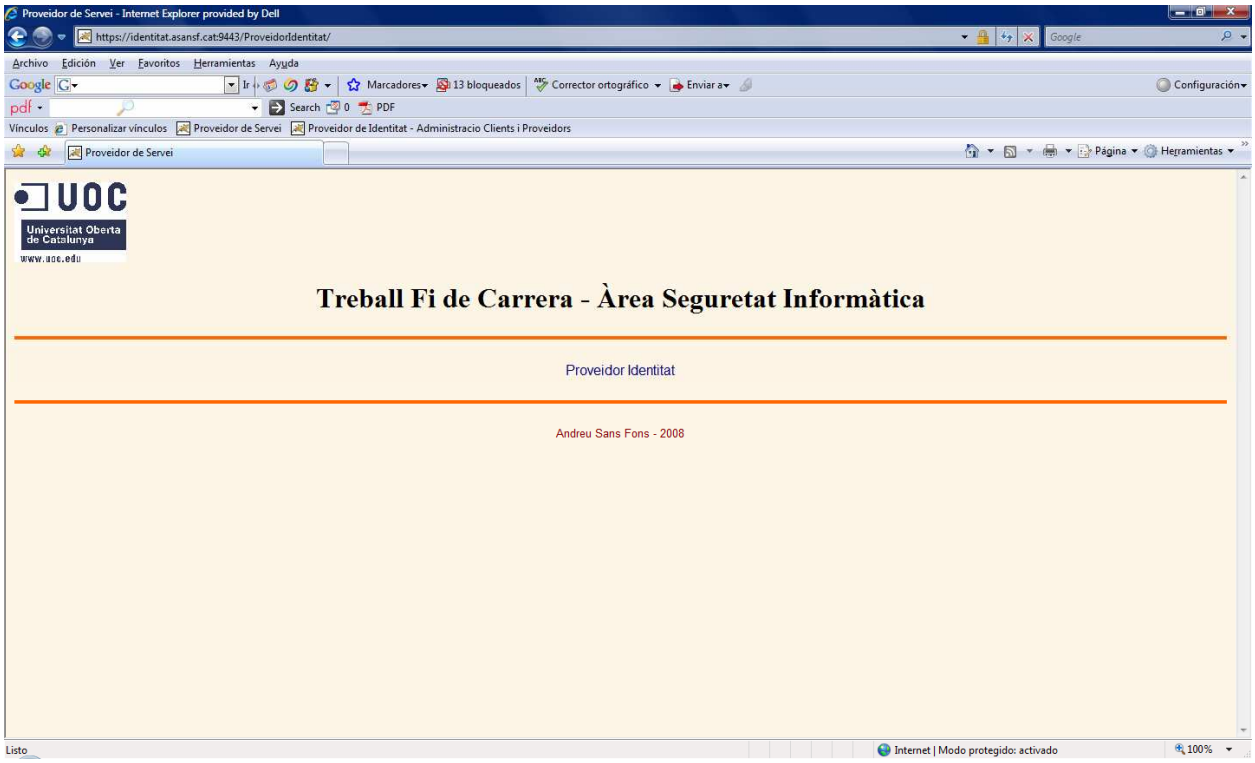


Figura 31

Un cop rebut el missatge, realitza les comprovacions de validesa de les signatures, validesa del certificat utilitzat en la signatura i consulta a la base de dades dels permisos. Amb el resultat de la validació és genera un missatge SOAP de resposta que conte les dades de la validació, una contrafirma de la signatura del proveïdor de servei i la signatura de les dades generades. *(Veure detall en l'apartat de implementació)*

5.6.4 Administració de Clients i Proveïdors

Per accedir a l'aplicació d'administració d'usuaris i proveïdors de serveis, cal accedir a la url https://identitat.asansf.cat:9443/ProveidorIdentitat/index_adm.html. L'accés a aquesta aplicació és autenticat mitjançat el certificat de client específic per aquest producte:

Figura 32

Un cop autenticats disposem d'una plana web senzilla que ens permet en primer lloc crear les taules de dades, esborrar-les o veure el seu contingut. La base de dades consta de dues taules, la de client y la de proveïdors. En la primera taula guardem el *subject* del client, el *subject* del proveïdor de servei i el recurs al que tenim permís per accedir. En la taula de proveïdors guardem el proveïdor i el nombre de recursos disponibles.

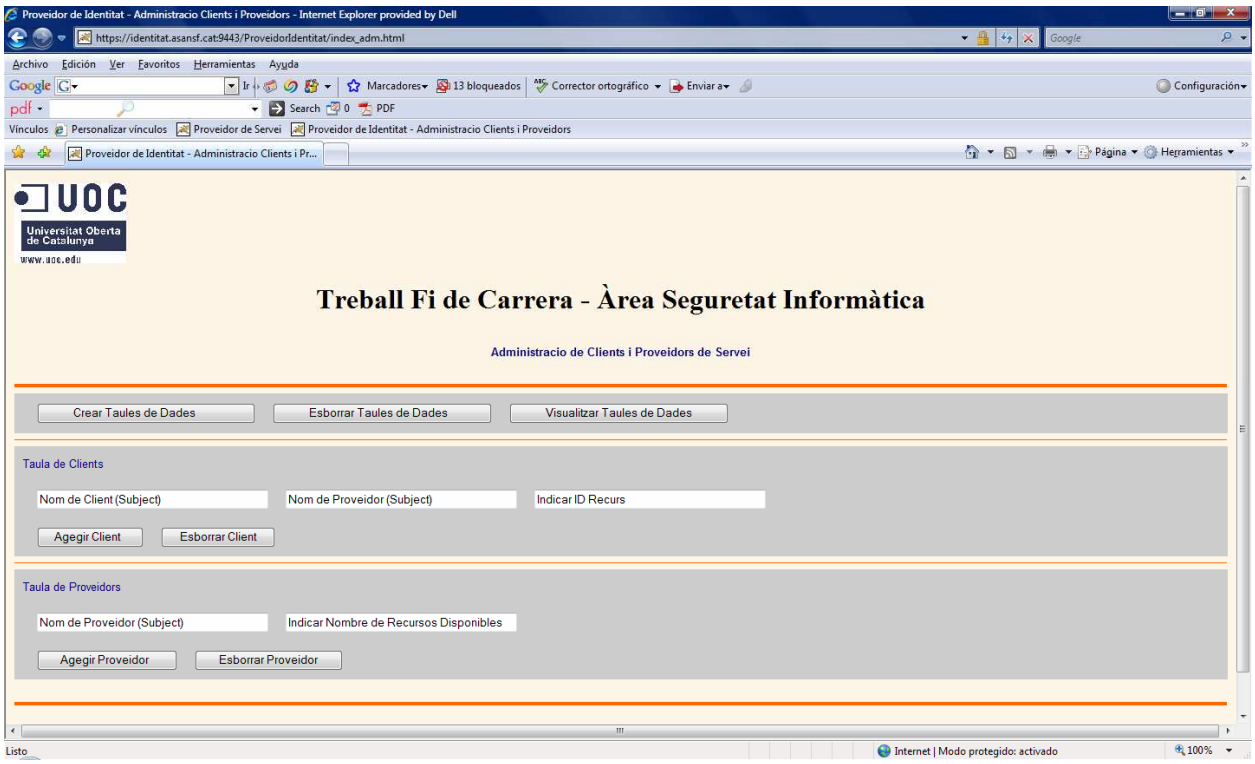


Figura 33

En la següent captura de pantalla podem visualitzar el resultat de la opció *"Visualitzar Taula de Dades"* que ens mostra les dos taules de dades i el contingut de cada una d'elles.

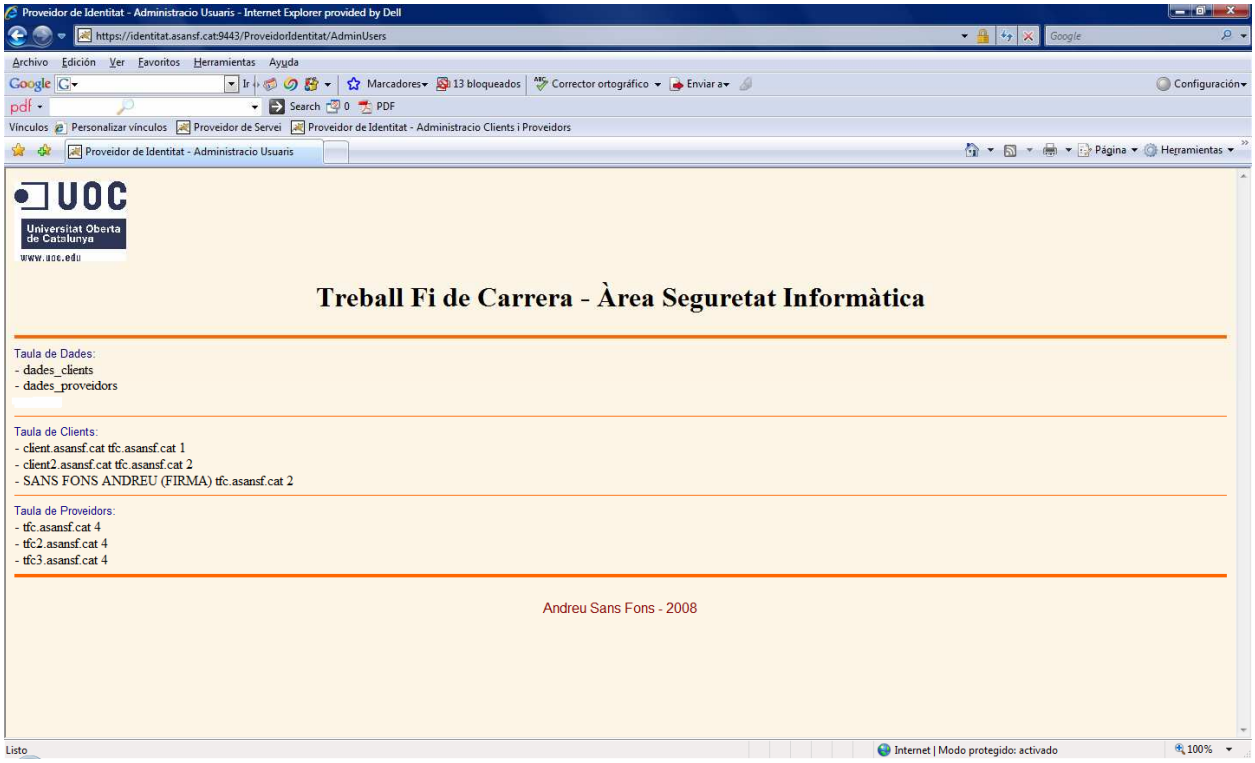


Figura 34

Mitjançant els botons d'afegir o Esborrar Client, afegim o traiem de la base de dades el client corresponent. Cal indicar el *subject* de client, el *subject* del proveïdor de servei i el recurs al que volem donar permís d'accés. De la mateixa manera podem afegir o treure de la base de dades els proveïdors de servei i el nombre de recursos que tenen disponibles.

6. Glossari

W3C	World Wide Web Consortium
XML	Extensible Markup Language
SOAP	Simple Object Access Protocol
Signatura Digital	Mètode que associa la identitat d'una persona o entitat a un missatge o un document. Un dels seus objectius és assegurar la integritat del missatge o document.
Certificat	Document digital en que una autoritat certificadora de confiança garanteix la vinculació entre la identitat del subjecte titular del certificat amb la seva clau pública.
CA	Autoritat de Certificació
Canal Segur	Establiment de connexió que garanteix la confidencialitat mitjançant xifrat i assegura que la connexió és fa contra el servidor que diu que s'estableix (autenticació de servidor).
J2EE	Java Platform, Enterprise Edition
Subject	Camp d'un certificat que indica el subjecte titular del certificat.
Applet	Component d'una aplicació que s'executa en el context d'un altre programa, en aquest cas un servidor web.
DNIe	Document Nacional Identitat Electrònic

7. Bibliografia

- Infraestructura de Clave Pública DNI Electrónico – *Ministerio del Interior*
- Material Docent Assignatura Criptografia – *UOC*
- Material Docent Seguretat en Xarxes – *UOC*
- Material Docent Sistemes de Comunicació – *UOC*
- Libro Electrónico de Seguridad Informática y Criptografía - *Jorge Ramió Aguirre*
- Tutorial Java - *SUN*
- XML-Signature Syntax and Processing – W3C
- Documentació de TomCat