



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

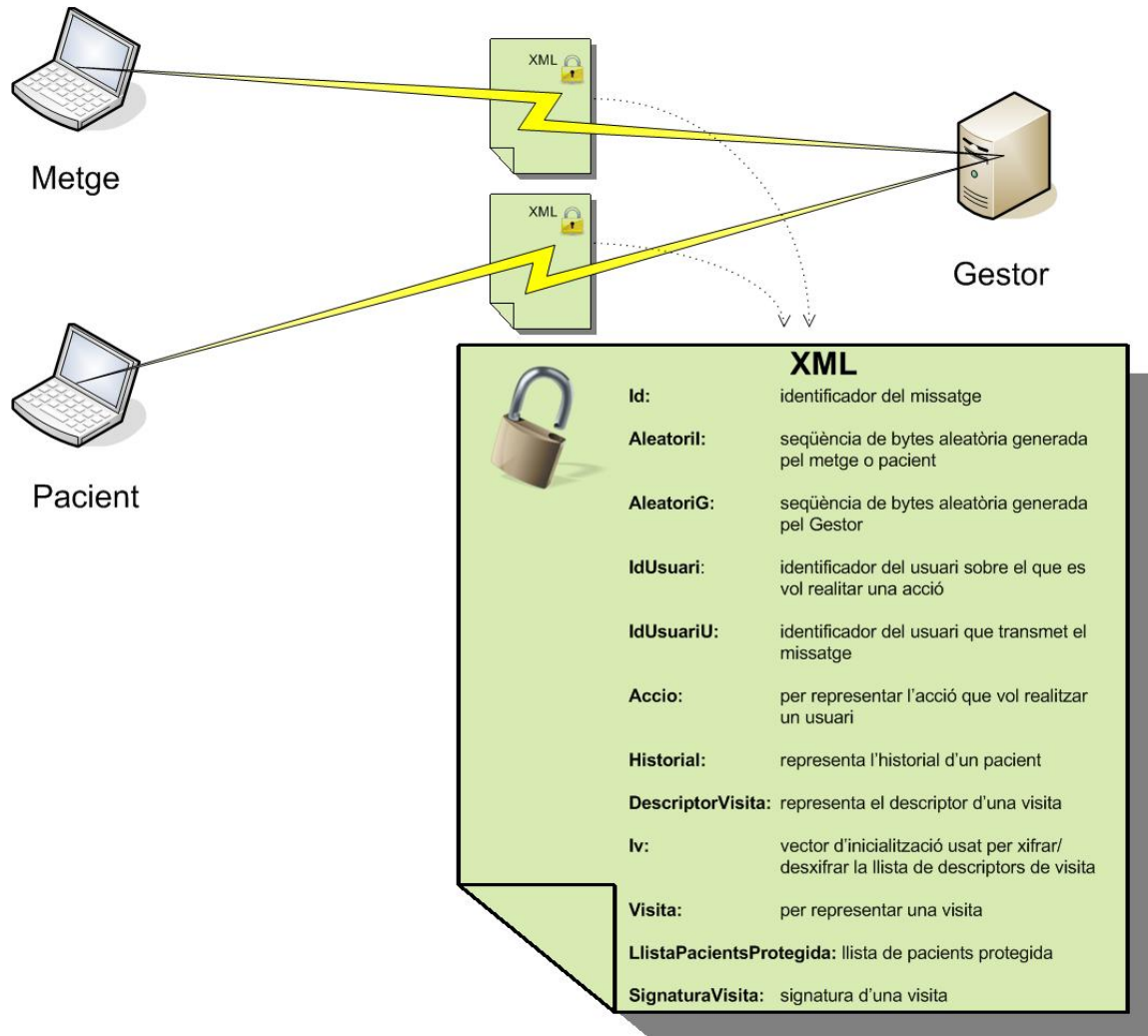
Implementació de l'esquema de seguretat

- 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

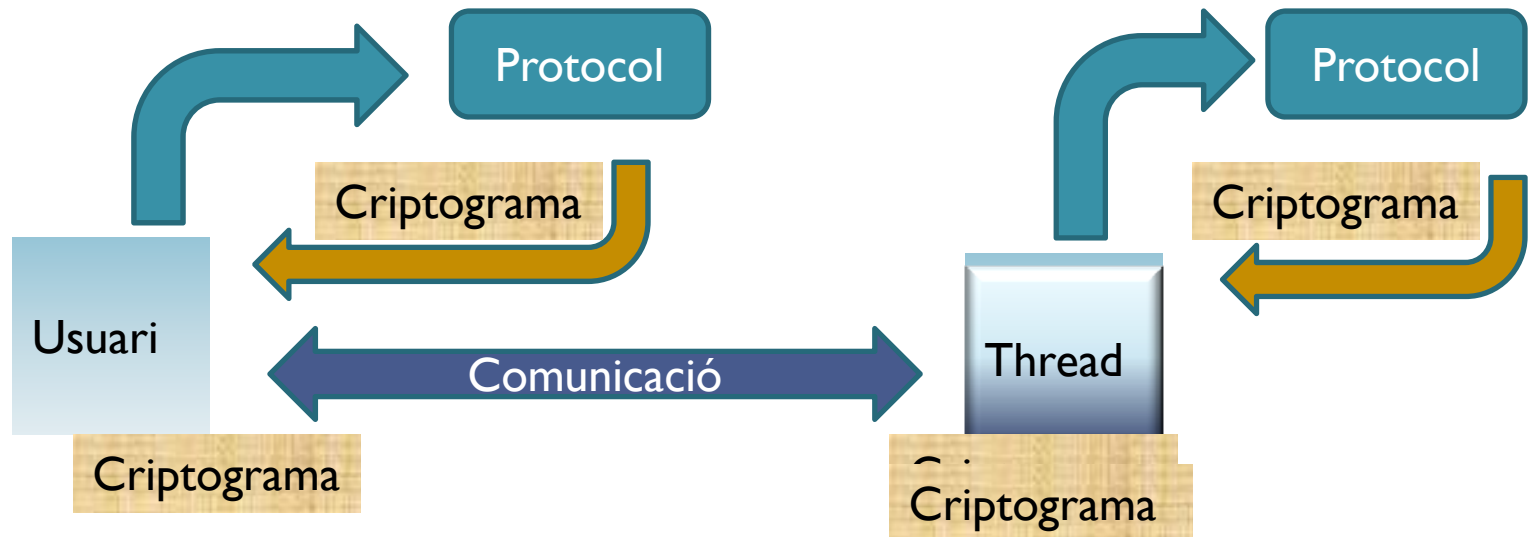
- **Protocols implementats**
 - Consulta de les dades generals d'un pacient
 - Consulta d'una visita d'un pacient
 - Consulta dels pacients assignats a un metge
 - Afegir una visita a l'historial mèdic d'un pacient
- **Autenticació contra el gestor**

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:

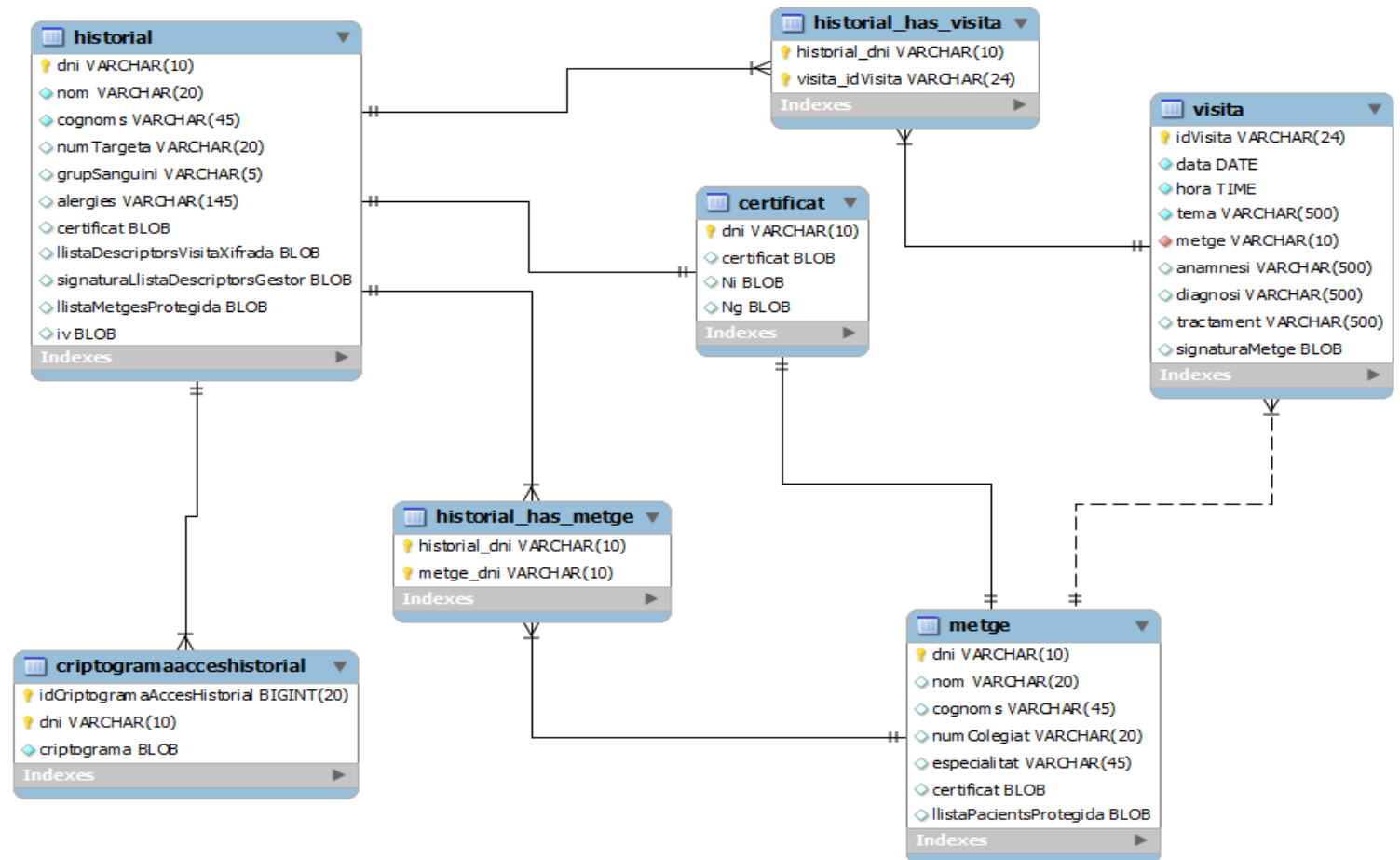


Gestió de la informació: BD

- 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

Client

Accions Configuració

Configuració client

Servidor 192.168.1.151 Port 1234

Password P12 *****

Certificat C:\provar iak\metge.crt ...

Fitxer P12 C:\provar iak\metge.p12 ...

Certificat Gestor C:\provar iak - copia\gestor.crt ...

Acceptar

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

Consulta dades Generals

Consulta visita

Nom Fortià Cognoms Bofill Espada DNI 00000001-B

Num. Targeta 1233242 Grup sanguini B

Alergies cap

Id	Data	Hora	Tema	Metge
PJlcJ6A7GC9+Rxhwp5CGx...	13/01/2011	09:31:09	revisió cardíaca	00000002-C
Q+Y/msJSZ8a9kxHHRtHef...	13/01/2011	09:33:03	prova d'esforç	00000002-C
e5FmoH++OA+EWc18vWhh...	13/01/2011	11:25:45	prova esforç	00000002-C
P6QO/ay50ni3GhrpEf8UPg==	13/01/2011	11:30:39		00000002-C
uxKdgDaEQugC5DwumOC...	13/01/2011	11:33:52		00000002-C

Interfície gràfica (client)

- Consulta d'una visita

Client

Accions Configuració

Consulta dades Generals

Data	13/01/2011	Hora	09:31:09	Metge	00000002-C
Tema	revisió cardíaca				
Anamnesi	no té antecedents				
Diagnosi	No presenta cap alteració rítmica				
Tractament	cap				

Tornar

- Llistar els pacients d'un metge

Client

Accions Configuració

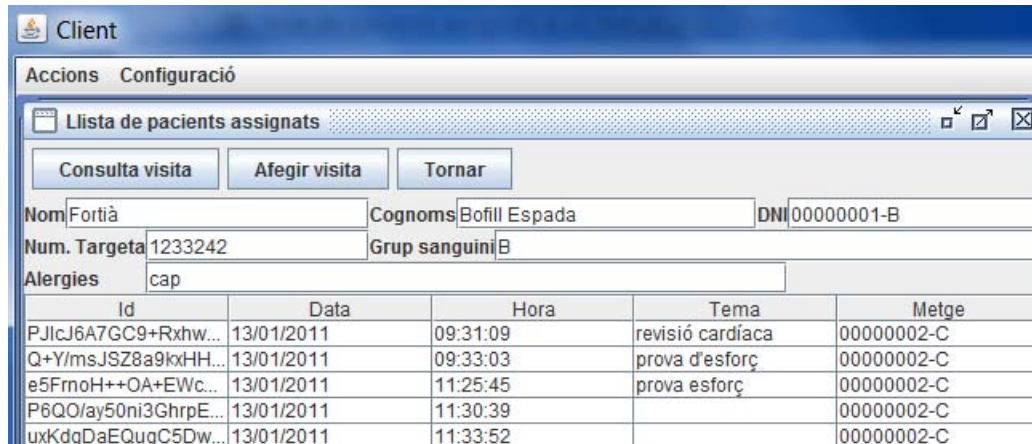
Llista de pacients assignats

Consulta dades generals del pacient

DNI
00000001-B
58243567-D

Interfície gràfica (client)

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



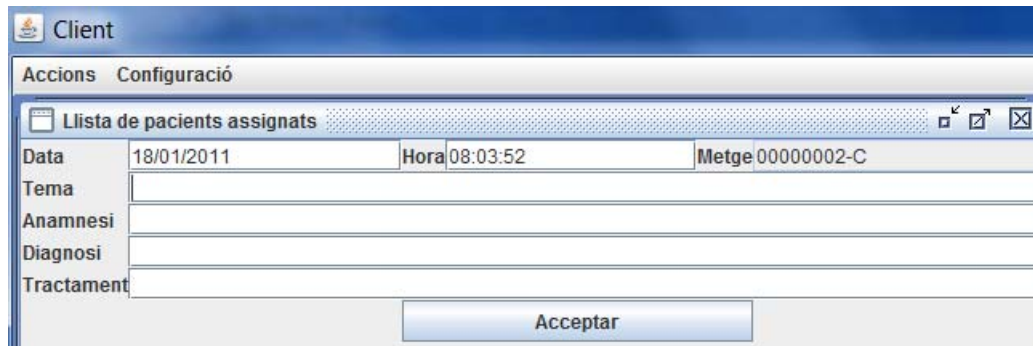
The screenshot shows the 'Client' application window with a menu bar containing 'Accions' and 'Configuració'. Below the menu is a title bar for 'Llista de pacients assignats'. There are three buttons: 'Consulta visita', 'Afegir visita', and 'Tornar'. The patient information is displayed in a form with the following fields:

Nom	Fortià	Cognoms	Bofill Espada	DNI	00000001-B
Num. Targeta	1233242	Grup sanguini	B		
Alergies	cap				

Below the form is a table with the following columns: Id, Data, Hora, Tema, and Metge.

Id	Data	Hora	Tema	Metge
PJlcJ6A7GC9+Rxhw...	13/01/2011	09:31:09	revisió cardíaca	00000002-C
Q+Y/msJSZ8a9kxHH...	13/01/2011	09:33:03	prova d'esforç	00000002-C
e5FmoH++OA+EWc...	13/01/2011	11:25:45	prova esforç	00000002-C
P6QO/ay50ni3GhrpE...	13/01/2011	11:30:39		00000002-C
uxKdgDaEQugC5Dw...	13/01/2011	11:33:52		00000002-C

- Afegir visita a un pacient del metge



The screenshot shows the 'Client' application window with a menu bar containing 'Accions' and 'Configuració'. Below the menu is a title bar for 'Llista de pacients assignats'. The form for adding a visit is displayed with the following fields:

Data	18/01/2011	Hora	08:03:52	Metge	00000002-C
Tema					
Anamnesi					
Diagnosi					
Tractament					

At the bottom of the form is an 'Acceptar' button.

Interfície gràfica (servidor)

- Servidor (gestor)
 - Configuració del servidor

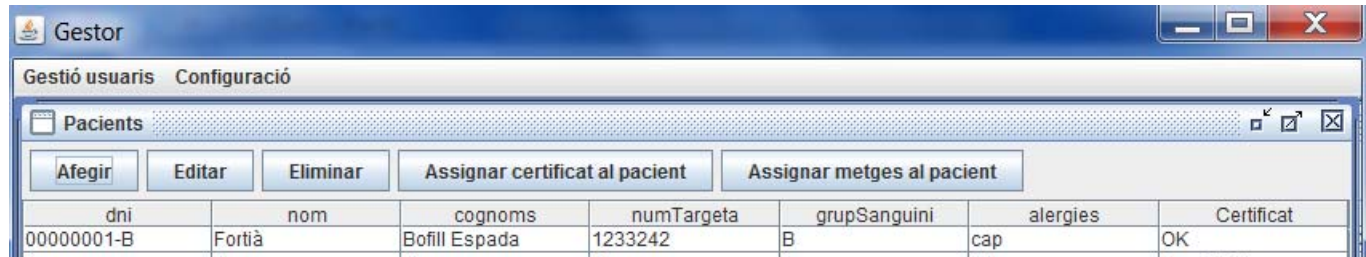


- Gestió dels metges

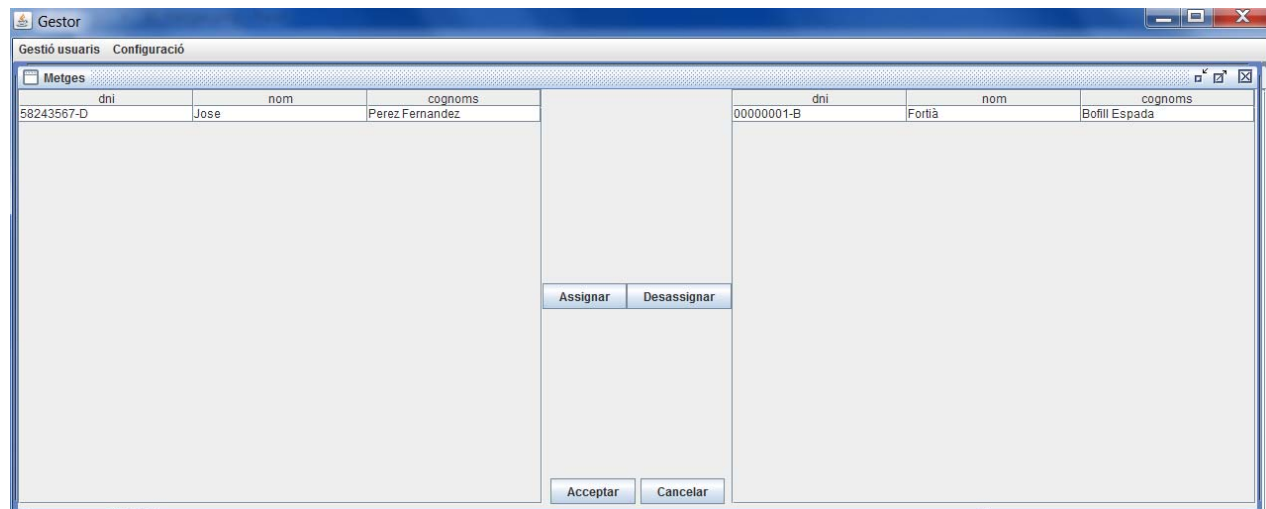


Interfície gràfica (servidor)

- Gestió dels pacients

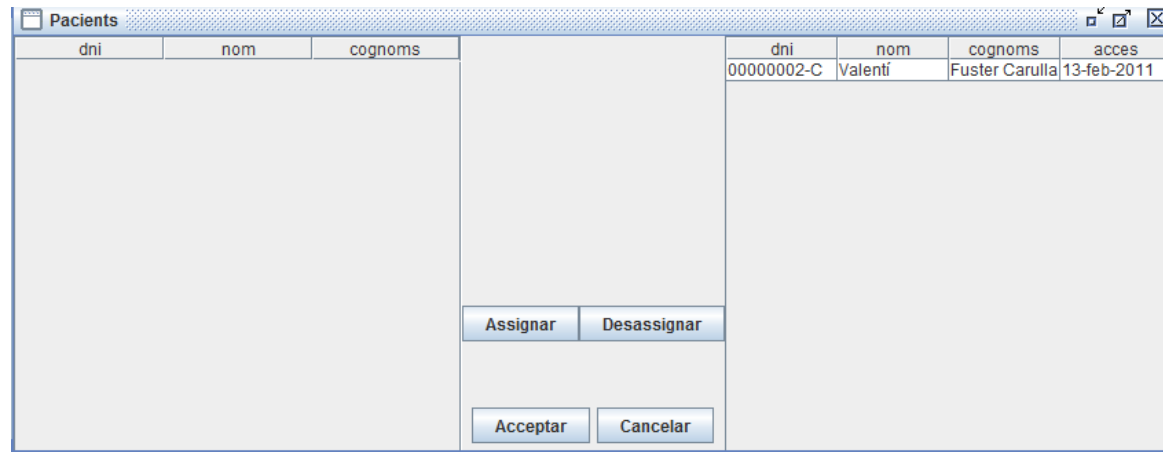


- Assignar pacients al metge

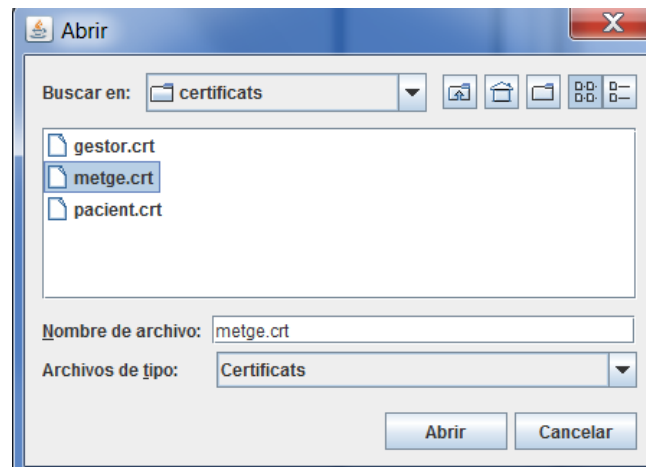


Interfície gràfica (servidor)

- 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