IC卡系統設計與應用心得報告

主講人: 侯廷偉 教授
系級: 資科研一
學號:92753036
報告撰寫人: 陳文婷

30.9.2003

健保 IC 卡在全國各地的推廣與使用, 引起社會大衆熱烈的討論。有些人對於健保 IC 卡的安全性感到質疑; 在推行健保 IC 卡的同時, 也有民衆對於此舉將侵犯個人隱私權提出抗議。到底健保 IC 卡是什麼樣的一張卡? IC卡有哪些種類? 對於其安全性有又什麼樣的設計與保護? 主講人侯教授提出了深入淺出的介紹, 並且以在澎湖推行實驗健保 IC 卡五年的成功經驗, 來跟我們談 IC 卡的設計與應用。

1 演講摘要

從澎湖健保IC 卡的發展與推行, 侯教授從 IC 卡的技術與發展趨勢、IC 卡運作模式、澎湖健保 IC 卡資訊系統 運作架構, 以及中華民國國民健保卡簡介等五個方面來介紹 IC 卡的設計與應用。
首先, 我們知道構成卡片 的要素, 除了合乎 ISO 標準的塑膠材質以外, 還要含有記憶體、邏輯控制單元, 甚或是微處理器的晶片, 以及與 外界溝通的介面。此外,IC 卡的相關硬體設備裡, 需要有相容的讀卡機、以及資料儲存的系統, 並且提供相關 的作業系統。而 IC 卡的相關規格標準, 主要是符合 ISO7816和 ISO14443。

對於 IC 卡的基本分類, 若以是否含有 CPU 來區分,IC 卡主要分爲兩種:Memory Card, 和 SmartCard 兩類。以讀取資料時, 是否與讀卡機接觸與否來區分, 則可分爲非接觸式卡和接觸式卡。非接觸式卡, 例如: 捷運的 悠遊卡; 接觸式卡片, 則如健保 IC 卡、IC 電話卡等。此外, 二合一型複合式 IC 卡 (2 in 1 IC Card) , 可以結合 接觸式 IC 卡與非接觸式 IC 卡的結構特性於單一卡上, 讓使用者可以同使享受兩種卡

片設計的優點。

IC 卡有其生命週期, 所謂的生命週期, 是指從 IC 卡的晶片設計、作業系統的設計, 設計其卡體與線圈, 並 將 IC 晶片放入卡體, 接著將作業系統燒入晶片之中, 隨之將個人資料初始化, 實行開卡的動作就可以使用了。若不再使用卡片, 則進行關閉使用應用程式的步驟, 此 IC 卡的生命週期就此結束。

IC 卡在目前世界各地的應用範圍很廣, 在美國、法國、德國, 中國大陸等國家, 都有許多應用的實例。舉例來說, 像是中國大陸的自動加油管理 IC 卡系統, 在顧客每次加油的時候就可以刷 IC 加油卡, 指定加油的 金額與油量, 全國各地的加油站都可以連線取得加油消費的資料, 減少許多加油業者感到困擾的人爲弊端。此外, 校園中所使用的學生智慧卡, 可以便利於圖書館流通借閱的使用。還有像是: 酒店管理系統方案、電話管理系統、電子錢包系統、健保系統、非接觸 IC 卡考勤管理系統等 (惠光科技,2000), 生活中的應用 不勝枚舉。

在世界各地,IC 卡的使用漸漸成爲一種趨勢的同時, 在台灣, 侯教授以澎湖的健保 IC 卡實施經驗, 提出 了幾項問題提供大家思考。在澎湖實施的時候, 曾發現以下問題: 多卡、換卡、中斷健保、以及醫療資源浪 費和醫療詐欺等問題。健保 IC 卡的實施, 主要是想藉由 IC 卡的安全、快速, 並且電腦化後資料可流通的特性 與優點, 期望可以藉此控制監督全國醫療資源的使用, 減少醫療資源的浪費與詐欺事件。但是在實行的過程 中, 技術的部分其實大致已經可以提供安全、保密, 以及便利的服務功能, 主要的問題還是在於人。人如何 去利用 IC 卡, 才是大家產生爭議的焦點。然而, 對於 IC 卡的設計與應用, 我們仍然保持樂觀的態度, 期望國 內能夠不斷提昇自己的技術, 運用 IC 卡的種種優點, 在生活各個層面提供更爲安全便利的服務。

2 要點整理

對於IC 卡的設計, 整理要點如下:
1.IC卡的構成要素:
IC卡構成的要素, 主要有符合 ISO 標準之塑膠卡片、一個由微處理器或記憶體與控制邏輯所組合而成的晶片（ IC CHIP), 以及可提供與外界通訊的介面。

2.IC卡的特點: 具運算機能、高安全性、記憶容量大、攜帶方便。

3.IC卡與磁卡的比較如下:
a.抗破壞性: 磁卡的特點具有在遇到磁場、扭傷、刮傷等情形下, 存在裡面的資料容易遺失的缺點, 且壽命較短; 但 IC 卡抗上述破壞的能力強, 壽命也長。
b.儲存資料的容量與靈活性: 磁卡能夠儲存資料少,IC 卡儲存容量高。在資料的修改上,IC 卡便於修改資料。
c.加密性: 磁卡的加密性很低, 容易遭到複製造成損失;IC 卡具有 CPU 和邏輯電路, 加密性高, 並且可以加入許多 加密演算法, 不易被複製。

4.IC卡的生命週期 (ISO10202-1):
其生命週期, 主要是由五個步驟所完成。第一個步驟, 是卡片晶片的設計、卡體的製作, 以及卡片作業系統設計。第二步驟, 燒錄卡片作業系統於晶片上, 完成作業系統設定。第三步驟, 規劃卡片應用程式, 完成個人資料初始 化。第四步驟, 是啓用卡片。第五步驟, 則是關閉卡片的使用, 例如: 關閉某個應用程式。

5.ISO7816和 ISO14443:
這兩項標準, 是侯教授在演講時最強調的兩種標準。對於 ISO7816的標準, 教授列出了四項 主要的區分:
ISO7816-1: 物理性質的標準, 如: 紫外線容許度、電氣阻抗、靜電、熱擴散、電磁場、及彎曲、扭曲等之測試。老師演講時, 曾舉例播放一段影片, 影片中呈現的, 是成功大學正在對 Java Card 進行摩擦測試。目的在測出該 IC 卡 所能承受的摩擦次數, 是否符合此一標準。
ISO7816-2: 規範了卡片金屬接點的尺寸與規格。
ISO7816-3: 電器信號和傳輸規約如: 使用接點、卡片運作程序、卡片與介面設備之傳輸方式、回應重置信號 (Answer To Reset) 等。
ISO7816-4: 規範相容性的指令與回應。
ISO14443的標準, 是一種非接觸卡, 可以在0 10cm 的距離中被讀取。它在生活應用的實際例子如: 悠遊卡。

6.EEPROM:
侯教授的演講資料中, 有一項要提升爲128KB 的 EEPROM, 並曾表示 EEPROM 會影響 IC 卡資料運算的速度。EEPROM Electrically Erasable Programmable ROM。電流可消除可程式唯讀記憶體。EEPROM 必須用電壓才能更改資料。可用在存放電腦的 BIOS, 早期 BIOS 修改的機會不多, 但近年來 BIOS 經常更新, 在方便性考量下, 已逐漸被 Flash(快閃記憶體) 所取代, 因此,EEPROM 朝往通訊用途發展, 如用於大哥大手機, 在此我們則看到它被使用 在 IC 卡的設計上。

3 評論

對於健保IC 卡的全國推行與實施, 國內學者莊庭瑞 (民國 91) 在自由時報的自由論壇中曾提出數點質疑。該 學者認爲, 目前台灣的全民健保屬於強制性保險, 民衆在這次的 IC 卡推行使用推行過程中, 並沒有發言的餘地, 有損民衆投保時的權利。健保 IC 卡的目的在於可將被保險人的就診紀錄, 記載於卡片的 IC, 希望藉此達到控管 醫療資源的使用。然而, 健保紙卡的設計早已可以達到此一要求, 並沒有必要花費龐大經費推行健保 IC 卡。此 外, 更質疑健保 IC 卡的功能會帶來民衆在就業時的權益損傷。根據侯教授的介紹, 健保 IC 卡中具有幾個項目內 容: 個人基本資料檔、健保業務資料檔和其他資料檔。這樣的內容, 其實已經超出當初健保 IC 卡用來控管醫療 資源的出發點。若有企業主在聘僱人員時, 透過管道調出該應徵者的健保資料, 可以藉此不聘請某些人, 傷害 民衆工作權。舉例來說, 若有位婦女應徵工作前, 曾有去過婦產科的就醫記錄, 企業主可能推測該女性爲孕婦, 於是不聘請該名婦女。然而, 該婦女還尙且不知是由於健保就醫記錄外洩所致。

對於這樣的質疑, 其實我個人也有相同的疑問。就技術層面上, 確實 IC 卡的設計已漸趨成熟, 安全性也日益加 強。但對於個人的隱私權, 確實有所疑慮。主要的問題, 已經不在於技術、機器的發展, 還是在於人對於相關 資料的取得與使用, 是否會傷害到民衆的權益。就以侯教授所舉的例子: 美國退伍軍人協會, 預計在2002年以 含有 IC 晶片的多用途智慧卡取代以往的磁卡、凸字和條碼, 也利於網路互動資料傳送。由於 IC 智慧卡具備許多 功能, 內可儲存的資料, 不是退伍軍人可自己決定的, 極可能退伍軍人正隨時受到政府的監控, 個人隱私權也 將受損。因此, 若 IC 卡的使用, 晶片中可以存取的資料範圍應由政府立法規範, 將可一定程度地減低個人資料 被濫用的風險。若能將 IC 卡用以結合多種功能, 於生活中使用, 但個人資料是有法令限制的登錄項目, 將可結 合 IC 卡的便利性、安全性、耐用性等優點, 民衆出門也不需要帶一堆卡。舉例來說: 若將 IC 卡設計具有交通費 收取、電話費收取、停車費收取、過路費收費, 以及圖書館借閱等功能, 卡片中只記錄民衆的姓名、性別、身 份證字號和聯絡電話等, 受限制但可供識別的的個人基本資料項目, 民衆就不需要擔心重要資料外洩, 而且一卡在手行遍各地的便利服務。

IC卡資料的安全性, 也是民衆所關心的問題。民衆深怕 IC 卡所儲存資料, 被不法人士所複製盜取。關於這一點, 從侯教授的演說中, 我想是可以放心的。因爲 IC 卡本身的設計中, 就有對於保密的相關設計。此外, 在 IC 卡的 相關設備中, 讀卡機也設有安全模組。當讀卡機遭到拆解的時候, 配有自動銷毀設計, 或者是 IC 卡與讀卡機設備 相配合的自動銷毀設計。因此, 對於報紙上民衆曾提出: 若有其他廠商提供相容性讀卡機, 但品質較差, 醫療院 所若採用其他廠商之讀卡機, 是否自己的 IC 晶片卡會被盜取資料呢? 然而侯教授也提到, 若非健保單位所提供之 讀卡機, 則讀卡機無法通過密

碼的驗證, 無法讀取其資料, 所以能夠克服此疑慮。

不過, 我個人還有一個顧慮, 就是醫療系統的安全問題。若健保 IC 卡的設計、讀卡機的設計等, 雖已達到我們所 需要的安全標準, 但若有心人士從醫療網路系統、主機中直接進行盜取密碼, 或者病毒的散佈等相關破壞行爲, 那麼個人的重要資料和醫療資料, 是否仍然有外洩的顧慮? 對於承包 IC 卡設計和讀卡機設計的廠商, 政府是否有 相關的管制和輔導措施? 我想這是我們接下來所要關心、解決的問題之一。技術層面的問題, 往往容易克服; 但 與人相關的問題, 卻總是困難重重。期待台灣對於與 IC 卡有關的政策、法律規範都能夠跟上技術發展的脚步。

4 參考文獻

1. JavaCardSecurityWhitePaper
http://java.sun.com/products/javacard/JavaCardSecurityWhitePaper.pdf/
2. Java.iso7816API
http://www.citi.umich.edu/projects/smartcard/JavaCard/sld012.htm
3. 莊庭瑞 (民國91年)。從健保 IC 卡談個人資料保護。自由時報—自由廣場。
http://www.tahr.org.tw/pada/Juang.htm/
4. 智能卡知識介紹。
http://www.fairkong.com/fkick1.htm/
5. 電子/儲存媒體。
http://www.moneydj.com/z/glossary/glexp2629.asp.htm