行動支付創新之商業營運模式發展趨勢

翁世吉 / 財金資訊公司研發部網路設計組組長

一、前言

根據西元 2014 年 10 月 Google 與模範市場研究機構 (TNS) 共同合作的《消費洞察報告》(Consumer Barometer) 及《臺灣線上購物與多螢研究》報告，臺灣地區近 80% 消費者透過各種電子設備及網路搜尋功能，進行產品規格功能、價格、促銷優惠或使用者評價等多層面評估，作為購物決策參考；其中 68% 消費者係使用商店行動版網站購買產品 (比例為全球最高)，顯示臺灣地區民眾透過行動裝置進行購物的模式，已然成為電子商務不可忽略的新通路。

據報載，大陸阿里巴巴集團於同年 11 月 11 日 (雙 11) 舉辦之購物狂歡節當日，交易總金額約人民幣 571 億元 (約 95 億美元)，比 2013 年的 362 億元成長約 58%，更超越同年美國黑色星期五 (Black Friday) 及網路星期一 (Cyber Monday) 交易合計金額 29 億美元，其中透過行動電子設備完成整體購物交易比例者約達 42.6% (約人民幣 243 億元)，較 2013 年的 20% 可見明顯成長，其中整體瞬間購物交易透過手機完成的比例最高約 70%。

美國蘋果公司 Apple Pay 行動支付方案於 2014 年 10 月 20 日正式上線服務，72 小時內就有超過百萬張信用卡啓用該功能，初期先完成美國境內 22 萬家商店受理 Apple Pay 端末設備佈建，提供 500 家金融機構所發行之 VISA、MasterCard 及 American Express 信用卡持卡人消費購物服務。Apple Pay 支付服務以支付憑證代碼 (Token) 取代傳統使用信用卡卡號作為交易憑證模式，因此在行動裝置或支付交易處理流程中，無須留存或傳輸信用卡卡號等敏感性資料，可有效提高持卡人交易安全及降低營運處理風險，有助於行動支付業務推廣。

近年來，我國電子商務發展突飛猛進，金融業積極開發各種行動支付模式與應用推廣，財金資訊公司 (以下稱財金公司)、聯合信用卡處理中心 (以下稱聯卡中心) 及台灣票據交換所 (以下稱票交所) 合作邀集各會員銀行於 2014 年 9 月成立「臺灣行動支付公司」，共同推動 NFC (Near Field Communication) 行動支付方案，計劃於年底前上線服務，預期必將帶動國內行動支付產業加速成長。

綜上，國內外各項行動支付服務蓬勃推展，相關行動支付應用技術也不斷推陳出新，爰此，本文將從行動電子商務相關發展情形，

探討目前最新行動支付憑證代碼化 (Payment Tokenization) 技術，分析其作業設計機制及未來應用發展，提供參考。

二、行動電子商務發展趨勢

資訊技術應用是發展行動電子商務主要動能，根據國際電子商務產業研究機構 (First Annapolis Consulting) 調查結果，簡單分析未來行動電子商務創新趨勢，說明如下：

(一) 安全控管變革
－「安全可靠」為發展基礎

電子商務服務首重對相關安全規範的遵守 (Compliance) 以保障交易環境安全，支付服務整體作業之規劃設計應在便利性與安全性間取得最佳平衡，建立相對合理且可行之營運模式、完善之風險管理機制，並不斷汲取新技術以強化作業服務水準、持續確保消費者權益及安全性，進而提升客戶的信任度與忠誠度，是發展創新行動電子商務的成功基礎；因應各種行動電子商務變革，未來交易安全控管、身分認證機制等相關創新技術發展，將深受關注。

(二) 銷售通路變革
－「全通路」時代的來臨

全通路 (Omnichannel) 銷售是指企業提供全方位銷售通路組合的服務類型營運模式，包括實體商店、電子 (網路) 通路商店與網路溝通平台 (如企業網站、客服中心、社群媒體) 等，以滿足消費者購物、娛樂或其他服務等各種需求。商店如何提供安全可靠之支付選擇方案、簡便的行動裝置螢幕操作介面及整合式 (傳統實體商店與網路) 行銷通路，以因應來自各種不同銷售通路的服務需求，建構快速交貨物流機制、有效簡化交易流程、提升銷售服務效率的消費模式，將是企業最大的挑戰。

(三) 消費習性變革
－「社群」行銷模式興起

隨著消費者使用行動電子裝置日益普及、網路社群溝通平台逐漸興起，透過社群或團購網站行銷 (Social Commerce)，消費者可很快速地找到所需商品或服務，有些網站則可依據消費者需求，提供客制化商品過濾、比價或使用經驗分享等服務，因此，「社群」行銷模式越來越受消費者青睞；此外，透過巨量交易資料的分析，商店或金融機構更容易精準掌握消費者喜好及需求，再透過各項消費紅利獎勵措施，有效提高消費體驗價值與品牌忠誠度；未來，商店如何掌握社群脈動及與消費者快速互動，將成為企業發展電子商務致勝關鍵。

(四) 連網模式變革
－「穿戴設備」引領「沙發電子商務」新潮流

隨著蘋果 Apple Watch、谷歌 Google Glass、澳洲 BPAY 公司 Wristbands、MasterCard Nymi 等穿戴設備 (Wearable) 產品推出，未來此類新興型態的電子商務 (躺著也能消費的「沙發電子商務」) 模式，能否繼智慧手機後成為另一項熱門行動支付工具，值得樂觀期待。

（五）物流創新變革
－「快速運籌」奠定電子商務決勝關鍵

物流 (Logistic) 是整體電子商務服務之最終、最困難也是成本最高的作業流程，因應消費者普遍要求提供快速交貨服務，各企業無不絞盡腦汁改善物流服務效率，比如我國網購業者推出網路交易後 6 小時完成交貨；大陸阿里巴巴集團自建物流體系，承諾中國境內消費者網路下單後 1 天內可完成交貨服務；美國網購巨擘「亞馬遜」(Amazon) 發展遙控飛機交貨服務等等；可見未來如何快速運籌以完備電子商務「最後一哩路」，已成為電子商務產業另一競爭戰場。

三、行動支付創新模式發展現況

目前全球行動支付應用技術發展，主要是透過行動裝置的瀏覽器、行動 APP、電子錢包支付等 3 種介面工具，分別於近端非接觸式支付 (如 NFC、RFID － Radio Frequency IDentification 等)、遠端行動 APP、簡訊、USSD (Unstructured Supplementary Service Data，非結構化補充資料服務技術；手機系統業者在非洲等通訊基礎設施較不普遍國家，所特別設計的特殊服務模式) 或瀏覽器模式，執行各種支付作業服務；如圖 1 所示。

圖 1　行動支付作業模式發展
資料來源：www.customerthink.com 網站

美國蘋果公司推出的 Apple Pay 行動支付方案，由持卡人使用行動設備 (iPhone、iPad、iWatch 等) 介面，透過 Touch ID 元件以指紋進行身分辨識，當完成 Apple Pay 註冊程序後，透過行動設備 APP 及蘋果錢包伺服器 (Apple Wallet Server) 網路，傳送啟動服務請求，至發卡銀行指定的支付憑證代碼服務商 (Token Service Provider，以下簡稱代碼服務商) 取得供該行動設備使用之支付憑證代碼 (Payment Token，以下簡稱代碼)。當持卡人於網路商店完成購物，選擇以 Apple Pay 辦理付款作業時，經行動設備提示相關付款明細，持卡人再按壓指紋完成身分確認，隨即由行動設備 App 發送交易授權請求訊息 (含代碼)，

透過商店及支付網路系統請求發卡銀行就該交易進行授權。

有別於大部分行動支付模式，須將信用卡卡號等資訊，以各種軟硬體方式加密後儲存於行動設備中，Apple Pay 係採用 PassKit 控制元件，將代碼以加密方式儲存於實體安全元件 (SE，Secure Element) 晶片中，且代碼與實際信用卡卡號之關係及其產生機制是由發卡銀行決定，支付訊息傳輸過程均以代碼做為交易授權依據；持卡人行動裝置或商店資訊設備，均不儲存卡片資訊，網路駭客亦無法於交易訊息傳輸過程中，截取代碼加以還原而取得卡片資訊，可避免信用卡卡號等資訊外洩風險。

以下即以蘋果公司發展的近端非接觸式支付及遠端行動 APP 支付創新模式－行動支付憑證代碼化 (Tokenization，以下簡稱代碼化) 機制為例，概述其技術設計重點與營運作業流程。

(一) 代碼化作業機制

Apple Pay 的代碼機制係遵照 2014 年 3 月國際晶片卡組織 EMVCo 所公布的「支付憑證代碼化標準」(EMVCo Tokenization Specification v1.0) 進行設計，並且是首項依據該標準正式提供商業營運服務的行動支付系統；主要是以 EMV 晶片卡在卡片提示類交易 (Card-Present Transactions) 所取得的防偽造成就，再造另一項非卡片提示類交易 (None-Card-Present Transactions) 防偽的機制，期望同時能達到避免未經授權使用持卡人帳戶資料，以及擴大規格適用範圍成為跨通路均能使用的作業標準)，以解決目前非卡片提示類交易，將信用卡資料留存於行動設備、交易過程傳送信用卡卡號等，所可能衍生的偽卡或盜刷等營運作業風險；Tokenization 與 EMV、Encryption 在卡片提示類交易與非卡片提示類交易的保護事項與控管機制，請參表 1。

表 1　EMV, Encryption, and Tokenization 交易資料防護機制說明

How EMV, Encryption, and Tokenization Protect Transactions

	Card-Present Transactions		Cord-Not-Present Transactions	
	Protects against:	**Using:**	**Protects against:**	**Using:**
EMV	Counterfeit cards	Card authentication	Not applicable. Can be used with separate reader, but not widely deployed.	Not applicable
	Re-using stolen data	Dynamic data		
	Lost/stolen cards (with PIN)	Cardholder verification (PIN)		
Encryption	Stealing data in transit	P2PE or E2EE	Stealing data in transit	P2PE or E2EE
	Stealing data at rest Re-using stolen encrypted data	Various methods of encryption	Stealing data at rest Re-using stolen encrypted data	Various methods of encryption
Tokenization	Stealing data in transit Stealing data at rest Re-using stolen data	Specific-use or limited-use token replacement for payment card data[31]	Stealing data in transit Stealing data at rest Re-using stolen data	Specific-use or limited-use token replacement for payment card data

資料來源：Smart Card Alliance

（二）流程控管機制

1. 代碼產製流程

持卡人將信用卡卡號 (PAN，Primary Account Number)，透過商店或電子錢包經由代碼請求單位 (Token Requestor，以下簡稱請求單位)，向代碼服務商 (依據 EMVCo 規劃是由 VISA、MasterCard、American Express 等卡片支付處理機構擔任，或由發卡銀行自建系統提供服務) 轉送經發卡銀行確認之持卡人資訊及卡片狀況 (Token Assurance (ID&V)) 後，依發卡銀行指示授權或拒絕發予持卡人代碼，再循原交易訊息路徑，透過錢包伺服器，將代碼傳送至持卡人行動裝置電子錢包系統，如圖 2 所示。

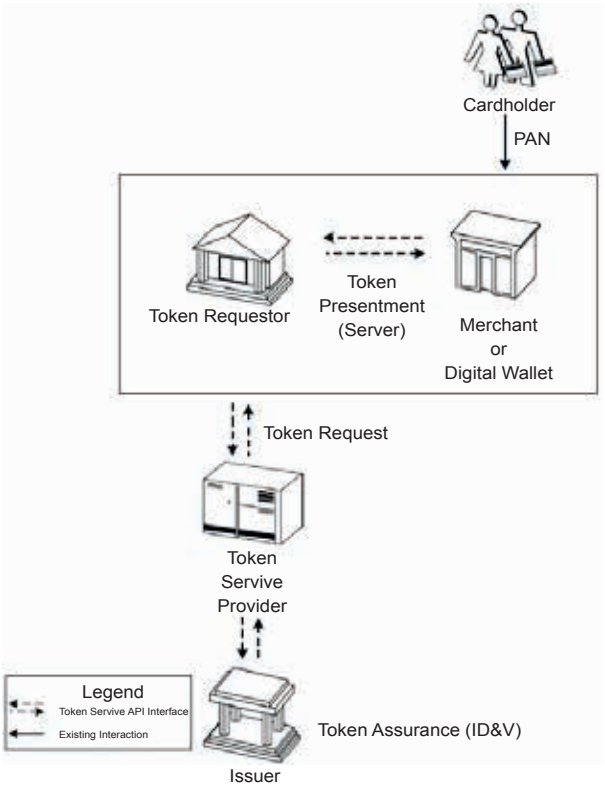

圖 2　支付憑證代碼產製流程圖

資料來源：EMVCo Tokenization Specification v1.0

2. 請求單位的註冊管理

依據前項代碼產製流程，持卡人透過請求單位向代碼服務商請求持卡人代碼，因此請求單位應如何管制，將是一項極重要之安全防護議題，依據 EMVCo 規範，申請成為請求單位者，應向代碼服務商遞送請求單位相關資訊、代碼使用控管方式及持卡人代碼賦予認證等級等三項資料，通過審核後，將取得一組請求單位代號 (Token Requestor ID)，作為後續相關代碼作業處理認證代號；如圖 3 所示。

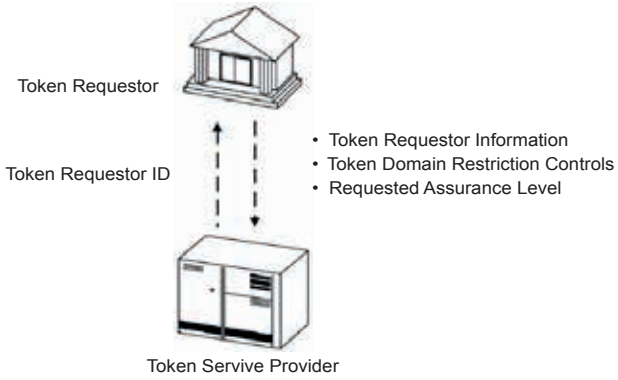

圖 3　支付憑證代碼請求單位的註冊管理流程

資料來源：EMVCo Tokenization Specification v1.0

（三）付款交易作業流程

當持卡人完成代碼產製及儲存程序，日後於商店購物選擇信用卡 (代碼) 付款時，透過行動設備電子錢包 (或網路交易商店) 送出代碼，商店循既有授權交易通路，將授權交易訊息傳送至收單銀行轉送跨行授權網路，由跨行授權網路將代碼轉請代碼服務商確認及回應代碼原信用卡卡號後，跨行授權網路將原信用卡卡號 / 代碼，轉送持卡人發卡銀行請求交易授權，發卡銀行確認持卡人相關認證及帳戶情形後回應結果，交易訊息及代碼再循原授權通路，反向回應給商店，確認交易付款是否成功；如圖 4 所示。

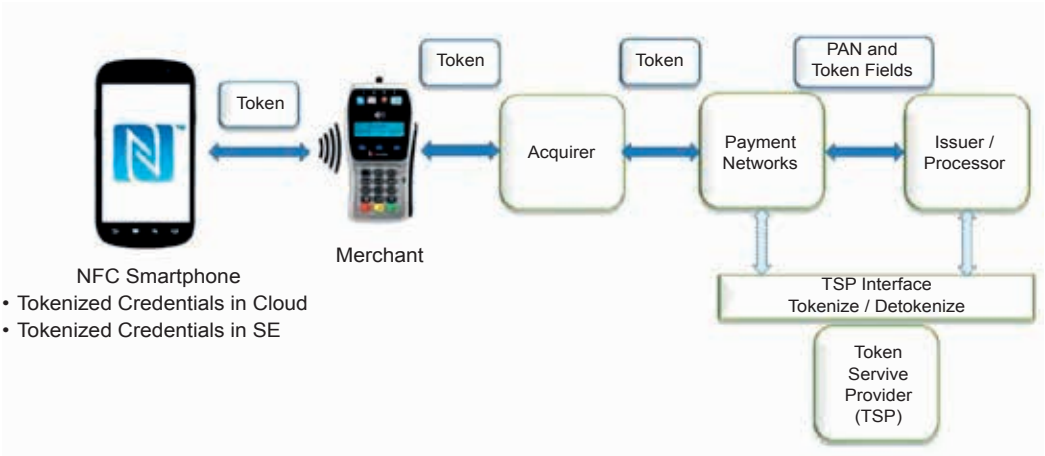

圖 4　支付憑證代碼交易作業流程

資料來源：Smart Card Alliance 網站

（四）交易授權訊息傳輸規格

1.　代碼傳輸方式處理原則

根據 EMVCo 代碼化規格訂定目標，以不增加額外資料欄位、不影響既有各國際組織卡片業務交易訊息標準及各單位已經規劃發展中的代碼產生規範為原則；各國際卡片業務組織可以其現有交易訊息規格標準套用，並於交易授權訊息傳輸過程中，以代碼資料取代卡號欄位；各發卡單位可依據其選用代碼服務商的模式決定賦予發卡銀行卡片識別碼 (BIN， Bank Identification Number)，作為判斷發卡銀行代碼處理中心之依據；因此可簡化代碼化相關資訊在交易授權訊息傳輸上之複雜性，降低各單位資訊系統配合異動之幅度。

2.　代碼傳輸保護機制

相較於以往 EMV 實體晶片卡處理卡片號碼等資料保護模式，依據 EMVCo 代碼化規格規範，無論在卡片提示類或無卡片提示類交易，除原卡號以代碼取代外，交易過程中之認證也由原來發卡銀行、卡片之驗證，改為代碼、代碼服務商及代碼服務商、發卡銀行間兩段式驗證模式；如圖 5 所示。

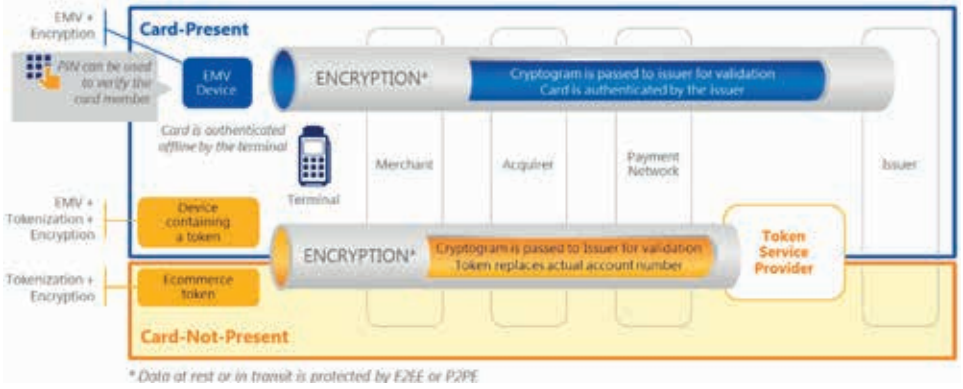

圖 5　EMV 卡片與支付憑證代碼交易模式作業流程

資料來源：Smart Card Alliance 網站

（五）代碼發行與控管機制

依據 EMVCo 代碼化規格發展方案，未來卡片業務發卡模式將朝一卡（帳戶）裝備、無卡片提示（或電子商務 EC 類）交易、QR-Code 支付類型交易、批次扣款或清算交易等，均使用代碼取代原信用卡卡號、授權交易訊息，並融合於各國際卡片業務組織 ISO8583 訊息傳輸標準中；因此，導入代碼化功能，收單銀行特約商店之刷卡端末設備，只要符合 EMVCo 晶片標準均可適用，無須特別配合修改，發卡銀行擇定代碼服務商作業模式後，只須小幅度修改與代碼服務商的代碼賦予及交易授權驗證系統訊息，即可快速提供代碼化作業模式服務；代碼化交易之作業流程及其與 EMV 卡片之發卡與交易處理差異，分別如圖 6 及 7 所示。

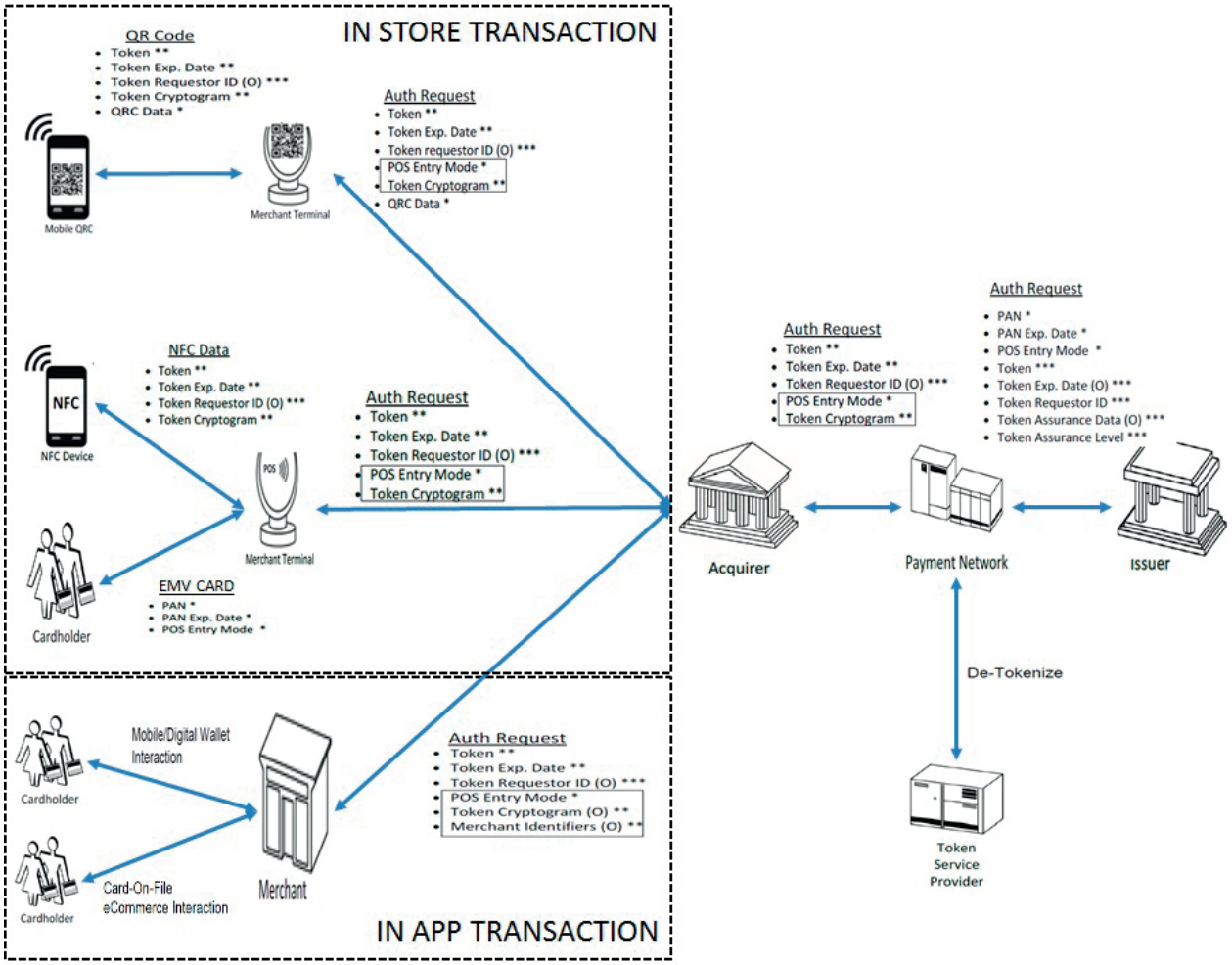

圖 6　支付憑證代碼化交易作業架構流程

資料來源：EMVCo Tokenization Specification v1.0

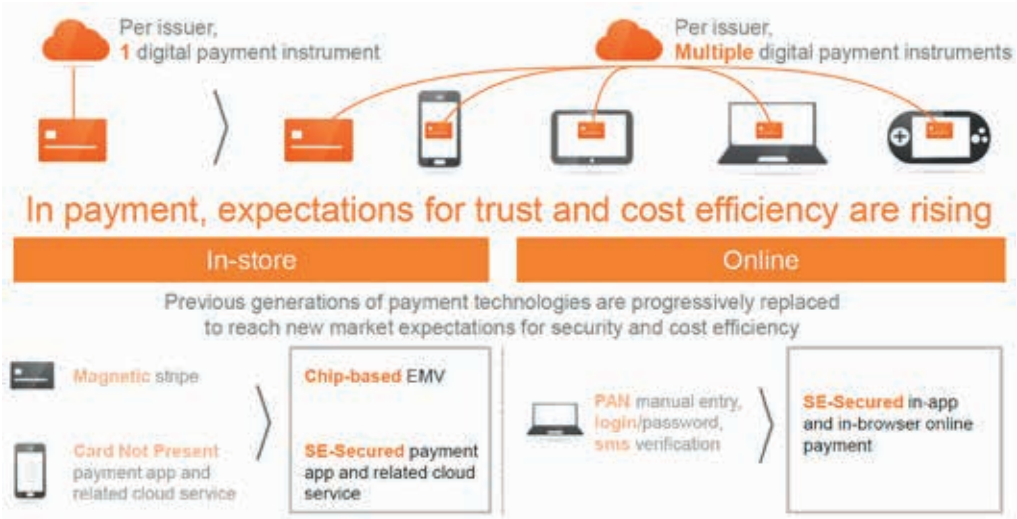

圖 7　EMV 卡片與支付憑證代碼交易模式之發卡與交易處理模式差異

資料來源：gemalto 公司網站

四、代碼化帶來的行動支付創新發展趨勢

近端 NFC 行動支付模式已明確成為主流發展標準，代碼化所造成創新之商業營運模式旋風，將更加速促進行動支付業務成功，謹就代碼化帶來的行動支付創新發展趨勢分析說明如下：

（一）代碼化具體實現

為克服卡片資料儲存與傳輸問題、提高行動支付交易環境安全，過去 VISA、MasterCard 及 American Express 三大國際發卡組織共同推動代碼化模式作業標準，但因全球信用卡晶片化不普遍、可受理晶片卡之商店設備不普及等，不利於代碼化模式發展的客觀環境限制，透過蘋果公司成功推動 Apple Pay 支付功能服務，美國在幾家大型商店配合辦理刷卡設備晶片化、500 大發卡銀行支持，成功營造出的行動支付環境，推出新一代支付憑證代碼化服務，獲得廣大消費者熱烈迴響，相信對於未來各國推動行動支付應有正面效果。

（二）代碼化簡化行動支付流程

除保障消費者交易環境安全外，創新支付工具能否成功的另一項重要因素，就是消費者使用的便利性。以往，行動支付模式作業繁瑣、複雜，而代碼化模式，持卡人無須到金融機構申請、換發任何設備或負擔額外花費，只須透過行動裝置幾項簡易操作流程完成服務啓動後，即可在各類網路或實體商店消費使用；代碼化仰仗其使用者操作的簡便性，對於提高消費者使用意願與消費感受體驗，以及未來成功推動行動支付業務，具有絕佳行銷效益。

（三）行動支付產業生態演變

催化支付業務能否蓬勃發展的主要動力，是產業生態各角色的分工合理及利益均衡，根據 EMVCo 代碼化作業模式規劃，未來代碼

化營運模式，將回歸由手機製造商 (如蘋果公司)、金融機構、信用卡組織所主導之模式，支付業務回歸支付產業機構，交易授權比照傳統模式，由商店、收單銀行、信用卡處理組織及發卡銀行所構成之支付體系處理，電信商在代碼化營運模式中，將回歸原資料傳輸角色；長久以來，關於信用卡資料儲存於通訊設備，所帶給金融機構與電信商間之困擾亦獲得解決。

(四) 資料儲存於實體晶片之安全性獲得肯定

NFC 手機支付模式發展過程中，普遍認為卡片資料儲存於硬體安全元件 (SE) 是較為安全可靠的做法，但由電信商所掌握之硬體安全元件，儲存金融機構卡片資料相關控制，其權益關係頗為複雜；其後由 Google 主導之 Android 手機體系，提出以 Host-based Card Emulation (簡稱 HCE) 概念之軟體方式解決硬體共用障礙，並在新版 Android KitKat 作業系統提供該項技術服務，HCE 技術架構固然解決 TSM 作業的諸多困難，也降低整體行動支付生態體系之複雜度，提供卡片服務供應商更多彈性空間，但是 HCE 以軟體儲存卡片資料，其安全受到嚴重挑戰；因此，代碼化非透過電信商控制，乃將代碼等資料儲存於硬體安全元件，因此一推出便快速獲得消費者肯定，相信將是非蘋果陣營未來推動代碼化成功的大助力。

(五) 代碼服務商的功能

代碼化之支付流程，將收單面與發卡面以信用卡卡號為基準的認證機制，改變為收單面的代碼、發卡面的信用卡卡號兩段式認證機制，透過中間代碼管理者 (代碼服務商) 進行兩方資料轉換及控管，因此代碼服務商所扮演的角色與功能至為重要，未來我們如果引進代碼化作業機制，應及早研擬規劃代碼服務商 (由各發卡銀行擔任、財金公司共用系統或國際組織提供相關服務) 的作業模式，以完備整體行動支付作業架構，確保業務營運順暢。

五、結語

Apple Pay 的成功推出已經證實代碼化模式之可行，未來預期將持續擴大行動支付之應用發展空間，因應創新技術引領各種不同的通路與支付模式發展趨勢，發卡銀行在資訊系統架構不變的情形下，將能更快速回應消費者需求，並且透過與代碼服務商合作模式，有效避免信用卡卡號等資料不當儲存或傳輸，降低營運作業風險。

再者，行動設備之發展日益蓬勃，行動支付也隨之多樣化，未來在代碼化技術發展帶動下，如何於交易安全與使用方便性間取得平衡，依然是推展行動支付服務之首要關鍵；而行動支付服務營運單位與金融機構之帳戶管理功能緊密結合的分工模式，將會是支付產業生態發展主流，妥善規劃行動支付分工作業模式，以確保行動支付交易安全、消費者權益、多方營運機構穩定獲利，成為行動支付穩定蓬勃發展的重要因素。因應國內支付產業生態之發展，財金公司、聯卡中心及票交所合資成立的臺灣行動支付公司，規劃採用 TSM 作業架構模式，整合信用卡、金融卡及相關支付帳戶作業功能，提供持卡人各種支付卡 / 帳號之遠端、近端支付服務，相信將可為我國行動支付產業與消費者，帶來全新不同的支付體驗與服務，值得各金融機構與商店共同參與推廣，以及早掌握行動支付業務發展契機。

※ 參考文獻 / 資料來源：

1. VISA 國際組織 (www.visa.com)。
2. MasterCard 國際組織 (www.mastercard.com)。
3. 蘋果公司 (www.apple.com)。
4. EMVCo (www.emvco.com)。
5. Wikipedia (en.wikipedia.org)。
6. www.customerthink.com。
7. www.gemalto.com。
8. First Annapolis Consulting, Inc. (www.firstannapolis.com)。
9. Android (http://developer.android.com/index.html)。
10. Smart Card Alliance (http://www.smartcardalliance.org)。