

## RFID 創新應用之安全與隱私權議題探討

**苑梅俊**

美和技術學院資管系助理教授

X00002217@meiho.edu.tw

**林筱增**

美和技術學院資管系副教授

X00002108@meiho.edu.tw

### 摘要

RFID 所具有自動化處理及精確可靠的編碼方式，在許多應用領域提供了許多創新與革命性的發展潛力。其獨特的功能包括在遠處，即使視線被遮蔽且無電力供應狀況下，仍可獲得特定物體或品項內建的數據資料，以做為物品管制與身份辨識之用。RFID 的特有功能提供了新的物品管理方式，進一步與資訊系統結合後，在經營管理與企業創新上具有很大的發展能量來改變原有的企業型態。然而，近幾年 RFID 快速發展，逐步實現其潛在的應用時，必須在安全議題與隱私權議題上給予更多關注。

### Abstract

RFID possess accurate and reliable automated processing and encoding, in many applications to provide a number of innovative and revolutionary potential. Its unique features included in the distance, even if the sight of line is obscured and no power supply conditions can be read specific objects or items of data in order to control and identity purposes. RFID's unique capabilities provide a new management concept, and further combined with the information systems in business management and innovation has a lot of ability to change the traditional type of enterprises. However, in recent years the rapid development of RFID, the progressive realization of its potential

applications, security issues and privacy must give more attention to the issue.

**關鍵詞 ( Keywords ): RFID , 隱私權 , 資訊安全**

## **壹、前言**

雖然 RFID 是一項已有數十年歷史的舊有技術，但它所具有自動化處理及精確可靠的編碼方式，在許多應用領域提供了許多創新與革命性的發展潛力。其獨特的功能包括在遠處，即使視線被遮蔽且無電力供應狀況下，仍可獲得特定物體或品項內建的數據資料，以做為物品管制與身份辨識之用。RFID 的特有功能提供了新的物品管理方式，進一步與資訊系統結合後，在經營管理與企業創新上具有很大的發展能量來改變原有的企業型態。然而，近幾年 RFID 快速發展，逐步實現其潛在的應用時，必須在安全議題與隱私權議題上給予更多關注。

RFID (Radio Frequency Identification, RFID) 是一種無線識別技術，透過內嵌在商品上的「標籤」，可將資料與適當資訊系統連結，用以識別、追蹤與確認商品的狀態，「標籤」是一種內建無線電技術的微晶片，晶片中可存放一系列數據，它可以做到極其微小，並可以隨附於所要識別的各種型態的實體上，以非接觸的方式，快速且大量地讀寫其內容資料，大大地提高了商品管理效率及節省人力成本，比目前條碼系統，具有更高效率與使用彈性。除了商品物流的管理，RFID 其他領域的應用亦非常廣泛，例如在藥品的管理上，美國食品及藥物管理局(FDA)採用 RFID，進行藥物的安全管理，以精簡藥物識別流程與防止冒牌的藥品。在醫院管理上，RFID 用以尋找與辨識病人，以減低醫療行為的誤失並提高醫療品

質。在 SARS 期間，工研院在新竹東元醫院中裝置 RFID 感應器，並且讓院內所有人都配戴 RFID 晶片的識別證，一旦查覺有人發病，就可以追蹤發病者和其活動路徑。除此之外，尚有動物晶片、農產品生產履歷、汽車晶片防盜器、門禁管制等典型應用，學童、行李、郵件、包裹、票券、停車場管制等亦可利用 RFID 以掌握其動向，配合 RFID 標籤價格之日益降低以及網路技術和資料庫功能的快速發展，RFID 應用已逐漸進入我們日常生活中的每一個角落。

由於 RFID 快速的發展，以及在各領域蓬勃的應用，相關安全上的議題也逐漸受到重視，依據歐洲「建構 RFID 通用環境(Building Radio frequency Identification for the Global Environment, BRIDGE)」計畫所提的「RFID 標籤白皮書」中指出，RFID 應用有三個重要的安全情境必須考慮。

- 一、當 RFID 應用在既有的作業流程時，由於 RFID 自動化辨識的特性，當人為錯誤產生時，其產生的風險與安全因素，將較傳統方式所產生的危害更大。
- 二、RFID 技術本身可能產生新的風險，有別於傳統條碼辨識，當 RFID 標籤被用於與資料安全的應用，例如票務，門禁管制和產品認證等領域。由於 RFID 的非接觸讀取的特性，在有效的反制技術尚未應用或是啟動前，非法的讀取者可能在未被發現前，即已造成傷害或是破壞。
- 三、RFID 是一個大量數據收集和自動處理的測量技術，它可以應用在新開發的領域，展現比以往更有效率的活動與精準的作為，但是，可靠性及安全

性問題，仍是在這些新開發的應用領域中，必須優先考量的。

從 BRIDGE 的安全研究小組觀點來看，必須確保 RFID 安全技術無虞的前提下，才能支持 RFID 技術應用在相關領域中。對於 RFID 應用的開發者而言，RFID 安全性不僅是必要的，它也是 RFID 技術開發者有力的競爭優勢。

在討論 RFID 安全問題的同時，另一個隱私權問題也必須一併討論，越來越多的民眾在享受 RFID 所帶來的便利時，常常不知道其個人資料，被有心人士或是無意地被流失出去。請想像一下以下情節：喜好精品的 A 君，為了購買名牌用品，長久以來入不敷出，被信用卡循環利息壓迫的變成標準卡奴，不幸地因為經濟不景氣，又被公司裁員，不得不靠著社會救助而過活。在歷經一段艱苦與心情低落日子後，所幸經一位律師朋友的協助，利用「消費者債務清理條例」與銀行協商後，獲得免除多數債務機會，讓他獲得略微喘息的機會而心情大好。某日在領到社會救濟金，於回家經過精品店時正好碰到折扣大促銷，勾起他壓抑已久的購買慾，依據卡債銀行協商的約定，A 君這段期間是不能購買奢侈品，但 A 君心想反正用現金，不會留下證據被發現，於是利用現金買了一個限量皮夾。在回家的公車上剛好坐在一位銀行債務催收人員的旁邊，他身上所攜帶具有 RFID 讀取器的手機，同時讀取到 A 君以前公司的 RFID 識別證以及新買限量皮夾的 RFID 識別碼，並將兩者關聯後，電腦系統推斷 A 君違反了債務協商的約定，開始追討被免除的卡債，他的社會救助也跟著被取消了。

雖然 RFID 廠商信誓旦旦說以上情節純屬虛構，但是 RFID 非接觸讀取是它

主要特性，如同現在網路交易業者口口聲聲的說，他們對於個人資料的安全措施多嚴密，但是個人資料流入詐騙集團手中的例子，已經多到上不了新聞版面，如何讓民眾相信廠商不會濫用 RFID 讀取個人隱私的片面之詞。

## 貳、RFID 技術簡介

RFID 可是說是一種舊的技術，最早的 RFID 應用大約是在第二次世界大戰末期，英軍應用這樣的設備來識別從戰場上飛回的飛機是友軍或敵機，也就是利用無線電波當做訊號以識別正在接近中的飛機。在第二次世界大戰之後，民間的應用也對這項技術引起興趣。在 1970 年間，RFID 技術應用開始逐漸成長，從汽車的電子車牌辨識到動物的晶片植入；在 1980 年早期，當 RFID 專家系統正為物件自動辨識進行試驗時，第一個交通工具自動收費系統也於挪威正式實施。在 1990 年到 2000 年間，總計核發超過 350 個與 RFID 裝置有關之專利；在 2000 年之後，與 RFID 裝置有關之專利便如雨後春筍般紛紛冒出。

### 一、RFID 運作原理

RFID 是使用無線電波來達到讀取品項資料的目的，其運作方式，是將微晶片和天線封裝在 RFID 標籤 ( Tag ) 中，而標籤依據應用領域的不同，有各種不同型式及大小依附在需要辨識的品項上，利用讀取器可以在一定距離外獲得標籤中，品項特有的數據資料，利用中介軟體 ( Middleware ) 與不同資訊系統結合，配合達到辨識、追縱及管理特定品項的目的。

簡單的來說，RFID 只是一種利用無線電波讀取特定品項資料的方法，但

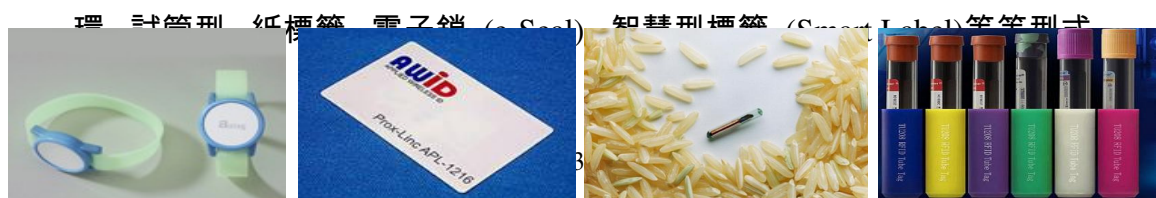
是 RFID 標籤可依不同需求及目的，製作成各種不同的型式與外觀，例如可以列印在標籤上黏貼在需要辨識的物品、將微晶片封裝成卡片型式做為人員身份辨識、將米粒大小的 RFID 標籤植入畜牧產品做為食品安全管控、將 RFID 標籤結合環境偵測器作為低溫物流及醫護監測使用、將 RFID 標籤巧妙地隱藏在特定物品中以管制其流向……等，RFID 標籤應用隨著各種技術的發展，已多到無法想像的地步。

## 二、RFID 特色

提到 RFID 常常有人拿條碼作比喻，雖然 RFID 快速發展的始作俑者，是 WalMart 企圖利用 RFID 全面取代條碼，以加速其整體商品物流管理的效率，然而 RFID 在商品的辨識應用只是 RFID 多樣化應用的一部份，每隔一段時間就有廠商宣稱開發出 RFID 的新應用，部分批評者指出 RFID 應用雖然多樣化，其標籤的價格將是 RFID 發展的絆腳石，但是不可否認的，RFID 標籤價格會隨著 RFID 發展日益下滑，RFID 應用的魅力所在，則是它可以依需求設計不同型態的標籤型式，以下簡單歸納 RFID 標籤的共同特性：

### (一)外觀的多樣性

RFID 標籤的基本架構不外是微晶片以及無線電天線的組合，依據其供電特性而有被動式 ( passive ) 主動式 ( active ) 以及半被動式 ( semi-passive ) 等三種型式，外觀上卻沒有特定型式，例如卡片型、塑膠鈕、錶帶型、米粒



錶帶型

卡片型

米粒型

筆管型



如圖 1。

圖 1 各式 RFID 標籤

#### (二)不須視線接觸

當在產品上利用 RFID 標籤來辨識、追蹤物品時，不需要看見物品上 RFID 標籤，甚至不需要看見物品。事實上，對於收納在包裝或是貨箱內的一種或多種產品 RFID 標籤，透過讀取器無線電波會自動地掃描，就可以獲得包裝或是貨箱內物品的相關資料。

#### (三)長距離讀取範圍

RFID 標籤依據標籤頻段不同與系統設計，讀取範圍可以由數公分到數十公尺。RFID 標籤讀取範圍對於不同應用範圍是非常重要的。藉由裝置在棧板上的標籤，貨品自離開工廠，經由層層的物流分送到賣場貨架上，可以不必拆封，就可以即時、正確地掌握其流向、位置及數量，大大減低盤點及核對數量時間與人力，這也是 WalMart 力推 RFID 的主要原因。

#### (四) 更強的辨識物品能力

在現今日益重視的食品安全上，畜牧養殖業、物流業和全球供應鏈市場

中，不僅要有追蹤與追溯產品的能力，還要有了解物品生產履歷的能力，RFID 便提供這項功能。

對畜牧及養殖產品的飼養與加工處理過程，在產品一開始植入 RFID 標籤，可以從產品的飼養到最終超市貨架上，建立完整的生產履歷。在一些國家，已經要求特定的產品必須要能夠追蹤產品從原物料到最終產品整個履歷的能力。

#### (五)惡劣環境的耐久性

RFID 標籤可以被封裝在堅固的塑膠外層中，在他們能通過嚴峻的生產製造和運輸操作流程後仍可持久的被追蹤。標籤可在油脂、污垢和油漆環境中仍被讀取，無線電波能夠穿越許多非金屬材料，而不像條碼可能會因為惡意的刮除或無意的磨損而無法判讀。

#### (六)資料可重複讀寫

除了部分列印式的 RFID 標籤，一旦列印在標籤上後就不可被修改，或是應用特性必須採取唯讀式 RFID 標籤。對於多數 RFID 標籤來說，資料是可多次重複書寫或修改，理論上可達十萬多次的重複書寫。

#### (七)大的資料儲存量

即使是最簡單的列印式 RFID 標籤，其資料儲存量也比過去條碼的高數倍之多，何況大多數 RFID 標籤還可以內嵌記憶體，可以儲存多達數百萬位元的資料。



## (八)同步讀取資料

大多數的 RFID 系統可以在天線有效範圍內,同時辨識與擷取多個 RFID 標籤資料。對於傳統條碼只能每次讀取一個條碼,當我們需要讀取數以千計的物品時,若利用傳統的條碼系統光這個程序就可能花上好幾個小時或好幾天的時間,而 RFID 系統僅需數分鐘即可完成同樣的工作。

## 參、RFID 安全與隱私議題

RFID 技術雖然為大家帶來了許多便利,一張悠遊卡可以坐捷運、購物、停車或作為身分識別;物流與零售業也在 WalMart 推波助攔下,掀起一股 RFID 熱潮,迄今仍方興未艾;RFID 應用在醫療照護與用藥管理上,提昇了不少醫療與用藥安全;圖書館導入 RFID 後,管理員也不用為了找一本書,在汗牛充棟的書堆中尋尋覓覓;有了 RFID 生產履歷保證,再也不擔心黑心產品下肚了;在 RFID 安全校園環境中,老師家長也不用擔心,哪一個過於活潑好動的學童,去了不該去的地方;嵌入 RFID 標籤的軍品,在管理上將更加嚴謹。但是在使用 RFID 上一定會想到的問題就是,這樣的技術安全嗎?我的個人隱私資料會不會被侵犯呢?無線電波辨識 RFID 標籤的同時,對於我的身體是否有危害?關於上述的問題,可以分成三個層面來看,分別是有關資訊安全問題、個人隱私資料問題、以及身體健康安全等面向。

### 一、資訊安全

RFID 只是一種利用無線電辨識物品資料的技術，其真正效能的發揮必須利用中介軟體與後端資訊應用系統的連結，所以只要有資訊軟體的應用，就會有資訊安全上的疑慮，此外，在讀取器與標籤透過空氣交換資訊的過程中也有可能被有心人士竊取或破壞，造成資料外流或是破壞，一般來說，常見影響資訊安全的包括幾種方式：

(一)竊聽：

RFID 是利用無線電讀取訊號，如同無線網路傳遞訊號時，就有被竊聽的可能，何況一般 RFID 標籤的設計概念是不會拒絕讀取器的讀取，只要讀取器的頻率與通訊協定符合，標籤都可以被讀取。因此，標籤在被讀取時，標籤的持有者並不知道此時標籤正在被讀取或是已經被讀取，這樣的問題多數是發生在讀取距離較遠時，例如 UHF、主動式或是微波系統。如果標籤內記載有屬於個人資料，將嚴重的影響到個人隱私與安全。

(二)追蹤：

近來高雄捷運公司推出，可以使用手機搭乘捷運，台北捷運也有手機結合悠遊卡功能，也就是手機內嵌有 RFID 標籤，紀錄有個人的搭乘交通工具與消費記錄資料，如此一來，那麼使用者的行為活動就有被追蹤的可能性。

(三)偽造：

雖然 RFID 系統強調標籤辨識碼具有唯一性，而且有高度資訊安全防護力，可以設定多組金鑰，但有心人士仍有可能變造出符合讀取器讀寫的標籤

資料格式，達成偽造欺騙的目的，尤其當這樣的 RFID 系統有牽涉到儲值扣款時，狀況將變得更加複雜。

(四)資料竊取：

從讀取器與標籤是透過無線電波方式交換資訊，到中介軟體轉換資料、後端資訊系統處理資料，中間任何一個環節都有可能造成資料被竊取，對於很多 RFID 系統的應用將產生極大的危害。

(五)阻斷服務：

雖然 RFID 的優點可以一次讀取大量標籤，但是事實上讀取器與標籤每次都是一對一讀取，只是透過適當的時間或頻段分配來讓每個標籤被輪流讀取，達成一次讀取多個的錯覺，因為這樣的時間讓使用者快到沒有感覺差異。但是，如果今天有一個標籤一直佔著讀取器不放，則其他標籤將永遠沒有機會跟讀取器進行資料交換，這就是所謂的阻斷服務，如果這樣的技術被有心人士或是駭客使用，將造成讀取器的失效，將會對 RFID 系統造成危害，而這樣的阻斷服務往往是非常難察覺的到，被發現時往往也已經造成了一定的傷害。

## 二、隱私權議題

在大多數的 RFID 應用情境中，所採用的 RFID 標籤上會記載一個獨特的識別碼，如產品電子碼 EPC，這些識別碼都是獨一無二的，因此每個標籤都具有唯一識別的特性，而標籤上的記憶體也讓標籤可以儲存比傳統的條碼更多的

資訊。若是商品上的標籤在未經同意的情況下被任意讀取或寫入，或是遭受先前提到 RFID 的各種安全威脅，標籤上的資訊將可能因此洩漏給有心人士，因而延伸出相關的使用者隱私議題，這些問題包含：(一)身分隱私、(二)購物隱私、(三)行蹤隱私。以下將個別介紹這些隱私侵犯的問題是如何發生的。

### (一)身分隱私

儘管標籤上儲存的資料可能不是個人資料，但如果這些資料可以跟使用者產生關聯，導致攻擊者可以藉由標籤的讀取來得知某個使用者的身分，便有可能侵犯使用者的身分隱私。而使用者身分隱私的威脅包含：

#### 1.關聯威脅

若標籤具有一個唯一識別的資訊，則此識別資訊將可能與標籤的持有者產生關聯，即使標籤上並未儲存跟持有者相關的資訊，但有心人士仍可透過標籤的識別資訊來判斷持有者的身分。

#### 2.群聚威脅

群聚威脅跟關聯威脅的概念相同，若使用者身上攜有數個以上的標籤，這群標籤的集合也可能與此使用者產生關聯。也就是說，雖然標籤本身所攜帶的資訊不是唯一的，但是多個這種標籤群聚之後，仍然能夠產生識別的效果。當讀取器一直讀取到同一群標籤，有心人士由標籤來推定是某使用者的信心就可以增強。

#### 3.麵包屑威脅

麵包屑威脅是由關聯威脅所延伸出的，因為標籤的識別資訊可與持有者產生關聯，如果持有者的標籤遭竊或丟棄，可能會被有心人士利用來假冒原先持有者的身分，進行不法之行為，因而陷害原先的持有者。

## (二)購物隱私

由於有心人士可以藉由標籤的讀取，來取得使用者所購買之商品的資訊，甚至可以透過這些推論出使用者的偏好、意圖跟行為。因而將侵犯到使用者的購物隱私，而使用者購物隱私的威脅包含：

### 1.動作威脅

個體(使用者)的動作、行為及意圖可以透過觀察標籤的動態或者訊號來推測。例如某個汽車旅館已嵌入 RFID 標籤液晶電視的標籤訊號突然消失，旅館即可推測是否有使用者想進行偷竊。

### 2.偏好威脅

由於標籤上可能記載著商品的相關資訊，如商品種類、品牌和尺寸等，因此可以藉由收集某個使用者所持有商品標籤的資訊，來推測此使用者的購物偏好。商家及可以透過這些偏好資訊來對使用者進行特定的廣告行銷。

## (三)行蹤隱私

在 RFID 應用中，可以利用標籤來追蹤貨品的流向或是位置。同樣道理，當使用者身上持有 RFID 標籤時，有心人士便可透過標籤來追蹤人的行蹤，

因此將侵犯到使用者的行蹤隱私。由於標籤具有一個唯一識別的資訊，且標籤的讀取具有一定的範圍，當讀取器讀取到某個標籤，即代表這個標籤正在讀取器的讀取範圍內，因此可以透過標籤來追蹤商品或使用者的位置。假如對標籤的位置做長時間的觀察，進一步還可以追蹤使用者的行進路線。

### 三、健康安全

有關於健康安全的議題可以先從行動電話談起，一般民眾使用行動電話，總是希望可以走到哪講到哪，享受通話的快感，但也常常看到許多民眾誓死抗爭不讓基地台設立在自家屋頂或是附近的大樓上，形成一種諷刺的對比。但是民眾抗議的原因，就是大家對於基地台發出的電磁波存在有影響健康的疑慮，而 RFID 也屬於電磁波通訊的一種，自然會有相同的疑慮產生。

RFID 系統的發射功率是低於一般行動電話的發射級數，並在世界衛生組織 ( World Health Organization , WHO ) 所規定的安全發射級數標準值之內。因此，任何關於行動電話設備安全性的研究結果，都可套用於 RFID 系統上。不過，截至目前為止並沒有相關證據能證明這些低功率設備，可能會對使用者或一般大眾造成任何健康風險。根據現有研究顯示，低功率無線應用與健康議題之間，並無明確關聯。

但是因為缺乏更有利的證據與更長時間的追蹤研究，所以這樣的證據仍然是無法說服民眾接受這樣的結果，所以有關於健康安全的疑慮仍然存在，只能等待未來有更多的證據與研究來解除大家的疑慮，也許研究結果是證明 RFID

電磁波確實對人體健康有害。

對於 RFID 的 LF 與 HF 系統因為都是靠電磁感應方式讀取，限制了讀取距離，因此所發出的功率都不強，對健康的危害都不大。但是針對 UHF 或是主動式系統，雖然設備都通過國家規定的功率認證，但是如果人員需要長時間處於這樣的環境下工作，誰也無法擔保不會因為時間的累積而產生問題。因此使用 RFID 的業者有義務主動告知使用者或是員工，讓員工知道有這樣的電磁波環境存在。

除了直接對身體健康的影響外，美國食品暨藥品管理局 ( Food and Drug Administration, FDA ) 曾做過一個實驗 ( 參考網址：<http://www.rfidjournal.com/article/articleview/1961/1/1/> )，使用頻率為 915 MHz 的 UHF RFID 讀取器對一個裝滿液體胰島素，外表貼有 RFID 標籤的玻璃瓶距離約 14.4 cm 連續讀取 1 小時，發現胰島素的溫度升高約 1.7°C，雖然無法實際證實這樣的胰島素如果用在人體身上是不是會有什麼影響，但是很多的藥品只要有溫度變化，就有可能產生化學變化，造成藥效失效或是藥效改變。這部份是 RFID 實際使用在藥品管制上，最容易被忽略掉的部份。

## **肆、RFID 安全與隱私議題防範方法**

### **一、資訊安全的防範方法**

為使 RFID 技術在使用上能同時顧及資料在傳輸過程中的安全性，根據一

般 RFID 系統的主要元件，即標籤端、應用端、與中介軟體等，分為標籤資料保護、資料傳輸防護、作業控管、中介軟體安全等四方面說明 RFID 系統應有的安全防範技術。

#### (一) 標籤資料保護

根據美國國家標準與技術局的 RFID 安全指南所述標籤資料保護可分為四個方面，分別為標籤記憶體的存取管制、標籤資料的加密、自毀命令的設定、篡改的防制等。

1. 記憶體的存取管制上，目前許多標籤硬體採取以密碼管制標籤讀寫權力的方式。一般而言，標籤記憶體存取管制可以避免標籤的內容遭受不當修改，其效力與密碼管理機制的健全程度有關。
2. 在標籤資料的加密方面，由於 RFID 標籤的成本因素，很難在標籤內建加密機制，RFID 標籤的內容可在寫入標籤前，由 RFID 系統伺服器或 RFID 讀取器先行加密，以達到資料加密目的。
3. 在自毀命令設定方面，RFID 標籤在確定失去再利用價值時，應具備自毀指令終止該標籤的一切活動，以避免該標籤遭受不當的再利用，造成資訊的流失。
4. 在標籤資料篡改防範方面，部份 RFID 標籤在啟動後具有防止篡改的功能，可避免攻擊者修改或移除標籤內容。較常見的是在 RFID 標籤裡使用易毀損的天線裝置，一旦標籤被移離其貼附物品，則標籤的電路連結



便遭受破壞而使標籤失去運作能力。此類功能也可用於檢驗該 RFID 標籤所代表的物件是否曾遭受意外破壞。

## (二) 資料傳輸防護

為防止發生對 RFID 標籤進行未授權的讀取與寫入及避免系統中出現遭到複製或修改的 RFID 標籤，RFID 系統可利用密碼、雜湊訊息驗證碼、簽章等方式。

- 1.在標籤密碼保護方面，一般 RFID 標籤內有部份指令須通過密碼認證才能執行，這些指令包括資料寫入、記憶體存取、以及自毀模式的觸發等，以確保資料安全性。
- 2.雜湊訊息驗證碼，在 RFID 資料傳輸過程中，將標籤與讀取機採取共用密鑰以相互驗證身分，強化資料傳輸安全。
- 3.數位簽章採取非對稱式加密機制。一般而言，RFID 標籤在製造時即被賦予唯一的識別碼，使用時 RFID 讀取機根據標籤的識別碼與其他通訊資料計算加密出一數位簽章並交由 RFID 標籤儲存，其他 RFID 讀取機在讀取簽章後便可經由比對，以確認過去存取記錄的合法性。

## (三) 作業控管

RFID 系統的作業控管包括實體控管、資料銷毀、操作訓練等方面。

- 1.實體控管為在 RFID 系統的應用環境中設置阻隔無線電波的障礙物以限制訊號讀取，其目的在於防止攻擊者接近 RFID 設備進行不合法修改、

破壞、竊取 RFID 裝置的機會。同時，障礙物的阻隔能力也可以防止未經授權的讀取動作發生。

- 2.在資料銷毀方面，對於失去利用價值的 RFID 標籤，應予徹底銷毀而不是單純的丟棄。銷毀資料的目的在於避免 RFID 標籤被當作追蹤的工具、防止機密資訊外洩與減少有心人士藉由分析丟棄的標籤找到攻擊系統的方法。
- 3.操作訓練可讓使用者熟悉使用 RFID 應用系統時，必須遵守的流程和資訊安全與隱私保護規範，完整的操作訓練可以避免使用者人為疏失，而減低了原系統應有的安全層級。

#### (四) 中介軟體的安全性

中介軟體負責接收 RFID 讀取機得到的標籤資訊，並加以整理再轉送給資料庫與分析軟體。中介軟體可以簡化企業內資料庫管理員與分析員的工作複雜度，使其不必考慮資料收集時煩瑣的硬體配置而得以專注於資訊的處理。為增進中介軟體的安全性可使用加密機制，加強中介軟體安全性。

然而，即使 RFID 系統使用了最安全先進的加密機制，若系統密碼因管理不當而外洩，則 RFID 系統安全仍將毀於一旦，故資訊管理機制的完善與合理程度攸關 RFID 系統中介軟體的安全性。此外在開發中介軟體時應對其程式進行軟體安全驗證，減少如緩衝區溢位等漏洞發生的可能性，並且對中介軟體之作業系統做定期的更新與漏洞修補以降低攻擊者的入侵機會。

## 二、RFID 隱私的防範作為

在發現到 RFID 所可能產生的隱私問題之後，相關廠商也開始思考因應之道，因為這些問題如果無法解決，將可能影響 RFID 的發展，而目前已有許多研究針對 RFID 的隱私問題，提出解決方案。以下將介紹幾種較常見的保護方法。

### (一)採用特殊設計的標籤

採用特殊設計的標籤主要是將標籤透過電路設計，來達成額外的功能或支援特殊指令而達到保護作用，較常見的有標籤銷毀指令(Kill Command)、標籤休眠指令 (Sleeping Command)以及密碼保護，以下面將進一步說明這些方法。

#### 1.標籤銷毀指令

若標籤支援 Kill 指令，如 EPC Class 1 Gen 2 標籤，當標籤接收到讀寫器發出的 Kill 指令時，便會讓自己永久失效，使得這個標籤之後對於讀寫器的任何指令，如讀取或寫入，都不會有任何的反應，因此可保護標籤資料不被讀取。但由於銷毀這個動作是不可逆的，一旦使用了銷毀指令就等於是作廢了這個標籤。

#### 2.標籤休眠指令

這個方法與銷毀標籤概念相同，當支援休眠指令的標籤接收讀取器傳來的休眠(Sleeping)指令，標籤就會進入休眠狀態，之後將不會回應任何

讀取器的查詢。必須在標籤接收到讀取器的喚醒(Wake Up)指令之後，標籤才會恢復正常的運作。與銷毀指令相比，休眠指令比較具有彈性，不需要作廢標籤即可達到保護持有者隱私的功能，也使得標籤可以回收使用。

### 3.密碼保護

此方法利用密碼來控制標籤的存取，在標籤中儲存特定的密碼，讀取器查詢標籤時必須同時送出密碼，若標籤驗證密碼成功才會回應讀取器，以保護標看內的資料被合法讀取。

## (二)阻隔標籤通訊

這類保護方法則是利用額外的設備，來防止或干擾標籤跟讀取器的正常通訊，藉此避免標籤被讀取，如此一來有心人士就無法順利讀取標籤上的資料，即可保護持有者的隱私。常見的方法有法拉第籠、主動干擾和阻隔標籤。

### 1.法拉第籠

這種方法是將標籤放置在由金屬網罩或金屬箔片組成的容器中，這種容器稱作法拉第籠，可以有效的屏蔽外電場的感應，來避免標籤被讀取器所讀取，達到阻隔通訊的目的。

### 2.主動干擾

這項方法是使用能夠發出無線射頻訊號的設備，持續地發送干擾訊號，主動干擾讀取器的查詢，因此可保護標籤不被讀取。但使用此方法也可能干擾其他合法無線電設備的使用，有違法之虞，因此本方法通常較少

採用。

### 3. 阻隔標籤

這種方法使用一種經過特殊設計的標籤，稱為阻隔標籤，這種標籤會持續對讀取器傳送訊息，以混淆讀取器，藉此阻止讀取器讀取受保護之標籤。例如商家可提供嵌有阻擋標籤的購物袋給使用者，使用者將購買的商品放入購物袋中，便可以保護商品上的標籤不被讀取。但當受保護之標籤離開阻擋標籤的保護範圍時，則安全與隱私的問題仍然存在

圖 2 和圖 3 為貼有阻擋標籤之護照封套及紙袋，在封套跟紙袋周圍或內部的標籤即受到保護，任何讀取器將無法讀取這些標籤。



圖 2 貼有阻擋標籤的護照封套 ( 資料來源：FoeBuD 網站 )



圖 3 貼有阻隔標籤的紙袋 ( 資料來源：FoeBuD 網站 )

### (三)建立密碼機制

以密碼學為基礎的解決方案，通常需要標籤具有基本的運算能力，例如亂數產生器、互斥或(Exclusive OR, XOR)運算、循環冗餘檢查(Cyclic Redundancy Check, CRC)以及雜湊(Hash)運算，以利採用適當加密機制進行保護，所以相對的硬體成本也比較高。

## 三、現行法律上的規範

目前台灣雖尚未有針對 RFID 所設計的法令產生，但是仍有部分法令可以加以規範，以保護個人隱私或是權益，藉由這些法令來規範廠商對於 RFID 的使用，避免侵害隱私權。這些法令包含有電腦處理個人資料保護法、個人資料保護法草案、商品標示法以及使用者保護法。以下分別簡單介紹這些法令，針對企業使用 RFID 時，保護使用者應有的權益。

### (一)電腦處理個人資料保護法第七、八、十八及二十三條以及個人資料保護法草

案規定公務或非公務機關對個人資料之利用或處理必須經當事人書面同意，不得侵害當事人權益，因此可以用來規範廠商透過 RFID 收集個人資訊。由於 RFID 技術存在著隱私侵犯的問題，而目前安全的保護方式也較不明確，因此事先向使用者告知商品使用 RFID 技術，被認為是一種有效的保護使用者的方式。

(二)根據商品標示法第九條第五項的規定，商品於流通進入市場時，生產、製造或進口商應標示下列事項，除了商品名稱、生產及製造商資料、商品內容以及製造日期外，其他則依中央主管機關規定之應行標示事項。因此當企業使用 RFID 技術時，主管機關可以要求廠商標示相關資訊，讓使用者知道商品含有 RFID 標籤，以保障使用者隱私權。

(三)在使用者保護法第十四條第四項提及，定型化契約中若有明顯不利於使用者之情形者，視為違反平等互惠原則。所以當使用者認為企業使用 RFID 技術對於自身權益有所損害時，可以透過使用者保護法向商家拒絕使用 RFID 技術，以保護使用者應有的權益。

#### **四、國外相關的規範與草案**

目前越來越多人已經注意到 RFID 科技使用上的疑慮，許多注重隱私權的團體開始發動抵制使用 RFID，並要求制訂相關法令規範，這些法令的目的即是規範企業對於 RFID 技術的使用，以及保障使用者在面臨廠商使用 RFID 技術時，相關權益的確保。以下介紹幾項 RFID 有關的規範：

(一)美國電子隱私資訊中心(Electronic Privacy Information Center, EPIC)的 RFID

使用指導綱領明白律定廠商在利用 RFID 技術時，必須標示的相關責任、不應該有的行為、以及使用者應有的權利。

(二)電子權利法草案(Electronic Bill of Rights)主張禁止在未告知使用者的情況下

收集、儲存和公開透過 RFID 技術獲得的資訊，並且需事先徵得使用者的同意，才得以開啟 RFID 設備。

(三)RFID 權利法草案(RFID Bill of Rights)主要提出使用者在商家使用 RFID 的情

況下應享有的權利。

## 伍、結語

RFID 科技的運用與隱私權保護間，有如流水能載舟亦能覆舟，當人們對於科技越來越依賴，讚嘆手機和網路交易便利的同時，人們也對詐騙行為、非法監聽、電磁波疑慮產生困擾。就如同近十年間網際網路的快速發展，創造了許多生活便利性與多樣性，但是它也將色情、垃圾郵件、電腦病毒滲透到日常生活中，也讓我們的孩子每天暴露在充滿打鬥流血、暴力和色情的環境中而不自知。RFID 創新技術已在身份識別、圖書資訊管理、醫療照護系統、畜牧管理等方面發揮了作用，於物流管理方面更是在銷售策略上的利器。RFID 技術所帶來的無「線」便利與應用將可能使我們對「便利生活」作出不一樣的定義，但是伴隨 RFID 科技背後的滾滾利潤，誘惑著廠商在未完成審慎評估之前就大力推廣，將使用者放在資訊洪流上的一葉扁舟上，隨時會沒入洪流中。在現代社會中，網路科技與無



線射頻科技的創新發展下，我們的生活無時無刻被監視與記錄，傳統隱私權中所謂「獨處不受干擾(to be let alone)」的權利越來越受到挑戰，本文提醒人們沈浸在 RFID 創新科技運用的同時，也應該主張個人隱私權的保護理念，以保障個人控制自己資訊應該如何被處理與使用的權利。

## 參考文獻

中文文獻：

行政院主計處(1995)，「電腦處理個人資料保護法」，<http://www.dgbas.gov.tw/>

法務部網站 ( 2007 ) ， 「電腦處理個人資料保護法修正草案條文對照表」，

<http://www.moj.gov.tw/>

陳昱仁 ( 2009 ) ， 「RFID 概論」，長庚大學 RFID 物流與供應鏈資源中心

陳穆臻，陳凱瀛 ( 2009 ) ， 「RFID 應用」，教育部 RFID 推動辦公室

周湘琪 ( 2004 ) ， 「RFID 技術與應用」，旗標出版股份有限公司

奚正德、張克章 ( 2006 ) ， 「 RFID 相關應用與安全機制簡介」，資通安全專論，

國家實驗研究院科技政策研究與資訊中心

蕭榮興、蘇偉仁、許育嘉 ( 2004 ) ， 「RFID 技術運作的神經中樞 - RFID Mid-

dleware」，電子商務導航，第六卷，第十四期

曾龍、黃亦銘、林政穎 ( 2007 ) ， 「RFID 安全性議題」，RUN!PC 雜誌

謝穎青 ( 2005 ) ， 「通訊科技與法律的對話」，天下遠見出版股份有限公司

陳宏宇 ( 2004 ) ， 「RFID 系統入門無線射頻辨識系統」，松崗

錢樵清 ( 2006 ) , 「無線射頻辨識應用於軍械及庫儲運管先導實驗研析」 , 聯合  
後勤季刊 ,

RFID 應用推動辦公室網站 ( 2007 ) , 「RFID 使用於病患管理之個人隱私保護  
相關法規研析」 , <http://www.rfid.org.tw/>

英文文獻 :

Aigner, M. and Burbridge, T.(2008), “Building Radio frequency IDentification for the  
Global Environment, White Paper”,pp.5-6.

Banknotes, E. ( 2003 ) , ”Financial Cryptography (FC’03)”, Vol. 2742, pp.103-121.

Juels, A. ( 2005 ) “RFID Security and Privacy: A Research Survey,” RSA Labora-  
tories.

Juels, A. and R. Pappu ( 2004 ) , “Squealing Euros: Privacy Protection in RFID

Juels, A., R. L. Rivest and M. Szydlo( 2003 ),“The Blocker Tag: Selective Blocking of  
RFID Tags for Consumer Privacy,”8th ACM Conference Computer and Comm.  
Security, pp. 103-111.

Karygiannis, T., B. Eydt, G. Barber, L.Bunn, T. Phillips ( 2007 ) , “Guidelines for  
Securing Radio Frequency Identification (RFID) Systems (Special Publication)”.

Ohkubo, M., K. Suzuki and S. Kinoshita ( 2003 ) , “A Cryptographic Approach to  
'Privacy-Friendly' Tag,” RFID Privacy Workshop.

William, Oliver and Hedgepeth ( 2006 ) , “RFID Metrics: Decision Making Tools for  
Today's Supply Chains,” CRC Press.

<http://rfid.cgu.edu.tw/xoops/modules/tinyd3/print.php?id=6>

<https://shop.foebud.org/stoprfid/rfid-kartenschutzhuelle-einfach.html>