Implementació d'un esquema criptogràfic per gestionar de forma segura els historials mèdics dels pacients a través d'una xarxa de comunicacions.

Nom Estudiant: **Gerard Farràs i Ballabriga**
Enginyeria en Informàtica

Nom Consultor: Jordi Castellà-Roca

Data Lliurament: 7 de Gener del 2007

Índex de continguts

- **Introducció**.
  - Objectius
  - Justificació
- **Esquema de seguretat dels expedients mèdics.**
  - Funcionalitats implementades.
  - Requeriments de seguretat.
- **Planificació del projecte.**
- **Implementació de l'esquema de seguretat.**
- **Representació de les dades: XML.**
- **Comunicació entre els components del sistema (RMI).**
- **Gestió de la informació (BBDD).**
- **Interfície gràfica.**
- **Joc de proves.**
- **Conclusions.**

Introducció

- L'aplicació de les **noves tecnologies** (TIC) en el sector sanitari obren noves i múltiples possibilitats.
- Entre elles, la possibilitat d'accedir via remota a historials clínics, transmissió de proves, representació i avaluació de resultats, entre altres: El que és coneix com a **telemedicina**.
- Tot i això, aquestes noves tecnologies incorporen també nous reptes: El de la **seguretat de la informació**.
- Les dades sanitàries son dades de caràcter personal que, per Llei, han de ser especialment protegides.

Definició d'objectius

- L'objectiu principal d'aquest PFC és implementar un sistema per a que pacients i metges puguin accedir de forma **segura** de forma **remota** a historials mèdics a través d'una xarxa (per naturalesa **insegura**) de telecomunicacions.

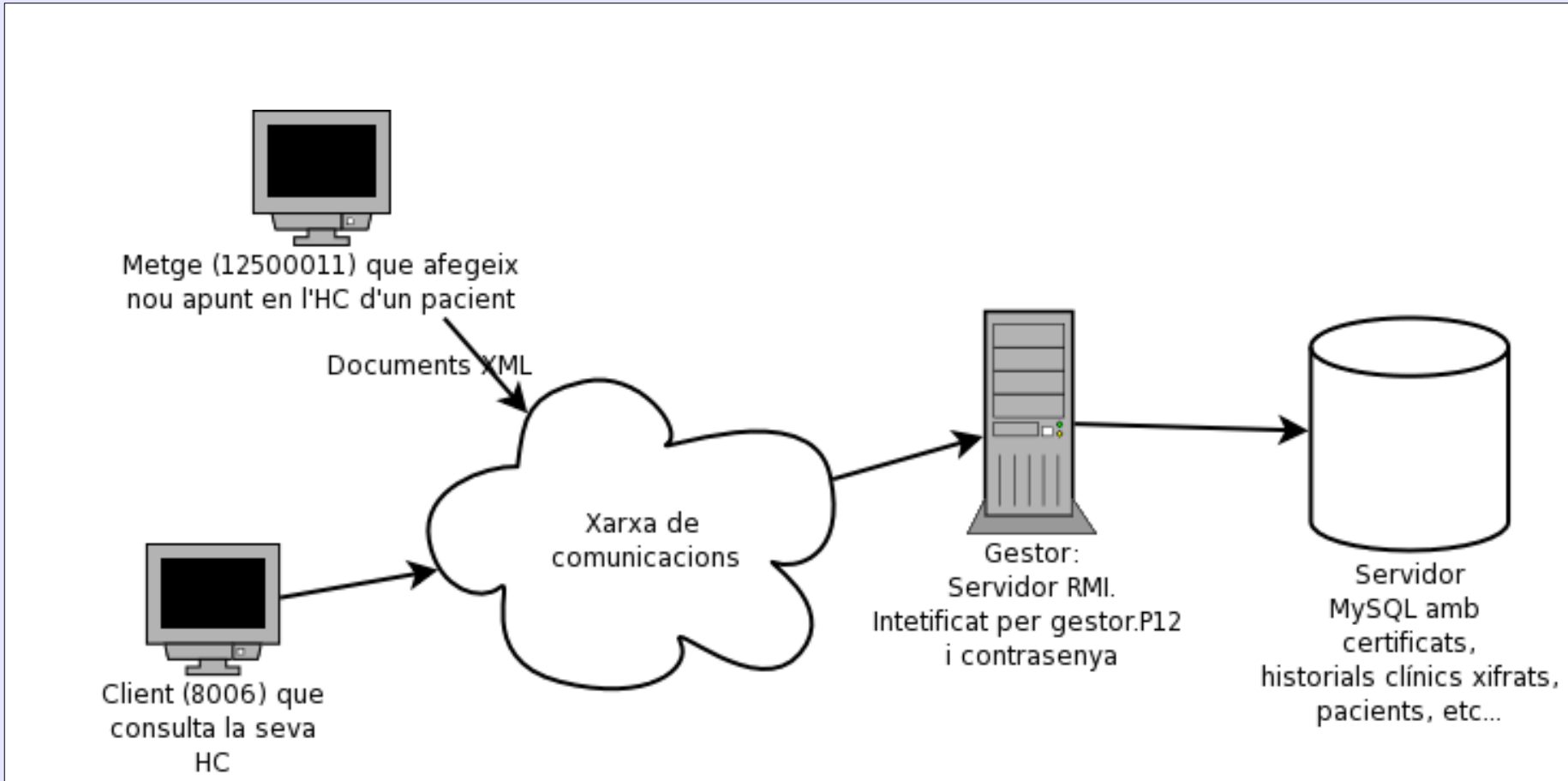
- Per aconseguir-ho:
  - Es generarà una **PKI** amb certificats digitals per a tots els usuaris.
  - S'implementaran un conjunt de **protocols criptogràfics**.
  - Les dades entre actors es transmetran via **XML**.
  - Les comunicacions es faran a través de **RMI**.
  - Les dades romandran xifrades en un servidor de **base de dades**.
  - Existiran **interfícies gràfiques** per als usuaris.
  - A més, es documentarà rigorosament tot el que es generi.

Justificació

- **El per què d'implementar un HIS (Hospital Information System)**
  - L'aplicació de les noves tecnologies en l'àmbit sanitari aporta un gran conjunt d'avantatges: Entre elles, la gestió de la informació de forma centralitzada, en digital, que es pot explotar i analitzar, que es pot controlar i auditar, etc...
  - Les telecomunicacions poden permetre l'accés de forma remota a aquests historials.

- **El per què d'implementar un esquema criptogràfic.**
  - Tot i això, els historials clínics son dades de caràcter personal amb especial protecció, tal i com regula *Ley Orgánica de Protección de Datos de Carácter Personal*. No solament la LOPD regula el tractament de dades sanitàries, també la llei 14/1986. L'article 10.3 de la Llei 14/1986 General de Sanitat estableix el dret del ciutadà a la confidencialitat de les seves dades.
  - S'ha de partir de la base que les xarxes de **telecomunicacions** son **insegures**.

Esquema de seguretat d'expedients mèdics



Funcionalitats implementades

A continuació, el llistat de **protocols** amb **base criptogràfica** implementats:

- **Autenticació en el sistema** (A través d'un fitxer P12 i la contrasenya d'obertura d'aquest).
- **Consulta d'una història clínica** (HC).
  - Vista per part del pacient.
  - Vista per part d'un professional sanitari.
- **Consulta del llistat de pacients** assignats a un metge.
- **Inserció de nous apunts** en l'historial mèdic d'un pacient per part d'un metge.

Requeriments de seguretat

- **Confidencialitat**: S'ha de preservar en tot moment la confidencialitat de les dades presents en l'historial mèdic dels pacients.
- **Autenticitat**: Les anotacions presents en l'historial mèdic han de contenir proves autèntiques i que hàgin estat realment escrites per als professionals pertinents.
- **Integritat**: Un cop la informació ha estat generada s'ha de garantir la seva integritat: Que no es pugui, per exemple, modificar-se de forma il·legítima.
- **No-repudi**: Si un usuari (ex. Un metge) del sistema fa certa acció (ex. Escriu un cert apunt en una HC), més tard no ha de poder negar-la (ex. Dir que ho ha escrit un altre).

Planificació del projecte

- PAC 1: IAIK i PKI (23/09/2007)
- PAC 2: Protocols criptogràfics (21/10/2007)
- PAC 3: Documents XML (4/11/2007)
- PAC 4: Comunicacions amb RMI (18/11/2007)
- PAC 5: Base de dades (02/12/2007).
- PAC 6: Vista client (16/12/2007)
- PAC 7: Vista gestor (30/12/2007).
- PAC 8: Documentació (7/01/2008).

Implementació de l'esquema de seguretat: PKI i llibreria IAIK

- Es requereix d'una PKI (***Public Key Infrastructure***)per tal de gestionar les claus, certificats i fitxers P12 digitals dels usuaris (pacients, metges i gestors) de sistema.
- La PKI es generarà a través del programari lliure **http://www.openssl.org/**.

- Per a la implementació dels protocols criptogràfics s'emprarà: Llibreria IAIK Java Cryptography Extension (IAIK-JCE).

- IAIK Java Cryptography Extension (IAIK-JCE) és un conjunt d'APIs que implementen funcionalitats criptogràfiques que NO es troben en el JDK per defecte de SUN.

Representació de dades: XML

- **XML**: Llenguatge de marques per a documents que contenen informació estructurada. Acrònim de "***eXtensible Markup Language***".

- En aquest projecte s'ha utilitzat XML per a representar les dades que s'intercanvien els usuaris (pacients i/o metges) i el gestor.

- Per al tractament d'aquests fitxers s'empra la llibreria amb llicència GPL "Jdom": http://www.jdom.org/

Comunicacions entre els components del sistema: RMI

- El sistema d'**Invocació Remota de Mètodes** (RMI) de Java permet a un objecte que s'executa en una màquina virtual de Java cridar a mètodes d'objectes que estan en màquines virtuals diferents, ja sigui en un mateix ordinador o en un de remot.

Comunicacions entre els components del sistema: RMI

- Comuniquem objectes "Metge" o "Usuari" amb el "Gestor" amb els mètodes :
  - XMLDocument procedure2(XMLDocument);
  - boolean pas4(XMLDocument)
  - boolean verPacMetge(Pacient , Metge)
  - XMLDocument procedure3 (Pacient , Metge)
  - XMLDocument procedure5 (id_usuari)
  - boolean pas4InserirVisita (apunt)
  - XMLDocument retornaLlistatCIE ()
  - XMLDocument getDadesAdminPacient (id_usuari_vull , id_usuari_peticio)

Gestió de la informació: BBDD

- Per a emmagatzemar totes les dades del sistema, s'empra una base de dades relacional.

- Escollim el sistema gestor de base de dades MySQL a causa de la seva robustesa, facilitat d'ús, eficiència, al fet que és programari lliure i al fet que és multiplataforma.

Gestió de la informació: BBDD

- Per a emmagatzemar les taules, s'empren les següents taules:
  - **certificats**: Amb els certificats dels diferents actors del sistema.
  - **codCIE9**: Amb el llistat de malalties associades al codi CIE-9.
  - **diagnostics**: Amb els diagnòstics associats als pacients.
  - **metges**: Amb la informació dels professionals sanitaris.
  - **pacients**: Amb la informació dels pacients.
  - **sessionsges**: Per a emmagatzemar dades de sessions.
- Per a crear les taules en el servidor MySQL, executar les comandes següents:
  - *mysqladmin -u root -p create pfchistorials*
  - *mysql -u root -p pfchistorials < src/pfchistorials.sql*

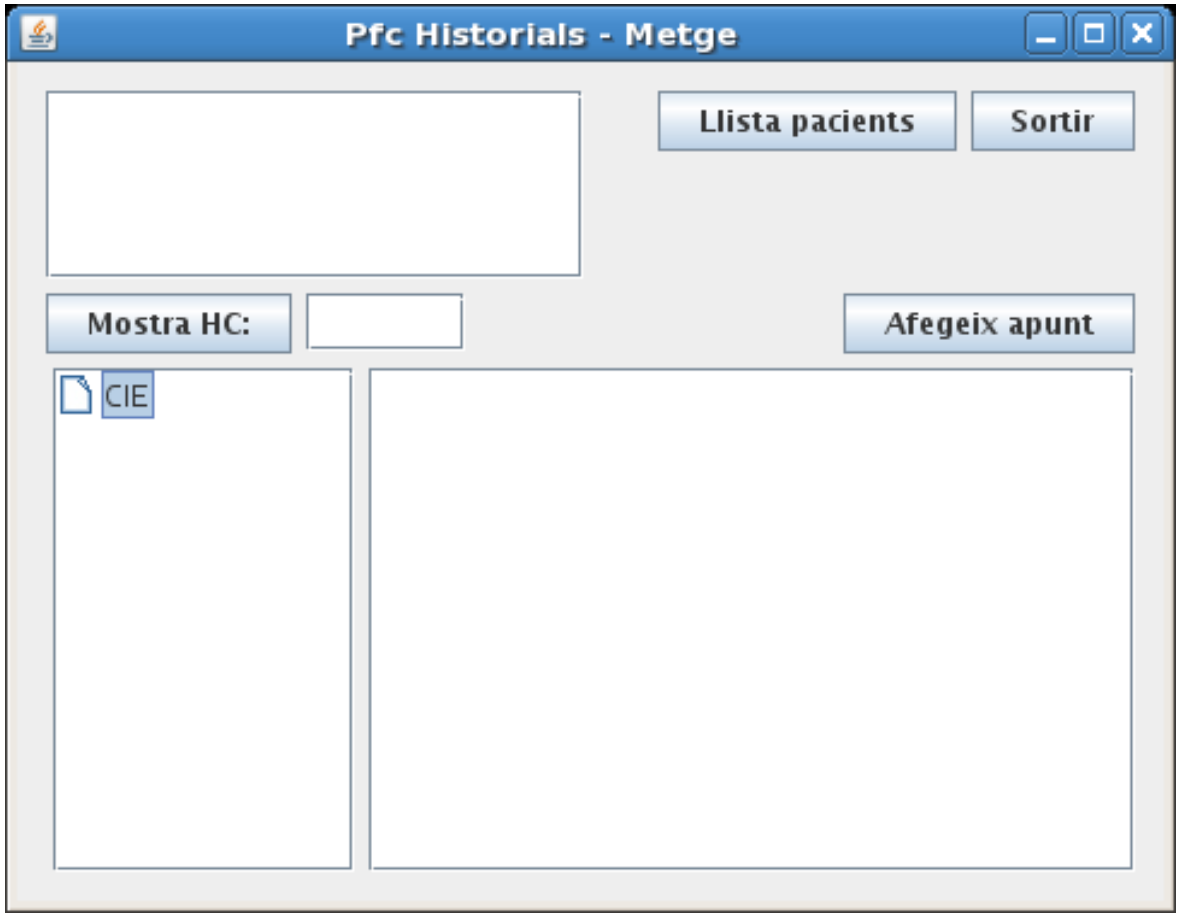
Interfície gràfica

- S'implementarà una interfície gràfica per a poder realitzar les operacions de forma còmoda.

- Per a la interfície gràfica del gestor i dels clients s'utilitzarà la llibreria de Java: **javax.swing**.

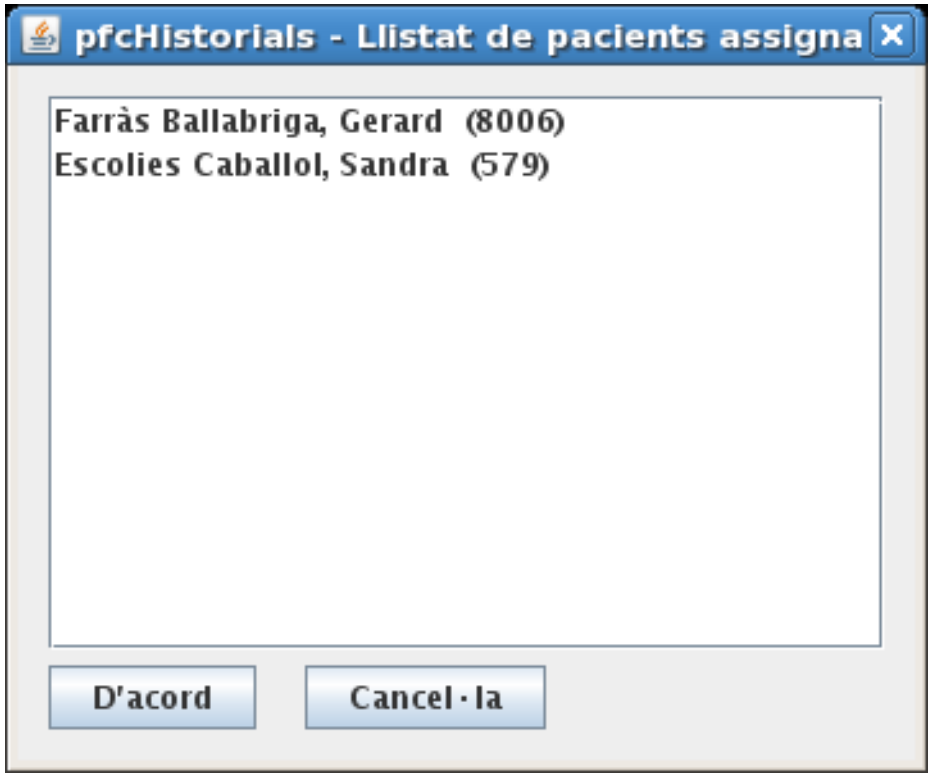
- Per al disseny de les interfícies s'ha emprat el programa: **NetBeans**: "*The NetBeans IDE is a free, open-source Integrated Development Environment for software developers.* "

Interfície gràfica: Captures de pantalla de l'aplicació



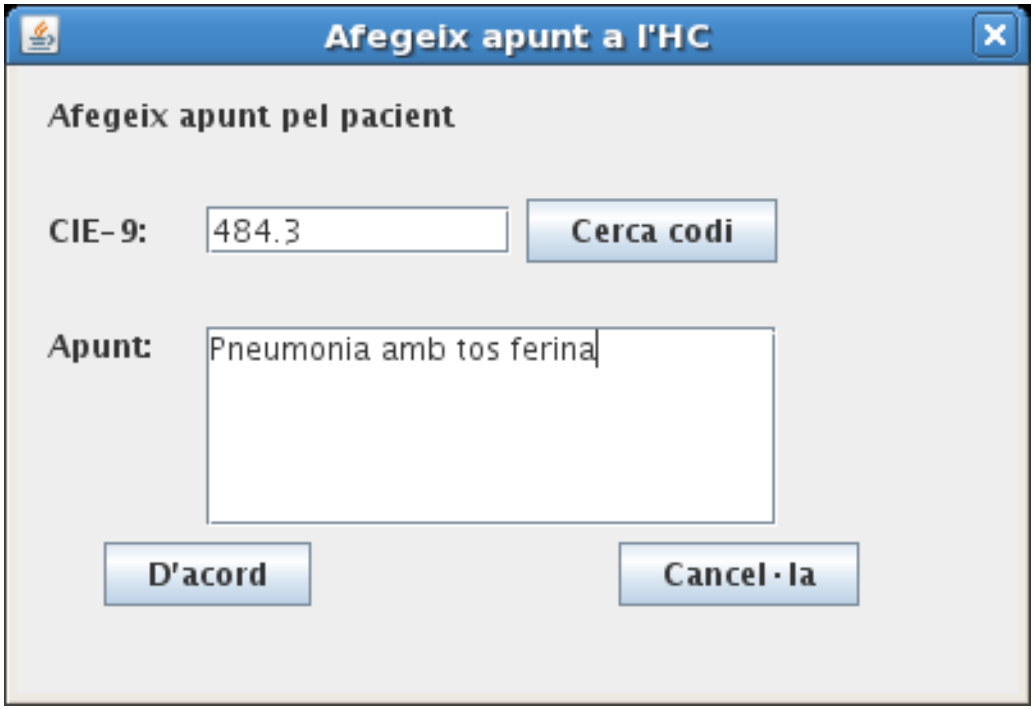
Pantalla principal per a professionals sanitaris. Interfície creada a través del programa NetBeans.

Interfície gràfica: Captures de pantalla de l'aplicació



Llistat de pacients assignats a un metge. Interfície continguda en el fitxer **pfcGuiLlistaPacients.form**

Interfície gràfica: Captures de pantalla de l'aplicació



Pantalla per afegir un apunt a un pacient.

Cada apunt s'associa a una malaltia identificada per al codi CIE-9.

Joc de proves: Instal·lació

Per a instal·lar el programa és necessari disposar de:

- Java Platform SE 1.6.
- Llibreria IAIK (iaik_jce_full.jar).
- OpenSSL.
- MySQL.
- JDOM (jdom.jar).
- mysql-connector-java-5.0.7-bin.jar

Jocs de proves: Instal·lació

- Crear una BBDD en el servidor de MySQL (ex. **Mysqladmin -u usuari -p contrasenya create pfchistorials.**).
- Importar-hi l'estructura bàsica:
  mysql -u root -p contrasenya < src/pfchistorials.sql.
- Configurar el fitxer bin/cfgBBDD.txt amb els paràmetres de connexió a la base de dades.

Jocs de proves: Funcionament gestor

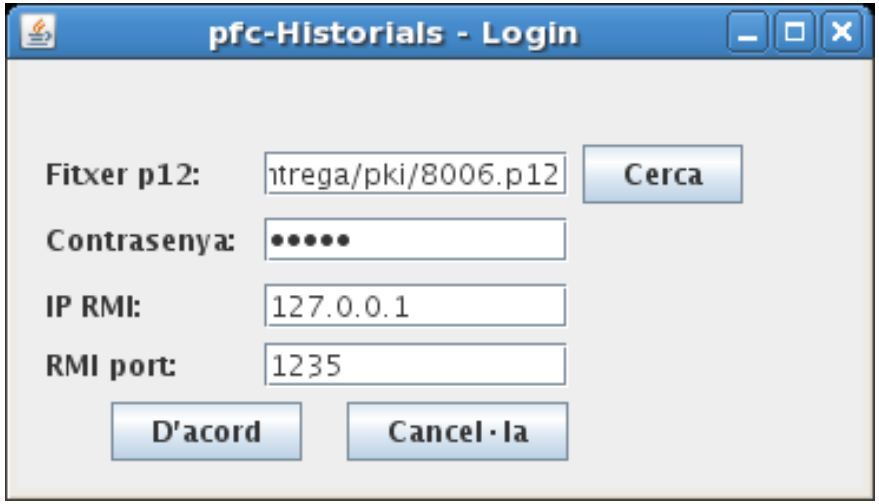
- Per a posar en marxa el programari, primer executem el gestor:
  cd bin/
  ./executaGestor 2099 &

- Serà necessari introduir el port RMI (2099), el fitxer P12 (pki/gestor.p12) del gestor i la seva contrasenya d'obertura (uoc07).

Jocs de proves: Funcionament client

- A continuació, posem en marxa el client:
  cd bin/
  ./executaClients.sh

- Serà necessari introduir el port RMI del gestor (2099) i el fitxer P12 de l'usuari que vulguem emprar (pki/8006.p12 per a un pacient) o (pki/125000011.p12) per a un metge. Contrasenya: uoc07.



Conclusions

- S'ha desenvolupat un sistema per a poder **accedir de forma remota i segura a historials clínics.**

- Conjunt de protocols criptogràfics que permeten:
  - **Autenticar** a metges i pacients en el sistema.
  - **Mostrar historials clínics** a pacients i metges.
  - Per als metges, mostrar un **llistat amb els seus pacients.**
  - Possibilitat d'afegir un **nou apunt en la història clínica** d'un pacient.

- S'ha implementat la majoria dels altres objectius: Representació de dades via **XML**, comunicacions via **RMI**, base de dades **MySQL**, **interfícies gràfiques** per a clients i gestor. NO s'ha desenvolupat interfície per a afegir nous usuaris en el sistema.