Signatura Digital

Projecte Fi de Carrera
Carlos Vila Mateos
Enginyeria en Informàtica
Tutor: Josep Maria Camps Riba
Tardor 2010

Resum

Aquest projecte tracta la Signatura Digital des del punt de vista d'un Enginyer de Software que ha d'iniciar un projecte que doni serveis de Signatura Digital a un projecte més ampli d'Administració Electrònica

El projecte contempla:

- els conceptes bàsics de la Signatura Digital
- les particularitats de la Signatura Digital
- les funcionalitats i serveis que pot proporcionar a una plataforma de tramitació electrònica
- els requeriments de Signatura Electrònica per l'AE
- la selecció d'un proveïdor de serveis de Signatura que cobreixi els nostres requeriments i els de l'AE
- funcionalitats del proveïdor CATCert (plataforma PSIS)
- i, a traves d'aquests estudis, la realització de l'anàlisi, disseny i construcció d'un mòdul que pugui subministrar autenticació, identificació i signatura digital a una plataforma d'AE

Introducció

- Nous paradigmes en la relació humana amb l'impacte de les noves tecnologies i TIC.
- Forma de comunicar-se de la societat, de treballar, de relacionar-se, de pensar, d'educar-se, de l'oci, tot això està canviant a formes més àgils, més immediates, més complertes, amb més mitjans i variants gràcies a les noves tecnologies.
- Transició de l'Era Industrial a l'Era Digital o l'Era de la Informació.
- Canvien les formes tradicionals del funcionament de les organitzacions públiques i privades, l'economia, la política, comerç, marketing, impacte cultural i educatiu.
- Millora de processos, eficiència, reducció de paper, de desplaçaments i intercanvi d'informació física, reducció de redundància, comunicació immediata i telemàtica.
- Millora de les AAPP, LAECAP (Llei d'Administració Electrònica) i d'altres que indiquen que s'ha de poder treballar amb qualsevol tràmit o procés de l'administració de forma que es puguin executar de forma electrònica o on-line i que cap ciutadà o empresa hagi de presenciar-se a l'administració .
- Necessitem eines per donar suport a aquestes noves necessitats.
- Ens centrarem amb **una de les eines tecnològiques fonamentals** necessàries per a que aquesta **Societat Digital** pugi ser-ho, la **Signatura Digital**.

Objectius Principals

- En l'àmbit d'un projecte global d'AE (Administració Electrònica), aquest projecte té com objectiu principal **conèixer les possibilitats de la signatura digital i les primitives PKI, els proveïdors de serveis.**
- Cobrir els requeriments de Signatura Digital i serveis PKI fidels a les lleis d'AE i en l'àmbit d'una Plataforma de Tramitació Electrònica sense haver de desenvolupar la complexitat de la signatura digital.
- L'altre objectiu principal és el de realitzar una **integració amb les funcionalitats de signatura digital i proveir dels serveis de Signatura a l**a resta de programadors de la plataforma i usuaris. Aquest objectiu s'assolirà a través de la construcció d'un mòdul J2EE: **ProveidorSignatura**.
- La signatura digital serà un procés transparent pels usuaris de la nostra plataforma, de forma que aquests no hagin de ficar-se ni conèixer la complexitat de la signatura digital, donant així una capa de serveis de més alt nivell, que per sota es connectarà amb diferents, proveïdors, llibreries i serveis experts en la signatura digital. S'integraran les funcionalitats PKI i s'adaptaran per a que doni resposta als requeriments del nostre programari.

Assegurament dels Objectius

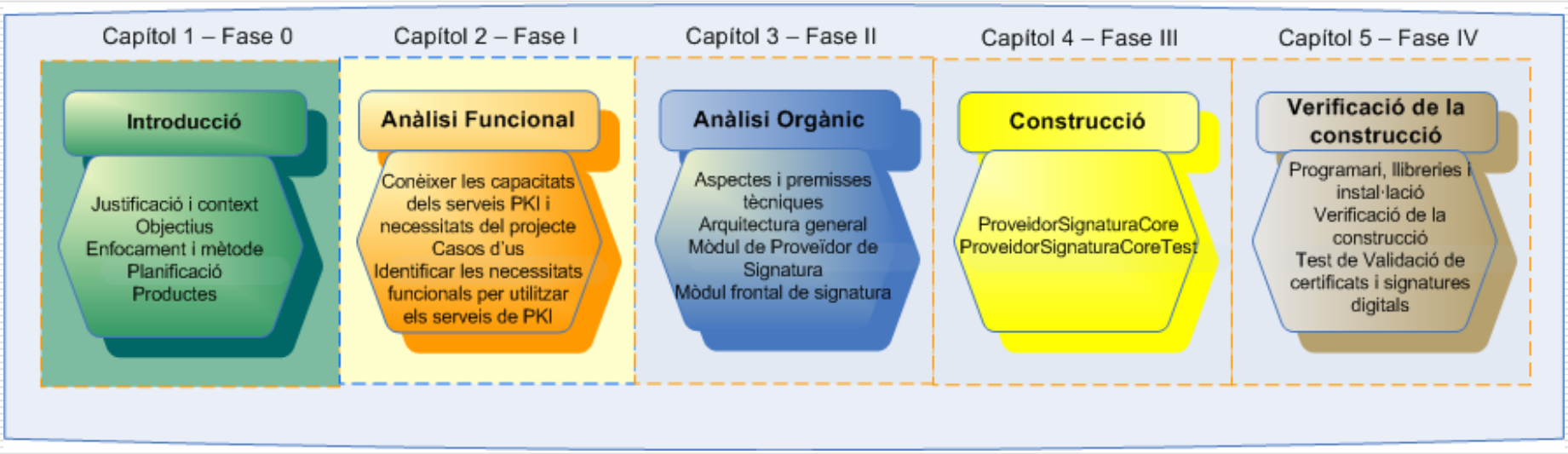
Per assolir aquests objectius s'ha preparat un desglossament en Work Breakdown Structure (WBS) a tres nivells per facilitar l'organització del projecte i el seguiment en blocs d'aquests. Aquesta estructura esta basada en l'extensió dels objectius de primer nivell en tasques realitzables per aconseguir aquests objectius.

Per això els objectius s'han desglossat en tres nivells:

- **Nivell de Fase**: Identifiquem 4 grans fases en el projecte que segueixen el sistema més clàssic de cicle de desenvolupament d'un projecte informàtic: Anàlisi Funcional (AF), Anàlisi Orgànic (AO), Construcció (CO), Proves i validació (PV)
- **Nivell macro-activitat o objectius de primer nivell**: Els objectius de primer nivell són els objectius principals a assolir, essent els objectius claus a complir.
- **Nivell tasques o objectius de segon nivell**: Els objectius clau, es descomponen en objectius de segon nivell o tasques amb la resolució de les quals s'han de veure complits els objectius de primer nivell (claus).

Estructura del PFC

Podem veure el cicle de vida de l'elaboració del projecte desglossat en fases, capítols de la memòria i i objectius de primer nivell. A més aquesta estructura ens ha servit per planificar el projecte i les seves fites.



La Signatura Digital

- En l'entorn de la Societat Digital s'havia de cobrir un àmbit essencial per a que la gent i les empreses poguessin realitzar els processos habituals bàsics de la seva rutina diària: la signatura d'un contracte laboral (empresa-treballador) o qualsevol altre tipus de contractes que es realitzen, la creació d'avals, els processos de facturació, els metges i els seus processos, les receptes, els accessos als bancs de forma segura, les interaccions entre AAPP (interoperabilitat), les interaccions entre AAPP i ciutadans, etc.

- Qualsevol procés que requerís la identificació de la persona física o jurídica, qualsevol procés que requerís documentació física (papers), tots aquests processos que es poden englobar perquè requereixen aquesta característica d'identificació i documentació fins ara es tenien que realitzar de forma presencial i amb el trasllat de documentació física cap a tots llocs. S'ha hagut de buscar una eina que permetés portar aquests processos a l'Era Digital, la digitalització i la signatura digital.

- La Signatura Digital i les seves variants ens ha permès convertir aquests processos en digitals i reconeguts amb la mateixa validesa legal que els processos tradicionals.

- Actualment ja no cal presenciar-se a cap lloc per realitzar aquests processos, ja no cal traslladar la documentació física.

- Han sorgit i seguiran sorgint aquests processos en l'àmbit digital com: la recepta digital, la factura digital, la identificació digital (DNIe), els càrrecs digitals, els notaris digitals, els contractes digitals, evidències digitals, etc.

- Per a donar solució a aquestes **necessitats de la Signatura Digital** es va crear la infrastructura de clau pública o PKI, el projecte es centrarà doncs en aquesta tecnologia i en la **construcció d'un mòdul de serveis PKI, el ProveidorSignatura**.

Instruments

- X509 v3: Us de certificats digitals basats en els algoritmes de clau pública o asimètrica
- Garantia de secret de les dades i comunicacions
- Garantia d'Autenticació i no repudi
- Integritat documental electrònica
- Us de protocols i estàndards de signatura: DSS, CMS, XMLDsig
- CA i TSA: Us d'un proveïdor de serveis de signatura reconegut: CATCert i la seva plataforma PSIS
- La filosofia J2EE: escalabilitat, seguretat, interoperatibilitat, transaccionalitat, distribuïble

Eines utilitzades

- IDE Eclipse Helios
- JDK v1.5 i Plataforma J2EE
- Programari i normatives de CATCert:plataforma PSIS, protocol DSS sobre XML i extensions, CMS, XMDSig, XADES, CADES, Certificats X509
- Framework de test: Junit
- Altres llibreries: Psis-beans, XMLBeans, XFire, Wsdl4j, Wss4j, Jdom

Funcionalitats

Construcció d'un mòdul J2EE com a Proveïdor de Signatura que integri els següents serveis de PSIS:

- Validació de signatures digitals (CMS i Cades).
- Validar segell de temps (CMS).
- Creació de segells de temps.
- Validació de certificats X509
- Extracció d'informació de certificats i signatures (normalització atributs).
- Validar Signatures CMS sobre documents pdf.
- Signatures Digitals Avançades (ADES):
  - Validar signatura.
  - Validar atributs: timestamps, validar cadena de certificació.
  - Completar atributs ADES.

Diagrama de casos d'us

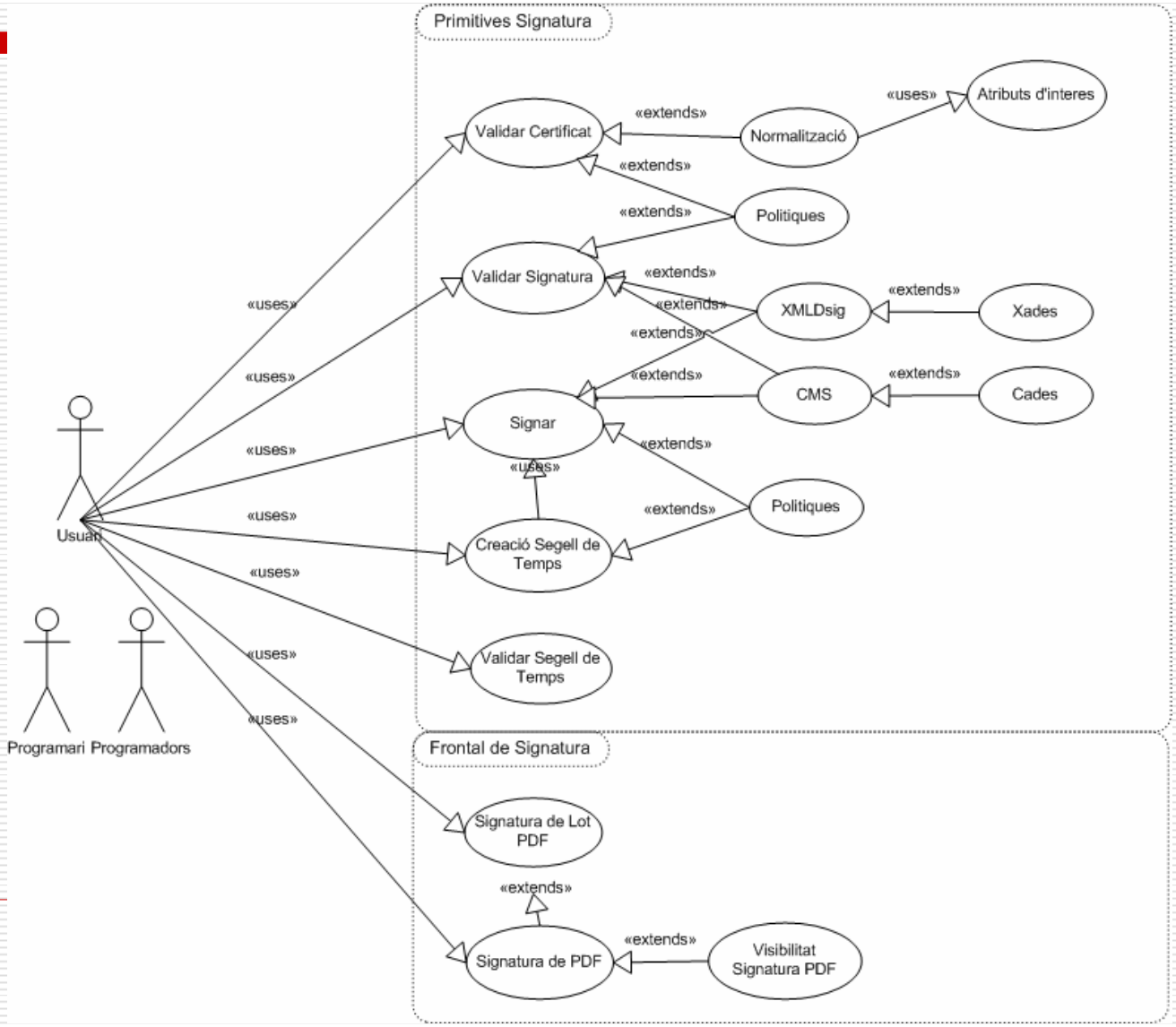


Diagrama de components

- Podem veure el diagrama de components i com es relacionen aquests en el marc de la plataforma de tramitació.
- Però centrarem els esforços en el desenvolupament del component ProveidorSignatura

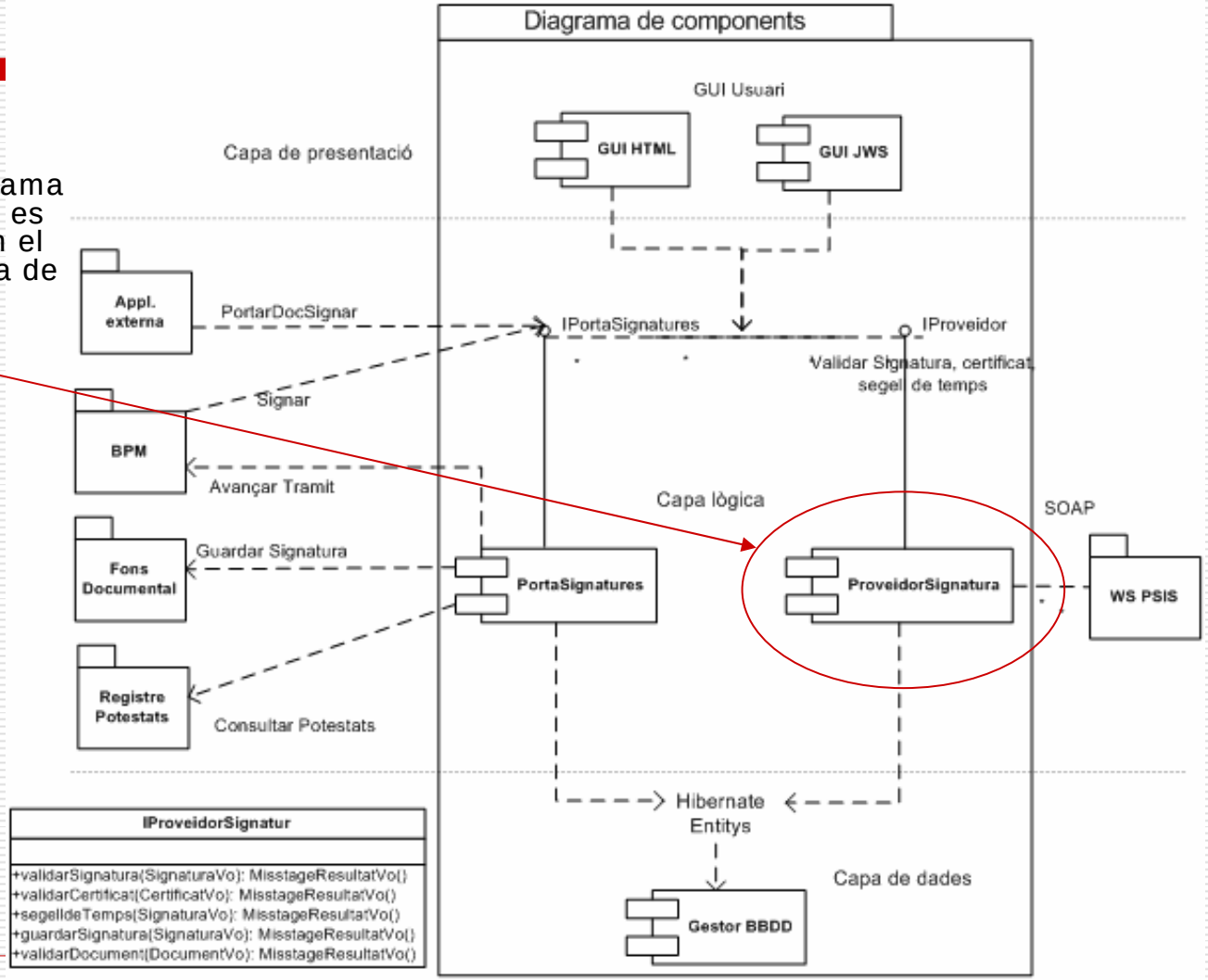
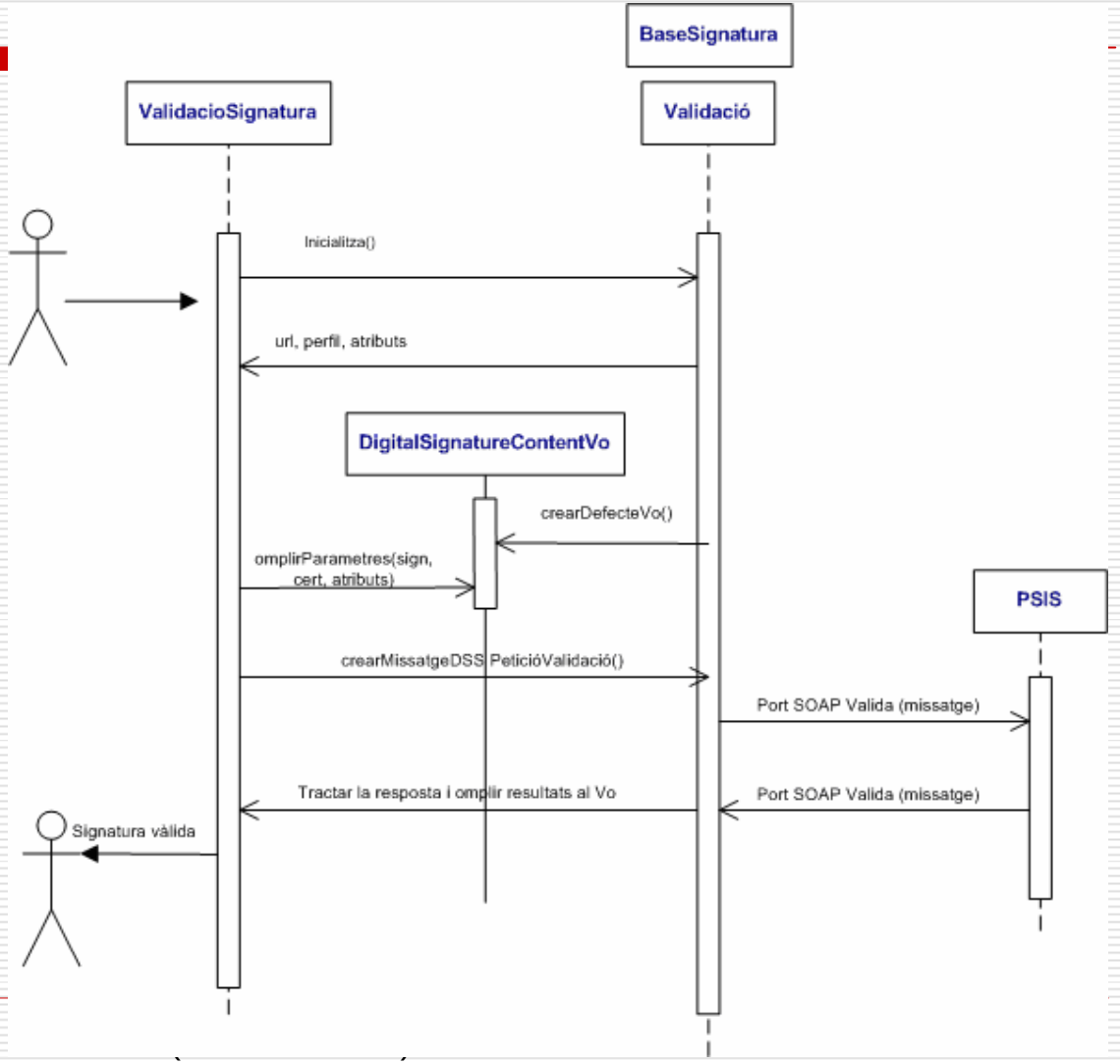


Diagrama de seqüència



Productes obtinguts

- **1) ProveïdorSignaturaCore.jar**: És una llibreria que ens permetrà a partir d'una API simplificada utilitzar serveis de Signatura Digital. Les Constants de Configuració i parametritzacions bàsiques estan predefinides de forma que les funcionalitats bàsiques tenen un fàcil accés i us. Aquesta llibreria també permet funcionalitats més complexes de Signatura afegint les parametritzacions avançades. Aquesta llibreria s'anirà ampliant amb noves funcionalitats.

- **2) ProveidorSignaturaCoreTest:** Paquet que ens permet provar les classes de signatura a través de la classe que exten TestCase SignaturaTest. Aquesta classe es centrarà en la lògica de negoci pròpia per realitzar les proves unitàries. Tindrem diferents mètodes per a provar cadascun de les primitives PKI implementades.

  Hem organitzat aquest paquet ProveidorSignaturaCoreTest com a un paquet independent en comptes d'afegir la classe a ProveidorSignaturaCore perquè així podem realitzar la prova definitiva des de fora del paquet core i crear el ProveidorSignaturaCore.jar, provar d'incloure'l en un altre paquet i veure que es poden realitzar totes les crides de forma correcte i amb les llibreries necessàries.

- **3) ProveïdorSignatura.ear:** El component de ProveidorSignatura estarà format per subcomponents o paquets que formaran una gran aplicació (enterprise o EAR) i que implementaran la lògica de negoci necessària per respondre a les necessitats de l'actor (appl. externa) segons els seus casos d'us. S'encarregarà de resoldre els casos d'us de l'actor appl. externa: validar certificat, normalització d'atributs, validar signatura, segell de temps, consultar documents signats i validar-los en un moment donat de temps. Aquest component donarà una interfície per accedir a les seves funcionalitats IProveidor. A aquesta interfície només podran accedir les aplicacions amb els permisos necessaris. Com hem vist en l'apartat anterior lliuràvem un .jar, una llibreria d'utilitats que hom podrà utilitzar al afegir al seu projecte. Si es vol incloure les mateixes funcionalitats amb un component distribuït o EJB en una plataforma escalable donem la possibilitat de fer-ho convertint la llibreria en aquesta tecnologia.

Conclusions

- Aquest projecte ens ha servit per a conèixer el món de la Signatura Digital i utilitzar les primitives bàsiques de PKI a través de proveïdors fiables de serveis de Signatura com CATCert.
- En aquest hem pogut comprovar com les eines informàtiques poden ajudar a resoldre problemes competitius a les empreses i ha facilitar l'accés digital a les persones.
- Hem vist quines eines eficaces existeixen pels serveis de Signatura Digital o PKI, sobre quins estàndards es recolzen aquesta infrastructura (DSS, XSS, XML, X509, XMLDSig, CMS) i quins proveïdors d'aquests serveis podem utilitzar. En aquest sentit hem entrat en detall en els serveis que proporciona CATCert a través de la seva plataforma de serveis d'identificació i signatura reconeguda, PSIS. A partir d'aquest punt hem analitzat, dissenyat i implementat una llibreria que proporciona abstracció a una futura plataforma de tramitació electrònica que a partir d'aquest punt anirà creixent i evolucionant juntament amb la Societat Digital i l'Era de la Informació.
- Això ho hem realitzat a partir d'una estructura de gestió de projecte dividida en quatre fases i planificada amb activitats per a complir els objectius del projecte. Cal destacar que a la fase funcional s'expliquen els conceptes i requeriments de la Signatura Digital i del projecte, a la fase orgànica s'explica les decisions principals en temes tècnics, de disseny i de construcció, a la fase de construcció s'explica l'estructura tècnica del programari i decisions d'implementació i a la fase de verificació es fa una validació formal i detallada del funcionament del programari integrat i desenvolupat.