感應式技術之金融應用與安全防護

黃建隆 / 財金資訊公司安控部資訊安全組高級工程師

一、前言

本文所謂的「感應式技術」係指由無線射頻識別 (Radio Frequency Identification；RFID) 所發展出的技術，目前無線射頻識別技術於生活中之應用十分普遍，舉例而言：植入所飼養寵物體內的「寵物晶片」、圖書館藏書中的防盜晶片、高速公路依里程計收費用的 eTag、搭乘捷運所使用的悠遊卡、感應式金融卡與信用卡等，林林總總均屬於此類技術之應用。這類應用基本上是由無線射頻識別電子標籤 (Tag)、感應式卡片與感應式讀卡機 (Contactless Reader) 等元件所組成。因相關技術與規格過於龐雜，故本文僅限定範圍於金融應用的感應式晶片卡與其相關技術。

感應式 (contactless；亦稱為非接觸式) 技術應用於非手機之載具，例如：感應式門禁卡片、感應式支付卡片等，已行之有年，近年來隨著行動支付議題的火熱，與國內 MNO (mobile network operator) 電信 TSM (Trusted Service Manager)、PSP (Payment Service Provider) 金融 TSM 的陸續建置與投入市場，感應技術應用於行動支付已然成為兵家必爭之地。2013 年 10 月，隨著 Android 4.4 版的發表，Google 推出主機卡模擬技術 (Host Card Emulation；HCE)，自此，Google 的行動支付擺脫使用安全元件 (Secure Element；SE) 的架構，改推雲端的純軟體支付平臺，同時此技術也獲得 Visa 與 MasterCard 等國際組織的支持。2014 年 9 月，Apple 公司則發表 Apple Pay，不僅採用內建的安全元件與支付卡憑證化 (Tokenization) 技術，更結合指紋辨識功能，可謂是在安全與方便性上取得一個平衡點。前述兩大陣營的近端感應支付技術，其實是行動裝置與近場通訊 (Near Field Communication；NFC) 結合，所衍生的新形態感應支付工具，以信用卡收單行而言，刷卡機基本上無須配合改造，只要可受理感應式信用卡即可。因此，該兩項技術可望成為未來行動支付的明日之星。

二、感應式技術的發展

感應式卡片的技術誕生於 1990 年代，相較於既有的磁條卡或接觸式晶片卡，該技術憑藉其不需電源供應、操作便捷與壽命更長等特性，於問世後，便引起極大關注，並迅速地拓展應用市場。甫推出時，載具是以實體卡片的

形式存在，時至今日，已衍生出諸多相關不同型態的樣貌，其中又以行動裝置上的近場通訊支付技術尤為熱門，儼然成為當代之顯學。

圖 1 所示者為 combi 卡片，即同時具備感應式與接觸式二種介面的卡片；感應式的運作，基本上是透過無線電波在感應式卡片與感應式讀卡機間進行讀寫動作，卡片本身僅須透過無線電波的電磁轉換提供能源即可作業，與接觸式卡片兩相比較下，硬體的差異性基本上是在天線部分。

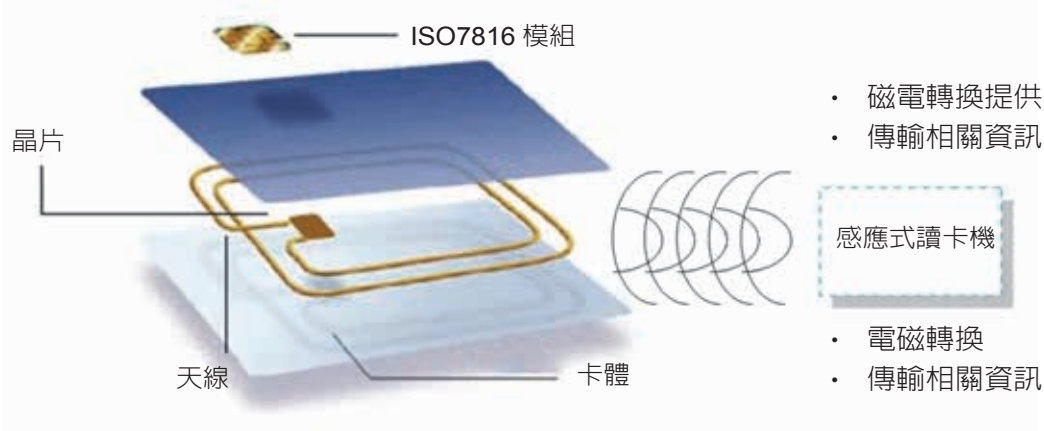

圖 1　感應式卡片運作示意圖

(資料來源：Calypso Handbook)

值得一提的是，一般人對於接觸式與感應式卡片之差異有一種誤解，亦即卡片相關資料的存放，認為感應式卡片將之存放於天線中；事實上，兩者均將資料存放在晶片中，天線僅只是溝通介面罷了。

瞭解運作原理後，以下將針對目前較常見的感應式技術有關國際相關規格概述之，亦著墨於近場通訊 (NFC) 方面。

(一) ISO/IEC 14443「短距離非接觸式晶片卡」，特性如下：

1. 工作距離：0~10 公分。
2. 工作頻率： 13.56 MHz。
3. 卡片類型：CPU 卡片或 Memory 卡片。
4. 應用：金融支付 (例如：感應式金融卡、信用卡等)、身分識別 (例如：晶片護照) 與交通票證 (例如：悠遊卡、一卡通等) 等運用，主要都使用該項標準。

(二) ISO/IEC 15693「鄰近非接觸式晶片卡」，特性如下：

1. 工作距離：0~1 公尺。
2. 工作頻率：13.56MHz。
3. 卡片類型：Memory 卡片。
4. 應用：一般應用於圖書館書籍管理、貨物追蹤、大眾運輸等。

(三) ISO/IEC 18092「近場通訊」

「近場通訊」又被稱為「近距離無線通訊」，是一種短距離的高頻無線通訊技術，可使電子裝置進行感應式點對點資料傳輸或資料交換。

該項技術是由飛利浦半導體 (現為恩智浦半導體 ; NXP)、諾基亞 (Nokia)、索尼 (SONY) 等公司共同研發，其基礎是無線射頻識別及互連技術。近場通訊是一種短距高頻的無線電技術，以 13.56MHz 頻率於 20 公分距離內運作。目前近場通訊已分列為 ISO/IEC IS 18092 國際標準、EMCA-340 標準與 ETSI TS 102 190 標準等三種標準。該項技術可運作於被動與主動模式，被動模式之運作不需要電池，但缺乏獨立發射訊號的能力；主動模式則相反。其工作模式可再細分為下列三種：

1. **卡片模擬 (Card Emulation) 模式**

此模式主要用於取代目前實體的感應式卡片，例如：感應式金融卡、信用卡、悠遊卡、門禁管制卡、車票、門票等等。在此種模式下，卡片透過感應式讀卡機的無線射頻場 (RF field) 供電，因此即便遇寄主裝置 (HOST，例如：行動裝置等) 沒電，仍可運作。另外，近場通訊的裝置若要使用卡片模擬模式的相關應用時，必須搭配安全元件晶片。

2. **讀卡機 (Reader/Writer) 模式**

以裝置作為感應式讀卡機，可讀取一般實體的感應式卡片或無線射頻識別電子標籤，例如：可透過行動裝置讀取智慧型海報上所提供之網址或說明等。

3. **點對點模式 (P2P) 模式**

此種模式主要用於資料交換或配對，例如：可透過近場通訊的方式，在多裝置間，如：相機、電腦等，進行資料交換。舉例來說，目前新型的相機通常具備 NFC 功能，開啓後，可透過手機的 NFC 功能與其連接，並擷取其中的照片，抑或控制相機拍照等。

三、感應式設備介紹

隨著感應式技術的演進，目前常見之感應式相關設備大致說明如下：

(一) 卡片

感應式卡片之呈現型式具多樣化，不一定為實體之卡片，也可能是應用於手機上的安全元件。主要可分為以下兩大類：

1. CPU 卡片：卡片內建有 CPU，具加密運算功能，例如：卡片可提供 3DES 及 AES 等運算，故成本較高，但安全性相對較高，主要運用於金融相關之應用。
2. Memory 卡片：運用一些保護技術 (如：隱藏磁區)，將金鑰或憑證儲存於記憶體中，相對成本較低，加上是透過軟體程式呼叫演算法，且 Memory 卡片只有密碼 (PIN Code) 及資料加密保護，所以不論效能或安全性都較低，主要之運用如：一代悠遊卡或一般門禁卡片等。

(二) 讀卡機

感應式讀卡機之呈現形式大致有以下四種：

1. **刷卡機使用之感應式讀卡機 (一般稱之為 dongle)。**

2. **個人電腦所使用之感應式讀卡機**。

3. **以配備近場通訊裝置的手機做為感應式讀卡機**。

4. **其他，例如：捷運收費門柱等**。

綜上，感應式技術由卡片演進到行動裝置，利用裝置上的使用介面並結合安全元件與近場通訊裝置，可應用的範圍將更為寬廣，已然成為未來支付之趨勢。但在面對眾多型態之載具與諸多的感應式讀卡機裝置的組合運作下，相關的安全性更值得我們的關注與跟進。

四、安全認證

感應式技術相關之安全認證，大體上可分為以下兩部分進行說明：

（一）晶片（卡）/安全元件安全之相關組織

1. 共同準則 (CC：Common Criteria)：依晶片的安全強度定義一套共通的量化標準進行安全評估，共分為 7 級；目前我國銀行業所使用之晶片金融卡，其晶圓至少應符合第 5 級 (EAL 5，Evaluation Assurance Level 5)。
2. 中華民國銀行商業同業公會全國聯合會：定義 BC (Banking Criteria) 相關規範與認證。
3. EMVCo：由 American Express、JCB 、MasterCard 及 Visa 共同成立，係以研訂晶片卡規格為主要任務的機構，亦有相關之卡片、安全元件、讀卡機等之認證。
4. VISA、MasterCard、銀聯等國際組織：針對產品是否符合各自制定之規格備有相對應之認證，例如：感應式卡片規格與安全、安全元件、讀卡機或手機等。
5. GlobalPlatform (GP) 國際組織：GP 定義諸多卡片、裝置與系統的規格供相關廠商應用，並可申請相容性認證。面對行動支付的相關技術，傳統對晶片卡認證的概念已經無法滿足其作業要求，因而該組織提出組合模式的認證架構 (Composition Model Security Guidelines for Basic Applications)，可兼顧安全元件上多個應用程式動態複雜的組合，又能兼顧高安全性要求的支付等重要應用程式的安全性，因此，GP 組織的組合模式將是未來相當重要的一項參考標準。

（二）讀卡機/手機安全之相關組織

1. EMVCo：具有連接刷卡機的感應式讀卡機 Leve 1 認證。
2. VISA、MasterCard 等國際組織：針對產品是否符合各自制定之規格備有相對應之認證，例如：手機的安全認證。

五、安全威脅

上述諸多安全認證機構之作業，雖非完全為感應式之安全性而制定，但感應式技術因其特性也衍生出相對的威脅：

（一）交易過程中的溢波偵測（Leakage）

因無線電波具發散性之特性，當交易進行中，感應式讀卡機與感應式卡片間所傳送之訊息，有可能於傳輸過程中被側錄，就此，可能的風險控管措施為：

1. 避免傳輸敏感資料或於通訊加密。
2. 建置防止重送攻擊 (Replay Attack) 之機制。
3. 良好的特店管理。

（二）遠距讀取

感應式技術是透過無線電波運作，其接收端之功率與距離的平方成反比，然與天線發射的功率則成正比。曾有實驗證實，在 30 英尺之外仍可能偵測到感應式卡片的訊號，對此，可能的風險控管措施為：

1. 將卡片隔絕於電磁波無法穿透的容器或皮夾中。
2. 對於行動裝置使用近場通訊卡片進行模擬部分，建議在一般狀態下，關閉近場通訊功能，僅於交易時再行開啓。
3. 錢包的設計邏輯，卡片須於交易時才被啓用，且若超過交易時限 (例如：60 秒) ，則自動關閉該卡片，卡片應非一直處於啓用狀態。
4. 敏感性資料須具有權限者才可進行讀取作業。

（三）中介傳送攻擊（Relay Attack）

透過模擬假卡片或模擬假讀卡機，躲藏於其中進行攻擊。就此，可能的風險控管措施為：

1. 須具備卡片真偽之驗證機制。
2. 須具備讀卡機真偽之驗證機制。

（四）針對行動裝置因提供感應技術而衍生之安全威脅

此部分並非感應式本身所導致之議題，乃因裝置特性所致。就此，可能之風險控管措施為：

1. 安全元件的存取應有認證機制，須限制可存取卡片之 App。
2. 相關支付 App 或錢包之軟體，應進行妥適的動態或靜態安全性檢測，以防範因軟體漏洞而產生之風險。
3. 相關支付 App 或錢包，應禁止經 Root (破解 Android 裝置取得最高權限) 或 JB (Jailbreak；破解 iOS 裝置取得最高權限) 處理的裝置安裝其軟體。

綜上所述，通過前述相關安全認證機構認證之卡片或設備，基本上可確保於金融運用上具一定程度的安全性。但良好的交易安全機制是環環相扣的，非單一控制點即可達成所謂的安全，故對於金融應用而言，相關軟硬體應確實通過所屬之認證或安全檢測為佳。

六、感應式技術的金融應用

感應式技術之應用，主要著重於方便性之考量，對於金融交易而言，實體感應式卡片基本上多屬於無須輸入密碼或免簽名的小額支

付，但尚須搭配其他控制措施進行風險管控為宜，例如：設定單筆交易金額上限 (目前為新臺幣 3,000 元)、交易日限額，抑或類似子帳戶可與一般帳戶區別等方式，以利進行風險控管等。另一方面，在行動裝置上，因裝置已具備操作介面，可供進行密碼驗證或其他確認機制，可應用的空間較為充裕，有利於風險之降低。

有關目前感應式技術相關的金融應用，分為以下三個方面進行概述：

(一) 實體感應式卡片

此類的應用，目前於現實生活中已是司空見慣，例如：使用信用卡 (VISA paywave、MasterCard paypass、JCB J/Speedy、銀聯閃付等) 或感應式金融卡進行消費的支付或繳費 / 稅等，結合第三方支付的 O2O (Online To Offline) 線下交易則是另一種應用。

(二) 結合行動裝置的近場通訊 (卡片模擬)

對此類近端的感應式交易而言，基本上與實體卡片差異不大，但其應用的技術則有極大之差異，此部分的技術大致可分為三類說明：

1. TSM 與安全元件：

將金融卡或信用卡載入至行動裝置的安全元件中，可進行近端感應式與遠端金融交易。但此種運作模式，過去在擁有安全元件的電信營運商與金融機構間的競合、架構複雜度高、相關投資所費不貲情況下，談論多年，難以付諸商轉。這一兩年來，終於陸續有相關系統進行建置。惟，此刻面對來勢洶洶的 HCE 與 Apple Pay 兩個競爭對手，未來營運將會是一項極大的挑戰。

2. HCE

此技術為 Google 所提出，為擺脫安全元件的依賴，於 Android 4.4 以上版本開始支援本項技術。既有讀取行動裝置上的卡片，是透過近場通訊傳導到安全元件，HCE 則是傳導到軟體式卡片，此卡片資料是由雲端伺服器所產生，僅供單次且具時效性的使用。此技術的核心是 EMVCo 的支付卡憑證化 (Tokenization) 規格，為純軟體式的技術。目前 VISA、MasterCard 等國際組織已宣布支援此技術，對金融機構而言，這也是一項自主性較高的感應式支付解決方案，但其安全性仍有待考驗。

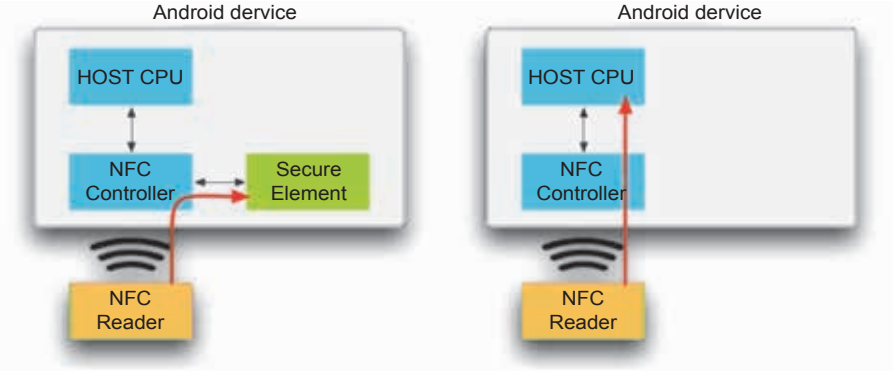

圖 2　HCE 運作示意圖
(資料來源：Google)

3. Apple Pay

Apple 的此項技術亦是近場通訊與支付卡憑證化的結合，但與 HCE 不同的是，在自家軟硬體整合的優勢下，此項技術將內建的安全元件 (embedded SE) 與指紋辨識納為安全機制的一環，對於安全性與方便性間取得一個平衡點，因此，此技術未來之發展實在不容小覷。目前，此項技術已在美國境內應用於近端感應式或遠端支付 (信用卡或金融卡均可支援) 服務。

(三) 實體卡片與行動裝置近端通訊結合

透過行動裝置的 App 與近場通訊讀取實體感應式卡片，再進行支付，雖然此類的應用在國外已有先例 (例如：香港八達通卡片可以手機進行「拍卡」(即感應)，嗣於淘寶網支付款項)，但必須先審慎考量完整的安全性配套措施，以防止不法之使用，例如：須事先申請將行動裝置與感應式卡片綁定，經一定時間後核准，方可進行交易等，或者，僅能用自己名下的卡片繳交自己的費用等。

綜合上述，感應式卡片的交易其實已行之有年。在國內，行動裝置的近端支付雖方興未艾，但 HCE 與 Apple Pay 的應用則指日可待，期近端與遠端交易可畢其功於一役。

七、結語

綜觀感應式技術的演進，載具由卡片發展至行動裝置，其應用亦隨之更為豐富。由 Gartner 發布的報告可一窺行動支付發展之狀況，如表 1 所示的金額包含近端感應式與遠端的網路交易，以後者為大宗，預估近端的交易金額之成長率將由 2012 年的 2% 成長至 2017 年的 5%。但在行動裝置方面，近端的感應式與遠端的網路交易之安全實為一體兩面，互為影響。因此，對於相關支付 App 或錢包之軟體安全實應更為審慎考量，例如：OWASP Top 10 Mobile Security Risks 所列之風險應納入此類軟體的檢核標準等。

表 1　Gartner 全球行動支付交易報告

項目	2012 年	2013 年	2017 年	年成長率 (2012-2017)
全球行動支付交易總金額	1,631 億美元	2,354 億美元	7,210 億美元	35%
全球使用行動支付的用戶數	2.008 億戶	2.452 億戶	4.5 億戶	45%

(資料來源：Gartner)

另一方面，感應式的技術應用於行動裝置實為未來之趨勢，前述之 HCE 及 Apple Pay 的支付卡憑證化技術核心，基本上可以解決信用卡長期以來的敏感性資料外洩問題，並相容於目前既有的感應式刷卡設備，對於發卡行應具莫大的吸引力，其後市可期。然而，我國晶片金融卡若要融入這些支付技術，尚須考量相對之風險 (指純軟體式的 HCE) ，並進行相對之作業與安全機制調整。

最後，對個人而言，感應式的交易基本上是以便利性為主要考量，並搭配相對應的配套措施進行風險控管。因此，以實體卡片而言，除遺失的風險外，相對風險較低。但反觀行動裝置，執行環境複雜，又可進行近端與遠端交易，相對風險較高，建議個人應做好自己的風險控管，亦即須提升自我的資安意識，例如：於裝置上安裝軟體或點選相關連結時，應保持警覺性，以策安全。

※ 參考文獻 / 資料來源：

1. Calypso Handbook Part II。
2. 非接觸式晶片卡之安全性考量與解決方案 (作者：陳清煌)。
3. 晶片支付卡安全及發展趨勢 (作者：蘇偉慶)。
4. Gartner 2013/6 報告。

讀者心聲

首先，感謝您撥冗閱讀「財金資訊季刊」！

請您提供我們寶貴的意見或建議，給我們一個攜手共進的機會，我們將儘可能符合您的需求，也豐富季刊的內容，提升對您的服務。

敬請　不吝賜教，並請您將寶貴的意見或建議以電子郵件傳送至財金資訊公司管理部文書組張小姐 laura_chang@mail.fisc.com.tw。