

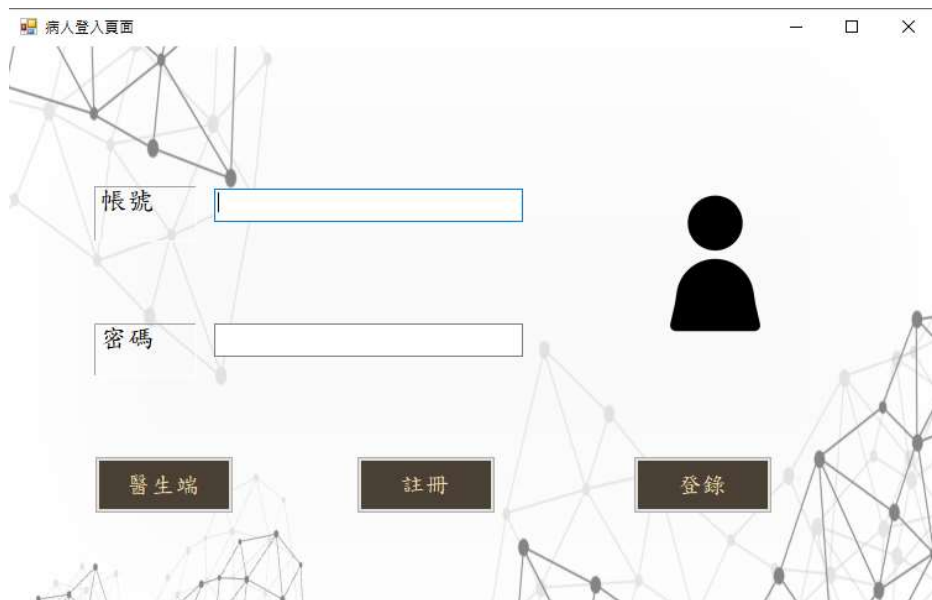
3.4 使用工具

1. PUF 程式碼:C#
2. Server 端程式碼:C#
3. 資料庫:Visual Studio SQL
4. 使用者介面:使用 C# Windows Form 來進行開發，並連接 Visual Studio 的資料庫

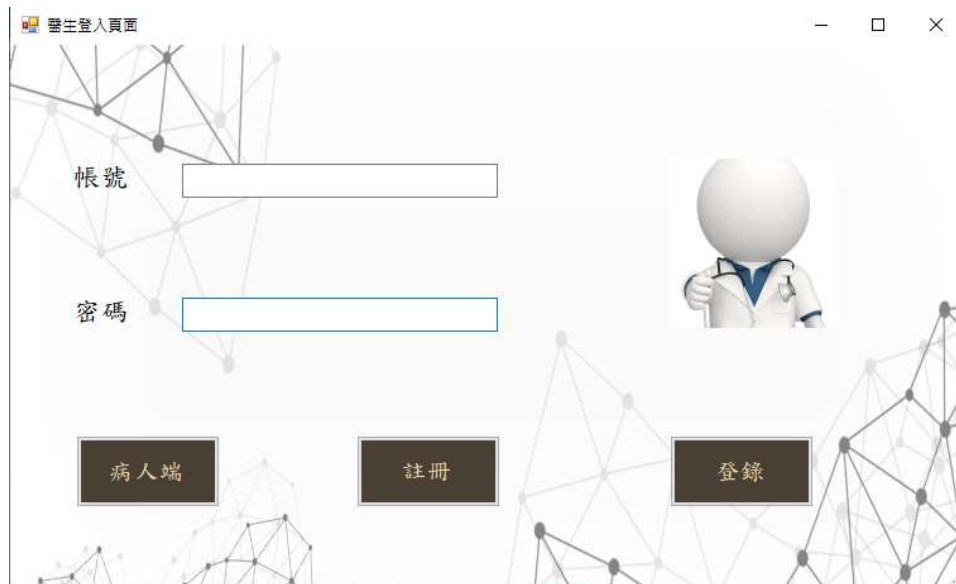
3.5 執行畫面

1. 登入頁面

輸入帳號、密碼，驗證成功後，進入身分驗證頁面。



圖十三病人端



圖十四 醫生端

1. 身分驗證頁面

- (1) MCS 的驗證碼:是本次驗證要計算的驗證碼，收到時要使用 Share Key 做 XOR 解密，在執行 PUF 計算，算出要驗證的驗證碼和下次做認證的驗證碼
- (2) 這次認證的 PUF:是這次要傳送給 MCS 的驗證碼
- (3) 下次認證的 PUF:是下一次要做登入認證時要傳送的驗證碼，透過 hash 雜湊後，傳給 MCS 儲存，做下次驗證答案使用。



圖十五 身分驗證頁面

2. 主要操作頁面

2-1 病歷讀取

醫生端

- (1) 向病人要求病歷資料:醫生要使用病歷時，使用此功能，向病人請求授權病歷。
- (2) 查看病歷內容:當病人同意授權此病歷時，可以在此查看病歷內容。
- (3) 新增病歷:在此做新增的功能
- (4) 緊急清況讀取病歷:當病人因故無法授權病歷時，透過此功能，緊急讀取病歷資料。



圖十六 醫生端基本頁面

病人端

- (1) 接收醫生端通知:當醫生請求讀取病歷與新增病歷授權時，病人會在此處接收通知。
- (2) 向 MCS 授權認可病歷:當病人要同意(拒絕)授權，在此處做授權處理。



圖十七 病人端基本頁面

3. 醫生請求讀取病歷流程

醫生端

當醫生向病人要求病歷資料，輸入病人的編號，並搜尋該病人的病歷編號，透過傳送向 MCS 發出授權請求。



圖十八 醫生端:向病人要求病歷資料頁面

病人端：

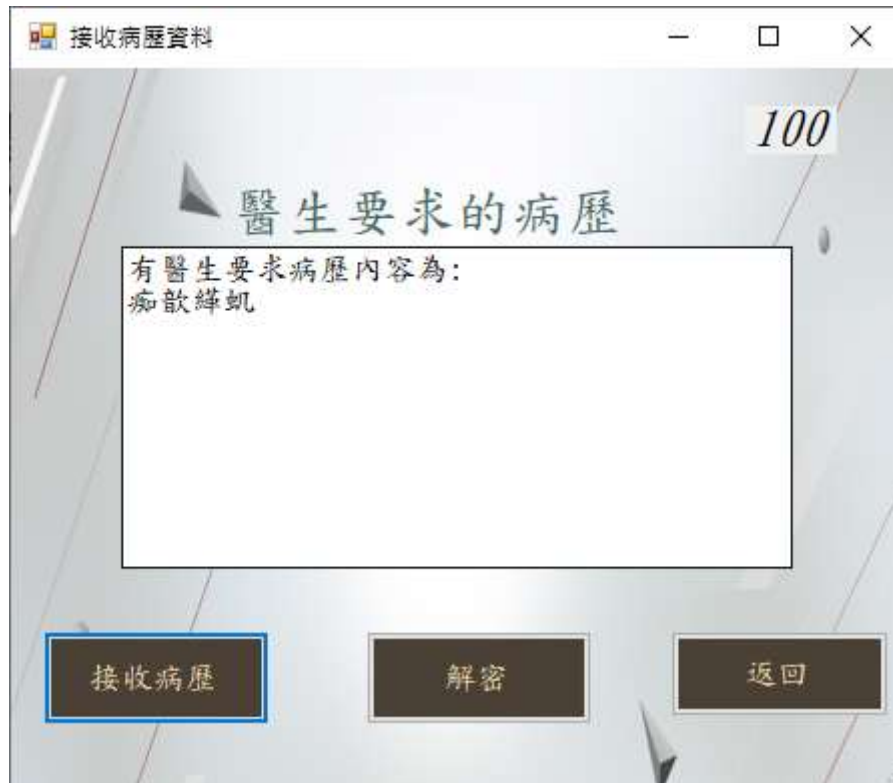
此時病人端接收醫生通知時，進行病歷的使用授權，並回傳給MCS。



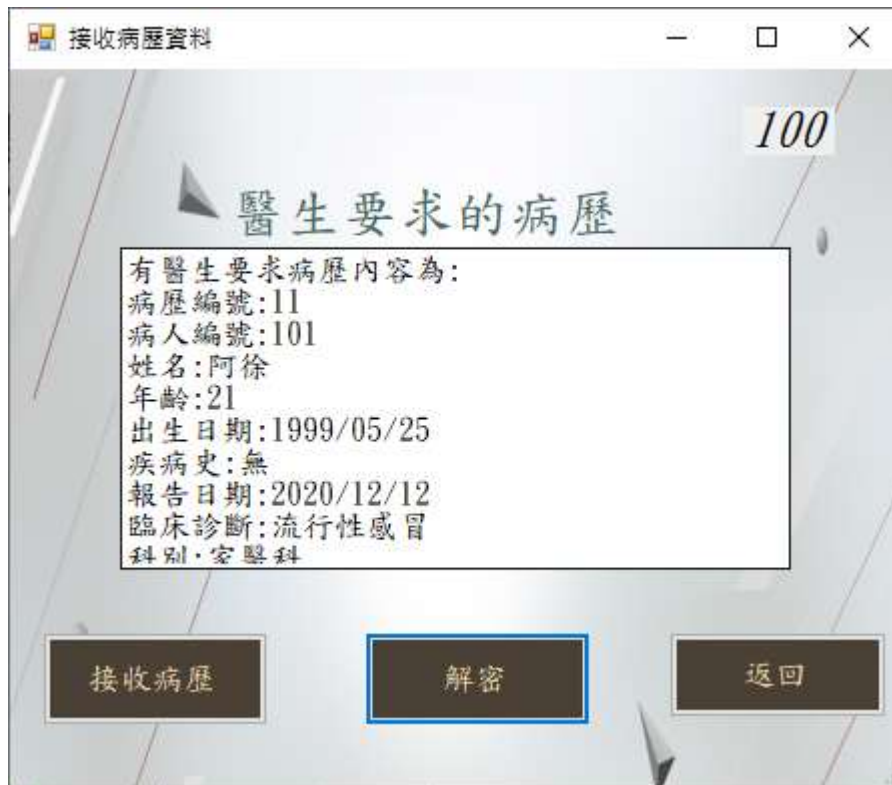
圖十九 病人端:授權病歷頁面

醫生端

病人同意病歷授權後，MCS 就會把醫生要求的病歷，以 Session Key 加密傳送給醫生，這時醫生就能用登入時算出的 Session Key 解密，取得病歷資料。



圖二十 醫生端：查看病歷內容(加密的病歷)



圖二十一 醫生端:查看病歷內容(解密後的病歷)

2-2 新增病歷

醫生端

當醫生要新增病歷時，請求病人端授權，並把病歷資料傳送給MCS，存進資料庫當中。

新增病歷

新增病人資料

病人編號: 101

要求授權

查看授權結果

授權結果:

病人同意新增病歷

病人姓名: 阿徐

性別: Man

出生日期: 1999/05/25

年齡: 21

疾病史: 無

臨床診斷: 流行性感冒

科別: 家醫科

報告日期: 2020/12/12

加入

取消

圖二十二 醫生端:新增病歷頁面

病人端

收到新增通知，進行病歷的新增授權，並回傳給 MCS。

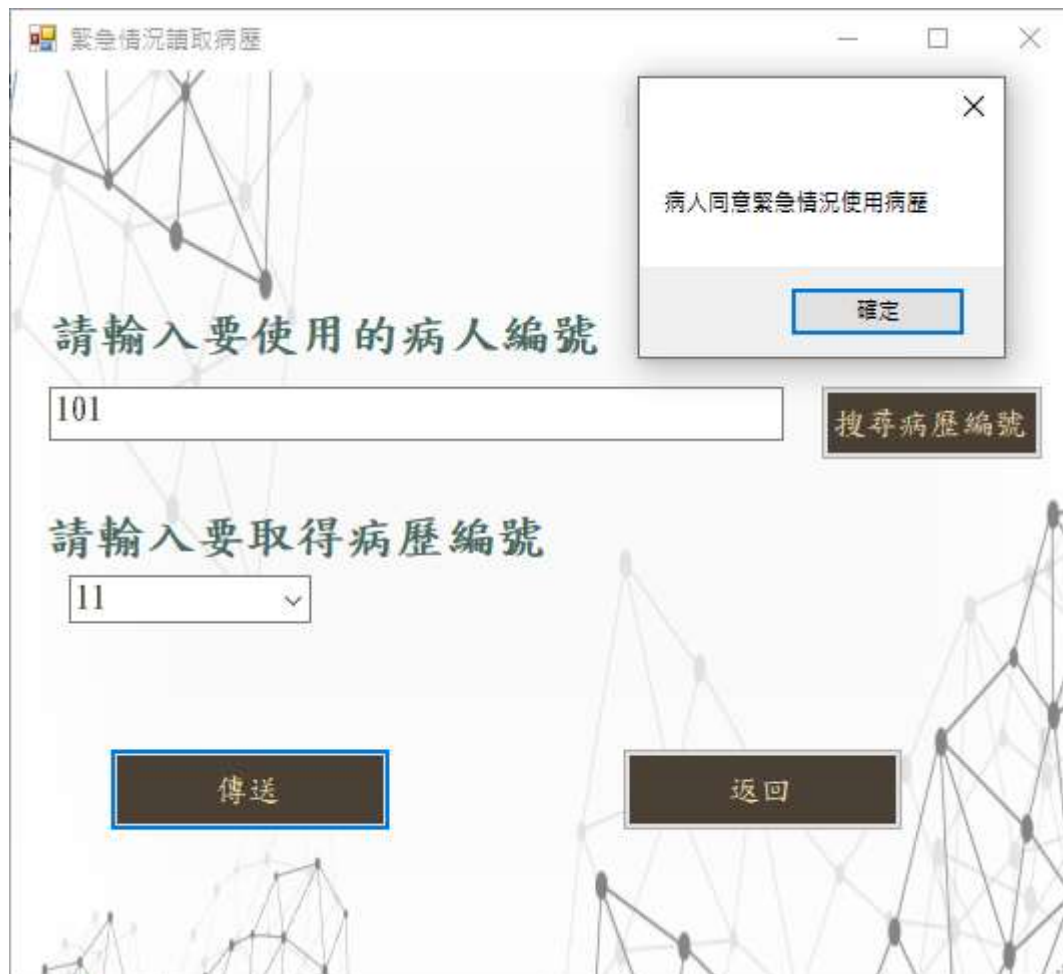


圖二十三 病人端:授權病歷頁面

3-3 緊急情況

醫生端

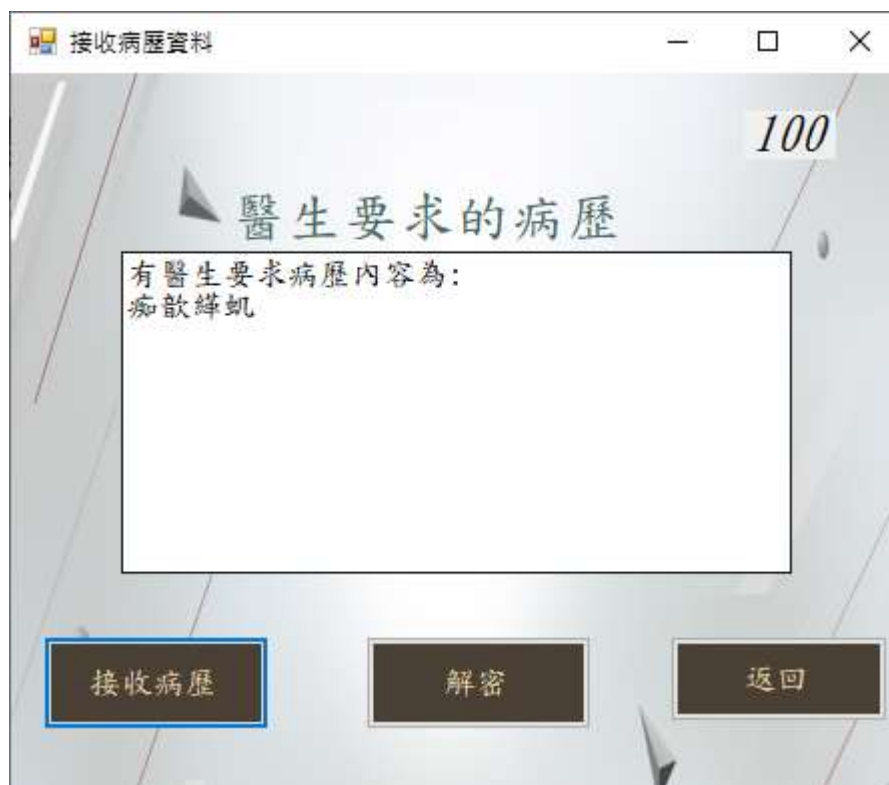
當病人無法授權時，醫生進入緊急情況頁面向 MCS，進行病歷的讀取請求。



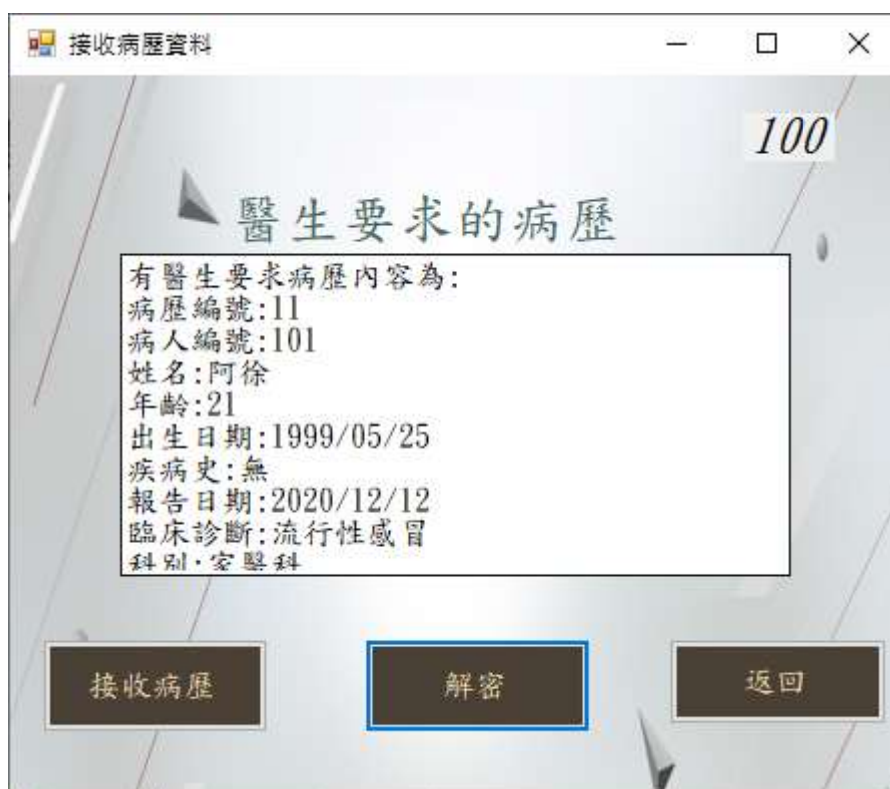
圖二十四 醫生端：緊急情況讀取病歷

醫生端

MCS 把病歷資料加密後，傳送給醫生。



圖二十五 醫生端:查看病歷內容(加密的病歷)



圖二十六 醫生端:查看病歷內容(解密後的病歷)