演講主題與摘要:

主題:IC 卡系統設計與應用
主講人: 國立成功大學工程科學系 侯廷偉教授

摘要:

此次演講內容第一部份主要著眼於 IC 卡的基本介紹、歷史演進、IC 卡的構成、IC 卡的特性、生命週期、種類及卡片安全技術等做一些基本的介紹, 第二部份則以其所負責的澎湖健保 IC 卡爲例, 說明一個 IC 卡系統要能夠使用, 從發卡到一張卡片使用結束, 其中各種工作的實行情況。包括讀卡機、卡片上的作業系統、電腦上的應用程式、整個系統的通訊網路、資料的處理換卡機制等等。做一些說明 及其中種種工作所遇到的困難和問題的解決等。

要點整理:

- IC 卡簡介與歷史發展: IC 卡是一張像名片一般大小的卡片, 上面貼一小張 IC 晶片, 達到記憶、識別、加解密及傳輸等功 能。這些塑膠卡片不是隨便的卡片, 它是符合 ISO 標準的塑膠卡, 嵌入的 IC 晶片則內含微處理器或 記憶體與控制邏輯, 另外還得有一個可提供與外界通訊的介面。雖然早在1968年, 德國發明家 Jurgen Dethloff 和 Helmut Grotrupp 就提出了將積體電路加入身份識別卡中的想法, 但直至1974年整個智慧卡的實際運作概念才由法國人 Roland Moreno 提出, 第一張的 IC 卡也是由法國人製出。

- IC 卡的構成: IC 卡的構成主要有三, 符合 ISO 標準之塑膠卡片、微處理器 (8051) 或記憶體與控制邏輯所組合而 成的晶片 (IC Chip)、以及一個與外界通訊的介面。

  1. 塑膠卡片: 此爲 IC 卡的基本外形所在, 規格爲85.60mm x 53.98mm x 0.80mm 與一般信用卡大小致相同。塑膠卡片的主要功能爲保護卡上的晶片, 提升使用者攜帶的便利性。
  2. IC Chip: 晶片包含了微處理器 (Central Processor Unit,CPU)、唯讀記憶體 (Read Only Memory,ROM)、隨機在取記憶體 (Random Access Memory,RAM) 及 可覆寫可程式化的唯讀記憶體 (Electronic Erasable Programmable ROM,EFPROM)。

     (a) CPU: 通常是一顆8051晶片。

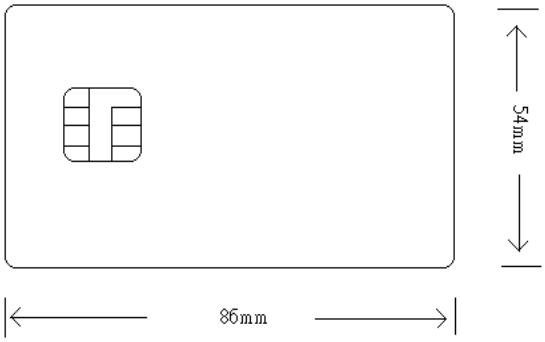


Figure 1: IC卡外觀

(b) ROM: 儲存控制及安全程式。

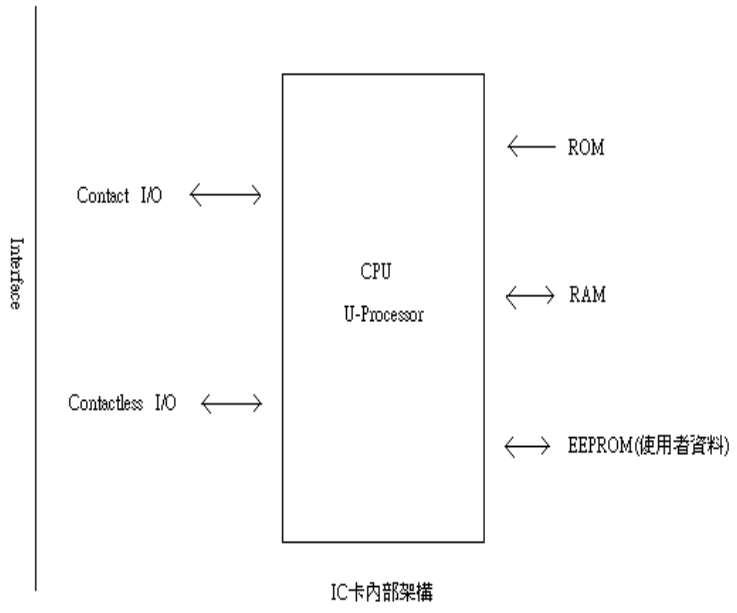
(c) RAM: 處理運算及控制邏輯。

(d) EEPROM: 資料記錄區, 可利用電流改寫資料。

3. 外界通訊介面: 分爲六個接點和八個接點兩種, 根據 ISO 7816/2(接觸式), 智慧卡晶片上提供了八個接觸點, 如下圖所示:

- IC 卡生命週期: 可分爲五個階段。

1. 製造階段: 此階段的製程序包含了 IC 半導體設計及軟體設計程序、IC 製造程序、IC 裝配程序及 IC 嵌入程序。
2. 預備階段: 包含了卡片的個人化 (Card Personalization) 及公用資料檔之啓動 (Common Data File Activation)。
3. 資料檔預備階段:
   (a) 應用資料的配置。
   (b) 應用資料個人化。
   (c) 應用資料啓動。
4. 使用階段: 此階段是持卡者正常使用卡片的階段, 此階段可以行使的功能包含了卡片的使用、應用系統的使用及邏輯檔案的存取控制。



IC卡內部架構

5. 結束階段: 在此階段中, 所終止的部份包含了卡片和內部資料及 Key 的終止。

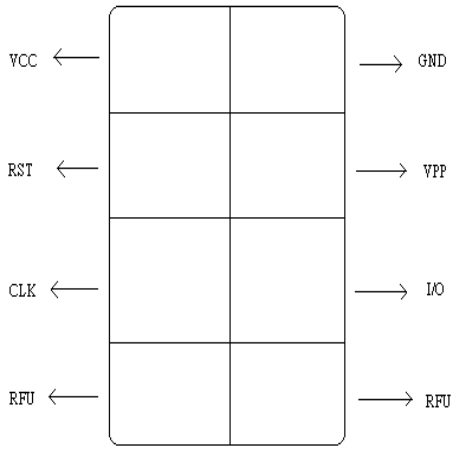
- IC 卡的種類: 就用途來分:

  1. Memory Card: 包含邏輯電路與記憶體, 如一般的預付卡、電話卡、識別證等。
  2. Smart Card: 由微電腦和記憶體組成, 例如金融卡、信用卡、健保卡等。

  就使用方式來分:

  1. 接觸式 (Contact Card)
  2. 非接觸式 (Contactless Card)

- IC 卡特性:



晶片接腳圖

1. 記憶容量大: IC 卡的記憶容量可達64Kbit(約8,000字), 可反覆讀寫, 具連線及離雙重處理能力, 可成爲手攜式資料庫, 儲存大量同性質應用資料, 使用彈性大, 具有發展爲多目的、多功 能卡的潛力。
2. 安全性高: 此特點爲 IC 卡優於其它媒介的主要原因之一。IC 卡的安全保護具有好幾層, 卡片眞僞辨認 (Authentication)、持卡人 (Identification)、資料存取安全 (Secure Read/Write)、資料傳輸安全 (Encryption) 以及交易認證 (Certification)。透過多層的安全保護措施, 使得 IC 卡被僞造的機率極低。充份維持資料隱私, 避免誤用及竄改, 更可防止同張卡片上之不同應用領域間的資料的不當修改。
3. 具有邏輯運算及控管能力: 透過卡內之微處理機功 能及邏輯處理電路的應用,IC 卡能對記憶體資料設定各種不同的取用控制, 針對不同的使用者對 IC 卡內部不同的資料, 給予不同的取用或寫入權限; 並能根據內部預設之邏輯, 來判斷允許外部系統介入的層次, 例如連線交易。

- 澎湖健保卡介紹: 以侯教授實際負責實做的澎湖地區健保卡實驗爲例, 指出實際在使用 IC 卡時, 除了發卡之外, 其相對應的讀卡機系統、網路、資料管理、安全機制、配套措施等。都是很煩瑣且不易爲。因此從剛開始的規劃一直到最後使用及管理階段, 侯教授及其他參與人員幾乎大部份的工作都接手處理過。最後實驗結果顯示澎湖地區民衆對健保 IC 卡的接受度尙算良好。

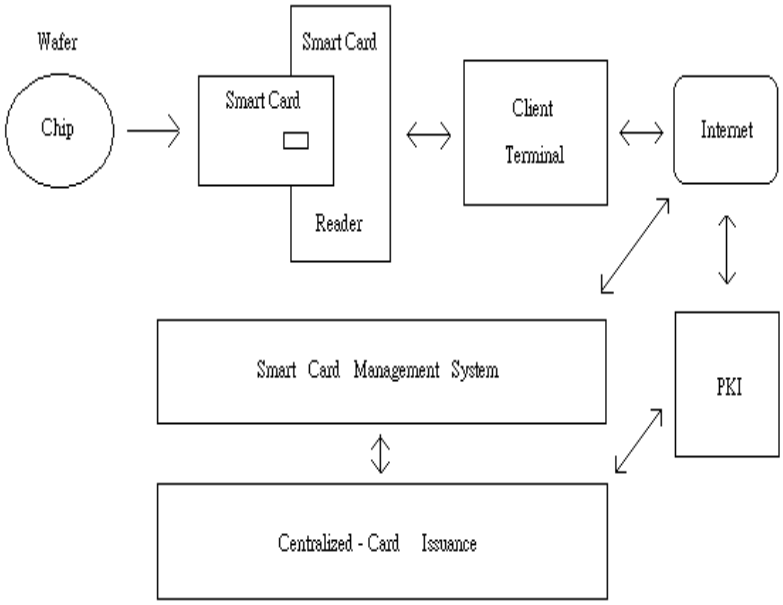


Figure 2: IC卡的運作

評論:

這次侯教授的演講對第一部份 IC 卡的介紹只算是基本中的基本, 對像我這種之前完全對 IC 卡沒概念的人而言, 雖然教授對於一些相關的技術因爲多種因素 (如商業機密) 並未詳細介紹, 且對一般非專業人員而言, 一些專有名辭及規格只聽個名字並沒什麼意義, 不過至少聽完後知道要使用一張方便的 IC 卡, 背後是很多辛苦的工作所組成的, 也大致了解 IC 卡的組成。基於上述原因, 在這個部份我並不想對一些相關技術或研究作深入的探討, 而是著眼於一般 IC 卡最爲人所垢病的地方, 即有關資料保密、資料安全和操作的穩定性方面, 對教授有介紹到的部份做一些想法和看法的說明。在侯教授所講的澎湖健保 IC 卡實驗中, 可以看到幾個問題, 包括讀卡機操作的不穩定性, 健保卡使用連線穩定性問題, 以及個人隱私資料外洩問題等。從問題的嚴重性來看, 根據台灣人權促進會的報告–

> 台灣目前個人資料外洩事件頻傳, 其中不少顯示了公部門對個人資料保護漫不經心的態度, 例如財政部爲最大股東的財金公司140萬筆個人資料遭到竊盜、花蓮縣「地價稅繳稅通知單」寄發未加封套, 納稅人身分證字號等資料全部「露餡」、國立屏東科技大學擅自將8000多筆師生資料交給銀行辦卡、警官自2000年即涉嫌盜賣民衆資料給徵信等。」

可以看見資料外洩的情況是非常嚴重, 且通常會在不經意間或有心人刻意而爲之下外洩, 雖然目前的健保在初期只記錄一些所謂的"基本資料", 但健保 IC 卡發卡前後, 行政機關對個人資料保全問題並未進行客觀討論, 只一味強調其採先進防僞技術。健保被保人無權選擇只顯示繳交保費紀錄與就診次數的紙卡, 均被迫使用 IC 卡, 承受個人資料外洩、隱私遭公開的風險, 其後果是小則難避免垃圾資訊與強迫推銷, 大則個人保險與工作權將因雇主、保險業者獲悉個人就醫紀錄與病史, 遭到極大衝擊。

> 『事實上, 媒體亦報導健保 IC 卡承包商東元電機 本已將提供健保 IC 卡登載民衆健康資料提供給保險公司列入其衍生計畫, 計畫五年獲得八十億元收益, 但因民間反彈不見得能落實計畫。』

政府發卡決定草率, 卡片未全面上路, 就出現製卡延遲、讀卡機卡住卡片、甚至試辦開始, 澎湖民衆仍對讀卡機判讀不穩抱怨頻頻的一籮筐問題; 試用 IC 卡的18家醫療院所一起連線取得健保局開機認證就要花100秒, 已有業者指出未來全台所有醫院診所同時開機認證, 網路塞車將嚴重影響就診者權益。再者, 根據侯教授的說法, 在澎湖實驗健保 IC 卡的期間, 發生了像讀卡機製造商停產, 由學術界的實驗團隊接手的情事, 雖說現今的承包廠商屬大型企業, 但是仍不能保證一定不會發生類似情事, 萬一不只是讀卡機停產的問題, 再外加其它如連線設備問題, 軟體問題等等, 我想這些問題沒有一個人敢說是有萬全準備的吧。撇開操作層面的問題, 從另一個角度來看, 假設將來健保 IC 卡並不會加入其他一些隱密資料, 而是維持今日的形式, 那我不禁要問, 爲何不維持紙卡形式, 而要花大筆公帑換成 IC 卡,

> 『中研院學者曾以專業建議以10.3億元成本改良現行紙卡, 毋需大費周章發行健保 IC 卡, 即可確認保費繳納、稽核醫療院所支出, 且其每年控制醫療資源浪費與醫療院所浮報效益爲健保 IC 卡三倍。惟政府仍無視中央與健保財政虧損加劇, 執意於三年內耗資40億成本, 罔顧全民隱私與國安危機, 發行功 能並非不可取代且欠缺法源依據、只有廠商得利的昂貴掛號證。』

如若是打算以後擴增資料量, 製作成類似之前提的「國民卡」, 在九月十五日一篇中國時報的報導中指出,

> 『行政院研考會昨日再度重申國民卡以「保護民衆隱私」、「 保障系統安全」及「尊重民衆選擇」爲最優先原則。在現有法律授權及安全技術許

可下, 以循序漸進方式推動, 並從技術、法制、管理及作業層面建立完整的「資訊安全機制」, 強化民衆的信心。』

我認爲政府單位的說法仍是太過於理想化, 就如侯教授所說, 很多時候即便是技術再完美, 仍沒辦法避開人的因素, 只要有人洩露, 不管意圖爲何, 大家就必須承擔一定的風險, 更何況世上是沒有所謂完美的技術。從目前各方面看到的消息來看, 政府推動健保 IC 卡, 並不單單只是想簡單的記錄一些基本資料, 而是想在往後推出功 能合一的 IC 卡, 就如前幾年所謂的國民卡, 但是世事難料, 誰也不敢確定到底會不會推行, 其實現在的情況就好像是商業界對消費者一樣, 政府就像是業者, 對自己的產品不斷的促銷, 保證自己產品的安全性, 以及使用的好處等等, 而一般大衆則像是消費者, 對 IC 卡這個新產品要多方考慮才決定購買與否。不過就我自己算是消費者一方而言, 存有許 多重要個人資料的 IC 卡, 在攜帶方便之外, 一定同時伴隨著風險集中的缺點, 一卡在手, 行遍天下, 但一卡遺失, 可能諸事皆廢。我個人比較同意侯教授的想法, 與其集多個功 能在一張卡上, 不如我有很多張卡, 而讀卡機卻能辨識這些不同種類的卡, 這樣子, 即便我丟了一張卡, 損失也相對的小, 也不會因爲這一張卡而使得一個人不能去做其它的事。但是大衆和一般消費者最大的差別是沒有選擇購買與否的權力, 只能被迫接受。雖然現在的健保 IC 卡只記錄基資料, 在一切運作正常的前提下, 的確會比較節省時間, 也比較方便, 不必帶一堆卡、手册之類的; 且政府的說法是若以後要加註其他資料, 會廣泛徵詢意見, 但是問題又回到前面所述, 所謂徵詢意見是誰的意見? 會否又跟現在一樣, 強迫大家接受。不過我個人到不是完全反對使用 IC 卡, 只是要看使用在什麼地方, 比如"悠遊卡"就是一種很方便的卡。看了這麼多的正反面意見, 我個人是比較反對 IC 卡記錄著太多個人資料, 不論它的用途爲何, 以學電腦資訊的人的角度去看, 我並不任爲現在的技術可以完全防止外洩的疑慮, 以後應該也不可能, 正是所謂「道高一尺, 魔高一丈」。

相關資料:

以下列出一些介紹內容比較多的網站，其他資料量比較少的網站就不列出:

IC卡介紹相關:
http://www.yfp.com.tw/ -----　永豐紙業
ttp://www.vcollege.org.tw/smartcity/collegeteach/card/pic/ic/ICMAIN.HTML ---IC卡教室
健保 IC 卡相關:
http://www.nhikb.gov.tw/-----　中央健保局高屏分局
ttp://www.enhi.com.tw/----　健保局 IC 卡宣導網站
ttp://members.tripod.com/jiuanyih-wu/krankenversicher.htm----德國健保卡的濫用問題與對策

ttp://jj.tmu.edu.tw/connection/iccard/page10091.html----健保 IC 卡導入資訊
IC卡相關問題:
http://www.tahr.org.tw/----　台灣人權促進會
ttp://www.wfdn.com.tw/ ----　人間福報
ttp://iwebs.url.com.tw/main/html/south/526.shtml ---- 智邦生活館@知識網