行政院國家科學委員會專題研究計畫成果報告

Java Card 在醫療資訊管理之應用

Java Card Applications in Healthcare Industry

計畫編號：NSC 89-2213-E-004-015-
執行期限：89 年 8 月 1 日至 90 年 7 月 31 日

主持人：廖文宏　國立政治大學資訊科學系
計畫參與人員：鍾文欽 蘇家樟　國立政治大學資訊科學系

一、中文摘要

本計劃之主軸乃針對醫學資訊（Medical Informatics）學門中與醫療管理相關之部分，探討 Java 智慧卡可能扮演的角色與其在實際應用上之妥適性。

Java 卡是可執行利用 Java 程式語言撰寫之應用程式(applet) 的智慧卡，具有跨平台、一卡多用、發卡後可再更新內容、物件導向架構等特點;因為 Java 卡具備高度的彈性，可伴隨需求之改變作即時的更新，在目前醫療保健自動化處理的長程規劃尚未有具體輪廓之際, 以 Java 卡技術為基礎的解決方案，可說是一個風險較低的選擇。

本計劃採用 Schlumberger 公司出品的 Cyberflex Access 卡及其提供的軟體發展環境(SDK)，參照衛生署健保局相關規定與醫療院所需求，對 Java 卡作為單純的健保卡，逐漸擴充為緊急醫療資訊卡，醫院病歷卡，以至於健康護照，其相關的資料格式訂定，資料的隱私性(privacy)，保密性(confidentiality)與安全性(security)，卡片功能調整的難易程度，需求功能個人化的可行性等課題作深入探討，盼能對目前正積極推行中的健保 IC 卡建置計劃提供具體並及時的建議。

關鍵詞：醫學資訊、健保 IC 卡、Java 卡平台

Abstract

This research investigates the potential application of Java cards to the healthcare information management system.

Java cards are smart cards with the capability to run programs (or *applets*) written in Java. These cards are designed to be platform-independent; multiple applets can coexist on a single card, and post-issuance of application is possible. Java card uses the latest object-oriented technology and is internet-ready. These features make Java card an ideal candidate for implementing a powerful, yet flexible solution when the long-term strategy for universal health care information system is still under development and subject to constant revision.

We employ the Cyberflex Access card and the associated software development kit (SDK) developed by Schlumberger Ltd. to study how Java cards can to be used as a simple insurance card that contains only ID and policy, or as a universal health passport that contains comprehensive medical and insurance information. We have examined critical issues such as the data format requirement, privacy, confidentiality and security of the medical record, incorporation of personalized service, and cost/efficiency of the overall system.

Keywords: Medical Informatics, Healthcare ID Card, Java Card Platform

二、緣由與目的

行政院研考會曾於 1998 年推動「國民身分健保合一智慧卡」專案，後雖因種種因素而暫緩實施，但衡諸網路與資訊技術之快速發展，電子商務軟體與硬體環境的日臻成熟，與未來電子化政府之必然趨勢，智慧型 IC 卡的應用必將日漸普及，含有身分辨識驗證功能的智慧卡，在 911 恐怖行動發生後更是格外受矚目。

衛生署中央健保局於民國 89 年發佈了『健保 IC 卡實施計畫』，民國 90 年與東

元電機簽約，預計在民國 92 年起以 IC 卡取代現行的健保紙卡[1]。由於此種大規模的智慧卡應用在國內乃屬首見，在系統建置過程中勢必有許多問題浮現並待解決，有鑑於此，本研究將針對 Java 智慧卡在醫療資訊與健保業務的相關應用，作廣泛而務實的探討。

三、Java Card 技術探討

常見的卡片式資料儲存裝置有三種:磁卡,memory 卡與 microprocessor 卡[2]。傳統的磁卡儲存的是靜態資料，功能單一且易於被偽造或破解。相對而言，memory 卡儲存的是動態資料(資料內容可隨時更新)、 靜態應用程式(在卡片製作時即需決定功能),雖彈性較磁卡高但仍有明顯限制，而新型的 Java 智慧卡因為內建了計算功能(8 or 16 bits CPU, 1-7.5MHz clock rate)，因此可儲存動態資料與動態應用程式(Java applets for smart cards, 又稱 cardlets [3])，卡片功能可視需求隨時做調整，同時內建 DES, 3DES, RSA 等密碼防護機制，使敏感資料不易外洩，符合健保 IC 卡的諸多要求。

由昇陽公司主導的 Java Card 平台最新的版本為 2.1.1[1] ,一個完整的 Java 卡平台包含三大部分[4]:

1. Java Card Virtual Machine(JCVM): Java 語言及 virtual machine 中與的智慧卡應用相關的子集合。
2. Java Card Runtime Environment (JCRE):定義程式執行相關之行為模式,如記憶體管理, cardlet 管理等。
3. Java Card Application Programming Interface (API):Java card 應用程式發展介面。

以 Schlumberger Cyberflex Access 卡為例，ROM size= 24KB, RAM size= 1KB, EEPROM size =16KB [5], 計算資源可說極為有限, 在此狀況下一方面要提供 Java card 系統基本功能,另一方面又要儲存資料及應用程式,因此記憶體的妥善使用成為首要考量,把 Java 卡當成儲存大筆資料或資料庫的想法在目前而言並不切實際[6]。

[1] 2001 年 10 月止, http://java.sun.com/javacard

衛生署中央健保局目前已定案的卡片內容中，分為四大資料段[7]：

1. 基本資料段：包含卡片序號、姓名、性別、出生日期、身分證號、相片等
2. 健保資料段：包含保險對象身分別、就醫次數、門住診費用、部分負擔費用、重大傷病註記、預防保健等。
3. 醫療專區:包含慢性病處方箋、用藥、檢查等。
4. 衛生行政專區：包含預防接種、器官捐贈註記等。

其中基本資料段與健保資料段為必要內容,而醫療與衛生行政專區則保留作未來使用,此一規劃明顯將健保卡定位為單純的健康保險識別專用證件,也就是側重於利用智慧卡資料存取的安全機制,這樣的做法在重大政策之推行初期不失為一控制風險的良策,不過 Java 卡的特點,尤其是運算的能力,並未在此應用中被突顯出來,此外,規格書中定義的 16K 位元組 EEPROM (或 Flash memory)空間已經有 12K 保留給資料區段,意味著即使未來有「一卡多用途」的計劃,其拓展的空間也十分有限,特別是加入身分辨識功能的想法可能難以達成[8],此項限制值得吾人重視。

為建立主機端(host)應用系統與驗證跨平台應用之可行性,本研究參考健保局制定的規格,實作了一個健康護照及管理系統的雛形,其中主要工作項目包含了:

- 應用程式發展平台架構之建立:建立一套以 Windows 作業系統為主的發展環境;另建立一套以 Linux 作業系統為主的發展環境，以驗證 Java 卡跨平台的特性，並比較此二種平台建置所需成本與開發環境的使用難易程度。
- Cardlet 的編寫與實際運作:每個 Cardlet 約佔用 800 Bytes-1000 Bytes, 因此可容納的應用程式數目以不超過十個為限。
- 各獨立 Cardlet 之間溝通之機制: 由於每個 cardlet 內都可能儲存高度敏感之機密資料,如電子現金餘額,指紋特徵或密碼等,因此資料之存取動作需作區隔, Java 卡內建 applet firewall 之功能來處理這類的問題,至於 cardlet

資料分享的功能(基本資料如姓名,性別等應可被許多 cardlet 分享) 則由 shareable interface object (SIO) 支援。

- Java Card 提供的 Application Programming Interface(API)集合標準 Java API 集合之比較:受限於計算資源與能力, Java 卡支援的資料型態只有最基本的 `boolean`, `byte` 與 `short`,而 Java Card API 所包含核心部分的 `java.lang`, `javacard.framework` 與 `javacard.security` 及延伸部分的 `javacardx.crypto`, 都是十分精簡的套件(package), 只涵蓋 Java 提供的一小部分功能,所以某些操作,如作浮點運算(如 Body Mass Index, BMI 值)時難以獲得高精確度之結果。
- Java 卡的安全性: JCRE 是一個單緒(single thread) 的執行環境,同一時間只容許一項應用程式執行,此外, 載入資料或應用程式之程序為 transactional, 載入過程若發生錯誤(如停電,意外將卡抽出卡機等),則卡片內容自動回復至前次修改時的狀態,以確保資料的完整性與安全性。
- Java 卡的密碼機制:提供 coprocessor 處理與密碼相關之運算[9],如 3DES, DES, RSA, 並內建 message digest (MD5) , random data, signature 等功能以保證資料與程式的可靠度,另外也可透過密碼機制與 cardlet 配合進行:
  -資料存取權限的彈性調整
  -敏感資料被存取或更動的紀錄(log)

四、結果與討論

本研究使用 Schlumberger Cyberflex Access 卡及軟體發展工具,實作了一個健康護照及管理系統的雛形[10],此一系統包含了前後端兩大部分,其主要功能說明如下:

一. 前端介面 Public Terminal (PT)
PT 包含讀卡機，以及 PT 主程式，分為兩種，一種提供一般民眾者使用(user PT)，可以放置於公共場所，一種提供管理者(醫療院所)使用(administrator PT)，可以更新卡內的資料。

A、 user PT 功能
(1) 提供個人基本資料的查詢,對於某些基本資料也可以提供自行更新修正的功能，如身高體重等。但某些敏感資料則需由 administrator 來修改，如特殊身份的認定。另外可查閱就醫紀錄或最近資料修改日期/項目等。
(2) 與 application cardlet 配合提供特殊功能:如健康體重的提醒,幼兒預防接種的提醒孕婦應注意健康資訊,慢性病患者的生活諮詢等。
(3) 提供最新健康資訊:這部份可以隔離 java card 來實作，也就是不需要將卡插入 PT 即可以得到資訊，如健康新聞，保健資訊。方法即實作一個類似 IE 的簡化瀏覽器，整合至 Terminal 中。

B、 administrator PT
(1) 更新 java card 中的資料：提供管理者介面。
(2) download 新版或新功能的 cardlet 至 java card 中。
(3) 傳送 APDU data, 與 Admin 互動。
(4) 提供 Converter，將使用者的.class 檔轉換成.bin，給 PT 讀取。

二. 後端 Cardlet
分為儲存純資料的 data cardlet 以及提供特殊功能的 application cardlet，並且透過 PIN 碼及編碼來加強安全性及隱密性。

A、Data cardlet
(1) 存放個人資料：血型、性別、姓名、身分證字號、出生日期、年齡、身高、體重、特殊身分(以代號來代表幼兒，孕婦，慢性病患者等特殊身分)。
(2) 提供個人資料：將個人資料封裝在 java card 中, 必須透過 PIN 碼認證機制才能讀取卡中的資料，PIN 碼認證分為兩層兩個 PIN 碼，第一層只提供資料的讀取但不能修改，通過第二層 pin 碼認證始可更新卡中的資料。

B、Application cardlet
以特定功能為導向來編寫的應用程式，依照應用程式的不同，可以由使用者自行下載至 card 中，或是必須由系統管理者來提供下載的功能。可能

的選擇有以下幾項:

1．健康體重的提醒
2．幼兒預防接種的提醒
3．孕婦應注意健康資訊
4．婦女保健資訊(子宮頸抹片檢查，乳癌檢查)
5．慢性病患者的生活諮詢
6．提醒 40 歲以上(或適當年齡)的成年人定期做健康檢查，並且可以紀錄每次檢查時間
7．在緊急狀況下(如車禍)使用的 cardlet，紀錄必要資訊(過敏藥物)
8．提供健康指標

以上項目實作的基本方式是由 cardlet 自行判斷使用者狀態，並且回傳給 PT 作顯示。在本研究中因為受限於記憶體空間,因此僅擇其中數項作概念之展示。

三. cardlet 的安全機制

1.使用 java card class library 所提供的 security 來做安全的防護。
2.配合 PT 使用 DES 對資料傳輸做加解密。

有關於跨平台發展工具之研究,由於未來的個人健康管理系統，很可能如現今的提款機（ATM）那般四處林立,以方便民眾隨時查詢其健康狀態[11]。提供此類服務的公共終端機其作業系統應符合成本低廉，運作穩定且適合作嵌入式的設計等條件，以目前市面上所提供的可能選擇,非 Linux 莫屬。在 Linux 上發展 Java card applet 的方式有兩種,一是使用昇陽公司的 Java card development kit, 另一種是使用製卡公司 Schlumberger 推出的 Cyberflex for Linux Starter's Kit 2.1。

一. Sun Java Card Development Kit:目前 Sun 提供 Java Card 的 package 最新版本為 2.1.2, 裡面包裝了許多有用的工具。

1. javacard 與 javacardx 等撰寫 Cardlet 的必備套件。
2. jcwde：用來模擬一台 Card Reader，讓我們跟虛擬的 CardReader 溝通介面。
3. capgen：Cardlet 產生器，搭配 export file 便可將自己寫的 Cardlet application 轉換成 Card Reader 可以辨識的格式。

二. Schlumberger 提供的開發套件可至 http://www.citi.umich.edu/projects/smartcard/cyberflex_starter/ 免費下載,然而其更新速度緩慢, 較 Windows 發展環境受重視的程度顯然有別。

本計劃執行過程出現以下問題,值得提出探討:

- 卡片內建之安全機制導致鎖卡(lock)之情形產生,必須將卡送回原廠才能重新設定使用。
- 在資料存取過程中將卡片抽出讀卡機仍可能造成卡片之損壞,此問題之嚴重性應再加以評估。
- SDK 相容性:Schlumberger 提供的 SDK (3c, Revision 1) 與 Sun Java Card Platform 2.1.1 並不完全相容,若干 package 之 class 名稱相同,但實際功能不同,易造成混淆,需特別留意。

五、計畫成果自評

本研究計劃實際執行之內容與原計劃所提大致相符,除執行初期因須向國外採購 Java 卡與發展環境造成些許延誤,以及測試過程中因故毀損若干卡片而需再行購買補充,與 SDK 相容問題導致編譯錯誤外,其餘研發過程尚稱順利。

本研究獲致的成果將可提供給醫療保健之相關決策單位，作為訂定政策或選擇系統時的重要參考依據,同時也一併探討了下列重要課題:

1. 對於醫學資訊所需之隱私性(privacy),保密性(confidentiality)與安全性(security)等問題有進一步之瞭解。
2. 組裝系統與使用 Java 卡軟體發展環境之經驗可延伸套用於電子商務，網路交易認證之應用。
3. 對於 Java 卡在醫學資訊系統中所扮演的角色有進一步之認識。

參與本項研究之工作人員獲得以下之訓練:

1. 了解智慧卡之基本結構及其在各國之應用現況及未來發展遠景。
2. 深入了解 Java Card 2.1.1 Platform 的架構及提供的 API。
3. 學習建立跨平台的 Java 卡開發環境（含 Windows 與 Linux 作業系統)。

4. 學習利用 SDK 發展跨平台之應用程式(cardlets) 。
5. 學習利用 Java 卡提供個人化之服務(personalized services)。

六、參考文獻

1. 『健保 IC 卡實施計畫』,衛生署中央健保局, 1999 年 12 月。(參閱 http://www.doh.gov.tw 網站文件)
2. Smart cards: A primer, Rinaldo Di Giorgio, Java World, December 1997.
3. Java Card Technology for Smart Cards, Zhiqun Chen, Addison-Wesley, 2000.
4. Java 2.1.1 Platform Specification, http://java.sun.com/products/javacard, Sun Microsystems, Inc.
5. Schlumberger Cyberflex Access Programmer's Guide, Schlumberger Ltd.,可連接至: http://www.cyberflex.slb.com/Support/support.html 下載
6. "Patient Health Record on a Smart Card" , A. Naszlady and J. Naszlady, International Journal of Medical Informatics, Vol. 48, 191-194, 1998.
7. 健保 IC 卡宣導網站, http://www.enhi.com.tw
8. Biometrics, Personal Identification in Networked Society, Anil Jain, Ruud Bolle, Sharath Pankanti, MacMillan Technical Publisher, 1999.
9. Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Edition, by Bruce Schneier, John Wiley & Sons, 1995.
10. "WWW+smart card: towards a mobile health care management system", A. Chan, International Journal of Medical Informatics, Vol. 57, Issue: 2-3, pp. 127 – 137, July 2000.
11. Java cards in healthcare industry, W. Liao, Proceedings of Medical Informatics Symposium in Taiwan, Oct. 1999.

行政院國家科學委員會補助專題研究計畫成果報告

※※※※※※※※※※※※※※※※※※※※※※※※※

Java Card 在醫療資訊管理之應用

※※※※※※※※※※※※※※※※※※※※※※※※※

計畫類別：■個別型計畫　　□整合型計畫

計畫編號：NSC　89－2213－E－004－015－

執行期間：　89 年　8　月　1 日至　90　年　7 月　31　日

計畫主持人：廖文宏

計畫參與人員：鍾文欽　蘇家樟

本成果報告包括以下應繳交之附件：

□赴國外出差或研習心得報告一份

□赴大陸地區出差或研習心得報告一份

□出席國際學術會議心得報告及發表之論文各一份

□國際合作研究計畫國外研究報告書一份

執行單位：國立政治大學資訊科學系

中　華　民　國　　90　年　10　　月　20　　日