Projecte Fi de Carrera

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

Fortià Bofill Espada
Enginyeria en Informàtica

Jordi Castellà Roca
Consultor

Introducció

Es vol proporcionar una solució en el camp de la sanitat perquè els metges puguin gestionar els historials mèdics dels seus pacients de forma remota i segura, i perquè els pacients puguin consultar la seva història mèdica també remotament i amb total seguretat en qualsevol moment i ubicació.

Introducció

- Objectius
  - Implementar esquema criptogràfic
  - Realitzar aplicacions
    - Metges/pacients
    - Gestor

Introducció

- Justificació
  - Millorar l'atenció mèdica que rep el pacient estalviant temps al metge
  - Estalviar temps al pacient
  - Compliment de la llei de protecció de dades de caràcter personal (LOPD)

Organització de la informació

- Historial
  - Dades generals (nom, cognoms, nº tarjeta sanitària, dni, grup sanguini,al·lèrgies, certificat)
  - Llista visites protegida
    - Llista de descriptors de visita xifrada per Ksessió
    - Signatura llista de descriptors del gestor
    - Llista d'accés (criptogrames de Ksessió dels metges que tenen accés, pacient i gestor)
  - Llista de metges protegida (xifrat pel gestor)
- Visita
  - Descriptor de visita (id, data, hora, tema,metge)
  - Dades de la visita (anamnesi,diagnosi, tractament)
  - Signatura digital descriptor i dades del metge
- Metge
  - Nom, cognoms,nº col·legiat, DNI, especialitat, certificat, llista de pacients protegida (xifrada pel gestor i metge i signada pel gestor)

Esquema de seguretat

- Funcionalitats implementades
  - Autenticació dels usuaris
    - Consulta de les dades generals d'un pacient
    - Consulta de les visites d'un pacient
    - Consulta dels pacients assignats a un metge
    - Afegir una visita a l'historial mèdic
    - Gestió dels usuaris

Esquema de seguretat

- Requeriments de seguretat
  - Confidencialitat
    - Visites dels pacients
    - Llista de pacients
  - Integritat
    - Dades de la visita
    - Relació visita-pacient
    - Llista dels pacients dels metges
  - Autenticitat
    - Accessos dels usuaris
  - No-repudi
    - Autoria d'una visita

Planificació del projecte

- Implantació de la PKI
- Implementació de l'esquema criptogràfic
- Representació de la informació
- Implementació de les comunicacions
- Base de dades
- Interfície gràfica

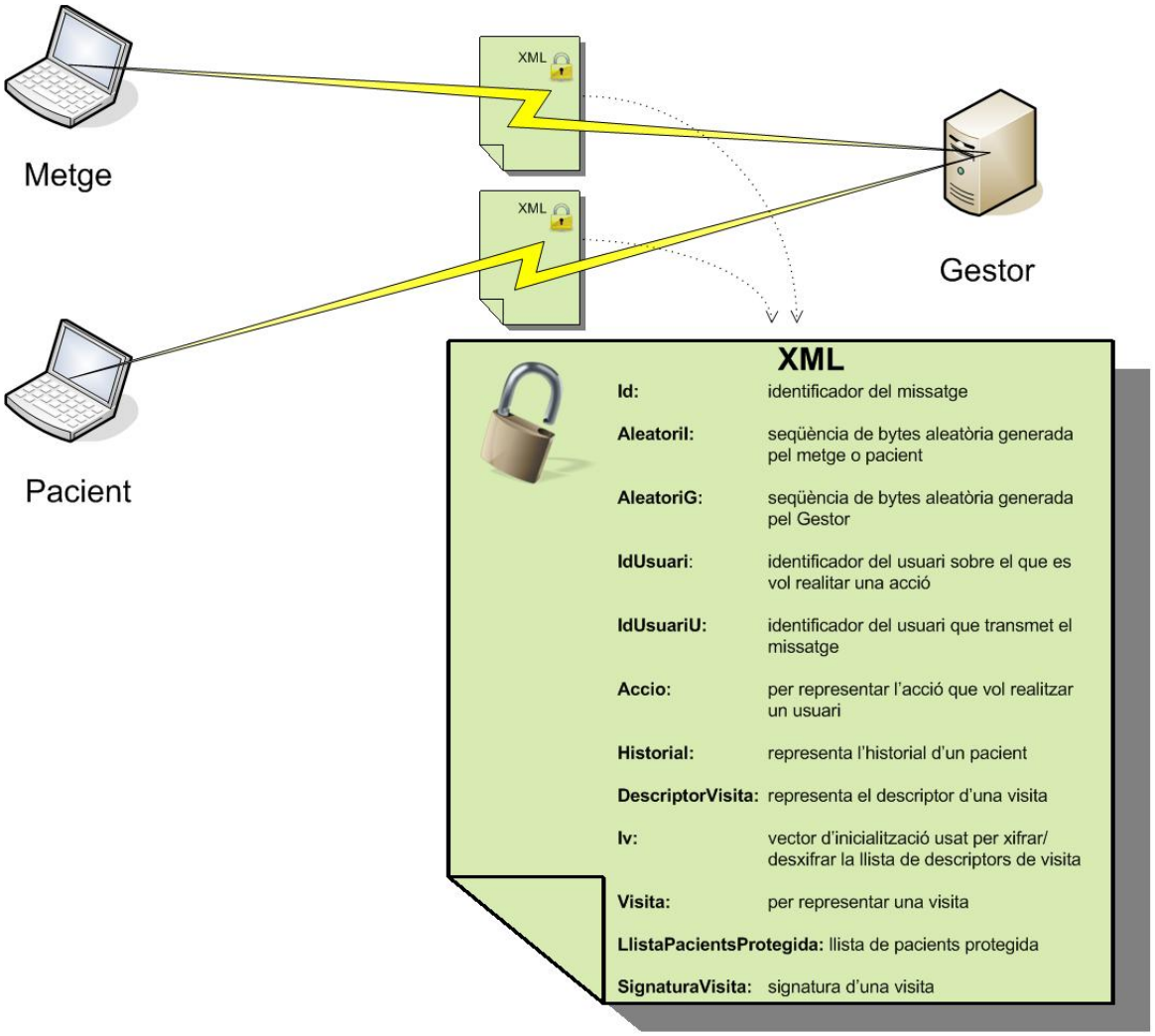
Implementació de l'esquema de seguretat

- PKI
  - Generació parella de claus 2048 bits CA
  - Creació certificat autosignat per la CA utilitzant les 2 claus anteriors
  - Generació parella de claus 1024 bits pels usuaris i gestor
  - Emissió petició de certificat pels usuaris i gestor
  - Emissió del certificat d'usuaris i gestor
  - Creació dels fitxers PKCS12 dels usuaris i gestor (parella de claus, certificat d'usuari i certificat de la CA)

Implementació de l'esquema de seguretat

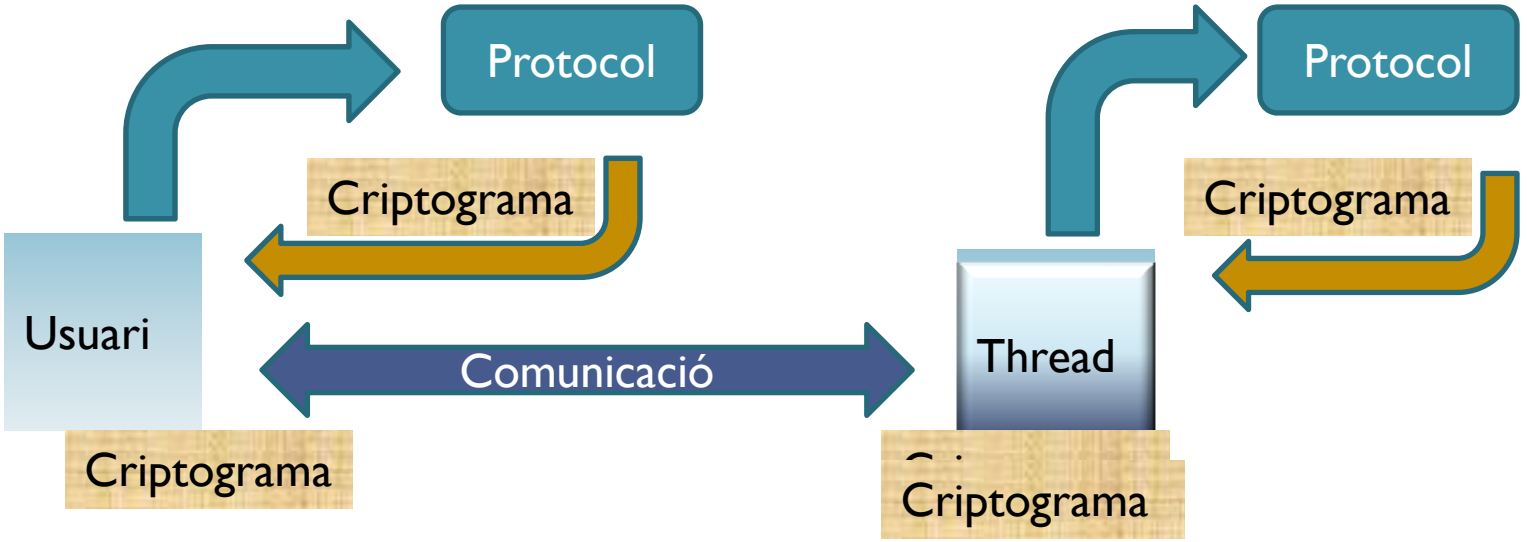
- Protocols implementats
  - Consulta de les dades generals d'un pacient
  - Consulta d'una visita d'un pacient
  - Consulta dels pacients assignats a un metge
  - Afegir una visita a l'historial mèdic d'un pacient
- Autenticació contra el gestor

Representació de les dades: XML



Comunicació entre els components del sistema

- Comunicació Client – Servidor per sockets
  - Senzillesa
  - Desenvolupament client smart-phone futur
  - Sockets de flux (TCP)
- Per cada pas d'un protocol a processar:

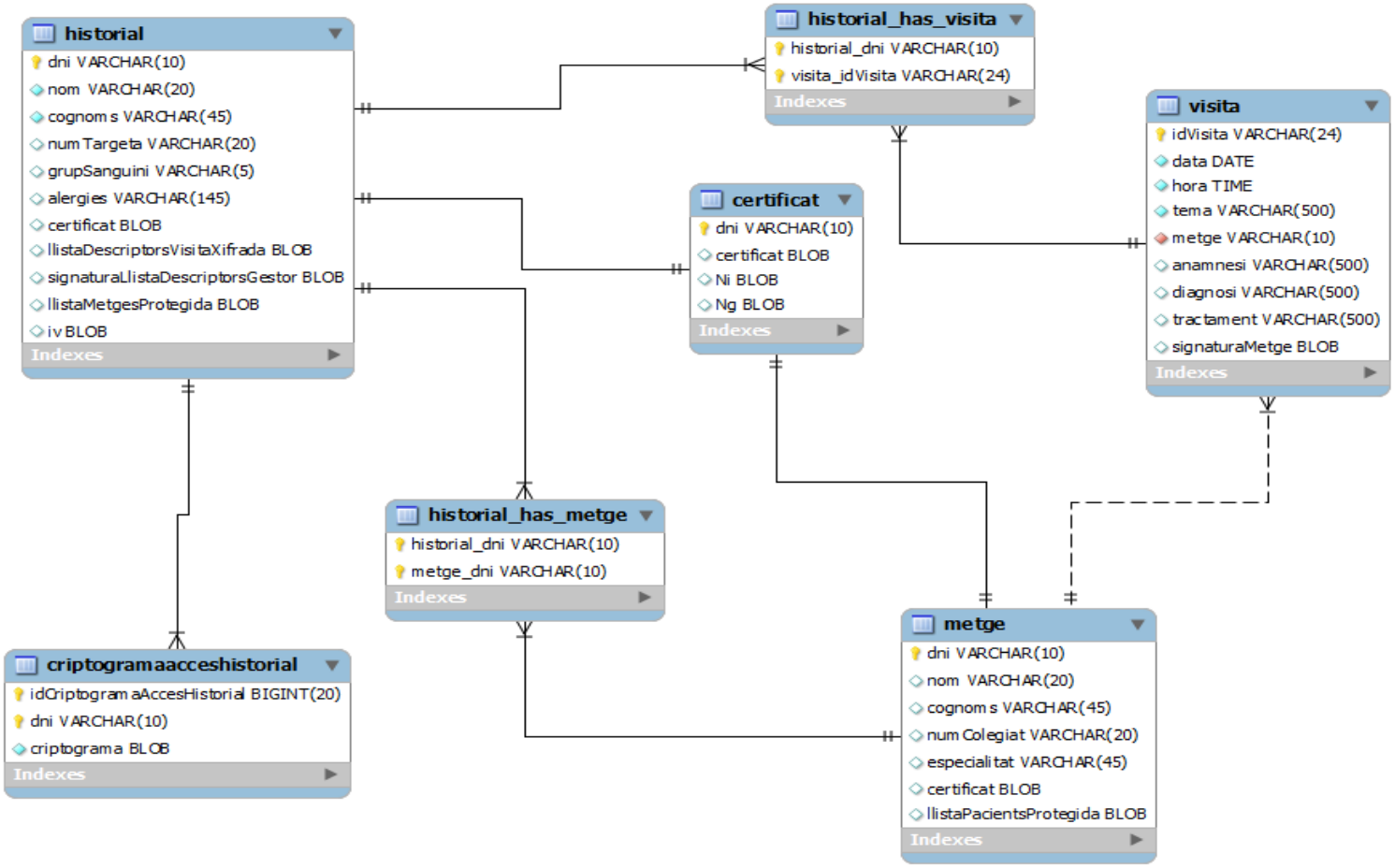


Gestió de la informació: BD

- Persistència de les dades SGBD de MySQL
- Connexió amb la BD JDBC Connector/J
- Taules de la BD:
  - Historial
  - CriptogramaAccesHistorial
  - Certificat
  - Visita
  - Metge

Gestió de la informació: BD

- Disseny de la BD

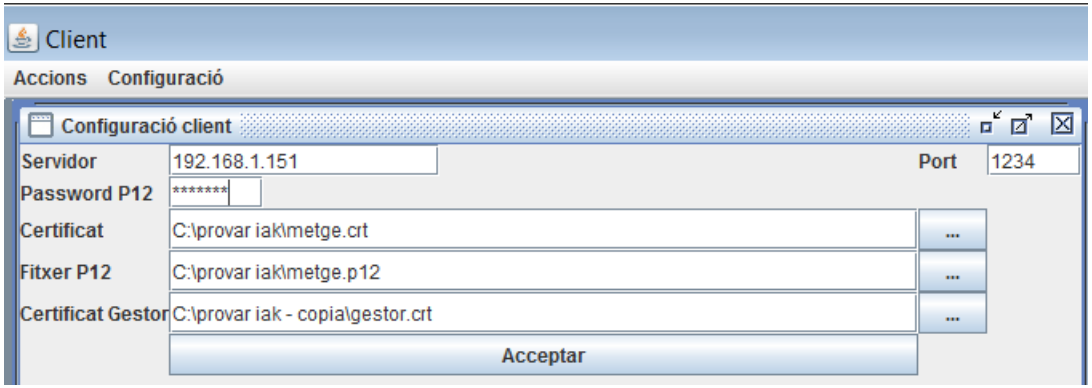


Interfície gràfica

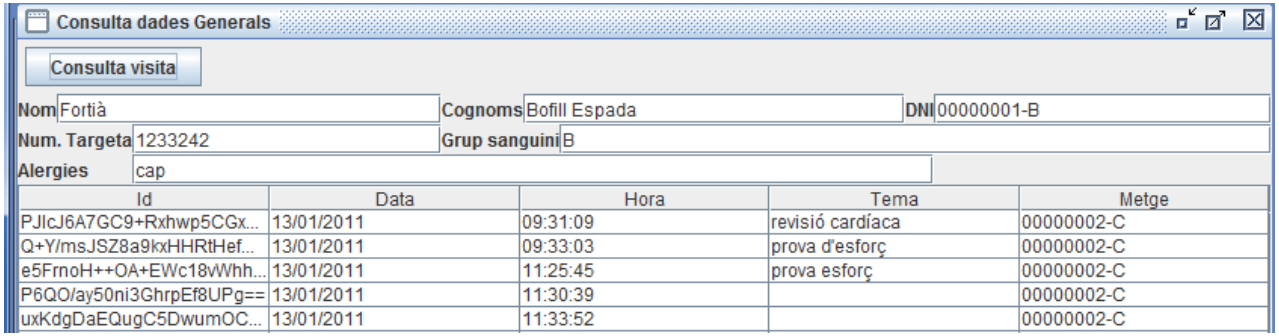
- Ús de llibreries Swing
- Interfície del gestor (servidor)
- Interfície del pacient/metge (client)
- Fitxers XML

Interfície gràfica (client)

- Client (pacient o metge)
  - Configuració del client



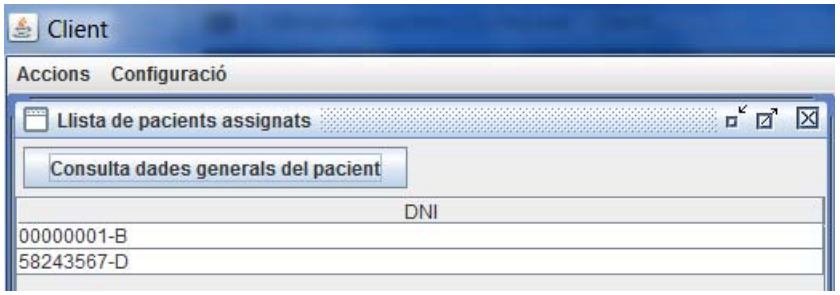
  - Consultar dades generals d'un pacient (demanat pel pacient)



Interfície gràfica (client)

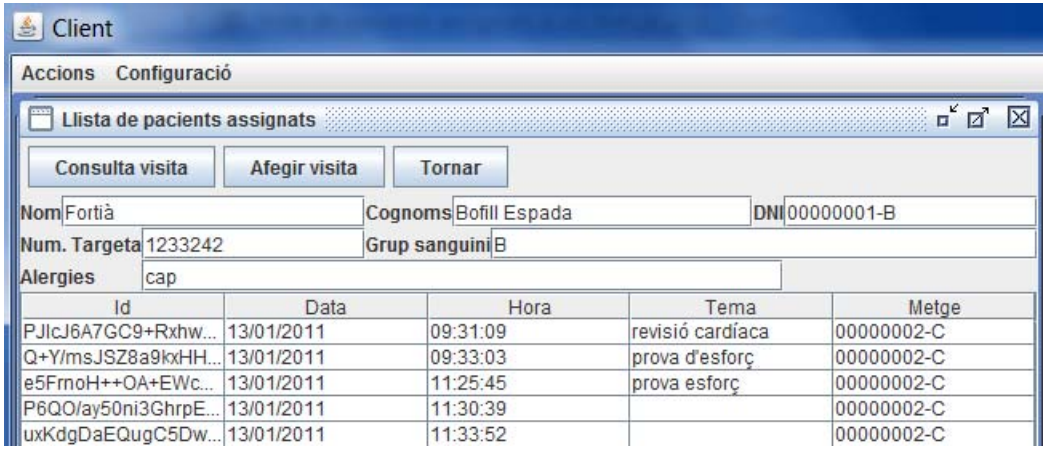
- Consulta d'una visita

- Llistar els pacients d'un metge

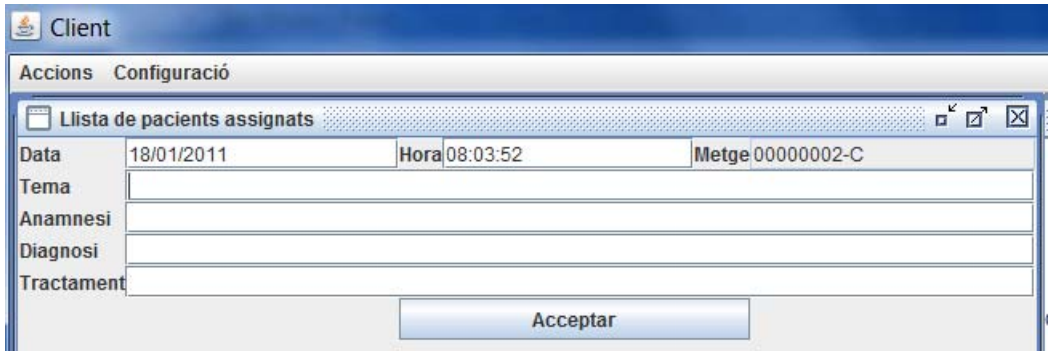


Interfície gràfica (client)

- Consulta de les dades generals d'un pacient (demanat pel metge)



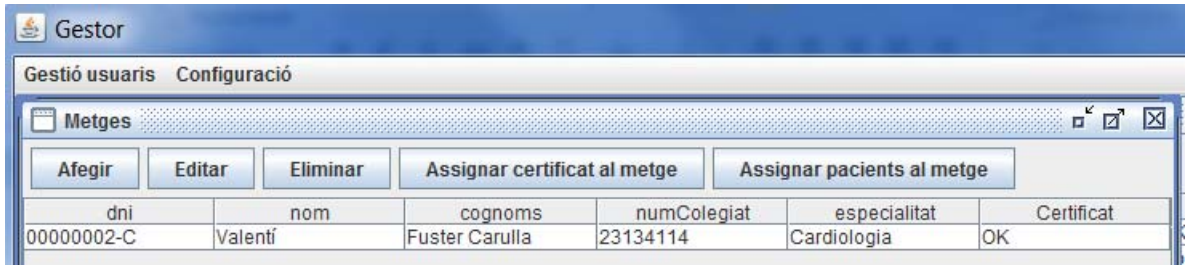
- Afegir visita a un pacient del metge



Interfície gràfica (servidor)

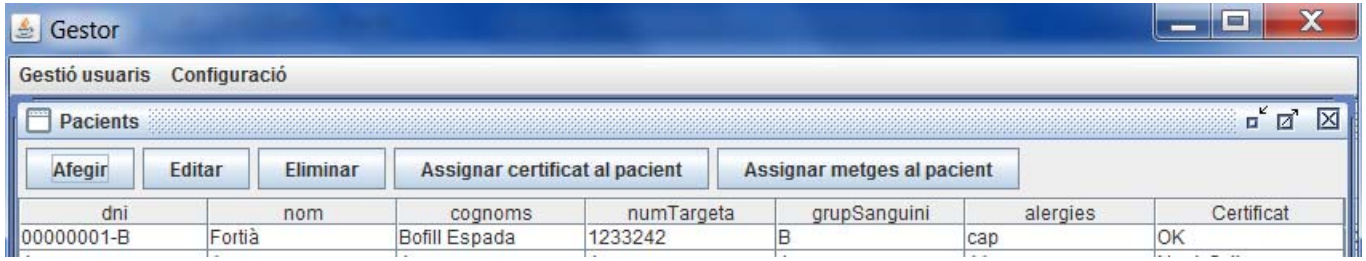
- Servidor (gestor)
  - Configuració del servidor

  - Gestió dels metges

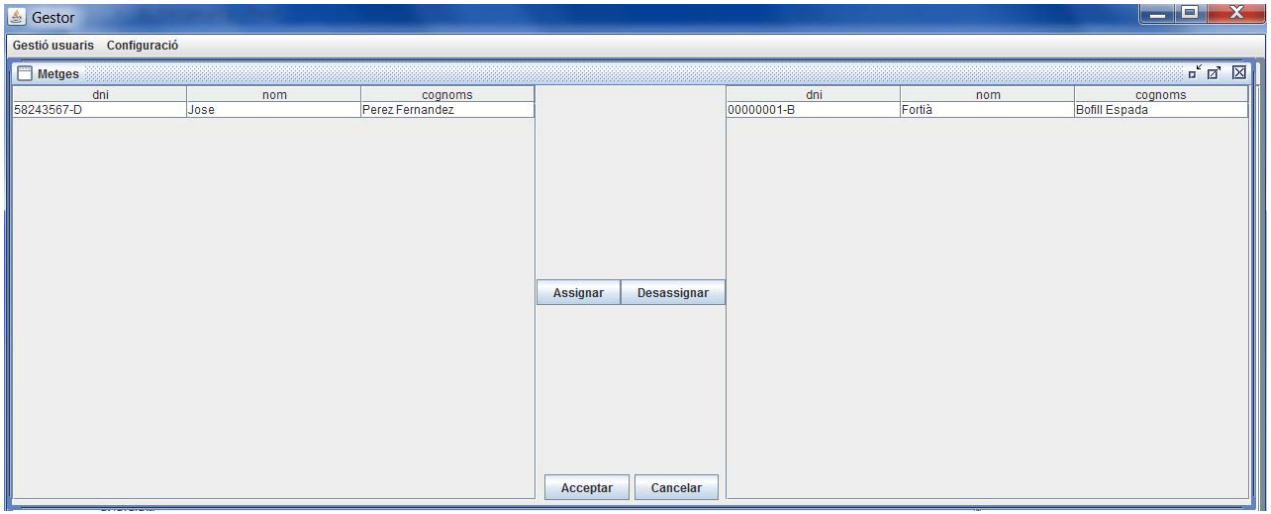


Interfície gràfica (servidor)

- Gestió dels pacients

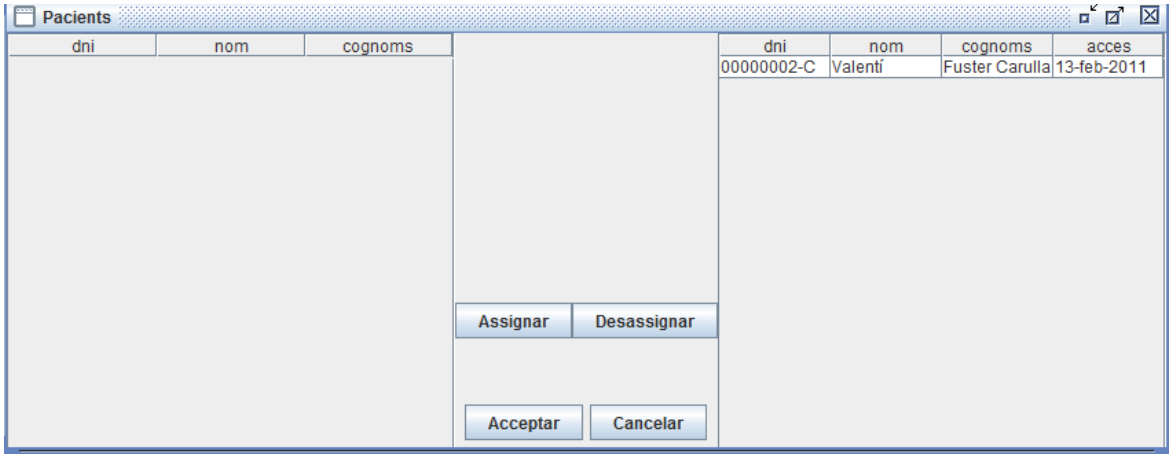


- Assignar pacients al metge

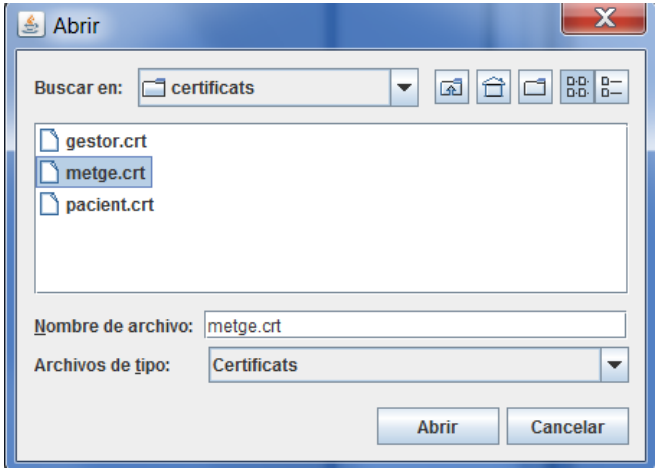


Interfície gràfica (servidor)

- Assignar metges als pacient



- Assignar un certificat a un metge o pacient



Conclusions

- S'ha desenvolupat un esquema criptogràfic per gestionar de forma segura els historials mèdics dels pacients a través d'una xarxa de comunicacions
- S'han obtingut tres aplicacions:
  - Gestor
    - Gestió dels metges i pacients de forma segura
    - Autenticar als usuaris
    - Guardar de forma segura els historials mèdics
    - Verificar les dades que s'insereixen o modifiquen
  - Metge
    - Consulta de les dades generals i consulta de les visites
    - Llistar pacients
    - Afegir visita
  - Pacient
    - Consulta de les dades generals (pròpies)
    - Consulta de les seves visites