我放在電子票證中的錢，會不會被有心人士神不知鬼不覺地偷走？

電子票證的安全性議題

◎ 魯明德

壹、前言

很多讀者都有這樣的經驗：來到自動販賣機前，發現口袋沒有零錢，或者零錢不夠，只能望機興嘆；上了公車才發現沒有 15 元硬幣，只能在下車時忍痛丟下 100 元大鈔；到便利商店消費時，換來一大堆零錢不知如何處理。

各方都在研究解決這個議題，先是銀行推出電子錢包的方案，繼而由非金融業者的悠遊卡股份有限公司(以下簡稱悠遊卡公司)推出悠遊卡、某連鎖便利商店推出 i-cash 卡，目前已占有相當的市場。

立法院於民國 98 年 1 月 13 日三讀通過電子票證發行管理條例，未來只要經主管機關核准，資本額在新臺幣 3 億元以上的股份有限公司，即可發行電子票證，隨即有人開始討論電子票證的安全性問題。本文將從資訊安全的角度來探討電子票證的安全性議題及解決方案。

貳、電子票證的安全議題

不論是電子錢包，或是悠遊卡、i-cash 卡…，都是利用無線射頻辨識(Radio Frequency Identification, RFID)技術所發展出來的產品，它是利用讀卡機(Reader)發射射頻能量到電子標籤(Tag)，以辨識及讀取電子標籤上的資料。

電子票證常用的 RFID 多爲遠耦合系統(Remote Coupling System)，其操作頻率可在 135KHz 以下，或 6.75MHz、13.56MHz、27.125MHZ。悠遊卡公司使用 HID 公司的 MIFARE 智慧卡，其工作頻率亦爲 13.56MHz。

由於電子票證上所儲存的餘額，經過讀卡機時即會依實際消費金額被扣除，而這些交易都是透過無線電傳輸來進行；惟無線電所用的頻率既是已知，於是有人質疑：既然交易需透過無線電進行，則任何人都可以設法讀取此電波，進而破解其所傳送的資訊，甚至複製出儲值的晶片或加值的機器。這將衍生的問題是：我放在電子票證中的錢，會不會被有心人士神不知鬼不覺地偷走？

除了國內有人質疑 RFID 的安全性，國外甚至已有人破解電子票證。據 2007 年 11 月某國外雜誌報導，倫敦地鐵及荷蘭捷運所用的悠遊卡，即被荷蘭某大學生所破解，並已測試成功可在倫敦搭乘地鐵。

參、電子票證的安全機制

電子票證所用的載體─智慧卡(Smart Card)，可視爲一個 RFID 的標籤，除了天線(Antenna)外，它還包含：可收發 RF 訊號的類比電路(Analogue Circuitry)、具有微處理器的數位電路(Digital Circuitry)及記憶體(Memory)，其中記憶體又包含了可保存資料的記憶體(Non-Volatile Memory)EEPROM 或 Flash、唯讀記憶體(Read only Memory, ROM)、隨機存取記憶體(Random Access memory, RAM)。而我們所擔心的票證資料，則是存放在可保存資料的記憶體上。

爲了讓智慧卡在使用上增加其安全性，國際標準組織(International Organization for Standardization, ISO)對於非接觸式的智慧卡(Contactless Smart Card)，提出三種技術標準：ISO10536、ISO14443 及 ISO15693；由於 ISO14443 及 ISO15693 爲進階技術，因此，目前少有業者以 ISO10536 的標準開發產品。

在 ISO14443 及 ISO15693 的標準中，規範以 13.56MHz 爲操作頻率，允許使用者的資訊被寫入智慧卡的微晶片上，並具有安全功能。在安全功能上雖未定義一個標準的方式，但目前常用的安全機制有：資料加密標準(Data Encryption Standard, DES)、進階加密標準(Advanced Encryption Standard, AES)、3DES(Triple DES)、橢圓曲線加密演算法(Elliptic Curve Cryptography, ECC)…等。

在每張電子票證上都可置入一個私密金鑰(Private Key)，電子票證上所儲存的現金餘額資料，係經私密金鑰透過上述演算法加密後的資料，必須經過身分認證後才能存取，因此，可以確保電子票證上的餘額不被人隨便更改，即使被竊取也無法放在自己的電子票證上加值。

當電子票證被讀卡機讀取時，透過無線電傳輸的資料，也是一個加密過的資料，縱然中途被截取，亦屬讓人無法辨識的亂碼，沒有經過公開金鑰(Public Key)解碼的資料，是無法分辨其內容的。

肆、結論

電子票證的推出，使一般消費者在小額消費時的付款更加便利；然而，若沒有一個安全的機制以保護個人財產的安全，就無法讓使用者安心使用。由於電子票證發行管理條例已經三讀通過，未來電子票證將更普及，惟具有嚴密的安全機制，才能加速此一金融產品的流通。