財金資訊

季刊精選集

財金資訊季刊 精選集

1998 年 12 月創刊

發 行 人／趙揚清
總 編 輯／林孟津
副總編輯／黃昱程
編輯委員／林國良　陳昌脩
陳柳元　陳明禮
徐憶玫　范姜群暐
蘇偉慶　廖君美
林弘斌　鄧介銘
馬德駿
執行編輯／綦聲聲

財金資訊股份有限公司
Financial Information Service Co., Ltd.

11485 臺北市內湖區康寧路三段 81 號
電話：886-2-2630-1234
886-2-2631-9800
傳真：886-2-2632-6296
www.fisc.com.tw

目錄

資訊應用篇

資訊安全篇

法令遵循篇

發行人手札

財金資訊季刊（前身為雙月刊，以下簡稱本刊）之發行，乃因本公司成立之初，網站技術未臻成熟，為推展業務，並增闢與參加單位間交流管道，爰創辦本刊，兼以建立本公司金融資訊之專業形象。

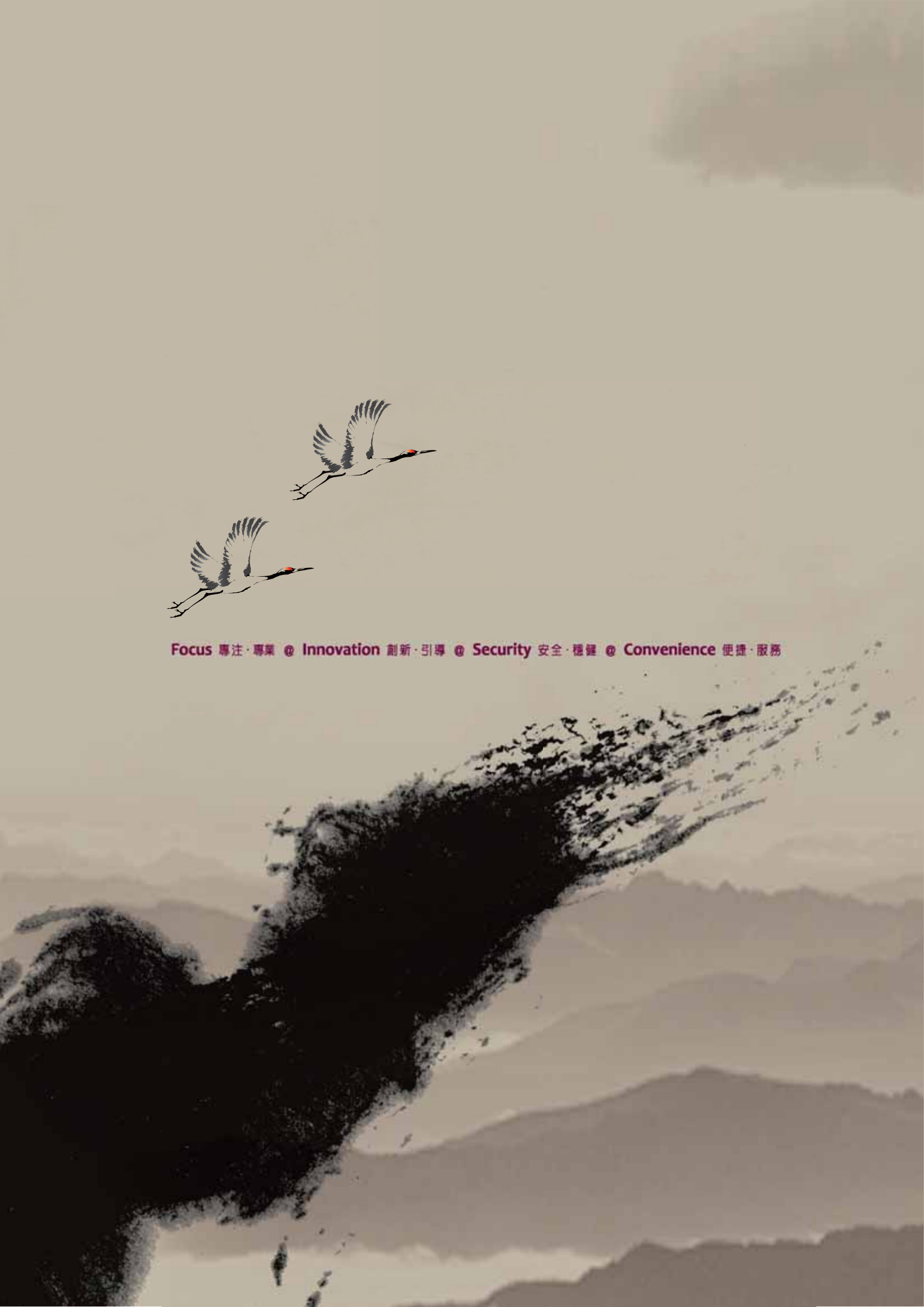
本刊於民國 87 年 12 月發行創刊號，承蒙時任財政部部長邱正雄提字祝賀，迄今已逾 17 年，期間為順應金融科技主客觀環境急遽變遷之需求，改以電子報及紙本出刊，截至 105 年 1 月止累計發行 85 期，所刊登文章計 933 篇。為利讀者閱讀，刊物內容之編排，依文章性質區分為企劃主題、資訊分享、業務宣導、活動花絮 / 紀實等四大面向，藉以傳達金融、資訊、安全等各類訊息，其中除有本公司同仁撰稿外，更廣邀相關業界執筆貢獻新知與分享經驗，以多樣化面貌及不同角度呈現刊物之深度與廣度，期與讀者分享。

本刊伴隨著本公司成長，扮演本公司與參加單位間之重要溝通管道。欣逢本公司發行「財金資訊 30 年紀念專刊」，為呼應「30」之主軸，爰以「電子金融」、「資訊應用」、「資訊安全」、「法令遵循」等面向精選 30 篇文章，彙集成「財金資訊季刊精選集」，以饗本刊讀者。未來，本刊將承續追求新知之風格，希冀提供更多元化的內容，服務更多關心金融科技發展的讀者。

發行人

趙揚清 謹識

民國 105 年 06 月


Focus 專注·專業 @ Innovation 創新·引導 @ Security 安全·穩健 @ Convenience 便捷·服務

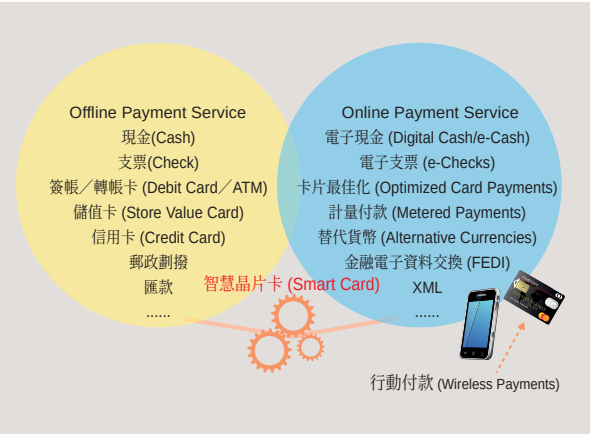
電子金融篇

金流服務的全球發展現況與趨勢

本篇摘自 2005 年 04 月出刊之財金資訊季刊第 39 期，由時任資策會網路多媒體研究所技術服務中心童啟晟經理撰寫。

隨著資訊科技的進步、網路的普及，電子商務在日常生活中扮演者日益重要的角色，尤在微利競爭激烈的今日，提供金流服務者已不限於金融機構，許多非金融機構跨足金流服務，因此，金融機構如何創新金流服務，訂定發展方針，將是未來創造營運利機的重要任務。

根據多項電子商務的研究報告顯示：全球電子商務市場遲遲無法有重大的進展與突破，消費者對於所謂的「金流服務」暨「付款機制」(Payment service & Transaction system) 的安全疑慮，一直是電子商務無法順利推展的重要原因。儘管如此，創新金流服務的提供，卻是電子商務生態環境中，最不可或缺的一環，因為只要人類有交易行為發生，最終都會有金流服務上的需求。本文將從全球金流服務的發展現況談起，進而觀察我國金流服務的發展趨勢，並剖析相關商機之所在。



圖一　金流服務的定義

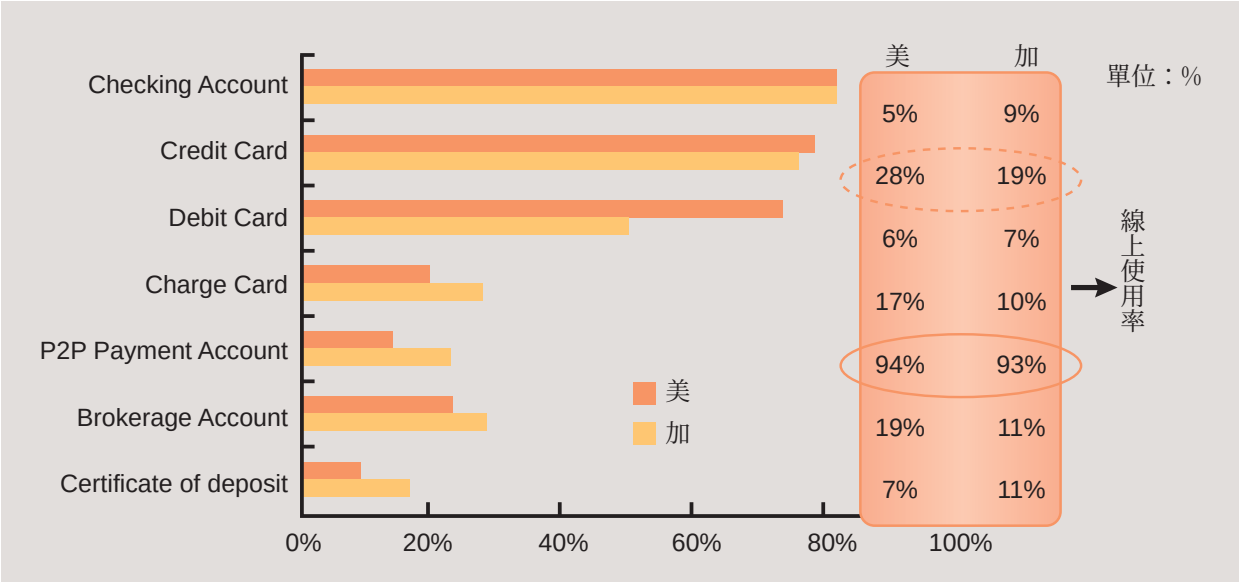
註：線上金流 (Online payment) 即俗稱的線上付款 (e-payment)

一、 全球金流服務的發展現況

（一） P2P 付款為 B2C 金流重要驅動力

個人對個人付款模式 (Person-to-Person；P2P)，已成為北美相當受歡迎的線上付款機制，在北美地區線上使用率超過 9 成（圖二）。

追溯 P2P 付款模式的成形，乃源於 1998 年底 PayPal 前身 X.com 所創，付款機制乃網友登入提供 P2P 付款模式的相關網站畫面後，只要輸入受款人 e-mail 與付款金額，就可以選擇在此 P2P 付款模式的帳戶完成扣款。由於顛覆了電子商務金流服務的傳統交易模式，提供快速而有效的付款機制，所以廣為市場接受，甚至已成為全球 B2C 金流服務發展的重要驅動力。



圖二　北美金流服務線上使用率

資料來源：Forrester

二、B2B 金流與產業供應鏈逐步串聯

根據美國普查統計局 (US Census Bureau) 的資料顯示，預估 2005 年北美資訊電子業 B2B 的交易量，將佔整體產業交易量的 10.1% 如（表一）。

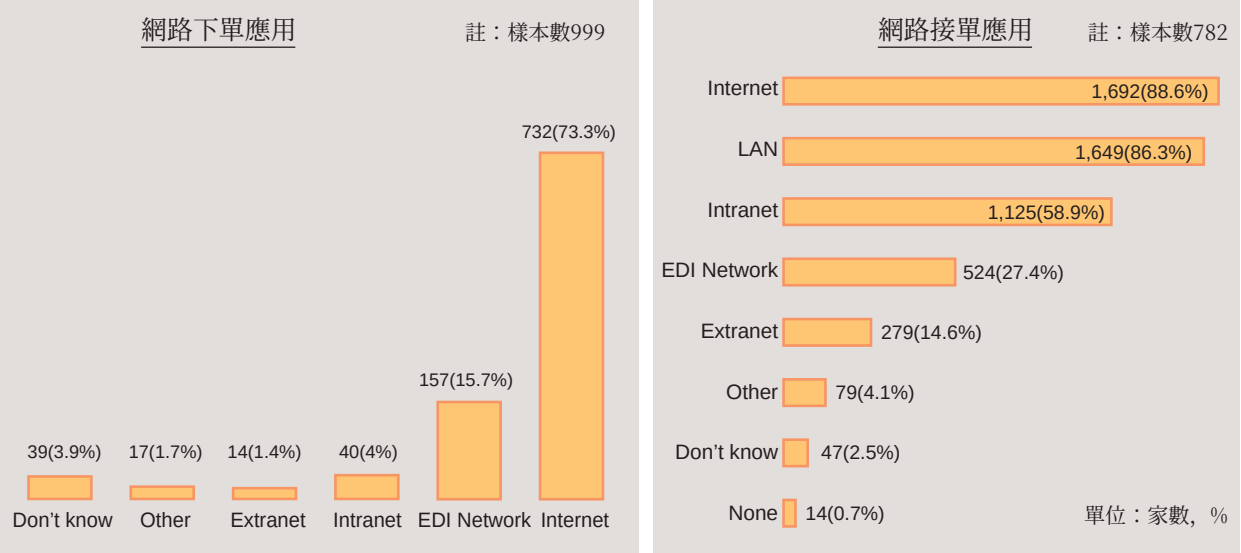
而資訊電子業在網路的應用上，則分別以 Internet(88.6%)、LAN(86.3%)、Intranet(58.9%)、EDI(27.4%)、Extranet(14.6%) 為主。在網路下單方面，以開放性的 Internet 應用家數最多，網路接單則以封閉式的 EDI 應用家數最多如（圖三）。過去企業習慣使用傳統的方式（例如：支票與信用狀）來進行交易，如今 Internet 讓相關的付款功能能更有效的傳遞，特別是將匯款資料（資訊流）與付款工具（金流）一同包裝，自動地將付款資訊整合到現有的 ERP 與帳務系統，然後再與整個產業的供應鏈逐步串聯，形成一個有效率的企業電子化金流付款環境。

表一　北美資訊電子業 B2B 市場規模

單位：10 億美元

	2001	2002	2003	2004	2005(e)
整體產業交易量	1,395	1,548	1,719	1,908	2,119
B2B(Internet) 交易量	47.75	79.77	121.21	167.55	214
B2B 佔整體交易量比例	3.4%	5.2%	7%	8.8%	10.1%

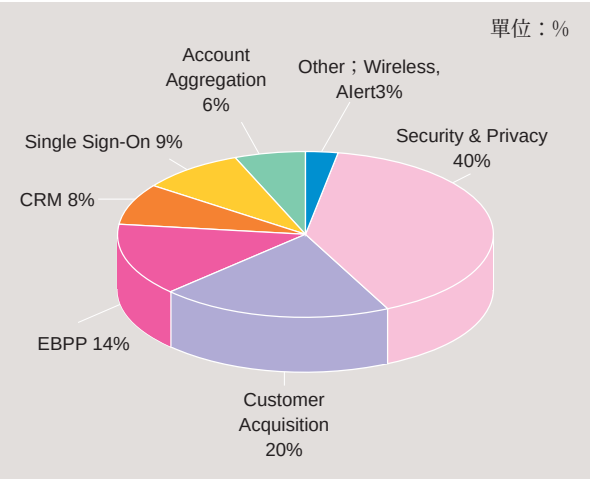
資料來源：US Census Bureau



圖三　北美資訊電子業網路下單與接單應用情形
資料來源：US Census Bureau 、eMarketer

三、EBPP 仍是銀行電子化的主要項目

電子帳單傳送付款系統 (Electronic Bill Presentment & Payment；EBPP) 已在北美推行多年且廣為各方接受，而 EBPP 的最大賣點即在於使用上的便利性，因為透過電子方式繳付帳單，除了將會自動更新消費者個人財務管理軟體中的資料，消費者更不需要打開信封、親手在支票上簽名、整理各種紙張紀錄，或者在所使用的財務管理軟體裡，再次輸入交易資料。Gartner 甚至指出，從 911 恐怖攻擊後的第一起炭疽熱案例以來，開始使用 EBPP 的機構數目增加了 20%，而相關金融機構也將 EBPP 視為銀行電子化的主要項目如（圖四）。



圖四　北美銀行電子化的預算配置
資料來源：Gartner

四、創新金流服務典範：PayPal 與 Paybox

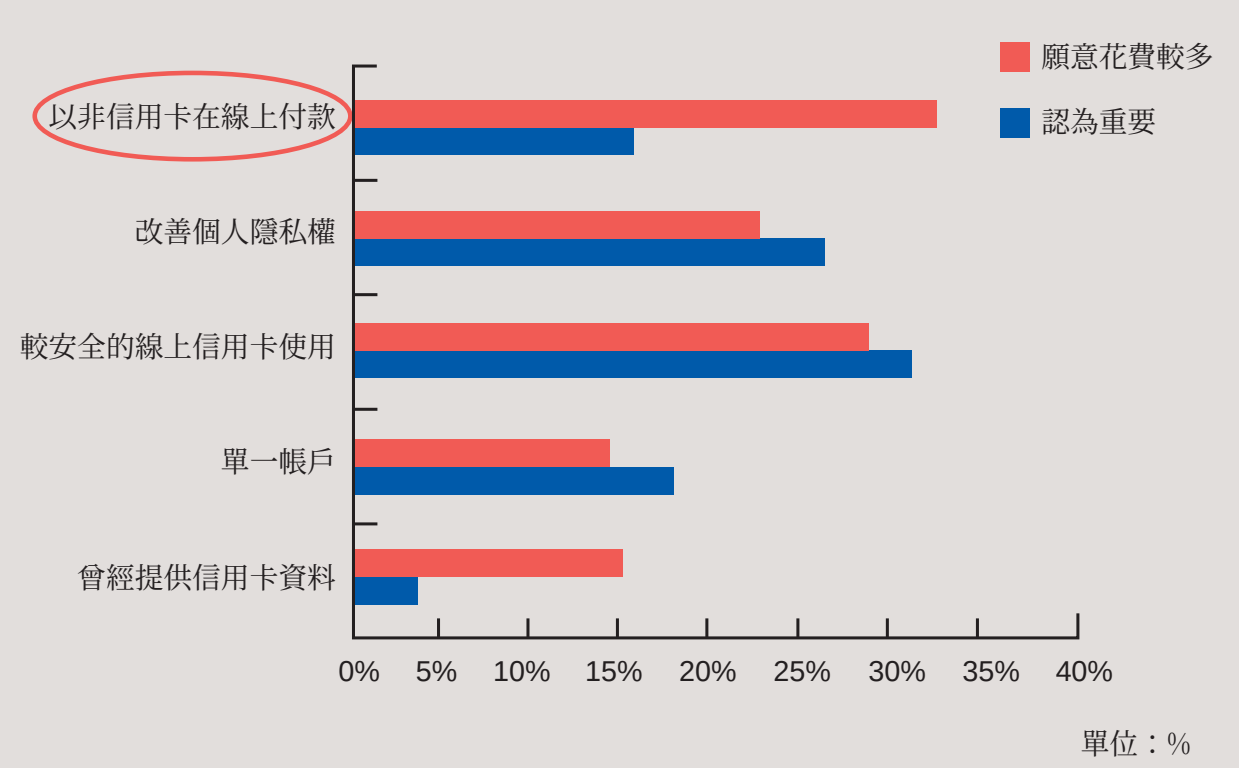
回顧全球金流服務的發展，則不得不提及兩個創新金流服務的典範，一個是在知名競標網站 eBay 大受歡迎，而後來亦順勢被 eBay 購併的 P2P 金流服務典範－ PayPal；另一個則是德意志銀行 (Deutsche Bank) 轉投資的 Wireless 金流服務典範－ Paybox。根據 Gartner 的 P2P 使用意識調查發現，有

高達 75% 的使用者，會在線上拍賣的網站付款；另一方面，由消費者在電子商店消費與付款的關聯性調查發現如（圖五），以「非信用卡在線上付款」最能讓消費者花費較多的預算，這也就是為什麼 PayPal 藉由 eBay 崛起，並以 email 方式傳遞付款訊息，成為「email Money」創新服務 Best Practice 的主要原因。

全球目前的手機系統業者紛紛透過手機，希望涉足金流服務並搶食相關商機，以歐洲為例，在西班牙有 Movilpago & Caixamovil，芬蘭有 SoneraMobile Pay，瑞典有 Mint，而這其中將創新構想發揮到極致的首推 Paybox。相較於 PayPal 利用 email，Paybox 則是將簡訊服務 (Short Message Service；SMS) 的功能加以發揚光大，而成為「SMS Money」的 Best Practice。基本上，Paybox 的付款流程是有別於 P2P 或計程車的行動付款模式，但這些金流服務有個共通的原則，便是不用輸入過多的個人資料，而以 Caller ID 來提高交易的安全性，完全打破舊有付款機制的交易思維，成為滿足消費者便利需求與金流服務機制的主流。

我國金流服務的發展趨勢

剖析我國金流服務的發展趨勢，有兩個重要的計畫：C 計畫與 IC 晶片卡換發計畫；以及與一個現象：虛擬貨幣顛覆 E 世代價值觀，特別值得觀察。



圖五　電子商店消費與付款的關聯性
資料來源：Gartner

一、FEDI 未來將漸被 XML 取代

過去幾年在台灣企業電子化的金流服務環境裡，金融電子資料交換 (Financial Electronic Data Interchange ；FEDI) 一直扮演著重要的開拓實驗性角色。已開辦 FEDI 作業之金融相關機構及參與的電子、資訊、汽車、貿易、醫藥、金融理財等各行業更超過 4,000 家以上，也因此造就培養了許多本土資訊服務業者在 FEDI 建置導入與系統整合的專業服務技能。然而隨著開放式環境的來臨，導入成本較高且專屬封閉式的 FEDI，已漸漸無法滿足企業電子化金流服務的需求，FEDI 未來勢必將逐步被 XML 取代。

有鑑於此，財政部請銀行公會邀集各會員銀行及財金公司，共組「電子商務金流作業研究暨推動專案小組」，積極規劃推動國內電子商務金流作業，並陸續完成國內金融業網際網路 XML 訊息標準之訂定，以及國內金融機構間透過網際網路進行跨行（銀行與銀行間）之資金移轉作業；另計畫於五年內輔導五萬家廠商建立金流自動化之能力為目標。並已於之前啟動「以 XML 為基礎之金流基礎建設 (Interbank Common Platform ；ICP) 計畫」，而此計畫也正是後來以串接「全球運籌體系」與 A、B 計畫為目標－ C 計畫的濫觴。

二、電子商務的催化劑－ IC 晶片卡

信用卡的安全問題，一直被視為電子商務無法推展的主要障礙之一（台灣信用卡盜刷量亦高居全球之冠），因此各種更為簡易、更具彈性、並可替代信用卡的付款機制便隨之產生。目前市場上的卡片（塑膠貨幣）業務，就付款時間以及付款金額區分如（表二），大致可分成三類：儲值卡 (Store Value Card)，亦稱為電子錢包 － 預付，付款金額約從新台幣 0-499 元；簽帳卡 (Debit Card) －現付，付款金額約從新台幣 500-2,000 元；信用卡 (Credit Card) － 後付，付款金額約在新台幣 2,001 元以上。

而凡是在此三種卡片內嵌 IC Chip，便可通稱為 IC 晶片卡或是智慧卡 (Smart Card)。過去由於磁條卡成本低，但相對的因為容易被偽造與盜刷，的確對電子商務金流發展造成一定程度的傷害。而 IC 晶片卡由於具有較高的保密性、可儲存性以及可程式性 (Promgramming)，對電子商務的技術安全提供了多一層的保障，並可消弭部分消費者對隱私與安全的疑慮，因此被認為是加速電子商務金流服務市場發展的重要利器。

表二　各種卡片業務比較

卡片種類	儲值卡 （又稱電子錢包） Store Value Card	簽帳卡 Debit Card	信用卡 Credit Card
付款時間	預付（Before）	現付（Now）	後付（After）
付款金額	NT$ 499 以下	NT$ 500~2,000	NT$ 2,001 以上

資料來源：III

三、虛擬貨幣顛覆 E 世代的價值觀

線上遊戲的興起，是近年來資訊服務業的大事，其藉由遊戲中的互動與族群匯集的效果，的確為整個數位內容產業增添許多創意與活力，但其所引申的許多問題與現象，卻也是改變電子商務金流服務模式的重要關鍵，特別是虛擬貨幣的產生，徹底顛覆了當下 E 世代的價值觀。以著名的線上遊戲－「天堂」為例，其虛擬貨幣－「天幣」，不僅成為社會新聞中相關犯罪的話題（如網路遊戲「天幣」遭竊、謊稱買「天幣」擄走網友、暴力搶奪「天幣」四嫌移送法辦等），更有部分 E 世代以「天幣」兌換「新台幣」，作為謀生工具，讓「天幣」不僅在虛擬世界可以流通，甚至漸漸在貨幣交換市場有交易行為發生。

我國金流服務的商機剖析

一、以 XML 為基礎的 SOA 架構將成主流

以 XML 為基礎之金流基礎建設計畫作業，包括全球收付款、帳戶整合、融資等功能模組的建置，並以導入產業運籌體系為目標。所以未來除了以 XML 為基礎的「服務導向架構」(SOA；Service-Oriented Architecture) 將成市場主流外，其對於金流服務所創造的商機更包括一：1.EDI 的替換（從 FEDI 替換成 XML，指銀行端與供應商客戶）；2. 付款閘道 (Payment Gateway) 的建置；3. 各供應商 ERP 財務模組的更新。

二、IC 晶片卡換發計畫衍生之商機

分析 IC 晶片卡市場，可將之區分為卡片與卡片上的作業系統與應用 (OS/Application)，以及讀卡設備等三個區隔。但在這個市場裡，專業服務與系統整合服務商多半是引進，或代理歐美的先進技術與解決方案為主如（圖六）。所以在進軍有關 IC 晶片卡標案的系統建置上，資訊服務商多半採取策略聯盟或專案統包的方式，因此，處處可見國際合作的經驗。以近來銀行公會訂定 IC 金融卡的換發計劃為例，其衍生的商機，包括 IC 金融卡片、通路（PCbased IC 卡讀卡機、商家系統讀卡機、企業儲值卡端末設備、ATM 升級等）與後台各項系統整合（銀行後台系統升級、個人化服務等）商機。

三、等待金流服務的果陀

迄今國內市場上 IC 晶片卡所提供服務對象最多的三種卡片，分別是神通集團提供專業服務與系統整合的「台北捷運悠遊卡」、東元集團提供專業服務與系統整合的「國民 IC 健保卡」、宏碁集團與 Master 合作的「Mondex 電子現金儲值卡」（可使用於包括台灣大車隊、萊爾富超商、公益彩券投注站、大專院校等管道）。其中捷運悠遊卡屬於非接觸式卡片，具有儲值卡功能；國民 IC 健保卡，初期以身份辨識與資料儲存功能為主，未來亦朝向儲值卡功能發展；Mondex 電子現金儲值卡則是定位為小額付款的金流服務，同時具有儲值卡與信用卡的功能。然而以上三種卡片背後的資訊服務建置商，對於商機的窺探，絕不僅止於部分身分註記或資料儲存的功能提供而滿足，三大集團其實都在等待相關法令開放之

前，做好 IC 晶片卡各項系統整合的準備，並能師法香港「八達通」的經驗，全力搶食金流服務的 Payment 商機。

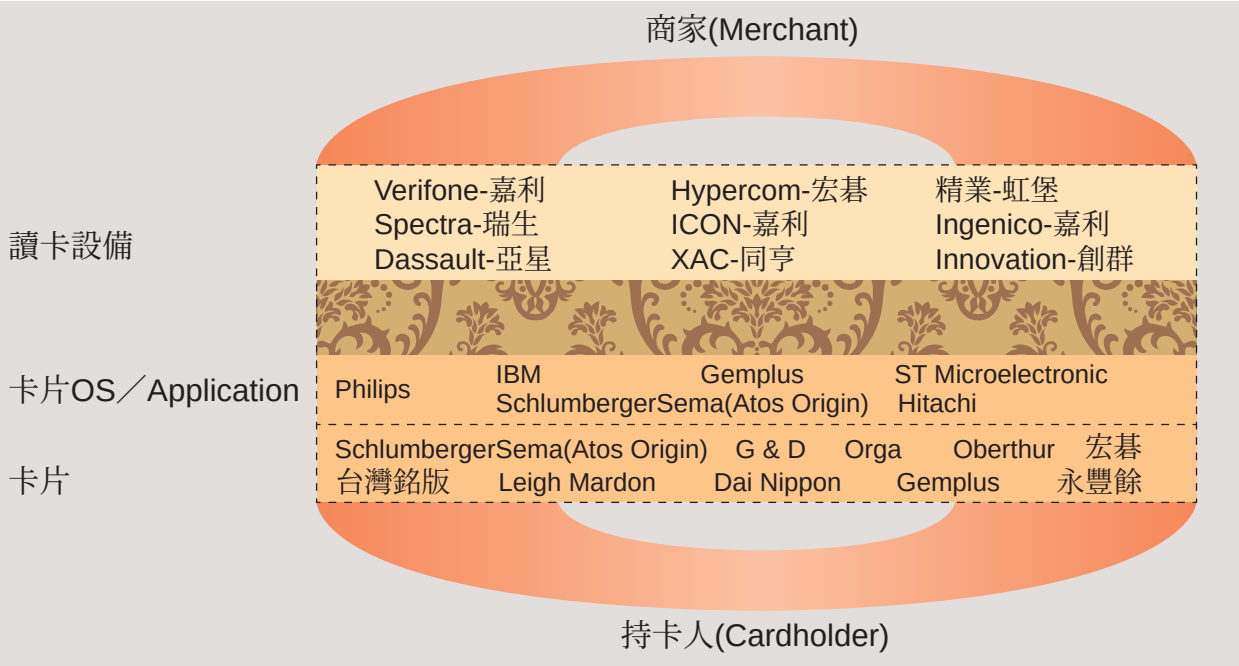
結論與建議

一、零售通路與電信業者對傳統銀行的威脅

提供金流服務不再是傳統金融服務業者（銀行）的專利，各方勢力的投入已經是大勢所趨，包括一些新進入者 (New Player) 如：零售業的 7-11、Tesco、汽車業的 BMW、VolksWagon、電子消費品牌 Sony 等為代表。以及利基業者 (Niche Player) 如 GE、AE、e*Trade、Fidelity 等為代表。其他產業如：多數的大哥大業者，及 ERP 業者的 PeopleSoft、SAP。因此傳統金融服務業者必須提供更多創新的服務，方有可能在金流服務市場立於不敗之地。

二、虛擬貨幣顛覆 E 世代的消費能力與行為

線上遊戲的虛擬貨幣除了改變原有電子商務的金流服務與付款機制，並將徹底顛覆了當下 E 世代的價值觀，實為所有金流服務業者當注意觀察的現象。



圖六　IC 晶片卡市場競爭態勢

資料來源：III

三、 未來二年是 XML 商機與 B2B 發展的關鍵

特別是以 XML 為基礎的「服務導向架構」(SOA；Service-Oriented Architecture) 之相關金流基礎建設，將影響國內企業電子化金流服務的關鍵發展。

四、 IC 晶片卡將影響國內電子商務相關應用

IC 晶片卡對電子商務的技術安全提供了較多的保障，並可消弭部分消費者對隱私與安全的疑慮，因此被認為是加速電子商務金流服務市場發展的重要替代工具，也必將是各方勢力競逐的市場。

五、 政府需主導金流服務已形風行草偃之效

相較澳洲政府的主動，與日本、美國的各種公協會藉由集體的力量主導金流服務與付款機制、標準的制定，我國政府在市場自由競爭與政策主導上，似乎陷入了兩難的境地，因此積極的介入，為相關業者找出方向，應是目前政府對金流服務應有的作為。

小額線上付款機制之發展趨勢

本篇摘自 2004 年 12 月出刊之財金資訊季刊第 37 期，由時任銘傳大學財務金融系張幸惠副教授撰寫。

網際網路與加密技術的發展促使電子商務的盛行，其中針對 B2C 與 P2P 電子商務金流有各種小額付款機制的推出。小額線上付款機制是由支付工具 (payment instruments) 與網路系統 (network) 所構成；支付工具可以利用原本存在的現金、存款、支票、信用卡、預付卡等，或者完全新創一種支付工具，例如：數位現金 (digital cash)，或者結合固網或行動電話的帳單付款方式。而利用加密技術，網路系統可以是完全或半開放性，至少在使用者端可以直接經由網際網路完成付款程序。本文將針對小額線上付款機制的發展趨勢，並透過記憶式資金移轉系統與電子貨幣的區別，說明小額線上付款機制的金流本質。

小額線上付款機制的發展趨勢

根據 2002 年中華民國電子商務年鑑，對台灣地區線上付款方式所做的統計，付款方式包括：ATM 轉帳、郵政劃撥、貨到付款、超商代收、支票 / 現金袋、信用卡傳真、信用卡 SSL 加密、信用卡 SET 加密及其他如 (表一)。其中 ATM 轉帳的支付工具是存款；郵政劃撥、貨到付款、超商代收的支付工具是現金。而不管是信用卡傳真、信用卡 SSL 加密、信用卡 SET 加密，其支付工具都是信用卡；但消費者於帳單到期時，最終須以現金或存款轉帳方式支付。因此，真正具有結清債權債務關係的支付工具是央行現金與銀行存款。

上述的 ATM 轉帳、郵政劃撥等付款方式，買方在網路上完成訂購手續後，通常被要求先至金融機構完成付款程序，再度上網通知賣方該筆款項已匯入其帳戶，待賣方確認後才進行物流程序，因此實際上並未達到電子商務所強調的資訊流、金流與物流一氣喝成的交易效率，因此設計一套不需中斷交易程序的線上付款機制有其必要性。綜合目前的各種小額線上付款機制的發展趨勢，所採用的支付工具主要可以歸納如下：

一、信用卡的延伸

即所謂的網路信用卡，消費者直接在網路上輸入卡號，完成付款程序。主要採用加密技術，以電子簽章作個人身份辨識和訂貨資訊加密，以保護個人隱私。例如：信用卡 SSL 加密、信用卡 SET 加密，目前也推出信用卡 3-D Secure。

表一　網路消費者付款方式

	ATM 轉帳	郵政劃撥	信用卡 SSL 加密	信用卡傳真	貨到付款	超商代收	支票 / 現金袋	信用卡 SET 加密	其他
2001	60%	56%	52%	46%	30%	22%	10%	4%	10%
2002	23%	19%	50%	20%	43%	52%	20%	5%	12%

資料來源：2002 年中華民國電子商務年鑑

二、支票的延伸

由於支票的清算成本相對較高，以改善支票處理效率的實驗相當多，美國聯邦準備銀行、銀行產業積極將支票交換過程電子化，其計畫成果稱為電子支票提示 (ECP)。而台灣的電子票據也已正式上路，但因國人對於小額交易並不習慣使用支票，因此主要應用在 B2B 電子商務上。

三、預付卡的延伸

即所謂的電子現金 IC 儲值卡，內建的 IC 晶片具有儲值功能且不易被偽造；IC 卡可視為電子錢包，利用相對應的機器補充卡內的現金；目前發展方向是一卡雙用，同時可在實體與網路商店使用，例如：Mondex 卡。此外，同屬預付卡的延伸，但只限於單一網站使用，例如：中華電信的預付卡。不管是像 Mondex 這種品牌預付卡或單一網站預付卡都可以方便無法或不想以信用卡在網路上消費的族群。

四、現金的延伸

即發行網路型電子現金，其材質非紙張或其他實體東西，而是一連串 0、1 數碼所構成。此類型支付工具完全採用網路系統，以電子化執行現金支付清算，由於可以相互支付清算，故可保有使用者的隱私權，如同現金不以個人信用為前提，即時進行支付，例如：Digicash，但該公司已在 1998 年宣告破產。

除上述的小額線上付款機制外，值得提出的是由電信公司所推出的電話帳單方式，通常是在其所設的網站上，允許消費者的線上消費以每月電話帳單方式付款。至於，電信公司推出利用具備電子錢包功能的行動電話付款，例如：日本的 DoCoMo 推出 I-mode Felica 手機，由於內建的記憶晶片具備電子錢包功能，可於購物後支付帳款。這種付款機制仍屬於預付卡的延伸，但應用在行動電子商務上。

電子貨幣

小額線上付款機制中，有些是現有的付款方式應用在網路上，例如：網路信用卡、電子支票，而電子現金儲值卡與電子現金依目前的設計需事先儲值才能消費，但利用加密技術確實可以做到具匿名性，如同現金交易。但小額線上付款機制中，哪些才是電子貨幣？哪些只是記憶式資金移轉系統 (Notational Funds Transfer System; NFTS)，由於意涵不同，推動的成本也大不同，故有必要加以區別。

依據狹隘的貨幣供給定義，貨幣是指央

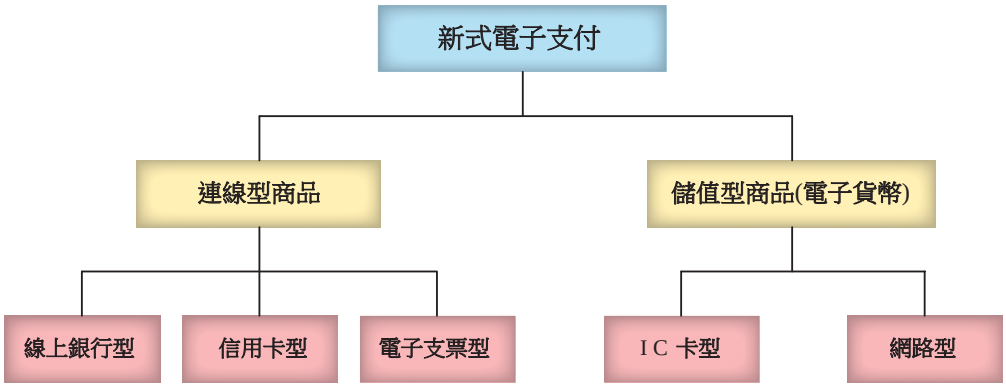
行發行的現金與銀行存款。以支票、信用卡付款，最終仍須經由封閉性的銀行網路 (bank net) 移轉銀行存款作結算、清算 (clearing and settlement)；因此支票、信用卡不是貨幣，只是支付工具之一，屬通路產品 (access products)。根據日本電子支付清算研究會 (1996) 對電子貨幣的定義，電子貨幣是經由開放性網際網路移轉資金，達到支付清算目的的交易媒介，同時具移轉性、匿名性與相對性，即電子貨幣是經由網路等方式，移轉其電子性的價值 (移轉性)，支付隱私不會被賣方、金融機構所得知 (匿名性)，交易時除買方與賣方雙方外，無第三者介入 (相對性)，而電子支付清算是上述三種特性有一項未被滿足。

此外，根據日本銀行所舉辦的「電子支付技術與金融政策操作相關性之研討會」的期中報告 (1996)，將電子支付手段分成連線型商品與儲值型商品；連線型商品不管是線上銀行型、信用卡型與電子支票型，皆須透過銀行存款做最後的結清；前半段交易，使用者可以透過網際網路直接付款，但後半的支付流程與原來封閉性銀行間的清算一樣，因此不認為這類型的新式電子支付是電子貨幣，只有儲值型商品包括 IC 卡型與網路型才屬於電子貨幣如 (圖一)。

目前儲值型商品仍必須以現金、存款交換電子價值，作為發行電子貨幣的前提，這並非是架構與技術上的限制，而是目前一般接受度仍低，加上金融管制等因素，故以現金、存款交換電子貨幣。此外，儲值型商品採分散處理架構，消費者間或消費者與商店間進行電子價值的讓渡時，並非採集中處理方式，而是利用 IC 卡、網路系統，採分散化處理的架構，因此讓渡後的電子價值不須回流發行機構，具有現金性質。採分散化處理可以降低交易成本，轉嫁至商店的手續費也相對降低。

記憶式資金移轉系統

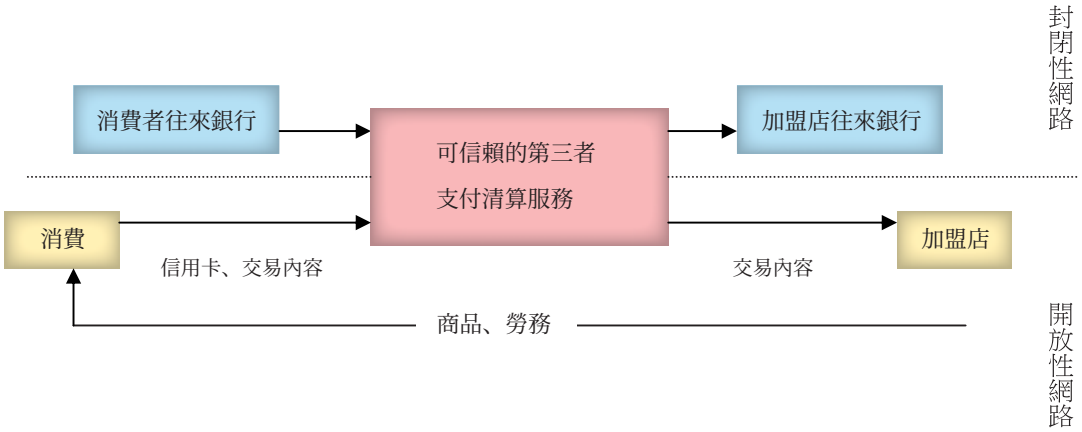
記憶式資金移轉系統是以支票或信用卡為基礎的線上付款機制，即 (圖一) 所歸類的連線型商品，其與傳統的電子資金移轉系統 (Electronic Funds Transfer System; EFTS) 不同；傳統的 EFTS 完全在封閉性網路內進行結算、清算，偏向於批發性資金移轉，而記憶式資金移轉系統已屬半開放性網路，可以將付款訊息 (信用卡號、銀行帳號等) 與訂單一起傳送，並延伸電子資金移轉系統的優點於小額交易上，改善消費者與商店的交易效率。



圖一　新式電子支付分類

資料來源：「電子支付清算技術與金融政策操作相關性之研討會」(1996)

(圖二) 是記憶式資金移轉系統的操作模式，使用者可以直接連結網路商店進行交易，傳送訂單、卡號資料，但是後續的結算、清算動作仍在封閉性網路內進行，故整個交易完成是橫跨開放性與封閉性網路。而可信賴的第三者 (trusted third party) 通常是指財務價值鍊服務供應商 (Value-Chain Service Providers)，這些供應商利用其在資訊科技的優勢，設計一套線上付款機制，提供支付清算服務，是金融業者的競爭合作對象。



圖二　記憶式資金移轉系統

根據 (表一)，顯示信用卡使用頻率確實相對較高，這與消費者已熟悉該商品有關，但以信用卡作線上付款，除安全性較受爭議外，仍有二點值得注意的；一是對於極小額的線上消費，例如：一篇文章、一首歌的下載，由於信用卡手續費相對較高，並不符合網路商店的成本效益，故有必要推出低手續費的小額線上付款機制，以吸引網路商店加盟。其二，對於並未持有信用卡的青少年族群，有必要發展一套適合他們使用的付款機制。

結語

小額線上付款機制不斷的推陳出新，有些屬於技術面創新，例如：加密技術應用於信用卡、支票；有些是結合技術面與管理面二種，例如：網路型電子現金、電子現金儲值卡；而有些則屬於金流管理的改良，將原有的付款方式包裝成一新的付款機制，以順利解決網路金流問題，例如:電話帳單方式。但根據貨幣觀點，網路型電子現金、電子現金儲值卡是可能觸及管制者神經的準貨幣產品，需要相關業者與政府間的協調，其在推動的過程相對繁瑣，而利用現有的支付工具應用在網路上則相對簡易。

自 1990 年代後期以來，各種小額線上付款機制不斷實驗，但也不斷失敗，其中相當大的原因是繫於使用者是否達到一定的量，而使用者 (買賣雙方) 接受與否，主要關鍵在於安全與簡便。有些小額線上付款機制的推展並不順利，主要是簡便上無法符合使用者的期望，以致使用者數無法達到一定的臨屆量，而網路信用卡在信用卡已廣被接受下，似乎有較大的優勢，但如何說服使用者其安全無虞，目前仍是一大挑戰。

電子銀行之趨勢與展望

本篇摘自 2004 年 04 月出刊之財金資訊季刊第 33 期，由時任國立政治大學資訊管理系曾淑峰副教授撰寫。

對銀行而言，透過電子銀行服務可以減少設立分行成本，將銀行服務由被動等客戶要求，轉為主動服務客戶，提昇行銷能力，並可使銀行經營結合其它商務活動，擴大業務範圍，使資金與資訊加速流通。

電子銀行是一種可以不須經由銀行櫃員之手，由客戶利用既有之電腦設備，配合金融應用軟體與通訊設備、通訊網路軟體等，即時享受銀行所提供之各種金融資訊及資金撥轉等服務，達到在家庭或工作場所即可享受銀行服務之便利性。

早期國內電子銀行的作業項目主要以財金公司 (原財政部金資中心) 推出的跨行系統為主，包括自動櫃員機作業、通匯作業、資訊查詢作業、銷售點服務作業、金融 EDI 作業等；還有各銀行因應客戶遠端服務需求而推出的電話銀行、企業銀行、家庭銀行、網路銀行、行動銀行等。近期國內活絡的電子銀行發展則有經濟部技術處推出的金流電子化計畫 (C 計畫)，重點在於將金融體系之金流服務與既有之電子化供應鏈接軌，以延伸並深化產業鏈之運作效能。

另一方面，台灣近年來金融機構併購與控股公司的形成造成金融機構重新洗牌，提供整合性入口網站以提供多元化的金融服務，也成為電子銀行發展的新焦點，相關的安全控管、共用平台及人才升級都是搭配業務發展，成就新一代電子銀行發展的基礎建設所需。

財金跨行資訊系統

一、 自動櫃員機

自動櫃員機 (Cash Dispenser/Automatic Teller Machine； CD/ATM) 作業是以金融單位發行之金融卡，在自動化設備上進行存款 / 提款 / 轉帳交易之作業，利用電腦提供 24 小時全天候的服務，是銀行櫃台作業的延伸，系統的可靠性、可使用性、服務性等特別重要。

二、 通匯作業

通匯作業 (Remittance System)，是客戶委託銀行將資金解付指定收款人及收款帳戶的作業，包含託收、匯兌、支付、同業資金撥轉等作業系統，每筆交易的金額比 CD/ATM、EFTPOS 交易高出很多，所以安全問題顯得更加重要。自動櫃員機與通匯為最早在金資網路開發的電子資金撥轉 (Electronic Fund Transfer；EFT) 應用系統。

三、資訊查詢作業

資訊查詢作業 (Credit Information System) 是提供客戶或銀行，有關票據退票、票據信用、徵信資料及通關資料等金融資訊查詢的服務，不涉及資金的撥轉。銷售點服務作業 (Electronic Fund Transfer Point Of Sale；EFTPOS)，是提供持卡人在特約商店消費後，利用電子資金撥轉 (EFT) 的方式，由金融機構整批轉帳以代扣消費帳款、代收帳款之服務，其安全性須考慮交易的認証性、交易的隱密性以及交易的正確性。

四、電子資料交換

電子資料交換 (Electronic Data Interchange；EDI) 是利用共通的交換標準，使電子文件在各相關單位間相互傳輸，用來解決企業間商流、物流及相關的資訊流之交換作業。而與金融相關的交易活動，如匯款指示、入扣帳通知等，其中必牽涉到資金的移轉 (如匯款金額) 與相關資訊（如發票號碼、匯款通知、或其他明細資料) 的傳輸，則藉由金融電子資料交換 (FEDI) 的作業方式來處理。國內已開發的 FEDI 系統有：貨物通關 EDI 稅費支付系統，貨物通關 EDI 稅費支付加值系統，商業 EDI 電子轉帳系統，金融 EDI 付款系統，金融 EDI 信用狀作業系統等。近年來由於網際網路應用的漸趨普及，EDI 相關作業也逐漸使用網頁技術作為前端處理介面，逐漸由專屬的加值網轉移到開放的網際網路上，資料交換格式的轉換則改用 XML(Extended Markup Language)。

遠端銀行服務

一、電話語音

電話語音可說是首先將銀行的服務延伸至客戶端，雖然所提供的服務有限，但這種服務標示一個新的趨勢，使銀行重新定義傳送服務的通路，進入 Delivery Any Time、 Any How & Any Function 所謂的服務新紀元。近年來的電話語音服務更進一步與人工櫃員服務作彈性結合，提供多元化且高品質的電話中心 (Call Center) 服務，正在各銀行如火如荼的規劃及佈署中。

二、企業銀行

企業銀行 (Firm Banking) 是以公民營企業機構為對象所建立之各種金融服務系統，包括：企業理財資料管理、客戶金融資訊通知，企業與銀行電子郵件溝通、企業銀行客戶之財政務部門人員帳務交易、基本金融資訊、理財諮詢、財經諮詢資訊查詢。

三、家庭銀行

家庭銀行 (Home Banking)，或稱個人銀行 (Personal Banking)，則是一種讓客戶坐在家中，也能得到銀行各種金融服務的業務，包括：金融商品介紹、付款、轉帳、匯款、查詢餘額等，進一步的理財分析（買賣股票、債券等）、金融市場脈動及資訊之查詢、消費顧問、資產諮詢、融資貸款等服務，以及提供銀行與客戶雙向溝通橋樑的電子郵件等。早期企業銀行、家庭銀行服務系統是透過專線或撥接線，將企業銀行的主機或 PC 與銀行主機連線，提供營業時間內或 24 小時的服務，目前已經轉移到網際網路上。

四、網際網路銀行服務

早期的電子銀行服務內容與形式比較有限，至網際網路興起，配合電子商務的發展，電子銀行服務產生革命性變化，「網際網路銀行服務」應運而生，使客戶透過網際網路瀏覽器，上線進入銀行網站，即可享有各種銀行服務。銀行與客戶溝通的系統由封閉轉為開放，透過網際網路無遠弗屆的特性將服務延伸至顧客所在地，自動化設備也逐漸由 CD/ATM、EFTPOS 延伸到電話、個人電腦等開放設備。

銀行的服務由原有固定點的分行、櫃員機、無人銀行等擴大到透過四通八達的網際網路，對客戶提供更快速便捷的服務，有即時處理、不受時空限制、自主性與隱密性提高等優點。對銀行而言，透過電子銀行服務可以減少設立分行成本，將銀行服務由被動等客戶要求，轉為主動服務客戶，提昇行銷能力，並可使銀行經營結合其他商務活動，擴大業務範圍，使資金與資訊加速流通。由於個人電腦日益普及，使用電腦進行交易的常識與意願增加，而且網頁技術成熟，簡單易學，親和力高，使得交易進行便利。

在無線通路方面，客戶可以透過手機或 PDA 接受行動銀行服務，進行查詢、交易、主動通知等業務，交易流程可在無線設備螢幕上顯示，不需聽取冗長的語音引導，操作流程表單化、選項化，交易進行可以輕鬆愉快。

C 計畫電子金流服務

繼「推動資訊業電子化計畫」(即 A、B 計畫) 成功協助國內資訊業者建立電子化供應鏈體系後，經濟部技術處於 2002 年開始進一步推動金流電子化計畫（C 計畫）。參與 C 計畫之銀行，初期有八家：國泰世華、富邦、中國商銀、華銀、彰銀、一銀、中信銀、遠銀，除延續資訊電子業供應鏈體系電子化基礎，成功與大同、華碩、神達、大眾、英業達、新寶、華宇、華通、仁寶、致伸、智邦等十一個中心體系連結外，觸角更延伸到統一、華城、特立、堤維西、遠紡等一百二十一個非資訊電子產業；以電子化供應鏈上之交易訊息為基礎，做到全球收付款、多行帳戶整合、線上融資等。C 計畫特別值得一提的獨創作業模式是融資部分，以交易資訊（免擔保品）進行線上（即時）融資方式，包括訂單前融資、訂單融資、驗收單融資、發票融資、應收帳款融資，供應商可在任何階段向銀行業者申請融資，即時彌補資金缺口。

C 計畫之推動涵蓋國內銀行、中心廠、供應商三方，由八家銀行共同組成 BWG(Bank Working Group) ，進行作業需求之訂定，包括訊息交換範疇、內容及標準制定時程，亦獲得銀行公會之大力支持，針對 BWG 所訂定之作業需求，負責訊息標準之制定與公布，其所採行之電子簽章標準更列入 IFX(Interactive Financial Exchange) 國際規格。

C 計畫對國內整體產業及金融發展之重要性已獲得普遍的重視，在金融產業方面，銀行公會已規劃出擴散 C 計畫之推動內涵及經驗至其他行庫之時程表，除參與經濟部 C 計畫之銀行依據 C 計畫執行進度導入外，其餘非 C 計畫之銀行至少需於 2004 年底完成建置以 XML 為基礎之金流作業 (含收付款、帳戶整合、融資等作業) 導入產業運籌。

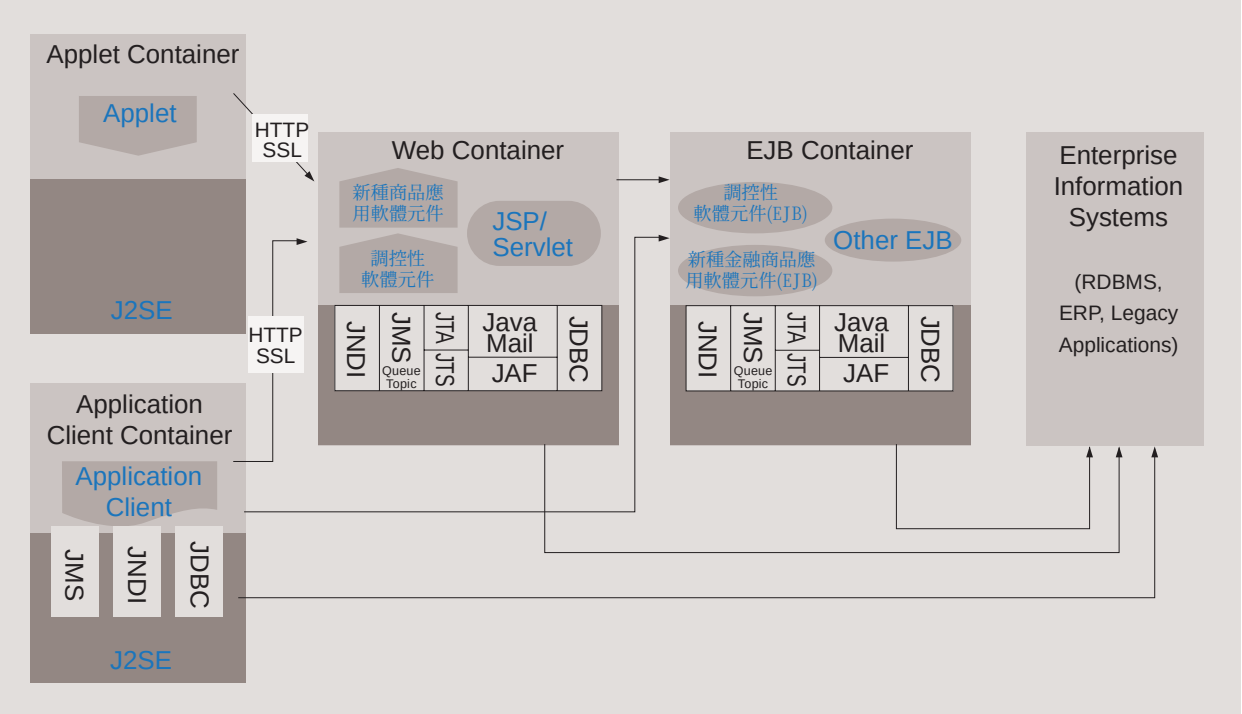
由於政府大力的推動與支持及銀行公會的極力配合，金融 XML 將是未來趨勢，由財金公司負責實體環境建設的跨行共通平台 (Interbank Common Platform) 應將會是資金

移轉最佳通路，藉此提供客戶更便捷安全的交易管道，降低人工介入之作業成本，並且結合網路銀行提供更便利服務，成為跨行電子化金融商品之共同交易平台。

整合性金融入口服務

傳統金融資訊系統的建置，只為追求達成單一業務功能，這種單線個別主機獨立的作業方式難以應付多元化金融商品的系統整合需求，在金融控股公司整併後，面對更形多元的跨機構金融商品整合需求，將使得連線管理愈加困難。在金控整合潮流下，各方業者均致力於思考金融機構合併後帶來的利益，如新金融商品的開發、資訊的共享、聯合銷售（cross-saling）的經營模式。過去無法進行的業務將因法令解禁而大幅成長，未來各種聯合行銷的新商品必定急速的增加，因而使得各機構中以 EAI(Enterprise Application Integration) 架構整合各型主機上的金融服務益形重要。而使用適當交易平台應有助於完成這複雜艱鉅的任務，在此平台中可以放入兩類的軟體元件：其一是易於切割、組裝及再用的新種金融商品應用軟體元件；其二是定義新種應用軟體元件或現有應用系統之間各式組合邏輯的調控性軟體元件如（圖一）。

使用此種架構來整合多種金融商品應該比較容易促成一次購足（one-stop shopping）且有彈性的個人化服務，同時，軟體元件技術的運用也可以使商品新增與系統維護的成本降低。例如：一個可以整合擔保品鑑估規則及其他核貸流程的貸款系統就可以使用此種架構，在系統執行時傳送訊息到保險子公司及證券子公司的資訊系統中查詢當事人的保單及股票相關資訊，藉此縮短核貸時程，促進貸款系統作業效率。

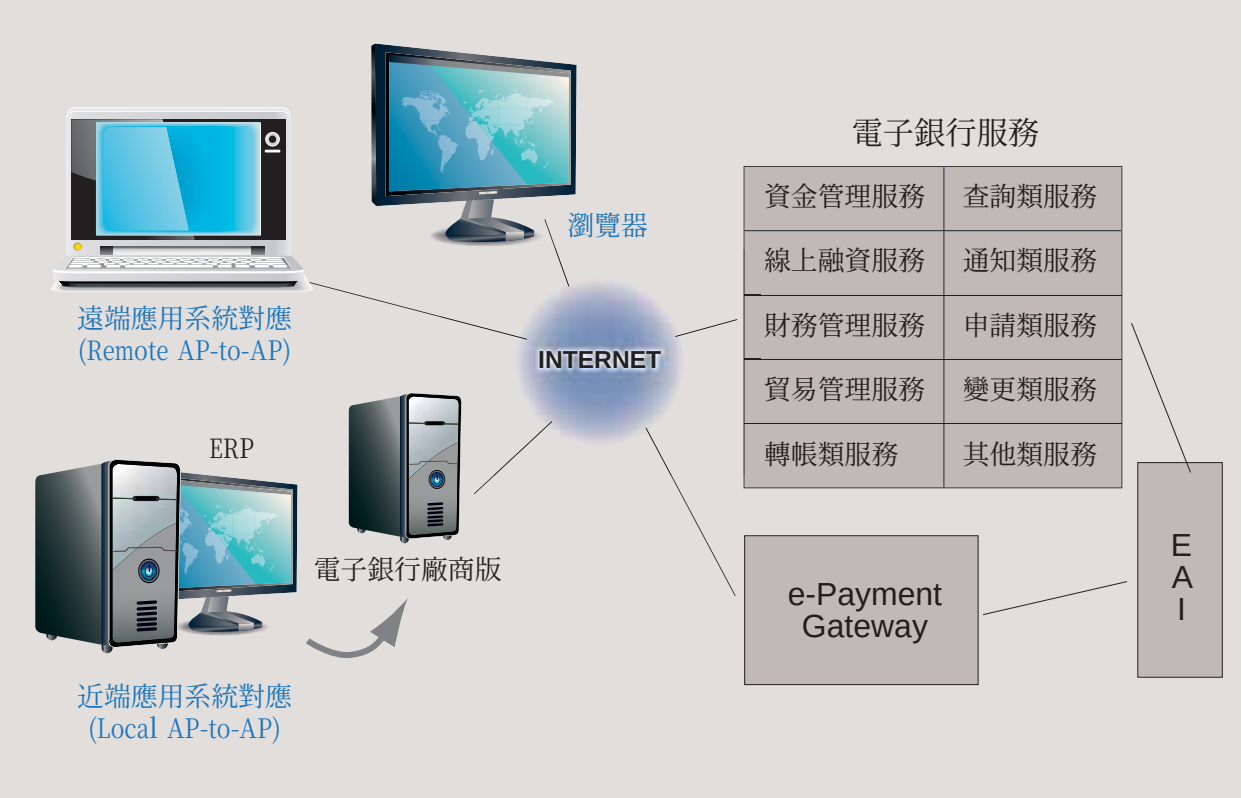


圖一　整合性金融商品交易平台

因此，新一代的電子銀行系統應該提供以客戶為導向的服務機制，配合快速、簡便、安全可靠的交易流程，有單一簽入 (single sign-on) 及個人化彈性機制，具開放、穩定、容錯能力強及可跨平台特性，以 XML 資料格式與 EAI 機制快速整合及銜接後端主機交易。應用系統開發應採縮短時間、降低成本、提高可維護性的物件導向方法，及畫面展示與商業邏輯分離設計的多層次架構，為多元通路之擴充需求預作準備，並加強軟體元件之再用效益。結合上述電子金流的發展趨勢，在個人金融方面提供：查詢、轉帳、掛失、申請、變更、理財、通知等服務。在企業金融方面提供資金管理系統，包括帳戶、付款、收款管理功能；線上交易融資系統，包括應收帳款融資及承購功能，以及發票、訂單、存貨融資功能；財務管理系統，包括支存自動轉帳、分公司資金彙整、分公司應收付結清等功能；進出口貿易管理系統，包括進口管理與出口管理子系統功能。電子銀行整合服務架構如 (圖二)。

新一代電子銀行的共用平台與人力升級

從資訊技術角度來看，新一代電子銀行交易平台整體環境是複雜的，出現問題時系統責任歸屬因而環環相扣，在這些平台上鋪陳出來各式各樣的應用系統，最好搭配整套系統開發及維護的好方法，以低成本的代價支援各種變化的多元性需求。新一代的中介平台 (middleware) 大多有這樣的設計，從底層建置共用平台，採用多層次的架構，前端支援各式



圖二　電子銀行整合服務架構

各樣的通路，中間有中介軟體及伺服器，軟體元件共用部份應該被抽離並佈署到平台上，而其後端再接不同的資料庫或主機系統。在這新興且複雜的平台環境中，穩定的優秀人才非常重要，需要有新一代元件式系統開發的能力，將應用系統分解並封裝成軟體元件的提供者與組合者，需同時扮演調控者角色要將軟體元件適當地佈署在交易平台上，另外系統管理者需要將應用軟體與網路交易環境安排適當的整合方式，在在都需要人才。

因應微利時代的來臨，金融創新服務需有即時回應顧客需求，以提高投資報酬率的營運模式，金融機構的核心競爭力也就建立在許多業務元件上，由業務活動搭配資訊系統、作業流程、組織結構與績效測量所構成，提供多樣的金融服務組合。元件導向的作業流程藉由共享式的服務架構，能重複且有效地使用各作業中心或區域中心之生產能量，使處理作業達到企業整體規模經濟，提昇成本效益。例如：信用卡或現金卡可由最具規模的電話行銷公司代銷，風險評量模型委請最具專業的風險顧問建置與維護，使得銀行內部的部門功能元件需與外部供給者做公平競爭，藉由市場機制調整，利用各種來源的最佳元件迅速回應市場機會。

另一方面，由於金融服務業仰賴 IT 提昇核心競爭力的現象將更明顯，在專業分工的潮流中，業者必需在資訊系統整合建置上將業務流程重新定義，並集中資源只作核心業務，將非核心的週邊業務委外處理。而在降低資訊風險考量下，銀行業務有許多涉及機密的部份不能委外辦理，需自行開發，銀行資訊人員的栽培更顯重要。但是現今銀行主管大多承接舊有系統之資訊背景，對以 PC 及 Internet 應用為主的新一代整合性金融作業平台的控管能力有限。

因此，結合上述共用平台的觀念，在現今電子銀行發展歷程中，建立新一代金融 e 化元件式系統設計人力服務平台，讓金融機構以顧問諮詢及人力駐點服務方式引進新一代金融軟體元件技術之知能與人力，減少核心系統委外開發之風險，不失為提昇電子銀行人力品質的解決之道。

結論

唯金融機構配合自身 e 化策略規劃，同步培育元件式金融 e 化專案管理及系統分析人才，適當管控系統導入及營運之作業風險，掌握核心業務知能，配合金融商品業務開發及行銷人員的養成，以及新種商品創意研發環境的營造，才能在面對 WTO 的國際化新興戰場中展現競爭優勢。

探討我國「外幣結算平台」之服務與發展

本篇摘自 2015 年 04 月出刊之財金資訊季刊第 82 期，由時任財金資訊公司研發部設計一組蔡佩珍高級工程師（現任為副組長）撰寫。

一、前言

因應金融全球化之發展，國際間貿易往來增加，跨境金融活動需求隨之提高，加上貨幣市場上致力減少結算風險，使得全球支付及結算系統間的互連與資訊傳遞更為緊密，惟因以往所採取傳統的外匯清算方式存在極高的風險，促使各國陸續建置其跨國及多幣別之外匯結清算系統，以提高支付的效率並降低外匯交易產生的清算風險；是以，財金資訊公司 (以下稱財金公司) 於 2012 年 10 月奉中央銀行指示，規劃建置「外幣結算平台」。

為考察香港外幣系統發展成功之案例，中央銀行率財金公司人員於 2012 年 11 月前往參訪香港銀行同業結算有限公司 (HKICL，Hong Kong Interbank Clearing Limited)、環球銀行金融電信協會 (SWIFT，Society for Worldwide Interbank Financial Telecommunication) 及中國 (香港) 銀行 (以下稱中銀香港)，期借鏡以觀形，謹簡介如后。

二、香港外匯支付系統服務

香港為強化其區域金融中心之地位，近年來致力於發展金融基礎建設 (如圖 1 所示)，特別是推動支付與結算系統的發展，從而促使國際及跨境金融活動能在香港以安全且有效率的方式進行。香港的金融基礎建設包含多幣別即時支付結算系統 (RTGS 系統)，在香港稱為 CHATS (Clearing House Automated Transfer System)，由香港銀行同業結算有限公司負責營運，以及債務工具中央結算系統，皆與境外系統互相連結，提供款券同步交割 (Delivery Versus Payment，簡稱 DvP) 功能、跨境交易及其他金融服務。

(一) 港元即時支付結算服務

香港 RTGS 系統於 1996 年 12 月首先推出港元即時支付結算服務，由香港金融管理局 (HKMA，Hong Kong Monetary Authority，以下簡稱金管局) 擔任清算銀行，提供港元與美元、港元與歐元、港元與人民幣等不同幣別間之款對款同步收付 (Payment versus Payment，簡稱 PvP) 服務；另外，尚與中

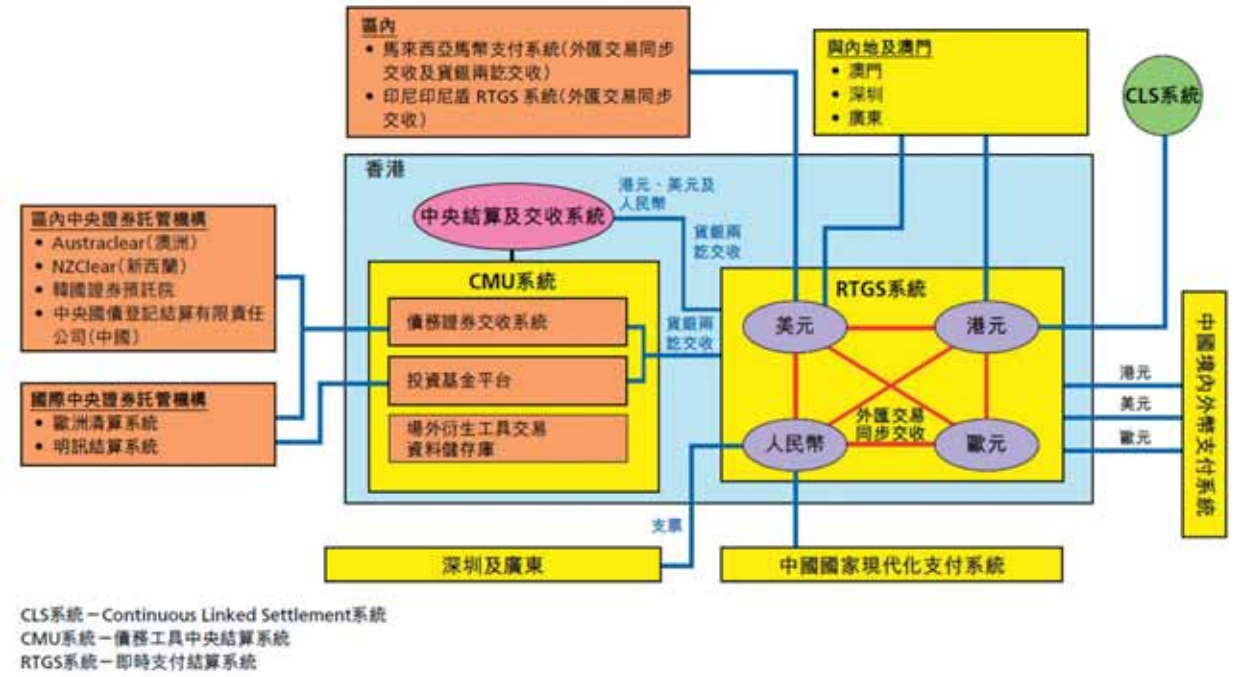


圖 1　香港金融基礎建設

資料來源：香港金融管理局

國境內外幣支付系統、內地與澳門系統相互連結，提升兩地間之外幣支付清算效率。港元 RTGS 系統於 2004 年亦與「持續連結外匯清算系統」(CLS 系統，Continuous Linked Settlement System) 連結，使港元可與 CLS 系統其他 16 種貨幣進行 PvP 清算。

(二) 美元即時支付結算服務

2000 年 8 月推出美元即時支付結算服務，由香港上海匯豐銀行擔任清算銀行，提供美元與港元、美元與歐元、美元與人民幣之 PvP 服務，美元 RTGS 系統除比照港元 RTGS 與中國境內外幣支付系統、內地與澳門系統相互連結外，並與馬來西亞馬幣支付系統、印尼 RTGS 系統連結，辦理馬幣與美元及印尼盾與美元之 PvP 服務，以及提供馬來西亞辦理美元證券之 DvP 服務。

(三) 歐元即時支付結算服務

2003 年 4 月推出歐元即時支付結算服務，由英商渣打銀行擔任清算銀行，提供歐元與港元、歐元與美元、歐元與人民幣之 PvP 服務，歐元 RTGS 系統與中國境內外幣支付系統連結。

(四) 人民幣即時支付結算服務

2007 年 6 月推出人民幣即時支付結算服務，由中銀香港擔任清算銀行，提供人民幣與港元、人民幣與美元、人民幣與歐元之 PvP 服務，人民幣 RTGS 系統並與中國現代化支付系統 (CNAPS，China National Automatic Payment System) 連結，港區人民幣跨境支付交易可即時清算，另外與深圳及廣東之支票結算系統連結，處理客戶在深圳、廣東消費所開立人民幣支票之結算交易。

(五) 債務工具中央結算系統

債務工具中央結算系統 (Central Moneymarkets Unit, 簡稱 CMU 系統) 於 1900 年建置，提供港元、美元、歐元及人民幣之債券結算、收付及託管等服務，並與港元、美元、歐元及人民幣 RTGS 系統連結，提供各幣別債券 DvP 功能，另外，CMU 系統尚與澳洲、紐西蘭、韓國、中國內地之結清算系統、歐洲清算系統 (Euroclear) 及明訊結算系統 (Clearstream) 連結，使香港與境外之投資者可以持有及收付存放在 CMU 系統及其連結系統之債券。

(六) 流動性節省機制

在港元 RTGS 系統推出前，銀行以日終淨額方式進行交割，亦即每家銀行只會向參與系統的其他銀行支付或收取當天所有交易之淨差額，雖然這種日終淨額結算機制對銀行資金需求壓力較小，但銀行須承受系統性風險，原因是只要有任何一家銀行未能支付日終淨差額時，就有可能使得其他銀行收不到預期之資金，進而衍生違約連鎖效應。在港元 RTGS 系統推出後，銀行同業間透過設立在金管局的結算帳戶，依序逐筆結算，與淨額結算相比，RTGS 機制消除了系統性及結算風險，但銀行卻須持有較多之日間流動性資金以支付逐筆的結算交易；爰此，金管局推出多項系統功能，以協助銀行解決日間流動性資金需求，包括在 2006 年 1 月推出的流動資金優化器 (RLO, RTGS Liquidity Optimiser)，即透過每 30 分鐘的週期，定時將 RTGS 系統內未支付的款項進行多邊互抵，從法律層面來看，這些交易仍是按照總額逐筆結算，只不過這些結算是同步執行；從數學層面來看，這個結算方法產生帳項相互抵銷效果，因此，提高 RTGS 之成交效率，亦減少銀行日間流動性資金需求，針對 RLO 有助提高銀行即日流動資金之管理效率，舉例說明如下：

資料來源：HKMA

三、我國外幣結算平台服務

財金公司「外幣結算平台」經考量既有系統之整合，且為減少參加單位建置開發等額外投資，爰規劃外幣結算平台結合現有外匯系統平台，並採 SWIFT 系統網路、架構及訊息格式，提供金融機構進行外幣收付交易處理之結算服務，於 2013 年 3 月 1 日正式上線營運，提供境內美元匯款服務，由兆豐銀行擔任清算銀行；嗣逐步擴大服務範圍，除配合人民幣清算行中國銀行台北分行之全球支付系統建置時程，於同年 9 月 30 日增加境內及跨境人民幣匯款服務，由中國銀行台北分行擔任清算銀行及跨境代理行外，續於 2014 年 2 月 14 日擴增兩岸美元匯款服務，由中國銀行台北分行擔任跨境代理行；再於 2014 年 2 月 17 日增加款對款同步收付 (PvP) 服務，因涉及新臺幣

PvP 交易，故與中央銀行同資系統連結；再於 2014 年 7 月 30 日提供美元及人民幣匯款流動性節省機制，於即時總額結清算 (Real Time Gross Settlement，簡稱 RTGS) 機制下，降低金融機構日間流動性資金需求；自今 (2015) 年起，於 1 月 28 日增加境內日圓匯款服務，並預計同年 5 月擴增至跨境服務，由日商瑞穗銀行擔任跨境代理行外，預計 6 月提供歐元匯款服務，由兆豐銀行擔任清算銀行及跨境代理行；於 7 月將與臺灣集中保管結算所 (以下稱集保結算所) 共同規劃，增加款券同步交割 (DvP) 服務。

(一) 採用國際標準 SWIFT 規格

外幣結算系統採用國際標準 SWIFT 規格，清算行、參加行及跨境代理行可於現有的 SWIFT 平台上，同時發送境內及跨境之美元、人民幣、日圓等外幣交易電文，透過 SWIFTNet 網路傳送至財金公司之外幣結算系統辦理結 (清) 算作業，如圖 2 所示，不須分別與各幣別清算行直接聯繫與處理後續作業，簡化金融機構作業流程。

外幣匯款作業係由匯出行發送 SWIFT FIN 訊息至匯入行，外幣結算系統則使用 SWIFT FINCopy 模式傳送至結清算中心處理，其特點為可選擇 FIN 訊息部分欄位或全部欄位傳送，基於中央銀行監管需求，外幣結算系統之 FINCopy 模式選用全部欄位傳送之作法。

(二) 提供便捷的網頁即時查詢系統

外幣結算系統除處理線上交易電文外，亦提供便捷的網頁即時查詢系統，提供下列功能：

1. 交易與基金餘額查詢

參加行可於發送匯款電文後，隨時查詢該筆交易之處理狀況，以及查詢自單位即時基金帳戶餘額；而匯入行亦可隨時查詢當日已結清算、預計應收之交易筆數及金額；此項網頁查詢功能，可減免參加行相關查詢系統之開發投資及交易電文之發送成本。

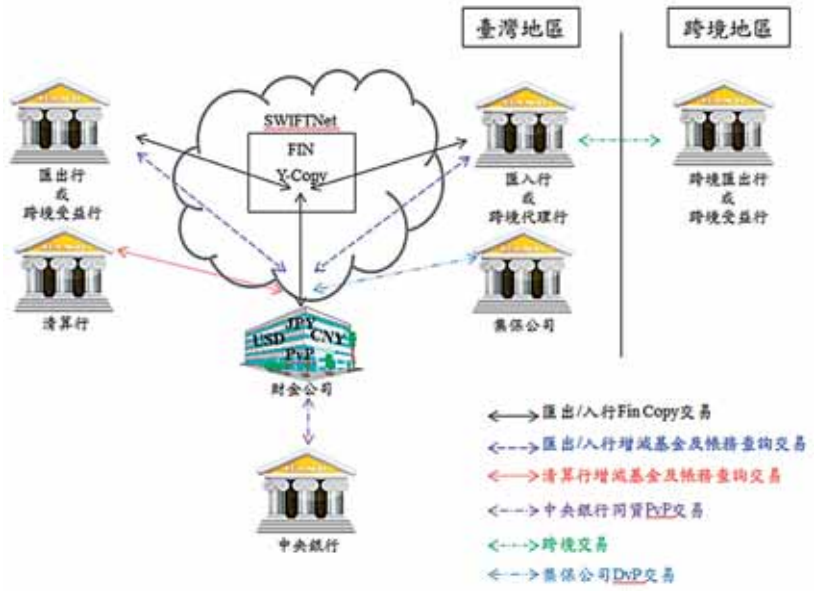


圖 2　外幣結算系統訊息架構圖

2. **報表下載**

參加行於日終結帳後，可透過本網頁立即下載當天各幣別之交易明細及統計報表，每月月底並可於月底當天日終結帳後，下載當月之交易月統計報表，有助於銀行人員即時核對帳務報表，增加人工帳務處理效率。

3. **參加行新增或退出通告**

參加行新增或退出某幣別服務時，財金公司除以函文通知全體參加行外，作業人員另於外幣結算系統輸入增刪之參加行資訊後，系統即自動產生參加行清單檔，並傳送至網頁發布供參加行下載，參加行依系統規格開發檔案格式後，每次只須將該清單檔傳送至自單位相關系統自動處理，便可立即更新參加行清單，降低人工維護處理之成本及風險。

4. **營業日公告**

外幣結算系統各幣別之清算行於每年年底提供翌年營業日與例假日明細，財金公司除轉發函通知各參加行外，系統規格亦定義幣別營業日檔之格式，由清算行透過網頁上傳幣別營業日檔至外幣結算系統，經財金公司覆核放行後，系統即自動傳送至網頁發布並供參加行下載，參加行可轉傳送至其自單位系統，減少銀行每年人工維護營業日之成本及風險。

(三) 預約交易

一般外匯交易，雙方外匯交易員於交易日 (Trade Date) 即已協議交割日 (Value Date) 為明日 (T+1) 或後日 (T+2) 或其他日期，而交易員在 Trade Date 即可透過外幣結算系統發送 Value Date (最長為 T+11) 之電文，外幣結算系統收到該筆電文時，先予以儲存 (Store)，直到 Value Date 當日再進行結清算作業；若 Value Date 為假日時，將遞延至次營業日辦理。此系統設計較符合現行外匯業務之運作慣性，亦有別於財金公司其他僅提供即時性交易之支付系統。

(四) 不足額佇列機制

現行財金公司其他結 (清) 算系統，於交易訊息進入系統時，立即檢查相關參加單位之基金餘額是否足額，不足額時即拒絕交易。然而，外幣結算系統於參加行清算基金餘額不足時，不予拒絕，而將交易訊息暫存於系統佇列等候，直至參加行自行或因匯入交易而增加清算基金後，重新進行處理。

又，如有大額交易先進入系統而基金餘額不足時，系統將自動跳過該筆大額交易，往後處理基金餘額足以支付之小額交易；亦即不因已有大額交易佇列等候，影響後續可足額支付之小額交易之進行。

此系統設計在交易電文先進先出之原則下，亦保留處理彈性，提供參加行於日終結帳前，減少因為一時之基金餘額不足致交易被拒絕後，須重新發送電文之成本。

(五) 取消交易

由於系統提供預約交易之功能及不足額佇列機制，故交易電文有機會儲存 (Store) 於系統中，等待 Value Date 當日或基金足額時再行處理，因此，外幣結算系統在交易結清算尚未處理前，提供參加行取消待處理交易之功能，可降低非因電文格式發送錯誤而須退匯時，匯出行與匯入行雙方所需辦理之相關作業。

(六) 調整佇列優先順序

考量參加行於交易訊息進入系統佇列等候期間，須因應客戶需求優先處理某筆交易，爰於網頁提供參加行調整佇列優先順序之功能，亦即參加行可自行於網頁查詢並調整佇列中等候處理之某筆交易排序，予以優先處理。

(七) 款對款同步收付 (PvP) 機制

款對款同步收付 (PvP) 機制是確保不同幣別的交易，於同一時間完成交割作業，外幣結算系統於 2014 年 2 月提供美元與新臺幣、美元與人民幣、人民幣與新臺幣之 PvP 服務，於 2015 年 1 月增加日圓匯款服務後，擴增美元與日圓、人民幣與日圓之 PvP 服務，交易類型包含即期、遠期、換匯交易，經由外幣結算系統確保兩家不同銀行間 PvP 交易之款項支付與結算，消除違約交割風險，另外涉及新臺幣之 PvP 交易雖然透過外幣結算系統收送電文，惟其新臺幣之款項撥轉仍使用金融機構設立於中央銀行同資系統之帳戶辦理，如圖 3 所示。

外幣結算系統之一般匯款及同業資金調撥交易均採用 RTGS 機制，即針對交易電文逐筆檢查付款參加行之基金餘額，足額才予以結 (清) 算，有效降低清算風險；然而，每筆均為大金額之 PvP 交易，如採用 RTGS 機制，恐造成參加行日間流動性資金風險，故規劃採用 RTGS、即時雙邊互抵及定時多邊互抵之混合式清算 (Hybrid Settlement) 機制，不僅保留 RTGS 結 (清) 算之優點，亦降低參加行之日間流動性資金需求，為國內支付系統之創舉；其運作機制如圖 4 所示， 說明如下：

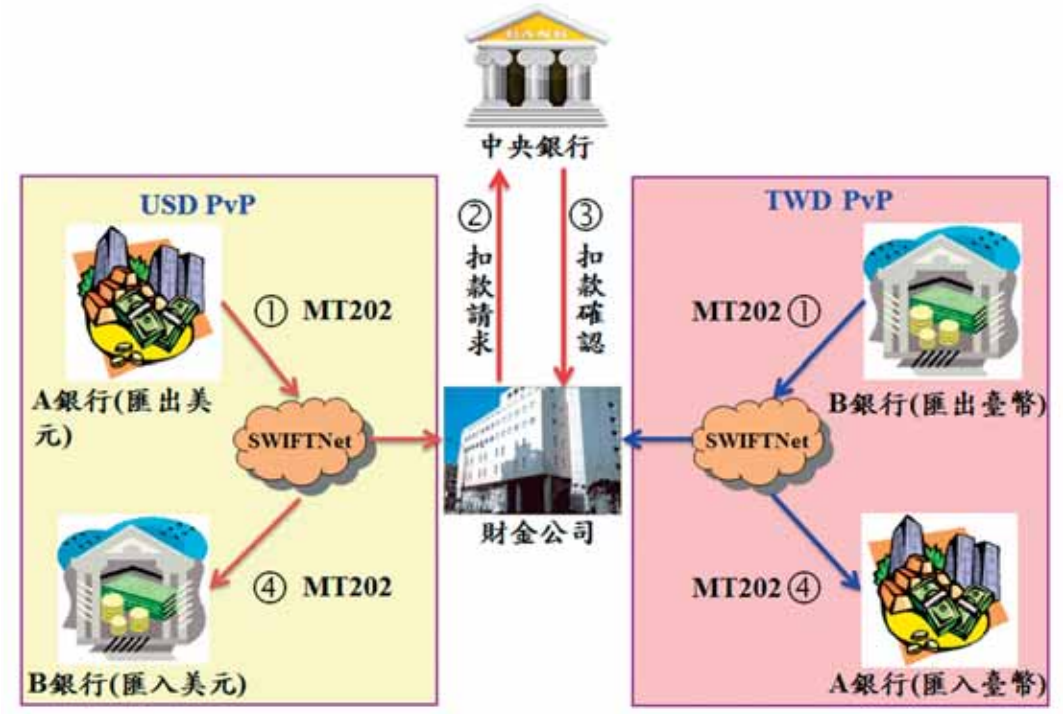


圖 3　款對款同步收付 (PvP) 美元與新臺幣交易架構圖

圖 4　外幣結算系統 PvP 交易運作機制

1.　**PvP 交易比對**

PvP 交易須處理兩種不同幣別之電文，系統收到電文後，比對交易者與其交易對手之應收付幣別金額等條件是否成對，如果成對，則將兩筆電文打包 (Bundle) 後進行結 (清) 算作業。

2.　**即時逐筆 RTGS 結清算**

每套 PvP 交易將先檢查其中一幣別之基金餘額，如足額則確認另一幣別之基金餘額是否足額，若都足額則該套 PvP 交易即採用 RTGS 結 (清) 算。

3.　**即時雙邊互抵**

如任一幣別基金餘額不足時，則不足額幣別之參加行是否有應收交易對手之 PvP 交易可進行抵銷，且雙方有否其他幣別可供互抵，若均成立，則該 2 套 PvP 交易即採雙邊互抵並以差額進行結 (清) 算。

4.　**定時多邊互抵**

若雙邊互抵不成立時，系統則每 30 分鐘一盤定時試算不足額佇列之 PvP 交易，核計每家參加行之任一幣別淨應收付總額後，檢查其基金餘額是否足敷交易所需，試算成功之 PvP 交易則採用多邊互抵以差額進行結 (清) 算；如仍不足額時，就不足額最高之參加行，抽出其 PvP 交易電文最後一套交易後重新試算，逐盤試算，直至所有參加行之任一幣別淨應收付總額皆足以支付佇列之交易。

(八) 流動性節省機制

外幣結算系統之流動性節省機制，對於 PvP 交易參加行之資金調度雖大有助益，然就一般匯款 (大多為小額交易) 及同業資金調撥 (多為大額) 交易而言，其效益無法彰顯，故自 2014 年 7 月開始，就美元、人民幣交易所提供之流動性節省機制，規劃採定時多邊互抵之結清算作業，如圖 5 所示。

圖 5　外幣結算系統流動性節省機制

四、未來發展

2012 年 10 月，財金公司依據中央銀行指示建置外幣結算平台，規劃系統架構設計為多幣別，作業架構多元且完整，為利系統穩定運作及提升運作效率，爰採四階段建置及擴充，目前已完成第一至三階段之建置作業 (詳如表 1)；2015 年將增加日圓及歐元匯款服務，且於系統上線時，同時提供日圓及歐元與其他幣別之 PvP 服務，日圓及歐元匯款於結清算部分亦採流動性節省機制，屆時外幣結算系統多幣別匯款服務即可依主管機關規劃全數到位。

表 1　外幣結算平台建置時程規劃

第一階段	• 採用 SWIFT 規格與境內美元匯款服務 (2013.3.1) • 提供 Web 查詢服務 (2013.4.15)
第二階段	• 境內及跨境人民幣匯款服務 (2013.9.30)
第三階段	• 跨境美元匯款服務 (2014.2.14) • 款對款同步收付 PvP 服務 (2014.2.17) • 流動性節省機制 (2014.7.30)
第四階段	• 日圓匯款服務 (2015.1.28) • 歐元匯款服務 (預計 2015.6) • 款券同步交割 DvP 服務 (預計 2015.7)

財金公司將賡續與集保結算所合作，共同規劃提供多幣別之款券同步交割 (DvP) 服務 (如圖 6 所示)，服務標的包含營業處所議價之國際債券 (含寶島債) 及外幣票券，買賣雙方於收付債票券時，可確保票券及資金於同一時間交割，以消除系統性結 (清) 算風險。

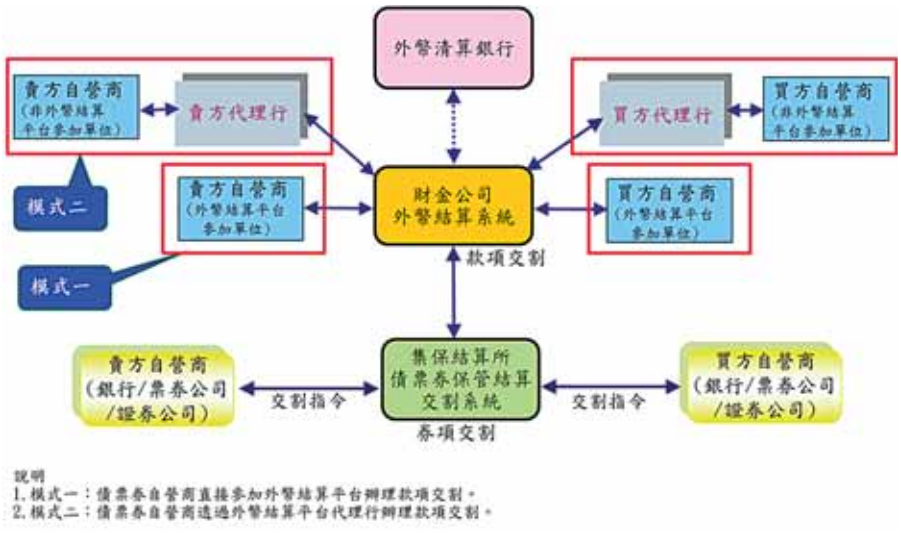


圖 6　款券同步交割 (DvP) 作業架構

五、結語

外幣結算系統截至 2014 年底，美元匯款參加機構共計 67 家；人民幣匯款計 57 家。自 2013 年 3 月 1 日系統上線至 2014 年 12 月 31 日止，美元匯款交易筆數及金額分別為 96.78 萬筆及 2 兆 638 億美元；人民幣匯款交易筆數及金額則分別為 13.69 萬筆及 2,673 億人民幣。

目前部分匯出行採用境外代理行方式辦理匯款作業，除資金調度考量外，主要是依照國際慣例處理，境外清算行自匯款金額內扣除中轉手續費，其中部分回饋金轉給匯出行，惟透過境外代理行時，其手續費較外幣結算平台者為高，不僅增加客戶手續費負擔，且未能「全額到匯」。現行外幣結算平台已提供境內匯款當日全額到匯服務，不必繞經國外轉匯，免除中轉行費用，大幅減輕客戶手續費負擔及金融機構因匯差所衍生之作業成本及清算風險。

外幣結算平台流動性節省機制的設計，亦大幅減少金融機構日間流動性資金需求，活絡外匯交易，增加結算系統平台之效益，以 2014 年 12 月 PvP 交易為例，流動性節省機制效益約達 5.5 倍，意即支付 1 美元約可進行 5.5 美元之交易，匯款者得以較低成本，金融機構則使用較少清算資產，提早獲得清算最終性及全額到匯款項，換言之，外幣結算平台是金融機構、企業與民眾外幣匯款服務多贏且優質的選擇。

※ 參考文獻 / 資料來源：

1. HKICL 簡報資料 (2012.11.5)。
2. 謝鳳瑛 (2013.1)，「香港支付系統之發展－兼述我國外幣清算系統之建置」出國報告。
3. 陳文雅 (2013.8)，「國際降低外匯清算風險之進展－兼論我國外幣結算平台系統運作概況」出國報告。
4. 香港金融管理局網站資料。
5. 香港金融管理局 (2013.2)，「香港的金融基建」。
6. 香港金融管理局 2008.3 季報，「即時支付結算系統的流動資金及風險管理－香港經驗」。

兩岸特色金融－「外幣結算平台」新紀元

本篇摘自 2013 年 07 月出刊之財金資訊季刊第 75 期，由時任財金資訊公司業務部卡片營運組陳詩蘋副組長（現任為專案企劃組組長）撰寫。

一、前言

近年來，全球經濟歷經金融海嘯、在美國經濟遲緩復甦之際，又有歐債危機的波動，致使各行各業都面臨嚴峻的挑戰。所幸，臺灣與大陸兩岸地區同文同種，雙邊往來與合作有其便利性與優勢性，因此，海峽兩岸相繼於 2009 年簽署「銀行業監督管理合作瞭解備忘錄 (MOU)」，及 2010 年「兩岸經濟合作架構協議 (ECFA)」後，開啟了雙方金融合作往來的新局。

面對兩岸經貿與民間往來的日益頻繁，透過雙方金融機構間跨平台服務的連結與互通，正是加速雙邊商務合作及民間交流的基石。在兩岸電子金融業務的推展進程中，自2010年起，配合政府「積極開放、有效管理」政策，正式邁向兩岸「跨行支付平台」連接的新世代，在財金資訊 (股) 公司 (以下稱財金公司) 與中國銀聯公司的合作下，逐年開辦了「銀聯卡在臺灣實體特約商店刷卡消費」、「銀聯卡在臺灣 ATM 取現、餘額查詢及預借現金」，以及「銀聯卡在臺灣網路特約商店刷卡消費」等服務。

目前，大陸人士只要手持一張銀聯卡，不論是來臺洽商、旅遊、留學，甚至上網購物，都能「一卡在手、自在暢遊」。根據相關統計資料顯示，自業務開通到今 (2013) 年 6 月底為止，銀聯卡在臺刷卡消費收單業務合作之特約商店約 9 萬家，累計交易筆數約 1,254 萬筆、交易金額約新台幣 1,170 億元；至於受理銀聯卡取現、餘額查詢及預借現金服務的 ATM 已超過 2 萬台，覆蓋率 85.08%，累計交易筆數約 728 萬筆，交易金額約新臺幣 1,042 億元。總計銀聯卡業務開通 3 年以來，帶動臺灣觀光相關產業之整體發展及效益超過新臺幣 2 仟億元，成果豐碩。

二、兩岸特色金融政策與目標

兩岸金融往來為兩岸經貿關係之一環，亦屬我國金融國際化之範疇，各主管機關依據政府大陸政策所規劃之開放進程，並配合兩岸經貿關係之發展現況，循序調整，以滿足民間從事兩岸貿易、投資所衍生對金融服務之需求，並在維護國內金融體系穩定之原則下，協助國內銀行業佈局兩岸三地，以提升國內銀行業之國際競爭力。

從兩岸金融往來的歷程回顧，可分為 (一)

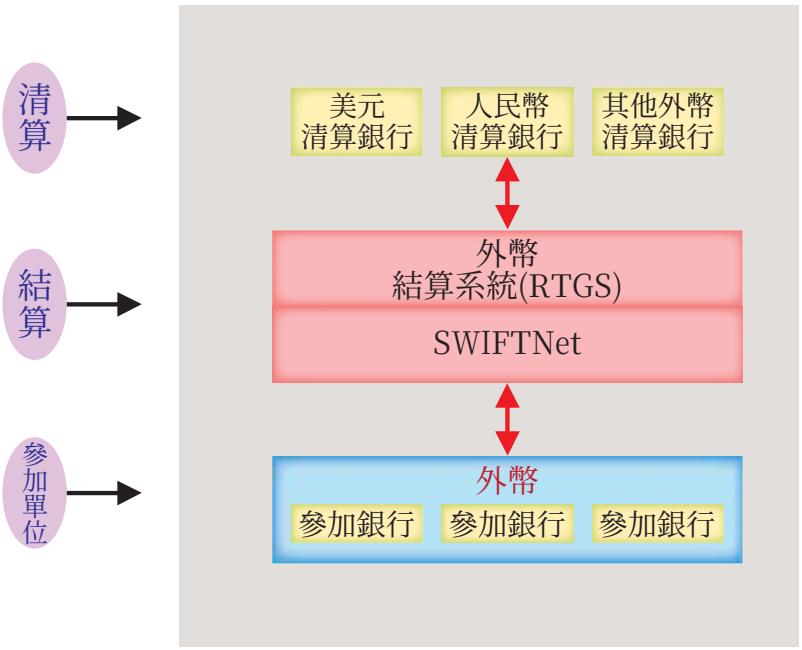
兩岸民間交流初期 (1987 年至 1992 年)；(二) 間接往來階段 (1993 年至 2000 年)；(三) 積極開放、有效管理階段 (2001 年至 2008 年)；(四) 直接往來階段 (2009 年迄今) 等四個階段。歷年來，兩岸銀行監理機構的各項協商成果，展現兩岸雙贏，協助臺灣地區銀行業者擴大對大陸市場的布局及業務經營，及大陸地區臺資企業發展，亦有助於大陸地區銀行及企業來臺投資，不僅強化兩岸的金融合作與互動，更有利於兩岸工商企業使用銀行業之金融服務。

鑒於兩岸經貿關係持續穩定發展，我國相關產業也在「兩岸經濟合作架構協議」下，實質交流互惠，行政院於 2012 年 9 月 6 日核定「發展具兩岸特色之金融業務」計畫，就外匯、銀行、資本及保險市場等面向，規劃相關推動措施，協助金融業者充分發揮其兩岸設有據點特色，俾拓展兩岸金融市場發展之經營利基，協助各產業部門有效掌握兩岸經貿商機，以創造更高的產業價值。

其中，「發展具兩岸特色之金融業務」計畫之亮點二－「兩岸現代化金流平臺」子計畫，經主管機關報奉行政院核定，由財金公司擔任「發展具兩岸特色之金融業務計畫」之「建立境內銀行人民幣跨行通匯系統」及「建立大中華區跨境中文匯款平台」協辦單位，並將規劃於「外幣結算平台」增加「人民幣」等外幣結算服務功能，俾利金融業者擴大對臺商、兩岸三地民眾之服務，以強化我國金融業者在區域金融市場之競爭優勢，有助臺灣爭取成為離岸人民幣中心。

三、外幣結算平台之規劃與建置

為落實「發展具兩岸特色之金融業務」計畫，促進國內支付系統平台之多元化發展、建構我國外幣支付系統，並與國際接軌，財金公司採用國際通用 SWIFT 規格及網絡 (以下簡稱 SWIFTNet) 擴建「外幣結算平台」，運



財金公司外幣結算平台系統架構

用 SWIFTNet 連結不同外幣之清算銀行及參加單位，以「即時總額清算 (Real Time Gross Settlement Systems，簡稱 RTGS) 機制」，辦理「跨行結算」服務。

「外幣結算平台」業於 102 年 2 月 27 日經中央銀行 (以下簡稱央行)、金融監督管理委員會 (以下簡稱金管會) 核准建置，並於 102 年 3 月 1 日上線營運，4 月 15 日提供「外幣結算平台網路服務及表報管理子系統」，以提升外幣資金收付的效率、與降低金融機構資金清算的風險，進而減輕企業及民眾辦理外幣資金收付的成本負擔。

本國、外國金融機構及其他經央行許可之單位，得向財金公司申請參加「跨行結算」服務，並在清算銀行開立清算帳戶，即可透過本平台辦理「跨行結算」作業。截至 6 月 25 日止，共計有 36 家金融機構參加，預計於 102 年底增至 43 家，其中本國銀行計 34 家，外商銀行 9 家，參與機構已涵蓋境內主要銀行。

本平台初期提供境內美元跨行清結算服務，自 102 年 3 月 1 日上線，至 6 月 25 日為止，累計交易筆數及金額分別為 4.7 萬筆、112.65 億美元，分別較去年同期增長 6 倍及 10 倍，其中交易量最高之金融機構為第一銀行 (單月交易筆數逾 2,800 筆)，依次為華南銀行、合作金庫銀行、上海銀行及中國信託銀行。經分析，美元匯款服務之交易量，屬於企業的資金調度、一般匯款超過 9 成，用途多為資金調度、貨款、遠期外匯交割、股本 (權) 投資、存款等。

目前「外幣結算平台」處理效能及相關作業已臻完備，各金融機構應儘速遵照中央銀行指示，將境內美元匯款交易導入「外幣結算平台」處理，俾發揮整合綜效，除可提升金融機構外幣資金收付效率及降低資金清算風險外，透過清算行與結算機構之分工，可確保客戶交易訊息之隱密性，且交易即時全額到匯，既便捷又安全。

四、外幣結算平台境內及跨境人民幣匯款服務

繼「海峽兩岸貨幣清算合作備忘錄」於 101 年 8 月 31 日簽署完成後，大陸人民銀行業於同年 12 月 11 日公告：由中國銀行臺北分行擔任我國「人民幣清算銀行」後，臺灣人民幣業務已逐步開辦，相關人民幣金融商品將陸續推出，央行總裁彭淮南表示，臺灣建立人民幣兌換與回流機制後，將為人民幣離岸市場拓展奠定重要基礎。此外，建置完善透通的金融基礎建設是人民幣活絡的主要關鍵。

過去，國內銀行辦理外幣結算，須各自與各幣別的清算行系統介接，例如辦理人民幣、美元結算，須分別與中國銀行臺北分行、兆豐銀行連線，沒有一個整合的平台處理各種外幣結算。「外幣結算平台」預計於 102 年 9 月提供境內及跨境「人民幣」匯款交易的結算及清算服務，國內金融機構可透過本平台和清算行進行外幣結算，資金不必再繞到境外清算，讓民眾與企業不再支付繞送至國外的國際郵電及手續費；當然也降低外幣運用的資金成本，包括匯款手續費、資金閒置與調度等成本，以及減少因時差所衍生的匯差風險，緊密連結兩岸經貿金融。

此外，過去兩岸匯款因涉及繁簡體字不一致之情形，民眾多使用英文填匯款單，但若不慎拼錯英文拼音，造成退匯情況。未來「外幣結算平台」將中文電報碼統一後，民眾匯款時只須填寫中文資料 (不論繁體字或簡體字) 即可完成，亦可同時支援中、英文交易訊息的傳

輸，妥善處理兩岸繁、簡體中文匯款訊息的轉換，提升兩岸間匯款效率及便利性。

中央銀行總裁彭淮南表示，「外幣結算平台」是臺灣金融市場一個非常重要的「基礎工程」，未來透過這個平台，不論對拓展美元或人民幣等業務，都有很大幫助，也有更多發展空間，各金融機構可透過「外幣結算平台」和清算行，在國內進行外幣結算，國內匯款可同日「全額到匯」，不必再繞到境外轉匯，除免除中轉行費用省下成本外，也能簡化金融機構的作業流程，提升外幣資金收付的效率，各金融機構間之外幣交易機密也不會在清算過程中外洩，以維持競爭公平性。此外，特別強調，全球人民幣市場可分為「境內人民幣市場」(CNY)、與現以香港為主的「離岸人民幣市場」，臺灣也希望成為「人民幣離岸中心」(CNT)。

金管會銀行局長桂先農表示，「外幣結算平台」開辦人民幣匯款後，至少有四大好處：一是人民幣匯款手續費下降，尤其以企業受惠最大；二是「當天到匯」，匯款零時差；三是國內外匯款可全額到匯，過去因銀行額度問題，衍生「到匯先到一半」將不復存在；四是從英文代碼，改為使用中文匯款，不再有拼音問題。

「外幣結算平台」初期以「美元」及「人民幣」業務為主；未來，配合主管機關政策、「發展具兩岸特色之金融業務計畫」規劃之進程、及肆應金融市場需求，擴增至其他外幣，以建構多元貨幣、多層面之安全及高效率之外幣金融基礎平台，原則上，財金公司業已研擬分四階段工作項目如下表：

基礎建設	**第一階段**	建置基礎建設，採用 SWIFT 規格與網絡，提供外幣支付服務，優先辦理「境內美元」業務。(已完成)
增建功能	**第二階段**	建置「外幣結算平台」網路服務及表報管理子系統，提供主管機關及參加單位即時查詢「外幣結算平台」交易明細、跨行基金餘額、結帳時間與系統公告等資訊，以及相關表報下載服務。(已完成)
	第三階段	配合其他外幣服務之提供，增建「新臺幣」與「外幣」間、以及不同「外幣」間交易之「同步即時收付」(PvP) 機制，並擴增至「跨境」外幣結算服務。
	第四階段	協同「資本市場」及「貨幣市場」相關機構，提供外幣交易「款券同步交割」(DvP) 服務。

上表之第一、第二階段皆已建置完成，未來，「外幣結算平台」第三階段，將配合其他外幣服務之提供，增建「新臺幣」與「外幣」間「交易同步即時收付」(Payment versus Payment，PvP) 機制，是指不同幣種資金同步進行交收並互為交收條件的結算方式，以美元與新臺幣換匯交易為例，PvP 可確保支付新臺幣一方，一定收到美元；支付美元一方，一定收到新臺幣，確保收付兩訖，消除違約交割風險。

後續第四階段，將協同「貨幣市場」及「資本市場」相關機構，提供外幣交易「款券同步交割」(Delivery versus Payment，DvP) 服務，係指債券或證券交易達成後，在雙方指定的結算日，債券或證券和資金同步進行相對交收並互為交割條件的一種結算方式，其核心內涵為債券或證券與資金的交收同時進行，以降低交易對手方的信用風險，消除賣方已交付證券卻未收到相應款項，或是買方已交付資金而未收到證券的本金風險，從而防範交收對手方的違約風險。

五、結語

我國「外幣結算平台」之建置，開創兩岸支付新紀元，更具備：(1) 採用國際通用之 SWIFT 規格，得支援傳輸中、英文交易訊息；(2) 透過 SWIFT 網路連結，可與國際接軌；(3) 屬多幣別之外匯支付系統，得處理美元、人民幣及其他幣別交易；(4) 兼具「境內」及「跨境」匯款服務功能；(5) 可處理金融機構間外幣即期、遠期、換匯與拆款等交易之結 (清) 算；(6) 設有「新臺幣」與「外幣」間、不同外幣間之「同步即時收付」(PvP) 與「款券同步交割」(DvP) 機制，以消除違約交割之風險；以及 (7) 建立清算行提供日終流動性機制等優勢，以確保系統穩定順暢運作等功能與特色，可發揮預期效益如下：

(一) 為擴大並提升社會大眾外幣資金收付之效率，財金公司遵照主管機關指示，秉持協助金融機構發揮整體效益原則，肩負起金流支付系統之結算角色，戮力規劃建置「外幣結算平台」，以促進國內支付系統平台之多元化發展、建構與國際接軌之金流基礎建設，提升我國金融機構之整體競爭力。

(二) 財金公司與國際通行 SWIFT 平台介接，規劃建置「外幣結算平台」，以肆應「海峽兩岸貨幣清算機制」所需，協助我國發展成為「人民幣離岸中心」，增強我國金融業者在區域金融市場之競爭優勢。

(三) 「外幣結算平台」上線營運後，可降低金融機構的交易成本，進而降低企業及民眾資金調度之成本、提高資金調度之靈活度，活絡外幣市場，增進我國經濟發展之整體效益。

由主管機關指導，財金公司與各金融機構共同建構之「外幣結算平台」，是我國與國際接軌的重要金流基礎建設平台，未來，在此平台架構下，財金公司將秉持以協助金融業佈局兩岸之需求，提供最完善的金流服務、最穩定的跨行系統，暨提升我國金融產業整體競爭力而持續努力。

晶片卡時代來臨

本篇摘自 2001 年 08 月出刊之財金資訊季刊第 17 期，由時任萬事達卡國際組織江威娜台灣區總經理撰寫。

晶片卡，這張二十一世紀的主流支付工具，即將佔據你的皮夾，進而深深得影響你我的生活。而對銀行來說，晶片卡除了可以大幅減少偽冒風險、降低作業成本外，更能進一步提供全方位的客戶服務，強化銀行的競爭力。

試著想像，在不久的未來，一張卡片將可以在你的生活中扮演著財務與總管的雙重角色，從早上起床開啟你的愛車，到繳交停車費或高速公路通行費、或是搭乘捷運公車，甚或公司的門禁管制、到自動販賣機購買飲料、報紙，乃至於記錄你的健康資料或是下了班到餐廳用餐、商店去消費、兌換禮品或電子折價，乃至在網路上做為身份辨識、電子商務和行動商務，都將可用一張卡片完成。晶片卡—這張二十一世紀的主流支付工具，即將佔據你的皮夾，進而深深得影響你我的生活。

晶片卡起源

晶片做為支付工具之運用，最早是由歐洲開始推動，包括：法國、英國、德國、瑞士、芬蘭…等，從 80 年代末期、90 年代初期開始陸續推動晶片卡、電子錢等系統，持卡人可使用晶片卡作為公用電話、超市購物、乘坐大眾交通工具、加油站、停車場等一般日常支付。特別是法國更是全球第一個推動晶片卡取代磁條卡的國家，雖然其間歷經全面更換晶片卡作業系統的陣痛期，但到今天，法國已成為全球各國在發展晶片卡時最重要的取經對象。

台灣也屬於早期發展 IC 晶片卡的地區，在約十年前，財金公司的前身—金融資訊服務中心便開始推動 IC 卡，結合信用、轉帳、提款與儲值四大功能，至今觀之，仍屬相當先進之設計，而隨著時間的演進，財金公司 IC 卡也從當初的四卡合一逐漸轉型為以儲值為主的 IC 電子錢。而過去十年間，各國信用卡組織也陸續將旗下的晶片卡產品引進台灣試辦，例如萬事達卡國際組織至今仍積極推動的 Mondex 電子現金等。

為何推動晶片卡

近年來，晶片卡升級的話題，不斷在金融機構間被討論，而晶片卡的推動與發展應從那些需求來考量，不妨從以下角度觀察：

1. 安全防偽需求：台灣的信用卡偽卡問題已不容忽視，特別是盜錄磁條碼等問題，因此晶片卡就被視為信用卡防偽的救世主，希望藉由晶片卡強大的安全機制，來防堵日益嚴重的偽卡問題。
2. 個人化風險管理：晶片卡不同於以往的磁

條卡，可以把龐大的個人資料存在晶片當中，因此可以做到個人化的風險管理，包括授權、信用額度與交易管控等，降低銀行的信用風險。

3. 離線授權：信用卡交易在不少國家遭受到的主要問題之一是連線授權的電信通訊成本，晶片卡有多數交易可交由晶片來做風險控管，可以離線方式進行授權交易，降低授權成本。
4. 業務需求：越來越多的零售通路、聯名團體主動提出發行晶片卡的需求，希望藉由晶片卡強大的儲存處理能力，進行忠誠顧客回饋、客戶管理等專案，因而有發行晶片卡能力的銀行，就會成為業務發展的最後贏家。

晶片卡科技

隨著二十一世紀來臨，越來越多的金融機構開始研發推動 IC 晶片卡的可行性，但在晶片卡究竟為何？所運用的技術及考量點又是什麼，則是在邁向晶片卡之路前不得不仔細思考與研究的議題。

晶片卡顧名思義是由矽晶片與塑膠卡片所組成，一張晶片卡的誕生，必須經過一定的過程，當矽晶圓生產出來之後，經過切割後成為矽晶片，這時候的晶片與沒有加入作業系統的電腦硬體相同，一點作用也沒有，必須加入晶片專屬的 OS 作業系統，才算賦予其基本的邏輯運算與記憶等功能。在加入作業系統後，矽晶片還須經微模組（Micro Module）的製程，才能與塑膠卡片結合，通常這個過程稱為晶片著床（Embedding），之後會交由晶片卡的製卡廠商（Card Fabricator），進行訂貨機構指定的相關作業程式（Application）處理，才能交由發卡機構進行個人化（Personalization），一張晶片卡才算大功告成。

晶片卡依不同分類方式，也有不同的晶片卡，以是否與讀卡機接觸來說，可分為接觸式（Contact）與非接觸式（Contactless），非接觸式一般是做為交通與門禁管制之用。另外依是否具有 CPU 處理能力，可分為記憶卡與 CPU 卡，前者只能儲存資料，後者則有邏輯演算等 CPU 處理能力，目前一般所稱之晶片卡多數以 CPU 卡為主。

如果只有晶片卡，而沒有作業程式，所有晶片卡的功能都將無用武之地，而要在晶片卡上加裝作業程式，就必須先有作業平台（Operation System），所有的功能程式才能往上添加。一般來說，晶片卡的作業平台應考慮多種層面，茲以萬事達卡國際組織所推薦之 MULTOS（Multiple Application Operation System）多功能開放式平台為例說明如下：

一、共容性

共容性可從實體、作業平台與應用程式三個角度來看，就實體面來說，一般是規範晶片的相關硬體標準規格，「MULTOS 作業平台」就符合 ISO7816 的標準。在作業平台上，MULTOS 由於從 OS 到 API（Application Interface）都有明確的定義，因此無論向那家製卡廠商購買 Multos 晶片，都無須擔心相容性的問題。最後是應用程式的共容性，以信用卡、轉帳卡來說，國際標準的規格就是一般熟知的 EMV 標準，萬事達卡開發的 EMV 標準 PAYMENT 的規格稱為 M/Chip，意即未來在晶片卡上進行 MasterCard/Cirrus/Maestro 的交易，都必須符合 M/Chip 規格。如果是行動電話的應用程式，則有 GSM 等標準。

二、安全性

不少國家地區推動晶片卡的重要因素就來自於晶片卡完整的安全性，在交易過程中，是卡片上的晶片與讀卡機晶片，以及發卡機構主機系統交叉驗證的過程。以 MULTOS 為例，符合 ITSEC E6High 的標準（ITSEC, Information Technology Security Evaluation Criteria），是屬於國防安全等級的標準，安全認證相對高於其他的開放式作業平台。

三、應用程式開發彈性

應用程式的開發彈性關係著晶片卡功能的未來發展，MULTOS 目前支援 C、MEL、VB 與 JAVA 等程式開發語言，讓程式開發者可以依需求開發出所需的應用程式。

如前所述，有了晶片卡作業平台後，應用程式才能發生作用，CPU 晶片卡和電腦一樣，有所謂的 ROM 記憶體，一般所稱 16K、32K 則指的是 EEPROM 的容量，容量越大，可以存入的程式越多，除了上述的 EMV、GSM 等應用程式規格外，通常會應用在晶片卡的還有非接觸式的規格如 Myfair 等，以及身分辨識及忠誠顧客回饋計畫（Loyalty Program）等。

以 MULTOS V.5 為例，目前就可支援 GSM 行動電話應用程式、以及 Myfair 非接觸式晶片應用程式等。

晶片卡在生活上的應用

對銀行來說，晶片卡除了可以大幅減少偽冒風險、降低作業成本，更能進一步提供全方位的客戶服務，強化銀行的競爭力；並將客戶關係從單純的「金融服務」延伸到「生活服務」，舉凡個人身分認證、電信、醫療、忠誠客戶計畫、門禁管制，乃至於交通票證，涵蓋的範圍幾乎遍及食衣住行育樂等等生活所需。

以萬事達卡旗下的晶片卡產品 Mondex 電子現金卡和 MULTOS 多功能開放式平台，在亞太區就已被廣泛運用：

1. 在台灣：宏碁集團、富邦銀行和萬事達卡國際組織試辦的 Mondex 電子現金卡，在試辦期就廣獲持卡人的喜愛，無論是買炸雞、吃牛肉麵、在自動販賣機買飲料，甚至是上網的小額購物，都可一卡搞定；晶片餘額不足，還可選擇由信用卡帳戶加值，相當方便。
2. 在香港：Mondex 也已正式上路，持卡人可以在香港的 7-11、百佳超市等連鎖商店，甚至是小型公共巴士，使用 Mondex 刷卡付款。
3. 在韓國：Mondex 卡就已運用在 Set-Top Box（機上盒）、Kiosk 電子便利站、捷運和公車上，讓持卡人看電視上網，還可刷 Mondex 卡支付看付費電影、上網購物，或是直接在電子便利站上點餐、付款，用非接觸式感應付款支付捷運和公車費用。

事實上，晶片卡在行動商務的趨勢下，更具有無比的優勢。行動電話的 SIM 卡就是 IC 晶片卡，新一代的 IC 晶片容量足以儲存一組虛擬卡的卡號和持卡人基本資料，配合 WAP 手機，持卡人打大哥大上網，就可隨時使用 SIM 卡中的虛擬卡，支付行動商務的各種費用。甚至在未來，配合情境服務（Location Service）和藍芽計畫（Blue Tooth），進一步可讓持卡人更「科技」地支付一切費用、享受各種服務，例如拿著大哥大，對著販賣機按號碼，自動掉出可樂或報紙；走出捷運站大門，立刻收到捷運站旁有那些商店提供 MasterCard 獨享優惠等。

晶片卡在台灣的發展

目前財政部與銀行公會正嚴肅思考全面升級到晶片卡的議題，而萬事達卡國際組織除了持續依主管機關及全球組織時程推動之外，也配合會員銀行需求，投入技術及行銷支援，例如最近即將發卡的萬泰銀行京華城晶片聯名卡，萬事達卡國際組織就投入國內的技術人員提供顧問服務，這張國內第一張百貨公司晶片聯名卡，將提供持卡人更便利、安全的支付工具。而萬事達卡國際組織也將持續配合會員銀行的需求，讓晶片智慧卡時代早日來臨。

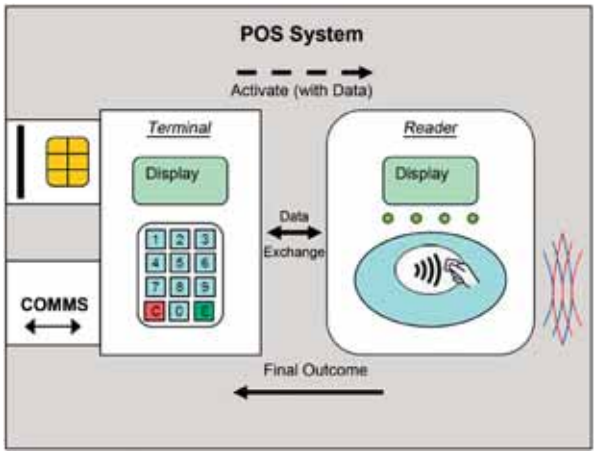
未來金流之鑰
－感應式金融卡

本篇摘自 2015 年 04 月出刊之財金資訊季刊第 82 期，由財金資訊公司研發部卡片設計組洪國峻組長、張銘洪工程師撰寫。

一、前言

目前金融消費市場的卡片支付產業隨著資訊科技進步，持續新增各種便捷應用且不斷快速成長，如何在這瞬息萬變的電子支付市場中建立消費者忠誠度與提高產品能見度，是一項非常重要的課題。以交通票證卡為例，之所以能夠如此普遍及大眾化，除本身積極與政府、金融機構、商家合作推廣外，其最大特色即採用感應式 (Contactless) 方式進行交易，卡片無須交由服務員代為刷卡或插卡，而是使用者自行持卡直接與讀卡機感應，即可快速完成交易，大幅降低消費者攜帶現金與找零的不便。根據 MasterCard 於 2014 年發布之感應支付交易統計顯示，全球使用感應支付交易量年成長率高達 35%，顯見感應支付確實能有效提升使用者之消費習慣。

國內發行之感應式卡片，大多採用與國際卡組織相同之現行標準 ISO 14443 (Contactless integrated circuit cards － Proximity cards，13.56MHz) Type A/B 主流技術，進行生產、開發、設計作業，該標準除可確保信號完整性外，更易於整合現有各類型感應式卡片與端點設備，如悠遊卡搭配信用卡所推出的悠遊聯名卡系列；另由 Europay、萬事達卡 (MasterCard) 與威士卡 (VISA) 3 大國際組織共同創立的 EMVCo，也是依循 ISO 14443 標準 (近端卡片感應) 制定 EMV 感應卡的相關規範，其中包含端末設備 (Termianl)、讀卡機 (Reader)、卡片 (Card)、Entry Point、核心功能 (Kernal) 相互間溝通協定作業方式。



資料來源：EMVCo，Book A，Architecture and General Requirements

本文謹就全球卡片感應技術之應用與國際卡組織之感應式支付交易 (Contactless Payment) 發展現況進行說明，並探討財金資訊公司 (以下稱財金公司) 感應式金融卡之應用及未來發展。

二、感應技術發展趨勢

全球最早出現的感應技術為 RFID，該技術原為二次世界大戰期間為識別敵我雙方戰機所開發，其後移轉至民間，但由於成本偏高，且有資訊外洩之虞，並未獲得廣泛應用。直至 1990 年代後，各項創新技術逐漸嶄露頭角，由 RFID 改良的技術如藍芽、QR Code、NFC 等陸續問世，感應技術開始被廣為應用。以下就目前國際上較為常見的感應技術應用，簡要說明之：

(一) RFID

RFID (Radio Frequency Identification, 無線射頻辨識) 是透過無線射頻方式取得物體標籤 (Tag) 上的資訊，與一般的二維條碼採掃描方式不同，其「工作頻率」依據應用環境有所不同，介於 120 KHz ~ 10GHz。在卡片支付市場中，目前國內消費者普遍使用的悠遊卡、一卡通、非接觸式信用卡即採用此項技術，且符合 ISO-14443 標準。

(二) IrDA

IrDA 技術係由紅外線數據協會 (Infrared Data Association) 所發表，一般用於軍事、工業或醫療產業中，如家電遙控器、臺灣的高速公路電子收費系統 (ETC，Electronic Toll Collection)；在支付市場中，則提供無卡支付方式，常應用內建於手機、PDA (Personal Digital Assistant)、手錶等手持式電子產品，並透過紅外線訊號進行交易。

(三) Bluetooth

藍芽 (Bluetooth) 技術由 RFID 演變而來，最早是由易利信 (Ericsson) 創制，並於 1999 年由易利信、IBM、英特爾、諾基亞及東芝公司共同成立 Bluetooth SIG(Bluetooth Special Interest Group) 組織，負責制定藍芽規範與推動藍芽技術，採用的是 IEEE 802.11(無線區域網路) 標準，主要應用於個人無線網路 (Wireless PAN，Wireless Personal Area Network) 行動裝置，如手機裝置、手錶、3C 產品、醫療設備、Mpos(Mobile point of sale，行動刷卡機) 等，目前最新的技術為藍芽 4.2，其工作頻率 2.4 GHz，傳輸速率理想可達 24 Mbps、感應距離最大可達 60 公尺，具有高速、低功率消耗優點。

(四) QR Code

由日本 Denso WAVE 所創制的 QR Code (Quick Response Code) 二維條碼讀取技術，比起傳統的二維條碼，在存取上較為方便，且儲存空間也較大；一般應用於自動化文字傳輸、數位內容下載、網址快速連結、身分識別與商務交易。

(五) NFC

NFC(Near Field Communication，近距離無線通訊) 係由 PHILIPS、NOKIA 與 SONY 共同研發，也是以 RFID 為基礎演變而來的

近端感應技術，規格涵蓋 ISO 14443、ISO/IEC 18092、FeliCa，主要應用於行動裝置中，NFC 感應距離在 20 公分內，工作頻率 13.56MHz，雖然其傳輸距離不及 RFID 與藍芽，但設定程序上較為簡單，且安全與保密性也較高，可應用於 NFC Tag 的資訊、NFC 設備間資料交換或模擬實體卡片 (搭配安全元件) 行為。

附表：感應技術相關應用

感應技術	RFID	IrDA	Bluetooth	QR Code	NFC
一般應用	門禁卡 電子鑰匙 eTag 倉儲管理 電子票證等	家電遙控器 手持裝置	智慧手機 手錶 PC 週邊	購票 身分識別 資訊提供	電子標籤 行動裝置 卡片模擬
優 點	距離較長	成本低 安全性高	傳輸速度快 距離較長	下載對應 app 即可使用	操作較簡單 安全性高 保密性較高
缺 點	大部分偏被動 成本較高	傳輸距離短 易受阻礙	操作較複雜	操作較繁瑣	傳輸距離短

隨著感應技術基礎建設日漸完善、個人行動裝置普及化及行動支付功能越加多元，消費者支付方式將逐漸由卡片進展至行動裝置，亦即消費者到商家消費，只須透過行動裝置進行感應，即可快速完成交易，大大減少使用者多卡在身的困擾。

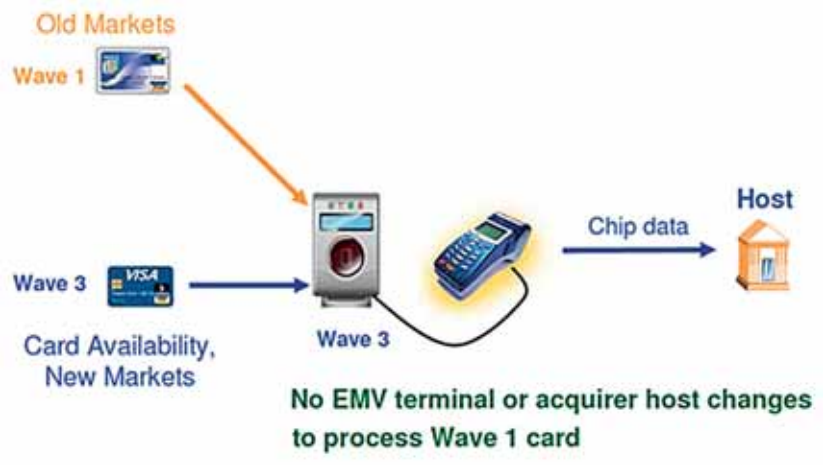
三、國際卡組織就感應技術之發展應用

目前，各國際卡組織在感應技術發展上，雖各有其制定的標準，但原則上皆遵循 EMVCo 規範發展，以下簡要說明 VISA、MasterCard、JCB、UnionPay 近幾年的感應式交易應用：

(一) Visa payWave

VISA 於 2007 年推出具感應功能的 payWave 卡後，根據 VISA 統計，西元 2014 年 7 月在新加坡地區已有超過 2 百萬以上的用戶，約佔新加坡總人口數約 500 萬的 40%，且每個月有超過 21.5% 的持卡人使用感應式功能進行交易，全球交易則每年成長 20~30%，可見感應式技術所產生的影響不容小覷。

VISA 發行的感應卡，目前共有兩種規格，早期所發行的 WAVE 1 卡並未提供晶片感應功能，安全性上也較低，而後期所發行的 WAVE 3 卡即為晶片感應卡，也相容於舊款感應式收單端末機台。



資料來源：VISA

VISA 感應技術規格，是在 EMVCo 的規範下所發展出的 VCPS(Visa Contactless Payment Specification)，所有受理卡片的端點設備及發行的感應卡，皆須依循 VCPS 規範設計，同時最新的 VCPS 2.1，也支援行動支付的相關功能延伸。

(二) MasterCard PayPass

MasterCard 所推出的感應式系統 PayPass，因應消費環境差異，提供兩種感應模式，一種專門提供給美國地區使用的磁條感應模式，另一種則是提供給其他地區使用的晶片感應模式。

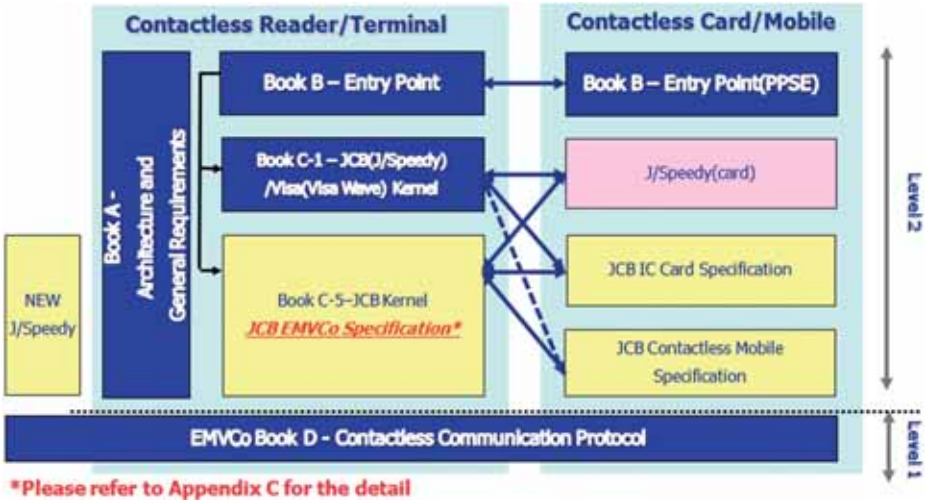
資料來源：MasterCard

在磁條感應模式上，MasterCard 提供Dynamic CVC3 (Card Validation Code) 的驗證方式，用以提高交易安全性；而晶片感應模式則採用與接觸式交易相同的 ARQC (Authorization Request Cryptogram) 驗證方法。

(三) JCB J/Speedy

由於感應市場具有極大商機，JCB 國際組織於 2007 年與 VISA 國際組織合作，推出具感應功能的 J/Speedy，使得 JCB 感應卡可於我國任何符合 VISA 認證的端末機台進行交易，惟其於我國所推出之感應卡，僅適用於國內，無法提供跨國功能；嗣為服務客戶，於 2014 年 7 月再推出 New J/Speedy，相容於原 J/Speedy 環境，且適用於國外，更納入未來手機行動支付相關功能。

JCB 發布 New J/Speedy 功能後，財金公司於同年底完成 JCB 收單平台感應式交易及發卡授權功能之建置，目前正配合金融機構與 JCB 進行收單及發卡相關測試，待完成整體認證後，即可協助金融機構於國內偕同 JCB 快速發展感應式業務。



資料來源：JCB

(四) UnionPay QuickPass

銀聯國際組織 (UnionPay International) 早期所推出的銀聯晶片卡，是依循中國人民銀行所發布的晶片規格 (簡稱 PBOC)，其後為增加品牌國際化與能見度，在 2014 年 5 月正式加入 EMVCo，其晶片規格也正名為 UICS (UnionPay International Chip Specification)，而銀聯國際組織所發行的具感應功能的銀聯閃付 (QuickPass) 卡，則是架構於 UICS 下的產品，僅支援晶片感應式交易，目前在大陸、澳門、香港皆已實際應用。

財金公司於 2013 年第二季完成國內銀聯收單平台晶片化，嗣於 2014 年第三季完成銀聯收單平台感應式交易系統功能建置，合作金庫銀行於 2015 年 1 月底通過該平台認證，預計同年第一季前完成特約商店佈建，成為臺灣第一家支援銀聯閃付功能之收單金融機構。

資料來源：UnionPay International

四、感應式金融卡之特色及應用

科技不斷創新變革，感應技術之應用不再只侷限在卡片上，更延伸至任何可搭載感應式功能的載具上，如鑰匙圈、手機背套、行動裝置等，放眼未來，感應技術可應用於身上的配件，如電子手錶、電子手環等電子設備，甚至可透過指紋辨識或特定手勢，做為身分識別的工具，提高交易安全及便利性，感應技術所帶來的效益，不僅大幅改變現行金融消費市場之支付行為，更是行動支付未來發展的重要利基。為快速協助金融機構發展各國際組織之感應式卡片應用外，也為擴展我國金融卡感應式功能，財金公司每年參與 Visa、MasterCard 國際組織年度各類會議，研讀國際組織公告及規格，清楚掌握各組織新種業務之推出及發展脈絡，以持續不斷地進行相關業務發展及技術研究，並因應市場變化，積極投入系統建置，協助金融機構及時、快速並以最低投資成本切入市場，期能成為金融機構發展卡片業務之堅實後盾。

近年來，財金公司持續針對金融卡功能不斷創新突破與提升，隨著感應技術日趨成熟，已於 2014 年 3 月完成感應式金融卡平台之建置，並採用國際標準 ISO14443 通訊機制，在小額支付應用上與現行信用卡相同，即消費金額 3,000 元以下之交易不用輸入密碼、無須簽名，即可快速完成結帳 (交易流程詳如下圖)，對消費者與商家而言，方便性與安全性都大為提升；現行所推廣的「感應式晶片金融卡」，除具備原有免簽名、免現金 (亦可避免收到偽鈔)、免找零、免手續費、免儲值之便利外，更進一步提高商家與消費者交易的速度，適合在一般商家、攤販、停車場、醫療院所等須快速結帳的環境使用。

資料來源：財金公司 (感應式金融卡交易流程)

謹臚列下表，方便讀者快速瞭解各產品間之差異性。

組織	FISC	VISA	MasterCard	JCB	UnionPay
品牌	SmartPay	payWave	payPass	J/Speedy	QuickPass
Logo					
卡片感應方式	晶片	磁條 / 晶片	磁條 / 晶片	磁條 / 晶片	晶片
端末受理方式	晶片	磁條 / 晶片	磁條 / 晶片	磁條 / 晶片	晶片
安全驗證	TAC	iCVV/ARQC	CVC3/ARQC	CAV3/ARQC	ARQC
授權方式	Online	Offline/Online	Offline/Online	Offline/Online	Offline/Online
相關規格	FISC 6.20	VCPS VSDC	PayPass － Mag Stripe & M/Chip4	JCB-IC-CPS	UICS
ISO 標準	ISO 14443 (Contactless)、ISO7816 (Contact)				
行動支付 感應方式	NFC	NFC	NFC	NFC	NFC

自我國於 2003 年進行金融卡全面晶片化起，財金公司即全力協助金融機構拓展晶片金融卡相關應用，包括金融卡 SmartPay、自助加油等，甚且延伸觸角至日本，建立晶片金融卡與全球接軌的第一個重要里程碑。財金公司刻正積極協助金融機構開拓感應式晶片金融卡消費據點至小額消費市場，除活絡小額及感應式交易市場外，也提高商家每筆交易之速度並增加營業收入，且可有效減少現金管理問題。此外，財金公司也與臺灣行動支付公司合作，利用「感應式晶片金融卡」之安全及便利性，於 2014 年底提供民眾使用行動裝置搭載金融卡 SmartPay 應用服務，進行近端或遠端之消費，感應式晶片金融卡將以實體及行動兩種不同方式呈現，讓民眾時時刻刻體驗金融卡帶來之方便性。目前，感應式金融卡收單機構計有土地銀行、合作金庫銀行、華南銀行、台新銀行等 4 家參加，刷卡設備佈建台數於 2015 年 1 月已達 1,115 台。

綜觀國內民眾的消費習慣，現行大部分仍採用「現金」為支付工具，然藉由「感應式晶片金融卡」推動消費者體驗更便捷與安全的支付方式，進而常用乃至慣用，可望改變我國整體消費習性，促進健全之支付環境，持續開創更多創新及便利的金流體驗。

※ 參考文獻 / 資料來源：

1. EMV Contactless Book A: Architecture and General Requirements。
2. 財金資訊季刊第 79 期－小額支付大變革：感應式金融卡。

我國行動支付邁入新紀元

本篇摘自 2015 年 01 月出刊之財金資訊季刊第 81 期，由時任 IDC 國際數據資訊公司卞志祥台灣區總經理、吳乃沛資深市場分析師撰寫。

一、前言

有關「行動支付」的商機與挑戰，從 2007 年智慧型手機出現之後就一直是科技業、電信業、金融業與零售業者所關注的重要議題之一。正由於行動支付生態系統涉及以上多方產業的不同專業資源與標準；如何制定商業協議與技術介接之標準化，就是拓展異業結合與推廣行動支付產業應用的首要課題。目前國際組織包括全球行動通訊系統協會 (Global System for Mobile Communications Association，簡稱 GSMA)、全球平台組織 (GlobalPlatform，簡稱 GP)、歐洲支付委員會 (European Payments Council，簡稱 EPC) 以及近距無線通訊論壇 (NFC Forum) 等，都同意以「信任服務管理者 (Trusted Service Manager，簡稱 TSM)」來稱呼此中介角色。

截至今 (2014) 年 10 月底，我國共有 4 家 TSM 公司：中華電信公司、聯合行動國際支付公司、群信行動數位科技公司以及今年 9 月 5 日甫成立的「臺灣行動支付公司」。其中臺灣行動支付公司結合國內三大結算機構、27 家金融機構及悠遊卡公司等共同建置國內行動金流平台，預計第一階段金融支付將於 12 月底上線。此舉讓眾多關注我國行動支付產業發展的人認為：喊了多年的行動支付將真正於 2014 年底全面起跑，開啟我國行動支付的新紀元。而隨著 Apple 在 9 月 9 日 iphone6 的發表會上宣布將以 Apple Pay 進入支付服務市場的消息公開，更是炒熱了行動支付市場的行情。

本文將從全球行動支付市場規模談起，討論最近的新興技術與商務模式發展，並從消費者行動化、異業結合的生態系統、法規的修訂以及終端設備的整合與升級等四大條件來分析我國推動行動支付產業的機會與挑戰。

二、全球行動支付市場的發展

根據 IDC Financial Insights 的估計，2014 年全球行動支付的市場規模約為 3,338 億元美金，其中透過手機等行動裝置進行線上交易的傳統遠端行動支付占比目前高達 96.9%；而透過 NFC 技術與 Barcode 掃描的近距支付目前占比雖只有 3.1%，但後續成長力道可期。IDC Financial Insights 預估，近距支付未來三年將以 205.5% 的年複合成長率快速成長到 2017 年的 2,966 億元美金，其對整體行動支付市場的占比也將大幅增長到 27.2%。(見圖 1)

圖 1　全球行動支付市場規模 (2013~2017)
資料來源：IDC Financial Insights, 2014

如果進一步以「點對點平台 (Peer-to-Peer Platforms, 簡稱 P2P)」、「行動商務 (mCommerce)」、「近距無線通訊 (NFC)」以及 Barcode 掃描等四種傳輸行動支付的方式來看未來市場的發展，則遠距支付的 P2P 與 mCommerce 雖仍分別以 51.8% 與 35.7% 的高年複合成長率擴展市場規模，但近距支付的 NFC 與 Barcode 的成長力道更加強勁，IDC 預估兩者的年複合成長率將分別達到 226.6% 與 150.2%，快速影響整體行動支付市場的占比分配 (見圖 2)。

圖 2　全球行動支付方式市場規模占比 (2013~2017)
資料來源：IDC Financial Insights, 2014

對於遠距支付與近距支付在未來行動支付市場占比的消長，IDC 認為主要原因來自於新興技術與商務模式的發展，對使用經驗、服務供應商的自主權與安全性層面所帶來的革命性衝擊。

三、 行動支付的新興技術與商務模式

近來與行動支付相關的新興技術 (特別是在近距支付部分) 與商務模式發展有：

(一) 主機卡模擬 (Host Card Emulation，簡稱 HCE)

今年 3 月，NFC 論壇發表公開聲明，表態支持 Google Android 4.4 作業系統 KitKat 中內建的 HCE 技術。HCE 的概念，就是透過手機中的 app 或是雲端的伺服器軟體來完成安全元件 (Secure Element，簡稱 SE) 的功能：NFC 控制器自外部讀寫從前端接收到的卡片資訊後，由作業系統發送到手機中的 app，或是透過行動網路發送到雲端的伺服器來完成資料交換，兩種過程都不需要透過存放在手機中的 SE 晶片來完成。這使得金融機構或支付服務供應商不再受到手機內置 SE 的限制，不但可以直接透過 app 取得控制權，也可免除行動支付服務過程中來自運營商的「空中下載 (Over-The-Air，簡稱 OTA) 平台」等介接費用而降低建置與營運成本。更重要的是，服務供應商可以自主開發或整合 app 加值功能，創造額外的營收。

另一方面，傳統將 SE 晶片放到「用戶識別卡 (subscriber identity module card，簡稱 SIM 卡)」的模式仍有其獨特的好處。除了 SE 的實體隔離可確保一定程度的安全性之外，最主要是 SIM 卡並不受到開啟手機電源與連網等的限制，可以完成各種離線 (offline) 的近距支付交易 (見圖 3)。

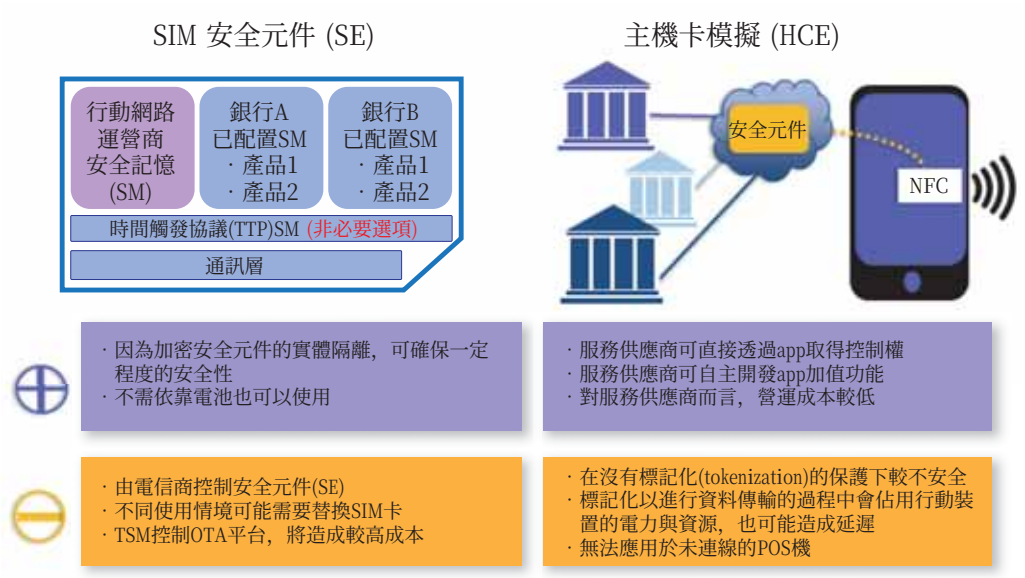


圖 3　SIM 安全元件與 HCE 模式的比較
資料來源：IDC Financial Insights, 2014

(二) EMVCo 標記化 (EMVCoTokenization)

今年 9 月 Apple 公司宣告以 Apple Pay 進入行動支付市場，並宣稱該解決方案已取得 EMVCo 的標準，引起大家對 EMVCo 的關注。EMVCo 是負責制定與維護國際支付晶片卡標準規範的專業組織，其現有成員包括 MasterCard、Visa、JCB、Discover、美國運通 (AE) 與中國銀聯等六大國際發卡組織。今年 3 月，該組織正式公開發表一套標準規範：在消費者持信用卡進行行動支付的過程中，交易資料的交換是將信用卡「永久帳號 (permanent account number，簡稱 PAN)」轉換成某種隨機編碼產生的 token 後再傳給商家，商家收到 token 透過收單機構傳給國際發卡組織再傳給消費者的發卡銀行，發卡銀行將 token 還原為用戶帳號之後完成交易授權。值得一提的是，整個 tokenization 是透過特定的區域支付網路來完成。此外，這套標準的制定其實與行動支付風險管理的責任分攤息息相關，最主要是要解決「線上信用交易或卡片不在場 (Card-Not-Present，簡稱 CNP)」的安全問題。目前，這套新的標準是否能夠得到大多數零售商家的支持仍有待觀察。

(三) 行動 POS 第二代 (mPOS v2)

目前有越來越多外掛於行動裝置的卡片讀取器，或是可下載的行動應用程式，可以支援小型商家完成實體卡片或行動信用卡的讀取或寫入來傳輸交易資料。為了在競爭激烈的市場中勝出，行動 POS 第二代的解決方案新增許多加值功能，將朝向行動 POS 支付的個人化應用發展，目前主要的新增功能與使用案例包括：客戶消費紀錄分析、識別客戶的往來銀行、個人專屬銷售代表或客服、加速熟客的交易時間、依照消費喜好發送不同的促銷廣告等等。

(四) 巨量資料分析 (Big Data Analytics)

在支付過程中，無論是發卡或收單機構都會收集到許多的資料，包括：交易資料、通訊系統中的 email 往來、表單、與即時訊息等的文字、點擊流與網路日誌、錄影與錄音紀錄、各種機器與機器間的資料交換、社交網路上的聊天紀錄以及行動裝置傳送的「全球定位系統 (Global Positioning System，簡稱 GPS)」等等。金融機構以往收集這些資料之後，大都是儲存管理而沒有善加分析利用，但有越來越多的金融機構將這些資料交互分析之後，據以進一步改善營運效率或推出新的應用與行銷活動 (見圖 4) 。

(五) 支付中心 (Payments Hub)

今年 9 月，銀行與支付技術服務的全球領導廠商 FIS(www.fisglobal.com/) 宣佈以 4.93 億元美金完成對 Clear2Pay 的收購。根據 FIS 的說法，這項併購最主要是來自於其金融業客戶對於「支付流程集中化管理」的強大需求。Clear2Pay 具有以「服務導向架構 (service-oriented architecture，簡稱 SOA)」為基礎的組件程式庫作為其「開放式支付框架 (Open Payment Framework)」，同時可以為 FIS 帶來如測試、培訓與諮詢等的附加服務。

事實上，許多大型的金融機構很早就建置類似「支付中心」的平台 (見圖 5)，不過隨著各種新興支付商務模式的發展，中小型金融機構也將產生這類的需求。此外，IDC 預測將有

顯著比例的支付類型會因為跨境支付 (cross-border payments)、通路的複雜化、高手續費、較長的結算流程等因素，將外包給外部或雲端的支付服務平台。

應用	資料來源	使用案例
促銷	交易＋社交	聯昌國際銀行：金融卡促銷活動
以位置為基礎的行銷	交易＋位置	華僑銀行：分行地理圍欄 (geo-fencing)
消費者資料分析與分類	交易＋外部	華僑銀行：羅賓森卡
個人化財務管理	交易	華僑銀行：支出追蹤服務 馬來亞銀行：People like you
防偽管理	交易＋位置	Visa：即時偽卡記分
防偽管理	交易＋社交	Monext SAS：識別詐騙
營運效率	交易＋物聯網	星展銀行：ATM 網路優化

圖 4　金融機構在巨量資料分析上的應用與使用案例
資料來源：IDC Financial Insights, 2014

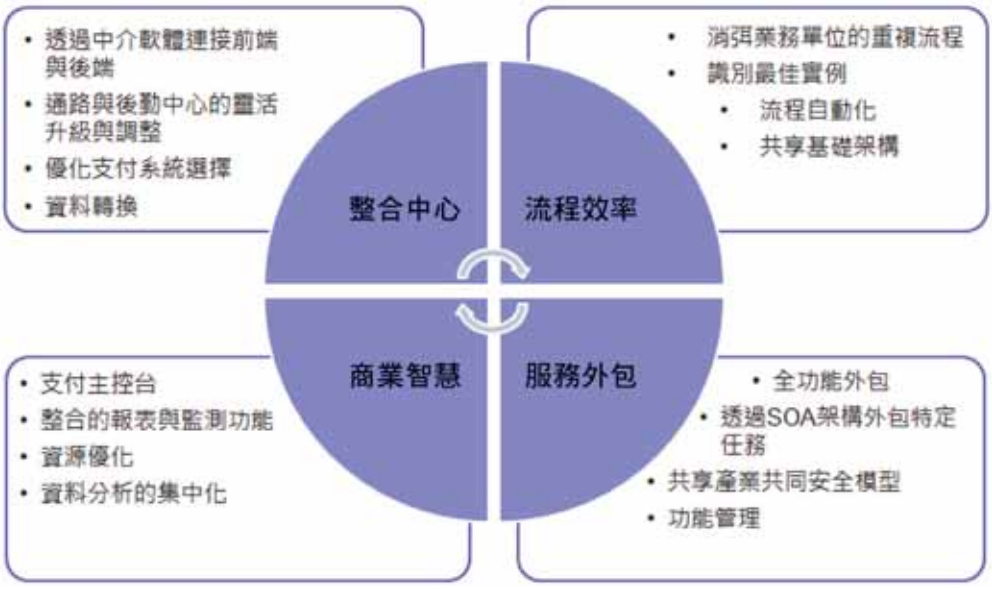


圖 5　支付中心來自金融機構對支付流程集中化管理的需求
資料來源：IDC Financial Insights, 2014

四、我國行動支付邁入新紀元

(一) 我國消費者對行動化的擁抱

根據 IDC 的行動電話追蹤報告，我國市場的智慧型手機與功能型手機的年出貨量，從 2007 年迄今呈現極為明顯的一漲一跌情況；2007 年，功能型手機年出貨量約為 643 萬支，當時智慧型手機的年出貨量還不及其十分之一。其後，智慧型手機以驚人的成長率於 2011 年正式超越功能型手機的年出貨量。IDC 預估，今年我國智慧型手機的年出貨量將逼近 900 萬支，是功能型手機出貨量的近 18 倍 (見圖 6)；而近三 (2012~2014) 年的智慧型手機總出貨量將達 2,258 萬支，直逼我國人口總數。

圖 6　我國手機年出貨量 (2007~2014)
資料來源：IDC Mobile Phone Tracker, 3Q14

不僅智慧型手機的普及率快速攀升，消費者的手機使用情況也有大幅度的轉變。根據 IDC 行動服務市場追蹤報告，行動數據與行動語音兩領域之間也呈現出類似的漲跌情形。2010 年我國行動電信市場的規模為新臺幣 1,985 億元，其中 85.6% 來自行動語音服務，14.4% 來自行動數據服務；然而到了 2013 年，雖然整體行動電信的規模成長至新臺幣 2,148 億元，但行動語音的營收占比降至 63.9%，行動數據則相對升高至 36.1%(見圖 7)，這意味著人們對於智慧型手機的依賴，更多地轉向上網、收發 email、行事曆安排、各種遊戲或影音娛樂等非傳統通話功能。

圖 7　我國行動電信營收占比 (2010~2013)
資料來源：IDC Mobile Services Tracker, 2H13

可以預見的是，在一指連網的時代，消費者將越來越依賴智慧型手機這個集多功能於一身的工具，來管理生活中的各個層面，不僅是更高效的工作與無遠弗屆的社交娛樂，也包括不受時空與金額限制的交易與消費。

(二) 異業結合的生態系統

行動支付的生態系統主要跨及三大產業：行動、金融與零售。以往這些產業都有相關的法規、標準與商業模式形成其各自的生態系統，而要推動整體行動支付產業，在確認消費市場中行動化的普及率之後，首要課題就是跨產業間依據共通標準來升級基礎架構、介接技術平台並達成商業協定。行動支付生態系統中的中介平台，主要包括行動運營商與發卡機構間的 OTA 平台與 TSM 平台，以及收單機構與商家之間的支付平台與訂單執行平台。這些介接平台之所以重要，除增加消費者的便利性之外，最主要就是：一張智慧晶片卡 (不管是實體還是裝置在手機上的虛擬卡片) 本身並沒有直接輸出的能力，而必須依賴行動裝置、終端機、介接平台與後端主機等的作業環境與應用程式中的安全機制，才能確保消費者的交易安全以及商家與認證機構的風險控制。此外，中介的平台也能降低小型機構或商家的進入門檻，而能進一步擴展行動支付的市場發展。(見圖 8)

圖 8　行動支付生態系統
資料來源：IDC Taiwan, 2014

目前我國 4 家 TSM 公司主要就是要完善圖 8「行動生態系統」與「金融生態系統」之間的中介運作。此外，4 家電子票證機構 (悠遊卡、一卡通、愛金卡與遠鑫) 與多家銀行為加速推動行動支付服務，也陸續推出各類結合行動應用的智慧卡或電子錢包服務。截至今年 9 月底止，我國各類智慧卡的流通數量與交易金額如圖 9 所示，可以看出金融卡無論是在流通卡數或交易金額上都較另兩類卡高出許多，IDC 預期未來我國推出手機金融卡的服務，使手機可以轉帳與繳稅，將有利於行動支付市場的大幅成長。

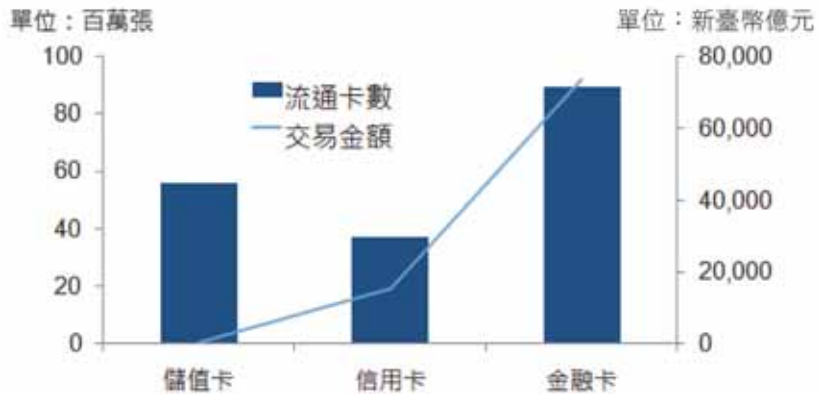


圖 9　我國各類智慧卡的流通數量與交易金額 (截至 2014 年 9 月底)

資料來源：金管會

此外，隨著消費者對行動技術的熟悉度逐漸提高，對商家與金融機構的期望也已經改變。在此趨勢之下，IDC 認為商家與金融機構將快速面臨到來自用戶經驗轉變以及新型態服務系統等的挑戰；而如何讓消費者有感並追求發展各種與行動應用相關的加值功能與創新服務，以建立未來行動商務模式，即成為兩大產業在短期間未來維持戰略的重要籌碼與致勝關鍵。

(三) 法規的修訂與增訂

事實上，要使金融機構與零售業之間更緊密地合作拓展行動支付市場，另一個重要的關鍵在於圖 8 右上方「支付平台」的有效運作，這涉及國內相關法規是否因應新的消費趨勢而有所修正。根據臺灣行動支付公司統計，2013 年我國消費者在網路上的交易，光是在信用卡跨行交易部分，金額就高達新臺幣七千多億元，相當於全年境內信用卡交易金額的 36.8%。對於金融機構來說，除電子商務結算業務的快速成長之外，網路交易與跨行交易之認證與結算的流程都將複雜化並增加風險，因此有必要透過支付中心平台來協助處理。許多電子商務快速發展的國家，皆允許非金融機構經營電子支付平台，並立法管理第三方支付業者。今年 9 月，行政院終於通過「電子支付機構管理條例」草案，使我國電子商務的發展出現新契機。

有關我國金融法規方面，尚有部分不利於行動支付市場擴展的規定，包括：電子票證的儲值金額限制、銀行投資非金融相關事業的持

股比例上限、以及手機信用卡的申請規定等。此外，未來手機金融卡、跨境支付、 Apple Pay 等服務推出之後，會有哪些限制與管理辦法也值得持續關注。

(四) 終端設備的升級與整合

目前全臺灣的支付終端設備數量如圖 10 所示 (截至今年 9 月底)。其中，符合 EMV 感應式標章的信用卡感應式終端機 (contactless payment terminal) 約三萬多台，僅占整體支付終端機 (含傳統刷卡機與晶片讀卡機) 的 10% 左右，升級的成長空間仍大。以往，我國零售商家有關這部分的軟硬體投資，大多是與發卡機構合作，估計這種模式在行動支付的時代也不例外。此外，我國還有四萬多台的電子票證感應器，支援目前流通卡數逼近 5600 萬張的儲值卡或電子票證智慧卡。交通部公路總局已公布公共運輸多卡通電子票證整合補助辦法，有利於交通運輸業者的系統升級或整合。至於零售業部分，目前電子票證公司的做法主要是利用集團的力量跨業水平整合，以增加整體集團的利益。

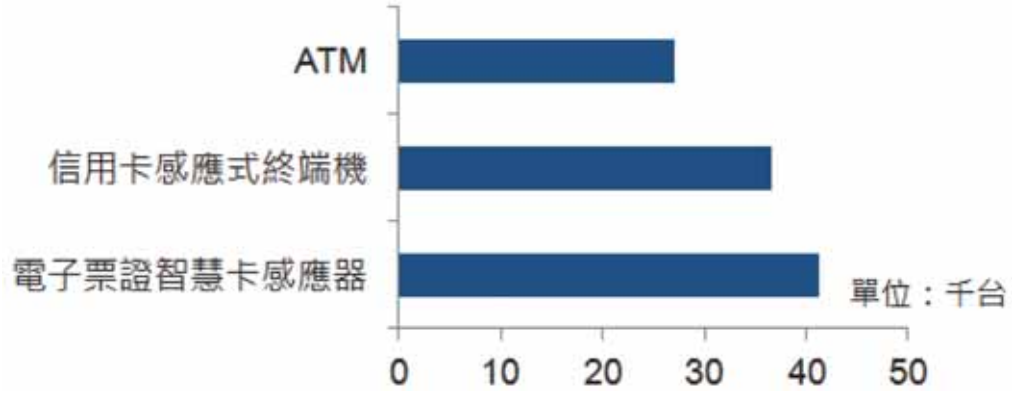


圖 10　我國支付終端設備數量 (截至 2014 年 9 月底)

五、結語

Apple Pay 的推出，再次炒熱行動支付的議題，很多的討論都圍繞在手機是否真的能取代實體錢包，以及各種「無貨幣」時代的想像；但 IDC 認為，這樣的改變並不會在一夕間發生。本文從消費者行動化、異業結合的生態系統、法規的修訂以及終端設備的整合與升級等層面來看我國的發展情況，認為目前確實是客觀條件已俱備、主觀認知也相對成熟的起跑位置。尤其是金融機構，從行動遠距支付這個更大的市場著眼，希望在明年推出「手機金融卡」服務，若能有主管機關即時且良善的管理辦法以及中介平台的安全機制配合，將有利於行動支付的快速成長。此外，電子票證業者透過集團力量進行跨業水平整合的商業模式，也將刺激傳統金融機構與零售商家或電子商城之間的合作，進一步透過新興技術發展出創新的服務以吸引消費者。

至於新興市場的開發，像是民宿、傳統夜市或小吃店等，因為涉及開立發票與營業稅的議題，恐怕不適合於現階段討論。畢竟，還有 90% 尚未升級為感應式終端機的 30 幾萬家特約商店，等著有興趣競逐行動支付市場的金融機構著手評估合作。整體來說，IDC 認為現在這個時間點對行動支付產業發展是有利的：因為消費者與媒體的關注與興趣，將有助於大眾對行動支付世界的想像，也會促使業者加速各種解決方案的開發。

※ 參考文獻 / 資料來源：

1. IDC FutureScape: Worldwide Financial Services 2015 Predictions, November 2014 Doc #252315。
2. The many new things in payments, October 2014, Doc #AP250828。
3. Is Apple Pay Good or Bad News for Mobile Payment Rivals?October 2014, Doc # lcUK25185314。
4. Technology Selection: Worldwide Mobile Payments 2012–2017 Forecast, November 2012 Doc #FIN237814。

整合金融資源 共創支付產業新紀元－我國之「PSP TSM 平台」

本篇摘自 2014 年 04 月出刊之財金資訊季刊第 78 期，由財金資訊公司業務部專案企劃組陳詩蘋組長、董乙璇專員撰寫。

一、前言

隨著行動裝置快速普及，智慧型手機、平版電腦已經成為民眾每日重度使用的重要媒介，更進一步衍生出行動應用服務的潛在市場。據網路設備業者－思科系統公司 (Cisco Systems, Inc.) 預測，至 2016 年全球行動連網設備將超越 100 億台，而連網設備流通數亦將超越全球 73 億人口數，如能結合「行動支付」功能，讓行動裝置變身為數位皮夾，使民眾透過智慧型手機、平版電腦就能輕鬆付款，處理日常生活之消費購物、轉帳、繳納帳單及稅款等事宜。

綜觀全球電子商務發展，「行動支付」已成為未來金流服務的新趨勢，傳統的卡片產製與生命週期管理，因為發卡者與服務提供者多為同一金融機構，發卡者也是卡片的擁有者，然而「近場無線通訊」(Near Field Communication，以下簡稱 NFC) 技術的興起，行動設備上用來儲存各服務應用程式的安全元件 (Secure Element，以下簡稱 SE)，如 USIM 卡、SD 記憶卡、手機內建 NFC 晶片或外掛式裝置等，已非單一服務供應商或發卡者能獨自擁有。為確保相關應用服務於卡片的安全性及動態之特性，卡片應用的下載、安裝、個人化等，乃至於後續的管理，已逐漸朝向「空中下載」(Over The Air，以下簡稱 OTA) 技術發展，亦即金融機構支付工具與相關應用服務可透過安全的網路傳輸方式置入行動裝置 SE 中。

而「信任服務管理平台」(Trusted Service Manager，以下簡稱 TSM) 即全球行動通信協會 (Global System for Mobile Communications Association，簡稱 GSMA) 為解決行動支付、行動商務新技術領域所提出的一項新概念，TSM 即接受服務供應商 (Service Provider，如信用卡、金融卡、儲值卡、電子票證、點數卡、優惠券等之發行業者) 之委託，進行相關行動支付、行動商務服務的下載、安裝及個人化的被信賴獨立第三方機構。

TSM 可說是「行動支付」成功運作之核心關鍵，目前全球 TSM 發展現況，除新加坡由政府出面主導外，其他國家 TSM 服務多朝向依產業特性、技術規格、作業需求等專業領域，各自發展金融業 PSP (Payment Service Provider，支付服務供應商) TSM，再與電信業 MNO (Mobile Network Operator，行動網路運營商) TSM 介接之趨勢。

鑑於各國結算機構，如中國銀聯公司 (中國銀聯)、香港銀聯通寶公司 (JETCO)、韓國 KFTC (Korea Financial Telecommunications and Clearings Institute)、紐西蘭電子支付公司 (PAYMARK) 等，紛紛出面經營並主導金融 TSM 發展；為協助我國金融產業發展，避免重覆投入造成資源浪費，並促進「行動支付」系統之健全發展，特由具備「PSP TSM」特性與跨行金流服務經驗機構，即財金資訊股份有限公司 (以下稱財金公司)、財團法人聯合信用卡處理中心 (以下稱聯卡中心) 及財團法人台灣票據交換業務發展基金會 (以下稱台灣票交所) 共同籌設「臺灣行動支付股份有限公司」(以下稱「臺灣行動支付公司」)，並邀集全體金融機構參股，共同規劃建置我國金融「行動支付」服務管理平台 (PSP TSM)，以打造完善的「行動支付」環境。

二、全球市場發展概況

在「行動支付」生態系統中，係由金融機構、電信運營商、服務提供者、TSM 等單位扮演核心角色，目前全球歐美與亞太主要國家地區無不陸續投入「行動支付」發展，以下分就各國推動 TSM 平台發展概況說明之。

(一) 日本

自 2005 年起，日本的非接觸技術主要採用其特定的 FeliCa 規格，該項規格目前與其他地區普遍使用的 ISO 14443 的 NFC 標準並不相容。FeliCa 已使用在許多的商業性產品，不只是一般的晶片卡，也包含行動裝置、個人電腦及消費性電子產品。在非接觸式付款的應用上，日本已發行 1 億 3,500 萬張 FeliCa 卡片，且至少有 2,500 萬個 FeliCa 晶片裝置於行動設備上。FeliCa 於 2004 年開始行動非接觸商業服務 (手機電子錢包)，截至 2011 年已經有 70 種以上的應用，且提供超過 100 款不同的行動設備互通使用。據 FeliCa Networks 表示，在日本已有 6,600 萬的用戶擁有手機電子錢包，且有約 80% 新銷售的手機具備 FeliCa 晶片。儘管 FeliCa 在日本的發展相當成功，但近年來 FeliCa 技術於其他國家的推展並不順利，且有不少地區捨棄該項技術。

基於目前國際商業市場上均採 ISO 14443 的 NFC 標準，因此，近年來日本的電信業者也開始思考支援該項標準。目前日本 TSM 係採專業分工、業務合作的方式辦理，共計有三 個 MNO TSM (NTT DOCOMO、KDDI、SOFTBANK) 及 二 個 PSP TSM (DNP、TOPPAN) 以多對多的方式相互介接。

(二) 美國

美國三大電信行動業者 Verizon Wireless、AT&T Mobility 與 T-Mobile USA 於 2010 年底合資成立 ISIS 公司，整合資源共同建置具備全國性採用智慧型手機及 NFC 技術之 TSM 行動商務平台 (簡稱為 ISIS 商務平台)。另，金融產業如 American Express、Chase、Wells Fargo 亦已建置 PSP TSM，與 ISIS 介接，換言之，經由 ISIS 商務平台，信用卡服務即可透過特定行動裝置與各金融機構伺服器直接連結，以 ISIS 商務平台為中介，並不會從中擷取任何敏感資料，僅提供技術性應用服務。

(三) 新加坡

新加坡資訊通信發展管理局 (IDA) 於 2011 年正式宣布通過「合作徵求計畫」，並與晶片卡製造商 Gemalto、星展銀行、花旗銀行、付費卡供應商易通公司 (EZ-Link)，以及三家電信公司 (第一通、新電信及星和) 共七家公司，共同建立具備互通性之 NFC TSM 整合性系統平台。自 2010 年 12 月開始持續 8 個月試營運，由 Gemalto 負責開發 TSM 平台，星展銀行、易通公司及花旗銀行透過此 TSM 平台發行支付卡產品，採用 NFC「行動支付」解決方案 (N-Flex)，並於 2012 年 8 月正式付諸商業運轉。除支付業務外，Gemalto 也將與服務供應商合作，共同部署 NFC 非支付行動應用服務，如互動式 NFC 海報廣告、行動優惠券與票務服務。消費者只須購置 NFC 手機或相關 NFC 裝置，即可享受 NFC 服務帶來的便利。

(四) 南韓

目前，韓國三大行動通信系統業者－SKT、KTF 及 LGT 均已各自發展 MNO TSM 服務，另韓國銀行清算機構－韓國金融電信及清算研究所 (Korea Financial Telecommunications and Clearings Institute, KFTC)，與 SKT、KTF 合作，於 2013 年 3 月宣布推出 NFC 支付服務 BankWallet，該支付服務以銀行帳戶為基礎，有 18 家韓國銀行已經簽署協定並為其消費者提供該服務，BankWallet 系統會將持卡人的授信憑證存放於 NFC 手機的 USIM 卡中，以手機進行支付服務。

(五) 中國大陸

中國銀聯整合中國全體金融機構，建置 PSP TSM 服務，2013 年 6 月中國銀聯與中國最大手機營運商 (中國移動通信公司) 合作，實現雙方 TSM 對接，9 家銀行參與手機空中開卡業務，為手機支付部署了 140 萬非接觸式終端機，第一輪在 14 個城市啟動移動支付，電子錢包中發布了 13 個電子卡片的應用，率先與北京公交卡公司開展手機支付行業合作，用手機即可在北京搭乘公車及地鐵，並於 2014 年與中國聯通、中國電信等二家 MNO TSM 介接。

(六) 香港

銀聯通寶公司 (JETCO) 於 2013 年 6 月已整合會員銀行，成立「PSP TSM 平台」，向參加之會員銀行收取一次性三年會費，之後再由董事會評估收費方式。另提供會員銀行卡片空中下載 (OTA Personalization)、自有品牌「數位皮夾」(white label wallet)、電子優惠券 (e coupon)、電子票券 (e ticket)、積分獎賞計畫等服務；並將於完成上述行動商務之發卡業務後，即進行下一階段開拓特店收單業務。

(七) 紐西蘭

紐西蘭之 TSM 係由金融業與電信業合資成立，稱為 TSM NZ，其中金融部分係由 Paymark 持股 52%，Paymark 乃紐西蘭四大主要銀行 (ASB、Bank of New Zealand、Westpac and ANZ National) 於 1989 年籌組成立，提供跨行金融資訊、交易轉接等電子金流支付服務；另外 48% 持股，則屬 Telecom NewZealand、Vodafone NewZealand、Two

Degrees Mobile 三家電信業者所有。目前 TSM NZ 係採以 Gemalto TSM/C-SAM Wallet 之技術解決方案，其目的在與更多服務供應商、支付產業結合，共同推動 NFC 行動支付生態圈，公平開放為其宗旨，預計 2014 年下半年於紐西蘭推出 NFC 錢包解決方案。

綜上，隨著「行動支付」服務之技術日趨成熟，以及電信、金融兩大產業間競合關係之磨合與演進，可見各國 TSM 服務已朝向依個別產業特性發展，其中金融服務多由金融業或金融體系中具獨立、公正之跨行金融中心 (如金融結算機構) 主導，諸如日、美、南韓、香港、中國大陸等，建置 PSP TSM 服務，專責於「金融支付工具」之互通與管理，以及金融安全防護，並與電信業 TSM 介接合作，除可提升「行動支付」之安全與效率外，並具備「專業分工」之異業結盟優勢。

三、我國之「PSP TSM 平台」

據萬事達卡國際組織 2013 年 4 月公布的手機上網購物行為調查顯示，曾用手機購物人口的所占比重之前五名為印尼、中國、泰國、香港、南韓，臺灣在亞太 14 個市場中排名第九。而國家通訊傳播委員會的資料顯示，2013 年第 2 季我國行動電話門號達 2,952 萬戶，平均每人擁有 1.26 個門號，行動上網帳號數達 1,901 萬戶。從資策會產業情報研究所 (MIC) 針對臺灣持有行動裝置的消費者進行「2013 年行動購物調查」發現，57.1% 的行動裝置消費者在過去一年內，有使用行動裝置購物的經驗，較去年 3 月資策會 MIC 調查結果的 16.4% 大幅成長，顯示消費者使用行動裝置購物意願已經有提升的跡象。此外，影響消費者使用行動上網購物的因素，前五名分別為「習慣使用該網站 (66.6%)、售價比較便宜 (45.6%)、商品資訊豐富 (42.9%)、較方便搜尋 (39.0%)、付款方式方便 (24.9%)」，在在顯示我國行動發展商機無限。

而金融監督管理委員會於 2013 年初，頒布「信用卡業務機構辦理手機信用卡業務安全控管作業基準」，開放發卡銀行經營手機信用卡業務，法令限制的鬆綁為「行動支付」市場開啟了一扇大門，茲依我國 TSM 市場發展時序摘要說明如后：

(一) 中華電信公司 (中華電信) 自建 MNO TSM 及 PSP TSM 平台，並自 2013 年 5 月起陸續與國泰世華銀行、中國信託銀行、玉山銀行、台新銀行等金融機構合作進行手機信用卡員工試辦方案，搭配中華電信所發行的 USIM 卡，可透過 OTA 的方式，將信用卡資訊傳輸至中華電信 Hami 智慧錢包 APP 中，使用者即可如同一般實體信用卡使用萬事達卡 Paypass 感應式手機，辦理信用卡支付服務。

(二) 開南大學、法商歐貝特 (Oberthur) 及安侯國際財務顧問公司於 2013 年 2 月成立「聯合國際行動支付 (股) 公司」(簡稱「聯合國際」)，發展以 SD 記憶卡作為安全載具，經營 PSP TSM 平台業務，並已於 2013 年 9 月上線營運，與高雄捷運共同推出一卡通 iPass 服務。

(三) 中華電信、遠傳電信、威寶電信、亞太電信與台灣大哥大等五家電信業者，以及悠遊卡公司，於 2013 年 11 月發起成立「群信行動數位科技 (股) 公司」(簡稱「群信公司」)，計劃同時經營 MNO

TSM 及 PSP TSM 二大平台業務，預計 2014 年 12 月上線營運。

(四) 財金公司、聯卡中心、台灣票交所三家機構應金融業殷切期盼，共同籌設「臺灣行動支付公司」，開放所有金融機構參股，並於 2014 年 2 月成立籌備處，建置「PSP TSM 平台」，以協助金融產業發展「行動支付」。

金融機構可藉由「臺灣行動支付公司」「PSP TSM 平台」發展行動信用卡、金融卡、電子票證等銀行卡片之近端與遠端支付服務，提供加值服務，經營客戶關係，強化競爭力，進而增進我國社會及經濟活動之發展。鑑於「PSP TSM 平台」建置係國家「金流發展」之重大基礎建設，乃發展「行動支付」之關鍵，掌握銀行支付卡之「發行」與「管理」，對民眾帳戶安全與銀行作業風險至關重要，能否安全穩定運作攸關國家經濟發展與整體競爭力。因此，擔任「PSP TSM 平台」角色應具備下列責任及條件，方能為社會大眾、金融機構及金融監理機關所信賴。

1. 金融業主導及專業跨銀行金流服務經驗，確保系統安全穩定運作。
2. 具信賴、專業及獨立公正之特性。
3. 具確保金流資料之隱密性與安全性，並符合主管機關及金融機構對個人資料保護之要求。
4. 以協助金融產業發展為優先，不以營利為唯一目標，具備為金融業爭取有利發展條件與機會等特質。

從「PSP TSM 平台」角色特質觀之，由財金公司、聯卡中心與台灣票交所三家機構，共同籌設公司建置「PSP TSM 平台」，可有效整合運用金融體系資源，避免重複投資，並有助健全金融支付系統之安全與穩定運作。

以下謹就「臺灣行動支付公司」規劃之我國「PSP TSM 平台」服務架構、運作機制及交易流程概述如下：

(一) 架構說明

在「行動支付」生態系統中，係由金融機構、電信運營商、服務提供者及 TSM 平台單位共同組成，並由「PSP TSM 平台」擔任核心角色，其服務架構 (如圖 1 所示) 中各角色簡述如后：

圖 1　PSP TSM 服務架構

1. **服務提供者**

包含國內發行各項支付工具之金融機構，可透過 TSM 平台提供消費者申請行動支付所需要的個人化資料派送及更新、金鑰管理、驗證碼的產生及管理等；而企業儲值卡、票券 / 票證、特約商店優惠券、紅利積點等各種行動商務應用之服務提供者，亦可透過 TSM 平台進行 OTA 下載至消費者之手機中。

2. **TSM 平台**

「PSP TSM 平台」支援 USIM 卡、SD 記憶卡、手機內建晶片、外掛裝置等四種安全元件，並因應科技發展及行動設備提升，提供相對應之行動「支付服務」。透過「PSP TSM 平台」與電信業者所建置之「MNO TSM 平台」或其他安全元件供應商介接，可將服務供應商的各種行動支付應用，快速安全地發行至使用者之行動載具。

3. **消費者**

透過數位皮夾可進行信用卡、金融卡、電子票證、銀行帳戶等支付工具之下載，以及優惠訊息、紅利點數、廣告、優惠券、帳單查詢等加值服務之應用，實現「一機在手，通達任我」之數位行動生活。

(二) 服務範圍

「PSP TSM 平台」之服務範圍，除金融業者之信用卡、金融卡、電子票證及銀行帳戶等支付工具外，亦包括非金融產業之識別證、交通票證、帳單管理、eDM、優惠券、票券、紅利積點等行銷及加值服務 (如圖 2)，PSP TSM 提供的主要服務項目如下：

1. **建立安全「空中通道」**

(1) 協助金融機構提供客戶申請行動支付所需要的個人化資料派送及更新、金鑰管理、驗證碼的產生及管理等。
(2) USIM 卡變更 / 電信業者變更管理。
(3) 手機變更或遺失管理。
(4) 服務維護運作及異常管理。

2. **提供「生命週期」管理**

(1) 提供金融專屬之「數位皮夾」(Digital Wallet) 服務。
(2) 產品 / 服務上下架及發行管理。

圖 2　「PSP TSM 平台」之服務範圍

3. **「近端」及「遠端」之支付服務**

提供行動裝置上「數位皮夾」的服務與管理，民眾利用「數位皮夾 APP」，可提供各項消費購物、繳費稅、轉帳等功能。

4. **行銷活動與多元應用**

(1) 行銷活動服務管理。
(2) 提供支付工具、票券 / 票證、帳單通知、紅利積點、eDM/ 優惠券等下載服務。

(三) 作業流程概述

消費者向金融機構申請「行動支付」服務，金融機構經核對客戶身分及相關申請資料審核通過後，將個人化資料傳送予 PSP TSM，並透過與 MNO TSM 之介接或其他安全元件，即可「空中下載」(Over the air, OTA) 所申辦之信用卡、金融卡等行動支付服務至消費者之行動裝置中，後續消費者可透過數位皮夾 APP，管理及使用行動裝置中之支付工具。

1. **數位皮夾安裝註冊及下載卡片流程說明 (如圖 3)**

消費者至 APP 平台 (如 Google Play 或 APP Store) 下載並安裝「數位皮夾」，開啟「數位皮夾」並依指示進行註冊，輸入 OTP (One Time Password，一次性密碼) 進行驗證，「數位皮夾」開通後，選擇新增支付工具，依發卡銀行核卡通知函之說明，進行卡片下載流程，輸入下載驗證碼後完成下載。

圖 3　數位皮夾安裝註冊及下載卡片流程示意圖

2. **近端支付流程說明 (如圖 4)**

本流程以消費者於可接受感應式交易之特約商店購物為例：結帳時，消費者開啟「數位皮夾」，選取欲使用之信用卡、金融卡，輸入密碼後進行近端感應式付款，後續交易同現行交易機制，特約商店透過收單機構、授權轉接結算平台，至發卡機構取得授權，並由授權轉接結算平台進行發卡機構、收單機構之清算作業；收單機構撥付款項予特約商店，發卡機構則以約定方式通知消費者付款。

圖 4　近端支付流程示意圖

3.　遠端支付流程說明 (如圖 5)

本流程以消費者透過行動裝置瀏覽網路特約商店並進行購物為例：消費者瀏覽購物頁面並選購商品後，透過「數位皮夾」進行結帳，選取欲使用之信用卡、金融卡，輸入密碼後進行付款，後續交易同現行交易機制，特約商店透過收單機、授權轉接結算平台，至發卡機構取得授權，並由授權轉接結算平台進行發卡機構、收單機構之清算作業；收單機構撥付款項予特約商店，發卡機構則以約定方式通知消費者付款。

圖 5　遠端支付流程示意圖

四、結語

多年來，隨著票據、匯款、轉帳、信用卡、金融卡等非現金支付工具的大量使用，我國現金的使用相對量雖呈現下降趨勢，但非現金支付比重仍僅約 25%，遠較鄰近韓國、新加坡等國家卡片支付比例超過 70% 比重為低，顯仍有大幅發展空間。隨著智慧型電子產品推陳出新，消費者對支付型態的多樣化與便利性接受度逐漸提高，使用電子支付的需求將日益提升；對商家通路而言，現金管理的人力成本與風險很高，故提供支付工具的多元應用，打造無現金之環境，可促進產業發展，更有助於拓展臺灣市場至國際舞台。

智慧型行動裝置與網路頻寬不斷擴增、雲端及巨量資料技術的日益精進，金融業、電信業、零售業、服務業、製造業與科技研發相關產業均紛紛投入資源，國際卡組織、第三方業者及虛擬貨幣商等網路支付業者，亦積極發展安全便捷的網路與行動支付服務。由金融業主導之「行動支付」是最符合電子商務發展的支付工具，能整合現行各類型卡片服務，並可大幅提升網路交易安全，藉助 NFC 服務的拓展，亦可同時兼具面對面交易支付功能，勢將成為支付工具的主流。

當民眾使用網路的習慣、頻寬、物流及資訊流日臻完善後，電子商務躍進的關鍵就在行動商務應用。透過相對安全的行動技術，跨越終端設備之間原本存在的溝通限制，不僅可以將購物、身分識別、交通票證、門禁保全等相關應用與民生消費結合，也可用於行動廣告、社群媒體。網路無國界、不受時間與空間的限制，電子商務勢必朝向全球化擴展，善用我國優良的資通訊產業基礎，提供安全便捷的「行動支付」，正是電子商務發展不可或缺的重要因素之一。

然而「行動支付」的成功關鍵，有賴相關產業相互合作，其中涉及技術開發、界面開放、標準及規範建立、終端設備普及等關鍵因素，在發展過程中必須兼顧電信運營商、金融機構、商店、消費者多贏的局面，才能獲致成功的業務模式。當然也需要相關產業主管機關及擁有不同專業背景與資源的政府部會積極投入，方能克盡全功。

由金融業主導之「PSP TSM 平台」提供服務供應商及安全元件發行者資料交換的管理機制，提供行動服務之整合應用與市場動能，將可縮減產業間的溝通與介接成本，促進不同產業之供應商更廣、更多樣化及高品質之服務，有利於為消費者提供更多行動便利新生活的選擇。

未來，「臺灣行動支付公司」成立後，現有之支付工具可整合至行動裝置，將有利於支付市場快速發展，透過相關產業相互合作，協調共通之技術及建立開放、標準之介面及規範，促進終端設備之普及等，藉由共同提供 PSP TSM 服務，以降低系統重覆建置之成本，促發並提升「行動支付」市場之運作機能，拓展市場效能並創造多贏的局面，共創支付產業新紀元。

雲端行動支付利器－HCE 及 Tokenization 共用平台

本篇摘自 2016 年 01 月出刊之財金資訊季刊第 85 期，由財金資訊公司業務部專案企劃組陳詩蘋組長撰寫。

一、前言

隨著行動裝置快速普及，手機、平版電腦已經成為民眾每日深度接觸的重要媒介，更進一步衍生出行動應用服務的潛在市場。根據國際市場研究機構 TNS (Taylor Nelson Sofres) 公司 2014 年「消費者跨裝置上網研究」(Connected Consumer Study) 調查報告指出，臺灣智慧型手機的普及率，由 2012 年的 32%，快速提高至 2014 年的 67%；換言之，臺灣每 10 人就有近 7 人屬於「滑世代」的一員。又依 Millward Brown 於 2014 年發布 AdReaction 研究，觀察全球 32 個市場，其中臺灣地區民眾每日平均使用「智慧型手機」上網時數為世界第一，長達 3 小時多 (197 分鐘)，高出全球平均數值 (142 分鐘) 近 1 小時。

另外，根據市調機構 Strategy Analytics 表示，2014 年出廠且裝有 NFC (Near Field Communication) 晶片的智慧型手機比率達 28.9%，估計今 (2015) 年滲透率將進步至 39.8%，明 (2016) 年更將突破五成，上看 52.4%，也就是說明年出廠的手機，每兩支就有一支裝有 NFC 晶片。除此之外，Strategy Analytics 還看好未來幾年，搭載 NFC 晶片的智慧型手機將持續以 4-5 個百分點往上成長，2020 年滲透率將來到 71.8%。

由上可知，「行動浪潮」來勢洶洶，數位化、智慧化已是個人、企業、城市，乃至於國家融入「數位時代」的必要條件，也是競爭力的具體指標。根據 Visa 國際卡組織公布「感應支付臺灣消費者行為研究」顯示，2014 年臺灣地區透過 Visa payWave 感應交易的消費總金額，已超過新臺幣 638 億元，相較於 2013 年增長 42.8%，名列亞太第二，僅次於馬來西亞；另高達 82% 臺灣消費者表示曾透過「感應支付」進行交易，顯示消費市場已漸以「感應支付」取代現金支付。探究消費者使用感應交易的三大主因，分別為快速、便利與安全，其中包含透過感應即可完成付款、小額付費免簽名，以及無須將卡片交予店員的快捷、安心等使用體驗。

為因應全球發展情勢，協助我國金融產業構建安全便捷之「行動支付」服務，支援產業拓展「行動商務」，進而提昇我國金融產業與整體經濟之競爭力，我國三大結算機構—財金資訊公司、財團法人聯合信用卡處理中心

與財團法人台灣票據交換業務發展基金會整合 32 家金融機構及悠遊卡 (投控) 公司共同投資，於 2014 年 9 月 5 日正式成立「臺灣行動支付 (股) 公司」，建置「金流信任服務管理平台」(Payment Service Provider TSM，以下簡稱 PSP TSM 平台)，藉由「t wallet」APP，提供手機信用卡持卡人透過空中下載 (Over The Air，以下簡稱 OTA) 方式，將信用卡載入已取得信用卡國際組織認證的安全儲存媒介 (Secure Element，以下簡稱 SE)，如電信業者的 USIM 卡，以及 SD 記憶卡、手機內建 NFC 晶片或外掛式裝置等其他 SE，持卡人在安全環境下，透過手機 NFC (近距離無線通訊) 交易模式，進行信用卡刷卡交易；或依信用卡國際組織或國內銀行公會信用卡自律規範，辦理遠端購物服務。

然而，隨著如何針對不同消費族群的特性，量身打造合適的服務方案，乃產業面臨之重要課題，面對全球化的行動浪潮，以及國際間雲端行動支付服務趨勢，金融機構如何善用既有優勢，重新整合並包裝行銷，提供客戶 (持卡人) 更多元、便捷安全的行動支付服務乃刻不容緩之議題。

二、行動支付市場現況

綜觀全球主要的「行動支付」平台，約可分為以下三種模式：

(一) PSP TSM

PSP TSM 平台業經 VISA、MasterCard 等國際組織認證，以空中下載 (OTA) 技術，既便利又安全地將「支付工具」發行至「安全元件」，如 USIM 卡、oti WAVE 嗶嗶熊外掛式裝置等，TSM 機制之安全性最高，相關標準及規範亦均已俱全，惟生態系統成員眾多，競合關係較複雜，目前全球約有超過 100 個此類平台。

(二) Tokenization

VISA 及 MasterCard 組織推行之 Tokenization，由雲端平台編發「虛擬卡號」(Token)，並將 Token 及其金鑰儲存於「手機內建晶片」，交易時，透過手機模擬信用卡向發卡銀行取授權，發卡銀行須先驗證「Token」之正確性與有效性，再還原回「實際卡號」，旨在將實際卡號轉換為 Token，並限制 Token 的使用場域，以降低原實際卡號使用時遭竊取盜用之風險。Apple 於 2014 年在 iOS 推出之 Apple Pay，為目前使用 Tokenization 最成功案例之一，目前於北美、英國試行，惟僅適用 Apple 手機，生態系統成員雖較單純，但相關應用受制於手機廠商，未來銀行發展數位金融亦可能受限。

(三) HCE (Host Card Emulation)

1. VISA 與 Google 於 2013 年合作，在 Android 作業系統利用手機應用程式模擬晶片，發展出 HCE 方案，將「支付工具」資訊儲存至雲端伺服器，為保護支付工具卡號資料及其「交易金鑰」，由發卡機構另行編製一組實際上不存在的「虛擬卡號」，取代原有卡號 (PAN，Primary Account Number)，並將原本存放於「安全元件」之「交易金鑰」，改存至「雲端主機」，只派送「限制用途之交易金鑰 (Limited Use Key or Single Use Key)」

至行動載具上的「行動支付應用程式 (Mobile Payment Application)」，以避免卡片資料外洩與遭偽冒之風險。又因「行動支付」應用程式上的「交易金鑰」具效期、用途等限制，可設定「交易金鑰」效期縮短至約數小時至數天不等，即「交易金鑰」逾期後，須適時由雲端平台增派至手機，因此，對網路之依賴程度較高。

2. HCE 機制降低安全儲存媒介 (SE) 購置成本；惟因屬純軟體解決方案，其安全性較低，未若使用安全元件之 TSM 具高安全度。換言之，其生態系統成員最為單純，可不受電信商或手機商的約制外，進而有效提昇行動支付應用之普及性與便利性。現階段未支援 Mifare 非接觸式智慧卡然適用 HCE 之手機 (Android 4.4.4 以上高階機種) 少於 TSM 機制適用者。

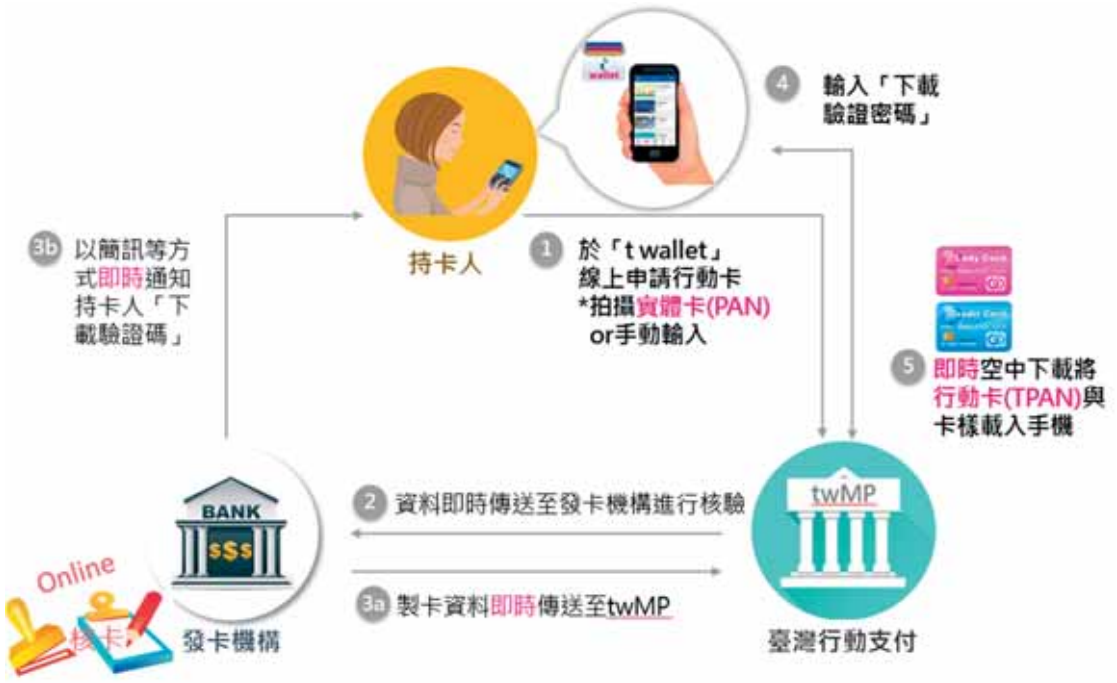
反觀我國，臺灣行動支付公司之 PSP TSM 平台於 2014 年 12 月 30 日上線營運，截至 2015 年 10 月底為止，計有 37 家金融機構參加，其中 23 家開放一般民眾申辦「行動支付」業務，不僅大幅減輕金融機構、商店參與「行動支付」服務市場之系統建置成本，簡化個別金融機構與電信業者或其他安全元件供應商間之溝通、介接與合作，更整合「行動支付」生態體系成員，支援相關產業拓展「行動商務」。

三、HCE 及 Tokenization 雲端行動支付共用平台

VISA 表示，依據其研究所獲數據顯示，臺灣地區消費市場已逐漸以感應支付取代現金支付，因此未來臺灣在行動支付市場之發展將更為蓬勃。也因此，各金融機構為邁向金融 3.0 時代，對於我國 HCE 及 Tokenization 雲端行動支付共用平台之建置，更為期盼與支持。

為持續協助金融機構因應不同風險等級、客層及業務發展之需要，發展多元行動支付服務，以肆應國際行動支付業務及技術發展情勢，臺灣行動支付公司業已邀集 23 家先導金融機構，啟動「HCE 及 Tokenization 雲端行動支付共用平台」建置作業。

該共用平台由該公司擔任 TSP (Token Service Provider)，客戶 (持卡人) 於 t wallet 上，以「拍攝本人實體信用卡」或「手動輸入實體信用卡卡號」方式，線上申請「手機信用卡」服務，發卡機構經審核通過後，將個人化資料傳送予該共用平台將 PAN 轉換為 TPAN，並 OTA 至客戶之行動裝置中，客戶輸入發卡機構提供之「下載驗證碼」，即可完成卡片下載作業，大幅簡化「行動支付」申請流程，未來，申請手機信用卡亦將更為便利與即時；其後，客戶可運用 t wallet 管理及使用行動裝置中之手機信用卡。「HCE 及 Tokenization 雲端行動支付共用平台」透過「TPAN」與金鑰確保交易的唯一性與有效性，滿足不同消費客群的多元需求。



OTA 空中下載流程示意圖

手機信用卡下載成功後，客戶即可持手機信用卡進行近端感應式或遠端網路交易，在信用卡特約商店結帳時，客戶開啟 t wallet，輸入「持卡人密碼」，選取欲使用之手機信用卡，將手機靠近刷卡機，即可輕鬆嗶一下完成感應式付款；亦可持行動裝置瀏覽網路特約商店網頁或 APP 選購商品後，選擇 t wallet，輸入「持卡人密碼」，選取欲使用之手機信用卡，隨時隨地進行購物並完成付款。

四、行動支付多元應用與推廣策略

臺灣行動支付公司 2014 年底建置完成之 PSP TSM 平台，是國內唯一整合最多銀行 (37 家金融機構參加)、最完整支付工具 (VISA、MasterCard 信用卡、FISC 金融卡、ACH 銀行帳戶)、最多國際卡組織認證 (VISA、MasterCard、銀聯) 的 TSM 平台；然在電信業提供 MNO (Mobile Network Operator) TSM 整合服務前，也僅能與中華電信 MNO TSM 平台介接，無法提供所有消費者完整的行動支付方案，甚為可惜。

HCE 及 Tokenization 等雲端支付技術，可由金融產業自主發展，不必仰賴電信業者，在客戶體驗及業務推動上皆更為便利，我國發展雲端行動支付服務之腳步亦不能落後於國際。臺灣行動支付公司之「HCE 及 Tokenization 雲端行動支付共用平台」，對於推動行動支付業務具有多項優勢：

(一) 行動支付生態環境單純，金融機構掌握發卡「主動權」

雲端行動支付技術無須依賴電信業者或 SE 發行者，可由金融機構自主發展，在客戶體驗及業務推動上皆更為便利。

(二) 一站購足，快速發卡，持卡人體驗佳

過往 TSM 平台發卡，除須請持卡人先申請 SE 外，亦須重新申請一張行動支付卡片；而 HCE 模式下，持卡人可持既有金融機構信用卡，即時下載行動卡片，發卡過程較短，客戶無須等待，體驗也較佳。

(三) 透過既有網路、行動銀行通路，引導持卡人升級為行動支付用戶

金融機構可透過龐大的網路、行動銀行客戶，輔以靈活多樣的行銷方案，把原來僅使用網路、行動銀行客戶線上功能的用戶轉到行動支付，提供完整近端 NFC、遠端支付等服務。

(四) 發行「差異化」的手機信用卡產品

金融機構可根據自身特點、聯名卡產品發行不同主題、不同權益的手機信用卡，並可與優惠券、積分等功能整合，充分發揮行動支付的優勢。

五、結語

全球非現金交易蔚為趨勢，丹麥政府於 2015 年 5 月間公布一系列創新的措施，並已立法要求零售商未來不再接受消費者的實體現金支付，在 2016 年 1 月起實施，成為全球第一個出門不用帶現金的國家，顯見國際間推動電子化、行動化支付環境之趨勢已不可擋。

另，據美國商業智能 (Business Intelligence，BI) 的分析報告，在金融科技中，行動支付的使用率最高，從行動支付民間消費滲透率曲線發現，其滲透率在第一年是萬分之 4、第三年是千分之 1.3、第五年是百分之 1.7，各金融機構應及時提供完整的金流服務，以因應客戶 (持卡人) 對行動支付的需求。

為肆應「行動支付」之快速發展，臺灣行動支付公司「HCE 及 Tokenization 雲端行動支付共用平台」，除了提供手機信用卡 HCE 雲端支付服務外，未來更無縫與 Apple Pay、Samsung Pay、Android Pay... 等國際手機製造商之支付方案整合，現有之支付工具可更方便快速地整合至行動裝置，透過相關產業相互合作，協調共通之技術及建立開放、標準之介面及規範，促進終端設備之普及等，加速「行動支付」服務之推展，不僅有效降低重覆建置之成本，更有助於提升金融機構整體競爭力，並期待主管機關及政府其他相關部會鼎力支持，俾利整合各界資源，共創支付產業新紀元。

※ 參考文獻 / 資料來源：

1. 2014 年 8 月 14 日，蘋果日報，「全球第一　台人手機上網 每天 197 分鐘」。
2. 2014 年 10 月 29 日，ETtoday，「Google 台灣：跨裝置行動是現在式，不把握就會被淘汰」。
3. 2015 年 5 月 6 日，卡優新聞網，「Visa payWave 破 800 萬卡　嗶卡交易量亞太第二」。
4. 2015 年 9 月 16 日，Money DJ，「蘋果行動支付加持，NFC 手機明年挑戰五成滲透率」。
5. 2015 年 10 月 02 日，工商時報，「發展金融科技 國銀拚行動支付」。

雲端行動支付利器－HCE 之金融應用

本篇摘自 2016 年 01 月出刊之財金資訊季刊第 85 期，由財金資訊公司研發部蘇偉慶經理撰寫。

一、前言

有關使用近場通信 (Near Field Communication，簡稱 NFC) 技術，解決近端行動支付的話題，至少已經持續被討論 10 年以上。每次參加相關技術研討會時，總是不斷被告知 NFC 設備即將普及、NFC 的生態環境即將成熟、NFC 時代即將到來、NFC……，但希望卻一再落空。而為解決 NFC 設備的支援問題，出現許多過渡的技術及產品，但因為缺乏既有手機的整體設計考量，總還是存在或多或少的問題，無法讓人滿意。

隨著智慧型手機的普及，直到近一兩年，NFC 模組似乎已逐漸成為中高階智慧手機的標準配備，此時又燃起大家的希望。然而不論是由電信產業提出的 NFC SIM (NFC Subscriber Identity Module) 安全元件方案、抑或是手機廠商主導的內嵌安全元件方案 (如：蘋果公司的 Apple Pay、三星公司的 Samsung Pay 等)，總還存在跨業合作的議題。因此，Google Android 提出了透過行動裝置應用程式來模擬卡片的技術，讓服務供應商可完全掌握從發卡到使用的所有作業。只是，缺乏安全元件的 NFC 技術，真的可兼顧到便利與安全嗎？本文將從 HCE (Host Card Emulation) 的技術基礎談起，再敘明現行的 Visa 及 MasterCard 是如何運用此技術，最後則討論在缺乏實體安全元件的狀況下，HCE 的安全防護重點為何？

二、HCE 之基礎

NFC 技術剛被提出時，安全元件總被視為 NFC 的標準核心元件，其主要型態有三，包含：(一) 電信卡 (SIM)、(二) 內嵌安全元件 (Embedded Secure Element，eSE)、或 (三) 安全記憶卡 (Secure Memory Card，SMC)。由於 NFC 行動裝置已經具備與多個安全元件溝通的機制，因此透過行動裝置的應用程式來模擬卡片的方案，就硬體上，並不會增加額外的成本，而只是將原來 NFC 模組訊號的繞送路徑，由原來的安全元件，新增可繞送至行動裝置的中央處理器 (Central Processing Unit，CPU)，由作業系統及對應的行動裝置應用程式，模擬卡片須回應給商家終端機的所有指令。目前主流的 NFC 手機大部分支援 eSE 或 NFC SIM 安全元件，甚至很多手機可同時支援 eSE 與 NFC SIM。倘若再加上未來可同時支援 HCE，則其架構詳如圖 1 所示：

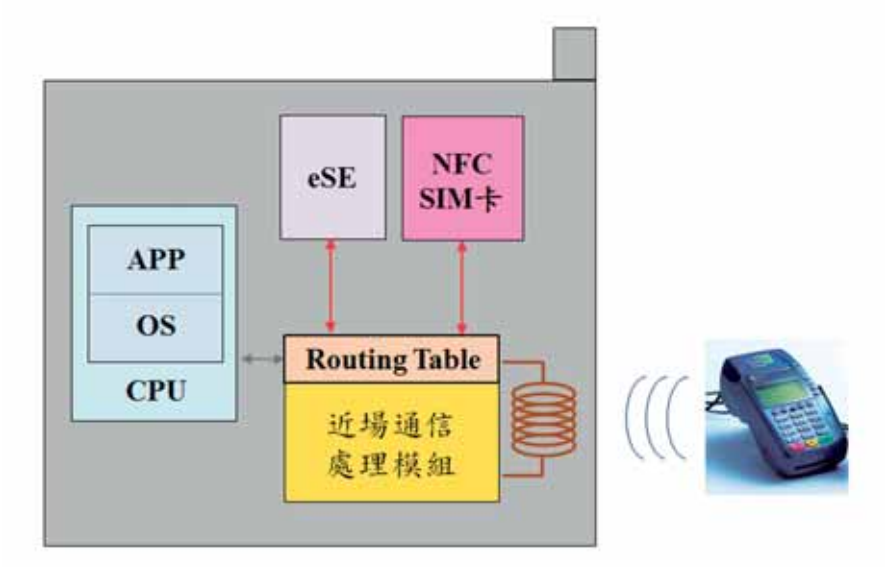


圖 1　安全元件及 HCE 架構圖

Android 在 4.4 (KITKAT) 版本後，允許來自外部的支付相關指令，可透過適當的繞送設定，指定傳送至 CPU 上進行相關處理。其邏輯上便是透過 Android 作業系統與應用程式內備妥的處理邏輯，模擬原有的卡片所有行為，以回應終端機完成交易。由上圖可知，如果 HCE 應用與另外兩種安全元件同時存在於某個應用程式、或存在於多個應用程式時，如何設定好 Routing Table，讓終端機的相關指令可傳送到使用者所指定欲使用的卡片上，也就成為重要關鍵，事實上也更形複雜。

在 Android 4.4 版本下，僅可在應用程式的 Manifest 檔案中，描述可處理某些特定的卡片應用 (透過 Application Identifier，也就是 AID，指定)，或者是透過安全元件處理。但對某個應用程式來說，如果希望某些特定的卡片應用可同時儲存在安全元件或直接透過應用程式模擬，則唯有動態進行 Routing Table 的改變始足以因應。至於 Android 5.0 (LOLLIPOP) 版本，則提供一項應用程式介面函數 registerAidsForService，透過它，便可在使用者選擇某個支付卡片時，要求作業系統更新 NFC 模組的 Routing Table，動態改變繞送路徑，讓終端機的指令可傳送到正確的模擬卡片上。

當所有模擬卡片所需的金鑰或設定資料皆儲存於手機上時，HCE 應用程式便可獨立模擬出任何原有實體卡片的行為。然而，因手機端所能提供資料或運算邏輯的保護有限，因此 HCE 的解決方案通常會搭配強大的後端平台，讓儲存在手機上的機敏資料愈少或限定其使用次數及時間等，並透過後台系統的風險偵測與管控，減低此機制的安全風險。因此，兩大卡片組織分別提出 Visa Cloud-Based Payments 及 MasterCard Cloud-Based Payments 的解決方案，並已公告相關之技術規格。

三、現行卡片組織之應用技術

本節僅以國內目前最普及、且已公告 HCE 相關技術規格的兩大國際卡片組織－ Visa 及 MasterCard，就其重要的概念或差異的部分進行說明，以利有興趣的金融機構瞭解規格的內涵，當然詳細的實作，尚須直接參考該兩組織之規格。

(一) 整體架構

在系統的功能模組組成方面，其實內容是大同小異，唯獨功能切割之界線不同罷了 (如圖 2)。Visa 的整體後台稱為 Cloud-Based Payment Platform，此平台分為以下幾個主要核心功能：

1. Provisioning －也就是依據卡片的類別，決定相關卡片資料，編製對應的虛擬卡號 (替代卡號或 Token)，並將相關卡片資訊下載 (發行) 至特定的持卡者手機裝置上。已發行的卡片相關資訊必須與 Transaction Verification 模組同步，以確保交易驗證時相關資料的正確性。
2. Active Account Management －主要提供發卡後續的金鑰更新 (可以是手機端的應用程式主動要求或於交易處理過程中發動)，也就是當手機上的金鑰使用次數或時間限制即將到達前，將新的金鑰下載至手機上，以便交易得以順利進行。
3. Transaction Verification －也就是進行交易的驗證，交易驗證同時必須參考目前發行卡片的參數設定，以及相關金鑰的狀態。
4. Life Cycle Management － 也就是卡片發行後的生命週期管理，可以是由持卡者或發卡行發動，包含如：終止、暫停及恢復等作業。

MasterCard 同樣將相關功能，分隔成幾個子系統：

1. Account Enable System (AES) －整個帳號的管理均透過此模組負責，提供標識化 (tokenization) 及數位化 (digitization) 服務，讓下游的 CMS 系統可以將相關的卡片數位資訊發行至某個指定的 Mobile Payment Application (MPA) 上。數位化的服務，可讓發卡行將原來儲存在實體卡片的持卡者帳號資訊，轉換並發行至行動裝置上。AES 與 Visa 雲端平台中 Provisioning 的部分工作是類似的，但不負責將相關資訊下載 (發行) 至特定的持卡者手機裝置上。另外，Visa 的 Life Cycle Management 應該也是屬於此模組的功能範圍。
2. Credential Management System (CMS) － 主要負責下載與更新資料 (包含金鑰) 至 MPA 上。CMS 可說是整體作業的核心模組，因為它與 AES、TMS 及 MPA 都有介接溝通。
3. Transaction Management System (TMS) － 主要根據目前 CMS 中所有卡片的相關設定及金鑰狀態等，進行交易的驗證。當交易驗證完成後，也將回饋相關狀態給 CMS，以利後續對手機端應用程式的作業。TMS 與 Visa 雲端平台的 Transaction Verification 是對應的。

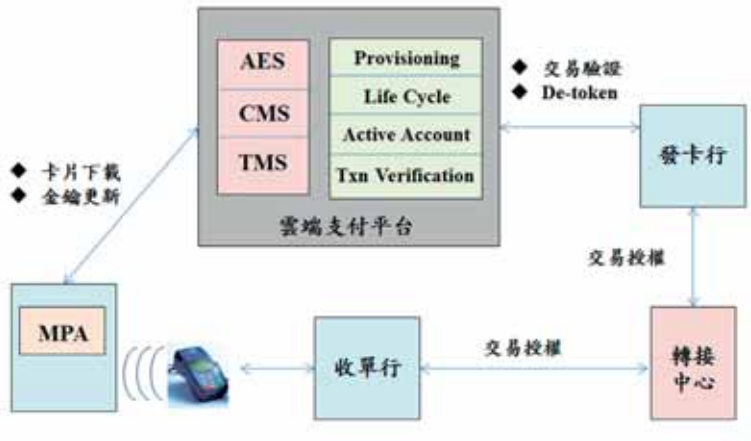


圖 2　雲端支付架構圖

(二) 金鑰概念

不論是 Visa 或 MasterCard，真正下載到 MPA 的金鑰，均非實體卡片的卡片金鑰，而是具使用限制的 Session Key。茲就兩者在金鑰的各個項目做一比較，說明如下：

表 1　Visa 及 MasterCard 金鑰使用比較

項目	Visa	MasterCard
1. 卡片金鑰	使用發卡行的一把 Master Key，依據卡號及序號產生一把卡片金鑰。	使用發卡行的一把 Master Key，依據卡號、序號及序號變化產生兩把卡片金鑰。
2. Session Key	使用卡片金鑰，透過時間參數及序號產生一把 Session Key，稱之為 Limited Use Key (LUK)。	由兩把卡片金鑰，依據 ATC (Application Transaction Counter) 產生對應的兩把 Session Key。其中一把在下載至 MPA 前，會先與持卡者於雲端設定的密碼 (Mobile PIN) 進行 XOR (Exclusive OR) 運算，此 Key 稱之為 Single Use Key (SUK)，事實上另一把也只能用一次。
3. 交易驗證使用 Application Cryptogram (AC) 的計算	使用 Session Key 對交易相關資料進行運算，此演算法為 CVN (Cryptogram Version Number) 43。	MPA 計算 AC 前，會要求持卡者輸入 Mobile PIN，並再次與 SUK 進行 XOR 運算而得到原有的 Session Key。再以原有的演算法進行 AC 運算，此值可同時驗證設備 (卡片) 及持卡者的合法性。而另外一把與 PIN 無關的 Session Key，也會產生另一個 AC，驗證設備 (卡片) 的合法性。
4. Session Key 使用限制	可依據時間、交易次數及交易累進金額進行限制。	僅可使用 1 次。

(三) 持卡者認證

持卡者認證在支付過程當然是相當重要的一環，因為它可確保交易是合法使用者所發動。在支援安全元件的行動支付上，由於密碼可以安全地儲存在安全元件上，且具備非法重試鎖定的機制。因此，雖然其名稱二大組織各自不同，Visa 為 Pass Code，MasterCard 為 MPin，但均採離線認證的方式進行。

至於在 HCE 的應用上，因為沒有安全元件的保護，MasterCard 便放棄離線持卡者認證的模式，而改採上節 (金鑰概念) 所描述的 SUK 機制，於交易驗證時進行持卡者驗證。本質上，此方式較接近傳統的 Online PIN，但使用者是在手機上直接輸入，而非於商店的刷卡終端機。採用此機制的好處是不論 MPA 是否

連結至雲端後台，都可以執行交易。缺點則是須交易經授權後，才知道密碼是否輸入正確。

Visa 在持卡者認證則提出另一項「設備端持卡者驗證」(Consumer Device Card Verification Method，簡稱 CDCVM) 概念，而 Visa 也舉出以下三種形式：

1. 雲端 **CDCVM (Cloud-based CDCVM)** －也就是連結至雲端平台進行認證，因為所有的認證資料儲存在雲端，且重試鎖定的機制也由後台控管，安全性最高。但缺點是交易時必須連網。
2. 設備 **CDCVM (On Device CDCVM)** －也就是直接參考使用者既有解鎖設備的機制，其優點是對使用者來說最方便，缺點則是應用程式對其掌控性 (如：安全強度、安全防護及異常處理) 較差。
3. 應用程式 **CDCVM (Mobile Application CDCVM)** －也就是將認證資料儲存於應用程式中，直接離線於應用程式進行持卡者驗證。採用此方式最不安全，但可在未連網的狀況下進行交易，因此建議搭配其他較安全的機制 (如：雲端 CDCVM) 使用。

綜上，可看出兩個組織在持卡者的驗證上差異頗大，如果發卡行希望在同一數位皮夾上，同時支援兩種品牌的卡片，又希望持卡者有較一致的使用體驗，則將是一個相當具挑戰的難題。

(四) 不支援離線交易

為進行離線資料認證 (Offline Data Authentication)，卡片端必須儲存卡片私密金鑰 (ICC private key)，但在 HCE 的應用下，因為缺乏安全元件，所以無法確保此金鑰儲存於手機的安全性，因此不論 Visa 或 MasterCard 都不支援離線直接核可交易。

但為支援國外某些公共交通的應用，則建議支援離線資料認證，比較特別的是 MasterCard 又將原來的 CDA (Combined Dynamic Data Authentication) 做了一些限制而改稱之為 LDA (Local Data Authentication)，主要是強迫將生效日 (Application Effective Date) 設定在到期日 (Application Expiry Date) 之後，讓離線核可交易不可能發生。

四、HCE 之安全防護重點

(一) 行動支付應用程式的安全

目前所有的交易運算都在手機應用程式中進行，且所有的交易機敏資訊 (如：金鑰) 也都儲存在手機應用程式的儲存空間中。由於手機應用程式是在客戶端執行，後端平台無法掌控，因此如何確保手機應用程式的安全性，將變成一個相當棘手，但卻又非常重要的課題。

有關行動裝置應用程式的安全議題，OWASP (Open Web Application Security Project) 已經提出「Top 10 mobile controls and design principles」，而中華民國銀行商業同業公會全國聯合會也針對行動裝置的開發制定「行動裝置應用程式注意事項」，這些都是目前應參考的規範。至於整體安全防護，則可歸納成以下幾個重點：

1. 確保執行環境的安全性

當執行環境不安全時，將增加應用程式遭受攻擊或分析的可能性，因此應用程式應盡可能偵測相關環境，避免在遭受破解 (如 root 或越獄等)、處於開發或偵錯 (Debug) 等環境下運作。

2. **確保執行程式的正確性**

本防護重點旨在避免攻擊者竄改程式，進而避開 (Bypass) 程式中的重要檢核邏輯，如：密碼檢核等。一般須先對程式碼產生其訊息摘要，並在執行過程中插入程式碼完整性的檢核，如發現異常，即中斷程式執行。

3. **防止反組譯工程**

因為手機程式完全暴露於客戶端，本防護重點在如何防範攻擊者於可取得執行碼的前提下，無法輕易進行逆向工程，而取得所有程式的邏輯，甚至透過程式的再造 (注入非法的程式碼)，而產生使用者無法辨識的惡意程式，或透過惡意之程式碼進行相關之攻擊。通常採用混淆 (obfuscate) 技術進行防範，經過處理後的程式碼，其正向執行的邏輯及流程並不會有所改變。簡單的混淆工具可以只是將程式碼中的變數或函數名稱等轉換成另一個較無意義的字串，進階混淆工具則可讓反組譯工具進行反向處理時，產生多種可能性，或者轉換後之程式碼無法成功編譯。

4. **白盒加密** (White Box Cryptography，**簡稱** WBC)

由於整個作業的安全技術核心，仍在於如何確保儲存在客戶端的交易金鑰及與後端認證金鑰的安全性。保護交易金鑰，可防止攻擊者自被攻擊者的手機端，取得甚至大量蒐集此金鑰之資訊，而於其他的設備上進行非法交易。至於保護與後端認證金鑰的安全性，則在防止攻擊者自被攻擊者的手機端，取得甚至大量蒐集此金鑰之資訊，而可偽冒合法使用者向後端平台要求取得交易金鑰之資訊。白盒加密的主要目的，則是在加解密運作過程暴露在使用者面前的狀況下 (視為白盒或白箱)，如何透過邏輯及資料的混淆，仍可保護加解密金鑰或過程的安全性。白箱加密雖然重點在防止取得明碼金鑰值，但仍應注意攻擊者是否有可能在不取得明碼金鑰的情況下，利用客戶端所蒐集到的資料，使用程式中的加解密模組，產生偽冒交易的可能性。

(二) 客戶端與後端平台的認證

HCE 應用的一個重點是在需要時，才自雲端取得交易所需的最少資訊，但另一個重點是如何確保僅有合法的持卡者才可以取得相關資訊，否則如果客戶端與後端平台的認證不夠嚴謹，使攻擊者可任意偽冒取得正確資料以進行交易，則雖然重要資料都儲存在雲端，也沒有任何的意義。

客戶端與後端平台的認證，一般可在註冊時，先進行持卡者的識別與驗證 (Identification & Verification)，成功驗證後，再透過安全的方式建立兩者間認證所需之機密資料，如 MasterCard 的 Mobile Keys 包含加密用與押碼用金鑰，可確保日後合法 MPA 與後台系統連結時，相關訊息傳送的來源辨識性、完整性與隱密性。

另，設備綁定驗證也是另一個防護重點，如此可確保僅註冊綁定的手機始能進行相關資料的交換，可提高攻擊者以任意手機偽冒持卡者竊取資料的難度。

此外，金鑰的補充更新可以說是 HCE 應用中最重要的一項作業，在 MasterCard 的規格中，提供所謂的雙通道防護機制。也就是先透過推播之管道，將某些進行金鑰補充更新必要的機密資料傳送到 MPA，然後再由 MPA 利用這些資料，以另一管道連結至後台進行相關

作業，因為攻擊者必須先破解推播管道的機制，因此也增加攻擊的難度。

五、結語

(一) 雲端支付的安全須考量多重安全機制

雲端支付由於缺乏硬體式的安全元件，其安全機制一直是支付產業最關心的議題。從現行各信用卡組織所提出的解決方案，不論是採用手機應用程式確保執行環境的安全性、確保執行程式的正確性、防止反組譯工程或白盒加密等防護，都是在無安全元件的情況下，防止客戶端機敏資料曝光之安全防護機制。

此外，持卡者註冊時手機的綁定及透過雙通道進行交易金鑰的補充更新，則是防止非法使用者冒名下載金鑰之補強措施，如再搭配風險控管機制，更可有效降低異常的偽冒交易。因此，只要輔以多面向的安全防護，雲端支付應用的交易風險，仍應可控制在可接受的範圍內。

(二) HCE 的應用限制

目前，HCE 的應用範圍，仍以 EMV 卡片為主，基於安全考量，尚無法模擬電子票證業者 (如：悠遊卡、一卡通等) 採用的 Mifare 規格；此外，現行 HCE 亦不適用於離線交易，不管是採用 EMV 的 PKI 機制、或者是傳統的對稱性加解密方式，交易時若無法透過連線與後端平台進行檢核，將無法確認交易所使用金鑰的安全性。

因應不同客群及風險管理需求，TSM 平台可在 OTA (Over-The-Air) 下載悠遊卡、一卡通等行動支付應用，其 SE 防護卡片資料之安控機制也較為嚴密，故目前 TSM 與 HCE 平台二者並存營運，確有其市場之需求性及必要性。

※ 參考文獻 / 資料來源：

1. https://developer.android.com/guide/topics/connectivity/nfc/hce.html - Host-based Card Emulation。
2. https://developer.android.com/reference/android/nfc/cardemulation/CardEmulation.html - CardEmulation。
3. MasterCard Cloud-Based Payments Product Description Version 1.0。
4. MasterCard Cloud-Based Payments Issuer Cryptographic Algorithms Version 1.1。
5. MasterCard Cloud-Based Payments Issuer Security Guidelines Version 1.0。
6. MasterCard Cloud-Based Payments Credentials Management System - Functional Description Version 1.0。
7. Visa Cloud-Based Payments Program Minimum Requirements and Guidelines Version 1.2。
8. Visa Cloud-Based Payments Program Description Version 1.2。

就政策面談全國性繳費 (稅) 業務

本篇摘自 2004 年 08 月出刊之財金資訊季刊第 35 期，由時任金融監督管理委員會銀行局方鏘傑稽核撰寫。

全國性繳費 (稅) 業務，係以建立通暢的金融支付服務基礎環境，發展共通繳費 (稅) 付款平台，強化國內電子付款機制、擴大電子金融服務範圍為目標，建立民眾、事業單位或企業及銀行三贏局面。

自八〇年發展開放性網路技術後，隨著資訊網路產品成熟，網路服務已成為各產業必備應用之技術工具，形成虛擬交易型態取代傳統實體商業交易的趨勢。國內在八十八年間開放金融機構開辦網際網路銀行業務，截至九十三年六月底，本國銀行，除中國輸出入銀行、中華開發工業銀行、台灣工業銀行、台東區中小企銀及花蓮區中小企銀等少數專業銀行，基於業務特殊性及區隔性，尚未提供網際網路銀行業務外，五十家本國銀行已有四十五家提供網路銀行業務，提供比率達百分之九十以上，相較其他產業之應用比率偏高。

除上列網際網路通路之外，各種新興電子工具及電子媒體通路，如無線手機、機上盒、端末交易機等，亦均成為銀行提供客戶進行資金移轉服務之應用工具。因此，通暢各種不同電子支付工具，建構整合性收費平台，成為金融業、各產業及民眾三方迫切需求。

共通性為核心功能

鑑於國內金融支付體系，在跨行零售電子金融支付領域，就功能別而言，包涵四大功能：一、銀行間支付訊息傳送交換；二、銀行間資金結算作業；三、連結清算銀行瞬間完成資金清算；四、儲存相關交換傳送訊息紀錄軌跡等。由於金流是商業交易中解除交易雙方之權利義務關係最終程序，因此，對於各產業及民眾之經濟及商業活動，所涉及不同銀行間資金流動，勢必與上列跨行零售支付有密切關係，在隨著電子化工具應用普遍化之際，整體後端支付系統之互通問題，為監理支付系統最重視課題。

有關系統的互通性，可從兩方面探討；在開放性網路架構上，強調以設計理念，透過垂直及水平整合，有效貫通各產業及銀行間訊息傳送；另一方面，不論開放性網路或封閉性網路均可應用共用性系統設計方法，達到共通目的。

創新支付系統

網路科技進步一日千里，各種新興科技產品不斷推陳出新，銀行面對該多變技術，如何運用科技並戰勝科技，創新為發展電子商務之要務。九十二年度行政院電子、資訊及電信策略會議，對於發展策略性服務產業策略與支援環境議題，海外專家學者建議應加速建立通暢的金融支付服務基礎環境，發展共通繳費 (稅) 付款平台，通暢國內電子付款機制。

鑑於上列具體策略作法，有益於全體金融機構、企業及民眾，並且基於該策略的執行，與支付系統之發展架構息息相關，其推動及執行為金融監理課題，銀行局在考量該付款平台之運作，亦與各金融機構的電子金融系統連結互動有關，爰將銀行公會列為執行單位，並指由該會成立專案小組研究推動，經過半年多研究，在企業、公用事業及稅賦收費之殷切需求下，加速該策略發展計畫的進行。

目前該項計畫預計執行二年，第一階段執行目標為建置計畫，預計民國九十三年六月三十日完成建置工作，第二階段為全面推廣階段，期能整合各項費用之電子收費方式，促使民眾有多元電子收費管道，除可解決銀行委託超商代收市場外，亦加速資金回流企業或事業單位的效率，以降低資金流動成本。

系統設計理念

從該計畫之具體執行內容，該平台功能有四種，一、即時性（Online in Online out）；二、整批性（Batch in Batch out）；三、整批轉即時性（Batch in online out）；四、預約性 (Online in Batch Out)(研議中)。依上列；四項交易功能，整批性資料輸入多屬各事業單位或企業委託入 (扣) 款需求，而線上輸入模式，則多屬民眾繳交相關公用費用、企業費用等需求。在運作上，各收款單位、企業及事業單位必須與其往來金融機構合作，由銀行界面進入該平台，民眾則可透過各種管道連結至該平台進行支付，至於政府之稅收部分，則直接由跨行中心處理。

有關該平台之系統設計模式，在線上即時處理，係以跨行系統為中心，擴大該功能使用，整批處理，則因不具即時性，係以原整批代繳代發系統為中心開發建置。當然，該平台連結架構，前端採以網際網路為中心，後端採專屬性跨行系統。

全面推廣使用

推出一新系統平台其成功之道，即是有效推廣、全面使用，其乃最重要且最困難部分。由於該平台實務運作，涉及民眾、企業、政府及銀行多方參與，因此，推廣該業務之前置性教育訓練、深化及簡單化等工作，甚為重要。爰其推廣策略，可區分為：一、建立銀行共識階段 : 無論銀行已往來之事業單位或新加入的企業，均應以使用該平台；二、擬具推廣文宣：透過各金融機構或銀行公會向所有事業單位或企業，進行專案說明；三、充分向民眾宣導：透過自動櫃員機（ATM）、網際網路（Internet）、電話語音、手機（Mobile Phone）、PDA 及機上盒等，均可快速有效繳交任何費用，並以廣告方式教育一般大眾。當然，推廣之同時應充分揭露該平台具有之高度安全防護措施，俾以維持該平台運作之信譽水準。

收費制度合理化

小額支付作業，因單筆價金低，倘直接加計系統每筆之處理成本，計價成本過高，將造成使用該平台之效益不足及誘因有限現象。由於該平台已歸屬全國性繳費之基礎支付系統，在收費制度上，應端視不同收款或繳款規模及事業單位或企業願意支付成本，採市場合理價格，在以量取勝前提下，全面納入，並採建立多元收費制度。期望在銀行公會全力推動下，全體金融機構及系統營運者能有具體共識，始能真正實現政府推動該計畫美意。

結語

展望未來，金融市場將因金融商品多元化、銀行業務多樣化，使電子金融服務的品質及效率日益重要；然相對的，由於金融競爭日趨激烈，金融市場除應整備高度通暢性支付系統外，對於金融機構風險管理的機制及因應環境變化的能力應同時提升強化，期透過銀行公會研發具前瞻性及共通性之電子支付作業，並擴大電子金融服務範圍，建立民眾、事業單位或企業及銀行三贏局面，此亦是政府執行公共政策一貫之基本立場。

從「巨量資料」綜觀全國性繳費即時交易的成長遠景

本篇摘自 2014 年 10 月出刊之財金資訊季刊第 80 期，由財金資訊公司業務部業務企劃組鍾珍珠高級專員、郭玉慧專員撰寫。

一、前言

為配合「行政院 2003 年產業科技策略會議」決議：「加速建立通暢金融支付服務基礎環境，發展共通繳費 (稅) 付款平台。」中華民國銀行商業同業公會全國聯合會 (以下簡稱銀行公會) 於西元 2004 年通過「建置全國性繳費 (稅) 機制」方案，同年 9 月及 12 月財金資訊公司 (以下稱財金公司) 先後完成活期性帳戶繳費 (稅) 及晶片金融卡繳費 (稅) 平台的建置工作；「全國性繳費 (稅) 平台」旨在提供社會大眾：不限地點 (Anywhere)、不限時間 (Anytime)、任何金融帳戶 (Any account)、任何連網設備 (Any device)、24 小時服務不中斷 (Always on) 的多元化繳費 (稅) 付款機制。

「全國性繳費 (稅) 平台」(系統架構如圖 1 所示) 連結政府機關、金融機構及事業單位，支援各類型支付工具，提供線上帳單查詢及繳納費 (稅) 服務，社會大眾可透過事業單位臨櫃或網站、金融機構臨櫃或網站或「eBill 全國繳費網」等通路，進行各項費 (稅) 繳納，既安全又便捷；是項業務自 2004 年開辦以來，交易量 (值) 逐年穩健成長，2013 年度參與的事業單位家數已達 4,800 家 (截至 2014 年 6 月事業單位家數近 6,000 家)、交易量突破 6,500 萬筆、交易金額高達 1 兆 7,800 億元；其中，尤以全國性繳費即時交易量的增長最為耀眼，其 2013 年度交易量 1,250 萬筆，較 2012 年度 1,061 萬筆，增長 189 萬筆，增長率達 17.8%；而 2014 年 1~6 月交易量 732 萬筆較 2013 年同期 590 萬筆，增長 142 萬筆，增長率達 24.1%，再創新高。本文試圖應用巨量資料分析，探討全國性繳費即時交易的成長遠景，俾提供金融同業瞭解並掌握發展趨勢，協同推動業務，共創佳績。

二、巨量資料分析應用

依據「國際數據資訊公司 (International Data Corporation，簡稱 IDC)」2013 年發布的報告中提到，預估 2012 至 2016 年期間，巨量資料 (Big Data) 市場將呈現高度成長之勢，全球巨量資料技術與服務的市場規模年複合成長率 (Compound Annual Growth Rate, CAGR) 更將高達 31.7%；對照國內研究機構

圖 1　「全國性繳費 (稅) 平台」系統架構

資訊工業策進會「資訊市場情報中心 (Market Intelligence Center，MIC) 」亦於今 (2014) 年 4 月的研究分析報告中指出，2014 年軟體四大趨勢為：行動應用、巨量資料、雲端運算及社交媒體。足見國內外研究機構一致的觀點，巨量資料分析應用是當前及未來數年成長極為快速的產業，深受各國政府所重視，並視為國家發展策略的重要課題。

所謂「巨量資料」，係指兼具「量大 (Volume)」、「複雜 (Variety)」且「動態即時 (Velocity)」，遠超過一般軟體技術所能夠處理的資料規模。巨量資料分析應用不僅受到各國政府重視，更逐步為全球大型公 (民) 營企業及政府機關 (構) 廣泛地應用在諸如：零售、通訊、運輸、金融及健康照護等領域，應用巨量資料不僅可大幅提升公、私部門生產力，更可掌握趨勢變化，以快速回應外在經濟環境及客戶需求之變動並做好充分準備；藉由愈來愈多巨量資料分析應用的開發及最佳實務 (Best Practice) 的展現，勢將為相關產業及資訊軟體技術的發展，帶來深遠影響。

以全球電子商務巨擘 eBay 為例，其線上商品交易每日數以百萬筆計，資料庫系統須負荷每日遞增的 1.5 兆筆交易紀錄，總計每日增加的資料量超過 50「兆」(Terabyte，TB，即 10 的 12 次方)；而為進一步優化交易效能，以迅速提供各種交易媒合，eBay 的系統尚須處理每日超過 50「拍」(Petabyte，PB，10 的 15 次方) 的資料量，俾進行 5 千多項商業以及使用者行為分析。隨著巨量資料時代的來臨，越來越多的企業面臨如同 eBay 般「PB 級」規模的巨量資料挑戰！IDC 預測，全球資料量急速攀升，將從 2013 年的 4.4「皆」(Zettabyte，ZB，10 的 21 次方) 增長至 2020 年的 44「皆」，足足成長 10 倍！資料量不僅巨幅成長，資料的種類與態樣 (數位內容、物聯網及社交媒體等) 也將愈趨複雜，而企業面對量大、複雜且動態即時的訊息，要求快速分析以預應變化的需要，自然愈顯迫切。

三、全國性繳費即時交易分析

企業面對爆炸性成長的各式內、外部大量 (Volume) 資料，以及多元複雜 (Variety) 的各種結構化與非結構化資料等等難題，如何即時 (Velocity) 地整合不同的資料來源，彙總成有用的資訊及商業智慧，以提供組織與高階主管進行前瞻規劃及決策分析，正是巨量資料分析應用的關鍵價值。

財金公司肩負「全國性繳費 (稅) 平台」建置、開發及營運之重責大任，藉由系統資料庫掌握的即時性繳費各上線事業單位與帳務代理行交易情況，以及所使用的支付工具與各項繳費類別交易量等資料間之交叉統計分析，茲彙總整理全國性繳費相關報表分述如后：

(一) 2013 年度各項繳費類別交易量統計表

單位：筆

排名	繳費類別	交易量	帳代行家數	各類別前 3 大交易量帳代行				
				金融代號	金融機構名稱	交易量	小計	占比
1	基金及證券費	4,009,912	10	017	兆豐國際商業銀行	2,376,484	3,644,110	90.9%
				806	元大商業銀行	711,317		
				006	合作金庫商業銀行	556,309		
2	信用卡費	3,665,791	30	021	花旗 (台灣) 商業銀行	2,606,298	2,965,970	80.9%
				805	遠東國際商業銀行	251,022		
				812	台新國際商業銀行	108,650		
3	電信費	3,154,418	10	004	臺灣銀行	1,933,082	3,124,836	99.1%
				805	遠東國際商業銀行	603,404		
				017	兆豐國際商業銀行	588,350		

1. 前 3 大項繳費類別占整體交易量八成以上

繳費類別前3大項依次為：基金及證券費、信用卡費、電信費，交易量合計 1,083 萬筆，占全國性繳費業務整體交易量的 86 .7%，詳如下：

(1) 基金及證券費

2013 年度交易量逾 400 萬筆，國內主要投資信託機構多數已參加「全國性繳費平台」，其整批轉即時 (授扣) 作業可於同一營業日發動多次扣款，相較於傳統的批次作業，更具彈性，交易模式貼近各投信公司基金扣款需求，深受依賴。

(2) 信用卡費

交易量超過 366 萬筆，排名第二，僅次於基金及證券費；最為特殊的是，本項帳務代理行家數總計 30 家 (2014 年 4 月再新增 1 家－滙豐 (台灣) 商業銀行，達 31 家)，居各項繳費類別帳務代理行家數之最，國內 33 家信用

卡發卡銀行當中，僅澳盛 (台灣) 商業銀行及星展 (台灣) 商業銀行尚未加入，最值得分析的是從 104 年 5 月起，每月繳信用卡費的交易量均超過 40 萬筆，排名已超過基金證券費，預估今年年度交易量將躍居首位。

(3) **電信費**

交易量逾 315 萬筆，名列第三，其中，前 5 大電信公司：中華電信、台灣大哥大、遠傳電信、亞太電信及威寶電信之交易量合計達 312 萬筆以上 (詳表 1)，占電信費交易量 99 .1%，交易量集中情況，可見一斑。

表 1　102 年度 (前 5 大電信公司) 電信費交易量統計表

名稱	用戶數	交易量 (單位：筆)			
		102 年度	排名	101 年度	增減率
中華電信股份有限公司	10,614,514	1,935,313	1	1,754,139	10.3%
台灣大哥大股份有限公司	7,203,581	538,639	3	375,202	43.6%
遠傳電信股份有限公司	7,161,750	603,404	2	504,527	19.6%
亞太電信股份有限公司	2,156,153	24,257	5	21,300	13.9%
威寶電信股份有限公司	1,675,885	24,786	4	24,657	0.5%
總計	28,811,883	3,126,399	-	2,679,825	16.7%

備註：本表「用戶數」源自 **103** 年 **1** 月台閩地區行動電話業務概況表。

2. 各項繳費類別之前 3 大帳務代理行交易量占比，舉足輕重

檢視 18 項繳費類別當中，排除「交通加值費」僅臺灣銀行 1 家帳務代理行，以及占比 79.0% 之「貸款」、74.3% 之「管理費」 與 69.6% 之「會費」等項外，其餘 14 項之前 3 大帳務代理行合計交易量占比，均超過八成以上，可見帳務代理行「大者恆大」之態勢明顯。

1. 前 10 大帳務代理行交易量占比，居整體交易量九成以上

上表所載交易量前 10 大帳務代理行所創造之交易量，占比合計高達 91.4%，遠高於其他 24 家帳務代理行所累積之交易量 (占比 8.6%)；再次驗證「帳務代理行大者恆大」之業務發展趨勢。

(二) 2013 年度前 10 大帳務代理行交易量概況表

單位：筆

排名	金融代號	金融機構名稱	交易量	整體交易量占比	前 3 大項繳費類別
1	017	兆豐國際商業銀行	3,386,094	27.1%	基金及證券費、電信費、仲介費
2	021	花旗 (台灣) 商業銀行	2,646,690	21.2%	信用卡費、停車費、貸款
3	004	臺灣銀行	2,061,325	16.5%	電信費、交通加值費、公用事業費
4	805	遠東國際商業銀行	871,044	7.0%	電信費、信用卡費、貸款
5	006	合作金庫商業銀行	832,462	6.7%	基金及證券費、醫療費、公用事業費
6	806	元大商業銀行	716,524	5.7%	基金及證券費、信用卡費、醫療費
7	013	國泰世華商業銀行	338,318	2.7%	基金及證券費、信用卡費、服務費
8	812	台新國際商業銀行	223,595	1.8%	信用卡費、仲介費、基金及證券費
9	050	臺灣中小企業銀行	179,014	1.4%	仲介費、公用事業費、信用卡費
10	008	華南商業銀行	170,223	1.4%	信用卡費、仲介費、基金及證券費
合計			11,425,289	91.4%	

2. 前 3 大帳務代理行所代理之繳費類別，各擅勝場

綜觀本表與前項「2013 年度各項繳費類別交易量統計表」交叉分析結果，前 3 大帳務代理行所代理繳費類別之交易情況，各有擅場，茲依序分述如后：

(1) 獨占鰲頭的兆豐國際商業銀行

兆豐國際商業銀行 2013 年度交易量高達 338 萬筆以上，排名第一，為金融機構推動全國性繳費業務的最佳典範；在 18 項繳費類別交易量排名前 3 大的帳務代理行名單中，兆豐國際商業銀行就多達 10 項，占一半以上，其中居首位的有：基金及證券費、仲介費、貸款等 3 項，業務霸主地位穩固。

(2) 表現驚艷的花旗 (台灣) 商業銀行

花旗 (台灣) 商業銀行所代理的帳單事業單位僅有 2 家 (自家及臺北市停車管理工程處)，所參加的繳費類別也只有 3 項 (信用卡費、貸款及停車費)，無論就上線帳單事業單位家數或繳費類別項目，皆遠遠不及其他的帳務代理行，但卻成功創造高額的交易量，達 264 萬筆以上，表現令人驚艷；其中，單是信用卡費交易量就占 260 萬筆，其信用卡繳費推展模式，實值得所有發卡銀行效法推廣。

(3) 穩紮穩打的臺灣銀行

公股銀行龍頭臺灣銀行交易量達 206 萬筆，名列第三，在 18 項繳費類別當中，臺灣銀行代理的帳單事業單位類別就占 15 項之多，而業務推展最為出色且居首的繳費類別包括：電信費 (主要代理為中華電信) 、保險費 (主要為中央健保局) 、學雜費 (代收學校機構逾 1,200 家) 等 3 項，業務推動成績斐然。

四、業務發展趨勢及遠景

Bank 3.0 時代，無疑宣告新興的資訊科技與創新的商業模式，將打破並顛覆金融產業的既有疆界及規則，維持現有服務已無法滿足客戶的需求，為因應變革，金融機構之致勝關鍵即為接受變局，並勇於創新，善用「行動力」與「資訊力」，以貼近客戶生活模式與需要，持續提供創新金融功能與多元便捷的金流服務；誠如 Bank 3.0 作者 Brett King 所說：「銀行不再是一個地方，而是一種行為 (Banking is no longer a place you go, but something you do.)」，台灣金融研訓院鄭貞茂院長在譯版序文中指出「隨著科技發展，在新一代消費者的認知中，銀行已漸由一個場域的概念，轉化為無處不在的服務。」因此各家金融機構勢必得在大環境的變化中，找出生存與獲利的方法，才能在新世代中勝出。

(一) 行動力

依據 Google 行動網路及使用者行為調查報告所載，臺灣智慧型手機之普及率超過 5 成且持續穩定成長，臺灣人對智慧型手機的依賴度更是亞太地區之冠 (81%)；智慧型手機可說是永不關機、如影隨形，改變臺灣民眾習以為常的生活形態，更以其「隨時」、「隨地」的優勢，傲視各產業行銷通路，當行動產業透過行動裝置，創造無限（線）商機的同時，金融機構更應善用自家的專業與優勢，開創行動支付服務，以創造業務佳績。

為迎接行動支付世代的來臨，由台灣票據交換所、聯合信用卡處理中心及財金公司所共同規劃建置之 PSP TSM (Payment Service Provider, Trusted Service Manager) 平台服務，預計將於 2014 年底上線，未來，各家金融機構即能透過金融 PSP TSM 平台作業，將所發行的晶片金融卡，利用空中下傳技術 (Over The Air，OTA) 載入手機，提供客戶更為便捷的繳費支付機制；屆時，結合全國性繳費業務的多元整合服務，客戶可隨時隨地透過金融 PSP TSM 平台，於行動裝置享受「全國性繳費平台」逾 6,000 家事業單位、超過 13,000 種的帳單繳納服務。

(二) 資訊力

善用資訊力者如：Google 經由分析每月高達 1,000 億筆搜尋結果，分區別類歸納熱門搜尋排行，甚至能預測股票市場走勢與經濟指標；而 FaceBook 藉由分析使用者行為，決定使用者能「看到」的最新動態與廣告內容，不僅增加使用者對 FaceBook 的黏著度，更確保廣告用「對的方式」傳達給「對的人」；而在網路商城購物時，也經常會出現「買這件商品的人，同時瀏覽 / 買…」，這些都是巨量資料的商業應用，在使用者 / 客戶享受巨量資料帶來便利的同時，也為懂得善加利用巨量資料優勢的企業及商家，創造無限商機。

展望未來，大量的支付交易勢將透過虛擬通路進行，交易過程中所隱藏的巨量資料，當可協助金融機構揭開客戶交易背後的神秘面紗，藉由分析客戶使用的繳費管道、繳費類別、支付工具，甚且是繳費時間、支付頻率…等資料，以歸納客戶屬性與交易行為，並從中思索最佳支付方案，或結合現有業務、或推出全新商業模式，以提供客製化、差異化金流服務，進一步擴大營運規模；資訊力可幫助金融機構挖掘新的客群，也可協助找回遺失的客戶。

五、結語

巨量資料應用並不是新的技術，多數金融機構現已進行的資料倉儲、商業智慧、顧客關係管理等等，都屬於其中的一環，經由行動裝置與社群網路的普及，使非結構化資料的重要性日益增加，而雲端運算技術的興起，更加速巨量資料處理、分析與應用，關鍵就在於資料中的「含金量」，分析的目的在於品牌定位、精準行銷、促進交易與提高市占率，嗣為金融機構創造價值。

綜觀全國性繳費即時交易，因應數位時代浪潮來襲，行動支付應用的趨勢非常明確，尤其是身處 4G 時代，如何提供更有利的 M 化網路環境，以因應多通路、多介面的支付樣態，並為滿足新世代族群交易習性的變化，金融機構可藉由巨量資料分析，篩解出資料內含的各種「價值」，及早掌握客戶需求、洞察商機，積極開發潛在客群並深耕既有客戶；尤其，面對眾多來勢洶洶的非金融業者之挑戰與競爭，全體金融機構更須緊密互助合作，善用「全國性繳費平台」，邀請更多的帳單事業單位參加，金融機構的代收市場才能進一步擴大成長，以提供社會大眾無遠弗屆、24 小時全年無休，兼具安全及便捷的共通性繳費平台，為實踐無現金社會的全方位金流服務而賡續創新。

※ 參考文獻 / 資料來源：

1. 國家發展委員會新聞稿「巨量資料的發展將改變世界」，網頁 http://www.ndc.gov.tw/m1.aspx?sNo=0019482。
2. 2014 年 4 月，資訊市場情報中心 (MIC) 資深產業分析師翁偉修「雲端運算市場發展現況與趨勢」；以及資深產業分析師童啟晟「巨量資料在軟硬體整合趨勢下產業價值體系的建構」。
3. 2011 年 6 月 24 日，iThome「巨量資料來襲」，網頁 http://www.ithome.com.tw/node/68277。
4. 2014 年 5 月 1 日，iThome「2020 年全球資料量將成長至 44ZB」，網頁 http://www.ithome.com.tw/article/87190。
5. 2013 年 Google 行動網路及使用者行為調查報告。

繳費 e 化、行動未來－整合利用既有的基礎建設，提供快捷便利的繳費服務

本篇摘自 2012 年 09 月出刊之財金資訊季刊第 72 期，由時任財金資訊公司研發部設計二組林弘斌組長（現任為代理經理）、研發部設計二組林書玉工程師撰寫。

一、前言

資訊科技日新月異，每隔一段時間都會有新的技術突破與創新。於民國 84 年至 90 年間，網際網路快速發展，爰此，財金資訊公司 (以下簡稱財金公司) 在既有的金融機構跨行作業基礎上，於 93 年 9 月完成全國繳費 (稅) 平台，提供社會大眾便捷的繳費服務及靈活的繳費模式。自 96 年 6 月 iPhone 在美國上市開始，蘋果公司 (Apple Inc.) 的 iPhone 與 iPad 系列，以及 Google Android 開放式平台之智慧型手機與平板電腦，已然成為近幾年來最受矚目的行動裝置；這些行動裝置創新的使用者友善界面及幾乎無所不能的各種應用，使消費者能夠隨時隨地即時完成各種商業交易或服務。

隨著行動化時代的來臨，我們的生活得以越來越舒適與方便，行動化服務之相關應用更加速推動日常生活與資訊科技之跨領域整合。繳費 e 化朝向行動化服務發展，代表新的通路與支付工具之間的整合，背後的思維常須考量如何整合利用既有的基礎建設，以快速有效及最低成本的方式提供民眾更新及更快捷便利的繳費通路。

本文將輔以時間為軸，指出繳費服務 e 化的發展歷程，並歸納整理金融機構因應行動世代來臨而發展出的各式各樣行動繳費身分認證機制之現況，進而提出整合金融機構與全國性繳費 (稅) 服務之跨行繳費體系的想法，發展 APP 繳費業務模式，以此策略創造核心服務的價值，持續拓展與強化多元化的繳費通路，提供大眾更優質完善的 e 化繳費服務。

二、從傳統網頁到行動繳費

(一) e-Bill 全國繳費網

配合行政院 92 年產業科技策略會議之「加速建立通暢金融支付服務基礎環境，發展共通繳費 (稅) 付款平台」決議，中華民國銀行商業同業公會全國聯合會 (銀行公會) 於 93 年通過「建置全國性繳費 (稅) 機制」，財金

公司於同年 9 月及 12 月先後完成以活期存款帳戶及晶片金融卡為支付工具之全國性繳費 (稅) 平台跨行交易建置工作，全國性繳費 (稅) 平台「多事業單位帳單」對「多金融機構帳戶」(請參圖 1) 的業務設計，以及“ 本人帳戶限繳本人帳單 ” 原則與晶片金融卡的安全設計，民眾無須事先向金融機構提出申請，就可以透過事業單位及金融機構佈建的繳費通路 (例如事業單位網站、MOD、網路銀行、ATM、eATM 等) 繳納各項費用帳單。

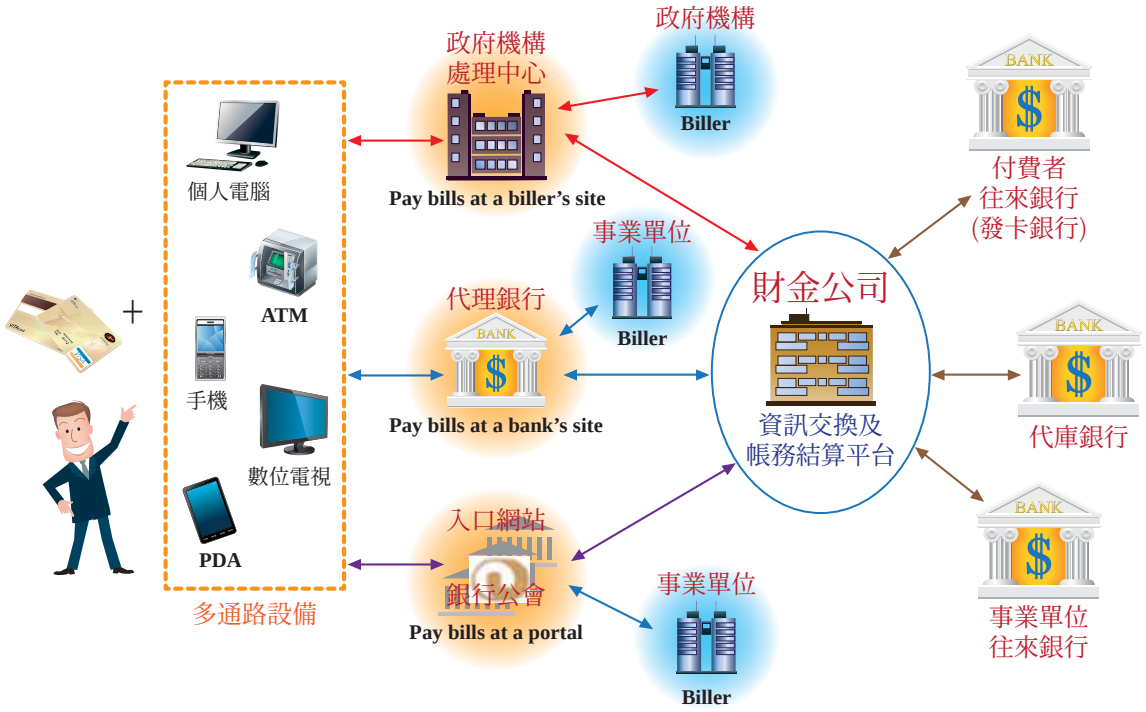


圖 1　全國性繳費 (稅) 平台「多事業單位帳單」對「多金融機構帳戶」示意圖

不論是事業單位或是金融機構佈建的繳費通路，在個別通路上可以繳納的費用項目事實上不多，通常僅限於事業單位本身所收取的服務費項目或金融機構與事業單位簽約可以代收的費用項目。是故，若民眾手上持有 A 事業單位及 B 事業單位的帳單，而 A 事業單位的費用帳單委由甲銀行代收、B 事業單位的費用帳單委由乙銀行代收，則民眾必須分別使用甲銀行與乙銀行佈建的繳費通路才能完成這兩張帳單的繳納作業；也就是說，雖然 e 化讓繳費作業變得快捷，但分散的通路對於便利性的提升卻未必有太大的幫助。有鑑於此，94 年 8 月財金公司完成建置全國性繳費 (稅) 平台專屬入口網站「全國繳費網」(或稱為 e-Bill 網站或 e-Bill 全國繳費網，網址為 https://ebill.ba.org.tw，如圖 2)，該網站在建置概念的專屬性與共通性讓民眾可以免除面對多繳費通路的困擾，享受“ 一站購足 (One-stop Shopping) ” 的繳費便利性，直接在 e-Bill 網站上使用晶片金融卡與活期存款帳戶繳納參加銀行所代收的費用項目，提升了 e 化繳費作業的便利性。

圖 2　e-Bill 全國繳費網首頁

e-Bill 全國繳費網的操作流程大致說明如後：民眾以個人電腦的網際網路瀏覽器連結 e-Bill 網站首頁，在首頁上選擇費用項目，並依事業單位寄發的帳單輸入紙本登載的銷帳資訊及金額，最後選擇繳款方式並進行繳納。

e-Bill 全國繳費網接受的支付工具有晶片金融卡與活期性帳戶，晶片金融卡憑其高安全性的優勢，不僅可用以繳納所有的費用項目，同時也是全國性繳費 (稅) 平台建置初期最重要的支付工具；至於以活期性帳戶為支付工具，基於交易安全性考量，以及保障帳戶所有人之權益，作業設計面以 “ 本人帳戶限繳本人帳單 ” 為原則，是以於繳費時，必須同時輸入帳單所有人的身分證字號，此作業機制稱為 “ ID+Account ”，也因此，在 “ ID+Account ” 作業機制下，可以繳納的費用項目較為受限 (註 1)，大致上僅限於留有帳單本人身分證字號的金融業、大型事業單位及公共事業單位之費用，例如信用卡費、電信費及交通資費等，茲整理 e-Bill 全國繳費網支援以活期性帳戶繳費的代收費用項目如下表 (表 1) 供參，其中 “ e-Bill 即查 ” 一欄表示該費用項目可以在 e-Bill 全國繳費網完成查繳銷 (線上即查、即繳、即銷) 一次性作業。

表 1　e-Bill 全國繳費網活期性帳戶繳費項目一覽表

費用類別	費用項目	事業單位	e-Bill 即查
金融	信用卡費	合作金庫商業銀行、華南商業銀行、彰化商業銀行、上海商業儲蓄銀行、台北富邦銀行、花旗 (台灣) 商業銀行、臺灣新光銀行、陽信商業銀行、聯邦商業銀行、元大商業銀行、永豐商業銀行、玉山商業銀行、台新商業銀行、日盛國際商業銀行、安泰商業銀行	
	繳納貸款	花旗 (台灣) 商業銀行、三信商業銀行、安泰商業銀行、遠東國際商業銀行	
電信	中華電信費	中華電信公司	V
	遠傳電信費	遠傳電信公司	V
	台灣大哥大電信費	台灣大哥大公司	V
	大眾電信費	大眾電信公司	
	威邁斯電信費	威邁斯電信公司	
交通	國道高速公路交通資費	遠通電收公司	V

(二) 行動版 e-Bill

除了作為全國性繳費 (稅) 平台專屬的入口網站外，財金公司為了進一步提供費用帳單線上即時查繳銷一次完成之便利服務，陸續與事業單位洽談合作，並進行雙方資訊系統的主機連線作業 (註 2)。藉由系統面的連線整合與即時性的資訊交換，民眾可直接在事業單位的服務網站上查詢帳單後，進行線上即時繳銷，也可以在 e-Bill 全國繳費網上 (透過主機連線作業) 查詢事業單位帳單資訊後進行線上即時繳銷，適用的費用項目有電信費、停車費、水費及信用卡費等，詳細內容可上 e-Bill 全國繳費網查詢。上表 1 主要臚列 e-Bill 全國繳費網所支援以活期性帳戶繳費的代收費用項目，權充參酌，惟未納入支援查繳銷但僅接受晶片金融卡繳納的水費、停車費等費用項目。

近年來，隨著電信業者寬頻通信技術的進步，以及行動應用加值服務的創新發展，國內使用行動上網服務之消費者與日俱增。根據國家通訊傳播委員會的資料顯示，我國行動通信用戶普及率已逾 120%，也就是說每 100 位民眾持有 120 個手機門號，其中 3G 用戶數占行動通信總用戶數之比例已達六成七以上。再者，可使用行動上網服務之總用戶數亦高達 1,949 萬戶，占行動通信用戶比例提升至 70%，顯見行動上網的應用正快速融入民眾日常生活當中。資策會 FIND 調查預估：至 104 年底前，將有超過半數消費者使用智慧型手機，可見行動化服務的時代已經來臨。

因應行動化繳費服務需求，並響應政府「優質網路政府計畫」，財金公司於 100 年 12 月推出行動版 e-Bill 全國繳費網 (https://ebill.ba.org.tw/MPP，如圖 3)，希望以優質便利的行動化服務，提供讓民眾安心的快捷便利的繳費通路。

圖 3　行動版 e-Bill 網站首頁

在設計上，行動版 e-Bill 網站的網頁編排，採用適合智慧型手機 (例如 Apple iPhone、Google Android) 螢幕大小的單欄式設計，去除過於繁複的圖片及文字，以提供使用者簡約、清晰的操作介面，同時可以增加行動網頁瀏覽的順暢度。

在使用上，民眾僅須透過智慧型手機的 Web 瀏覽器，以隨處可得的無線網路連結至行動版 e-Bill 網站，即可輕鬆使用本人之活期性帳戶，繳納本人的信用卡費、貸款及電信費等費用；相較於傳統的 e-Bill 全國繳費網，其快捷度與便利性顯然略勝一疇。依據 StatCounter 在西元 2011 年 3 月份所提供的行動裝置瀏覽器市占率統計資訊 (圖 4)，iOS 為 24.27%、Opera 21.02%、Nokia 15.94%、Android 15.28%，以該等市占率觀之，全球行動裝置的瀏覽器各自擁有一定比例的愛好者，且非由特定的瀏覽器所獨大，然而反觀臺灣的行動裝置瀏覽器市占率，則是以 Android (38.02%) 和 iOS (35.61%) 所搭載的瀏覽器為主流，合計超過七成的高市場佔有率，因此在開發行動版 e-Bill 網頁時，以 Google Android 及 Apple iOS 兩個行動平台的相容性為優先考量，未來則會持續依市場的發展狀況，提高行動版 e-Bill 網站在其他行動平台的相容性。

在支付工具的選擇上，囿於硬體規格的限制，智慧型手機的 Web 瀏覽器無法存取晶片金融卡，故活期性帳戶是唯一可行的支付工具，這同時也表示行動版 e-Bill 網站上可繳納的費用項目比較受限。雖然目前還無法做到在行動版 e-Bill 網站上繳納所有的費用項目，但所有在傳統 e-Bill 網站可以用 " ID+Account " 作業機制繳納的費用項目，都可以在行動版

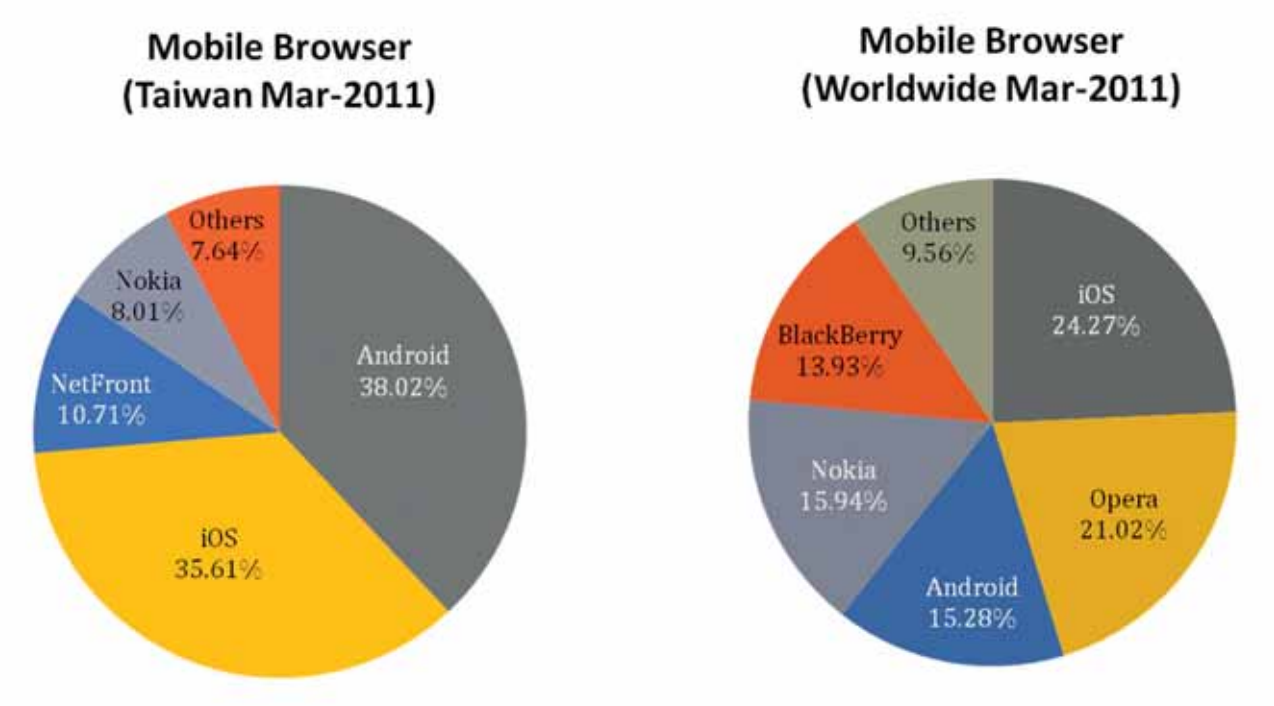


圖 4　行動裝置瀏覽器市占率

e-Bill 網站上架服務 (參考表 1)。原本在傳統 e-Bill 網站上不甚突出的 " ID+Account " 作業機制，意外實現了行動化繳費服務，當真是始料未及；而大型事業單位因收取服務費用之目的而收集帳單本人身分證字號之人工作業所累積的資訊資產與基礎建設，在 e-Bill 全國繳費網加以有效整合利用之後，使 " 本人帳戶限繳本人帳單 " 原則得以確保，則是實現行動化繳費服務背後不可或缺的重要因素。

三、行動 APP 與 APP 繳費

所謂的行動 APP (Applications)，是指安裝於行動裝置 (通常指 iPhone、Android 等智慧型手機或 iPad 平板電腦) 上各式各樣的應用程式，有別於行動版 Web 瀏覽器 (可用以連結並使用行動版 e-Bill 網站)，這些應用程式是全球行動軟體開發商及服務提供者 (金融、電信、網路業者) 所提供的個人化加值型應用程式，其應用的領域包括遊戲、行動購物、行動銀行、社交網路等，使用者必須透過行動裝置進入線上軟體商店購買 (或免費) 後，再行下載並執行安裝。

國內金融機構搶搭行動 APP 的熱潮，紛紛開發 iPhone、Android 等平台的行動銀行 APP，為的是希望透過多樣化的應用服務，以便客戶可在第一時間掌握更精確的理財資訊，以提高客戶的忠誠度。目前國內已有 20 家金融機構開發專屬的行動銀行 APP，每家金融機構依據其主打的業務提供豐富的服務項目，包含銀行帳戶管理、信用卡帳單查詢、基金買賣及換匯等功能，其中全國性繳費 (稅) 業務參加銀行所開發的行動銀行 APP 則提供繳費功能，可稱之為 APP 繳費。

財金公司的行動版 e-Bill 網站基於“本人帳戶限繳本人帳單”原則，僅能代收有限的繳費項目；然有異於此，金融機構因有客戶的帳戶資料且能自製專屬行動 APP 的身分認證機制，故其 APP 繳費的服務項目並沒有太大的限制，通常可以涵蓋該金融機構代收的所有費用項目，惟如同本文在介紹“e-Bill 全國繳費網”時所述，個別的全國性繳費（稅）業務參加銀行所代收的費用項目不會太多，通常只限於金融機構與事業單位簽約代收的費用項目。

茲整理全國性繳費（稅）參加銀行之行動 APP 提供的繳費項目如下表（表 2），其中可以看到各式各樣的身分認證機制，包括帳號密碼、簡訊 OTP、簡訊非約轉密碼、簡訊動態密碼、Display Card 動態密碼、晶片金融卡 OTP、OTP 密碼精靈、行動網銀憑證、裝置認證及行動支付 X 卡等 10 種，顯而易見地，金融機構因有客戶帳戶資料而具有自製專屬之身分認證機制的能力，此非 e-Bill 全國繳費網可以輕易達到的。

對民眾而言，使用行動版 e-Bill 網站或行動 APP 繳費的便利性優於使用傳統的 e-Bill 網站，然而由於繳費項目的限制，削減了此便利性。囿於行動裝置瀏覽器之技術限制只能使用活期性帳戶做為支付工具，行動版 e-Bill 網站的繳費服務在繳費項目上不會有爆發性的成長，現階段唯有保持穩定發展；至於 APP 繳費方面，已經在市場運作的各式各樣的身分認證機制是相當重要的投資成果，若能善加整合利用，設法克服系統面的限制，將金融機構行動銀行 APP 的後端系統和 e-Bill 全國繳費網的主系統建立主機連線，就有機會以 e-Bill 全國繳費網的服務內容為基礎，進行擴充 APP 繳費服務的費用項目，進而創造使用者（快捷便利的繳費）、金融機構（豐富的 APP 繳費服務與客戶的忠誠度）及財金公司（增加全國性繳費交易量）三方三贏的局面。

四、結語

推動全國性繳費（稅）業務的目標，旨在提供優質便捷的繳費通路與安全完善的支付環境，經由全體金融機構的共同努力，近年來仍持續增加了許多代收費用類別，例如醫療住院費、慈善捐款、報名訓練費…等，並提供超過 3,800 餘家事業單位的帳單代收服務。在提供便捷的繳費通路的同時，無紙化「即查、即繳、即銷」的繳費服務，亦對環保貢獻了一份心力。

財金公司以穩定與安全的跨行平台，提供金融機構、企業及社會大眾便捷的金資流服務，也擔負全國繳費（稅）服務 e 化發展、推動及整合的重任。面對未來不斷推陳出新的行動加值服務及數位化家庭應用（例如行動銀行、數位家庭多媒體平台等），將戮力引導全國性繳費（稅）平台朝向服務導向之雲端跨行金流資訊中心的方向發展，並由財金公司制定服務介接的協定與規格，金融機構發展各自的前端繳費認證機制，如此，行動支付工具可不必侷限於活期性帳戶，進而拓展更多可能的繳費通路，提供民眾更優質完善的 e 化行動繳費服務。

表 2　全國性繳費 (稅) 業務參加銀行之行動 APP 繳費項目一覽表

金融機構	非約定轉帳認證機制	行動繳費 / 支付認證機制	行動 APP 繳費項目
中國信託銀行	簡訊 OTP	帳號密碼	信用卡費 (自行)、貸款費、中華電信費、遠傳電信費、威寶電信費、台電電費、台北市水費
玉山銀行	無	帳號密碼	信用卡費 (本人)
彰化銀行	晶片金融卡 OTP、簡訊 OTP	晶片金融卡 OTP、簡訊 OTP	信用卡費 (自行)、水費、電費、中華電信費、代收學費
土地銀行	無	帳號密碼	信用卡費 (自行)、貸款費 (自行)
元大銀行	簡訊非約轉密碼	簡訊非約轉密碼	信用卡費 (本人)、省水水費、台電電費、中華電信費
第一銀行	OTP 密碼精靈	OTP 密碼精靈	信用卡費 (自行)、期貨保證金、水費、電費、學雜費、中華電信費
華南銀行	OTP	帳號密碼	信用卡費 (本人)
永豐銀行	簡訊動態密碼、Display Card 動態密碼	簡訊動態密碼、Display Card 動態密碼	信用卡費 (本人 / 非本人或自行 / 他行)
台北富邦銀行	簡訊動態密碼	簡訊動態密碼	公共事業費 (中華電信費、台北市水費、台灣高雄市水費、台電電費、陽明山瓦斯費)、富邦產險保費、勞保費、信用卡費 (自行)
臺灣銀行	無	帳號密碼	信用卡費 (自行)
合作金庫銀行	行動網銀憑證	行動網銀憑證	信用卡費 (自行)、中華電信費、台灣自來水費、電費、健保費、勞保費、國民年金、學費
台新銀行	裝置認證	裝置認證	信用卡費 (自行)、中華電信費、威寶電信費、遠傳電信費、台北市自來水費
花旗銀行	無	無	信用卡費 註：可使用他行活期性帳戶繳納，限繳本人
兆豐商銀	動態密碼卡	無	無
國泰世華銀行	無	帳號密碼	信用卡費 (自行)、國泰人壽保費
遠東商銀	無	帳號密碼	信用卡費 (自行)、遠傳電信費
新光銀行	無	帳號密碼	信用卡費 (自行)、新光人壽續期保費
澳盛銀行	無	帳號密碼	信用卡費 (本人)
日盛銀行	無	帳號密碼	信用卡費 (本人)
萬泰銀行	無	行動支付 X 卡	高鐵 T-EX、良興電子資訊廣場 註：此非萬泰行動 APP 提供之費用項目，須另外安裝高鐵 T-EX、良興行動金賺軟體

近年，Nokia、Google、Apple 等紛紛推出搭載近距離無線通訊技術 NFC (Near Field Communication) 晶片的手機，顯見相關硬體技術已經到位，惟目前 NFC 行動付款機制仍侷限在電子錢包、小額付款的應用層面 (註 3)，未來若能利用手機 NFC 非接觸式的通訊介面讀取晶片金融卡，發展可與全國性繳費 (稅) 平台整合的跨行支付作業，將可提供更實用的非約定轉帳與 e 化繳費服務，此乃行動支付致勝的關鍵。NFC 技術牽涉的應用層面相當廣泛，有賴金融機構、電信業者、手機軟體開發商等攜手連袂，共同解決技術以外的應用門檻，方能進一步發展成為兼具安全性與便利性的行動付款機制，為行動支付的未來奠定新基石。

註釋：

1. 有關使用活期性帳戶在 e-Bill 網站上繳納費用之作業設計，請參考財金資訊季刊／ No.70 ／ 2012.3 之專題報導：簡政便民繳稅 e 化新增服務。
2. 有關即查、即繳、即銷的相關內容，請參考財金資訊季刊／ No.70 ／ 2012.3 之專題報導：即查、即繳、即銷之全國繳費網。
3. 有關 NFC 行動付款機制的相關內容，請參考財金資訊季刊／ No.69 ／ 2011.12 之專題企劃：我國行動支付之業務應用探討。

參考文獻 / 資料來源：

1. 財金資訊公司網站 (www.fisc.com.tw)。
2. 國家通訊傳播委員會新聞稿 (http://www.ncc.gov.tw/Chinese/print.aspx?table_name=news&site_content_sn=8&sn_f=18725)。
3. 資策會 FIND 網站 (www.find.org.tw)。
4. StatCounter Global Stats (gs.statcounter.com)。


e-Bill 全國繳費網
eTag儲值
臺北市停車費
新北市停車費
臺中市停車費
高雄市停車費
汽機車燃料使用費HOT!
陽光交給你
帳單交給全國繳費網
eTag儲值、停車費、汽機車燃料使用費，
透過網路繳納，輕鬆方便又省時
e-Bill 全國繳費網
ebill.ba.org.tw
ios
Android
財金資訊股份有限公司
FINANCIAL INFORMATION SERVICE


Focus 專注·專業 @ Innovation 創新·引導 @ Security 安全·保障 @ Convenience 便捷·服務

資訊應用篇

消費金融－卡片支付業務發展新趨勢

本篇摘自 2014 年 01 月出刊之財金資訊季刊第 77 期，由財金資訊公司研發部卡片設計組洪國峻組長、陳廷豪工程師（現任為副組長）撰寫。

一、前言

我國信用卡發展歷史，乃自民國 63 年發行第一張信用卡，至今已有 40 年，在國際組織及眾多發卡銀行積極地行銷推廣下，信用卡已逐漸成為國人除現金外最常用的支付工具。依據金融監督管理委員會之統計資料顯示，至 102 年 10 月底，全國共有 3,629 萬張流通卡，約為總人口的 1.58 倍，月簽帳金額更高達 1,722 億元，由此所產生的經濟效益至為顯著，信用卡業務已然成為金融機構的重要消金業務與必爭市場。因應生活的需要，卡片的種類與應用日趨多元與普及，而金融卡、儲值卡亦相繼進入消費領域。

提供持卡人以各類卡片進行交易之實體通路，雖甚為廣泛，惟隨著電子商務市場快速崛起，網路交易比例更大幅增加；嗣拜科技進步之賜，電腦網路與行動通訊日益發達，支付工具與金流系統也隨之展現嶄新的面貌與無窮的應用，而越是經由便捷的收單系統，就越能促進「電子商務」交易的成長，也使得商業活動更為興盛。

近年來，「行動支付」(Mobile Payment) 亦為快速發展之新興支付方式之一，根據趨勢分析研究機構 Gartner 調查顯示，2013 年全球行動支付交易額將達 2,354 億美元，較 2012 年之 1,631 億美元成長 44%，預期 2012 年到 2017 年間，全球行動交易量與交易額將以平均每年 35% 的幅度成長，至 2017 年行動支付總市值預測將達 7,210 億美元，2013 年金融轉帳與商品購買分別占總交易額的 71% 與 21%，預期未來「行動支付」掀起的熱潮與商機將無可限量，為快速且完整支援各項新穎支付工具之應用，系統架構的設計亦將朝更多元化及彈性化方向發展。

然支付相關營運系統與處理機制尚須具備完整與完善的設計，減免錯誤與防範風險，業務方能順利營運與推展。本文謹就財金資訊公司 (以下稱財金公司) 收單共用平台為例，扼要說明卡片支付業務核心系統及前端支付應用之設計與發展。

二、財金收單共用平台

財金公司初期因應少數金融機構的基本業務需求，所提供的共用平台功能較為簡易，嗣經國際組織的協助、實務上的摸索，並結合多年經營跨行平台的經驗，復歷經市場實際考驗，凝聚出穩定可靠的系統架構與功能，以及具備支援所有卡種交易之收單共用平台，此開放且安全穩定的卡片交易處理平台，可大幅降低金融機構開辦卡片收單業務的阻力，以及免除一般自建者必須投入的龐大建置成本，協助金融機構快速地開展卡片業務與穩定妥適地處理信用卡交易，在電子商務興盛的時代更可協助侷限於開發網路商店的金融機構建構純網路與行動支付收單平台，以結合其信貸業務共同開發商戶服務。以下分別就「交易訊息轉接授權」、「批次帳務清算處理」兩層面敘述。

三、 交易訊息轉接授權

由於卡片交易流程涉及持卡人、特約商店或稱特店、收單銀行、發卡銀行、處理中心、國際組織等多項角色 (如圖 1 所示)，因此，交易資訊的往來傳遞亦十分複雜。

此外，考量 ATM 預借現金、繳交規費稅、語音 / 傳真購物、企業採購卡等，都是收單銀行可發展的通路，財金公司爰提供開放性與多元性之收單共用平台，以便各項來源通路易於串連該平台，金融機構即可快速推展各種卡片收單業務。該平台之交易轉接授權可分收單來源通路、連線訊息處理系統及外部單位連結三大模組說明之 (如圖 2 所示)。

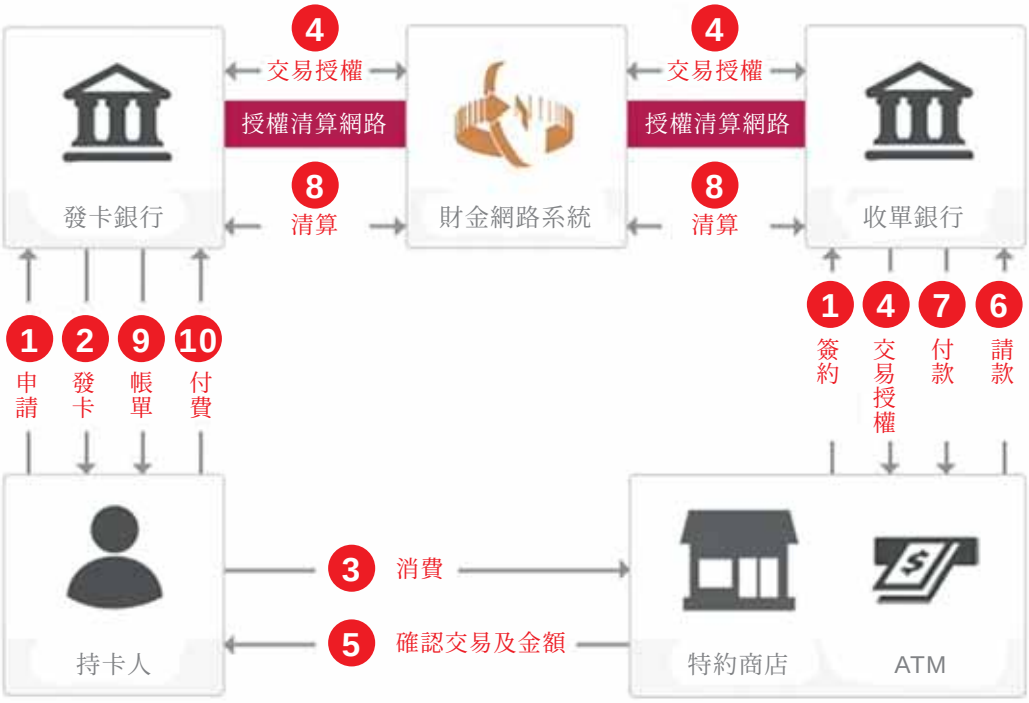


圖 1　卡片交易處理流程圖

圖 2　交易訊息轉接授權流程圖

(一) 收單來源通路

目前財金收單共用平台所支援之收單來源通路大致上可分為實體特約商店、網路商店、信用卡預借現金 / 銀聯卡提款與餘額查詢、人工 / 批次授權作業及繳交規費稅等五大類。

1. 實體特約商店

一般實體特約商店為面對面交易，特約商店於客戶付款時，利用刷卡機將卡片交易訊息連線至收單共用平台，並由該共用平台將訊息繞送至發卡銀行進行授權。

至於連線方式，特約商店可透過一般電信撥接線路或 ADSL 專線與該共用平台連接，除可受理 VISA、MasterCard、JCB 三大國際組織的卡片外，自 96 年起，增加我國的晶片金融卡刷卡消費購物交易，並於 99 年間開始支援中國銀聯磁條卡，嗣於 102 年 4 月間納入銀聯晶片卡，合作金庫銀行成為臺灣首家支援銀聯晶片卡之收單銀行。

此外，該共用平台亦提供收單分期付款、紅利折抵等多樣加值功能，滿足商店之業務需求，在收單共用系統彈性架構支援下，協助收單銀行提供更多元、更安全之收單服務，更增加持卡人的方便性，從而促進特約商店卡片交易之成長。

2. 虛擬網路商店

依連線訊息而言，持卡人在網路商店完成商品訂購並以卡片進行結帳作業時，提供下列兩種方式供網路商店連結：

(1) **共用付款網頁** (URL, Uniform Resource Locator) **模式**

持卡人於網路商店完成購物後點選「結帳」，網頁即轉換連結至財金收單共用系統的付款網頁，持卡人於該網頁輸入卡號等相關資訊後，該等資訊即被繞送至發卡銀行進行授權。

(2) **網路商店專屬付款網頁** (API，Application Programming Interface) **模式**

持卡人點選「結帳」，網頁停留於網路商店的付款網頁，持卡人於該網頁輸入卡號等相關資訊後，網路商店即利用財金公司提供的 ToolKit 加入卡號等相關參數傳送至財金收單共用系統，再繞送至發卡銀行進行授權。

所支援的卡別除既有之 Visa、MasterCard、JCB 外，自 101 年 4 月起亦開始支援銀聯卡，以抓取大陸民眾至我國網路商店交易的商機，擴展及提高網路商店交易量。

3. **信用卡 ATM 預借現金 / 銀聯卡提款與餘額查詢**

若持卡人利用 ATM 以信用卡進行預借現金交易，該交易即由收單銀行傳遞至財金公司的跨行交易處理系統，轉送至轉接系統再繞送至發卡銀行進行授權。另有鑑於大陸民眾來臺人數遽增，自 99 年 6 月起，銀聯卡持卡人可於國內貼有「Union Pay 銀聯」標誌之 ATM，進行取現及餘額查詢交易，相關訊息透過財金轉接系統繞送至大陸銀聯發卡行進行授權，提升商務交流與觀光旅遊之便利性。

4. **人工 / 批次授權作業**

當特約商店之刷卡機無法使用時，店員可撥打客服專線與收單銀行聯繫，由客服人員發動連線訊息交易，以人工作業執行後續授權流程；如刷卡時卡片讀取異常，店員亦可撥打客服專線與發卡行聯繫，以確認該卡片的有效性，為降低會員銀行建置客服中心的成本，財金公司已提供 24H 服務的客服專線，由值班同仁協助會員銀行進行連線作業相關處理機制。

若持卡人進行語音 / 傳真購物，特約商店可將交易分批彙整成檔案，轉送收單銀行進行後續授權作業，收單銀行可透過 Web 介面將檔案上傳財金公司，由收單共用系統將檔案拆分後，逐筆傳送至轉接系統或授權共用系統，進行後續授權處理。

5. **繳交規費稅**

現行持卡人繳費稅之通路十分多元，除可至 e 政府平台 (http://www8.www.gov.tw/school/index.htm) 進行繳費交易外，亦可撥打中華電信數據語音系統 (412-1111) 繳交交通電信監理資費，此類交易均由中華電信公司直接轉接至財金收單共用系統，再透過轉接系統統繞送至發卡行進行授權，簡化收單銀行處理作業。

(二) 連線訊息處理系統

針對連線交易訊息提供多項系統模組進行處理，分述如下：

1. **收單共用系統**

為降低金融機構發展收單業務之建置成本，提供收單共用系統，實體刷卡機、網路商店可直接與該系統連結，進行交易授權處理；收單銀行可設定檢核參數，以確認連線交易的有效性，如特店代碼是否存在、該特店本日交易次數 / 刷卡累積金額是否已達上限等，協助收單銀行進行特店風險管控，避免偽冒交易之產生。在請款作業部分，針對刷卡機 / 網路商店當日結帳交易，自動產出請款檔轉由後端帳務系統進行處理，收單銀行無須自行產製，提高請款處理時效。

2. **轉接系統**

轉接系統係提供發卡行與收單共用系統連結，以便進行授權。已加入財金發卡授權共用系統之發卡行，其交易相關訊息由轉接系統導至該共用系統進行授權作業，而未加入者則由轉接系統透過主機轉送至發卡行為之。本系統也與國際組織 VISA、MasterCard、JCB、銀聯連結，若授權屬跨國交易者，依卡別繞送至各該組織；至於屬聯合信用卡處理中心 (以下稱聯卡中心) 會員銀行之交易，則繞送至聯卡中心處理。

3. **發卡授權共用系統**

發卡授權共用系統 (以下稱授權系統) 可降低發卡銀行的系統建置成本，授權交易經由該系統檢核卡片的有效性及消費額度的控管，提供下述功能：

(1) **連線授權處理**

授權系統負責處理各來源通路所傳送之授權訊息，依客戶、帳戶、卡片額度及狀態進行檢核與處理，檢核項目包含：卡片的有效性、黑名單、緊急替代卡、掛檔紀錄、高風險特店、高風險行業類別 (MCC，Merchant Condition Code)、VIP 客戶等，並提供信用卡語音開卡之服務。

(2) **批次作業處理**

依金融機構上傳之檔案，進行金融機構、客戶、帳戶、卡片等相關資料之異動作業，並產生報表及檔案回傳金融機構，以利維護資料的正確性及消費額度的控管；系統依預設排程進行之定時維護作業，包含：檢查系統狀態、監控服務狀態、產製交易分析報表、資料的備份與過檔及 Housekeeping 作業等，確保系統持續穩定運作。

(3) Web **介面管理**

提供晶片登入元件、異動紀錄查詢、權限控制管理及放行控制管理等安全機制；網站功能尚包含人工授權、客戶資料管理、帳戶資料管理、卡片資料管理、基碼主檔管理、Online 授權信用檢核、授權風險檢核、銀行主檔管理、預設帳戶等級主檔管理、一般卡別主檔管理、悠遊聯名卡主檔管理、緊急卡人檔建置、假日控制檔管理及採購 / 配銷卡管理等，提供客服中心及會員銀行使用 Web 介面以進行作業管理與相關參數設定。

4. **分期平台系統**

為特約商店可接受持卡人進行信用卡分期付款交易，收單銀行可於分期平台系統設定合作之發卡銀行，供其於連線時決定特約商店可否接受分期付款交易，並協助收單銀行於月結時，計算應支付發卡行之每月分期回佣手續費與應收取之發卡交易處理費。此外，收單銀行亦可透過 Web 介面進行建立分期活動資料、交易及帳務查詢、報表匯出等功能。

5. **風險偵測系統**

為降低持卡人卡片被盜用風險，建置風險偵測系統，提供發卡銀行依其經驗法則或參照同業作法設定檢核規則，於交易產生時分析其是否違反檢核規則，違反者將於 Client 端軟體跳出警示訊息，供風管人員判讀，且為得即時通知持卡人該交易相關訊息，本系統也提供發送簡訊的加值服務。

6. **網路商店外掛模組 / 網路 3D Secure 認證系統**

由於網路交易屬非面對面之消費模式，通常只須持有卡號、效期、CVC2 (Card Verification Code 2) 等資訊即可進行交易，風險遠高於一般實體交易，有鑒於此，國際組織針對網路交易導入 3D Secure 認證模式，由持卡人至發卡銀行的 ACS (Access Control Server) 網路認證系統註冊密碼，以作為日後網路交易付款之認證，惟網路商店亦須具備外掛模組 (Merchant Plug-In)，當持卡人進行付款作業時，透過外掛模組將持卡人資訊傳送至國際組織 Directory Server，由 Directory Server 繞送至發卡銀行 ACS 系統，以確認該持卡人是否已註冊認證碼。

依據國際組織規範，當該筆網路交易於日後被判定為偽冒交易時，若網路商店未具備外掛模組，則由收單銀行負擔損失，又，若是發卡銀行未提供 ACS 系統，則由發卡銀行負擔。財金公司已建置網路商店外掛模組及網路 3D 認證系統供會員銀行使用，以降低收單銀行及發卡銀行於網路交易之風險。

(三) 外部單位連結

為協助收單銀行擴增實體特約商店及網路商店支援卡片類型的多樣性，與信用卡國際組織 VISA、MasterCard、JCB、銀聯所建立之連線，針對持用國外卡片於我國進行交易部分，可透過轉接系統先傳送交易訊息至卡片所屬國際組織，再由各國際組織轉送後端發卡行進行授權驗證；至於持用我國卡片且其發卡銀行參加聯卡中心體系者，亦可透過轉接系統傳送至聯卡中心。再者，透過完整的主備援專線建置及 24 小時不間斷的傳輸監控，可確保收單銀行交易訊息可迅速而安全地傳遞至外部單位。

四、批次帳務清算處理

卡片交易完成並成功付款後，屬財金體系之請款作業，即透過跨行清算系統進行後續帳務處理，帳務處理服務包含清算作業、收單銀行之特店管理作業、網站資料查詢及報表產製作業、檔案收送作業等 (如圖 3 所示)。

圖 3　批次清算帳務處理流程圖

(一) 帳務清算系統

財金帳務清算系統 (以下稱清算系統) 主要提供清分 (Clearing) 處理作業、清算 (Settlement) 處理作業、手續費計算作業三項功能。

1. 清分處理作業

清分處理作業主要係來源檔案之處理及目的檔案之產製與交換，清算系統就各通路上傳之交易檔案，首先進行欄位型態正確性檢核，確認資料已符合宣告型態；其次是欄位數值合理性檢核，辨別欄位值是否為定義之數值，如交易代碼、POS 機輸入型態等；最終依業務邏輯將交易資料進行欄位轉換，並就資料所屬類型分別依自行 / 自系交易、跨系交易、跨國交易，產出符合目的通路規格定義之交換檔案，提供各有關單位進行後續帳務處理。

2. 清算處理作業

清算處理作業主要是於營業日進行收單銀行與發卡銀行間應收付帳款之計算，並透過金融機構設立於中央銀行之同業資金帳戶進行款項撥轉。以一般請款交易為例，由發卡銀行將交易金額撥付予收單銀行，反之若為退貨交易，則由收單銀行將交易金額返還予發卡銀行，此外，尚有爭議款交易、費用類交易等，皆可透過財金清算作業一併彙整計算。另外有些會員銀行並未在國外開戶，若有跨國交易產生，可委託其他金融機構透過其帳戶供國際組織進行款項撥轉，當帳務資料由國際組織傳送至財金清算系統時，即透過清算處理作業進行金融機構與其受委託金融機構間之帳務處理，簡化會員銀行帳務處理作業。

3. 手續費計算作業

手續費計算主要分為二項，第 1 項即計算會員銀行間之求償費 (Reimbursement Fee)，若為一般 POS 請款交易，乃收單銀行回饋予發卡銀行之費用，反之，若為 POS 退貨交易，係發卡銀行須返還收單銀行之費用；若為 ATM 預借現金交易，則為發卡銀行回饋予收單銀行之費用。除上述交易外，若遇爭議款交易，則依其交易類型分別處理。第 2 項則為計算會員銀行應給付予財金公司之手續費，依交易類型採取不同之費率。

(二) 特店管理共用系統

為協助收單銀行對其所屬特約商店進行帳務管理，財金公司建置特店管理共用系統，提高金融機構導入收單作業之佈建時效，相關功能說明如下：

1. 特約商店維護及查詢作業

主要提供收單銀行設定特約商店相關資料，包含基本資料、收單銀行對該店之手續費率、特店撥款頻率、發票資料等，若為連鎖商店，亦可設定中央付款指示，以調整對帳單之分開列示。其次，提供查詢介面，藉以查詢特店之歷史交易量彙總資訊，或是以往請款紀錄，協助收單銀行監控特店交易頻率；再者為提供款項撥付之設定，如付款狀態是扣押或解除扣押，可針對問題特店暫停付款。

2. 爭議扣款管理作業

一般作業係由收單銀行向發卡銀行發動請款交易，惟因應發卡銀行發動之沖正交易，勢須再次請款，或收單銀行自行發動更正交易調

整請款金額，該等交易類型可利用爭議扣款管理作業，經由選擇原交易並輸入必要欄位進行帳款相關作業，縮短處理時效。

3. **請款 / 撥款處理作業**

請款處理作業是彙整特店每日每批結帳資料，依其屬性分類產製請款明細；撥款處理作業則依各家特店設定之撥款頻率產製撥款檔，供收單銀行下載並進行後續帳務撥款流程。

4. **檔案產製作業**

檔案產製分成三類，一是特店管理類檔案，包含：特店資料異動檔、端末機資料檔；二是帳務類檔案，包含：撥款明細、電子對帳單明細、請款明細；三是申報資料，包含：提交金融聯合徵信中心之特店資料及請款資料、提交財政部財政資訊中心請款明細及彙總資料及關貿電子發票檔案。

(三) 網站查詢暨報表管理系統

為提供會員銀行快速而方便之交易查詢介面，建置網站查詢暨報表管理系統，供會員銀行進行查詢作業及報表下載。

1. **授權資料查詢**

會員銀行可針對 180 天內的連線授權交易進行狀態查詢，以確認交易之詳細授權資訊。

2. **帳務資料查詢**

會員銀行可針對 180 天內的帳務資料進行各項欄位確認，以及查詢清算帳款、手續費計算結果等。

3. **爭議款交易維護**

針對預借現金或 Debit 卡之爭議款交易，提供 Web 介面協助會員銀行進行沖正、更正、再請款等交易類型。

4. **國際組織偽冒交易申報**

依國際組織規範，若有持卡人反應其卡片遭受偽冒盜刷，發卡銀行須向國際組織申報，以利風險控管，發卡銀行可利用 Web 介面新增申報資料，以簡化作業程序。

5. **報表下載**

會員銀行可下載各項帳務清算報表、手續費收費報表、稅務報表等檔案，也可利用既有介面即時產製報表，並依作業需求匯出 Excel、PDF 等檔案格式。

(四) 檔案傳輸系統

為利與會員銀行進行檔案收送，財金公司建置檔案傳輸系統，採 FTP (File Transfer Protocol) 通訊協定進行雙方檔案交換，並藉由屬性檔內之資料押碼值 (MAC，Message Authentication Code) 以確認檔案正確性及有效性，其中資料押碼基碼 (EFTPOS MAC Key) 乃透過財金公司基碼檔予以交換，至於通訊亂碼基碼 (Cross Domain Key) 則依雙方約定機制進行交換。

為強化檔案傳輸之安全性及作業一致性，計劃於 103 年起，調整系統收送機制，先行改善通訊協定，由現行 FTP 提升為 FTPS，並將現行財金公司與參加單位互為 Client Server，調整為財金公司為 Server，參加單位為 Client 之模式，簡化雙方作業複雜度，降低問題發生

機率。繼之為加入數位簽章及整檔加密機制，由現行使用 MAC 進行檔案完整性驗證，提升為數位簽章加整檔加密，增加不可否認性及隱密性。

五、新興支付應用之發展

卡片支付業務之拓展，首重前述核心系統完整與妥善的規劃與設計，以及前端支付應用貼附市場脈動，此外，支付工具之新發展，服務之多元化與加值化為業務開展目標與重要課題。為因應國內網路交易蓬勃發展，強化買賣雙方交易流程之安全性，降低偽冒詐欺發生機率，導入公正第三者代收付服務之第三方支付已成為網路商店擴展商機及提升交易保障不可或缺的加值服務，也成為各家收單銀行積極提供之收單功能，財金公司已規劃建置透過網路收單共用平台訊息標準，供網路商店進行線上交易訊息傳遞，以協助收單會員銀行及網路商店快速建置其第三方支付作業服務。

現行收單銀行佈建在實體商店之實體刷卡機成本並不低廉，隨著智慧型行動裝置功能越來越強大且成本越來越低廉之情況下，為協助更多微型特店及個人商戶更容易將現金交易轉換為電子交易，近幾年市場上已陸續出現於行動裝置上搭載小型讀卡機 (mPOS)，作為實體刷卡機外之另一解決方式，財金公司規劃開發符合 Visa 及 MasterCard 等國際組織技術規範之相關系統功能，期協助收單會員銀行在業務發展上能有更多元之選擇。

基於智慧型行動裝置日漸普及，以空中製卡 (OTA，Over The Air) 方式將卡片應用程式安裝至行動裝置上，再利用行動裝置內建的無線傳輸技術 (如 NFC，Near Field Communication)，即可使用行動裝置與非接觸式刷卡機感應溝通，並完成後續授權流程，財金公司參照國際組織非接觸式卡片技術規範，規劃開發相關系統功能，且代為處理不同國際組織間訊息轉換及繞送服務，以因應行動支付應用之持續發展。

六、結語

財金公司多年來致力於金流業務系統之開發與拓展，為因應市場需求與瞬息變化，除與國際組織及專業團體建立良好互動合作關係，持續吸收新資訊與引進關鍵技術外，尚於內部組合優良的技術團隊，保有系統自行開發、維護的能力，且透過與時俱進的研發工作，不斷強化提升原有的跨行系統與卡片業務共用平台，期能協助金融機構降低系統建置與維運成本。展望 103 年，為協助我國金融產業拓展安全便捷之行動支付服務，健全金融支付系統之運作，財金公司計劃透過 PSP TSM (Payment Service Provider Trusted Service Manager) 平台，藉由 OTA 技術整合手機與金流，實現手機信用卡、手機儲值卡、手機購物之便利性支付新應用，進而推動無紙化社會，也冀以更多的加值服務，提升金融機構拓展業務之整體競爭力。

※ 參考文獻 / 資料來源：

1. 財金公司網站－信用卡業務說明 (http://www.fisc.com.tw/TC/Default.aspx)。
2. 財金公司 6.11 銷售點服務系統檔案規格。
3. 金融監督管理委員會銀行局－信用卡業務統計。
4. 數位時代雜誌，2013 年 10 月號。

淺談晶片金融卡消費扣款的安全機制

本篇摘自 2007 年 03 月出刊之財金資訊季刊第 50 期，由時任財金資訊公司研發部晶片卡組蘇偉慶高級工程師（現任為研發部經理）撰寫。

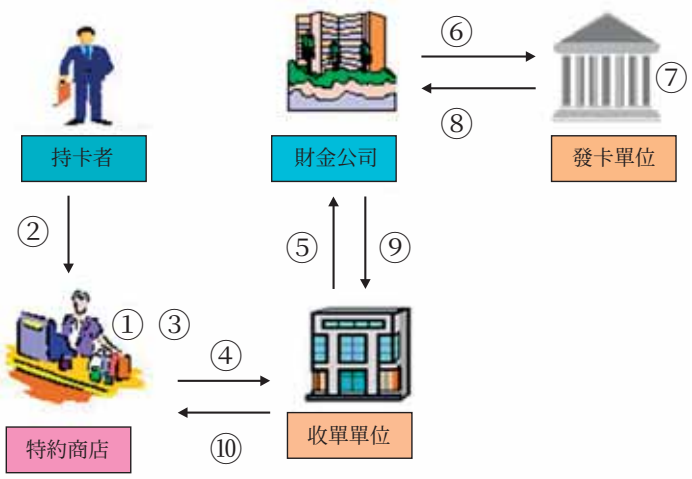
前言

一個新的支付工具，不論就銀行或消費者而言，安全絕對是其首要之考量且關心的議題。晶片金融卡消費扣款作業，其訊息之安全設計，依然承襲現行自動櫃員機提款與轉帳之高安全機制。然而交易訊息的安全設計僅是作業安全的一個環節，本文除將討論交易流程的安全機制外，更從卡片的安全、使用環境 (設備) 的安全等面向，進一步探討晶片金融卡消費扣款安全機制，最後再與 EMV 線上授權作業一同比較，使大家更了解其在安全設計上，與國際規格的對應關係。

交易流程安全機制

消費扣款的安全機制與持卡者在銀行的自動櫃員機發動相關交易是一致的，所有交易乃由持卡者確認、同意 (輸入正確的密碼) 後才可啟動，交易的合法性是由發卡單位驗證後才可放行。其為點對點的安全設計，可確保交易訊息的來源辨識性及正確性。以下將就消費扣款作業中之購貨與退費作業之訊息與安全設計予以詳細說明。

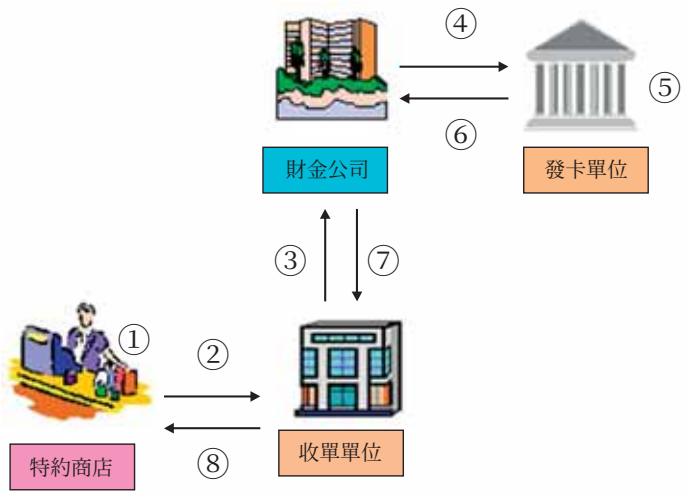
一、消費扣款購貨交易流程訊息作業與安全機制說明



	訊息作業說明	安全機制
1	端末設備出現消費金額，並要求插入晶片金融卡。	
2	持卡者插入卡片，並被要求輸入密碼。	• 卡片身分認證，可確保合法持卡者方可啟動卡片，以作進一步使用。 • 卡片密碼鎖住設計，可防止攻擊者以暴力法猜測密碼，進而使用卡片。
3	端末設備組成交易核心訊息（包含交易金額、交易日期時間、端末機查核碼、持卡者帳號、特約商店代號 … 等）送入卡片，卡片將根據此輸入資訊與卡片內自動遞增的 IC 卡交易序號產生交易驗證碼（Transaction Authentication Code，簡稱 TAC）。	• TAC 可確保交易訊息的正確性與來源辨識性。 • IC 卡交易序號可確保交易的唯一性，防止重送攻擊（Replay Attack）。
4	特約商店傳送交易訊息至收單單位。資料傳送前，可視狀況需要與否，利用如端末設備安全模組 (Terminal Security Access Module，簡稱 TSAM) 對部分或全部交易訊息做押碼（MAC）處理，或對敏感訊息做加密處理。	• 交易訊息押碼可確保特約商店至收單單位間訊息的來源辨識與正確性。（建議為 Mandatory） • 敏感訊息加密可確保特約商店至收單單位間訊息傳輸之隱密性。（Optional） • TAC 仍可確保此段資料傳輸過程中，交易核心訊息的正確性與來源辨識性。（但收單單位不驗證）
5	收單單位組成消費扣款訊息，傳送至跨行系統（財金公司）。	• 訊息押碼可確保收單單位至財金公司間訊息的來源辨識與正確性。 • TAC 仍可確保此段資料傳輸過程中，交易核心訊息的正確性與來源辨識性。（但財金仍不驗證）
6	財金公司轉送消費扣款訊息至發卡單位。	• 訊息押碼可確保財金公司至發卡單位間訊息的來源辨識與正確性。 • TAC 可確保此段資料傳輸過程中，交易核心訊息的正確性與來源辨識性。
7	發卡單位處理消費扣款訊息，確定正確無誤後，發卡單位依交易金額扣持卡者之帳戶。	• 訊息押碼可確保財金公司至發卡單位間訊息的來源辨識與正確性。 • 發卡單位將驗証 TAC，確保交易核心訊息的來源辨識與正確性（交易資料確實來自其合法的持卡者，且未被非法竄改）。 • IC 卡交易序號可確保交易的唯一性，防止重送攻擊（Replay Attack）。
8	發卡單位回覆同意扣款之訊息至財金公司。	訊息押碼確保發卡單位至財金公司間訊息的來源辨識與正確性。
9	財金公司回覆同意扣款之訊息至收單單位，收單單位依交易金額入特約商店帳戶。	訊息押碼確保財金公司至收單單位間訊息的來源辨識與正確性。
10	收單單位回覆完成扣款之訊息至特約商店或端末設備。	訊息押碼確保收單單位至特約商店或端末設備間訊息的來源辨識與正確性。（建議為 Mandatory）

註：本交易訊息之設計為 3-Way（Request、Response 及 Confirm），以上忽略 Confirm 部份的說明。

二、 消費扣款退費交易流程訊息作業與安全機制說明



	訊息作業說明	安全機制
1	端末設備組成交易訊息 (包含：退費金額、交易日期時間、特約商店代號及持卡人帳號 … 等) 。	
2	特約商店 (端末設備) 傳送交易訊息至收單單位。資料傳送前，應利用如 TSAM 對重要或全部交易訊息做押碼 (MAC) 處理，或對敏感訊息做加密處理。	• 交易訊息押碼可確保特約商店至收單單位間訊息的來源辨識與正確性。 (建議為 Mandatory) • 敏感訊息加密可確保特約商店至收單單位間訊息傳輸之隱密性。 (Optional)
3	收單單位驗證特約商店傳送之退費訊息正確無誤後，組成退費訊息，傳送至跨行系統 (財金公司) 。	訊息押碼可確保收單單位至財金公司間訊息的來源辨識與正確性。
4	財金公司轉送退費訊息至發卡單位。	訊息押碼可確保財金公司至發卡單位間訊息的來源辨識與正確性。
5	發卡單位處理退費訊息，依訊息中之交易金額與持卡人帳戶入帳。	訊息押碼可確保財金公司至發卡單位間訊息的來源辨識與正確性。
6	發卡單位回覆完成退費處理之訊息至財金公司。	訊息押碼確保發卡單位至財金公司間訊息的來源辨識與正確性。
7	財金公司回覆完成退費處理之訊息至收單單位，收單單位依交易金額自特約商店的帳戶扣除。	訊息押碼確保財金公司至收單單位間訊息的來源辨識與正確性。
8	收單單位回覆完成退費之訊息至特約商店或端末設備。	訊息押碼確保收單單位至特約商店或端末設備間訊息的來源辨識與正確性。 (建議為 Mandatory)

註：本交易訊息之設計為 3-Way(Request、Response 及 Confirm)，以上忽略 Confirm 部份的說明。

持卡者晶片卡的安全

持卡者的晶片卡是整個作業的安全核心，銀行公會有鑑於確保晶片金融卡安全問題之急迫性，乃採兩階段性進行。

第一階段已於 2005/09/02 公告「晶片金融卡安全評估作業之銀行安全準則」相關辦法，除了針對晶片卡制訂「晶片金融卡產品安全需求」(Security requirements of BAROC for financial chip card approval and implementation)，也對產品認證的程序制定「晶片金融卡產品安全評估作業程序」(Requirements and procedure for security evaluation of chip card products for the Taiwanese payment system)，最後因安全認證的專業性，也制定了「晶片金融卡產品安全評估實驗室資格核定」(Accreditation of security evaluation laboratories to the BAROC approval scheme)，期望由專業且有經驗的實驗室，為晶片金融卡的安全把關。銀行公會在公告此辦法後，所有新開發的晶片卡產品，都必須先通過合格實驗室的安全認證後，方可進一步取得銀行公會的認證。另外，對於之前已通過的晶片卡產品，也可以再送至合格實驗室做安全功能補認的作業，只要通過認證，銀行公會將於原認證上加註已通過安全認證註記。此階段作業的目的，便是希望所有銀行都可確保其取得晶片卡的安全性 (不管是現有或新採購的卡片)。

第二階段乃是遵循目前國際上最熱門的資訊產品安全認證標準 (Common Criteria for Information Technology Security Evaluation, 也就是 ISO/IEC 15408) 做相關產品的認證。首先，乃由銀行公會主導制定晶片金融卡的保護剖繪 (Protection Profile，簡稱 PP)，所謂的 PP 可視為日後晶片卡實作的安全依據，它將可確保不同的實作廠商，在同一個安全功能需求與保證需求下開發其晶片卡。晶片金融卡的 PP(BAROC Smart Card Protection Profile，Version 1.2)，已於 2005 年 11 月完成制定，並於 2006 年 1 月通過德國國家資訊安全局 (Bundesamt fur Sicherheit in der Informationstechnik，簡稱 BSI) 的驗證 (證書編號 BSI-PP-0021-2006)。該 PP 除了採用一般公認金融應用必須符合的高安全保證等級 EAL 4 外，其在安全方面更要求達到 EAL 7(最高保證等級) 之需求。但由於 CC 的進入門檻較高，且國內驗證的環境也尚未成熟，因此目前仍未要求依 CC 標準做產品的認證。

端末設備安全模組

TSAM 在消費扣款交易中，是扮演建立特約商店 (端末設備) 與收單單位安全通道的重要元件，所謂的安全通道乃就是在確保商店 (端末設備) 與收單單位間資料傳輸之來源辨識性、正確性與隱密性。

尤其在退費與沖正交易中，資金是由收單單位中特約商店的帳戶撥轉至持卡者的帳戶，因此收單單位確認相關訊息是由合法的特約商店所發動 (來源辨識性)，且交易資料未經非法竄改 (正確性)，便顯得十分的重要。

為方便收單單位取得安全且價位合理的 TSAM，銀行公會乃於 95 年成立了「晶片卡安全模組工作小組」，目標在開發通過 EAL 4+ 認證之 TSAM。該工作小組目前正積極進行產品的開發中，預計於 96 年完成產品開發並通過認證。

使用環境的安全

訊息規範即使再嚴謹，倘若使用環境不安全，則一切都免談。以晶片卡消費扣款的應用而言，環境可能是實體的刷卡機，也可能是虛擬的網際網路。

簽你所見 (Sign What You See，簡稱 SWYS) 一直是資訊安全的最高指導原則，雖然其立意相當明確且合理，但在實際的運用上又談何容易。簽署執行前，你必須先確認所見資料的正確性，以晶片卡這樣值得信賴的元件而言，它卻先天缺乏與持卡者直接互動的能力，因此你只能往上求助。首先，可以想到的當然便是與卡片直接溝通的讀卡機，如果讀卡機的韌體可將與卡片的溝通訊息直接顯示，再透過讀卡機上的按鍵由使用者輸入相關資料或決定執行，它將可在最接近卡片的地方呈現最值得信賴的訊息。但為了讓訊息更具可讀性，而不只是單純顯示難以理解的原始輸入 (APDU) 訊息，因此讀卡機韌體必須對應用層的資訊做某種程度的解釋。其次，則是由讀卡機的應用程式來處理，應用程式處理的好處當然是彈性大且操作順暢，但是其缺點便是信賴的範圍將延伸至應用程式。

因此，為了確保使用環境的安全，收單單位或特約商店必須採購通過安全認證的讀卡機。而持卡者呢？則需選擇信賴的環境 (如：信賴的特約商店或網站) 使用其卡片，如此一來 SWYS 的目標才真的可達成。

與 EMV 之比較說明

晶片金融卡的三個主要安全設計：持卡者密碼、TAC 與 IC 卡交易序號，恰好可與 EMV 的 Offline PIN、ARQC 與 ATC 相對應，其相關之比較與說明如下表所示：

	晶片金融卡	EMV	說明
1	持卡者密碼	Offline PIN	持卡者認證。國內信用卡交易目前仍以手寫簽名為主，但英國則以密碼驗證為其使用之趨勢。
2	TAC	ARQC	線上授權時，用來驗證卡片與交易的合法性。同樣採用 Triple DES 。
3	IC 卡交易序號	ATC	線上授權時，用來確保交易的唯一性，防止重送攻擊。

換句話說，晶片金融卡的消費扣款作業與 EMV 的線上授權作業，若就安全機制面來看，其實是相似的。

另外， EMV 尚有離線資料認證、端末設備風險管理、卡片風險管理等安全作業，皆須由發卡單位與收單單位在持卡者卡片與端末設備上設定相關的參數，配合目前卡片的相關資料或交易特性而定。簡單的說， EMV 的精神是將發卡單位部分的風險控管作業移至卡片，而將收單單位部分風險控管作業移至端末設備，在離線作業是交易作業選項模式的前提下，這樣的設計絕對是必須且合理的。

然而國內的金融網路相當進步、安全且穩定，在此優勢的網路環境下，線上交易或許是更安全且易管理的作業模式，因為在線上作業的模式下，所有的狀況都可在發卡單位做最即時的反應。另外，雖然目前 EMV 採用 PKI 來解決離線認證互通性的問題，但就像是「憑證中止」在 PKI 作業處理所遭遇的問題一樣，EMV 也將遭遇到黑名單處理的問題 (資料量過大的下載與傳送問題或者是即時性的問題)。反觀，線上授權作業因採集中控管，當然便無此問題。

結語

整個晶片卡作業的安全設計，不單只是專注於訊息或卡片功能規格的制定，更期望透過持卡者卡片、端末設備的認證及端末設備安全模組的開發等作業，來強化整個晶片卡作業環境的安全。

晶片卡已經是目前公認較安全且可信賴的支付工具，而在金融卡晶片化作業完成後，晶片金融卡更是目前國內最普及的金融用 IC 卡。利用目前最普遍且安全的支付工具，搭配既有安全且穩定的金融網路，來實現消費付款，或許對銀行或一般消費者而言，都是一個聰明的抉擇。

晶片金融卡 CC 3.1 Protection Profile

本篇摘自 2008 年 03 月出刊之財金資訊季刊第 54 期，由時任財金資訊公司安控部資訊安全組林弘斌高級工程師（現任為研發部代理經理）撰寫。

晶片金融卡 CC 2.2 PP（Protection Profile）在 2006 年 1 月 18 日由德國國家資訊安全局依據 Common Criteria (CC) 2.2 驗證通過 (Certificate BSI-PP-0021-2006)，迄今將近兩年。期間 CC 歷經 CC 3.0 起草改版與試行，在 2006 年 9 月正式公告 CC 3.1 為新版標準，並計畫自 2009 年起全面採用。

作者就 CC 2.x 版與 3.1 版之差異及晶片金融卡 CC 3.1 PP 修訂等兩個主題，依個人見解撰文與讀者分享，倘有疏漏或識見粗淺之處，尚祈指教。

CC 2.x 版與 3.1 版之差異

CC 3.1 改版幅度最大的部分在 Part 3 之安全保證需求，而 Part 2 之安全功能需求大致上維持不變；不論是 CC 2.x 或 CC 3.1，對於資安產品的安全保證需求的驗證邏輯永遠不變。關於 Part 1、Part 2 與 Part 3 的差異，以及 CC 安全保證驗證邏輯，將以 4 個小節分述之。

CC 安全保證驗證邏輯

1. 產品安全是開發者（提供者）的責任，開發者必須描述產品的安全功能，並保證產品的安全性。使用者對於開發者的安全保證多半信心不足，且雙方對於專業術語的認知常有出入，使用者為增加使用信心，要求開發者將產品送給 CC 專業單位進行驗證。
2. CC 國際組織（由各國國家級單位組成）為求產品的安全功能描述能有一致的標準，於是將安全功能需求（SFR、Security Functional Requirements） 予以標準化及單位化（理論上可以測量），並將這些 SFR 以“類別（class）/ 家族（family）/ 元件（component）/ 元素（element）”方式分門別類，編寫成 CC Part 2。
3. 產品的安全功能必須被保證（開發者自行保證及專業第三單位的保證），安全保證能否被相信，必須檢視並論證相關的安全保證措施被確實執行（透過文件審查、獨立測試、滲透測試、實地查核），這

些措施包括產品的生命週期管理、開發設計方式、產品測試、開發環境安全及弱點分析，這些安全保證措施即 CC 的安全保證需求（SAR、Security Assurance Requirements）。CC 國際組織將必要的 SAR 予以標準化及單位化（同樣地，在理論上可以測量），並將 SAR 以類似 CC Part 2 的方式分門別類，編寫成 CC Part 3，並演繹出 7 組 SAR 套件讓安全保證得有等級之分（即 EAL 1 到 EAL 7）。

4. 開發者必須依據 CC Part 2 來描述產品的安全功能，並依據 CC Part 3 的規範提出安全保證措施被執行的證據。CC 驗證單位審查開發者提供的證據（包括開發設計文件、測試文件、管理文件、分析文件），對產品進行實驗室獨立測試及滲透測試，並到開發環境進行實地查核。當所有的證據都證明產品的安全保證達到宣稱的安全等級時，CC 驗證單位才據以發給證書。
5. 使用者可以由 CC 驗證單位的證書，對開發者宣稱的安全保證有認定的標準，進而增加使用信心。

CC Part 1: Introduction and General Model

CC Part 1 的內容在於介紹整個 CC 驗證體系的架構、闡述安全保證評估驗證的意涵、劃分 CC 的適用範圍、定義專有名詞及規定保護剖繪（PP、Protection Profile）與安全標的（ST、Security Target）等文件之規格，其中 PP 與 ST 在 CC Part 3 中有對應的 SAR 類別（APE 與 ASE），用以驗證該文件的合理性、一致性與完整性。

CC 3.1 Part 1 重新檢視所有專有名詞，並給予較明確與一致的定義。除此之外，PP 與 ST 文件規格亦有修訂，其差異對照如下表所示。

就 PP 與 ST 文件規格而言，CC 2.x 與 CC 3.1 這兩個版本間的主要差異如下：

1. CC 3.1 新增 Conformance Claims 章節，內容包括 CC 依循宣告、PP 依循宣告及 SAR 套件依循宣告。在 CC 2.x 時，這些依循宣告散佈在 PP/ST 的第一章與第五章，CC 3.1 將之統整在第二章。
2. 在 CC 2.x 時，安全目標（SO、Security Objective）的理由論述與 SFR/SAR 的理由論述被編排在同一章節（第八章、Rationale）中，PP/ST 不容易閱讀。CC 3.1 將 SO 及 SO Rationale 一併編排在第四章，提高 PP/ST 的可讀性。
3. CC 3.1 新增 Extended Components Definition 章節，內容包括使用者自定的 SFR/SAR 元件。在 CC 2.x 時，使用者自定元件與標準元件描述在同一章節（第五章、IT Security Requirements），導致 PP/ST 不容易閱讀（同第 2 點）。CC 3.1 將使用者自定元件獨立編排在第五章，且先於第六章的 Security Requirements，提高了 PP/ST 的可讀性。
4. 在 CC 3.1 的 PP/ST 中，沒有安全功能強度宣告（SOF Claim）。事實上，在 CC 3.1 中，SOF 已經被拆解並重新編排於 Part 3 AVA_VAN 家族（弱點分析）的各個 SAR 元件中，所以已經不需要特別強調 SOF 這個概念。

表格 1　CC 2.x 與 CC 3.1 PP/ST 差異對照表

CC 2.3	CC 3.1
1. PP Introduction A. PP Identification B. PP Overview	1. PP Introduction A. PP Reference
2. TOE Description	TOE Overview
As defined in section 5; modified and retitled as "Conformance Claims"	2. Conformance Claims A. CC Conformance Claims B. PP Claim C. Package Claim
3. TOE Security Environment A. Assumptions B. Threats C. OSPs	3. Security Problem Definition A. Threats B. OSPs C. Assumptions
4. Security Objectives A. SOs for the TOE	4. Security Objectives A. SOs for the TOE
B. SOs for the Environment	B. SOs for the Operational Environment
(7A below)	C. Security Objectives Rationale
(5A1 & 5A2 below: the explicit reqs)	5. Extended Components Definition
5. IT Security Requirements A. TOE Security Requirements 1. TOE SFRs [Part 2 & explicit reqs] [including SOF claim]	6.Security Requirements A. SFRs for the TOE (no SOF claim)
2. TOE SARs [Part 3 & explicit reqs]	B. SARs for the TOE
(7B below)	C. Security Requirements Rationale
B. Security Requirements for IT Environment	(requirements for environment are now optional)
6. PP Application Notes	(no separate Application Notes section; these can be put into PP Introduction)
7. Rationale A. Security Objectives Rationale B. Security Requirements Rationale	

CC Part 2: Security Functional Requirements (SFR)

CC 3.1 版 Part 2 之 SFR 與 CC 2.x 版 Part 2 大致上相同，仍維持 11 個 SFR 類別，包括：

- FAU: Security Audit
- FCO: Communication
- FCS: Cryptographic Support
- FDP: User Data Protection
- FIA: Identification and Authentication
- FMT: Security Management
- FPR: Privacy
- FPT: Protection of the TSF
- FRU: Resource Utilization
- FTA: TOE Access
- FTP: Trusted Path/Channels

就 Part 2 而言，CC 2.x 與 CC 3.1 這兩個版本間的差異為 CC 3.1 移除了 CC 2.x Part 2 中 的 FPT_RVM（Reference Mediation）與 FPT_SEP（Domain Separation）等兩個 SFR 家族（SFR 家族的數目減少為 65 個），個人認為移除的原因如下：

1. FPT_RVM 與 FPT_SEP 的用意在於規範開發者必須提供『產品本身的安全功能無法被規避』及『產品本身的安全功能不被破壞』這兩個安全功能，以確保產品本身的安全功能無法被規避與不被破壞。很明顯地，這兩個 SFR 有邏輯上的缺陷。
2. 『產品本身的安全功能無法被規避』與『產品本身的安全功能不破壞』實際上是安全功能的屬性（properties），應該藉由檢視產品開發者的開發設計方式與程式原始碼是否提供足夠的安全保證證據，證明其產品的安全功能具備這些屬性，才比較合乎邏輯。
3. 有鑑於此，CC 3.1 將上述 SFR 移除，並以CC Part 3的SAR家族ADV_ARC取代。

CC Part 3: Security Assurance Requirements (SAR)

回顧 CC 安全保證驗證邏輯乙節第 3 點，CC 提供 7 組 SAR 套件將安全保證等級分成 7 級（EAL 1 到 EAL 7），其對應的安全保證措施如表格 2 與表格 3 所示。

CC 2.x 從 7 個不同的需求面向（即 7 個 SAR 類別），制定 SAR 標準：

1. **組態管理**
（ACM、Configuration Management）

組態管理某種程度上相當於變更管理，控管產品本身及組態資訊的變更流程。良好的組態管理可用以確保產品本身及組態資訊的完整性，預防未經授權的變更，故對於『送驗的產品及文件』與『實際交予使用者的產品及文件』之間的一致性，可提供保證。

2. **交貨與運作**
（ADO、Delivery and Operation）

ADO 針對產品交貨、安裝及使用所需的措施、程序及依循標準，訂定 SAR 給產品開發者參考實施，以確保產品本身的安全防護功能不因遞送、安裝與啟用等過程而有任何的折損（compromise）。

ADO 之下包括 ADO_IGS（Generation、Installation、Startup） 與 ADO_DEL（Delivery）等兩個 SAR 家族，ADO_IGS 保證產品將以安全的方式被產製、安裝及啟用。因為產品類型與特性不一之故，產品的產製、

表格 2　安全保證需求分級套件

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration Management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and Operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance Documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life Cycle Support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability Assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

安裝或啟用程序可能發生在使用者端，也可能發生在開發者端。以晶片卡為例，絕大部分的開發者會先完成產製、安裝及啟用等程序後，再將產品交予使用者；以軟体系統為例，產製、安裝及啟用等程序則會在使用者端執行。

ADO_DEL 保證產品以安全的方式交付，開發者必須有一套交付程序，並依據程序執行交付作業；交付程序通常包括使用者需要配合的執行事項，而且“實作上（practically）”使用者必須知道這些配合事項。

3. **開發設計**（ADV、Development）

ADV 之下共有 7 個 SAR 家族，包括：

- ADV_FSP：Functional Specification，要求開發者提供功能介面規格，並規範該規格應包含的內容。
- ADV_HLD：High Level Design，要求開發者以“子系統”的角度撰寫產品安全功能的高階設計規格，並規範該規格應包含的內容。

表格 3　CC 3.1 安全保證需求分級套件

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life Cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	2	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability Assessment	AVA_VAN	1	2	2	3	4	5	5

- ADV_LLD：Low Level Design，要求開發者以“模組”的角度撰寫產品安全功能的低階設計規格，並規範該規格應包含的內容。
- ADV_IMP：Implementation Representation，要求開發者以“某種表示法”描繪產品的實作，並規範應被描繪的內容。就軟體產品而言，指的是程式原始碼；就晶片硬體而言，指的則是電路圖。
- ADV_RCR：Representation Correspondence，要求開發者論證（安全功能與功能介面）、（功能介面與子系統）、（子系統與模組）及（模組與實作描繪）兩兩之間的對應關係。
- ADV_SPM：Security Policy Model，要求開發者撰寫產品安全政策模型，並論證 ST 中的所有安全政策都包含在安全政策模型中，開發者同時必須論證產品功能介面與安全政策模型之間的對應關係。
- ADV_INT：TSF Internals，要求開發者以“分層（layered）”的方式描繪產品的內部設計結構。

就開發設計而言，安全保證牽涉到證明下列兩項重要的安全功能屬性：

- 安全功能必須正確地運作。
- 安全功能不能被破壞或規避。

CC2.x 藉由 ADV_FSP、ADV_HLD、ADV_LLD、ADV_IMP、ADV_RCR 及 ADV_SPM 來證明第一項屬性，至於第二項屬性（相當於沒有後門程式），由 CC 3.1 Part 3 新增的 ADV_ARC 處理，此為 CC 2.x 與 CC 3.1 的差異。

4. **指引文件**（AGD、Guidance Documents）

指引文件包括管理者手冊與使用者手冊，指引文件對於產品能否安全的運作，扮演重要的角色。

AGD 要求開發者保證其指引文件的可理解性、涵蓋度與完整性。對使用者而言，指引文件所需的安全保證，簡言之即“照著指引文件做，就不會出錯”這句話，故開發者除依據 AGD 的指引文件撰寫規範提供指引文件外，還必須依據 AVA_MSU（Misuse Analysis）對指引文件進行誤用分析。

5. **生命週期支援**
（ALC、Life Cycle Support）

CC 認為開發與維護的管控不足，會導致有瑕疵的實作，進而造成產品有安全疑慮。因此，CC 要求在開發生命週期的早期階段，建立一套開發維護模型 (ALC_LCD 、Life Cycle Definition)；此模型涵蓋開發與維護所需的安全性支援，包括瑕疵修正程序與政策（ALC_FLR、Flaw Remediation）、使用的工具及採用的技術 (ALC_TAT、Tools and Techniques) 及開發環境實體安全措施 (ALC_DVS、Development Security)。

事實上，整個產品生命週期內所需的安全性支援，個人認為還包括了組態（變更）管理與交貨控管，CC 3.1 也對 ALC 做了修改，將於後續內容說明之。

6. **測試**（ATE、Tests）

產品測試是為了保證產品的安全功能與 ST 所描述的一致。除了撰寫並執行測試個案外，ATE 還要求開發者必須對測試個案的廣度（依據產品功能介面規格）與深度（依據產品設計規格與程式原始碼）進行論述分析，以保證產品的安全功能與設計細節如預期般地運作。

7、 **弱點評估**
（AVA、Vulnerability Assessment）

AVA 之下共有 4 個 SAR 家族，包括：

- AVA_CCA：Covert Channel Analysis，要求開發者就產品內部與外界的傳輸介面（以晶片為例，例如電位、電流、電磁），分析是否有可被利用的隱匿通道。隱匿通道未必是開發者刻意留下的，大多數是因為設計不良（例如亂碼運算時有明顯的電位高低變化）導致的。
- AVA_MSU：Misuse Analysis，要求開發者就其管理者手冊與使用者手冊進行誤用分析，確保管理者及使用者可以即時地判斷產品的設定或運作是否有安全疑慮。
- AVA_SOF：Strength of Function Analysis，要求開發者就產品安全功能中與“機率”或“排列組合”有關的機制（例如個人密碼、Hash），進行安全功能強度分析。
- AVA_VLA：Vulnerability Analysis，要求開發者就“identified vulnerabilities”，分析這些可能發生的弱點在其產品中是否可以被利用，而違反（violate）產品安全政策（TSP、TOE Security Policy）。以密碼驗證為例，攻擊者可直接由產品功能介面（非隱匿通道）的設計弱點，利用密碼比對的時間差及斷電手法，逐字猜出個人密碼。

依據定義，TSP 乃產品 SFR 背後代表的規則，用以規範產品如何管理及保護其資訊資產。當有隱匿通道疑慮時， ST 中就會有相關的 SFR；當有 SOF 疑慮時， ST 中同樣也會有相關的 SFR。也就是說，隱匿通道與 SOF 理論上同屬於 " identified vulnerabilities "，AVA_CCA 與 AVA_SOF 理論上也應只是 Vulnerability Analysis 的一部分。

比較表格 2 與表格 3，CC 3.1 Part 3 與 CC 2.x Part 3 最明顯的差異為 CC 3.1 Part 3 少了 ACM 與 ADO 兩個 SAR 類別，這並不是說 ACM 與 ADO 的內容在 CC 3.1 中被刪除不用，而是被拆解並重新編排於 ALC 與 AGD 這兩個 SAR 類別中（如圖 1）。除此之外，ADV、AGD 及 AVA 等 SAR 類別也有相當程度的修訂，茲說明如下：

1. **拆解 ACM**

拆解 ACM 的原因，個人認為是因為 ALC 的範圍定義與實際規範內容不一致。CC 2.x 之 ALC 的定義，乃針對產品開發過程的所有階段所需的安全性支援，採用定義良好的（well-defined）生命週期模型，然而該類別之下只涵蓋瑕疵修正程序與政策、工具與技術及開發環境實體安全措施等支援性 SAR 家族。

事實上，產品開發過程所需的安全性支援還包括組態（變更）管理，也就是說，ACM 的內容理論上應歸類在 ALC 之下。因此，CC 3.1 將 ACM_SCP（CM Scope）的內容搬移到新增的 ALC_CMS（CM Scope）中，並將 ACM_CAP（CM Capabilities）與 ACM_AUT（CM Automation）的內容合併到新增的 ALC_CMC（CM Capabilities）中。

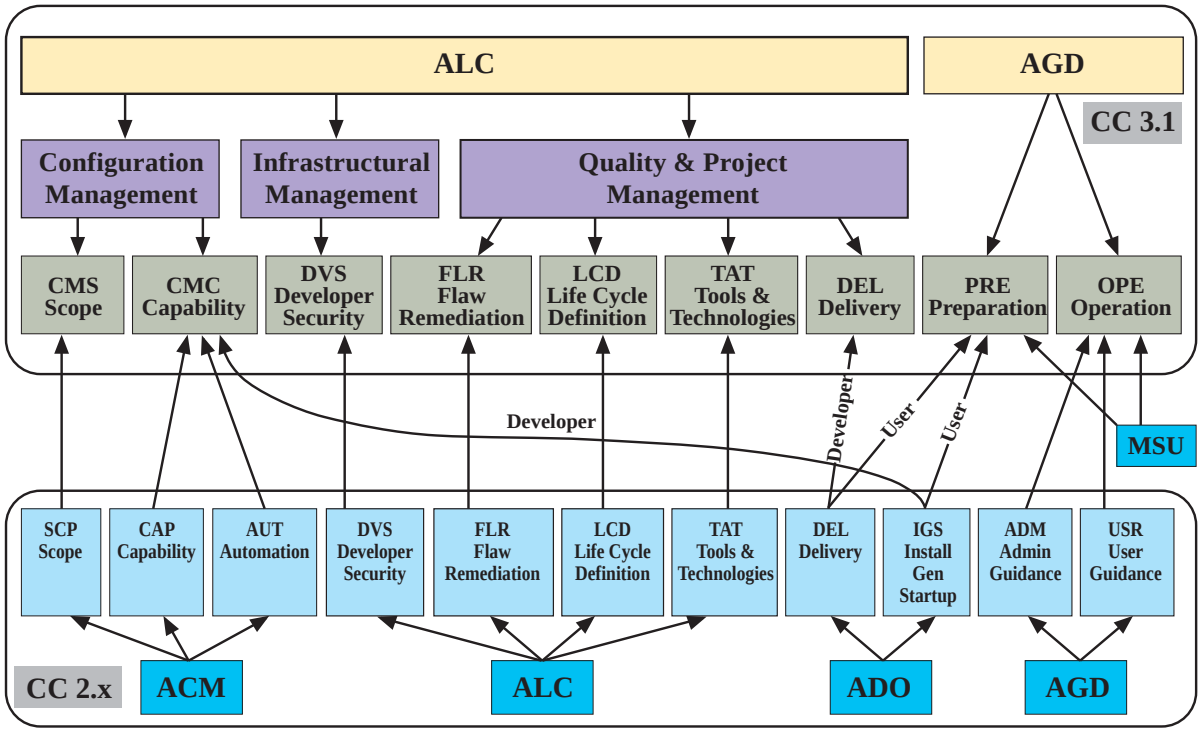


圖 1　ACM/ALC/ADO/AGD CC 2.x 與 CC 3.1 差異

CC 3.1 Part 3 已經沒有 ACM 類別。

2. **拆解** ADO

CC 2.x 的 ADO 之下，包括 ADO_IGS 與 ADO_DEL 兩個 SAR 家族。

由於產品的類型各式各樣，產製、安裝及啟用程序可能發生在開發者端，也可能發生在使用者端，造成 ADO_IGS 的規範必須同時套用於開發者與使用者。但是，開發者端執行的產製、安裝及啟用程序屬於組態管理，使用者端的程序則屬於使用者的準備事項。因此，CC 3.1 將 ADO_IGS 的內容加到 ALC_CMC 內，規範開發者的產品產製、安裝及啟用程序 (註 1)，同時也將該內容加到 CC 3.1 新增的 AGD_PRE（Preparative Procedures） 內，做為使用者準備程序的一部分。

至於 ADO_DEL，為了保證產品遞交的安全性，實作上使用者必須知道開發者的交付程序並予以配合。因此，CC 3.1 將 CC 2.x 的 ADO_DEL 內容拆解成兩部分，包括開發者的交付程序及使用者的準備程序，並將前者歸類到新增的 ALC_DEL，而將後者搬到新增的 AGD_PRE。

CC 3.1 Part 3 中已經沒有 ADO 類別。

(註 1) 產製、安裝與啟用原就屬變更管理的一環。

3. **重整** AGD

CC 3.1 認為，產品在交付後使用者會歷經“ 準備階段 ”與“ 運作階段 ”。在準備階段，使用者必須依據開發者的準備程序文件，執行交付配合程序（例如交付驗證），以確保產品在遞送過程中沒有折損任何安全功能；同時，使用者必須依據開發者的指示執行產製、安裝及啟用等程序，以確保產品可以如預期般地運作。這些屬於準備階段的程序需求，原規範在 CC 2.x 的 ADO 內，在 CC 3.1 已統一編排於新增的 AGD_PRE。

運作階段包括產品的管理與使用，分屬於 CC 2.x 的 AGD_ADM 與 AGD_USR，CC 3.1 將其內容合併到新增的 AGD_OPE（Operational User Guidance）。

值得注意的是，除管理者手冊與使用者手冊外，準備程序文件也是 CC 3.1 驗證單位依據 AVA_VAN 進行誤用分析時的對象。

CC 3.1 Part 3 中已經沒有 AGD_ADM 與 AGD_USR 這兩個 SAR 家族。

4. **合併** ADV_HLD **與** ADV_LLD

對開發者而言，CC 2.x 的 ADV_HLD 與 ADV_LLD 規範的“ 高階 ”設計規格與“ 低階 ”設計規格是相當令人垢病的專有名詞；在新式的開發流程觀念裡，設計規格就是設計規格，沒有所謂“ 高階 ”與“ 低階 ”之分。

然而，CC 2.x 的原意是要求開發者以類似“ 子系統 ”的概念將產品的設計結構分解成較小的區塊，以便於論證產品在設計面滿足其宣稱的安全功能。同樣地，ADV_LLD 的目的是，開發者以類似“ 模組 ”的概念將子系統再分解成更小的區塊，以便於論證產品的設計在運作上確實達到其宣稱的安全功能。

為了避免再造成類似的誤解，CC 3.1 將 ADV_HLD 及 ADV_LLD 的內容合併到新增的 ADV_TDS（TOE Design Specification）中，需注意的是，上述分解的概念（子系統、模組）仍予以保留，只是少了 ”高階 ”與 ”低階 ”這兩個讓大家困擾的專有名詞。

CC 3.1 Part 3 中已經沒有 ADV_HLD 與 ADV_LLD 這兩個 SAR 家族。

5. **新增** ADV_ARC

CC 2.x Part 3 的 ADV 只處理了『安全功能必須正確地運作』這項安全保證，但遺漏了『安全功能不能被破壞或規避』，這項等同於“程式沒有後門”，對使用者相當重要的安全保證，CC 3.1 Part 3 新增的 ADV_ARC（Security Architecture）適時地彌補了 CC 2.x Part 3 的不足。ADV_ARC 要求開發者提供產品安全架構描述文件，內容包括：

- 標示產品安全功能納管的所有的安全領域（Security Domain）。
- 證明產品安全功能的初始化過程是安全的。
- 論證產品安全功能可以保護自身不被破壞。
- 論證外在環境無法規避產品安全功能，直接更動安全領域中的資訊資產。

6. **重整** AVA

如圖 2 所示，CC 3.1 Part 3 將 AVA_CCA、AVA_SOF 及 AVA_VLA 重新拆解並合併到新增的 AVA_VAN（Vulnerability Analysis）家族中；事實上 CC 3.1 Part 3 的 AVA 類別之下只有 AVA_VAN。

除此之外，CC 3.1 版 AVA_VAN 最大的變革是其中已經沒有對開發者的要求事項，也就是說原來在 CC 2.x 版 AVA_CCA、AVA_MSU、AVA_SOF 與 AVA_VLA 之中要求開發者執行的分析工作，在 CC 3.1 版已全部改由要求實驗室執行。

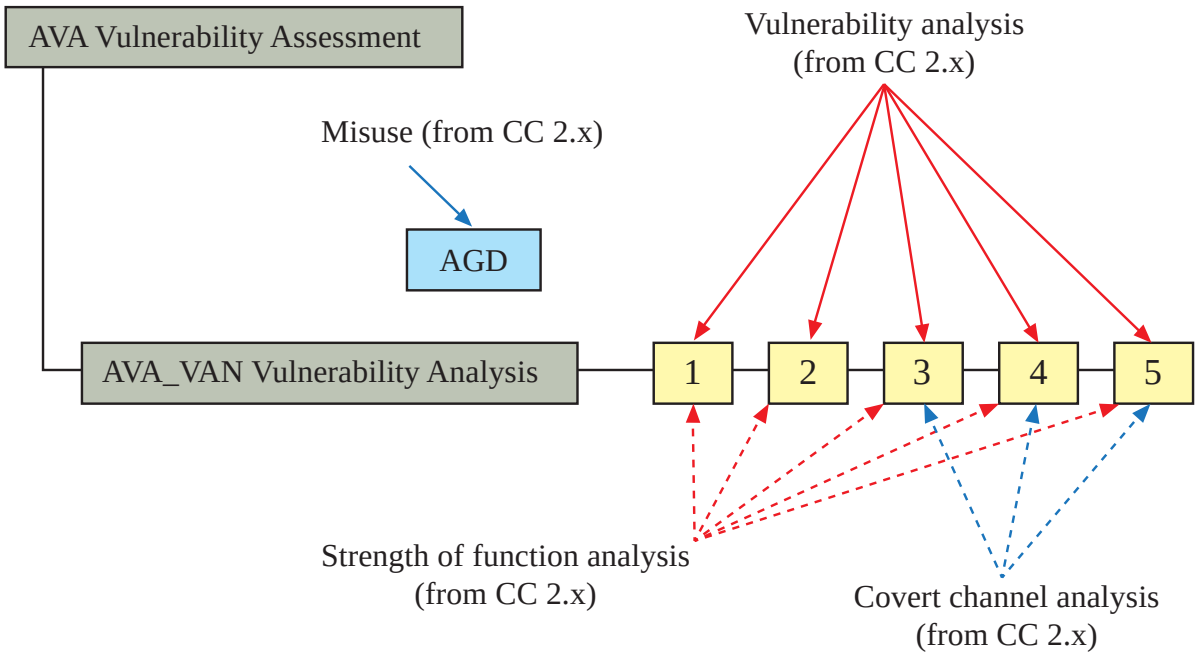


圖 2　CC 3.1 AVA 與 CC 2.x 比較圖

晶片金融卡 CC 3.1 PP 修定

關於晶片金融卡 CC 3.1 PP 之修定，除了將晶片金融卡 CC 2.2 PP（Certification ID BSI-PP-0021）的內容依新版規定加以修定外，更重要的是處理了後門程式與 Plain Text PIN Entry 議題。

後門程式

關於廠商開發的晶片金融卡，發卡銀行除了需要 CC 驗證單位檢測其安全功能外，更需要廠商及 CC 驗證單位保證該晶片金融卡沒有後門（木馬）程式（Backdoor、又稱為 Trojan）；然而，確保晶片程式中沒有藏匿後門程式是一項很難達到的 SAR，CC 2.x 版也沒有對應的 SAR 給廠商及 CC 驗證單位遵循。CC 3.1 版在新增的 ADV_ARC 家族中規範了所有與後門程式有關的 SAR，可以確保送驗的產品沒有後門程式。晶片金融卡 CC 3.1PP 的安全保證等級為 EAL 4+（此分級套件包括 ADV_ARC.1，參照表格 3），解決了晶片金融卡的後門程式議題。

Plain Text PIN Entry

首先，TOE（Target of Evaluation，例如晶片金融卡）因其中的資訊資產而面臨威脅。為了抵擋威脅，TOE 確實作了必要的安全措施，以降低威脅引發的風險。所有的安全措施都有弱點（Vulnerabilities），CC 驗證單位保證這些安全措施不存在可利用的（Exploitable）弱點，不會對資訊資產造成額外的風險。

其次，TOE 的發行組織可以制定其專屬的 OSP（Organizational Security Policy），CC 驗證單位確認這些 OSP 確實有對應的安全措施，但不檢測這些安全措施是否存在可利用的弱點。

晶片金融卡採用 PIN-based Authentication 機制認證持卡人，認證過的持卡人可以發送指令給晶片金融卡，使用內存的 TAC Key 在晶片內部產製 TAC。站在 CC 的觀點，PIN-based Authentication 機制包括 PIN 輸入、PIN 比對及 PIN 儲存，如果威脅討論的對象是 PIN-based Authentication，則因為最高等級弱點防護能力 AVA_VAN.5 的要求，PIN 輸入必須使用加密通道。

但是，晶片金融卡設計之初因管理作業成本及多通路應用考量，收單設備的安全機制與晶片金融卡的安全機制是各自獨立的，收單設備與晶片金融卡之間的 PIN 傳輸不使用加密通道。很明顯地，PIN-based Authentication 不能是威脅討論的對象，唯一可能的方式是將它列為 OSP。

如果只是將 PIN-based Authentication 列為 OSP，而沒有其它配套措施，無法保證晶片金融卡保護 PIN 的安全措施不存在可利用的弱點，尤其是廣為人知的實體攻擊（Physical Attack）及時間差攻擊（Timing Attack）。為此，晶片金融卡 CC 3.1 PP 將晶片內存的 PIN 列為受保護的資訊資產，要求 CC 驗證單位保證晶片的硬體安全措施不存在可被利用的弱點；並將 PIN 比對列為威脅討論的對象，要求 CC 驗證單位保證晶片金融卡的 PIN 比對功能不存在可被利用的弱點，例如比對時間差與斷電手法。

綜上所述，依據晶片金融卡 CC 3.1 PP 開發驗證過的晶片金融卡產品，除了 PIN 傳輸不使用加密通道外，其餘有關保護 PIN 的安全措施，皆符合最高等級弱點防護能力 AVA_VAN.5 的要求。

結論

關於 CC 3.1 版的 AVA_VAN 安全保證需求家族，所有與弱點分析有關的專業工作已不再由產品開發者提出執行證據，改由 CC 實驗室（檢測評估單位）處理。此舉不但符合 CC 使用者對 CC 實驗室專業能力的期待，同時也降低 CC 驗證的進入門檻（包括成本與專業技術），當然產品開發者仍需具備開發安全產品的能力。由此一變革可以預期，配合各國政府的推動，將會有愈來愈多的產品開發者願意藉由 CC 驗證來提高其產品的競爭力。

關於 CC 證書的跨國互通性，CC 3.1 版已經自 EAL4 提高到 EAL4+；也就是說，未來不論是由甲國或乙國驗證後發出的 EAL4+（AVA_VAN.5 augmented）證書，“ 理論上 ” 其弱點分析所達到的安全保證等級是一樣的。個人認為，即使各國的安全技術能力一定有某種程度上的差異，銀行公會應該不會規定晶片金融卡開發廠商只能自特定 CC 驗證國家取得證書。銀行公會如能積極培養自身的安全檢測與攻擊防禦等技術能力，應可覆審 CC 安全檢測報告，進而將 CC 3.1 驗證的跨國互通性轉化為提昇晶片金融卡安全保證的助力。

關於 Plain Text PIN Entry 議題，專案小組曾建議 PIN 與 Key 應可套用不同的安全保護等級，亦即 PIN-based Authentication 仍列為威脅討論的對象，但採用次一級之弱點防護能力需求（AVA_VAN.4），其餘安全措施則採用最高等級之弱點防護能力需求（AVA_VAN.5）。這種做法勢必直接衝擊 CC 現行“ 一張證書一個安全保護等級 ” 的架構，此一議題已經列入第 8 屆國際共同準則年會（ICCC 2007）議程，將由德國 TUViT 公司顧問以『Challenging the concept of one evaluation assurance level per evaluation』為題案進行討論，希望 CC 國際組織能從善如流，採納此建議，調整下一版標準之內容架構。果真如此，不僅晶片金融卡 PP 在 CC 3.1 新版標準驗證拔得頭籌，此建議也可算是專案另一項全球第一。

感應式技術之金融應用與安全防護

本篇摘自 2015 年 01 月出刊之財金資訊季刊第 81 期，由財金資訊公司安控部資訊安全組黃建隆副組長撰寫。

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。

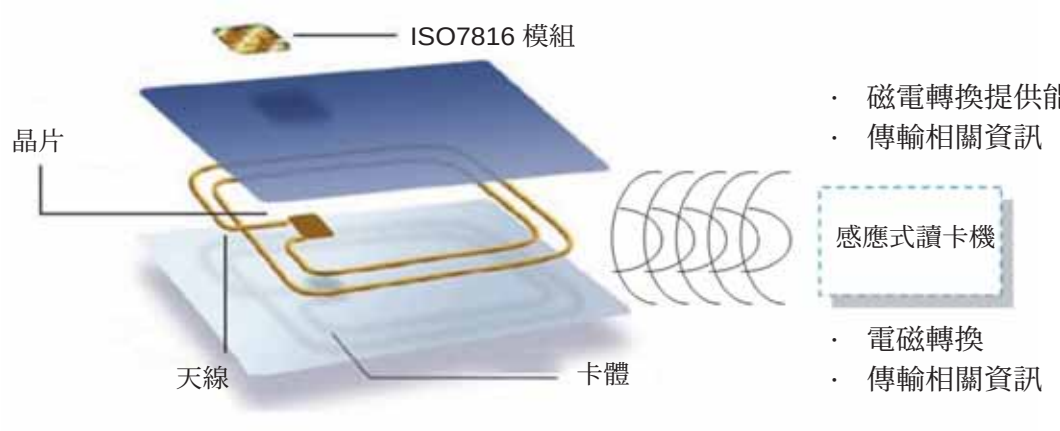


圖 1　感應式卡片運作示意圖
(資料來源：Calypso Handbook)

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，開啟後，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，僅於交易時再行開啟。
3. 錢包的設計邏輯，卡片須於交易時才被啟用，且若超過交易時限 (例如：60 秒) ，則自動關閉該卡片，卡片應非一直處於啟用狀態。
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。

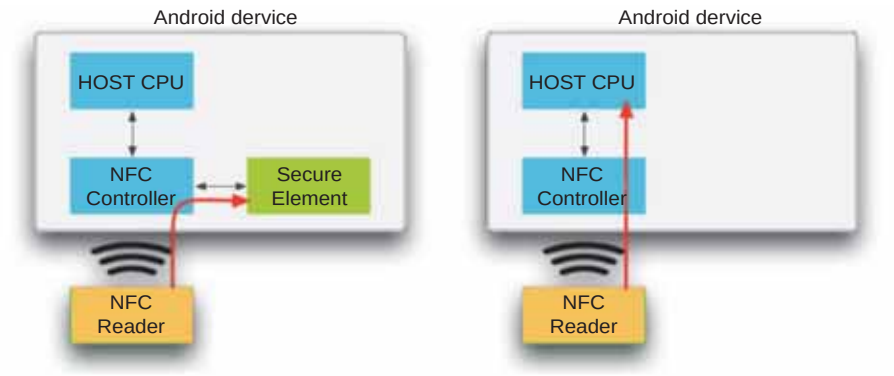


圖 2　HCE 運作示意圖
(資料來源：Google)

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。

新一代「雲端資料中心服務與管理」

本篇摘自 2013 年 10 月出刊之財金資訊季刊第 76 期，由時任財金資訊公司系統部系統組鄧介銘組長（現任系統部代理經理）撰寫。

一、前言

企業的資料中心之運作架構，源自於應用處理之解決方案，最初運用的批次處理推動大型主機的應用，嗣後網際網路應用則催生了主從應用程式，時至今日，該等應用仍然並存；加以，傳統的 IT 架構缺乏靈活調整的特性，當部署新的應用時，即以專用軟體獨立運作於專屬的硬體元件之方式構建，往往耗費較長的週期與不斐的成本，同時亦須投入大量人力與時間以維持運作，資料中心更因此成為業務應用系統零散的環境，也儼然成了系統的大雜燴。伺服器虛擬化雖為簡化前述先天複雜又欠缺靈活性的基礎架構邁出第一步，然仍有極多資料中心的營運，大幅受制於專用軟體與專屬硬體之間的依存關係。

當進入雲端時代後，新式之應用已經逐漸向網際網路應用、社交網路及移動設備靠攏，業務需要依靠 IT 驅動以為創新，進而加速超越競爭者；而 IT 所面臨的嚴峻挑戰，即是在更緊縮的預算限制下，以更為敏捷的速度滿足前述業務之需求，並須同時保持效能、治理與安全性服務層級的品質，這也促使企業積極尋求構建資料中心的新方法。

現今巨量資料、社交化及行動商務等創新應用正席捲整個 IT 產業，企業既有的營運模式和應用遭受前所未有之巨大衝擊，迫使傳統資料中心的老舊思維必須思圖改變，才能滿足企業前端商業的需求，同時須使 IT 單位成為企業策略的執行單位，才可快速因應市場的布局與變化，以及迎合新產品或新服務的推出時機。

二、虛擬化的下一步

舊有資料中心的建置模式，使用者須先選定硬體平台、資料庫、中介軟體及管理軟體，再選取適用之應用系統建構方案後，實施佈置；然而在新式「軟體定義的資料中心」建置模型下，使用者首先考慮的是應用，諸如：哪些應用模式類同、哪些屬核心應用，又有哪些是次級應用，然後根據這些應用配合搭建硬體平台。因此，軟體定義的資料中心也可解釋為應用定義的資料中心，亦即先行確定應用，嗣透過軟體設定實現硬體資源之調配。

軟體定義的資料中心將是 IT 演變的下一個階段，也是迄今較為有效的基礎架構方法，它並非透過重新編寫複雜之字集，以避開專屬硬體這類既有的不靈活特性，而是繞過這些束

縛，轉而改變資料中心所有服務之交付方式，藉由對儲存、網路連接、安全設定與可用性設定等資源處理集中化、抽象化和自動化，聚合所提供之服務，並結合策略原則、自動化資源調配和監控功能為使用。

軟體定義的資料中心係將資料中心所有的硬體資源予以虛擬化及軟體化；而其虛擬化進程乃啟自伺服器虛擬化，大多數 IT 人都非常瞭解虛擬機器的好處，但是網路與儲存是實體性偏強的資源，虛擬機器雖具有靈活性，惟尚未完全展現其成效於硬體外之其他資源。

綜觀企業發展的趨勢，IT 已然成為一項驅動業務成果的重要助力，可協助企業拓展賴以存續的收益流，不僅得以新的商機快速累積資本，並可打破市場局面及重新建立競爭性的佈局。以往，IT 組織往往受限於系統管理的脆弱、封閉式之基礎架構及過時之操作方法，資源與預算大都用於維持現狀，且辛勤工作卻僅足以支援現有的系統，即使馬不停蹄，亦難消化因新需求迭增致大量積壓的工作，一旦陷入這種反應式惡性循環模式，就完全無法致力於研發使業務成長並提供創新營運方法的系統與服務，如此，IT 單位與業務單位之間的關係勢將日益緊繃，而隨著不斷延誤營運服務的上線時程，企業亦喪失競爭力。

話雖如此，新式可臨時機動調配的 IT 傳遞方法，在本質上亦隱含風險，例如：在安全性、法規遵循與公司治理方面，企業常有多種不明確的標準，IT 若缺乏健全的運作與管理機制，以其主導安全性措施，則敏感性資料便有易於外流之虞；若以倉促的行動驅動創新，則將導致日後技術孤立的情況，而分散以不同方式來執行和管理各式基礎架構的多個管理區，將會限制 IT 運用共通環境以驅動自動化的能力；又若 IT 缺乏跨越環境的可移植性，將會限制其移轉工作負載之能力，從而降低企業達成最佳管理成本、風險管控及服務品質的能力。綜上，若仍採用原有資料中心作業方式，IT 組織將持續被動回應，竭盡資源也僅能支援現有的系統，毫無餘力遞送重要的新業務服務，所以建構軟體定義的資料中心就是用以打破這種不良循環的最佳途徑。

「軟體定義」某種程度來說就是將所有資源虛擬化，過去十多年間，伺服器虛擬化已開闢一條輝煌之路，此外，儲存虛擬化、網路虛擬化、桌面虛擬化等技術發展亦日益成熟，虛擬機器已由支持研發測試平台或簡單應用走向全面成熟階段，現今企業關鍵業務的應用也可以很穩定地運行在虛擬化平台上，據國際研究暨顧問機構 Gartner 調查，全球近 60% 的應用負載實現了虛擬化，虛擬化已然成為下一代資料中心的核心。藉由虛擬化實現資源管控之自動化，正是雲端運算的基礎，也是軟體定義的資料中心的靈魂所在。

三、「軟體定義的資料中心」之技術架構

傳統的資料中心只是一系列伺服器、儲存、網路、安全等技術個體的鬆散集合，在對作業環境分配資源時，需要直接且清楚描述應用系統對於基礎設施技術的一系列要求，事實上每一個作業環境是中央處理器、作業系統、儲存資源池、網路、安全及管理系統在縱向上的連結集合體。以傳統資料中心而言，通常需要數週的時間以完整地部署一個新的作業環境；然而在大多數虛擬世界裡，情況則較單純、簡化，但雖可在幾小時內即建妥並交付一個新的應用環境，卻還有許多後續工作必須進行，主要原因為建立一個新的虛擬機器雖簡單，但

複雜的部分在於須配套建立支援新應用系統所需的所有周邊基礎設施服務，其中包括儲存、網路、安全服務等，同時尚須考量其可用性與商業可持續性的要求。

透過一個完全動態且以軟體驅動的資料中心，即可簡化前述配套作業，使其如同配置及部署一個新的虛擬機器般簡單，而且幾乎是完全自動的。亦即針對新的應用需求，只須擬定以自動化方式供應相關基礎設施服務，並將該等服務收納在一個容器，即一個虛擬的資料中心 (如圖 1 所示) 內，以實現新應用需求的整體策略，就可以在幾分鐘、甚至幾秒鐘內，依需求部署完成一個新的作業環境。

圖 1　虛擬資料中心

軟體定義的資料中心，其主要特點包括：

(一) 標準化

將各個資源池之間的硬體基礎設備標準化，以消除不必要的複雜性。

(二) 整體化

提供統一的平台，以利整個資料中心架構進行優化，進而能夠靈活地支持各種工作負載需求。

(三) 最適化

提供使用者可自行彈性調整的基礎架構，依據不斷變化的應用需求，動態及重新配置環境，以得到最大的性能、靈活性和效率。

(四) 自動化

提供一個內建的自動化管理架構，減少複雜的管理規則及人為的介入，以達到顯著的管理成本節約。

(五) 彈性化

由於進化成以軟體為基礎架構，使得硬體故障不再影響業務運行，以最低的成本提供業務創新。

藉由軟體定義的資料中心的概念 (如圖 2 所示)，可建構新世代企業資料中心最佳的服務業務架構，此架構係立基於企業的服務水平協議 (或稱服務層級協議，Service-level Agreement，簡稱 SLA) 及遵守 IT 政策的關鍵理念，使應用程式得以定義自己的資源需求，

如：運算、網路、儲存、軟體等。為確保其可擴展性、靈活性及敏捷性，且最終目標能達成顯著降低整體維運之成本，必須著重於依據業務邏輯的要求以為定義，而非依技術要求進行配置，定義完成之業務邏輯元素，即編譯展開成一組應用程式之間的介面指令，供虛擬化之維運管理軟體據以進行相關資源之配置、移動、管理及相關的資源回收服務。總而言之，軟體定義的資料中心顛覆傳統以基礎設施為主的資料中心，其目的在於提供一個以應用程式或業務服務為重點的作業環境，專注於運算、網路、儲存元件等資源之妥適配置，確保業務服務可以正常運行。這種轉變使得以往扮演被動角色的服務提供者，轉身成為主動變革的推動者，督促及培育 IT 人員具備承擔未來工作負荷的能力。軟體定義的資料中心純粹以應用程式的工作負載需求，使企業用戶能以最有效和最符合服務水準協議的方式，部署和執行其所需之應用程式。

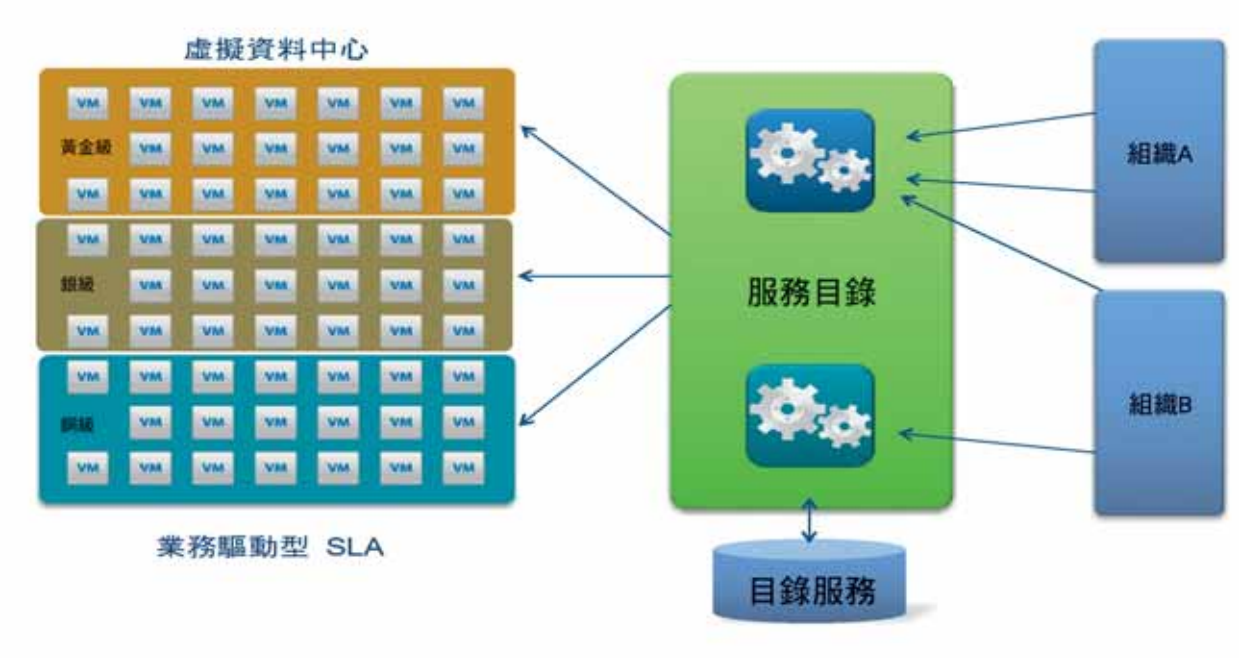


圖 2　軟體定義的資料中心的概念

軟體定義的資料中心是基於未來的需求進行定義，從實際的數據中心，根據定義所需的自動化和流程編排，僅僅需要調整自動化和業務流程工具，使每一個新的應用程式可依照工作量、服務水平協議或公司政策，確保達成業務用戶所要求之可靠性、性能和安全性等服務指標的應用程式環境。為確保可擴展性、彈性及成本效益，所有的自動化與管理任務，自儲存、網路乃至運算組件，都必須有效滿足應用程式對於性能、容量和生命週期管理的要求。軟體定義的資料中心可解決目前普遍存在於 IT 人員和業務研發人員之間的對立衝突，前者負責建置足夠容量的資源池，並以軟體定義形式規範，而後者負責設立業務規則，使軟體定義的資料中心在服務水平協議規範的方式下，完全承擔符合需求之工作負載。也就是說，所需

的應用環境都是立基於服務水平協議、政策及成本效益的綜合考量下，所得到的最佳化自動配置和工作負載。

四、「軟體定義的資料中心」之核心組件

(一) 伺服器虛擬化

伺服器虛擬化是組成軟體定義的資料中心三個核心組件 (如圖 3 所示) 中，發展最成熟的組件，現今也已刻劃出一套完整的發展趨勢，伺服器虛擬化採用單一窗口管理企業虛擬基礎設施之策略，大約可使企業在 IT 管理上，縮短資料中心之建置時間達 50%-70%，並可有效監控虛擬機與實體主機的效能。所以，伺服器虛擬化可應用至營運環境中各種不同的應用程式，將其建構為自動化虛擬基礎設施，以發揮最大之效能。因此，妥為配置伺服器虛擬化之虛擬機，並善加管理其生命週期及應用性能，則可發揮實體基礎設施所無法比擬的高效能性、延展性和可用性，企業組織可運用虛擬機即時移轉應用功能，避免計劃性停機，並利用自動負載平衡功能，依原則動態分配 IT 資源，可減少許多重覆設定與維護工作之負荷。雖然，企業實施伺服器虛擬化具有諸多好處，但是，嗣後伺服器虛擬化所面臨的資源回收，將成為伺服器虛擬化的一大挑戰，所以，必須於日常作業中適時進行系統運作之健康狀況、風險評估、效率等分析工作，以避免造成 IT 資源之浪費與耗損。

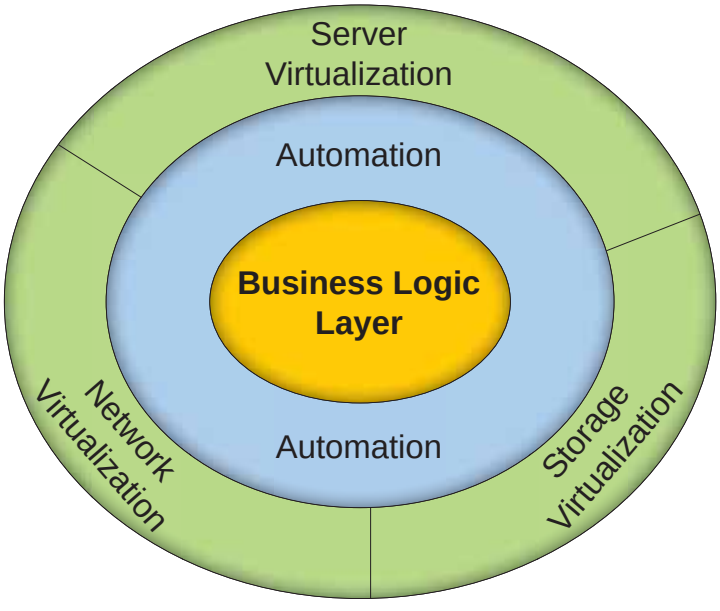


圖 3　軟體定義的資料中心核心組件

(二) 網路虛擬化

隨著雲端計算、巨量資料等眾多創新技術與應用的空前發展，以及智慧終端機的爆炸式增長，網路已成為企業與一般用戶無法瞬離的重要資源。然為支撐起規模龐大的應用，資料中心與資料中心之間及資料中心內部的網路，正逐漸成為制約虛擬化整體發展的瓶頸，時下在網路傳輸技術短期內仍難有快速成長的情況下，如何提高現有網路的利用效率，就成為目前資料中心首應解決的難題。

網路建置是配置新應用程式環境的主要工作，一般而言，在單純的 IT 環境下，通常僅需幾分鐘即可完成配置，然而如擬提供數量龐大的虛擬機使用，即須深入研析所需的網路資源，例如：是否需要使用半手動方式等，且須經由多個管理界面進行創建和配置，如此複雜的配置過程，不僅需要先進的網路技術，也由於人工介入之作業過多，容易導致配置不及或錯誤，也可能導致風險、安全等問題。軟體定義的網路 (如圖 4 所示) 允許用戶簡單地指定哪些伺服器必須連接、與其相關的服務水平協議是什麼，之後，利用軟體計算以最有效的方式滿足這些要求，排除典型的人工密集且複雜的配置過程，進而提升網路配置的時效，且減少人工配置錯誤的發生，提升應用程式服務的品質。

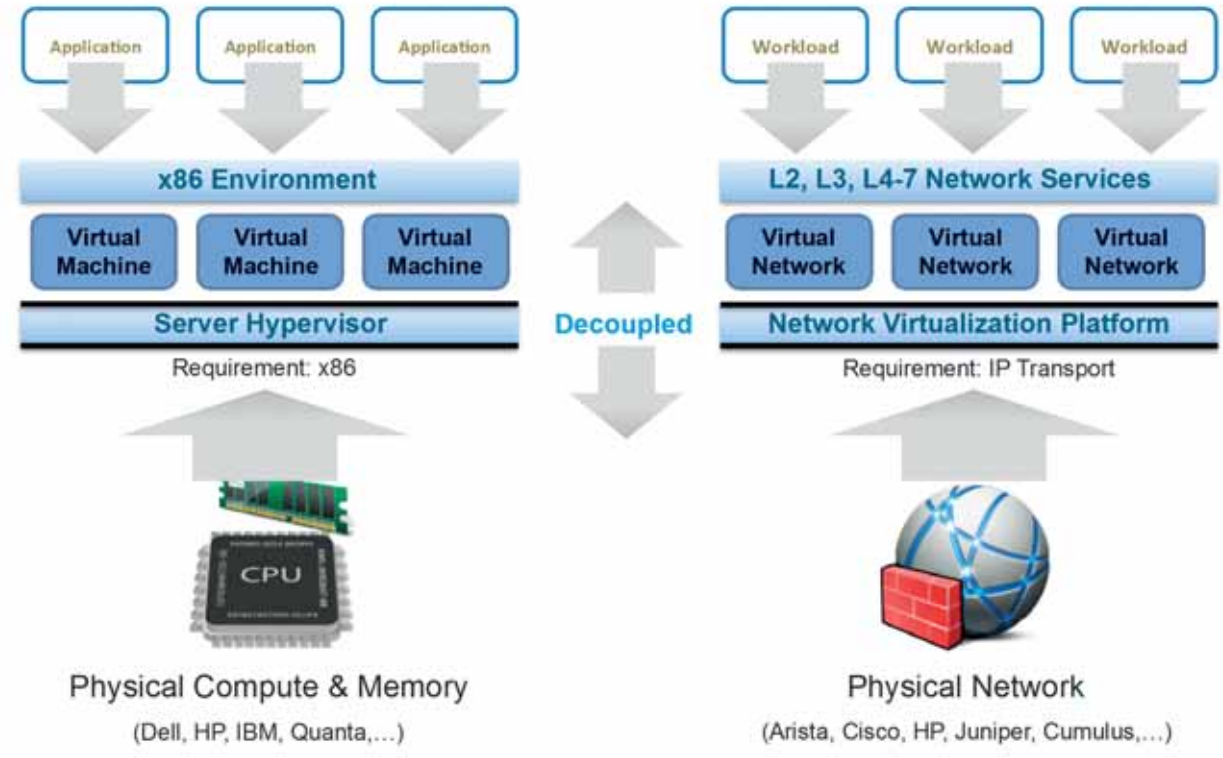


圖 4　軟體定義的網路

(三) 儲存虛擬化

軟體定義的儲存平台架構 (如圖 5 所示) 包括了兩層，即：「控制層」與「資料層」，在控制層建立虛擬陣列資源池之後，資料層再進一步提供資料服務目錄。

以軟體定義的儲存與傳統的儲存虛擬化截然不同，如擬實現自動配置功能以達成自動分配儲存資源，就得妥善管理 I/O；目前的儲存虛擬化作法，是同時結合自動配置與 I/O 管理予以虛擬化，但以軟體定義的儲存平台則將兩者分離，建構成一個可程式化的儲存資源分配平台，以避免遭遇儲存效能的問題，例如：峰時影響 I/O 效能。

在以軟體定義的儲存架構中，資料層負責儲存空間的自動配置，而硬體磁碟陣列則負責管理儲存效能、I/O 管理及例外管理等。透過前述的分離方式，不僅可保留原有不同磁碟陣列的特性，不必犧牲儲存陣列產品原有的功能，如：資料重複刪除或資料壓縮功能，且又能提供簡化的單一管理介面，以處理不同磁碟陣列的管理，如：設定維護等。

「控制層」可提供自動配置、自助服務、報表機制、自動化管理等功能，管理企業內部各種儲存陣列產品，包括不同廠商的磁碟陣列或儲存系統。至於「資料層」，除提供傳統的檔案和區塊層級的儲存服務外，尚可處理雲端儲存所新興的物件儲存，以及平行處理架構平台底層之檔案架構的分散式物件檔案系統服務，並提供抽象的儲存基礎架構，所有資料都來自虛擬陣列池，既可如同使用檔案那般存取資料，也可以物件形式存取相同的資料。

軟體定義之儲存平台可同時使用控制層與資料層兩者或透過預設策略控制的自動化功能，僅使用控制平面管理儲存陣列底層的智慧功能。有異於以往的儲存虛擬化，軟體定義之儲存平台完全建置在軟體上，可搭配不同廠商的磁碟陣列共同運作，不僅可如檢視檔案一般觀看物件的內容，檔案存取的速度亦極快，不致發生物件儲存延遲的問題。

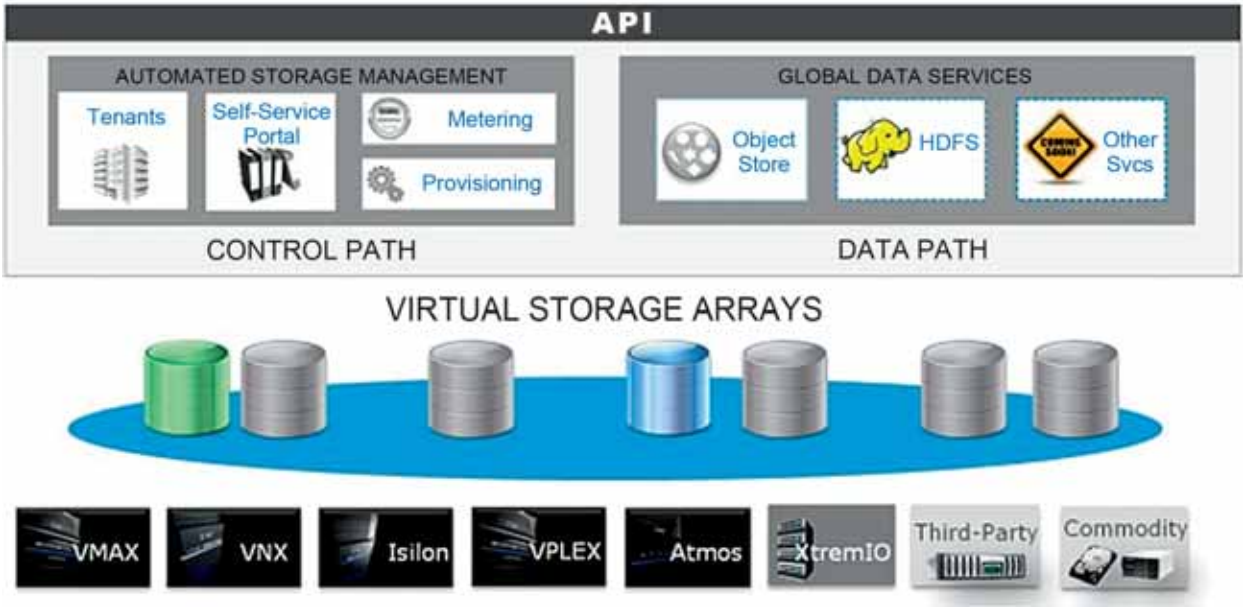


圖 5　以軟體定義的儲存

控制平台可大幅改善自動化的效率，乃因其虛擬化底層的儲存基礎架構，並抽離資源供應或轉移，因此，不同的儲存陣列可使用完全相同的方式管理，正如管理同一集中區內的資源一樣。目前管理高度複雜的功能時，只要使用單一點選的方式即可，就如同手持萬用遙控器即可操控電視、光碟機、串流影音裝置及數位錄影機等設備，在面對眾多異質化儲存陣列的情形下，不必再煩惱繁雜費力的流程，省去逐項選取及操作眾多管理介面的困擾。

儲存集中區一旦建立，各個應用立即予以劃分使用。為達此任務，控制平台提供自助式介面，供應用程式瀏覽儲存服務目錄，以便覓得最適合自己需求的供應服務資源；對於大多數傳統儲存基礎架構，控制平台能找出儲存資源，建立虛擬儲存集中區，將這些集中區釋放予應用程式使用後，就不再操控，前述過程並非在資料通道進行，而是交由陣列本身執行。控制平台的優點在於找出底層儲存基礎架構的資源，它能分擔底層陣列的處理工作，若陣列中備有智慧功能，也能善加運用之。

在這個資料爆炸性增長的時代，為因應在動態 IT 環境中關鍵架構管理所帶來的挑戰，可以軟體工具套件彌補實體資料中心與虛擬資料中心之間所存在的顯著管理差距，利用符合所需的自動化功能，以該等套件創建 IT 架構之管理框架，協助企業提升效率、優化資源、降低成本。另一方面，可使用視覺化工具，快速地分析 IT 複雜基礎設施自應用程式至儲存裝置的依賴關係，自動分析儲存架構的可用性與性能、配置與容量增長訊息，快速識別根本原因及風險狀況，並主動解決發生問題的業務所受之影響，以及在違反服務水準協議的情況發生之前，藉由分析自一終端至另一終端的性能、容量管理與報告，優化環境及控制成本。

透過資源優化功能，可確保服務等級，提高投資回報率，例如：服務故障套件可實現可用性、性能和配置管理，亦可簡化複雜的虛擬 IT 環境的營運管理，進而提高系統人員的生產力與工作效率；跨區域管理分析可橫跨網路、儲存設備、伺服器、實體與虛擬環境，確保關鍵應用與服務的運行正常；而儲存資源管理套件則具備儀表板和探索視圖、端點到端點之關係及拓樸視覺化的功能。

(四) 管理自動化

縱使伺服器、網路、儲存均予以虛擬化，然軟體定義的資料中心仍然需要一個具有自助服務、策略原則配置、自動化的基礎架構、應用與業務管理等的管理平台 (如圖 6 所示)。

軟體定義的資料中心在服務的部署上，除業務靈活性外，應提供運營效率的自動化治理、跨異質平台之基礎設施管理、應用程式與桌面服務、自動化中心等功能，其所建置之統一管理功能必須涵蓋虛擬桌面環境中跨虛擬與實體系統的伺服器；而自助服務所配置的軟體定義的資料中心，應提供安全的自助服務門戶之授權管理員，以及預先定義的用戶特定的選單，供開發人員或企業用戶申請新的 IT 服務及管理現有的資源 (如圖 7 所示)。

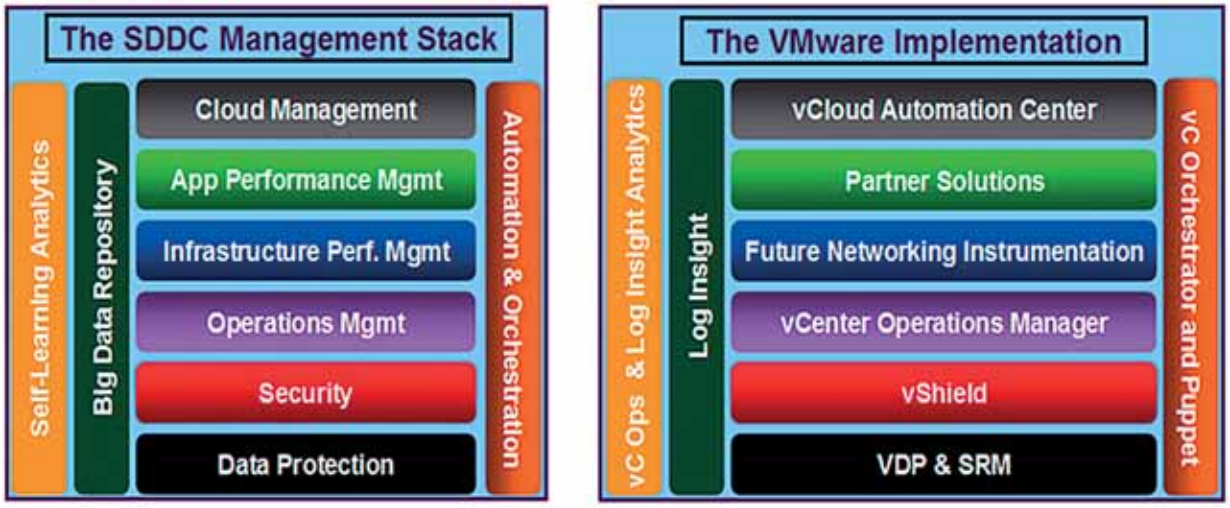


圖 6　統一的資料中心平台

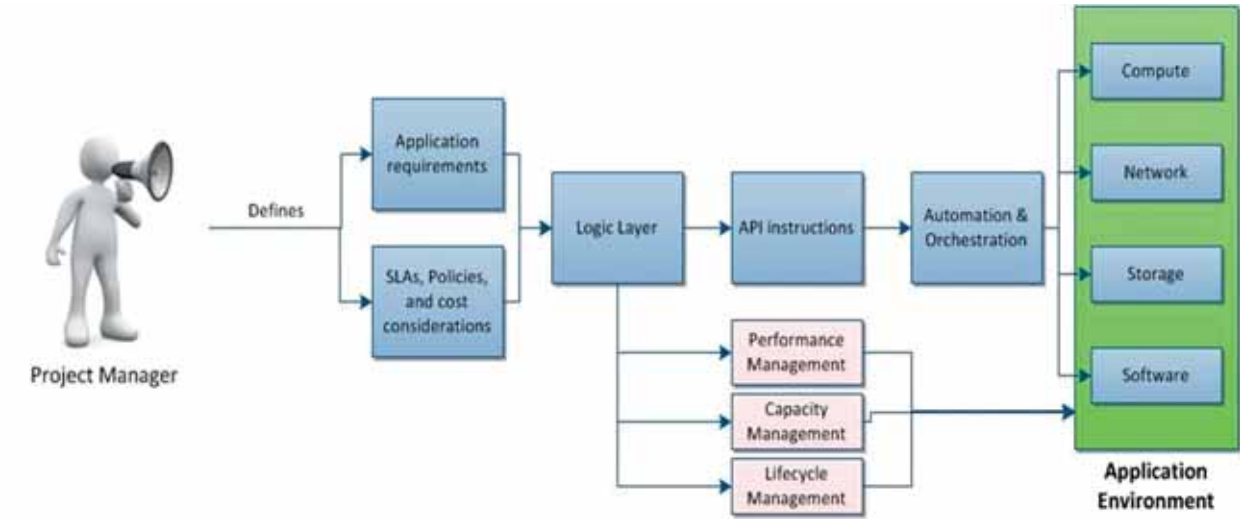


圖 7　自動化管理

五、未來發展趨勢

為什麼需要「軟體定義的資料中心」？其實透過伺服器虛擬化方式已大幅提升伺服器部署、維運的效率，企業可在幾分鐘、甚至幾秒鐘內為某個應用提供一個虛擬機器。惟任何應用的部署絕非單一虛擬機器即可解決，通常還需要額外的幾天時間，於配置網路、儲存、安全及管理等一系列的環節後，所需之應用才得以上線運營。拜新科技發展所賜，現下正是重新謹慎審視整體流程之合適時間點，將傳統伺服器虛擬化的優勢移植至其他環節，以加速應用的部署過程，不僅只在伺服器資源的調配方面實現彈性和自動化，也將這些優勢延伸至資料中心的儲存、網路、安全、維運管理等各個環節。

當重新設計整體資料中心時，審慎定義資料中心的組件為關鍵作業，爰此，最佳途徑乃引入虛擬資料中心的概念，透過虛擬資料中心將實體資源變成邏輯的資源池，為應用系統提供服務。開發者無須瞭解複雜的硬體架構，只須向彈性的資源池－即虛擬資料中心－提出清晰的需求，即可依據需求快速地備妥應用系統所需的計算、儲存、網路、安全和管理等元件，供應用系統即時運行無憂。

企業只須交付應用系統予虛擬資料中心，其他的事情皆透過新的架構平台－即軟體定義的資料中心－完成，傳統應用虛擬化部署的桎梏也隨之解銬。軟體定義的資料中心提供預先設定的安全性原則、災變備援計畫、網路配置策略等，其中包括為不同的應用系統提供互異的服務等級，這些預設的策略也可依據實際情況進行客製化，虛擬資料中心更成為構建軟體定義的資料中心的新磚瓦，使新一代資料中心的構建更為低價、快速與便捷，IT 人員也可自大量重複的勞動中解放出來，轉而更專注於業務的創新與發展。

「軟體定義的資料中心」可實現具有高彈性、高效率及高可靠度 IT 服務的雲端運算環境，將虛擬化技術的優點延伸至資料中心所有的領域，包含：運算、儲存、網路及相關可用性與安全性之服務等，其架構彙集了所有硬體資源，集結成為資源池後，在兼顧安全與效率原則下，自動依照應用需求實施最佳的資源分配。

完備的軟體定義的資料中心，必須具備跨越業界標準的硬體設備，並集結每一層資料中心基礎架構的軟體服務，使操作趨於簡化及自動化，同時能確保資源最密集的業務關鍵應用之服務品質，也必須整合構建、營運並管理雲端基礎架構所需的所有套件，包括：虛擬化、軟體定義的資料中心、策略性配置、災難復原、應用及營運管理等。

「軟體定義的資料中心」之營運管理 (如圖 8 所示)，乃運用軟體定義跨越原本不同實體機器之間的束縛，建立以服務為導向的資料中心。在設定調控、處理資料分離化、資源管理集中化及自動化的原則下，虛擬資料中心將軟體定義的服務，以符合企業策略的方式自動發布，並監控其使用情形。

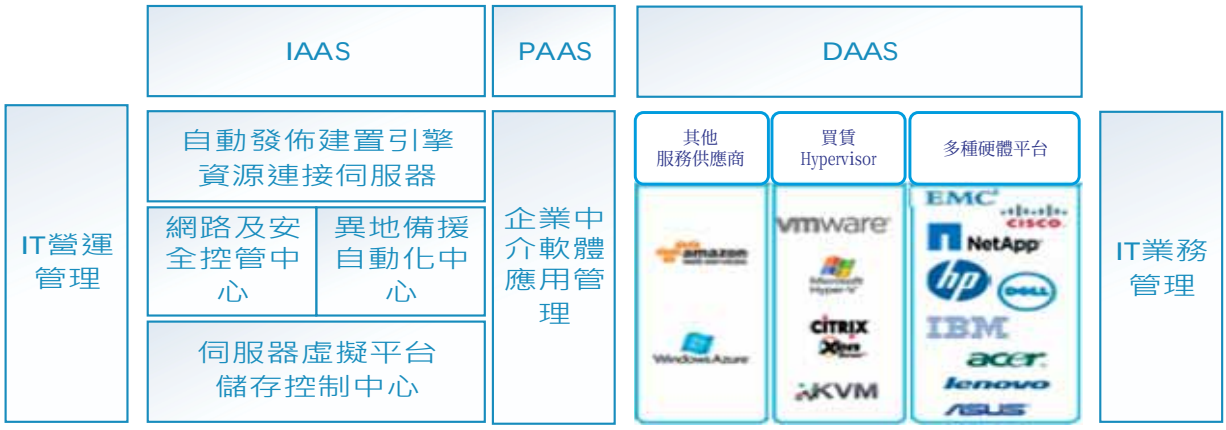


圖 8　「軟體定義的資料中心」下的營運管理

未來，專用軟體將替代專屬硬體，範圍則涵蓋資料中心的所有硬體資源，新的虛擬化形式與軟體定義的網路也將應用到 IT 架構的各個層面，這正意味著「軟體定義的資料中心」即將到來，進而為下一代的應用重新定義基礎設施。「軟體定義的資料中心」或將成為資料中心演進的新方向及趨勢，對於廠商而言，不僅必須在技術方向、合作夥伴，甚至銷售模式等方面配合調整，更需要強化人力培育，因為，在 IT 變革的進程中，最重要的影響因素往往是企業及使用者的認知與接受程度。

六、結語

「軟體定義的資料中心」在各種底層硬體架構上載入虛擬的基礎設施層，該基礎設施層也就順理成章成為「軟體定義的資料中心」的核心，此一核心提供資料中心彈性調適為因應新架構與新應用所需的管理，且底層硬體的任何變化都與上層應用無關，這就是「軟體定義的資料中心」的目標。總體而言，「軟體定義的資料中心」之優點可歸納分述如下：

軟體定義的資料中心為每一項應用提供了靈活性、高效率性與服務水平協議，無論是傳統的平台，或是創新的類型，如：高效能計算、巨量的資料、敏感性及無延遲型之應用等，未來的軟體發布是基於軟體配置的策略及管理自動化，變更時則透過軟體的自動調適，而非硬體層的工作負載平衡，並達成於合乎安全及法規規範的要求下，跨越內部資料中心與外部連接，使服務更具彈性，且業務創新更具優勢。

內建的自動管理架構，自發布、配置、設定乃至控制，皆使用政策定義的方式，最大幅地減少人工的干預，以便 IT 人員可發揮更多創新的商業價值。軟體定義的資料中心可取代傳統式僵化且複雜的專屬硬體設備，以軟體定義的策略方案完成共用資源池，提供高效能及最佳化的基礎架構。

軟體定義的資料中心可自動依資源池模式分配資源，使現有的實體硬體的容量得以達到最大的發揮及應用，提高 IT 投資的效用，也為關鍵業務提供最好的彈性，例如：軟體自動將工作負載依工作量進行調配，當發生硬體故障的問題時，軟體亦可即時將工作負載重新定向至其他硬體上，縮短服務水平的恢復時間。

綜上，軟體定義的資料中心願景，係將伺服器虛擬化的優勢移植至資料中心之其他各個環節，以加速應用的部署過程，其結果不僅在伺服器資源的調配方面實現彈性與自動化的優點，也將這些優勢複製至資料中心的存儲、網路、安全、維運等其他系統架構，嗣隨資料中心之發展逐漸趨向軟體化，企業用戶可藉此簡化及自動化系統的管理與營運功能，以實現雲端運算的效率與靈活性，強化建構新一代資料中心之速度與便捷性，IT 人員不再受制於大量重複的工作，有利其轉攻業務的創新與發展，為企業創造更高的商業價值。

※ 參考文獻 / 資料來源：

1. VMWARE 公司、EMC 公司。

金融憑證運用現況與改善方向

本篇摘自 2009 年 03 月出刊之財金資訊季刊第 58 期，由時任台灣銀行電子金融部張銘志中級專員撰寫。

一、前言

近年來，金融機構客戶端電腦遭惡意植入木馬程式，竊取客戶固定之帳號、密碼，進而損壞客戶權益事件時有所聞 (如：盜領受害存戶存款)。為了讓網際網路電子金融交易可在安全環境下日益蓬勃發展，金融機構依其業務需求與特性，於客戶端運用各項安全技術與設備以提高交易安全等級，例如銀行業採用晶片金融卡於網路銀行之轉帳確認事宜、保險業使用憑證於網路購買保單事宜、證券業使用憑證於網路下單事宜、銀行業採用憑證於各項銀行業務網路應用系統中等。

各金融機構藉由統一規格之晶片金融卡與其動態產生驗證資料之特性，在銀行公會實施「晶片金融卡網路應用系統開發注意事項」規範後，已可有效提高晶片金融卡於網路應用系統與跨銀行 Web ATM 上的使用安全強度，讓客戶可以使用晶片金融卡於各銀行的 Web ATM 中，而傳統木馬程式竊取靜態帳號密碼資料之技倆已不再影響交易安全，網路銀行交易安全性初步獲得確保。

對於使用憑證作為交易確認事宜之業務，因其憑證具有不可否認性之特性，非常適用於高風險性的網路交易。然而，目前因載具問題、憑證運用範圍等因素，各家自行發展應用，形成無法跨業運用或跨行運用之現象，亦即客戶需具多張憑證才能與多家金融機構往來，是憑證業務發展的一項瓶頸；另隨著網路交易更加普遍，駭客技術亦日益精進，現行使用憑證之網路應用系統，如網銀、金融 EDI、金融 XML 及其他的企業電子金融業務等也因信任客戶端已使用憑證，而忽略了可能潛在問題，例如憑證儲存方式、憑證載具或讀卡設備使用方式等等。

為增強使用金融憑證意願，憑證於跨行間之運用應該要加以解決，以達成客戶可使用金融憑證至各家銀行的網路應用系統完成交易的理想。因此，從憑證種類選用、載具功能規格、載具安全規範、應用系統使用憑證方式、憑證共通驗證等均需進行必要的檢討與規範標準。另為防範未來木馬程式或類似遠端遙控軟體發動不合法交易且藉由讀卡設備呼叫憑證硬體載具產生簽章資料，規範應用系統應在客戶端使用憑證前具必要檢核程序與應注意事項，讓持卡人可再自行確認交易並操作放行之處理流程機制確有其必要性。

二、目前已知之金融憑證

憑證機制能協助各種金融活動於網路上進行安全交易，目前已有不同金融領域之憑證，包括：證券網路下單憑證、網路保險憑證、電子股務憑證、網路銀行憑證、金融 XML 憑證、金融 EDI 憑證。同時，因應金控公司成立趨勢，亦有金控整合憑證以協助金控公司以單一憑證，進行旗下子公司業務之整合。

三、各類金融憑證運作瓶頸

這些廣義的金融憑證已各自在其適用領域運用，滿足網路交易之安全需求，但因其 CP、CPS、CA、RA、憑證作業流程與憑證載具均依業務需求不同而有不一樣的規範與建置作業方式，所以目前僅能於一家公司或各自領域中運用，無法跨公司或跨領域承認利用，造成客戶必須重覆申請多種或多家公司憑證之現象，徒增使用上的不便利性，也讓各公司之憑證資源浪費或需重複投資建置。以下是一些憑證運用推廣不易之瓶頸：

1. 目前憑證應用為僅適用同一家公司或某領域使用，並無法跨公司或跨領域運用。
2. 目前許多憑證應用為單一憑證單一應用，如：金融 EDI 憑證、證券網路下單憑證等，因此各公司需建置不同的憑證系統。
3. 目前各類憑證遵循不同規範與業務需求，例如身份登記方式、憑證儲存方式、憑證運用方式、憑證取得方式等各不相同，提高銀行採購與維運之成本，加上客戶操作複雜，徒增各項客服成本。

當然，我們也看到一些金控公司試圖借由金控整合憑證，而以單一憑證，進行旗下各子公司業務之整合，讓不同業務領域、不同子公司間使用單一憑證作業，提升與簡化憑證申請與使用效率。金控整合憑證的立意不錯，但卻無法解決客戶與不同金控公司往來時，相關憑證還是需要再申請，依然是滿手的各類憑證。

金融憑證的理想運作狀況為可跨公司 (同一領域) 或跨各金融領域承認與使用，而客戶只要於各跨公司及跨金融領域登記所擁有的單一金融憑證的可用業務後，即可進行各類網路交易。在此一理想下，憑證之推廣將可更為順暢的進行。

上述想法真的可以很快實現嗎？綜合以下幾項客觀因素，我們僅能說可先由銀行業間先行整合做起，先建立初步的成效，作為後續各類金融憑證之參考。

因為各類領域 CA 或各所屬 RA 的憑證如何整合運作，就各項已知的資料顯示，其技術上應較容易解決，但問題在於應用上如何整合：

1. 各類領域與不同的應用應遵循那個 CP 或 CPS？(如：每筆最高賠償金額、法律問題。)
2. 那一個單位可以作有效的決定與裁定？
3. 那一個單位可以要求參與之各領域與不同的應用必須遵循既有的規範？ (如：身份登記方式、憑證儲存方式、憑證運用方式、憑證取得方式)

換句話說，誰可以出面整合將影響憑證整合的成效，而這個單位必須要有說服力、具適當地位且適合出面推動整合。迄今，這個單位到底是誰還是沒有定論，甚或從未面對與討論過，所以各金融領域還是以其需求各自發展憑證運用，而市場上也就充斥各類金融憑證應用

服務，滿手憑證的客戶要適應各種憑證不同的操作流程，過程繁複令人心生畏懼，也不免增加金融機構之客服成本。

瞭解上述現況便可以瞭解某些外銀機構，其寧願提供較單純的安控工具（如 OTP token），並輔以其他身份認證措施，以簡化客戶網路交易之門檻並取得可接受的安全等級。

所以，我們已知道若要整合證券網路下單憑證、網路保險憑證、電子股務憑證、網路銀行憑證、金融 xml 憑證、金融 EDI 憑證，讓其可以跨領域或跨公司使用，對於所涉及的應用整合問題，迄今尚未看見可行的解決方式。因此，整合不同領域之憑證是一種理想也是一項長遠工作。

四、銀行間憑證整合互通的理想

但若由銀行業間的憑證應用整合開始著手應較為可行。因為，台灣的銀行業間已具有非常成熟的跨行交易功能與經驗，早期金融 EDI 憑證已可運用於跨網扣款 (企業可由 A 銀行之 EDI 付款系統發送扣款指示至 B 銀行，指示 B 銀行由企業帳戶內扣款並將其轉入往來廠商開立於 C 銀行之帳戶中) 的金融 EDI 交易，讓企業達到使用一家銀行金融 EDI 系統，運用相同 EDI 憑證即可調度開立於其他銀行帳戶的資金，各參加金融 EDI 銀行亦可接受客戶於其他銀行申辦的金融 EDI 憑證。當然，金融 EDI 憑證僅運用於金融 EDI 單一業務中，並沒有擴散運用於其他金融業務之明顯案例，但其概念卻於 2000 年財政部指示銀行公會成立金融 XML 訊息訂定小組之工作中被發揚光大，銀行公會於 2001 年完成金融 PKI 架構及金融最高憑證管理機構之規劃，而各銀行亦依「金融 XML 憑證共通性技術規範」建置 XML 憑證機制。XML 憑證已具有跨銀行間憑證互通的基礎，因為其由銀行公會出面制訂與規範，其架構與設計已考慮跨銀行業間的運作需要。

銀行業間憑證整合互通的理想，筆者認為至少需有以下三項：

1. 金融單一憑證可支援多種應用。
2. 金融單一憑證可支援企業透過代理銀行與付款銀行連線之運用 (如：跨銀行間跨行扣款運用)。
3. 銀行應用服務可接受其他銀行發行的金融單一憑證及載具。

五、XML 憑證運用情況

我們可逐一檢視現行 XML 憑證運用是否符合銀行業間的憑證整合互通的理想：

1. 現行金融 XML 憑證已可支援多種應用

各銀行已運用金融 XML 憑證，因應不同需求，發展出「憑證支援多種應用」，「憑證支援多種應用」指不同的應用能接受相同的憑證。對使用者而言，便是提升憑證使用的便利性及使用效益。對接受憑證的應用供應者而言，則是降低開發使用者的門檻，直接導入現存的客戶基礎。

2. 現行金融 XML 憑證已可支援企業透過代理銀行與付款銀行連線之運用

XML 憑證已被運用於銀行公會金融 XML 系統建置與訊息建置指引－付款訊息 (模式：付款人透過代理銀行與付款銀行連線) 之跨行扣款功能 (類似 EDI 跨網扣款功能) 中。另 98 年 1 月金融 EDI 業務亦將其使用憑證轉置為金融 XML 憑證。

3. 銀行應用服務尚無法接受其他銀行發行的金融 XML 憑證及載具

目前各銀行 XML 憑證註冊中心 (RA) 發給客戶的 XML 憑證載具，因其業務考量各有不同，且因憑證申辦異動作業不同、各載具驅動程式常互相衝突、憑證載具 API 介面使用方式不同、憑證載具規格不一致、憑證載具安全規範不同或網路應用系統使用 XML 憑證應開發注意事項不一。目前許多銀行無法接受客戶使用其他銀行發行的金融 XML 憑證及載具於自己的網路應用服務系統中，讓客戶與多家銀行往來時，仍需向個別銀行申辦另外的 XML 憑證。

六、現行努力目標

為了讓客戶使用金融 XML 憑證即可至各跨銀行間登記使用各類網路交易之理想，使憑證更為順利推廣運用，並提高整體安全控管水準，銀行公會業於 97 年 3 月份成立「金融 XML 憑證網路應用開發規範小組」，其已進行一系列的問題檢視與工作分組，希望於短期內研訂相關開發規範，達成「銀行間憑證整合互通的理想」的目標。目前已完成 XML 憑證之申辦異動作業、各載具驅動程式、載具 API 介面使用方式、載具規格、載具安全規範及網路應用系統使用 XML 憑證應開發注意事項與客戶端金融 XML 憑證載具驗證機制之相關規範草稿。將來，若各金融機構依循上述規範所簽發給客戶的憑證，應該可以達到「讓銀行應用服務可接受其他銀行發行的金融 XML 憑證及載具」的目標，並營造跨行間相對安全的網路交易環境，以利憑證網路應用系統業務可以蓬勃發展。

七、結語

憑證對於安全防護之效益已是電子金融業務發展的一項支柱，有了相對安全環境，電子金融交易始可穩定成長，但憑證運用無法普及或過於複雜也會讓電子金融業務發展遭受許多阻礙。因此，藉由銀行業間憑證整合互通的作業，各銀行將可以較少的投資，取得相對安全的憑證互通交易環境，這對於提升客戶使用憑證意願及電子金融的發展將是一項非常重大的助益，金融機構高階主管應正視與積極管理要求。另藉由銀行業間憑證整合互通的經驗，亦可提供跨金融領域憑證運作與互通的參考，讓客戶更願意使用憑證，享受其帶來的好處。

金融憑證載具 API 介面應用規範之制定

本篇摘自 2009 年 06 月出刊之財金資訊季刊第 59 期，由時任財金資訊公司安控部資訊安全組呂信德工程師（現任為資料管制組工程師）撰寫。

一、制定緣由

有鑒於目前國內金融機構使用金融憑證載具未有可供參考之最低標準規範，而金融電子資料交換（EDI）業務預計自 98 年初起採用金融 XML 憑證作業，為降低未來該項業務網路跨網扣款應用之風險，依據 97 年 01 月中華民國銀行公會金融業務電子化委員會－「電子銀行組組長暨技術應用分組聯席會」之決議，成立技術任務編組以研商金融 XML 憑證網路應用開發規範之制定，以利金融機構據以遵循。

開發規範制定之範圍涵蓋相容性規範之應用程式介面、載具功能、安全性規範、憑證註冊中心相關程序之標準化、網路應用系統開發注意事項及相關之驗證機制等。本文係針對 PKCS#11 之介面標準、應用概況、金融 XML 憑證載具 API 介面應用規範中之制定內容進行概要說明。

二、PKCS#11 介面標準

PKCS 的全名為 Public Key Cryptography Standard，PKCS#11 即為 PKCS 標準之一部分，係為 RSA Security 公司所提供的「公開金鑰密碼學標準」，此標準分為 15 個部份，其中第二與第四個部份已整合於第一個部份，PKCS 相關標準清單如下：

- PKCS #1: RSA Cryptography Standard
- PKCS #3: Diffie-Hellman Key Agreement Standard
- PKCS #5: Password-Based Cryptography Standard
- PKCS #6: Extended-Certificate Syntax Standard
- PKCS #7: Cryptographic Message Syntax Standard
- PKCS #8: Private-Key Information Syntax Standard
- PKCS #9: Selected Attribute Types
- PKCS #10: Certification Request Syntax Standard

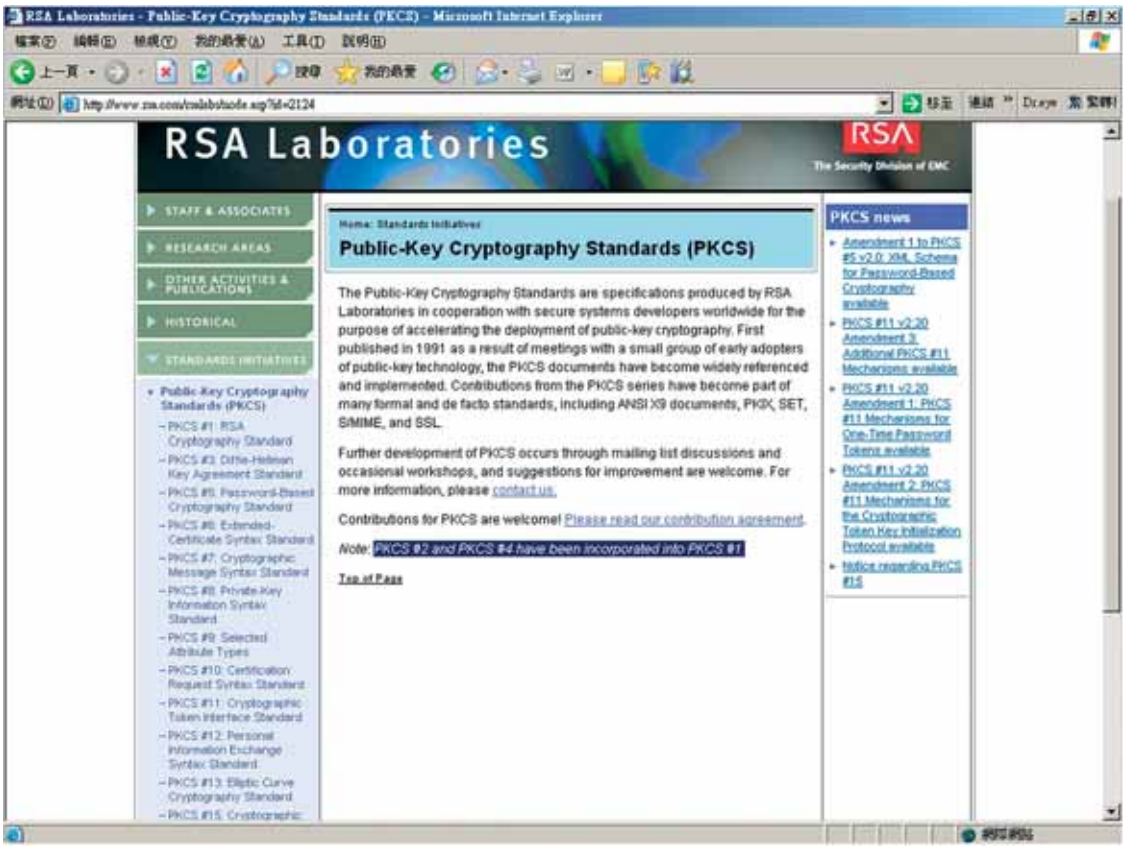


圖 1　RSA Security 公司網站

- PKCS #11: Cryptographic Token Interface Standard
- PKCS #12: Personal Information Exchange Syntax Standard
- PKCS #13: Elliptic Curve Cryptography Standard
- PKCS #15: Cryptographic Token Information Format Standard

PKCS「公開金鑰密碼學標準」的相關文件與規格書皆可至 RSA Security 公司的網站 (http://www.rsa.com/rsalabs/pkcs (如圖 1) 下載。

(一) PKCS#11 概述：

PKCS#11(Cryptographic Token Interface Standard) 係定義關於 Token 的密碼學應用介面標準，PKCS#11 為廣泛被業界所採用的 API(Application Programming Interfate，應用程式開發介面) 介面標準，應用於金融應用系統與金融憑證載具間所通用的 API，其目的係提供一組標準介面，供其他應用程式呼叫使用。PKCS#11 標準介面規格書的內容包含 PKCS#11 的定義、基礎概念、應用範圍、資料型態、密碼學運算機制、函式原型、範例…等。

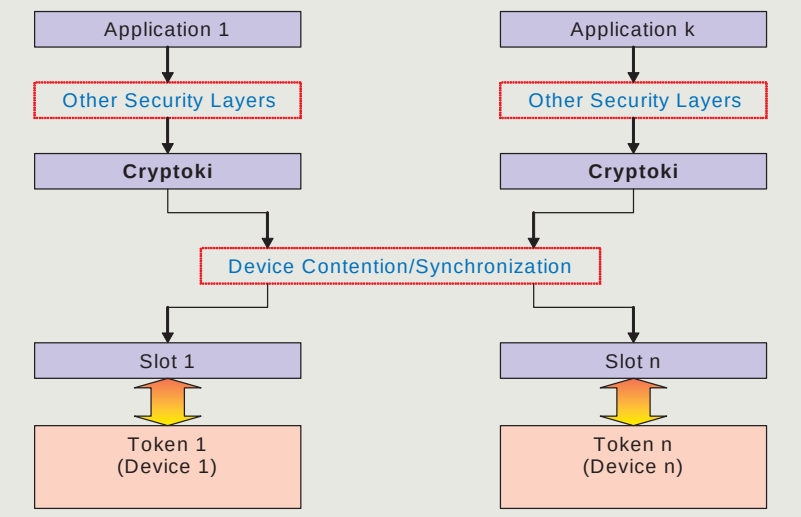


圖 2　General Cryptoki Model

(二) Cryptoki API 通用模式

PKCS#11 定義了一組「Cryptoki」的 API，有多種不同種類的函式 (Function)，供使用者透過開發工具以寫程式的方式，於建立與載具 (Token) 間的虛擬插槽 (Slot) 後，以控制載具及處理數位簽章或執行其他功能，並能支援符合此標準的憑證載具 (Token)，亦提供憑證載具硬體廠商作為開發硬體加密裝置的參考，Cryptoki API 通用模式 (如圖 2)。

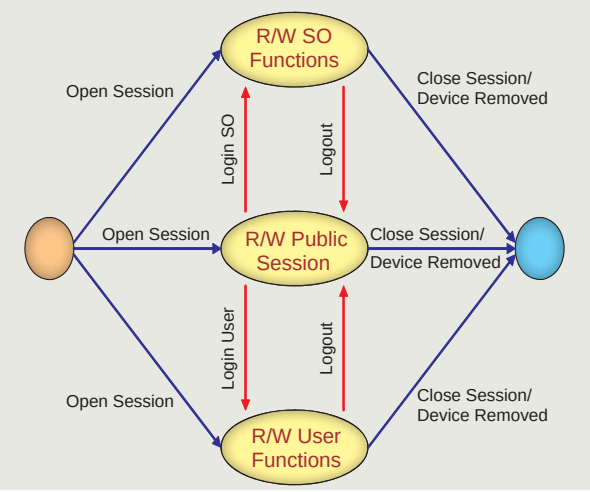


圖 3　Read/Write Session States

(三) Session & User 模式

物件之存取，以 session 狀態來管理。物件的讀寫權限分為 Read-Only 與 Read / Write 兩種，Read Only Session 可以對所有物件讀取或運算，但是無法寫入，而 Read Write Session 可以對所有物件讀取或運算，甚至修改內容；身分角色分為管理者 (Security Officer，簡稱 SO) 與一般使用者 (Normal User) 兩種，管理者之身分角色一般僅具備將 Token 初始化與產生一般使用者角色的權限，而一般使用者角色則具備對私有空間的金鑰物件進行存取的權限。當物件的讀寫權限搭配不同的身分角色即會產生不同的 session 狀態，以限制對金鑰物件的存取權限。

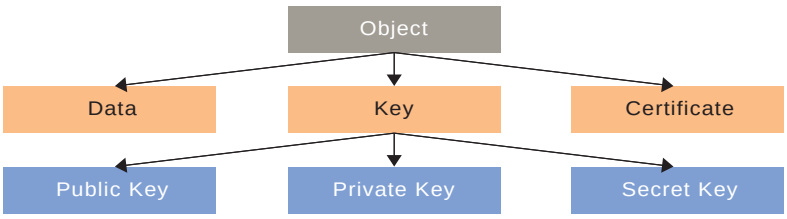


圖 4　物件種類

（四）物件模式與屬性

PKCS#11 介面標準的物件 (Object) 係由許多不同的屬性組成，物件分為資料物件 (Data Object)、金鑰物件 (Key Object) 及憑證物件 (Certificate Object)3 種，每一個物件皆可設定屬性，以限制對物件的存取功能權限。最重要的金鑰物件可定義所屬的空間屬性，空間屬性分為公有空間屬性 (public) 與私有空間屬性 (private)，搭配不同的身分角色可控制對金鑰物件的存取。

三、PKCS#11 應用概況：

2003 年 Asia PKI Forum 國際組織 -API 應用介面互通測試，由台灣之 PKI 論壇、日本 PKI 論壇、韓國 PKI 論壇、新加坡 PKI 論壇所共同進行，其目的為使不同供應商的應用程式彼此能夠相容互通，並確保 PKI 應用能夠在不同技術環境中均可適用。當時各國認證實驗決定採用最通行的 RSA PKCS#11 API 標準為基礎，並建立台日韓新共通之 PKI 應用介面（API）一般性規範，由各個參與單位分別依該規範建立其 API，並建立函式庫與 Web 應用（測試環境），再驗證其 API 之有效性，相關測試內容說明如下。

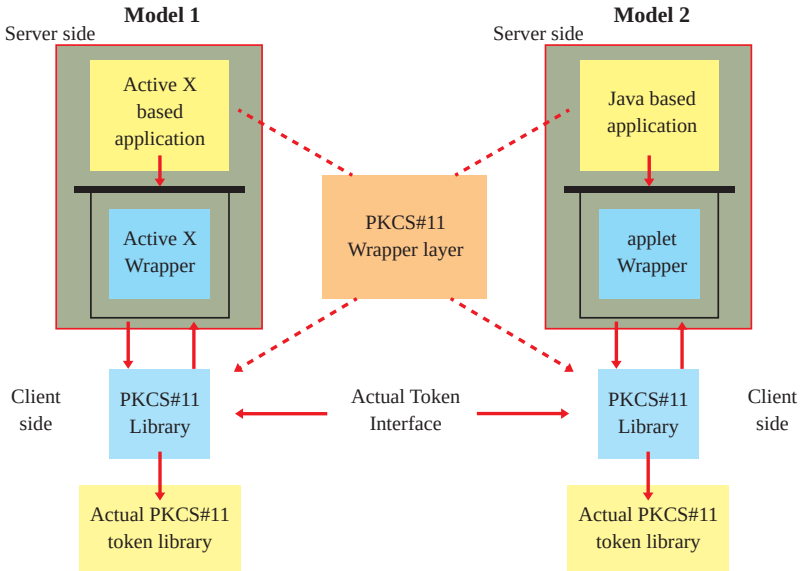


圖 5　應用介面互通測試環境

資料來源：NII 產業發展協進會 / PKI 中華台北推動委員會

(一) 各國應用介面互通測試環境

2003 年 Asia PKI Forum 國際組織 -API 應用介面互通測試，所使用的應用介面互通測試環境分為 Active X 的應用程式與 Java 應用程式 2 種 (如圖 5)。PKCS#11 載具概分為智慧卡與軟體載具 2 種 (如表 1)。

(二) 應用介面測試項目

2003 年 Asia PKI Forum 國際組織 -API 應用介面互通測試，訂定了 8 項標準 PKCS#11 共通函數 (如表 2) 作為共通規範供測試項目呼叫 (如表 3)：

表 1　各國應用介面測試工具

	PKCS#11 Wrapper	PKCS#11 載具
台灣	Active X	智慧卡
日本	applet	智慧卡
韓國	Active X	軟體載具
新加坡	applet	智慧卡

資料來源：NII 產業發展協進會 / PKI 中華台北推動委員會

表 2　共通函式表

共通函數	呼叫函式
login	C_GetFunctionList → C_Initialize → C_GetSlotList → C_OpenSession → C_Login
logout	C_Logout → C_CloseSession → C_Finalize
find_object	C_FindObjectsInit → C_FindObjects → C_FindObjectsFinal
sign	C_SignInit → C_Sign
verify	C_VerifyInit → C_Verify
get_attr_value	C_GetAttributeValue
create_object	C_CreateObject
destroy_object	C_DestroyObject

資料來源：NII 產業發展協進會 / PKI 中華台北推動委員會

表 3　測試項目

測試項目／說明	共通函數
iwg_login ／用正確的個人識別碼 PIN 登入	Login
	Logout
iwg_sign ／產生簽章	Login
	Find_object
	Sign
	Logout
iwg_getcert ／取得客戶端憑證	Login
	Find_object
	Get_attr_value
	Logout
iwg_putcert ／置入伺服端公開金鑰物件	Login
	Create_object
	Verify
	Destroy_ object
	Logout
iwg_verify ／檢驗簽章	Login
	Create_object
	Verify
	Logout

資料來源：NII 產業發展協進會 / PKI 中華台北推動委員會

四、金融 XML 憑證載具 API 介面應用規範之制定

有鑒於金融機構客戶端憑證載具，於使用金融 XML 憑證時，應用系統與載具間相容性與互通性議題，「金融 XML 憑證網路應用開發規範小組 - 技術分組」-API 介面應用規範制定小組，邀集「金融 XML 業務」與「金融電子資料交換業務」交易量前五大之金融機構系統開發維護廠商，提供關於憑證作業相關的 PKCS#11 API 函式與應用經驗，並由制定小組共同研商制定之。

考量應用架構與跨平台或同平台不同版本之相容需求，「金融 XML 憑證載具 API 介面應用規範」係依 RSA Security 公司 PKCS (Public Key Cryptography Standard) 之 PKCS#11(Cryptographic Token Interface Standard)API 標準為基礎，針對「API 介面層」訂定相關規範，規範之內容包含應用架構、應用通則、憑證作業、多金鑰作業、物件屬性…等，以達應用系統與不同載具間互通之目標，並供金融機構遵循。

(一) 應用架構

金融業務系統之客戶端載具於使用金融 XML 憑證時，應用架構區分為應用層 (Application)、安控應用函式層 (Other Security)、API 介面層 (PKCS#11)、中介層 (Middle Ware)、虛擬插槽 (Slot)、硬體載具 (Device)，架構圖如下：

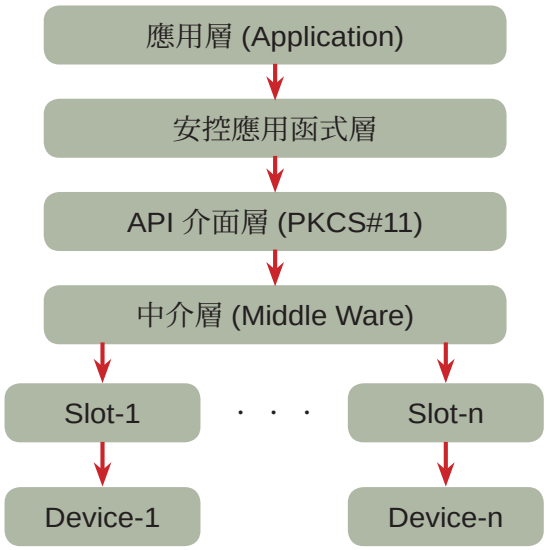


圖 6　應用架構

- 應用層：依金融業務系統交易規格所開發的應用程式 (如 Web 應用程式、Client AP 應用程式)。

- 安控應用函式層：應用層與 API 介面間之安控應用函式 (如 ActiveX 元件、Java Applet)
- API 介面層：本規範以 PKCS#11 為基礎 (如 C_Login、C_SetPIN)。
- 中介層 (Middle Ware)：API 介面層與硬體載具間之溝通介面 (如 DLL 檔)。
- 虛擬插槽 (Slot)：實體載具對應的 Slot。
- 硬體載具 (Device)：符合本會 (銀行公會) 安全規範並通過驗證之硬體載具。

(二)、 應用通則

圖 7　應用通則

金融 XML 憑證載具於應用 PKCS#11 API 介面時，其應用通則如下：

1. 簽章、變更密碼、加解密 .. 等均屬 Crypto-Operations。
2. 登入後，可依需求執行單一個或多個不同 Crypto-Operations 才執行登出。

機制 (Mechanism)	Functions			
	Encrypt & Decrypt	Sign & Verify	Digest	Gen. Key/ KeyPair
CKM_RSA_PKCS_KEY_PAIR_GEN				V
CKM_RSA_PKCS	V	V		
CKM_SHA1_RSA_PKCS		V		
CKM_SHA_1			V	

圖 8　機制 (Mechanism)

(e.g: 準備簽章時 (C_SignInit)，可使用 CKM_RSA_PKCS，選擇以 RSA 演算法做運算)

3. 使用 Crypto-Operations 時，可依需求使用下列機制 (Mechanism) 運用。

(三) 憑證作業

金融 XML 憑證載具使用 PKCS#11 函式之作業項目，可分為初始化作業、結束作業、連線作業、登入 / 登出作業、尋找物件、產生金鑰對、憑證請求檔、匯入憑證、變更密碼、雜湊、簽章、驗章、拔插、刪除物件、加解密等 15 種項目，相關函式說明如下：

1. **初始化作業** (Initialize)

(1). 動態載入「執行期動態連結 (Run-Time Dynamic Linking」。執行的前一刻才決定載入哪一個 Library File(e.g:DLL 檔), 使 USER 可隨意切換不同卡片。
(2). 使用 C_Initialize 函式開啟 PKCS#11 函式庫。

2. **結束作業** (Finalize)

(1). 使用 C_Finalize 函式，關閉 PKCS#11 函式庫。
(2). 將初始作業所載入的 PKCS#11 Library File 釋放掉，以符合動態連結 (Run-Time Dynamic Linking)。

3. **連線作業** (OpenSession/CloseSession)

(1). 使用 C_OpenSession 函式 (開啟為唯讀權限或可讀可寫權限) 開啟連線，對同一 Slot 拒絕重複 Open Session，狀態必須遵循 P11 標準。
(2). 使用 C_CloseSession 函式，以結束跟 Slot 的連線，並將 PKCS#11 函式庫清空與釋放記憶體，結束所有作業。

4. **登入 / 登出作業** (Login/Logout)

(1). 使用 C_Login 函式登入。
(2). 以 Normal User 角色及 PIN 登入成功後，始能進行作業。
(3). 僅允許以 Normal User 角色登入，執行產生金鑰對、加解密運算、私有空間物件運用之功能，私有空間物件拒絕以 SO 身分登入使用。
(4). 使用 C_Logout 函式登出。

5. **尋找物件** (FindObject)

(1). 使用 C_FindObjectsInit、C_FindObjects、C_GetAttributeValue、C_FindObjectsFinal 函式尋找物件。

6. **產生金鑰對** (GenerateKeyPair)

(1). 使用 C_GenerateKeyPair 產生金鑰對。
(2). 金鑰長度可介於 1024-bit~2048-bit，唯必須為 8 的倍數位元，其中 1024-bit 與 2048-bit 為必要選項。

7. **產生憑證請求檔** (CSR)

(1). 產生憑證請求訊息時，須將公鑰與憑證主旨 (Subject) 置入憑證請求訊息中，以私鑰做簽章產生憑證請求訊息 (CSR)。
(2). 憑證請求訊息格式須符合「金融 XML 憑證共通性技術規範」。

8. **匯入憑證** (Importcert)

(1). 使用 C_CreateObject、C_SetAttributeValue 函式匯入憑證。
(2). 匯入憑證物件前，應確認該空間之憑證物件與金鑰物件為同類同用途。

9. **變更密碼** (SetPIN)

(1). 使用 C_SetPIN 函式變更密碼。

10. **雜湊** (Hash)

(1). 使用 C_DigestInit、C_Digest、C_DigestUpdate、C_DigestFinal 函式進行雜湊。

11. **簽章** (Sign)

(1). 使用 C_SignInit、C_Sign、C_SignUpdate、C_SignFinal 函式進行數位簽章。
(2). 應用程式於簽章前，須列舉載具中所有的簽章用的憑證資料 (憑證序號、ISSUER、SUBJECT) 讓使用者選取，並找出被 USER 選取憑證對應的私鑰。

12. **驗章** (Verify)

(1). 使用 C_VerifyInit、C_Verify、C_VerifyUpdate、C_VerifyFinal 函式進行驗章。

13. **插拔** (Device Removed)

(1). 呼叫 C_GetSlotInfo 或 C_WaitForSlotEvent 函式並判別回傳值，確認使用者於回傳簽章值前完成插拔程序。

14. **刪除物件** (DelObj)

(1). 使用 C_DestroyObject 函式刪除物件。

15. **加解密** (Encrypt/Decrypt)

(1). 使 用 C_EncryptInit、C_Encrypt、C_EncryptUpdate、 C_EncryptFinal 函式進行加密。

(2). 使 用 C_DecryptInit、C_Decrypt、C_DecryptUpdate、 C_DecryptFinal 函式進行解密。

16. **憑證作業相關函式功能簡述如下：**

Function	Description
C_Initialize	initializes Cryptoki
C_Finalize	clean up miscellaneous Cryptoki-associated resources
C_GetFunctionList	obtains entry points of Cryptoki library functions
C_GetSlotList	obtains a list of slots in the system
C_GetSlotInfo	obtains information about a particular slot
C_GetTokenInfo	obtains information about a particular token
C_WaitForSlotEvent	waits for a slot event (token insertion, removal, etc.) to occur
C_SetPIN	modifies the PIN of the current user
C_OpenSession	opens a connection between an application and a particular token or sets up an application callback for token insertion
C_CloseSession	closes a session
C_Login	logs into a token
C_Logout	logs out from a token
C_CreateObject	creates an object
C_DestroyObject	destroys an object
C_GetAttributeValue	obtains an attribute value of an object
C_SetAttributeValue	modifies an attribute value of an object
C_FindObjectsInit	initializes an object search operation
C_FindObjects	continues an object search operation
C_FindObjectsFinal	finishes an object search operation
C_EncryptInit	initializes an encryption operation
C_Encrypt	encrypts single-part data
C_EncryptUpdate	continues a multiple-part encryption operation
C_EncryptFinal	finishes a multiple-part encryption operation
C_DecryptInit	initializes a decryption operation
C_Decrypt	decrypts single-part encrypted data
C_DecryptUpdate	continues a multiple-part decryption operation
C_DecryptFinal	finishes a multiple-part decryption operation
C_DigestInit	initializes a message-digesting operation
C_Digest	digests single-part data
C_DigestUpdate	continues a multiple-part digesting operation
C_DigestFinal	finishes a multiple-part digesting operation
C_SignInit	initializes a signature operation
C_Sign	signs single-part data
C_SignUpdate	continues a multiple-part signature operation
C_SignFinal	finishes a multiple-part signature operation
C_VerifyInit	initializes a verification operation
C_Verify	verifies a signature on single-part data
C_VerifyUpdate	continues a multiple-part verification operation
C_VerifyFinal	finishes a multiple-part verification operation
C_GenerateKeyPair	generates a public-key/private-key pair

資料來源：RSA/PKCS #11 v2.20: Cryptographic Token Interface Standard

(四) 多金鑰作業

金鑰載具中，最少必須可儲存二代類別物件，「當代 (有效)」類別空間與「前一代」類別空間中，各至少須可儲存 6 個物件，合計共 12 個物件。相關物件屬性如下：

- 同代同用途物件 (私密金鑰物件、公開金鑰物件、憑證物件)，之 CKA_Label 值必須唯一。
- 物件屬性 CKA_ID 與物件代別 / 用途，規範如下：

CKA_ID	代別 / 物件用途
01	當代 (有效) / 簽驗章用途物件
02	前一代 / 簽驗章用途物件
03	當代 (有效) / 加解密用途物件
04	前一代 / 加解密用途物件

(五) 物件屬性

載具內各物件屬性內容眾多，故規範基本重要物件屬性，內容如下：

- 非對稱式金鑰物件重要屬性

屬性	內容
CKA_CLASS	私密金鑰物件：CKO_PRIVATE_KEY 公開金鑰物件：CKO_PUBLIC_KEY
CKA_KEY_TYPE	CKK_RSA
CKA_TOKEN	CK_TRUE
CKA_LABEL	值必須唯一
CKA_ID	同 (四)- CKA_ID 規範。
CKA_VALUE	金鑰值 (The value of key)
CKA_PRIVATE	私密金鑰物件：CK_TRUE 公開金鑰物件：CK_FALSE
CKA_SIGN	私密金鑰物件：CK_TRUE 公開金鑰物件：CK_FALSE
CKA_VERIFY	私密金鑰物件：CK_FALSE 公開金鑰物件：CK_TRUE
CKA_ENCRYPT	私密金鑰物件：CK_FALSE 公開金鑰物件：CK_TRUE
CKA_DECRYPT	私密金鑰物件：CK_TRUE 公開金鑰物件：CK_FALSE
CKA_SENSITIVE	私密金鑰物件：CK_TRUE
CKA_EXTRACTABLE	私密金鑰物件：CK_FALSE

- 非對稱式憑證物件重要屬性

屬性	內容
CKA_CLASS	CKO_CERTIFICATE
CKA_CERTIFICATE_TYPE	CKC_X_509
CKA_TOKEN	CK_TRUE
CKA_LABEL	值必須唯一
CKA_ID	同 (四)- CKA_ID 規範。
CKA_VALUE	憑證值 (The value of certificate)
CKA_Subject	使用 DER 編碼之憑證 Subject
CKA_Issuer	使用 DER 編碼之憑證 Issuer
CKA_SerialNumber	使用 DER 編碼之憑證序號
CKA_PRIVATE	CK_FALSE

五、結語

金融憑證載具 API 介面應用規範係邀請國內發展「金融電子資料交換業務」主要金融機構之系統開發維護廠商，提供關於憑證作業相關的 API 函式與應用經驗，並由國內主要金融機構代表於銀行公會成立 API 介面規範制定小組，考量共通性、相容性與安全性議題共同研商制訂而成，可供國內金融機構客戶端載具於使用金融 XML 憑證進行跨銀行間跨網交易載具互通時之 API 介面標準。

PKCS#11 API 介面標準係應用系統與金融憑證載具間所通用的 API 介面標準，其目的為提供一組標準介面，供其他應用程式呼叫使用，符合跨平台系統的架構設計，與同平台不同版本的相容需求。

淺談企業運作韌性與持續作業

本篇摘自 2003 年 10 月出刊之財金資訊季刊第 30 期，由時任 IBM 公司胡光輝資深顧問撰寫。

企業運作韌性是長期的經營承諾，能協助企業降低風險，具備迅速的復原力與因應變動需求的彈性，藉以確保企業的永續經營。

前言

在全球化的資訊時代，經營者必須具備一套完整的管理哲學體系，才能落實企業永續經營的理念及維持企業持續的發展。而強化企業競爭力與運作韌性（Operational Resilience），則是企業賴以生存發展的憑藉。什麼是運作韌性呢？簡單的說，就是企業面臨風險（或是機會）時的應變能力與彈性。從風險的角度來看，運作風險直接考驗著企業運作韌性與持續運作（Business Continuity）的能力，其中所牽涉到的層面包括：策略、人員組織、作業程序、資料及應用系統、技術與設備…等等。

過去幾年全球各地經歷各種天災、人為恐怖攻擊（911）以及迅速蔓延的 SARS 傳染病，在在都顯示企業唯有全面考量其風險管理策略，並重新檢視其運作韌性與業務持續計劃，才能夠避免災變的痛擊，進而預防危機的發生。一般 IT 人員習於由技術面著手尋求解決方案；而事實上，技術只能事後減輕風險所帶來的衝擊，那只是整體風險管理中最為基本的一環。若要達到風險的預防，必須從作業程序面著手，並清楚定義組織職務與權責的對應。最為困難的環節在於人員之養成，當組織本身自覺自發，風險管理形成根深柢固的企業文化，才能近乎避免風險的產生。

業務持續的意義

風險觀念考量的是當客戶服務中斷時，所造成的影響與損失；商業法規的規範，則是要保障所有客戶與重要關係人。例如：金融業共同遵守的國際巴塞爾協定（Basel II），所規範的就包含作業風險。金融業的資訊處理首重安全控管與業務持續，現今的金融核心業務一般都是依賴電腦來作自動化的處理，日常的業務運作已達到無電腦即無法運作的地步；傳統僅只針對資訊基礎設備與設施的災害或是故障而作出應變的思維模式與作法，已無法達到現今金融業甚至其他各行各業的需求。

一般而言，業務持續運作計畫（Business Continuity Plan；BCP）是希望透過設計及提供解決方案，於資訊中心發生不可預期的停頓或無法正常運作時，儘可能於事先規劃的恢復時程內能夠恢復運作，以避免危及企業的正常營運。業務持續運作計畫包含兩個範疇：

一、維持業務持續所需的業務單位的作業程序和組織架構

當喪失資訊處理中心運作能力時，業務單位仍然能夠執行過渡時期替代方式的日常作業；轉移到備援中心時的災變備援作業；以及當資訊處理中心恢復運作能力後的資料補遺，與返回原資訊處理中心的回歸作業。

二、基礎建設（包括資訊技術和設備）的復原計畫

當在平時的作業地點，因為遭遇災害而導致其正常作業程序及基礎建設無法正常運作時，能夠賴以達成轉移到另一個替代的災備中心，執行全盤作業程序和組織架構計畫。

BCP 三大階段八大步驟

業務持續方法論，係由公司或組織負責業務持續的管理經理（Business Continuity Manager），於規劃企業的業務持續運作計畫與基礎建設復原能力時，所採用的一套準則來導引出企業的業務持續運作計畫。此項廣受檢驗與證實的執行方法論是由下列三個階段貫穿而成 (詳見圖一)：

第一階段：　分析階段

包含風險評估、業務衝擊分析以及對現行復原能力的分析。此階段提供各業務的潛在損失、各種衝擊及現行復原能力等量化及質化的評估，同時也根據需求，建議必須的措施及確切迅速的方針，以達到完全復原的目的。

第二階段：　設計階段

包含復原策略與企業整體解決方案的研究。此階段著重於規劃及設計出必須的行動綱領與解決方案，以達成整體組織與技術層面的復原需求。

第三階段：　執行階段

包含業務持續運作計畫及 IT 復原計畫的開發。此階段希望分別建置、執行及維護業務持續計畫及 IT 復原計畫。

前述業務持續運作計畫的三個階段，可因其特性分類為企業相關及技術相關的不同，區分為下列八大步驟：

1. **風險／威脅評估**
（Risk ／ Threat Assessment）：

對主要潛在的風險／威脅進行質與量化的評估，依照風險／威脅的嚴重性提出預防、補救與改進的措施建議。

2. **業務衝擊分析**
(Business Impact Analysis)：

收集、分析及彙整資訊系統一旦遭遇災害，對各項重要關鍵性業務的影響程度，估算可容許的中斷時程，依據其優先順序提出回復策略建議。

3. **現行回復能力分析**
(Recoverability Analysis)：

從架構、平台、科技、基礎設施與組織各層面來評估目前的復原能力，定義現行運作與技術環境下所需的最少復原資源需求。

4. **回復策略**（Recovery Strategy）：

定義最可能使用的解決方案及選擇最適合的方案。

5. **設計回復解決方案**（Recovery Study）：

詳細設計所選擇最適合的方案（稱為企業解決方案的研究）。

6. **業務回復計畫**
（Business Recovery Plan）：

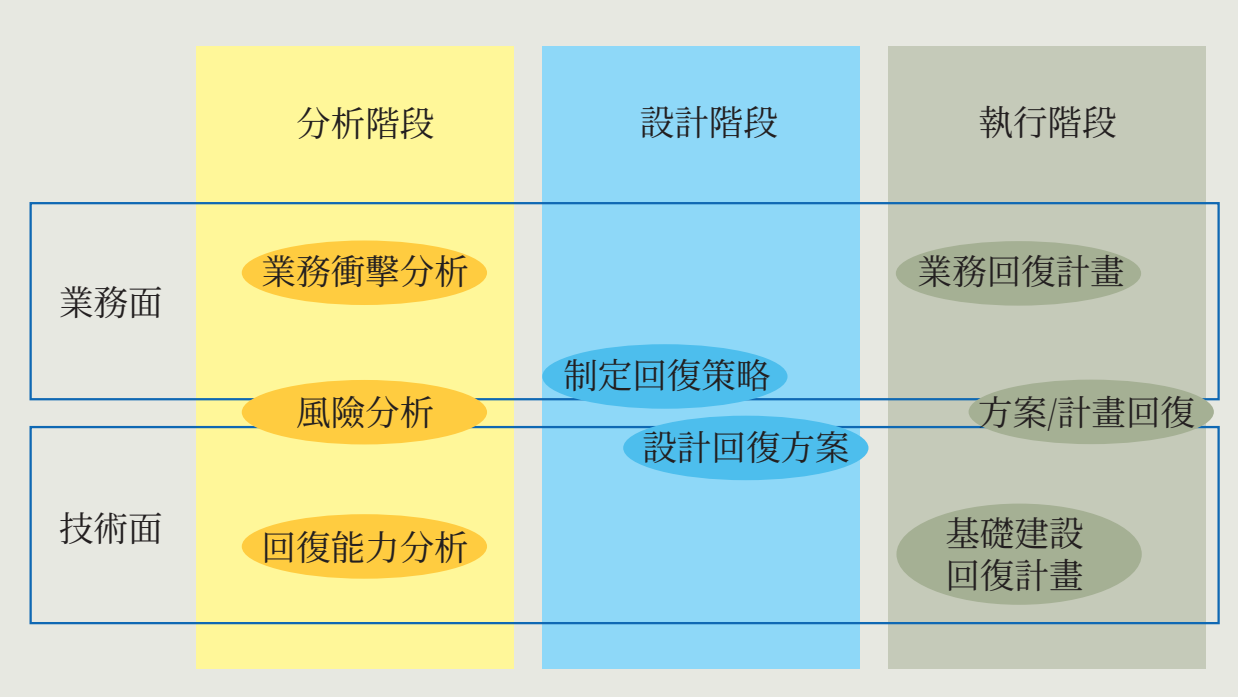
定義、制作與建置一套詳細實施程序細節，包括：人員組織與職掌、災變通報程序、各工作項目及時程、演練計劃、計劃維護處理規範、執行桌面演練及實施演練管理，以便於災害萬一發生時，業務單位與使用者必須依據且能執行重要關鍵企業業務功能的計畫，以確保各重要關鍵企業業務的持續運作。畢竟在災變發生時刻的一片忙亂當中，有很多事情是意想不到的。

7. **基礎建設回復計畫**
（Infrastructure Recovery Plan）：

建立一套災害萬一發生時，於災備替代環境如何復原資訊科技、資料與語音網路及相關設施的計畫。

8. **維護持續解決方案及計畫**
（Maintain Solution/Plan）：

確保解決方案及業務持續運作程序及復原計畫能夠保持於最新及有效。



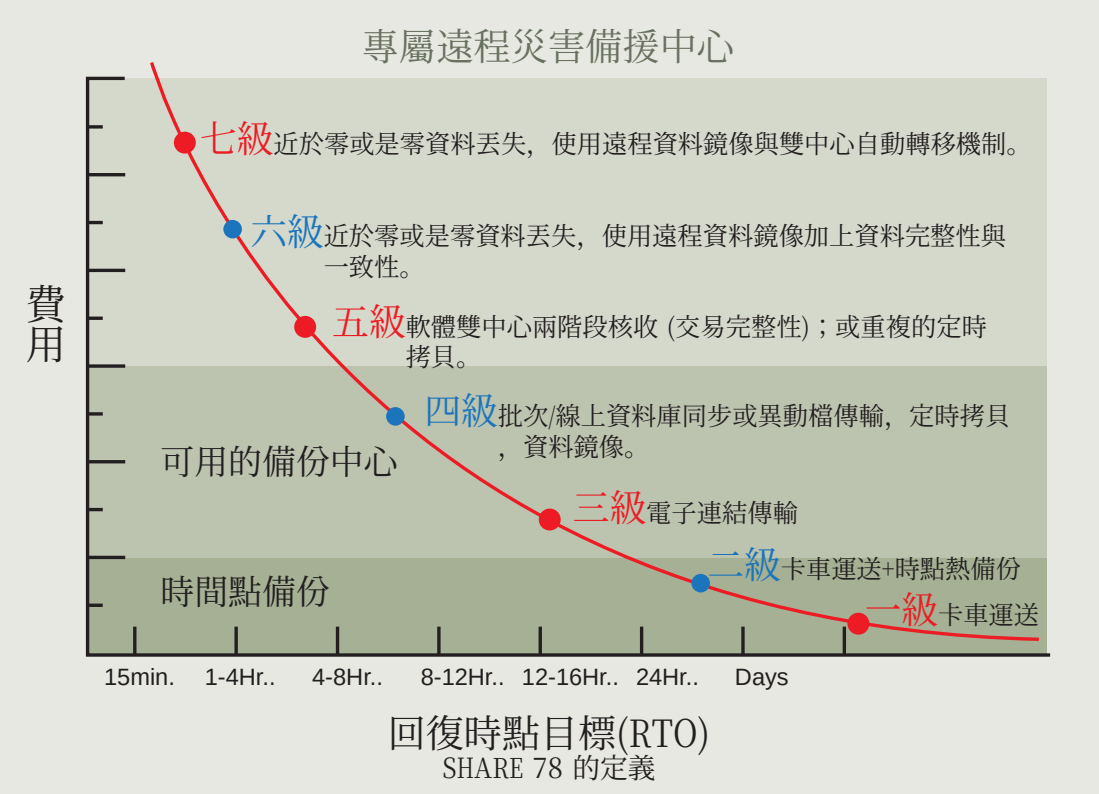
圖一　業務持續運作計畫的三個階段與八大步驟

復原等級

復原等級係根據行業規範及需求的不同，必須訂定標準的回復時點目標（Recovery Time Objective；RTO）及資料回復點目標（Recovery Point Objective；RPO），前者定義的是 IT 中斷多久後可恢復營業，後者則是確認系統資料的回復狀態以及對資料丟失的容忍範圍。以美國聯準會（Board of Governors of the Federal Reserve System）為例，對於重要金融相關行業，例如國際性重要金融機構，就要求 RTO 必須在二至四小時以內；而在票據交換與清算，則要求在一天以內必須回復。

因應企業組織對風險容忍度的差異，異地備援機制的等級也有明顯的不同。根據 1992 年在美國加州阿納漢制定的國際標準 SHARE 78 的定義，災難備援技術方案可以根據以下八大要點所達到的程度，而區分為七個等級（如圖二）。八大要點如下：

1. 備份／回復的範圍。
2. 災難回復計畫的狀態。
3. 主生產中心與災備中心之間的距離。
4. 主生產中心與災備中心之間是如何相互連接的。
5. 資料是怎樣在兩個中心之間傳送的。
6. 允許有多少資料被丟失。
7. 怎樣保證更新的資料檔案在災備中心被更新。
8. 災備中心可以開始進行恢復工作的能力。



圖二　國際標準 SHARE 78 定義復原等級分為七個層級

七個等級包含：

第一級：每天將營運資料備份至磁帶，再送至另一地點保存。

第二級：除了每天以人工備份並保存營運資料，還外加自建備援中心或是簽約服務商備援中心的使用權；也就是可在其中進行定期演練，以及狀況發生時的實際使用。

第三級：透過網路連線以批次方式，進行資料的傳送與備份。

第四級：以線上即時傳送的作法，送出每天的異動資料檔案。

第五級：正式進入備援機房的建立，雙向訊息往返以確保交易一致性，是其中關鍵。

第六級和第七級的目標，則都提升到資料零丟失，但在營運機房和備援機房勢必因為即時通訊而影響傳輸效能的前提之下，其間的連結迴路設計等技術考量，就有待於企業的取決。

金融業因為電腦化的程度極深，停機所受到的衝擊與損失相當可觀；因此，備援等級至少也都在第二級之譜，走向第五、六級則是大勢所趨，也是台灣許多大型行庫現已採行的作法。

結語

企業運作韌性（Operational Resilience）不應僅是被動地考量遭遇災難與破壞發生時的恢復能力，而是主動地考量提升到對於全盤業務管理系統多元化與自主運作的強韌彈力。因此，理解身處環境的潛在威脅，並且隨時做出適當的準備，以資訊技術面與業務面的緊密結合，將是達到業務管理與運作強韌化的有效方法。

總之，企業運作韌性是長期的經營承諾，能協助企業降低風險，具備迅速的復原力與因應變動需求的彈性，藉以確保企業生存的安全性與永續性。因此，改善運作韌性必須考量 IT 與業務相關元件，透過整合分析的方法論與專業的規劃建置，才能使企業具備最為強韌的運作能力，進而提升企業競爭力、創造客戶信賴感與品牌價值，達成企業生生不息永續經營目標的不二法門。

Focus 專注·專業 @ **Innovation** 創新·引導 @ **Security** 安全·穩健 @ **Convenience** 便捷·服務

資訊安全篇

潛在入侵安全之研究－惡意程式碼與潛在入侵防護能力初探

本篇摘自 2003 年 02 月出刊之財金資訊季刊第 26 期，由時任鈺松國際資訊公司研發處樊國楨協理撰寫。

「在資訊系統的設計及實作過程中，如能預先顧及安全程式等相關問題，同時加以處理；雖然不能保證不會發生不安全之事件，但至少其完成之產品、系統不至於在駭客眼中評比為「不堪一擊」。

關鍵詞：

1. 潛在入侵（Attack Potential）。
2. 共同準則（Common Criteria）。
3. 惡意程式碼（Malicious-code）。

前言

內政部警政署刑事警察局去（2002）年 4 月 22 日首度仿效美國相關單位方式發佈網路安全警訊，指出國內八成以上的官方網站與民間網站，面臨「資料隱碼（SQL Injection）」駭客攻擊手法的嚴重威脅，利用此方式，駭客可以化身合法使用者，輕易入侵網路伺服器，進而竊取各網站資料庫資訊。結構化查詢語言（Structured Query Language，簡稱 SQL）是關連式資料庫管理系統（Rational Database Management System，簡稱 RDBMS）與 C 語言、COBOL 語言等溝通的資料庫查詢語言標準，市面上常見的 DB2、IBM Informix、Microsoft SQL、MySQL、Oracle、Sybase 等均支援 SQL。且不論「SQL Injection」攻擊法的威脅性是否如媒體所述，由於 SQL 的普及，已引起各界的好奇與重視[1]。

「SQL Injection」攻擊法比較貼切的中文名稱應為「SQL 指令植入式」攻擊法，主要是駭客利用許多未做嚴謹之「Input Data Validation（輸入資料驗證）」之應用系統，將「資料處理程式碼（Data Manipulation Language，簡稱 DML；又名 SQL 指令）」當做一般資料交給伺服器處理，使得伺服器錯把駭客丟來的偽裝資料之「資料庫程式碼」當成正常的資料庫程式碼執行，藉而達成入侵的目的。

這類安全漏洞見諸駭客實現攻擊的文獻可以上溯至 1997 年，2001 年 2 月 14~15 日黑帽（Black Hat）駭客研討會之視窗安全討論會（Windows Security Conference）中，@stake 公司的 David Litchfield，在滲透測試工作時發現：「不需要知道正確的使用者帳號與通行碼，僅使用 ASP 程式之登入（Login）畫面，利用 URL 資料嘗試錯誤的方法，即可知曉資料庫管理系統圖格（Schema）的結構，

進而使用 Insert 指令加入攻擊者的帳號，再以 Update 指令增加權限。」之事實，發表論文：「Web Application Disassembly With ODBC Error Messages」，引發「SQL 指令植入攻擊法」實作之風潮，目前已成為資訊系統必須正視的安全問題。

其攻擊原理是使用資料驅動式（Data Driven），這種攻擊方法與指令通道式（Command Channel）、命令列式（Command Line Bugs）等攻擊法不同，防火牆與入侵偵測系統等能做的事不多；撰寫應用程式的人員應養成如同騎機車戴安全帽、開汽車繫安全帶之安全程式（Secure Programming）的撰寫習慣，方能對防堵及偵測「SQL Injection」等資料驅動式攻擊法有所幫助。

舉例而言，業界盛傳於 4 月 22 日測試成功之國內某知名機構網站，使用者於輸入身分證字號時，使用「SQL Injection」攻擊法即可獲得他人之敏感性資訊例；在身分證欄位之輸入資料驗證時，使用資料庫設計中定義域（Domain）的觀念，宣告第 1 碼僅能使用英文，第 2 碼僅能使用 1 或 2，第 3 碼至第 10 碼僅能使用正整數，即可有效防護。報載自動化防範「SQL Injection」攻擊法的程式，其原理如同 4 月 24 日聯合報民意論壇台大湯耀中教授讀者投書所言將「 ' 」等特殊符號之輸入資料摒除，但應無法保證 SQL Injection 攻擊法一定無法得逞，上述方式僅是資料庫設計定義域觀念的簡化。使用輸入資料驗證外，再使用「輸出資料驗證（Output Data Validation）」，除能落實輸入資料驗證外，尚可監控異常之輸出資料，應是預防「SQL Injection」攻擊法之工程面的解決方案之一。

「SQL Injection」在潛在入侵（Attack Potential）攻防中屬於「易守難攻」類【2~3】，在我國卻有 80% 以上之網站面臨威脅，顯見「安全程式」在我國尚屬萌芽階段，本文淺析安全程式的重要性以及潛在入侵損害衝擊等級【4~5】；最後，帶出本文的結論。

表一　惡意軟體 (Malicious-code Software，簡稱 Malware)

1. 源起：1988 年之 Internet Worm。
2. 生產力：2002 年估計值為 1 月有 500~800 個 Malware 問市。
3. 分類：
3-1 New e-mail attacks。
3-2 Open source Malware。
3-3 P2P Malware。
3-4 IM Malware 。
3-5 Keystroke-logging Malware。
4. 防禦技術例：沙盒 (Sandboxes)。

資料來源：Lawton, G. (2002) ,Virus Wars ： Fewer Attacks, New Threats, IEEE Computer, Vol. 35, No. 2, pp. 22~24.

表二：潛在脆弱性開採類別 (Attempted Exploitation of Potential Vulnerabilities, **簡稱** PAV) **之屬別** (Families) **與組件** (Components)

1. 開採花費時間 (Time taken to exploit，簡稱 PAV_TTE)：6 組件。
2. 專業技能 (Specialist technical expertise，簡稱 PAV_STE)：3 組件。
3. 評估標的設計與操作之知識 (Knowledge of the TOE design and operation，簡稱 PAV_KNO)：4 組件。
4. 機會之窗 (Window of opportunity，簡稱 PAV_WOP)：5 組件。
5. 開採所需之資訊技術硬體與軟體或其他設備 (IT hardware/software or other equipment required for exploitation，簡稱 PAV_HSW)：3 組件。

惡意軟體與安全程式

「安全是一種過程而非單一產品（Security is a process , not a product）」，資訊系統安全除了面臨不當使用與非故意之錯外，還需要面對「人為」心懷惡意的破壞與攻擊；「安全程式（Secure Programming）」根基於風險管理，探討如何寫出安全性的程式碼，諸如防止此應用系統出現暫存區溢位（Buffer Overflow）、格式化字串（Format String）等安全性問題，以及使用沙盒（Sand boxing）、軟體鎧甲（Software Wrapper）等技術增加軟體的安全性各方面的議題[2]。

國際標準組織針對 (表一) 所示之惡意軟體（Malicious-code Software，簡稱 Malware）已重新訂定潛在入侵（Attack Potential）威脅之全安評估標準如 (表二至四) 所示，表三即為表二所示 PAV 類別中 5 個屬別之組件的示意說明；抵抗攻擊者潛在入侵成功之能力的程式脆弱性評比級別如 (表五) 所示，在不同的使用環境下，可以做為應用系統開發人員撰寫面對如 (表六) 所示之安全軟體共同問題等之「安全程式」時之參考。

表三　潛在入侵 (Attack Potential) **計算對照表 (* 代表超越高度困難之潛在入侵，** 代表幾不存在可開採之潛在入侵路徑)**

因素	範圍	鑑別參考值
花費時間	小於一天	0
	小於一週	1
	小於一個月	4
	小於三個月	12
	大於三個月	*
專業技術層次	不切實際	**
	門外漢	0
	熟練者	2
	專家	5
需具有之評估目標相關知識	公開	0
	內部資訊	1
	敏感資訊	4
	關鍵資訊	10
	不需要 / 存取不受限	0
機會之窗	容易	1
	適度	4
	困難	12
所需之相關設備	無	*
	標準的	0
	特殊的	3
	特製的	5

資料來源：CCIMB (2002) Characterization of Attack Potential, Version 0.5, CCIMB.

表四　潛在入侵等級 (Attack Potential Levels，**簡稱** APL)

	APL1	APL2	APL3	APL4	APL5
PAV_TTE	1	2	3	3	4
PAV_STE	1	1	2	2	3
PAV_KNO	1	1	2	3	4
PAV_WOP	1	1	2	3	4
PAV_HSW	1	1	2	2	3

資料來源：CCIMB (2002) Characterization of Attack Potential, Version 0.5, CCIMB.

表五　脆弱性評比 (Rating of Vulnerabilities)

評估值範圍	0~2	3~5	6~12	13~ ？	*
抵抗攻擊者潛在入侵成功之能力級別	不評比 (no rating)	基礎 (Basic)	適度 (Moderate)	高 (High)	超越高級別 (Beyond High)

表六　安全軟體（Secure Software）**7 個共同問題**（Common Problems）

1. 緩衝區溢位（Buffer Overflows）
2. 競爭條件（Race Conditions）
3. 存取控制問題（Access Control Problems）
4. 似亂度問題（Randomness Problems）
5. 密碼學誤用（Misuse of Cryptography）
6. 輸入確認錯誤（Input Validation Mistakes）
7. 通行碼問題（Password Problems）

資料來源：McGraw, G.(2002) On Briks and Walls: Why Building Secure Software is Hard, Computer and Security, Vol.21, No3, pp.229~238

潛在入侵損害衝擊等級

1998 年 11 月 2 日的傍晚，康乃爾大學電腦研究所一年級生小莫里斯（Robert T. Morris Jr.）將 10 月 15 日正式列出功能需求，在當天 19 時 30 時完成的程式，從麻省理工學院人工智慧實驗室電腦下達釋放的指令。當晚，這隻後來稱為網蟲（Worm）的程式癱瘓了許多網際網路上的電腦，共造成數萬部電腦主機失效的莫里斯網蟲事件[6]，有如春雷乍響般，將美國國家安全局電腦安全中心孕育已久對於惡意程式碼將導致資通訊安全問題之隱憂，成為眾所矚目的焦點[7]。

不同程度的系統弱點，不同目的的入侵者，所造成的損害衝擊均不盡相同。在此，說明攻擊導致之六種不同程度的損害。損害程度由輕而重，如 (圖一) 所示分別為等級 1 至等級 6[8]。

等級一：郵件炸彈與阻斷攻擊：

郵件炸彈可以說是最簡易的攻擊方式，對攻擊者而言，完全沒有任何利益，和阻絕攻擊一樣是一種損人不利己的攻擊。應付這類型的攻擊，唯一的方法只有將來自涉嫌使用這種攻擊方法的網域所送來的封包全數過濾。然而這只能減輕影響，卻無法避免垃圾封包佔用頻寬的事實。目前已有不少網路安全軟體，可以自動找出可能的垃圾封包來源，加以過濾。

等級二：合法使用者有能力讀取未經授權的檔案：

透過某些系統弱點，或系統的存取控制設定失當，一般使用者可能有能力越權使用系統資源。在使用 shadow passwd 的 UNIX 系統，如 Solaris，將所有使用者的登入密碼加密後儲存於 /etc/shadow 檔案中，而為避免一般使用者檔案採用字典攻擊法，取得其他使用者的登入密碼，不開放 shadow 檔案的讀取權限給一般使用者。如一般使用者有能力讀取 shadow 檔案，就可以採用 Cracker 之類的程式，使用字典攻擊法猜測密碼。為增加字典攻擊法的困難度，目前許多系統，如 FreeBSD 已可選擇將傳統使用 DES，密文長度 13 字元的加密方法改為使用 MD5，密文長度為 128 bits 的加密方法。

等級三：合法使用者有能力寫入未經授權的檔案：

若一般使用者有能力寫入未經授權的檔案，將更加危險，以上述 UNIX 的例子而言，若一般使用者能寫入 /etc/passwd 或 /etc/shadow，就可以輕易地獲得管理者的權限。事實上在 UNIX 系統中，只要任何一個地方，出現存取權限為 srwxrwxrwx 且擁有者為系統管理員的檔案，就表示任何有能力登入該系統的人，都有能力取得管理員的權限。由於損害程度二與三中，獲取額外權限的是合法的使用者，一般而言所造成的危險程度較低，追查也較容易。

等級四：外來的使用者取得讀取系統內檔案的能力：

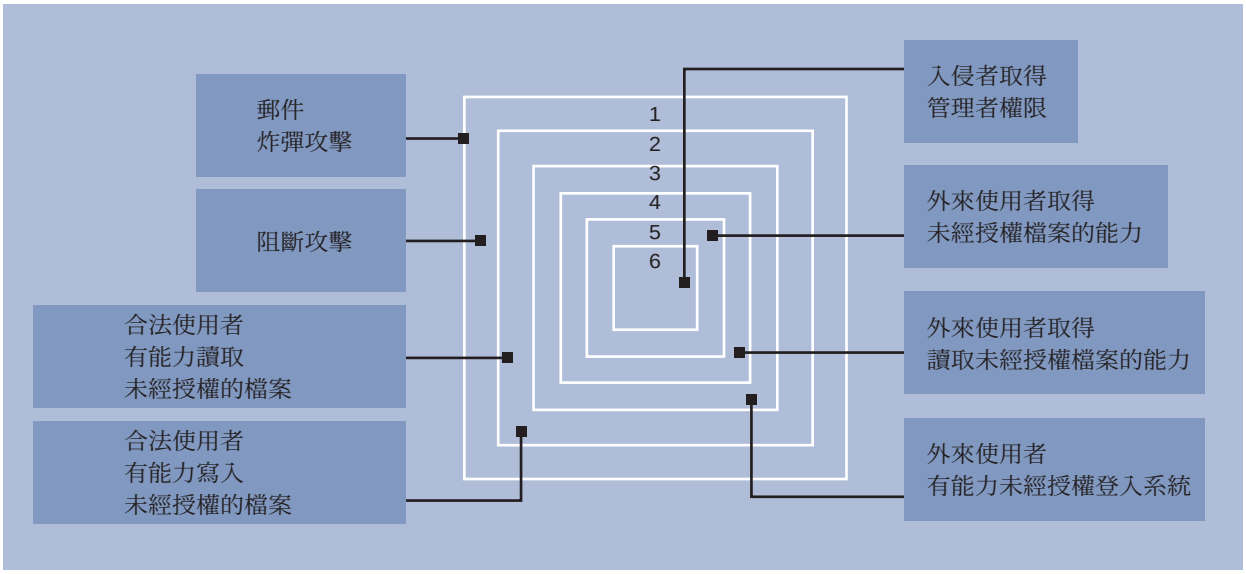
這裡所謂的能力可能包含讀取檔案或是列出目錄內檔案的列表。雖然此時入侵者並無法新增修改系統內部的檔案，但是讀取權限卻讓入侵者有機會能對系統進行瞭解，進一步發現更嚴重的系統弱點，並藉此取得更高的權限。當然對某些儲存機密資料的系統而言，如果機密資料的讀取權限被入侵者取得，可以說已經是最嚴重的損害了。

等級五：外來的使用者取得寫入系統內檔案的能力：

若入侵者已取得部分系統檔案的讀取、寫入權限，有相當大的機會，入侵者就可以取得管理員權限，至少已經比系統內的一般使用者擁有更高的權限。這是非常嚴重的狀況，距離系統瓦解只一步之遙了。

等級六：入侵者取得管理者權限

只要入侵者有能力寫入特定的系統設定檔，如 /etc/passwd，簡單的新增一個具管理員權限的使用者，立即可以取得所有系統的使用權。至此，整個系統就完全掌握在入侵者的手中了。



圖一　潛在入侵損害衝擊等級

結論

處在二十一世紀的今天，使用資訊系統已是人們生活中不可或缺的一環；然而，伴隨而來的另一個問題卻是「運籌於虛擬實境之外，決勝於方寸螢幕之中」的攻擊者潛在入侵的安全問題。

為因應資訊科技的日新月異，經濟合作發展組織（Organization for Economic Co-operation and Development, 簡稱 OECD），自 2001 年 9 月 11 日起，由資訊安全及隱私工作委員會（Working Party on Information Security and Privacy, 簡稱 WPISP）之專家群（Working Group）經過 4 次 6 天的討論後提出草案，再由 WPISP 經過 3 次 6 天的討論送交 OECD 大會（Council）審議，於今（2002）年 7 月 25 日公佈「資訊系統及網路安全指導綱要：朝向安全的文化（Guidelines for the Security of Information Systems and Networks：Towards a Culture of Security）」。

基於此，英國標準協會（British Standards Institute, 簡稱 BSI）在今年 9 月 5 日修訂公佈 BS 7799-2：2002 版，並在前言中明述遵照 OECD 之原則訂定在「規劃（Plan）、執行（Do）、檢查（Check）、行動（Act）（Plan-Do-Check-Act, 簡稱 P-D-C-A）模式建置資訊安全管理系統（Information Security management systems-Specification with guidance for use）之規範，經濟部標準檢驗局亦據以制定 CNS17800 國家標準：資訊技術－資訊安全管理系統規範。

OECD 公佈之指導綱要揭示：認知（Awareness）、責任（Responsibility）、回應（Response）、倫理（Ethics）、民主（Democracy）、風險評鑑（Risk Assessment）、安全設計及實作（Security Design and Implementation）、風險管理（Risk Management）及重新評鑑（Reassessment）九大原則，有鑑於此份指導綱要之關鍵性，我們將安排系列之文章介紹各個原則相關的標準規範。

表七　安全程式稽核示圖

稽核項目	風險所在	稽核方法
1. 確定開發者對於安全的程式技術是否有接受完善的訓練	程式撰寫員如果沒有接受適當的訓練，可能無意識的暴露出應用軟體的安全漏洞	驗證所有的程式撰寫員於安全的程式技術，都有接受過完整的訓練
2. 確定客製化程式（Custom scripts）是如何分析使用者的輸入資訊	程式如果不能分析使用者的輸入資訊，可能經常遭受到惡意入侵者從遠端執行命令的攻擊	所有處理使用者輸入資訊的程式碼必需經過仔細的過濾
3. 確定客製化程式是如何分析使用者獲得的輸出資訊	程式如果不能分析使用者獲得的輸出資訊，可能會遭受到惡意入侵者獲取無權檢索的資訊	所有處理使用者獲得輸出資訊的程式碼應有輸出資料驗證的規則
4. 確定客製化程式是否使用暫存檔	• 使用者可能在應用程式執行前先產生假的檔案來破壞使用暫存檔之 CGI 程式 • 存在不被保護目錄的暫存檔，可能被惡意的入侵者利用其內含之敏感性資訊	• 驗證所有使用暫存檔的程式是否能在安全的目錄下隨機的產生檔案名稱 • 驗證所有程式在讀寫檔前能核對檔案是否存在
5. 確定在回應客戶端需求，其程式是讀檔或是寫檔	根據使用者提供的資訊來存取檔案是一種不良程式設計，可能因遭受到破壞而允許惡意入侵者存取任何檔案	• 核對所有的檔案名稱被定義在主機端且沒有嵌入 HTML 中 • 核對程式謹慎處理上一層目錄的存取（../）
6. 確定在伺服器上儲存敏感資訊的應用服務程式	惡意的入侵者透過受攻擊的網站服務得到系統存取權限，可能再更進一步獲得安全傳輸資訊的存取權限	核對所有的敏感資訊均存放在受保護的檔案中或安全的遠端系統
7. 確定在網頁服務執行程式的權限	具高權限且易遭受攻擊的程式，可能導致惡意入侵者擁有更大的權限	• 核對以 SUID 權限 (UNIX) 執行的程式 • 核對非網頁服務使用者有權限執行的程式

「回應」及「安全設計與實作」是前述OECD九大原則中，於1992年11月26日OECD公布之「資訊系統安全政策指導方針（Guidelines for the Security of Information System）」中並未特調的兩項。攻擊手法日新月異，資訊系統的安全威脅亦與時推移，面對抵抗攻擊者潛在入侵成功之安全軟體的設計，除了工程面的解決方案外，利用教育與訓練建立完整的資訊安全觀念與能力；同時，建立資訊安全風險管理、如(表七)所示之安全程式稽核等之機制[9]，並定期由專業人員進行滲透測試的檢驗應是現階段比較完整的解決方案。

安全程式的問題，是網際網路時代的怪現象也好，是軟體產業品質不佳也罷；在軟體產業不斷推陳出新，讓產品快速循環，所暴露出的安全問題，一般估計，在1,000行程式中大約有15隻蟲(Bug)，這樣的調查報告換算到有50,000,000萬行程式碼的Windows 2000時，Windows 2000中應該有750,000隻蟲。

2001~2002年交際時，微軟公司董事比爾．蓋茲先生正式宣布：「微軟公司包括Windows在內的所有產品，安全與隱私的重要性，將凌駕各種新功能。」的重大策略轉變。同時，劍及履及，微軟公司去(2002)年2月停止研發新的作業系統軟體，派遣7,000名系統程式師接受軟體安全的特別訓練。

以建立商譽的角度來看，微軟公司以公開宣示進行「建立可信賴資訊系統戰爭」；誓言，「盡力做到像是電力、水力公司及電信業一樣安全的資訊產品。」換言之，在未來3~5年內，資訊技術人員必須在惡意軟體橫行的環境中撰寫安全程式方能確保資訊系統使用上的安全性。

「大陸駭客入侵，資安會報警訊」，去（2002）年8月1日，聯合報以顯著標題報導，指出其來源有大陸官方色彩，自7月21日起以攻擊包括政府骨幹網路及金融、醫療等機關在內之200多台電腦。前述「SQL指令植入式」攻擊法據聞某單位執行僅用「' '」之攻擊測試，千餘台電腦被攻入之比率大於4%。「以管窺豹」，我國安全程式的普及應尚在「長路漫漫路迢迢」的階段。鑑於兩岸情勢之特殊，我國若不儘速面對安全程式等教育訓練不足的問題隨著電子化政府、電子商務的發展等的推動；資訊服務之日益普及，已指日可待；台灣海峽彼方的有心人士將可輕易獲取大量我方的敏感資料，甚或植入木馬。4月22日、7月20日以及8月1日之上述三則新聞稿即為例證。

「只要是程式，沒有不出錯（bug）的！」本文探討面對攻擊者潛在入侵之安全設計中之潛在脆弱性開採的問題與安全程式等預防方法。在資訊系統的設計及實作過程中，如能預先顧及安全程式等相關問題，同時加以處理；雖然不能保證不會發生不安全之事件，但至少其完成之產品、系統不至於在駭客眼中評比為「不堪一擊」。

※ 參考文獻 / 資料來源：

1. 鈺松國際資訊股份有限公司（2002）SQL Injection攻擊法與安全程式，資訊安全論壇，第6期，頁3~7。
2. Viega, J. and G. McGraw (2002) Building Secure Software: how to avoid security problems the right way, Addison-Wesley.

3. Schiffman, M. (2001) Hacker ’ s Challenge: Test You Incident Response Skills Using 20 Scenarios, McGraw-Hill.
4. http://www.commoncriteria.org
5. 徐鈺宗等（2002）資訊系統安全評估及測試保證之研究，資訊安全論壇，第 9 期，頁 41~56。
6. Hafner , k. and J. Markoff(1991) Cyberpunk, John Brockmann Associates, Inc.。
7. 白方平譯（1996）捍衛網路，平下文化出版有限公司。
8. Anonymous (1998) Maximum Security, 2 nd ed. , SAMS。
9. 紀慧敏（2002）美國金融電子銀行業務之網路架構安全控管及稽核方式之研究（出國報告），中央存款保險股份有限公司。

中美駭客大戰與金融網路安全

本篇摘自 2001 年 06 月出刊之財金資訊季刊第 16 期，由時任政治大學金融學系殷乃平教授撰寫。

為因應駭客入侵事件日趨頻繁，各國無不致力於其電腦軟體的安全防護，以防止國家機密外洩。中美駭客大戰，更加凸顯出電子網站安全與維護的重要性！我國的金融機構進入網路世界者日多，也許應該多投資一點在其電腦本身的安全防護設施之上。

中美駭客大戰上演

五月初的中美駭客大戰在九日宣告結束，這個名為「五四大轟炸」駭客行動，共集合了中國三大駭客組織－「中國紅客聯盟」、「中華黑客聯盟」、「中國鷹派」，計千人以上，在網路上交換駭客經驗，提供對方網站的訊息。「中國紅客聯盟」宣佈此役戰績輝煌，自稱攻克了近一千個美國網站。據美聯邦政府在卡內基米濃大學的 CERT 監控中心指出，每天平均有 100 件以上入侵美國網站的意圖，但是主要的聯邦網站都已提高警覺，守得不錯，惟仍有不少安全措施不足者，遭到侵入。

這回主要的攻擊方式是「蓋頁」(Defaced)，就是用新網頁將原有網頁蓋過去；而也有用電子丟包，自動拷增電子郵件，將電腦主機容量漲爆、導致停機的阻斷服務 (Denial of Service)。媒體報導披露，被中共駭客「蓋頁」者包括有：美國能源部、勞工部、衛生部、眾院的職工網頁、鐵路管理局、美日關係協會、美國地理調查網站、雅虎…等處。其中以企圖入侵白宮的網站者最多，駭客先誤中副車，將民間經營的白宮歷史網頁蓋頁 (如圖一)，後來多次進攻白宮主網頁失利，只好採用阻斷服務的下策，讓白宮的網站被迫關閉兩小時。

圖一　被蓋頁的白宮歷史網頁

美國的駭客當然也不甘勢弱，估計至少有五十個大陸的官方網站被蓋頁，但是在五四以後，突然全部縮手了。據稱是美國的 FBI 藉機全面蒐集美國駭客的資訊情報，消息傳出，美國駭客立即停止動作。

在中美駭客大戰中，其它國家的駭客進入混水摸魚者也不少，如英國的國家廣播電台 BBC 網站就有開斯米爾獨立組織侵入；至少有三個微軟的國際網站被蓋頁；而阿根廷的麥當勞網站、美國的 MSNBC 網站都被國際駭客趁火打劫。至於台灣的網站夾在中美之間，也受到戰火波及，如番薯藤網頁就曾被迫更易；不過，這次要比兩國論期間，國內多數公、私網站受到電子丟包，阻斷服務的情形要好得多。

在這同時，美國有一名叫做 DarkSpyrit 的駭客，在網路上揭露微軟 Window 2000 的軟體中，列印驅動程式中有「蟲」(bug)，其中一個「jill.c」指令會導致電腦主機向入侵者投降，交出主機的控制權。一時之間，天下大亂，目前問題尚未解決。

網路安全倍受威脅

進入到電子網路時代，網路安全一直是所有運用者最關心的問題。美國 FBI 公佈的報告顯示，去年，有一百五十五個聯邦機構的網站被侵入。駭客為網路商機帶來前所未有的夢魘！因為與「蓋頁」相比，前者只是一個無害的警告而已。早在 2000 年 1 月 9 日，駭客「Maxus」侵入專在網路上出售 CD 唱片的 CD Universe 網站， 盜取了一千多個信用卡客戶資料，勒索十萬美金被拒後，Maxus 就在其網頁上公佈盜取的所有客戶信用卡密碼與相關資料，供其他有意犯罪者下載，並且在網路媒體上挑戰，表示可以隨時入侵盜得網路商店的信用卡資訊 (見圖二)。

去年的 2 月 7 日，網路世界的主要蒐尋引擎 Yahoo 突然失蹤了三小時，原來它遭受到電子丟包的阻斷服務。接著，eBay、Amazon、CNN、e*Trade、Excite@home … 都曾遭受到駭客攻擊，當 FBI 開始調查時，突然駭客又消聲匿跡；到目前，只抓到一個加拿大十五歲自稱為「mafiaboy」的駭客。

圖二　Maxus 公佈資料的網站

早年我國大同工學院學生所設計的 CIH 病毒亦曾癱瘓不少電腦，但是去年 5 月 4 日開始散播的「I love you」病毒，似忽有相同的威力。我國某一家電腦公司早上打開電腦，發現主機中突然增加了 32,000 個網址，還在以每秒 200 個的速度在倍增。這種病毒只要打開 e-mail，病毒馬上進擊，把整台電腦當掉。估計十八小時之後，全世界有一千萬台電腦中毒，受害者包括：英國國會、美國五角大廈、美國國會…等。源頭來自於菲律賓的一個電腦學生，他做的電腦程式被老師打了個不及格，一氣之下，全世界糟殃。至今，這種病毒仍然在網路世界中活動，它是利用微軟 e-mail 軟體的漏洞所設計的病毒，也就是常見的阻斷服務 (DOS)，這使得微軟的聲譽大受影響。

然而，讓微軟更難受的是在 2000 年 10 月 27 日，駭客進入微軟的主機，將其最新的產品設計藍圖與資訊完全盜出，這次事件號稱是二十世紀最大的駭客事件。主要的攻擊工具是個改良過的特洛伊木馬病毒「Qaz」，這個事件讓全世界的大企業、政府機關部門都大為緊張，因為連供應世界軟體的微軟公司主機都可以任由駭客進出裕如，那麼，所有電腦中的機密如何保護？隨後，美國的西屋、Visa、甚至於總統選舉時的共和黨內部機密資料都曾被「Qaz」入侵。

到了 2000 年 12 月，號稱美國最大、防護最周密的網路信用卡網站 CreditCard.com 被入侵，近 60,000 客戶的資訊與交易資料被駭客取得，敲詐二萬美元未果，隨即將資料公佈在網路上 (見圖三)。同時另一個 Egghead.com 金融網站也被入侵，估計有三百七十萬客戶資料庫的資料被駭客下載。一般認為這是一群烏克蘭與俄羅斯的駭客集團所為。美國的專家估計他們至少在美國的 40 個主要的網路商店中，取得一百萬個以上的信用卡號碼與密碼，而跨國的防止電子犯罪機制不全，使得美國的 FBI 查緝極為不易。

事實上，早在 1995 年，俄羅斯的駭客 Vladimir Levin 以一台筆記型電腦，破解花旗銀行高級主管的密碼，入侵其主機，將帳戶中交易的資金挪到設於各地的人頭帳戶之中，最為離奇的是巴西的券商正自花旗銀行的電腦中轉進一筆現金途中，被俄羅斯的駭客從中截走。這一役，花旗銀行自稱損失三百七十萬美元，市場中的流言卻稱其損失在五億以上。英國的駭客也跟進，自稱為「The Saint of E-commerce」者每天在網路上更新他從 13 個英國金融網站所竊取的信用卡號碼，最後英國警方發現這是兩個十八歲學生所幹的好事。

目前，在網路上駭客公然出售所取得的信用卡號碼的價格是一美元一個，而以這種號碼在網路上購物與製做偽卡的生意日增。易言之，金融機構與其客戶受到駭客入侵的成本愈來愈高，該如何防止類似的問題一再發生？

圖三　駭客在網路上公佈 CreditCard.com 客戶資訊

妥善因應電腦犯罪

揆諸國內，我國電腦犯罪業已出現，邇來更是時有所聞，今年五月一日台北刑大甫偵破一個失業電腦工程師在網路咖啡店中破解金融機構客戶密碼，盜領百萬存款的案例。同時，我國的信用卡市場中偽卡充斥，金融業者面臨了與國外業者同樣的難題。由於在網路上使用信用卡所衍生的問題過多，目前，國際上已經在討論以儲值卡取代信用卡的可能，並且進一步建立網路上較為可靠的支付系統。

除此之外，1995 年前後，美國的一個猶太人家族在網路上建立了一個「虛擬的國家」，如果仔細的核對這個國家所在的經緯度，應是南太平洋水深五百多公尺的深海中。這個國家設有財政部、中央銀行，發行自己的貨幣，也對外發行公債，在國際金融市場中從事各種金融交易，也從事一些外交活動。根據美國 FBI 的調查報告，該國設在香港的領事館似曾與我國商談建交事宜。最後，因為到期的債券引起一些投資者的懷疑，露出馬腳，乃被 FBI 偵破。

金融市場中的電子犯罪隨著網路商機的擴張而日益難以防範，業者如何因應其挑戰？依據 MSNBC 的電腦專家建議：

1. 永遠保留備份資料，縱使電腦與開放網路不相連接，仍然可能被駭客入侵，為防止金融資料庫受損，必須保留備份，並持續的更新。對於須保密的敏感資料，應採必要的加密措施。
2. 購置防毒軟體，並且定期的更新。
3. 所有網路上的金融工具交易必須要對交易對方有較為深切的認知，交易完成之後，進一步的複核也有其必要，畢竟安全與效率均應兼顧。
4. E-mail 是目前發生問題最多之處，未經防毒軟體掃瞄的 e-mail 不要開啟。同時在微軟視窗軟體未能有效解決其隱藏的「蟲」之前，應盡量不加以使用。而敏感的訊息的 e-mail 經由網路傳遞，亦應設法加密。
5. 盡量不在網路上給予他人個人的私人資訊。其中包括出生日期、電話號碼、地址等。以避免被他人截取利用。
6. 在網路上或在金融機構的個人密碼，盡量以他人不易破解的方式設計，如將英文、與數字，甚至標點符號混合，可增加其破解的困難度。

結語

為因應駭客入侵事件日趨頻繁，各國無不致力於其電腦軟體的安全防護，以防止國家機密外洩。但是道高一尺，魔高一丈，永遠無法求其絕對的完善。例如有俗稱捉鼠機的蜂蜜窩(Honeypot)，除了設計捉住入侵的老鼠之外，還以數台電腦，規劃路徑，建立幻境，以欺騙入侵的駭客。此外，樹立防火牆，以防衛敏感的資訊，提供駭客入侵的預警資訊，同等重要。筆者曾誤入一個不應進入的網站，立即有一個警告標誌，並且威脅如不立刻關機，即將摧毀所有筆者電腦的資訊，嚇的筆者立即退出關機。

總而言之，駭客大戰之後，更為凸顯出電子網站安全與維護的重要性，我國的金融機構進入網路世界者日多，也許應該多投資一點在其電腦本身的安全防護設施之上了。

如何做好無線網路之安全防護

本篇摘自 2006 年 04 月出刊之財金資訊季刊第 45 期，由時任資訊安全顧問暨台灣科技大學資訊工程系鄭博仁兼任教授撰寫。

自從電磁波被發現以來，無線技術就已經在我們周圍跟著我們。收音機與電視的發明更證明空氣可以是一個又好又方便擴散資訊的傳播媒介。然而，一直等到數位時代，無線通訊才成為每一個人生活方式的一部分。數位化的手機、無線 PDA 或配置無線 PC 卡的膝上型輕便電腦等都是在辦公室、大街上或家裡很容易看得到的一些裝置。

在過去的年頭，工業界已經很清楚地區分無線通訊的兩個重要應用：語音與數據資料。近年來無線通訊在影像的應用也逐漸盛行。語音的裝置主要是傳統的行動手機。由於隨後引進的傳呼服務、簡訊服務以及 IP 電話的技術逐漸向數據傾斜，使得之後語音與數據的應用有融合為一的趨勢。目前比較盛行的無線通訊網路有 802.11 WLAN、Bluetooth、與 GSM 等網路。

根據市場調查，全世界所有公司的手提電腦已經有超過 50% 以上配置無線區域網路 wireless LAN (WLAN) 連結，可以無線上網。WLAN 的快速部署是這個技術具有本身存在優勢的最好證明。很不巧的是，目前大部分部署的 WLAN 基本上都是不安全的。這種狀況是由兩個支配一切的問題所引起的。首先，這個技術本身相當新而且不成熟。其次，這個技術沒有表面上看起來那麼簡單。要部署一個 WLAN 的環境，基本上是很容易的。但是要部署一個 WLAN 的環境，做到滿足現存安全政策的需求，同時將商業風險減少到最低程度就很不容易了。WLAN 的安全是可以做到的，但是需要具體的規劃再加上確實的承諾，來處理一些 WLAN 重大的架構、建制與運作的課題。

本文將以探討 802.11 WLAN 無線網路之安全防護為主題，探討 802.11 WLAN 的安全需求以及如何做好無線網路之安全防護。本文首先瀏覽 WLAN 無線網路之技術及應用。其次將討論 WLAN 無線網路所遭遇到的安全威脅以及必須考量的安全課題。後續再描述 802.11 WLAN 的安全解決辦法。最後將提出一些有關如何做好 802.11 WLAN 無線網路安全防護之具體建議與忠告以及本文的結論。

WLAN 無線網路

一、IEEE 802.11 簡介

在 IEEE 所提議的無線區域網路 (wireless LANs (IEEE 802.11)) 的標準中，可以有兩種不同的方法來安裝一個網路：點對點傳輸模式 (ad-hoc) 與基礎建設 (infrastructure) 傳輸模式[1,3]。在點對點傳輸模式網路，電腦可以急促的被帶進來動態地形成一個網路。正如 Figure 1

所示，在這網路中沒有一個結構；沒有固定節點；而且通常每一個節點都能夠和另一個其他的節點通訊。ad-hoc 網路的一個好例子，是公司裡面的員工各自攜帶膝上型輕便電腦一起來開會，並透過無線網路來通訊及分享設計或財務資訊。雖然表面上看起來，這類型的網路很難維持次序，不過已經有像 SEA 的演算法[2]被設計出來推選一台機器擔任這個網路的「基地台」(主人) ，而其他機器則充當奴隸似的從動裝置。在 ad-hoc 網路架構的另一個演算法則使用一種「廣播」和「氾濫」的方式在所有節點之間來建立各自的身份與相互間的關係。

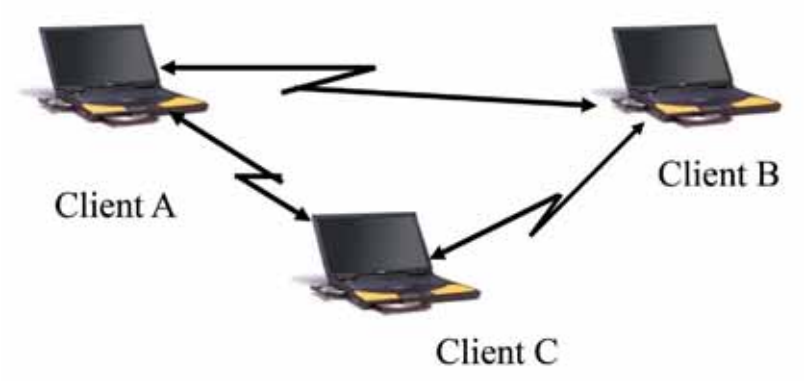


Figure 1：Ad-hoc Network

正如 Figure 2 所顯示，第二類型的無線區域網路結構是屬於「基礎建設」型。這個架構使用固定的網路「存取點」(Access Point (AP)) ，讓每個移動的節點可以與它通訊。這些網路「存取點」有時候連結到實體介質的線路，利用它來當作無線節點與有線節點之間的橋樑以擴張無線區域網路的功能。如果服務的地區重疊的話，有線與無線交接的情況就可能發生。這個結構和今天盛行全世界的移動電話網路很相似。

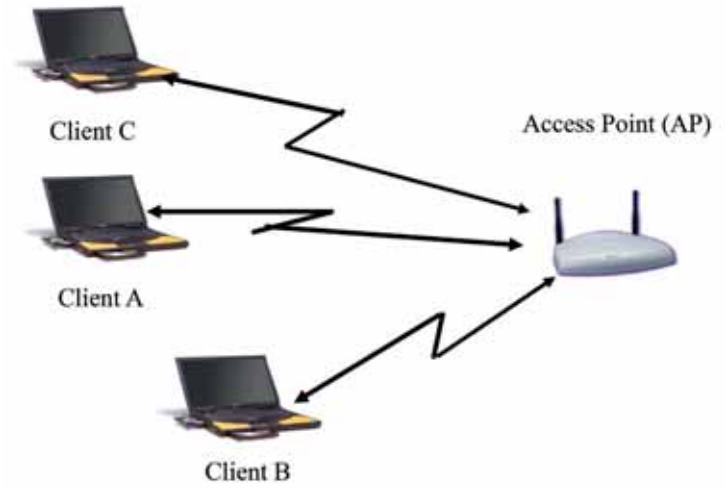


Figure 2：Infrastructure Network

二、IEEE 802.11 的層級

在 IEEE 802.11 標準中把規格訂定於網路實體層 (Physical Layer) 與媒介存取層 (MAC Layer) 的參數 [3]。實體層實際處理節點之間的傳輸，可以使用「直接序列展頻」(direct sequence spread spectrum)、「頻率跳躍展頻 」(frequency hopping spread spectrum) 或紅外線脈衝位置調變。以展頻傳輸為例，IEEE 802.11 提供的資料傳輸是運作於屬無需執照的 2.4 至 2.4835 GHz 的 ISM 應用頻帶，而且速率可達 1 Mbps 或 2 Mbps。至於紅外線傳輸則使用 300 - 428,000 GHz 頻帶。紅外線傳輸通常被認為較難竊聽，因為紅外線傳輸必須是「直線視野」(line-of-sight) 的連結 (除非在單純連結的空間才可以傳輸，拐了彎的角落就不行)；這和無線射頻傳輸正好相反，因為後者可以穿過牆壁在不知不覺之間被第三者截獲。然而紅外線傳輸會受到陽光不利的影響，而 802.11 的展頻通訊協定對一般的資料傳輸的確提供初步的安全保護。

MAC 層級是一套負責在使用共享媒介時維持次序的通訊協定。802.11 的標準規定一套 CSMA/CA 的通訊協定。在此通訊協定中，當某一節點接到一個要傳送出去的封包時，它首先傾聽來確認其它節點不播放。如果頻道是暢通的，它就傳送這個封包。否則它選擇一個隨意的「後退係數」(back off factor) ，用它來決定這個節點必須等待多少時間才允許它傳送出去它的封包。當頻道暢通的時段，正在傳送的節點會遞減它「後退係數」的數值，不過頻道繁忙的時候「後退係數」的數值是不會被遞減的。當「後退係數」的值，減到零時，這個節點就可以把封包傳送出去。由於兩個節點會選擇同一個「後退係數」的機率相當微小，封包之間碰撞就可以減到最少。乙太網路所使用的「碰撞偵測」CSMA/CD 並不適用於 802.11 無線射頻傳輸。其中的原因是，當一個節點在傳送的時候，由於它自己的信號會覆蓋任何其他抵達這節點的信號，所以它是聽不到系統內的任何其他可能也正在傳送的節點。

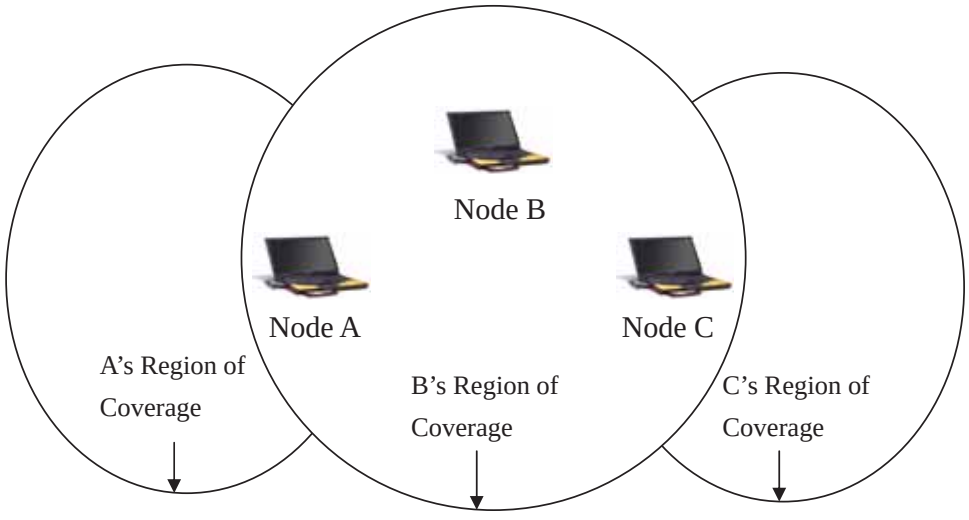


Figure 3：The Hidden Node Problem

任何時候有一個封包要被傳送時，傳送的節點會送出一個簡短的 ready-to-send (RTS) 封包內含被傳送封包長度的資訊。如果接收端節點聽到這個 RTS，它就會以一個簡短的 clear-to-send (CTS) 封包來回應。經過如此的資訊交換之後，傳送的節點開始傳送它的封包。當封包通過 CRC 檢查碼的 CRC 檢驗，成功地被接收後，接收端節點傳送一個「告知收到」(acknowledgment (ACK)) 的封包。這樣來回的交換是必須的以避免「隱藏節點」("hidden node") 的問題，如 Figure 3 所示。在 Figure 3 中，節點 A 能和節點 B 通訊，節點 B 也能和節點 C 通訊。然而，節點 A 卻不能和節點 C 通訊。因此 , 舉個例子來說，雖然節點 A 可能感應到頻道是暢通的，但這時候事實上節點 C 可能正在傳送封包給節點 B。以上描述的通訊協定，允許系統向節點 A 警示節點 B 正在忙碌中，所以節點 A 必須在傳送封包前稍做等待。

WLAN 無線網路的安全威脅及考量

所有的區域網路，不管是有線還是無線，都容易受到兩種型態的攻擊而受傷 :

其一為「主動式的攻擊」；像駭客取得區域網路的存取權進而破壞或塗改資料，以及「被動式的攻擊」；像駭客接近或使用區域網路，但只能竊聽所傳送的資料。無線區域網路更易受到這兩種型態的攻擊，因為駭客不需要有實體的連結到運作中網路的場地就可以展開攻擊。

一、主動式的攻擊 :

入侵者所發起第一種直接攻擊，意圖中斷網路的運作或資料的存取。它們的輪廓可以描繪如下 :

(一) **欺騙**:

這是最基本的一種主動式攻擊型態，入侵者藉由更改他們無線終端機的設定，使它們看起來像擁有跟經過授權的 AP 或無線終端機一樣的 MAC 位址，以便非授權的情況下存取無線網路。

(二) **阻絕服務** (DoS):

阻絕服務以無意義的資料淹沒頻寬的方式使網路停頓，來中斷一個網路。啟動一個 DoS 攻擊，入侵者先發現無線網路的一個存取點，然後送給它一連串無意義的資訊。這些資料串摧垮了存取點，使得它不能再使用。DoS 攻擊可以精密到像是以 802.11 的「分離」(disassociation) 管理訊框對無線終端機行騙，或簡單到使用一台 2.4 GHz 頻帶的 RF 產生器來干擾 RF 的頻道。

(三) **重播攻擊**:

入侵者監聽並擄獲一個無線終端機與存取點之間所傳送的封包。這通常經由一個被動式、在網際網路很容易取得的監聽用的免費軟體用品叫 " 嗅探器 (sniffer)"(譬如 Air Snort) 來完成。一旦封包被擄獲，駭客就可以經過這存取點重複傳送封包來啟動一個 DoS 攻擊造成伺服器主機的超載；或加速網路上的資料流動以減少為破解 WEP(Wired Equivalent Privacy) 加密金鑰所需蒐集資料的時間。

二、被動式的攻擊：

有兩種型態；(1) 在不中斷已授權的裝置之間的通訊下，蒐集正在運送中的資料，或經過一個安全漏洞來滲透無線網路。802.11 無線技術先天上就必須開放給任何 802.11 的無線電設備偵聽。因此，一個被動式的攻擊不需要精密地方法或工具就能竊聽與蒐集資料。

(一) 對抗式的操縱 (War-driving):

這是最常見的被動式攻擊的型式之一。802.11 網路的 RF 信號可以延伸至一個建築物範圍之外。一名駭客可以攜帶一台膝上型電腦或無線終端機，很簡單地駕車經過商業區被動地傾聽一個強烈的 RF 信號。假如 802.11 網路安全沒做好的話，要滲透這個網路是不需要花費太多功夫的。

(二) 人員在中間的攻擊 (Man-in-the-Middle):

這是一個需要精密軟體而且能造成重大的崩潰或資料損失的攻擊。駭客把自己介入於一台 AP 與一台無線終端機中間，以便擄獲正在傳送中的封包。這台無線終端機視駭客為一台經授權的 AP，而這個 AP 則視駭客為一台經授權的無線終端機。這兩台已授權的裝置皆未能察覺到這位駭客的存在，而且繼續傳送資訊。駭客因此擄獲合法的資訊而且把假的資料注入網路內，或發動一個 DoS 的攻擊。

除了可能遭受非授權的使用者攻擊之威脅外，802.11 無線網路還可能遭受來自內部的威脅。許多 802.11 網路被安裝時並沒有適當的措施來保證組態與管理功能的安全。並且，許多公司可能沒有執行安全政策或提供教育訓練來幫助員工了解無線網路以及它的安全隱喻。譬如說，為了減少使 WLAN 啟動起來立即工作的時間，某些無線設備的廠商提供他們的裝置時，把某些包括安全機制的功能關掉。這可能造成過度的暴露於某種攻擊。瞭解與適當的管理 WLAN 設備以減少受到攻擊的風險是很重要的。另外由內部造成網路風險的例子可能是員工引入一個未經授權的劣種存取點至公司網路內。現今，一旦接通電源就可工作的無線設備只需極少的安裝，而且每個人可使他們自己的無線網路很快動起來並立即工作。如此做而沒有適當安全機制控管的話，每個人無意中已經產生一個安全漏洞。假如 RF 信號又足夠強大的話，一個 "war-driver" 就可以接收到這個信號而且能夠存取公司網路。

802.11 WLAN 的安全解決辦法

本章敘述傳統 WLAN 安全做法以及 802.11 的安全標準與改進 [4,5,6]。

一、傳統 WLAN 安全做法

如同其他網路，WLAN 的安全集中於存取控制與隱私保護。健全的 WLAN 存取控制阻止非授權的使用者經過 AP (位於乙太網路上來連結 WLAN 的客戶至乙太網路的 WLAN 終端點) 來通訊。堅固的 WLAN 存取控制保證合法的客戶與可信賴的 AP 而不是敗壞的 AP 聯繫。WLAN 的隱私保護保證只有預期的聽眾才了解所傳送的資料。

只有當資料使用一把僅有預期的接收者才有的金鑰來加密，所傳送 WLAN 資料的隱私才受到保護。傳統的 WLAN 安全包括使用 SSID 身分證明、開放式或共享金鑰式的身分辨識、靜態的 WEP 金鑰、和可選擇性的媒介存取控制 (MAC) 身分辨識。這樣的結合提供一個初級的存取控制與隱私保護，但其中每一個元件都可能受到危損。

SSID 是在一個 WLAN 子系統裡每一個裝置的通用網路名稱；它是用來邏輯切割這個子系統。SSID 阻止任何不具 SSID 的客戶裝置來存取網路。然而由於初始設定值的規定，一個 AP 在它設置信標時就廣播它的 SSID。即使把 SSID 的廣播關掉，一個入侵者或駭客還是能以 sniffer 偵測到這個 SSID。

二、802.11 的安全標準與改進

802.11 的標準是一組由 IEEE 所制定的 WLAN 規格，它支援兩種客戶身分辨識：開放式與共享式金鑰。開放式辨識只牽涉到供應正確的 SSID。在共享金鑰式身分辨識裡，AP 送客戶裝置一個挑戰正文之封包，讓客戶必須以正確的 WEP 金鑰加密後回覆給 AP。假如客戶沒有金鑰或擁有錯誤的金鑰，身分辨識將無法通過而且客戶將不允許與 AP 聯繫。共享式金鑰的身分辨識並不被認為是安全的，因為一個駭客同時查出挑戰的原文與用 WEP 金鑰加密後的挑戰密文的話，就能夠解開 WEP 金鑰。

第一代的 802.11 安全標準存在很多弱點，包括差勁的加密器 (金鑰長度不超過 40 位元)，靜態的加密金鑰，並且缺乏一個金鑰分配的方法。不同的學術和商業的研究皆顯示即使在 WEP 加密之下，堅持不懈的駭客仍可能會很快攻破 WLAN 的安全防衛。WEP 只對偶然的窺探者有效， Wi-Fi 聯盟曾經警告過不能把 WEP 當作一個完全的安全答案，因為它僅保護客戶機器與存取點間的連結。另外 SSID 的安全技術對付惡意的攻擊也是無能為力。

為了和 802.11 安全弱點搏鬥，IEEE 等機構已經引介在以標準為基礎的技術上所開發出來的補強安全解答。IEEE 的 802.1X 標準 (Port Based Network Access Control) 提供強而有力的身分辨識與網路存取控制給 802.11 網路。Cisco 在 Extensible Authentication Protocol (EAP) 的原則之下開發了 Lightweight Extensible Authentication Protocol (LEAP) 。Fortress Technologies 的 Air Fortress 是建立於密碼標準，經過 FIPS 140-1 驗證過的安全解答並且提供強大的資料加密給 802.11 網路。無線加密的進化也從 WEP(Wired Equivalent Privacy) → TKIP(Temporal Key Integrity Protocol) → WPA(Wi-Fi Protected Access) → AES(Advanced Encryption Standard)，到最先進的 AES 加密演算法。

802.11 WLAN 安全防護之具體建議

本章所述為一些具體建議讓 802.11 WLAN 更加安全 [6]。

如何安全佈署一個無線網路基本上和佈署任何一個 LAN 是沒有多大區別。我們必須處理使用者的身分辨識，授予和管理委任的特權，稽核所做的行為，決定並管理網路位址如何核發，留意異常的行為，設計網路時做合理的分割來限制對網路敏感部分的存取，保證機密的資訊在運送的途中恰當地加密，以及對系統更改設定來提供只有最少套的服務。大多數的機構迄今還不能有效的處理這些議題。以下是一些証明有效的策略，可以讓公司行號來改善他們的情況。

一、基線評估：

大多數的機構不知道他們已佈署多少無線技術，也不了解它們是怎樣被設定組態。應該使用一個可信賴的第三者來做全面考察以找出並描繪每一個 AP 的特性。只有一個精確的全面考察才能讓你理解你的無線網路安全暴露的程度。

二、無線安全政策：

更新你特別針對無線部分的安全政策。你的目標必須是使無線政策與其配對的有線政策愈趨一致愈好。

三、最好的實作：

恰當地保衛無線環境並不容易但也不是什麼神祕的事物。準備一份二至四頁的簡報文件描述在一個 AP 被附屬到公司網路之前所需做的組態設定改變。

儘管有已知的安全風險，無線環境已經被大量佈署。面對這樣的現實，機構必須採取一些實用的措施使得整個環境儘量做到更安全。美國的 Rutgers 大學就有以下的建議 [7]：

(一) 假如你現有的無線網路沒有半點安全防衛的話，最容易做的事就是賦予它 WPA 或 WEP 的能力。這個方法蘊涵要有一些重要的支援當後盾：你將需要確認所有的使用者皆具備設定於他們系統內獨特的金鑰或通行碼。如果你還用 NIC 的位址做進一步的限制的話，你需要保持有每一位使用者 NIC 位址的名單。

(二) 對比較大的設施，建議在無線網路與其他網路之間安裝一個閘道器，或在企業的節點使用 WPA。請注意無論如何企業的節點裝 WPA 的話，所有的使用者必須具備並且使用 801.1x supplicant 軟體。到底如此做是否不切實際，目前尚無足夠的經驗來辨別。

Figure 4：Consolidated Wireless 802.11 LAN Recommendations

背景	建議
立即的改變	使用 WEP 來加密資料
	改變 SNMP 社群串的預先設定
	改變 AP 服務組套 ID(SSID) 的預先設定
	使網路失去廣播 SSID 的效能
	改變管理者帳戶預先設定的通行碼
改變組態設定	使用 MAC 層的過濾
	把 AP 放在你的 DMZ 裡
	不讓 AP 回答〝刺探 - 回應 (probe-response)〞之類的需求
	使網路失去 DHCP 的能力
天線的活動	全面檢視你的網點
	改變你的 AP 配置來控制覆蓋範圍
	使用方向性的天線
	減少信號強度
發展的活動	使用外部的終端 - 對 - 終端 (end-to-end) 的安全機制
	整合入侵偵測

(三) 在兩者之中任何一個實例，我們建議所有你提供給使用者的服務皆以終端 - 對 - 終端 (end-to-end) 的加密 (譬如 Slosh, 等) 來保護。當你使用企業網路的 Netted 和通行碼來接受他們的服務之時，這是務必的要求。

Figure 4 包含一個統一的 WLAN 安全建議名單 [6]。你必須自己決定那一些建議比較適合你的環境。

結論

現今大部分的機構佈署無線區域網路時，簡直沒有在安全方面下足夠的工夫。這樣做是不對的，但它的確存在這樣的事實。就像在有線世界裡，機關和組織僅會在發生一序列高度引人注目，而且財務上損失慘重的駭客攻擊之後，才會認真看待網際網路安全。同樣地，只有發生一連串類似的公共無線網路災難以後，才會催化機關和組織更嚴肅地了解無線網路安全。

雖然 802.11WLAN 的技術有它固有的一些安全問題，仍然有許多直截了當的安全措施可以減輕這些問題。如同許多新的科技一樣，一個最好的起步方法就是認清問題的所在，而且做一個重大的承諾去對付在你的環境中可以適度地解決的那些安全問題。要腳踏實地，切忌好高騖遠。

※ 參考文獻 / 資料來源：

1. L. Goldberg, "Wireless LANs: Mobile Computing's Second Wave," Electronic Design, 26 June 1995
2. K. Chen, "Medium Access Control of Wireless LANs for Mobile Computing," IEEE Network, September / October 1994.
3. K. Krizman, D. Lough, T. Blankenshi, " A Short Tutorial on Wireless LANs and IEEE 802.11", DLNET-01-22-2003-0127, 1997-05-10
4. Psion Teklogix, " 802.11 WLAN Security ", November 2003
5. Cisco Aironet 1200 Series, " Cisco Aironet Wireless LAN Security Overview " 2002 Cisco Systems, Inc.
6. B. C. Johnson, " Wireless 802.11 LAN Security: Understanding the Key Issues ", 2002 System Experts Corporation, white paper
7. Rutgers University, " Wireless Security Recommendations for Rutgers ", Last update, March 23, 2006

雲端運算服務之資安風險與挑戰

本篇摘自 2011 年 06 月出刊之財金資訊季刊第 67 期，由時任宏碁公司吳文進顧問撰寫。

一、前言

隨著網際網路快速發展，軟硬體技術不斷提升，使用者對於資訊服務的要求越來越高，雲端運算服務各種應用已逐漸在日常生活中實現，使用者可隨時隨地經由網際網路存取雲端的各式服務，企業也不必再投入大量成本，就能享受雲端服務供應商所提供的強大資訊科技運算能力。

然而企業組織在享受雲端服務便利性的同時，卻也存在不可避免的風險。當企業內部資料，甚至機敏資訊都儲存於雲端服務供應商的資料中心，我們不免懷疑：雲端服務供應商是否有足夠能力可以維護客戶資料安全？他們使用什麼機制防範非法存取或破壞？如何確保客戶資料的機密性、完整性與可用性？導入雲端運算服務是否會讓企業身陷資安風險？

因此，企業在導入雲端運算服務或享用其便利性之前，應先瞭解可能發生的資安風險，並經過適切的權衡評估，再決定採行何種導入策略與服務模式，以提升企業組織之競爭力。

二、雲端運算服務的特色

雲端運算服務主要包含兩個面向：一面是前端所提供的服務，另一面是背後涉及的複雜技術，如虛擬化與自動化管理等。換言之，雲端運算是一種透過網際網路分散式運算架構提供服務的模式，具備彈性（Flexibility）與擴充（Scalability）能力，且特別強調分散式運算與平行處理能力。如依較為寬鬆的認定方式，任何在網際網路上提供運算資源和隨選服務者，只要滿足彈性運用和擴充的特性，都屬於雲端運算服務，不一定要完全運用分散式電腦運算架構。

一般而言，雲端運算服務具備以下特性：

(一) 透過網際網路提供服務

電腦軟硬體均被定位為服務資源，提供使用者透過網路，依其自身需求使用。

(二) 資源動態調配

透過開放性技術，將軟硬體抽象化為動態可擴展、可配置的資源，允許使用者透過網路動態取用這些服務與資源。

(三) 分散式虛擬架構

在雲端運算中，資訊系統可能是在遠端的分散式系統上運作，而非當地的單一電腦或伺服器。這種分散式系統由網路相互連接，提供大量而穩定的網路服務給眾多的使用者，使用者不需知道服務從何而來、資料存放何處、資源從何而來。

(四) 依量付費

使用者透過瀏覽器直接使用網路服務，不需瞭解背後資源調配、整合等實際運作狀況。業務的建立、發布、執行和管理都可以透過分散式系統在網路上進行，只需依資源使用量或業務規模付費。

三、 雲端運算服務的類型

雲端運算服務的類型，可依其服務模式或部署方式加以區分。依服務模式可分為軟體即服務 (Software as a Service, SaaS)、平台即服務 (Platform as a Service, PaaS)、架構即服務 (Infrastructure as a Service, IaaS) 三類，分述如下：

(一) SaaS

透過網路提供商業應用軟體的一種新興服務模式，軟體的取得成本與使用方式都跟以往截然不同。以往使用商業應用軟體必須先購買使用權，而在 SaaS 模式下，使用者則是透過網路使用存在提供者端的應用軟體。

(二) PaaS

此模式提供平台服務，如 Google App Engine 或微軟的 Azure 平台。客戶可以將所開發的應用程式很容易地部署到雲端，給開發人員更大的方便與彈性。

(三) IaaS

亦稱為「公用運算」(Utility Computing)，提供客戶租用處理器、儲存體或網路等基礎設施及服務。客戶須能掌控作業系統、儲存體、網路及所部署的應用程式，但不需管理這些基礎設施底層的雲端架構。

雲端運算若依部署方式分類，可分為公有雲、私有雲及混合雲三種，以上任何一種服務模式皆可採用這三種部署方式，使用者則可依需求選擇適合的部署方式。一般而言，中小型企業和創業公司可能較傾向於選擇公有雲，而金融機構、政府機關和大型企業則傾向選擇私有雲或混合雲。這三種部署方式分述如下：

(一) 公有雲 (Public Cloud)

由若干企業和使用者共同使用的雲端運算環境，各使用者共享同一個獨立的雲端供應商提供的資源與服務。

(二) 私有雲（Private Cloud）

由某個企業獨立建構及使用的雲端運算環境，使用者均為企業組織內部成員，共用該雲端運算環境提供的所有資源，外人無法取用。

(三) 混合雲（Hybrid Cloud）

公有雲與私有雲的混合體。一般而言，對於安全性、可靠性與可監控性要求較高的企業組織，都是私有雲的潛在使用者。這些機關的 IT 基礎建設已具相當規模，只需少量投資即能升級現有系統，享有公有雲端運算帶來的靈活度與高效能，同時避免公有雲可能帶來的負面影響。

四、雲端運算服務之安全議題

由於雲端服務的創新運用與雲端運算科技的複雜性，企業在享受雲端服務便利性的同時，也必須面對下列安全議題的挑戰：

(一) 資料的安全性與隱私性問題

資料儲存於遠端雲端資料中心是否安全？會不會發生資料外洩？與其他企業共用伺服器來儲存資料，是否妥當？

(二) 服務效率與可用性問題

雲端服務提供者能否確保傳輸品質與運算效能，並同時兼顧可靠性？畢竟 Amazon、Salesforce.com 等雲端服務提供者均曾發生因當機而導致服務中斷的事件。

(三) 標準性與資料轉移問題

企業如何將既有的軟體或服務轉移至雲端服務提供者？保留在企業端的軟體與雲端服務供應商的服務如何整合？雲端服務供應商之間的服務能否相容？企業能否輕易將軟體由某一雲端服務供應商轉移至其他供應商？

五、雲端運算服務面臨的安全威脅

雲端運算安全涉及資料安全、存取安全、虛擬環境安全與資安監控等問題，就雲端服務的使用者而言，可能會遭遇下列安全威脅：

(一) 儲存於雲端的資料會不會不見？
(二) 雲端資料會不會被竊？
(三) 雲端資料有沒有加密？
(四) 從個人的電腦存取雲端服務是否安全？

(五) 雲端上是否有我的使用存取紀錄？
(六) 是否有其他人可以側錄我儲存於雲端的資料？
(七) 有哪些可能的攻擊手法可以取得我儲存在雲端的資料？
(八) 與他人共享資源，我在雲端的資料是否也被共享？
(九) 退租後，雲端資料是否確實刪除？

另一方面，雲端安全防護聯盟 (Cloud Security Alliance, CSA) 亦提出雲端運算可能遭遇的七大安全威脅，摘述如下：

(一) 濫用或誤用雲端運算服務

雲端運算服務供應商 (尤其是 IaaS 與 PaaS 供應商) 為降低使用門檻，通常不會嚴格審查使用者資料，甚而提供免費使用或試用期，這些方法雖可有效推廣雲端運算服務，卻也容易遭有心分子利用。事實上，已有殭屍程式、木馬程式等惡意資料被放置於雲端運算系統上，使用者若不察而下載安裝，可能會衍生危害。

(二) 不安全的應用程式介面

使用者通常透過使用者介面或應用程式與雲端運算服務互動，這些介面與應用程式會直接影響雲端運算服務本身的安全性，例如：使用者介面的驗證與授權功能是否安全、應用程式的相依性與安全性等，都必須注意。此外，如使用第三方的加值服務，也必須一併考量其介面與應用程式的安全性。

(三) 惡意的內部人員

內部人員所造成的問題是近年來許多組織關注的焦點，採用雲端運算會讓這些問題更加嚴重。使用者無法得知雲端運算服務供應商如何規範管理內部員工，是否有良好的存取管控與監視機制。再者，人員進用條件與程序均屬非公開資訊，是否有駭客、商業間諜或情報人員參雜其間？每天管理維護公司資料的人員會不會成為有心分子眼中待宰的肥羊？惡意內部員工的比例會不會比一般組織更高？

(四) 共享環境所造成的議題

雲端運算服務讓使用者好像擁有各自獨立的環境，但這些環境都是透過虛擬化技術產生的。這些虛擬化平台能否有效隔離不同的使用者，以避免彼此相互干擾而影響服務的正常運作或是避免彼此可以存取對方的資源，這些對於雲端運算的安全都是嚴峻的挑戰。

(五) 資料毀損或洩漏

資料毀損或洩漏對組織的影響，不僅止於實質的金錢損失，賠上的更是企業形象，如近期 SONY 接連發生兩次，累計超過一億筆的資料外洩事件，部分專家評估認為這可能是足以讓公司瀕臨倒閉的危機。而雲端運算服務的特色則使資料毀損或洩漏的問題更形嚴重，舉凡 AAA 機制（驗證、授權、稽核）是否完備、加密技術是否有效、如何滿足資料持續性需求、如何安全刪除資料，甚或災難復原、司法管轄問題等，都是必須考量的重點。

(六) 帳號或服務被竊取

帳號或服務被竊取的問題由來已久，在雲端運算環境更加嚴重。雲端運算不像傳統 IT 架構擁有實體，一旦帳號或服務被竊用，除非有其他方式佐證，惡意分子可以完全取代原先使用者的身分。而在傳統 IT 環境中，使用者至少還擁有硬體的控制權，即使發生帳號或服務被竊的狀況，也可採行事後補救措施，這些補救措施在雲端運算架構下卻未必適用。對於那些直接暴露於網際網路上的公開雲端運算服務，帳號或服務被竊取的發生率也會大幅提高。

(七) 未知的風險

就安全而言，「未知」猶如芒刺在背。不論是 IaaS、PaaS 或 SaaS 模式，都將雲端運算服務包裝成一個使用者不需瞭解、也無法了解的系統。使用者只要專注於「如何」及「方便」使用系統，至於網路架構、安全架構、軟體版本、與誰共享基礎建設或平台等資訊，可能無從得知，也就無法採取適當的監控措施。

六、結論

雲端運算服務不是新技術，而是一種新的運用，一旦資料進入未知的雲端，資料移動的特性將使傳統防護邊界消失，不僅機敏資料外洩的風險大幅升高，還須考量資料存取、虛擬環境安全、資安監控與隱私權等各種安全議題。國內「個人資料保護法」已修正公布，法務部與各目的事業主管機關正研訂施行細則中，未來這些條文內容都可能成為檢視雲端運算服務是否落實資安的依據。各企業組織導入雲端運算時，應充分瞭解可能衍生的資安威脅與風險，多方評估考量，選擇適切的服務模式，使資訊科技真正成為企業組織永續營運的助力，以提升企業組織的競爭力。

從「金融機構辦理電子銀行業務安全控管作業基準」談網路銀行服務之安全機制

本篇摘自 2011 年 09 月出刊之財金資訊季刊第 68 期，由時任財金資訊公司安控部資訊安全組黃偉倫高級工程師（現任為組長）撰寫。

一、 前言

目前我國對於金融機構辦理網路銀行服務具體應備之安全控管措施，並未訂定法律位階之作業標準，金融機構主要係以中華民國銀行商業同業公會全國聯合會 (以下簡稱銀行公會) 研擬並陳報主管機關核准之「金融機構辦理電子銀行業務安全控管作業基準」(以下簡稱安控基準)，為實施安全控管之準則。

隨著網際網路環境與技術快速發展，網路銀行逐漸成為提供金融服務之主要介面之一。由於網路攻擊與威脅日新月異，金融機構面對之資安風險已今非昔比，安控基準自民國 (以下同) 88 年公布以來，亦配合實際作業狀況修訂多次。現行最新版本係銀行公會金融業務電子化委員會資訊安全組技術分組於 99 年 8 月彙集會員銀行意見所修訂，經提報行政院金融監督管理委員會 (以下簡稱金管會)，銀行局於 99 年 8 月 31 日以金管銀國字第 09900311870 號函囑銀行公會所屬會員機構配合辦理。

本文將歸納解析安控基準對於網路銀行服務 (包含 Web ATM) 之安全規範內容，以供初次涉獵安控基準者參考。

二、 安控基準與木桶理論

資訊安全領域常引用木桶理論 (Cannikin Law) 來說明資安風險常發生於整體安全防護最脆弱之一環：傳統木桶係由數片木板 (防護措施) 緊密結合而成，木桶所能容納之最高水位 (安全強度) 取決於長度最短 (防護最弱) 之木板，若桶內水位 (資安風險) 持續升高，桶內的水將從木板最短處溢出 (產生資安事件)。

本文將安控基準對於網路銀行之安全控管要求歸納為「區分交易類別」、「交易安全」、「資料傳輸安全」、「認證安全」、「主機端安全」及「客戶端安全」六大面向，若套用前述木桶理論，「區分交易類別」或可視為從源頭降低木桶之進水量 (降低攻擊之誘因)，而其他五項則是維持桶內水位，防止溢出之木板，長度 (安全強度) 必須充足而一致，並緊密結合，才能有效保障網路銀行之交易安全。

三、網路銀行之安全需求

(一) 區分交易類別

經由區分交易類別，限制交易金額與筆數，減少駭客藉由攻擊所可獲取之非法利益，進而降低遂行攻擊之誘因，實為降低網路銀行交易風險最有效的措施之一。

安控基準係依交易指示執行結果對客戶權益之影響程度來區分交易風險之高低，對於提款、轉帳、消費等直接影響客戶權益之電子轉帳及交易指示類交易，除約定帳戶轉帳或約定及限定性繳費、繳稅外，若經由網際網路進行非約定帳戶之資金移轉，則經由每筆限額五萬元、日限額十萬元及月限額二十萬元等方式，降低交易風險。

金管會於 93 年指示各金融機構關閉網路銀行 (以帳號與密碼登入) 之非約定轉帳功能，僅允許以網路 ATM 進行交易。為降低詐騙發生率，94 年更要求金融機構設定單筆非約定轉帳金額上限為三萬元。金融機構若採行提升認證機制強度 (如 OTP) 等強化措施，可經核准酌情提高非約定轉帳金額上限。

(二) 交易安全

1. 一般性原則

銀行公會基於金融機構共通業務需求所研擬之電子資料交換介面，其安全需求係以安控基準為基準。安控基準針對不同的交易類別 (風險高低) 與傳輸途徑，分別規定應否採行訊息隱密性 (Confidentiality) 、訊息完整性 (Integrity) 、訊息來源辨識 (Authentication) 、訊息不可重複性 (Non-duplication) 、無法否認傳送訊息 (Non-Repudiation of sender) 與無法否認接受訊息 (Non-Repudiation of receiver) 等六項防護措施。如屬經由網際網路傳輸之高風險交易，前述防護措施皆為必要。

2. 系統應辨識外部網站及其所傳送交易資料之訊息來源及交易資料正確性

為因應網路購物、拍賣網站交易衍生之付款需求，金融機構常與電子商務業者合作，提供消費者使用金融支付工具進行付款或轉帳。針對這種未與金融機構直接連線，而是透過外部網站中介轉送交易指示之模式，安控基準特別規範收單銀行應比照銀行間訊息交換之安全需求，檢核外部網站轉接處理之交易訊息來源 (來源端認證) 與資料 (訊息完整性)。

3. Web ATM 端末設備查核碼

端末設備查核碼之設計自磁條金融卡時代即已具備，其原意係提供代理銀行確認交易訊息來自合法之端末設備。代理銀行通常使用預存於實體端末設備 (如 ATM) 內之金鑰，以押碼運算產製端末設備查核碼，以進行端末設備認證。

Web ATM 交易訊息由客戶端個人電腦產生，不適用上述驗證方式，因此各代理銀行改以固定值、遞增序號、隨機變數等方式實作端末設備查核碼。然而不論是固定值或遞增序號，客戶端皆可預先推測合法之端末設備查核碼，並以合法卡片離線非法產製多筆合法之交易驗證碼 (Transaction Authentication Code, 簡稱 TAC) ，後續不需卡片即可利用這些預存之交易驗證碼進行非法交易。為降低此風險，安控基準特別要求系統應針對每一筆晶片金融卡交易，動態產製隨機變動之端末設備查核碼。

4. **進行帳務性交易時，系統應每次輸入卡片密碼產生交易驗證碼**

交易驗證碼係晶片金融卡使用發卡行預存於卡片內之多樣化 (個人化) 金鑰，針對交易重要資訊 (如帳號、金額) 進行密碼學運算所產生，可供發卡銀行確認交易之來源辨識性 (合法卡片) 與完整性 (交易未經竄改) 。晶片金融卡收到來自端末設備 (ATM、POS、讀卡機等) 之產製交易驗證碼指令時，必須先檢核持卡人密碼是否已通過驗證，發卡銀行方可確認該交易指示是由合法的持卡人 (持有晶片密碼) 以合法的晶片金融卡 (發卡行預存之金鑰) 所產生。

然而依現行晶片卡設計，若晶片記憶體已註記持卡人通過密碼驗認，除非電源供應中斷，此狀態將維持有效。若持卡人完成交易後未及時取出卡片，惡意人士或程式即可趁機進行非法交易。因此，安控基準要求網路 ATM 應用程式應針對每筆帳務性交易，要求持卡人重新輸入密碼，而網頁應用程式於每筆交易完成後，應以重置 (RESET) 卡片或中斷卡片電源供應等方式，清除晶片記憶體之持卡人密碼驗證狀態。

5. **人工確認交易內容**

安控基準要求非約定轉帳或高風險交易「須於載具上經由人工確認後，才傳回交易驗證訊息」，以 WebATM 交易而言，實務上可透過卡片拔插或使用確認型讀卡機，由使用者確認交易內容後，人工放行以進行交易。由於惡意程式無法驅動卡片產生實際卡片拔插行為，可以有效防堵軟體攻擊行為，各金融機構皆已將卡片拔插列為產製交易驗證碼前之必要動作。使用確認型讀卡機則是較卡片拔插更為安全之人工介入機制，銀行公會認證之確認型讀卡機皆經程式碼檢核，確保無後門程式，並限制程式碼須寫入光罩唯讀記憶體 (MASK ROM)，以防竄改，可以提供最可靠之人工確認機制。若配合良好之使用習慣，落實確認讀卡機顯示之訊息內容，將是保障 Web ATM 交易安全之終極防線，值得強力推薦。

(三) 資料傳輸安全

安控基準要求經由網際網路公開傳輸之網路銀行交易，必須確保資料之隱密性，目前金融機構大多應用 TLS/SSL 技術維護客戶端瀏覽器與金融機構網站主機間之資料傳輸安全。TLS/SSL 可確保交易資料之隱密性、資料傳輸之完整性、網站主機之來源辨識性與不可否認性，是目前公認較為安全且廣泛使用之安全機制。

由於 TLS/SSL 加密運算所使用之演算法係客戶端與主機端雙方於通訊過程中所議定，若演算法強度較弱，可能會降低加密保護之強度。因此，金融機構可考慮限定主機僅支援強度較高之加密演算法，以維持加密通道之強度於可接受之水準。網路銀行客戶亦應建立檢視網站 TSL/SSL 憑證有效性之良好使用習慣，以確保連線安全。

(四) 認證安全

客戶認證機制是網路銀行交易安全之關鍵因素，傳統使用帳密 (帳號＋密碼) 認證之網路銀行，由於安全強度較低，僅限提供低風險交易之服務。對於使用者登入網路銀行之帳號 (用戶代號) 與密碼，安控基準訂有原則性規範，例如：長度 (位數) 限制、英數字元限制、不得使用客戶顯性資料、錯誤次數限制、首次登入變更密碼及定期變更密碼等。

網路銀行如欲提供低風險非約定轉入帳戶轉帳或高風險交易，就必須增設多因素認證機制，亦即於交易過程中，使用具兩項 (含) 以上技術設計之認證機制。以 Web ATM 為例，客戶必須同時持有卡片及卡片密碼方能進行交易，即為多因素認證機制之應用實例。

由於 Web ATM 客戶端須額外安裝晶片讀卡機與金融機構之客戶端元件程式，使用上稍嫌不便，部分金融機構另行增設利用離線載具或行動電話傳送之一次性密碼 (One Time Password，簡稱 OTP) 機制，以加強客戶認證機制強度，亦屬多因素認證之實作案例。

(五) 主機端安全

以往主機端之安全措施多著重於網路環境防護與作業系統弱點修補，然而網頁應用程式之安全才真正是網路銀行服務最大挑戰。依安全弱點之發展趨勢，屬於網頁應用程式之安全弱點已超過網路應用整體弱點總數一半以上，近年來，安控基準之修訂亦著重於網頁應用程式防護之強化。

1. 主機設備安全

為維護金融機構電腦資源之隱密性、完整性及可用性，防範外部入侵威脅與破壞，安控基準針對管理面所訂定之應辦理措施包含：網段隔離、入侵偵測與防禦、重要參數檔加密、病毒偵測軟體、弱點掃瞄與修補、系統漏洞修補、密碼定期更換等。

2. 網頁應用程式安全

(1) 人工介入機制

對於低風險非約定轉入帳戶轉帳或高風險交易，安控基準要求應設計圖形驗證碼 (GOTP，Graphic One Time Password) 、隨機按鈕、動態頁面等方式，執行人工介入機制。目前各網路銀行實作以前二項較為常見。

圖形驗證碼 (英文學名 CAPTCHA, Completely Automated Public Turing Test To Tell Computers And Humans Apart) 之設計原意在於防止有心人士利用機器人 (Bot) 散播垃圾留言及廣告 (Spam)，應用於網路銀行則可防止惡意程式逕送假交易或進行阻斷 (DoS) 攻擊。

隨機按鈕係以動態隨機方式配置輸入按鈕，防止惡意程式藉由側錄使用者點選之行為，取得使用者輸入之資訊。目前網路銀行對於密碼輸入方式之設計，除採用隨機按鈕外，亦多要求使用者以滑鼠點選取代鍵盤輸入，以防範鍵盤側錄工具 (keystroke logging) 之覬覦。

(2) 載具密碼不應於網際網路上傳送

以晶片卡進行使用者認證之網路銀行服務 (如 Web ATM)，使用者由網頁輸入之密碼僅供離線認證之用，並無網際網路傳輸之需求。惟部分網頁應用程式疏於注意，曾發生密碼於網際網路上傳輸之情形 (以 asp.NET 程式開發為例：將密碼輸入欄位設計於 webform 控制項內，於觸發 postback 事件時傳回)；雖然密碼於網際網路傳輸過程遭竊，不致直接造成損失 (仍須持有卡片，方能合法交易)，惟安控基準仍要求金融機構不得傳輸。

(3) **系統應設計連線 (Session) 控制及網頁逾時 (Time Out) 中斷機制**

利用連線控制機制，網頁應用程式可識別來自同一使用者、不同網頁之請求訊息，以進行適當之處理。連線識別碼 (session ID) 應選用足夠長度之隨機亂數或字串，降低駭客以嘗試 (trial-and-error) 或暴力 (brute force) 方式取得或預測有效之連線識別碼，遂行其偽冒攻擊行為。網頁應用程式之開發應儘量使用開發工具提供之連線管理機制，以避免自行設計連線控制時，因思慮不周而衍生漏洞與弱點。

網頁應用程式應設計適當之逾時中斷機制，避免因閒置時間過長，非法人士或惡意程式趁虛而入進行非法交易。目前提供 Web ATM 服務之銀行，除網頁皆已設計逾時中斷機制外，亦針對拔插卡片等人工介入過程設定逾時中斷機制，確定使用者在限定時間內完成流程，以確保 Web ATM 交易之安全。

(4) **系統應辨識客戶輸入與系統接收之非約轉交易指示一致性**

BHO (browser helper object) 係由微軟公司提供，於開發網頁程式時可以延伸瀏覽器功能之一項技術，目前常見的 yahoo 工具列、google 工具列或網頁翻譯等瀏覽器外掛功能，大多利用此技術追蹤使用者瀏覽網頁之行為，並依使用者需求，修改輸入資料或網站回應之輸出內容。此技術如遭惡意程式濫用，就可在使用者渾然未覺的狀況下，竄改網路交易資訊之內容 (如轉入帳號) 。

為防範 BHO 類型之中間人 (man-in-the-middle) 攻擊，使用者可以關閉 BHO 功能 (合法功能亦同時停用)，或以白名單方式檢核輸入資料之合法性 (如正面表列可接受之轉入帳號) 等。另一方面，網頁程式開發人員可自行撰寫使用者輸入之介面 (UI) 元件，並適當保護 (押碼或加密) 所輸入之資料，使 BHO 元件無法暗中竄改交易內容。

(5) **系統應避免存在網頁程式安全漏洞 (如 Injection, Cross-Site Scripting)**

Open Web Application Security Project (開放 Web 軟體安全計畫，簡稱 OWASP) 是極具公信力之全球非營利組織，OWASP 之主要目標係研議協助解決 Web 軟體安全之標準、工具與技術文件；依其統計資料顯示，注入 (Injection) 攻擊與跨網站腳本 (Cross-site scripting，簡稱 XSS) 攻擊分居 2010 年十大網頁應用程式風險排行榜第一、二位，是威脅網頁應用程式最嚴重之二種攻擊行為。

注入攻擊依其攻擊標的而有不同類型，最常見的是針對資料庫之 SQL Injection，有此弱點之網頁應用程式通常未確實檢核使用者輸入資料之合法性，攻擊者可經由合乎 SQL 語法，但內容不合理之查詢條件，對後端的資料庫進行逾越權限之存取行為，如讀取或竄改敏感性資料。近年來，這種攻擊行為更發展出編碼等變形方式，以規避輸入資料之合法性檢核。為降低攻擊風險，網頁應用程式之設計應注意相關安全事項，例如：避免使用最高權限帳號 (如 sa) 查詢資料庫、避免回應完整之資料庫查詢錯誤資料、針對使用者輸入資料進行格式合法性檢核、輸入時過濾特殊字元 (如 '、--、;、@ 等) 、利用預儲程序 (store procedure) 取代以網頁組合之 SQL 查詢指令等。

跨網站腳本攻擊亦有多種類型，而利用網站弱點將惡意連結植入網頁則是最受駭客青睞的方式。若使用者登入被植入惡意連結之合法網站，可能會被誤導而連線至惡意網站，下

載並執行惡意程式，引狼入室，造成敏感資料外洩。由於此弱點係網頁應用程式開發疏忽所致，落實客戶端傳回資料之合法性檢核，才是釜底抽薪的防禦之道。

(6) 系統應偵測網頁與程式異動，進行記錄與通知措施

本項要求旨在確保網頁及其相關應用程式之完整性，對於來自外部之網頁竄改 (如 XSS 攻擊)、來自內部的合法或非法程式過版與修改，皆應建立稽核軌跡留存及異動偵測之機制。實務上，有些網路銀行會定時 (每隔數分鐘) 進行網頁內容之雜湊值 (hash) 運算比對，以確認網頁內容之完整性。

(六) 客戶端安全

客戶端安全是網路銀行服務安全之關鍵，卻也是金融機構最難以企及者。金融機構對於自行佈建之自動化櫃員機、端末機等實體通路設備，大多具備健全之安全管理機制；然而對於網路銀行、Web ATM 等虛擬通路之應用，金融機構僅能提供必要元件與軟體，由客戶自行安裝，無法掌握其電腦環境之安全性。若客戶端電腦遭受惡意程式入侵，仍有交易資料遭竄改或外洩之風險。為保障交易安全，金融機構應落實安控基準關於客戶端元件之相關規定，並提醒及加強使用者應有之安全認知。

1. 元件應驗證網站正確性

客戶端元件收到交易指示時，應確認使用者係連線至合法網站，並取得來自合法網頁之訊息，以維資料之來源辨識性或完整性。網頁應用程式須配合提供相關之安全設計，將資料傳輸至客戶端元件處理時，可利用事先設計之識別與認證機制，如網址 (URL) 比對、預埋金鑰驗證、設計挑戰與回應 (challenge-response) 等，確保資料傳輸之完整性。

2. 元件應採用被作業系統認可之數位憑證進行程式碼簽章 (Code Sign)

安控基準要求金融機構之客戶端元件應經過程式碼簽章，以供使用者確認下載元件之合法來源。金融機構應維持元件簽章憑證之有效性，而網路銀行客戶在下載網路銀行元件時，應確認元件簽章憑證之有效性，以確保自身之權益。

3. 元件應設計存取卡片時限定為獨占模式

若客戶以晶片卡為網路銀行服務之交易載具，必須先下載金融機構提供之客戶端元件。安控基準要求在交易流程中，客戶端元件對於晶片卡之存取行為 (如密碼驗證、交易驗證碼產製) 應採獨占模式 (以 PC/SC API 為例，使用 SCardConnect 函式之 scard_share_exclusive 參數)，以防其他應用程式存取晶片卡。設定獨占模式之期間，至少應起自持卡人密碼驗證，全程維持至產生交易驗證碼後，晶片電源供應中斷為止，以避免其他應用程式利用持卡人密碼已通過驗證之狀態，非法產製交易驗證碼。

四、結語

隨著網路銀行應用普及，使用者接受度提高，經由金融機構網際網路服務進行理財及資金調撥之交易量節節攀升，以Web ATM為例，99年跨行交易量已達2千萬筆，交易金額超過新台幣4千億元。為因應資安威脅，降低駭客攻擊風險，銀行公會特別修訂安控基準內容，期能為網路銀行交易安全之縱深防禦建立原則性規範。金融機構應落實網路銀行服務之各項安控需求規範，並維持相當且一致之安全強度，防範資安風險發生於防護措施最脆弱之環節 (weakest link)。

近年來，報章媒體偶有針對網路銀行安全性之質疑，雖多屬概念驗證 (proof of concept) 性質，並無實質損害之明確案例，然其中不乏因未落實安控基準要求或防護強度不足所致，難免會影響民眾對於使用網路銀行之信心。金融機構建立網路銀行防護措施時，除將安控基準納入考量 (due care) 外，對於各項防護措施之有效性，更應持續地關注並適時補強 (due diligence)，以期及時因應網際網路日新月異之威脅與攻擊，降低交易風險。

※ 參考文獻 / 資料來源：

1. 中華民國銀行公會「金融機構辦理電子銀行業務安全控管作業基準」民國99年8月

異地備援之重要性及現況分析

本篇摘自 1999 年 10 月出刊之財金資訊季刊第 6 期，由時任 IBM 公司資訊服務暨產品支援事業部郭健男高級資訊工程師撰寫。

處在資訊科技的環境裏，企業對資訊作業的依賴日益密切，當企業追求永續經營的目標時，不停頓的資訊系統將成為企業保存其命脈的保護傘。異地備援建置就是提供企業永續經營的解決方案。

美國明尼蘇尼大學的研究報告指出，若企業在 14 天之內無資訊作業，則 75% 的企業業務會停頓，43% 的企業無法在 14 天後重新開張；而在度過無資訊作業的 14 天後，仍能繼續營業者，會有 29% 的企業在兩年之內倒閉。

沒有人會懷疑我們是處在資訊科技的環境裏，隨著電腦的進步及相關應用的多元化，我們依賴電腦作息的程度也隨之升高。根據美國 Contingency Planning Rearch Inc. 在 1996 所發表的研究報告顯示，航空公司的定位系統若中斷一小時，則該公司每小時損失 89,500 美元，銀行 ATM 每中斷一小時則損失 14,500 美元，證券商中斷一小時損失 6 百 45 萬美元，信用卡公司中斷一小時損失 2 百 60 萬美元。

處在資訊科技的環境裏，企業對資訊作業的依賴日益密切，當企業追求永續經營的目標時，不停頓的資訊系統將成為企業保存其命脈的保護傘。

資訊備援方式不一

資訊備援能保護當主中心資訊機房遭到天然災害或者人為破壞時，第二中心仍保有企業運作的資訊系統，針對一些提供即時服務的行業 (例如銀行、證券商、航空訂位服務等)，亦能在 2-4 小時之內回復主中心營運的作業，防止企業的直接與間接的損失，確保企業的永續生存。

同地與異地備援功能比較

	功能及特色	相關設備 (含主機、磁碟機、網路及相關維護費)	投資	優缺點
一、同地溫備援	1. 備援主機平日不開機或與測試開發主機為同一部 CPU, 營運主機無法操作時, 開啟備援主機接續作業 2. 單一套資料庫及程式庫 3. 營運作業回復時間約 30 min	1. 第二部備援主機 2. 與營運主機共享磁碟機與網路設備	低	優點: 1. 投資低 2. 人員, 設備, 程式及資料維護容易 3. 資料遺失率低 缺點: 1. 當區域性災害發生時, 所有設備無法繼續作業
二、同地熱備援	1. 備援主機開機 Standby 營運主機之運作, 伺營運主機發生狀況時, 取代營運主機之運作. 2. 單一套資料庫及程式庫 3. 營運作業回復時間約 10 min 4. 備援系統與測試開發系統均在同一部 CPU 上	1. 第二部備援主機 2. 與營運主機共享磁碟機與網路設備 3. 需額外支出備援主機之軟硬體維護費	中低	優點: 1. 營運系統享受高使用度之系統資源, 資料遺失率低. 2. 人員, 設備, 程式及資料維護容易 缺點: 1. 當區域性災害發生時, 所有設備無法繼續作業
三、同地平行處理	1. 二台(含)以上之主機共同處理交易資料, 當其中某主機當機時, 其他主機仍處理所有的交易, 使用者享受高可靠性之不當機系統 2. 單一套資料庫及程式庫	1. 需具備第二部(含)以上之平行處主機及相關設備 2. 共享磁碟機與網路設備 3. 需額外支出備援主機之軟硬體維護費	中等	優點: 1. 不停頓之系統作業, 資料遺失率非常低 2. 當需要增加處理能力時, 可增購主機連結至現行平行主機群, 可不需汰換現行主機. 缺點: 1. 當區域性災害發生時, 所有設備無法繼續作業
四、異地熱備援	1. 第二部主機於遠端接收主中心已完成交易之 LOG, 並對遠端的複製資料庫作同步更新, 以達到兩邊之資料庫幾乎同步之狀況. 2. 兩套同步之資料庫與程式庫 3. 營運作業回復時間約 1-2 小時 4. 與同地備援搭配建置, 以針對不同狀況發生時, 採取不同之備援方式與程序.	1. 需具備第二部(含)以上之異地備援主機及相關設備 2. 兩套磁碟機與網路設備 3. 額外支出備援主機之軟硬體維護費 4. 需投資雙中心之網路連線設備	中等	優點: 1. 具備區域性災害備援能力, 確保企業永續經營. 2. 可利用備援中心之系統資源執行與主中心不同之業務. 缺點: 1. 第二中心若無執行其他業務, 則系統資源有浪費之虞. 2. 第二中心若不設專職人員維護, 則人力支援較不易.
五、異地平行處理	1. 觀念與同地平行處理相同, 惟其他平行主機座落於其他地區 2. 主機間聯繫需較高之網路頻寬, 且兩中心之間有距離之限制	1. 需具備第二部(含)以上之平行處理主機及相關設備 2. 兩套以上的磁碟機與網路設備 3. 額外支出平行主機之軟硬體維護費 4. 需投資中心間之網路連線設備	高	優點: 1. 具備平行處理與部份異地備援之雙重優點 2. 未來之趨勢 缺點: 1. 投資非常高, 2. 技術尚未完全成熟
六、異地多中心相互備援	1. 各中心各執行不同之業務, 若某中心面臨區域性災害, 則將其業務移至其他中心繼續運作. 2. 使用者多為跨國(州)性之大型企業, 一般而言, 其中心均搭配同地備援設施.	1. 各中心維持獨立運作之必要資源, 包括機器, 辦公室, 維護與開發人員.	非常高	優點: 各區域中心除執行不同業務外, 尚能互相備援. 缺點: 投資非常高

異地備援建置

異地備援有其不可抹煞的優點，但投資也是相當可觀，異地備援要達到主、副中心相同之服務品質，兩邊之軟、硬體必須完全一樣，且須投入可觀的網路連線設備與通訊費用。

茲介紹異地備援建置完整的解決方案

1. **規劃階段**

了解業務風險評估及備援暨災害復原之需求，其工作項目包括：

- 檢討意外災害計畫政策
- 業務風險評估
- 業務衝擊分析
- 檢討意外災害回復計畫
- 備援容量評估
- 可行性備援方案

2. **準備階段**

根據規劃階段所決定之需求，配合災害復原政策目標，設計出備援及災害回復之藍圖並加以測試其可行性，在這一個階段中主要的工作項目包括：

(1) 設計意外災害回復計畫
(2) 設計意外災害備援與回復之演練及測試

3. **建置階段**

專業人員將開始構築安裝備援及災害回復系統，從機房的配備、空調、高架地板、供電系統開始，硬軟體的安裝，網路架設均為先期作業的必要步驟，其後主系統與備援系統之間的檔案資料同步和系統運轉狀況監視，為整個建置工作中技術要求最高的階段，而當切換演練作業手冊的概訂修正與教育訓練均需達一定的程度才可視為本階段完成。

4. **演練及檢討階段**

建置工作完畢後，已可確定備援中心的有效性，隨時演練與檢討將能有效地維持第二備援中心的功能。

永續經營的解決方案

日本銀行界的備援趨勢，已由同地熱備援加上異地溫備援 (註 1) 的作業形態轉換成同地平行處理加上異地熱備援的作業形態，而目前台灣地區之金融業是以同地冷或熱備援，再輔以委外的 BRS(Business Recovery Service) 服務為主。但國內一些大型的行庫，如郵政儲匯局，華南銀行，合作金庫，上海商銀，第一銀行，台灣中小企銀，基於對高使用度的資訊作業的殷切需求，已積極在建置其異地備援中心。

迎向未來的電子商務時代，可預見的是企業對資訊作業的依賴會日益密切，如何確保企業資料的完整性與資訊營運工具的高使用度，將會是企業經理人必需面對的嚴肅課題，而異地備援建置就是提供企業永續經營的解決方案。

註 1：異地溫備援，類似 IBM BRS 作業，在異地建置第二中心機房，平日此機房已建置基本設施，如主機、磁碟機、通訊設備及線路、電源、冷氣 .... 等，且將每日之備份磁帶運往該處，伺主中心有狀況時，在第二中心再安裝必要之資訊系統。


Focus 專注．專業 @ Innovation 創新．引導 @ Security 安全．穩健 @ Convenience 便捷．服務

法令遵循篇

標準領航 企業標竿

本篇摘自 2013 年 04 月出刊之財金資訊季刊第 74 期，由時任財金資訊公司安控部陳昌脩協理（現任為業務部協理）、安控部資訊安全組黃偉倫副組長（現任為組長）、業務部林國良協理（現任為副總經理）、業務部徐憶玫經理撰寫。

一、 前言

財金資訊公司 (以下稱財金公司) 為我國金融資訊系統與交易處理之樞紐，爰肩負提供金融機構及社會大眾「便捷的金流服務」、「穩定的作業系統」及「安全的交易環境」之重任，配合政府政策、金融業務發展情勢、以及社會大眾的需要，秉持「專業、創新、安全、便捷」之經營理念，致力於金融資訊系統之安全與穩定運作、提升服務效能及推動優質金流服務。

為確保跨行交易之互通性及相容性，與金融機構協力發展各項跨行服務，並依金融產業特性制定多項共用性標準，同時更參採國際規範，不斷力求公司管理制度標準化，建立作業品質、資訊安全、業務持續運作及個人資料保護等管理制度，並落實 PDCA (Plan-Do-Check- Act) 運作機制，持續改進作業流程，以維持系統之穩定與安全。本文謹就財金公司跨行業務，包括通匯業務、自動化服務機器 (Automated Teller Machine，ATM) 共用業務及其衍生性支付業務等核心系統，導入標準化制定成為領域標準、標準化推動對領域擴散之影響性及績效，以及引領金融產業標準化之推動獲頒「全國標準化獎」之肯定，臚列於后。

二、 標準化範疇與制定

(一) 標準化推動之範疇

1. 跨行交易處理及結 (清) 算作業標準化

財金公司所規劃、建置及維運之跨行金融資訊系統，乃屬提供多元支付服務的金流服務平台，連結中央銀行及全體金融機構 (包括本國銀行、外商銀行、郵局、農漁會、信合社等 390 家金融機構及其 6,300 家分支機構與遍佈全國的 26,524 台 ATM)，構成金融機構匯款與自動化服務機器服務的綿密網絡；也連結中央銀行國庫局、財政部財政資訊中心、國庫署等政府機關，完成多項庫款收支之自動化作業；並與 VISA、MasterCard、JCB、銀聯等國際卡組織網路介接，藉由提供國際收支服務，擴大國內金流市場的網路延伸至海外通路；同時，尚連結關貿網路、中華電信等網路及電信服務公司，以及繳費 (稅) 委託單位，以肆應民眾繳費 (稅) 支付自動化服務的需要；此外，更連結了加值網路業者，提供金融機構的企業資金調度服務，顯見已建構出一個標準化的金融資訊系統跨體系之整體金流服務平台，如圖 1 所示。

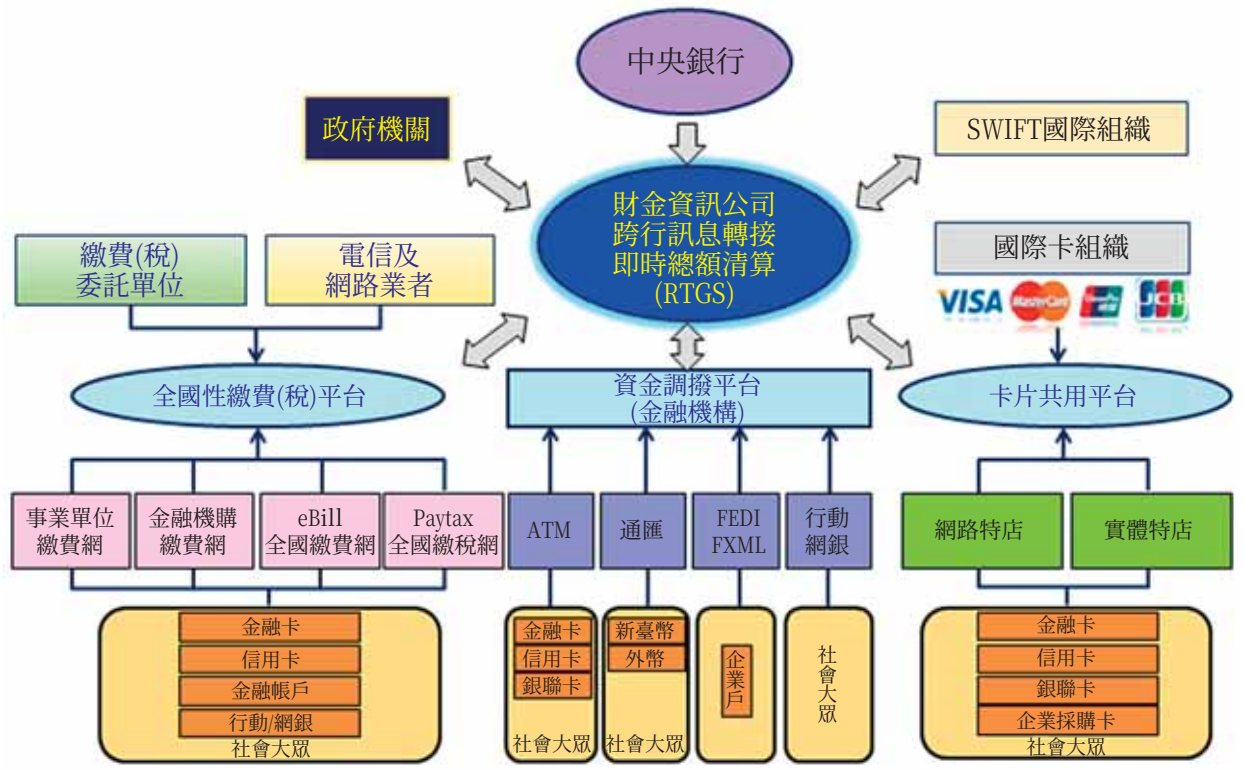


圖 1　金融資訊系統跨體系金流服務平台

本金流服務平台之核心，係源自中央銀行的清算機制，中央銀行為國內金融機構資金調撥之總樞紐，以「同業資金調撥清算作業系統」處理金融機構間資金撥轉及跨行清算基金部位調整，並辦理最終清算。

財金公司則在中央銀行的許可及金融監督管理委員會的監管下辦理跨行服務。在此核心體系所發展之「金融資訊系統跨體系金流服務平台」，連結了中央銀行、全體金融機構及相關維運單位，並整合：(1) 資金調撥平台、(2) 全國性繳費 (稅) 平台、及 (3) 卡片共用平台之功能，採「即時總額清算機制」(RTGS, Real Time Gross Settlement System)，且每日按時完成金融機構間帳務核對及與中央銀行清 (結) 算作業；即當支付指令被系統接受之同時，立即逐筆清算，金融機構須存放適足的跨行基金，交易才能順利完成，不但維持支付作業的順暢，也有助於避免個別支付的延遲，更降低整體支付系統流動性的風險。茲將此即時、安全與可信賴的跨行交易處理及結 (清) 算作業標準化的跨體系服務，分就三大功能平台扼要說明於后：

(1)　資金調撥平台

整合金融機構通匯、ATM、FEDI、FXML、網路銀行及行動銀行等電子支付服務，建構「資金調撥平台」，提供社會大眾運用金融機構所提供之資金調撥工具，辦理匯款、提款、轉帳、帳戶餘額查詢、付款轉帳等資金支付需求。

(2) **全國性繳費 (稅) 平台**

「全國性繳費 (稅) 平台」連結政府機關、金融機構、電信與網路業者及事業單位，支援各類型支付工具，提供線上帳單查詢及繳納費稅服務，社會大眾可透過事業單位、金融機構、全國繳費網、全國繳稅網或繳費稅委託單位等通路繳納費稅，安全又便捷。

(3) **卡片共用平台**

藉由「卡片共用平台」協助金融機構發展卡片業務，降低金融體系的系統建置成本，共同推展卡片支付 (塑膠貨幣) 服務，並與 Visa、MasterCard、JCB 及中國銀聯等國際組織介接，將金流服務拓展至國際，提供國內外持卡人在臺刷卡消費及 ATM 取現服務，活絡消費市場。

2. **內部管理作業標準化**

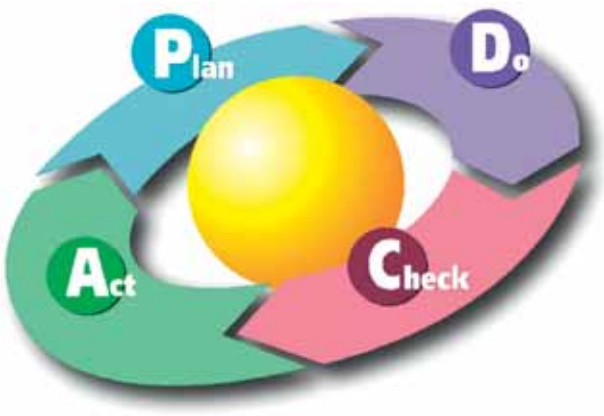
財金公司內部制訂管理系統規範及相關標準化文件，包括：(1) 資訊安全管理系統；(2) 品質管理系統；(3) 業務持續運作管理系統；及 (4) 個人資料管理系統等標準化，同時依國際清算銀行 (Bank for International Settlements, BIS) 支付及清算系統委員會 (Committee on Payment and Settlement Systems, CPSS) 所發布之「重要支付系統核心準則」，辦理通匯業務「核心準則」遵循性之「自我評估」作業，以符合重要支付系統「核心準則」之要求。

(二) 標準化組織、制度規章及運作機制

1. **組織及管理系統運作機制**

財金公司以「金融交易安全不鬆懈、系統運作穩定不中斷」為要務，除恪遵相關法規之規範外，亦導入並整合：(1) ISO 9001 品質管理；(2) ISO 27001 資訊安全管理；(3) BS 25999 業務持續運作管理；及 (4) BS 10012 個人資料管理等多項國際標準之管理機制，融入公司內部各項作業活動規範中，訂定相關標準化文件，包括了資訊安全管理、品質管理、業務持續運作管理及個人資料管理等標準化作業流程。標準化運作機制分為規劃 (Plan)、實施與運作 (Do)、監督與查核 (Check) 及維護與改進 (Act) 四個構面循環運作，持續改善、提升及精進內部作業流程 (請詳「標準化運作機制及管理承諾」如圖表 1 所示)。

圖表 1　標準化運作機制及管理承諾



管理承諾：
1. 制訂公司政策。
2. 確立管理系統之目標與計畫。
3. 訂定管理系統之角色與職責。
4. 宣導遵守管理系統、政策與法令規章、達成管理系統目標及持續改善之重要性。
5. 提供管理系統各項作業所需之資源。
6. 決定資訊安全風險可接受水準。
7. 執行管理系統之管理審查作業。
8. 組織分工權責。

圖表 1　標準化運作機制及管理承諾 (續)

標準化運作機制 (PDCA)	規劃 (Plan)	實施與運作 (Do)	監督與查核 (Check)	維護與改進 (Act)
資訊安全管理	1. 界定資訊安全管理系統之範圍，並制訂資訊安全政策。 2. 明訂風險評估程序。 3. 識別資訊安全管理系統範圍內之資產，界定其擁有者，分析其弱點與威脅，並評估風險發生之機率與影響程度。 4. 列舉評估各種風險處理方式，選擇適當之控制目標與措施。	1. 落實執行風險處理計畫，管理相關作業與資源，量測控制措施之有效性，以達成預期之控制目標。 2. 採行適當之控制措施與程序，以利及早發現異常事件，並迅速因應處理。	1. 內部查核 (Internal Audit) 管理系統定期進行內部查核作業，以檢討內部控制目標、內部控制措施與程序是否遵循相關標準、法令規章或資訊安全等規範，並依預期規劃有效執行與維持；內部稽核與自行查核之作業機制，依「內部稽核工作要點」與「自行查核工作要點」之規定辦理。 2. 管理審查 (Management Review) 為持續維護管理系統運作之適切、充足與有效，管理階層定期進行系統審查作業，審查範圍包括對於管理系統 (含政策與目標) 改進方案與變革需求之評估等，審查結果除要求改善外，並予以詳實記錄及妥善保存。	1. 維護系統運作 2. 持續改善 3. 矯正措施 (Corrective Action) 4. 預防措施 (Preventive Action)
品質管理	1. 彙整品質管理系統相關流程及其應用。 2. 確認相關流程的順序與彼此間之關係。 3. 訂定標準和方法，以確保流程運作與控制的有效性。 4. 確保取得適切的資源與資訊，以支援相關流程的運作與監督。	在資訊系統服務實施與運作的生命週期中，有關客戶服務每一階段相關部處之權責及對品質的要求，包含業務契約管理、開發與品質規劃、設計與製作、採購、營運服務管制、系統型態管理、客戶財產之管制、檢驗與測試、搬運、儲存、防護、複製、交付及服務與維護等，應依相關規範落實執行。		
業務持續運作管理	界定業務持續運作管理系統之範圍，並制訂業務持續運作政策。	1. 分析業務需求與可能造成業務中斷之異常事故，擬定因應措施，以維持業務持續運作。 2. 依據因應措施，發展相關作業程序，並準備所需資源。 3. 確保人員之執行能力與品質。		
個人資料管理	界定個人資料管理系統之範圍，並制訂個人資料管理政策。	1. 分析與鑑別個人資料檔案，評估其風險程度，以設計與實施必要之控制措施，並建置必要之保護機制。 2. 依據個人資料保護相關法令，考量公平、合法、適當且不過度等原則，規劃個人資料處理相關之作業程序。 3. 確保人員之執行能力與品質。		

2. 制度規章及跨行作業標準化制定

財金公司管理系統之相關文件架構，則係由上而下分為四個階層 (如表 2 所示)，且管理與作業相關文件均予以標準化。

在「管理系統規範」中，明訂管理系統之政策目標、組織權責、標準化架構及運作機制等事項，由管理代表督導推動單位，執行各管理系統之建置、推動與協調事宜，以要求所有同仁於日常工作之實踐過程中遵循相關規範，確保公司管理系統之有效運作，維護跨行金融資訊系統之作業穩定及交易安全，以及維持全國支付系統之順利運作。

為確保與金融機構間之資訊互通及作業安全，並維護共同權益，訂定「金融資訊系統跨行業務參加規約」、「金融資訊系統跨行業務處理規則」、「金融資訊系統概要設計規格書」、「金融資訊系統標章使用要點」、「參加單位作業手冊」、「內部作業手冊」等相關業務規範及技術標準，俾與各參加單位共同遵循。此外，尚成立「規約執行委員會」督導各項跨行作業規約之執行，並以「安全審查委員會」查核及落實參加單位資訊系統之亂碼化作業安全，以維繫全體金融資訊系統之順暢運作。

表 2　標準化文件階層

階層	內容	說明
第一階	管理系統規範	政策與管理系統作業原則。
第二階	管理系統標準暨全公司性層級之作業程序	管理系統之作業方法、流程與部門間的關係。
第三階	部處層級專屬之支援性作業規定	作業之執行細節，其文件名稱，如作業手冊、管理辦法、說明書、處理規則、準則、作業要點與程序等。
第四階	表單	記錄各項管理系統活動之證明，以確保管理系統作業的執行與追蹤查考。

(三) 跨行作業標準化參採國際標準，調和國內需求，制定成領域標準

金融資訊系統跨行交易訊息，財金公司參採國際標準，調和國內金融作業需求，制定成為金融領域標準。跨行交易訊息，包括 ATM、通匯、信用卡、網際網路等業務，訊息標準參採 ISO 8583 Financial transaction card originated messages — Interchange message specifications 標準，而金融 EDI (Electronic data interchange，電子資料交換) 跨行付款作業參採聯合國 UN/EDIFACT 之金融 EDI 國際訊息標準、金融 XML (Extensible Markup Language，可延伸標記語言) 作業則參採 IFX/XML 國際標準，並依國內跨行交易需求調和制定。此外，境內及境外美元與人民幣等外幣匯款訊息，採用 SWIFT (Society for Worldwide Interbank Financial Telecommunication，環球銀行金融電信協會) 標準與國際接軌。至於訊息之安全性，則採用符合美國國家標準與技術研究院 (National Institute of Standards and Technology，NIST) 所制定之 FIPS46-3 Triple DES 演算法，產製訊息驗證碼 (Message Authentication Code，MAC)，以確保交易訊息之完整性及來源辨識性；密碼學運算則藉由符合 FIPS140-2 Level 3 認證之硬體加解密設備進行。

另「ATM 提款卡」(晶片金融卡)之卡片規格，採用符合「ISO/IEC 7816」Part 1 (物理特性)、Part 2 (尺寸和接點位置)、Part 3 (電氣訊號及傳輸協定) 規格之產品，針對 Part 4 (產業間交換用命令) 則因應國內金融卡應用調和制定，非接觸式介面則參考「ISO/IEC 14443」 Identification cards — Contactless integrated circuit(s) cards — Proximity cards — Part 1~4 標準；「晶片金融卡」的安全認證係遵循 Common Criteria —「ISO/IEC 15408」，制定晶片金融卡之 Protection Profile，並通過德國 BSI (德國國家資訊安全局) 認證。

三、標準化推動之績效

(一) 標準化推動對企業及領域擴散之影響性

財金公司為維運跨行金融資訊系統，與金融機構共同訂定各項業務之標準化作業，以為推動及協助參加單位提升資訊作業水準，擴大業務應用範圍，多年來已收廣大且具體之成效，跨行金融資訊系統已然成為現今影響國家安全與社會安定之重要支付系統，不僅提供金融機構、政府機關一個標準、穩定、共用的金融資訊交換平台，更提供民眾與工商企業於日常提款、轉帳及資金調撥等，最為方便與安全的服務，並帶動其領域擴散。

1. 通匯業務之拓展

財金公司多年來致力於通匯業務標準化作業之推動，持續拓展其服務範圍 (詳如表 3)。在服務對象方面，由創建初期服務民眾及工商企業，進而推展至服務政府機關、證券商或票券商、票券實券保管等相關單位；在平台機制方面，由新臺幣單一幣別之資金撥轉調度，拓展至境內美元、境內人民幣及跨境人民幣匯款服務，將持續朝國際化及多幣別多元化之趨勢發展，以帶動國內企業及金融機構等相關領域經貿之活動。

表 3　通匯業務之拓展

日期	拓展項目與主要內容
76/08	開辦營運，提供民眾及工商企業之「入戶匯款」服務及金融同業間之「同業匯款」服務。
79/08	增辦政府機關之「公庫匯款」服務。
86/02	增辦證券商或票券商之「證券匯款」服務。
93/04	增辦處理實券保管帳戶交易之「票券匯款」服務。
99/12	增辦提供民眾與企業調度美元資金之我國「境內美元匯款」服務，涵蓋票券匯款、同業匯款及一般匯款等作業，以有效縮短境內美元資金交付流程、降低款項收付風險及成本，並活絡資金運用及節省轉匯費用，同時促進我國美元票券市場發展。
100/05	為遵循國家標準「CNS11643 中文標準交換碼」，完成通匯系統罕用字的規劃與建置，並輔導金融機構辦理轉置作業。
102/03	增辦採 SWIFT 訊息標準與國際接軌之我國「境內美元匯款」服務，並預計同年 7 月間增辦「境內暨跨境人民幣匯款」服務。

2. 金融卡 / 自動化服務機器 (ATM) 業務之拓展

財金公司對於金融卡暨自動化服務機器 (ATM) 共用業務服務領域之擴散，更是不遺餘力 (詳如表 4)。在服務項目方面，由創建初期的提款、查詢，進而推展至轉帳、繳費、繳稅、消費購物；尤有甚者，於 92 年 10 月將磁條金融卡予以晶片化，大幅提升交易的安全性，也提升了晶圓及卡片業者產值，連帶將服務領域，從實體 ATM 的提款、轉帳、繳費、繳稅及 POS 刷卡消費，拓展到網路 ATM 的轉帳、繳費、繳稅、購物及網路 POS 刷卡消費，擴大金融卡的市場服務；也順勢將觸角延伸至國外，與 VISA、MasterCard、JCB 等國際組織合作，提供國人於世界各國之 ATM 提領現金；更進一步與日本 NTT Data 公司合作，提供臺灣金融機構發行的金融卡於日本地區貼有財金跨行標誌的 ATM 跨國提領現金及特約商店刷卡消費之服務，以及與中國銀聯公司合作，提供銀聯卡在臺灣 ATM 提領新臺幣現鈔及在特約商店刷卡消費之服務，滿足國人赴日或大陸人士來臺進行商務交流、觀光旅遊等現金需求。未來，更將持續規劃拓展服務領域，延伸至其他地區，提升國人赴國外商務、旅遊、留學的便利性，同時也帶動了 ATM 及卡片資訊產業、網路事業及金融體系等相關支付業務之拓展。

表 4　金融卡 / 自動化服務機器 (ATM) 業務之拓展

日期	拓展項目與主要內容
76/01	開辦營運，提供民眾使用磁條金融卡於具跨行服務功能之 ATM (自動化服務機器), 進行「跨行提款」、「跨行餘額查詢」等服務。
80/07	延長服務時間為「24 小時全年無休」。
81/08	增辦「跨行轉帳」服務。
84/12	與 VISA 及 MasterCard 等國際組織合作，增辦「跨國提款」服務。
85/08	增辦國內 ATM 信用卡「跨行預借現金」服務。
86/05	增辦「跨行轉帳繳稅」服務。
92/09	ATM 全面提升為可提供「晶片金融卡」提款及轉帳服務，並於同年 10 月間，由 13 家先導金融機構首批完成磁條金融卡晶片化作業，晶片金融卡正式營運，而全體金融機構則於 95 年 3 月完成金融卡全面晶片化作業。
93/08	增辦「網路 ATM 跨行轉帳」服務。
95/01	增辦「跨行轉帳繳費」服務。
99/01	增辦「晶片金融卡於日本跨國提款及刷卡購物」服務。
99/06	增辦「銀聯卡在臺 ATM 取現及刷卡購物」服務，滿足大陸人士來臺商務交流、觀光旅遊等現金需求，為兩岸電子金融交流開展新里程。
101/03	增辦「銀聯卡在國內網路特約商店刷卡消費」之收單業務；並研議「臺灣發行之金融卡在大陸地區 ATM 取現及特約商店刷卡消費」服務。

(二) 標準化帶動上、下游支付產業鏈營運量值

為肆應金融市場自由化、國際化之發展情勢，財金公司在標準化的基礎下，與金融機構、政府機關、國際組織、事業單位等密切合作，戮力發展各項跨行金融業務，拓廣金流服務層面，提升金融服務品質，並帶動其上、下游支付產業鏈之績效。

1. 企業大額資金調度：通匯及金融 EDI/XML 支付服務

通匯業務係於 76 年開辦，提供金融機構間入戶電匯、公庫匯款、同業匯款、證券匯款及票券匯款等跨行資金調撥服務，為跨行金融資訊系統中提供社會大眾辦理跨行間大額資金調度之基礎建設，其跨行訊息標準系出國際標準與國內跨行交易需求；依據市場需求循此標準陸續推出之各項匯款服務，活絡我國電子支付之網絡，樹立安全便捷的金流服務。

由「歷年 (民國 88 至 101 年) 通匯 (新臺幣) 交易值變動趨勢」(詳圖 2 所示) 觀之，可知通匯業務與國內外經濟變動情勢息息相關，其中除 90 年受網際網路科技泡沫波及、98 年全球金融海嘯衝擊、以及 101 年經濟景氣低迷等影響，致交易值年增率呈負值外，整體而言，交易值從 88 年的 62 兆 3,000 億元，逐年增長至 101 年的 103 兆 8,255 億元。於 101 年底，新臺幣通匯業務計有 390 家金融機構參加，全年交易量 9,000 萬筆、交易值 103 兆 8,255 億元，較 100 年交易量略增 2.49%，但交易值則下降 4.19%。

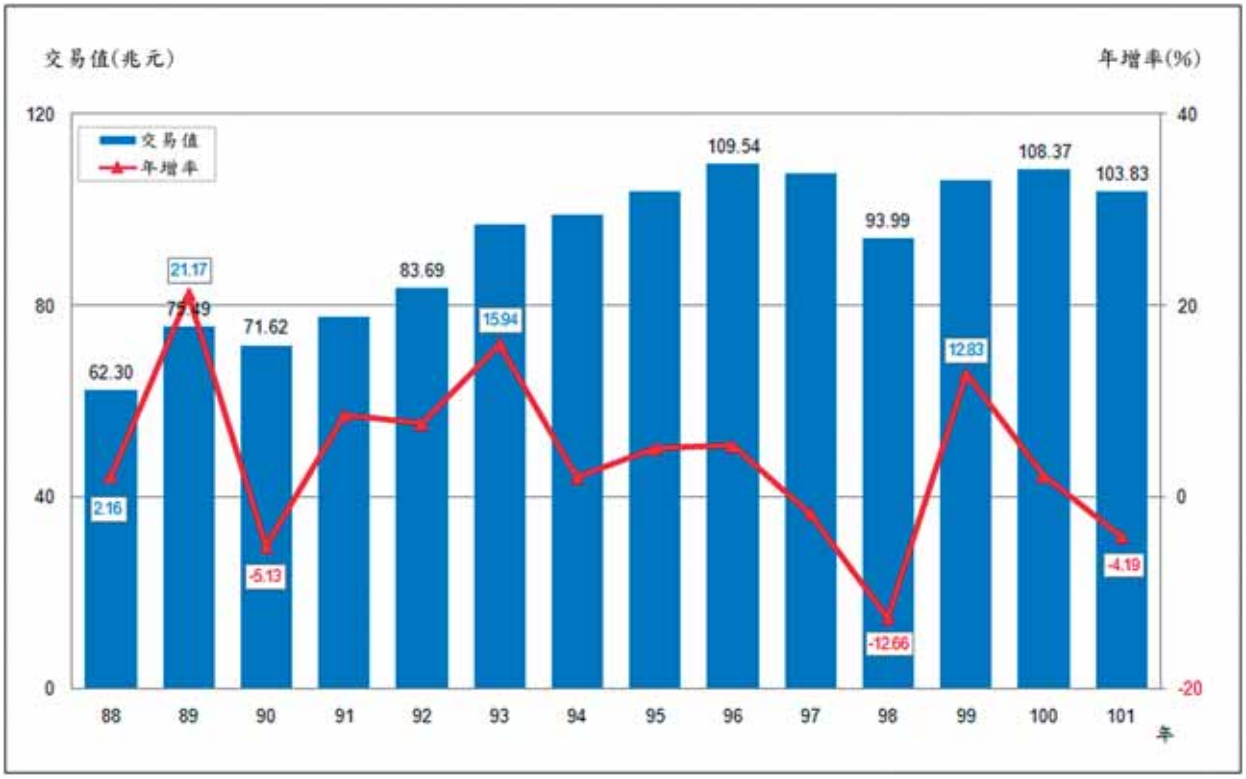


圖 2　歷年「通匯」(新臺幣) 交易值變動趨勢

隨著網際網路無遠弗界的發展，財金公司為延伸金融機構上、下游供應鏈之企業客戶服務，接續於 86 年提供 B2B 供應鏈體系「金融 EDI 業務」，採用聯合國 UN/EDIFACT 的國際標準訊息格式，協同金融機構將銀行跨行付款服務由營業櫃檯直接延伸至企業客戶端，企業客戶使用單一金融機構、單一平台，即可於企業內調度存放於其他金融機構的資金，完成跨金融機構資金調度的需求；嗣於 92 年開辦「金融 XML 業務」，採用國際 IFX/XML 訊息標準，協同金融機構針對企業客戶全天候全球運籌的財務及資金管理需求，提供透過 Web 網頁進行 24 小時全年無休、安全穩定的即時收付款轉帳作業。

就「歷年 (民國 95 至 101 年) 金融 EDI / XML 交易量值結構變動趨勢」(詳圖 3 所示) 觀之，在交易量方面，「金融 XML」交易量自 99 年起呈現跳躍式增長，與「金融 EDI」各約占交易總量之 50%，續自 100 年起「金融 XML」交易量正式超越「金融 EDI」，所占比重在 60% 以上；足見，政策主導與金融機構之配合，攸關跨行業務之興替。然而，在交易值方面，「金融 EDI」交易值始終高於「金融 XML」，仍為企業資金調撥之重要管道。於 101 年底，「金融 XML」業務計有 39 家金融機構參加，較早 6 年推出的「金融 EDI」業務僅有 20 家金融機構參加，可謂後來居上；二者全年交易量合計 785 萬筆、交易值 4 兆 6,386 億元，較 100 年分別增長 9.64% 與 3.30%。

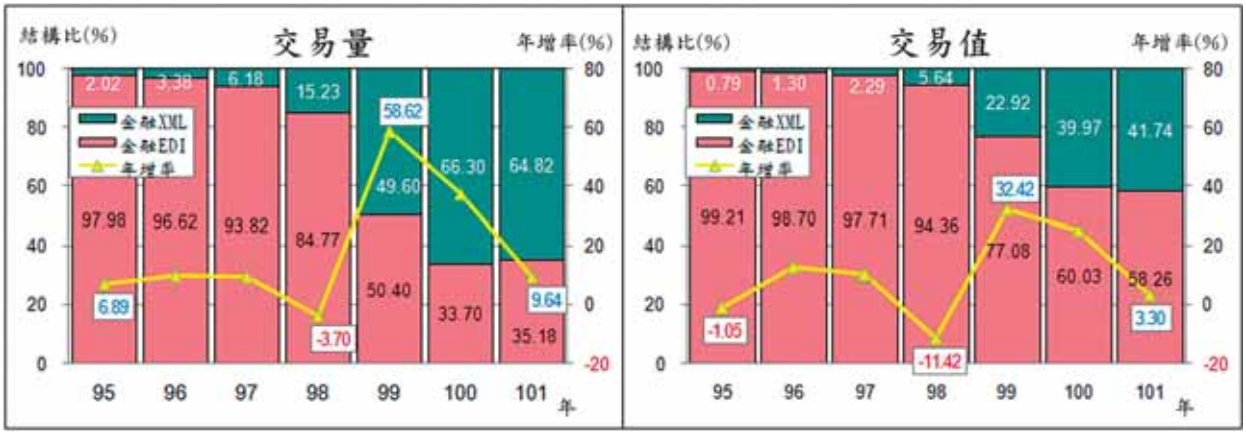


圖 3　歷年「金融 EDI/XML」交易量值結構變動趨勢

2. 社會大眾小額零售支付：金融卡 / 自動化服務機器 (ATM) 共用服務

自動化服務機器共用業務於 76 年開辦，提供 ATM 跨行提款 (含跨國提款)、轉帳 (含繳納費稅) 及餘額查詢等「24 小時全年無休」服務，嗣於 88 年 2 月起，將服務通路由「實體 ATM」擴增至「網路 ATM」(「網路 ATM」除跨行提款服務無法提供外，其餘服務與「實體 ATM」功能相同)，為跨行金融資訊系統中提供社會大眾辦理小額零售支付之基礎建設，其跨行訊息標準亦參採「ISO 8583」標準。

由「歷年 (民國 95 至 101 年)「ATM 提款 / 轉帳」交易量變動趨勢」(如圖 4 所示)

觀之，伴隨資通訊產業與網路服務的發展、以及金融卡於 95 年全面晶片化，「網路 ATM」服務自 96 年起交易量呈顯著增長，其占 ATM 總體轉帳交易量之比重，由 95 年的 0.29%，增長至 101 年的 21.85%。未來，隨著網路世代消費人口快速增加，「網路 ATM」交易量值，勢將進一步擴大。於 101 年底，自動化服務機器共用業務計有 369 家金融機構參加，ATM 台數 26,524 台，發卡量 5,941 萬張；全年交易量 3 億 7,400 萬筆、交易值 6 兆 4,968 億元，較 100 年分別增長 5.38%、2.55%。

再者，金融卡的應用功能由單純的提款及資金調度 (轉帳) 媒介，發展成具繳稅、繳費及購物等多功能的 SmartPay 支付工具；應用通路則擴展至政府機關、學校、企業、電信公司、民生費用及一般商店等有收款需求的機構，且由實體銷售點拓展至無疆界的網路平台。

在網路繳稅及繳費的應用上，配合政府推動繳稅 e 化政策及響應節能減碳措施，納稅義務人除可透過「Paytax 網路繳稅服務網」(https://paytax. nat.gov.tw)，使用金融卡搭配晶片讀卡機完成網路繳稅外，社會大眾亦可利用「全國繳費網」(https://ebill.ba.org.tw)、金融機構或事業單位繳費網查詢帳單資訊，並以金融卡直接進行線上繳費，不受代收機構營業時間或地點之限制，舉凡如水、電、瓦斯公司 (公用事業費)、公 (國) 立學校 (學雜費)、勞保局 (勞保費)、健保局 (健保費) 等均可繳納。

由「歷年全國性繳費 (稅) 交易量變動趨勢」(如圖 5 所示) 觀之，本項業務於 94 年、95 年間因業務推展成果逐漸發酵，致 95 年交易量達 1,747 萬筆呈 4.5 倍的增長，加上相繼於 99 年推出「金融機構臨櫃代收稅款」服務，交易量即由 98 年之 2,714 萬筆，大幅擴增至 100 年之 6,119 萬筆，平均每年增幅 1.5 倍。於 101 年底，全國性繳費 (稅) 業務計有 364 家金融機構參加，全年交易量 6,292 萬筆、交易值 1 兆 7,189 億元，僅較 100 年分別微增 2.8% 與 1.03%。

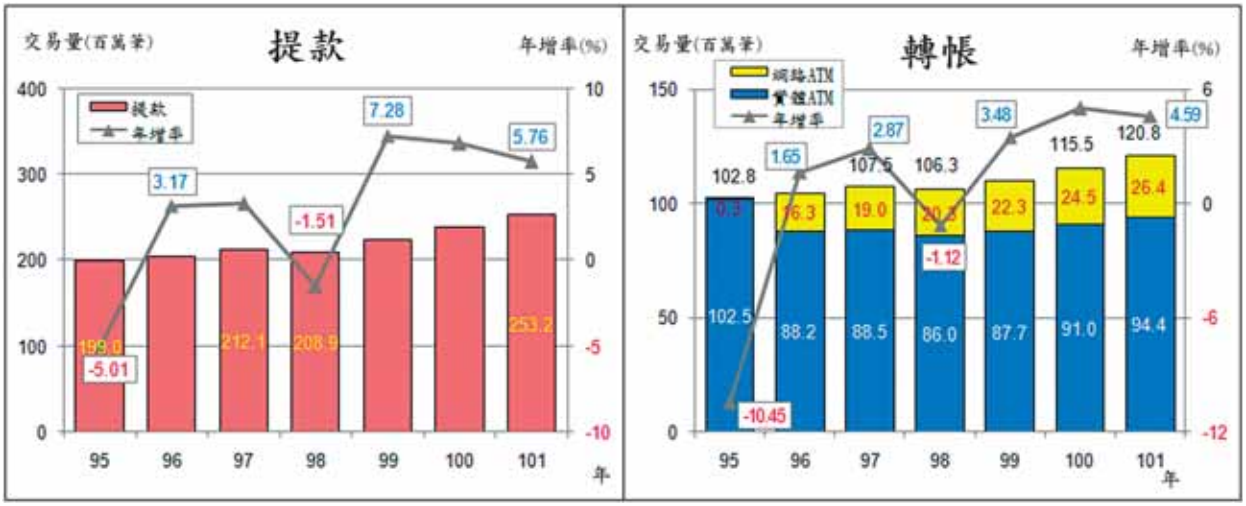


圖 4　歷年「ATM 提款 / 轉帳」交易量變動趨勢

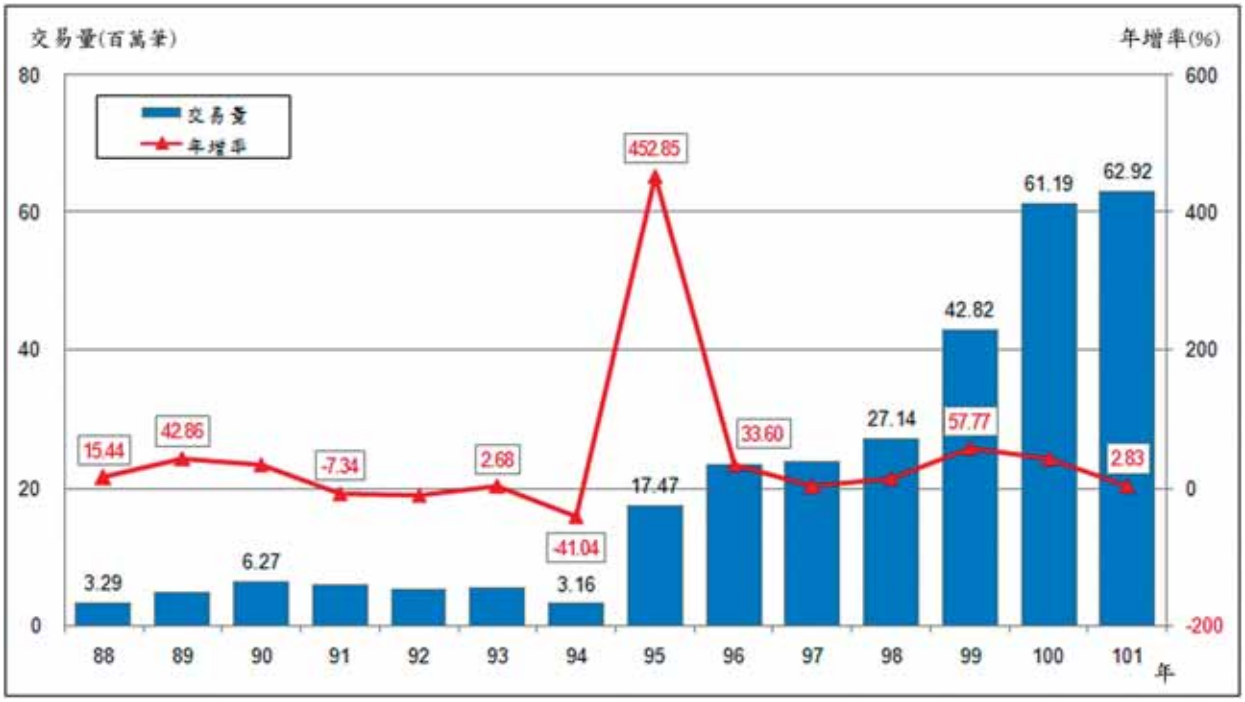


圖 5　歷年「全國性繳費 (稅)」交易量變動趨勢

此外，攸關本地規格國際化及支援國際規格本土之應用，99 年 1 月與日本 NTT Data 合作開辦跨國提款及刷卡消費之服務，不僅解決國人赴日攜帶現金受出入境管制及換匯之不便，還可透過臺日金融機構的直接合作，有效降低民眾在日本使用卡片服務的費用，提升民眾在日本活動的便利性，同時將臺灣金融卡的品牌及服務推上國際舞台；又，99 年 6 月開辦銀聯卡在臺灣提領新臺幣現鈔及刷卡消費之服務，更為兩岸電子金融交流開展新頁。

(三) 國際標準引進之本土化及特色之建立

財金公司兢兢業業維運跨行金融資訊系統與維護國際標準，並為豎立企業標竿，持續汲取國際新知、新技能，引進國際標準，配合國內需求予以本土化，提升企業與民眾在國內外活動的便利性，同時將臺灣金融卡的品牌及服務推上國際舞台，致力拓展與提升我國金流服務臻至完善。財金公司復於管理制度推動上的投入，也可說是前仆後繼，勵行多年，因此在金融資訊服務領域可屬先行者角色，也常藉分享推動經驗，帶動業界建立標準化管理之風氣，相關管理制度獲國內外相關組織驗證者，依其時序分述之：

1.　品質管理系統 (依據 ISO 9001：2008)

藉由對品質管理系統的導入及致力於品質工作的實踐與改善，達成公司政策與管理目標，提供客戶滿意的資訊服務，為客戶創造價值與成功，故自 88 年起即依照 ISO 9001 國際標準要求，建立及維持品質管理系統，並持續改善系統的有效性。

2. **資訊安全管理系統（依據** ISO 27001：2005)

為維護客戶與公司內部重要資訊資產之機密性、完整性與可用性，確保各項業務之持續運作，自 91 年起即依據 BS 7799 標準的要求，建立及維持資訊安全管理系統，並於 92 年 8 月取得 BS 7799-2:2000 認證，95 年通過 BS 7799 改版為 ISO 27001:2005 認證，為金融及週邊機構第一家取得認證者。

3. **業務持續運作管理系統（依據** BS 25999-2：2007)

通匯系統及金融卡 / 自動化服務機器共用系統提供社會大眾跨行交易服務，為攸關民生之關鍵核心業務，為確保業務運作遭遇威脅導致業務中斷時，仍能快速回復，自 91 年起即進行業務持續運作及應用系統災變應變措施之規劃，並於 98 年依照 BS 25999 標準的要求，建立及維持業務持續運作管理系統，為銀行相關行業第一家取得認證者。

4. **個人資料管理系統（依據** BS 10012：2009)

依據「個人資料保護法」及相關法令之規定，自 99 年起即著手進行個人資料清查及評估相關防護機制，並陸續加強導入各項資料保護措施。除技術性控制措施外，更自 100 年起依據 BS 10012 標準的要求，建立及維持個人資料管理系統，以確保對於個人資料之適法蒐集、處理及利用，已善盡良善管理之責任，避免人格權受到侵害，並促進個人資料之合理利用。101 年 3 月「個人資料保護法」正式實施前，即通過 BS 10012：2009 驗證，為金融及週邊機構第一家取得認證者。

四、榮獲「全國標準化獎」與肯定

經濟部標準檢驗局（以下稱標檢局）為激勵國內各行業、專業團體與企業機關制定及推行標準，以健全全國標準體系、提升國家競爭力及促進經貿蓬勃發展，自 89 年起每年舉辦中華民國「全國標準化獎」甄選活動，以獎勵與表揚對國內實施標準化具有貢獻、成效卓著之機關、機構、團體、公司及個人，至 100 年止甄選活動已辦理 12 屆。

「全國標準化獎」係依標準化之推行範圍及貢獻程度而評比，針對團體、公司及個人分別設立「團體標準化獎」、「公司標準化獎」、「標準化成就獎」及「標準化前瞻貢獻獎」等獎項，旨在鼓勵企業培育專業的標準化人才及促進國際交流。評審作業係由標檢局遴聘產、官、學、研各界人士擔任評審委員，並由標檢局局長擔任主任委員，共同組成「標準化獎勵評審會」，對參選單位（或個人）分三階段進行預審、初審及複審，遴選出得獎者，得獎名單由標檢局刊登於全國性刊物、相關網站，以及藉由新聞媒體公開表揚，並舉辦頒獎典禮，邀請相關政府首長頒獎，並邀各界人士蒞會觀禮。

「全國標準化獎」歷年獲獎單位多為具規模之高科技電子、傳產製造業、軍備工廠等製造業，而標準化原即為此類得獎單位之強項，其具有完備、嚴謹且按部就班之標準化技術及作業程序，可明確達成降低成本、提升產能等目的之特性，因此歷年服務業者獲獎次數屈指可數，金融領域之得獎單位更是付之厥如，更增添金融服務業者參與甄選之挑戰性。

經審慎評估及縝密思量，多年來財金公司與金融機構為促進跨行金融資訊系統自動化所進行之各項標準化作為，以及財金公司參採國

際標準所建立之管理制度，應有機會獲得評審之青睞；爰此，乃以「跨行作業標準化」與「公司管理制度標準化」雙主題形式，作為參與甄選之訴求主軸。嗣經前後為期約三個月之三階段評審作業，財金公司所提報之標準化成果，終獲評選委員「標準化推動績效顯著，不僅有效促進金融交易安全，更對國家整體金融管理作業帶來正面積極的卓越價值，堪為楷模。」高度之評價，並於 101 年 10 月 15 日獲頒「公司標準化獎」。

財金公司長年來為標準化所作努力已逐步開花結果，在欣見成果受肯定的同時，財金公司也願意作為一顆好的種籽，持續將標準化的精神與作法散播出去，讓未來的枝幹能繼續開枝散葉，傳承下去。

五、結語

財金公司為全國金融資訊跨行交易處理之樞鈕，擔負提供金融機構及社會大眾便捷的金流服務、穩定的作業系統及安全的交易環境之重任，多年來，與參加單位協力發展各項跨行服務作業時，均能以標準化為圭臬，力求各項作業服務之變化與精進，故能於金融資訊領域豎立起企業標竿，與金融機構共同見證我國金融自動化與標準化之成果。本次榮獲經濟部「公司標準化獎」的肯定，實為全體參加單位共同努力之成果，對於財金公司多年來推動跨行金融業務亦為一大鼓勵。

為因應科技環境與金融需求之迅即變化，未來財金公司於發展新型態支付業務與技術作業的過程中，仍將秉持一路走來推動標準化作業之精神，持續關切與參採國內外各項技術性及管理性標準，同時配合政府政策及金融機構業務推展需要，運用跨行金融資訊系統既有之優勢，積極發展雲端共用平台，持續朝政府「強化資訊流通 提升 e 化效能」的發展策略方向而努力。

※ 參考文獻 / 資料來源：

1. 經濟部，中華民國第 13 屆全國標準化獎紀實專刊，2012/10。
2. 財政部，當代財政第 25 期，2013/01。
3. 全國標準化獎官方網站 (http://www.std.org.tw/)
4. 維基媒體 http://commons.wikimedia.org/wiki/File:PDCA-Cycle.png

台灣資訊軟體品質提升與發展策略

本篇摘自 2008 年 09 月出刊之財金資訊季刊第 56 期，由時任資策會資訊工程研究所張子龍主任撰寫。

一、 前言

知識經濟的蓬勃發展，資訊科技業已成為國家數位神經系統的建構及維運者，同時也是所有產業升級、競爭力提升的關鍵，先進國家無不將資訊科技發展作為國力提昇重點。我國亦著眼於此，全面提升產業附加價值，以獲取龐大的邊際效益，最終目標則為促使我國資訊服務業朝創新應用、高附價價值邁進，使我國資訊服務業轉型成為具外銷競爭力之產業，並成為全球特定領域資訊服務之主要供應者。

「高品質」、「低成本」為印度軟體工業的代名詞；有趣的是「高品質」、「低成本」更是台灣硬體產業的寫照。依據資策會 MIC（Market Intelligence Center）的調查統計，全球資訊服務產值已超越資訊硬體，2000 年約為硬體產值的 1.5 倍且持續擴大中，預估至 2010 年將為 1.8 倍。

1992 年印度國家策略發展計畫喊出響亮的 IT for all 口號，國家各項經濟、教育政策全力配合推展軟體發展迄今，依據美國 Fortune 雜誌全球排名前 500 大企業中有 255 家資訊軟體服務委由印度，如此的成果，驗證了印度政府整體策略發展方向為國家帶來的效益，其於全球軟體工程發展之成就亦獲得全方面的肯定。

另外，軟體發展領域快速崛起的中國大陸，為提升其資訊軟體品質而推展 CMMI 制度，其目的並不全然為了準備成為軟體代工廠，而是為了有朝一日掌控龐大的內需市場，也就是所謂「衝出去的真正目的是打回」，因此將 CMMI 的認證視為取得國際出口的通行證以及領導角色的標章。

台灣在全球科技產業供應鏈中是相當重要的一環，消費性電子產品的生命週期平均是 6　8 個月，台灣資訊硬體產業對於生產製造的流程已經相當純熟，如果能夠掌握軟體的發展，便能夠充分掌握新產品的上市時間與品質，贏得先機。

二、 我國提昇資訊軟體品質 (CMMI) 計畫

為建構我國資訊軟體業健全有效的生產體系，以促進產業垂直分工與水平整合，特透過推展 CMMI 驗證制度以及重點輔導旗艦計畫強化業者之服務品質及國際競爭力。

2003 年始，行政院經建會、各服務業主辦機關等透過預備會議，及草案研擬審查通過，於 2005 年起由經濟部工業局啟動「提升資訊軟體品質計畫」四年計畫，以實現我國資訊服務業升級與外銷發展之準備。由於成效極佳，政府刻正於本年度 (2008) 著手研擬 2009~2012 年「提升資訊軟體品質計畫」二期方案 (如圖 1)，期持續提昇資訊軟體業者軟體工程能力以提高國際競爭力，將資訊軟體業轉型為外銷導向之知識產業。

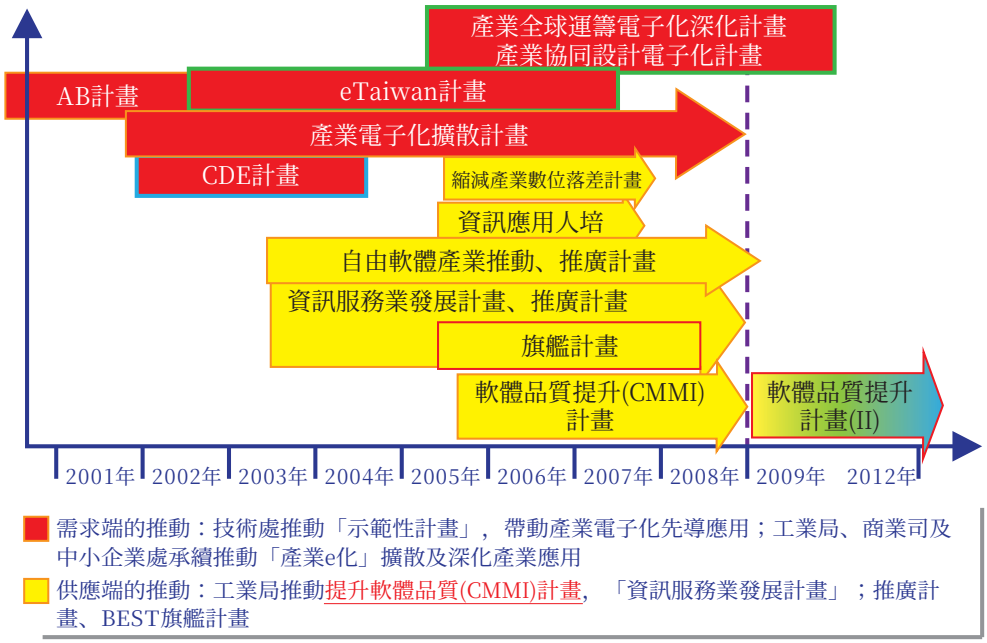


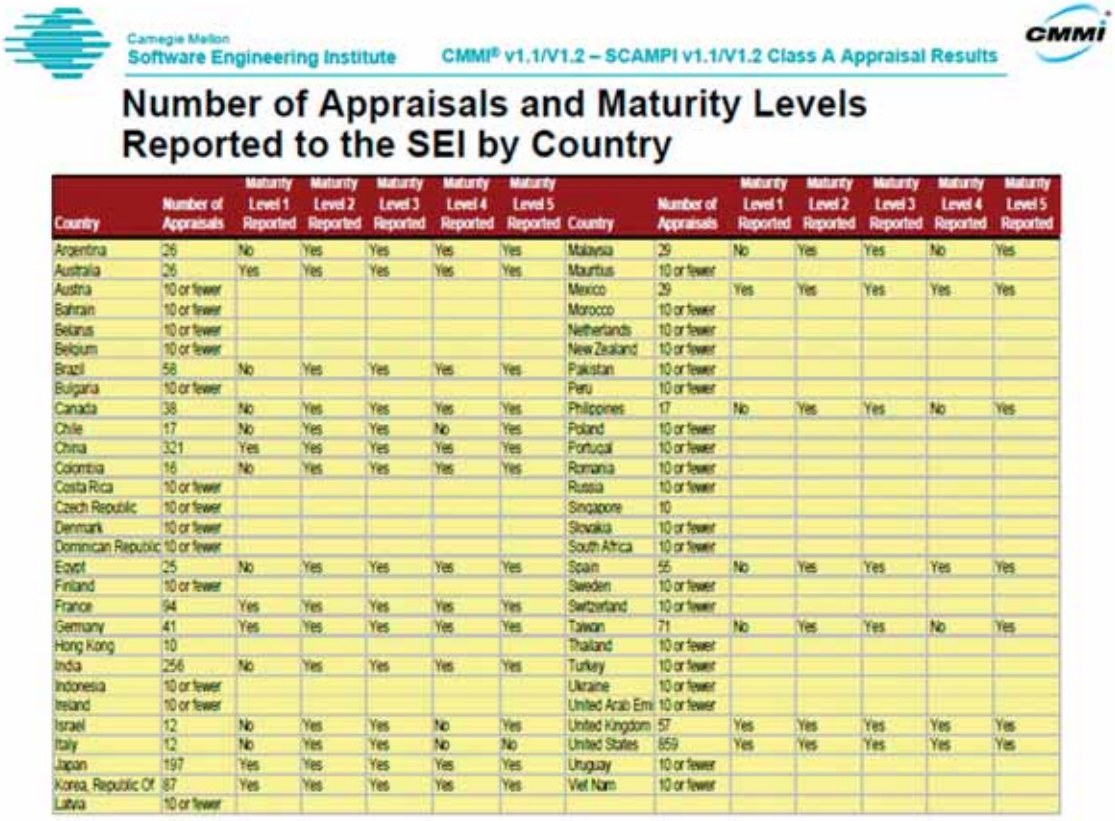
圖 1　政府推動的資訊軟體產業相關計畫

依據美國 SEI/ CMU (Software Engineering Institute, SEI/Carnegie Mellon University, CMU) 在 2007 年 9 月最新公布之各國通過 CMMI 家數之數據中，台灣排名第 7 名，超越巴西、英國、西班牙、德國、加拿大等先進國家，排名依序為美國、中國大陸、印度、日本、法國、韓國 (如圖 2)。

計畫實施三年以來，鼓勵具有規模與具有意願之廠商參與本計畫之 CMMI 導入輔導，為台灣資訊軟體塑造有利之環境並建全業者之資訊軟體品質。於北中南之輔導推動與宣傳下，全台已有 97 家次業者在工業局輔導下導入 CMMI，若包含自行導入者更可達 120 家次以上 (如表 1)。

表 1　CMMI 導入數量統計分析

地區	94 年度	95 年度	96 年度	合計
台北市	30	21	10	61
台北縣	5	2	3	10
桃園縣	1	0	0	1
新竹市	3	4	3	10
新竹縣	0	1	0	1
苗栗縣	1	0	0	1
台中市	3	0	3	6
南投市	0	1	0	1
高雄市	1	3	1	5
高雄縣	0	0	1	1
合計	44	32	21	97



Carnegie Mellon
Software Engineering Institute　CMMI® v1.1/V1.2 – SCAMPI v1.1/V1.2 Class A Appraisal Results

Number of Appraisals and Maturity Levels Reported to the SEI by Country

Country	Number of Appraisals	Maturity Level 1 Reported	Maturity Level 2 Reported	Maturity Level 3 Reported	Maturity Level 4 Reported	Maturity Level 5 Reported	Country	Number of Appraisals	Maturity Level 1 Reported	Maturity Level 2 Reported	Maturity Level 3 Reported	Maturity Level 4 Reported	Maturity Level 5 Reported
Argentina	26	No	Yes	Yes	Yes	Yes	Malaysia	29	No	Yes	Yes	No	Yes
Australia	26	Yes	Yes	Yes	Yes	Yes	Mauritius	10 or fewer					
Austria	10 or fewer						Mexico	29	Yes	Yes	Yes	Yes	Yes
Bahrain	10 or fewer						Morocco	10 or fewer					
Belarus	10 or fewer						Netherlands	10 or fewer					
Belgium	10 or fewer						New Zealand	10 or fewer					
Brazil	58	No	Yes	Yes	Yes	Yes	Pakistan	10 or fewer					
Bulgaria	10 or fewer						Peru	10 or fewer					
Canada	38	No	Yes	Yes	Yes	Yes	Philippines	17	No	Yes	Yes	No	Yes
Chile	17	No	Yes	Yes	No	Yes	Poland	10 or fewer					
China	321	Yes	Yes	Yes	Yes	Yes	Portugal	10 or fewer					
Colombia	16	No	Yes	Yes	Yes	Yes	Romania	10 or fewer					
Costa Rica	10 or fewer						Russia	10 or fewer					
Czech Republic	10 or fewer						Singapore	10					
Denmark	10 or fewer						Slovakia	10 or fewer					
Dominican Republic	10 or fewer						South Africa	10 or fewer					
Egypt	25	No	Yes	Yes	Yes	Yes	Spain	55	No	Yes	Yes	Yes	Yes
Finland	10 or fewer						Sweden	10 or fewer					
France	94	Yes	Yes	Yes	Yes	Yes	Switzerland	10 or fewer					
Germany	41	Yes	Yes	Yes	Yes	Yes	Taiwan	71	No	Yes	Yes	No	Yes
Hong Kong	10						Thailand	10 or fewer					
India	256	No	Yes	Yes	Yes	Yes	Turkey	10 or fewer					
Indonesia	10 or fewer						Ukraine	10 or fewer					
Ireland	10 or fewer						United Arab Emi	10 or fewer					
Israel	12	No	Yes	Yes	No	Yes	United Kingdom	57	Yes	Yes	Yes	Yes	Yes
Italy	12	No	Yes	Yes	No	No	United States	859	Yes	Yes	Yes	Yes	Yes
Japan	197	Yes	Yes	Yes	Yes	Yes	Uruguay	10 or fewer					
Korea, Republic Of	87	Yes	Yes	Yes	Yes	Yes	Viet Nam	10 or fewer					
Latvia	10 or fewer												

圖 2　美國 CMU/SEI 於 2007 年 9 月公佈全球 CMMI 評鑑家次排名
(資料來源：CMU/SEI Maturity Profile, 2007)

目前整體成果包括：

1.　培育產業人才，降低 CMMI 導入成本

國內已授權之主評鑑員 (CMMI Lead Appraiser) 已達 10 人[1]，大幅降低國內廠商評鑑成本；而授權之講師 (CMMI Instructor) 計 9 人[2]。

2.　研發技術文件，加速軟體工程推展

包含「 CMMI-DEV V1.2 」中文正體版公佈於 SEI 官方網站、CMMI 第三級、第四級教材以及指引、CMMI 簡介數位學習線上教材、採購流程 (CMMI-ACQ) 參考文件等；同時並展開下列研究以作為策略依據：「推動法規執行落差改善措施建議」、「我國軟體產業品質與生產力剖析 (SW Profile)」、「國內組織 CMMI 流程改善量化績效指標制定」、「印度推行 CMMI 實戰」研究等。

3.　目標市場商機推展，展現軟體實力

台灣 CMMI 資訊軟體業之日本東京、大阪、北海道交流訪問團，已獲得松下電工、SONY、NEC、OMRON 及 Hitachi 等國際大廠回應；凌群電腦 (CMMI ML 5) 則與日本 IT 大廠 Vic Tokai 舉辦合作簽約儀式 (96 年 1 月)，在工業局積極推動 CMMI 計畫輔導下，以全球軟體發展共通的品質與專案管理標準，是走向「大型化」與「國際化」的第一項成功實證。

4. CMMI-ACQ 導入成為產業正向拉力

研究發展採購流程文件不僅供政府機關引用，行政機關之採購流程提昇意識亦逐漸抬頭並導入採購流程：

(1) 財稅資料中心於 96 年導入 CMMI-ACQ 成為行政機關之示範單位；
(2) 行政院研考會於 96 年度先行導入建構管理、需求管理、採購管理及招標與履約管理等四個流程領域。
(3) 高雄市政府與台南軟協簽訂「導入 CMMI-ACQ 意向書」。

三、提昇資訊軟體品質 CMMI 計畫 (第二期規劃)

台灣軟體業者規模多屬中小型，軟體發展能力無衡量基準，承接國內大型或國際計畫能力薄弱，以致於國際能見度不佳 (如表 2)。CMMI 以嚴謹、科學的方法有效提升流程管理能力，可以協助業者面對系統日趨複雜化、大型化的多元需求下，有效管理開發流程，並可藉 CMMI 認證與國際接軌。印度通過 CMMI 認證廠商家數與軟體出口成長率具正關聯性，顯見台灣推動 CMMI 將有助於提昇國際形象與競爭力、提升軟體業產值。目前已有日商積極與台灣 CMMI 軟體業者接洽，期經由政府積極持續帶領，未來 CMMI Part II 能再創佳績。

(一) 台灣軟體產業競爭力 SWOT 分析

優勢 (Strength)：

1. 國內軟體業者達 120 家以上導入 CMMI，評鑑家數排名全球第七。
2. 特定領域的應用典範（電子、鋼鐵、醫療、紡織、電子化政府、中小企業等）已具國際知名度。
3. 主評鑑員、講師、種子人才的培育已具規模。

劣勢 (Weakness)：

4. 國內市場規模不大，較難產生具國際競爭力的大型軟體企業。
5. 缺乏國際市場行銷能力與通路。
6. 國內人力成本高，資訊從業人員能量低。

表 2　提升資訊軟體品質計畫 (I) 實施前後軟體產業差異概況

	導入 CMMI 前 (2004 年)	導入 CMMI 後 (2007 年)
國際知名度	國際能見度不佳	全球評鑑排名第七，提昇國際形象與競爭力，建立國際市場之能見度
軟體品質能力	1. 軟體品質無衡量基準，軟體技能參差不齊 2. 國內大型或國際計畫承接能力薄弱 (無標準品質流程)	1. 提昇軟體發展流程能力 2. 建立水平分工與垂直整合能力 3. 促進承接大型計畫與國際計畫之能力 (日本委外市場與東南亞計畫承包)
導入家數與效益分析	通過 CMMI 評鑑計 12 家 (生產力提升計畫)	協助企業導入 CMMI 達 97 家次

7. 買方市場對於軟體品質價值認同度低。
8. 我國資訊產業追求短期利益，較不重視基礎紮根的流程改善。

機會 (Opportunity)：

9. 亞洲各國（日本、中國、韓國、東南亞）對 CMMI 的認同與重視度高。
10. 亞洲開發中國家急需特定領域的應用典範。
11. 身為全球第二大 IT 市場的日本逐年釋出大量軟體委外商機。

威脅 (Threat)：

12. 印度與中國大陸人才充沛低廉，積極佈署人才國際證照。
13. 中國大陸的國家政策支持軟體服務外包，廣泛佈署日本軟體代工基地。

(二) 台灣軟體工程與軟體安全競爭力

2002 年以前，台灣資訊軟體發展著重於建立軟體元件技術，自 2003 年美國 SEI 發表 CMMI 後，台灣軟體業者即開始積極引進 CMMI 流程改善標準，以增強承接大型與複雜專案之能力。在「提升資訊軟體品質 (CMMI) 計畫」推動下，國內通過 CMMI 評鑑家次深具輝煌實績，是為台灣於國際市場嶄露頭角之墊腳石。2009 年以後台灣軟體發展的重點，應朝向持續深化、向下紮根，除繼續進階推廣 CMMI 高成熟度外，嵌入式軟體、驗證與確認、需求工程等相關軟體工程技術，亦是台灣軟體業者可著眼之處，有關台灣軟體競爭力推展的階段 (如圖 3) 所示。

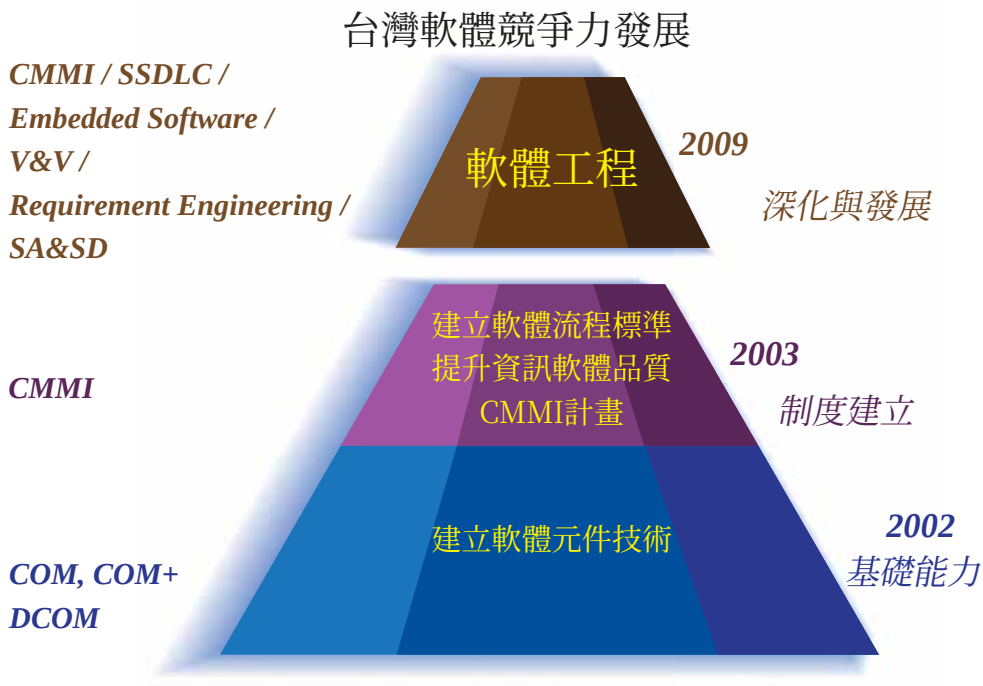


圖 3　台灣軟體競爭力發展階段

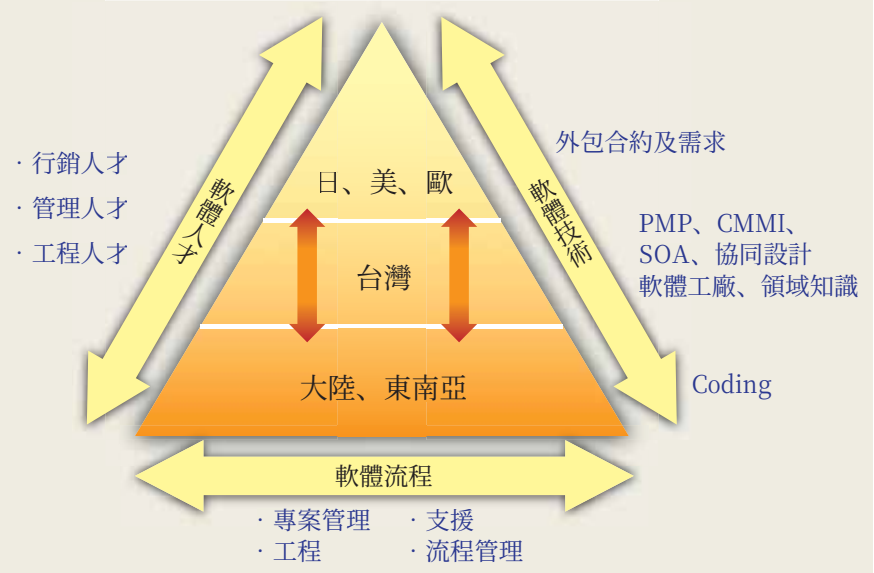


圖 4　台灣軟體產業鏈

(三) 台灣軟體產業鏈

從台灣軟體產業鏈之觀點 (如圖 4) 來分析，台灣扮演國際軟體主要委外市場 (日、美、歐) 與軟體代工市場 (中國大陸、東南亞) 的專業管理與整合之溝通橋樑。軟體人才 (People)、軟體技術 (Technology)、軟體流程 (Process) 三大構面，建構了台灣軟體業者進軍國際市場所必須擁有之基礎。此角色需要行銷、管理、工程等人才來執行國際合約與供應商管理，軟體技術能力則包涵領域知識、專案管理能力 (PMP)、服務導向架構 (SOA) 之規劃與佈置能力、協同設計等，而軟體流程能力的成熟度 (CMMI) 亦是承接國際專案不可或缺之重要能力。

以國際市場角度分析台灣軟體產業鏈，施力重點應在於協助資訊整合商拓展海外商機並培訓軟體分工之國際人才，輔導整合商與專業廠商之技術整合，強化專業廠商 (具 CMMI ML2 以上者) 之 Capability Level 3 能力，並持續深化業者之軟體工程與管理技術（CMMI / SSDLC / Embedded Software / V & V / Requirement Engineering / SA&SD / Agile /）。

根據台灣軟體產業競爭力的優勢與機會，以及台灣於國際市場軟體產業鏈 (如圖 5) 的分析總結，2009~2012 年發展機會 (如圖 6) 將以解決方案 (Solution)、系統整合 (System Integration)、資訊委外 (Outsourcing)，以及嵌入式軟體等作為外銷拓展的核心主軸，推動策略與作法如下：

1. 深化軟體工程技術與管理能力：推動高成熟度軟體發展能力。
2. 提升亞洲軟體委外市場承接能力：研究和導入目標市場之軟體開發平台與工法，推動成立大型軟體製作基地 / 平台。
3. 落實國內 (政府 / 大型企業) 市場軟體工程價值：推動大型資訊採購單位導入 CMMI-ACQ。
4. 目標願景冀望能重新建構台灣資訊軟體業價值鏈，強化軟體工程技術與管理能力，成為亞洲軟體市場主要供應國家。

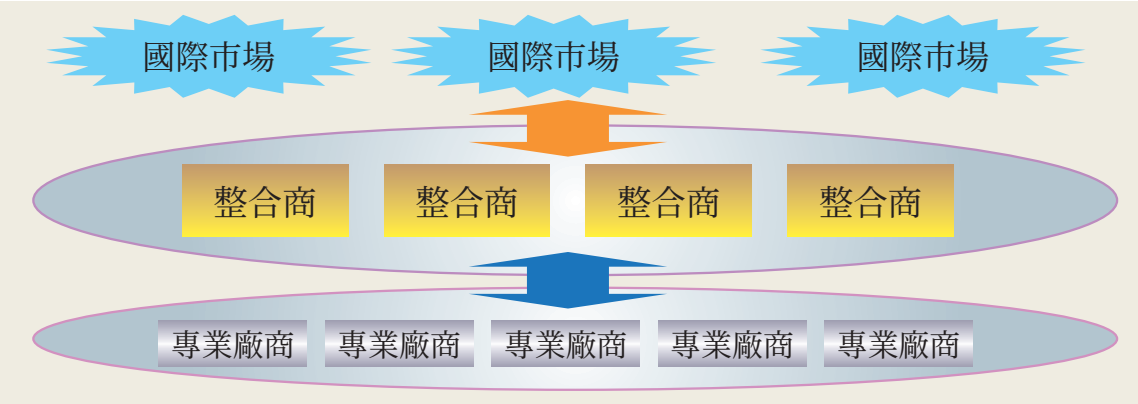


圖 5　以國際市場角度分析台灣軟體產業鏈

四、結語

台灣資訊軟體品質提昇發展策略重點將奠基於前一期計畫成果 (提昇資訊軟體品質 CMMI 計畫 a2005-2008 年)，並以下列三個重點發展方向為發展軸線：

1.　深化軟體工程技術與管理能力

目前全國導入 CMMI ML2 以上超過 120 家次，通過評鑑超過 76 家次，已具備相當軟體發展基礎，未來應持續深化軟體工程技術與管理能力，儲備國際發展能量。建議以目標市場（日本等）之開發方法與流程、領域專業知識為技術重點，持續深化軟體工程相關技術、制度及管理制度如 SOA，CMMI-DEV/ACQ/SVC， SSDLC 及 Agile 等；同時專注於嵌入式軟體 (Embedded Software) 產業發展之契機。

2.　提升亞洲軟體委外市場承接能力

日本為全球第二大軟體市場，並逐年釋出大量委外商機，近年來推動台日軟體合作已見初步成果，應進一步提升業者承接委外商機能力，藉此壯大產業。建議如下：

(1)　承接日本委外商機所需之軟體開發平台與工法：熟悉日本大型軟體開發實務，能以日語與客戶密切溝通的系統工程師，成立技術服務中心提供業者技術支援。

(2)　成立大型軟體製作基地 / 平台：在我國中南部、中國、越南等地擁有 1000 人以上的軟體開發代工團隊。

3.　落實國內 (政府 / 大型企業) 市場軟體工程價值

軟體業者推動軟體工程 (CMMI) 已具規模，但採購方 (政府 / 大型企業) 尚未正面回應，以致業者投入未獲得市場正面回應，成效無法彰顯。為有效落實國內市場軟體工程價值，建議積極推動大型資訊採購單位導入 CMMI-ACQ 以提升採購方之資訊軟體成本估算、規劃與委外管理能力，使供需雙方更加緊密的結合，進一步確保我國資訊軟體品質，從而提升資訊軟體市場之價值，創造政府、產業、人民多贏的契機。

註 1：工業局補助獎勵培訓 7 名主評鑑員。

註 2：工業局補助獎勵培訓 6 名講師。

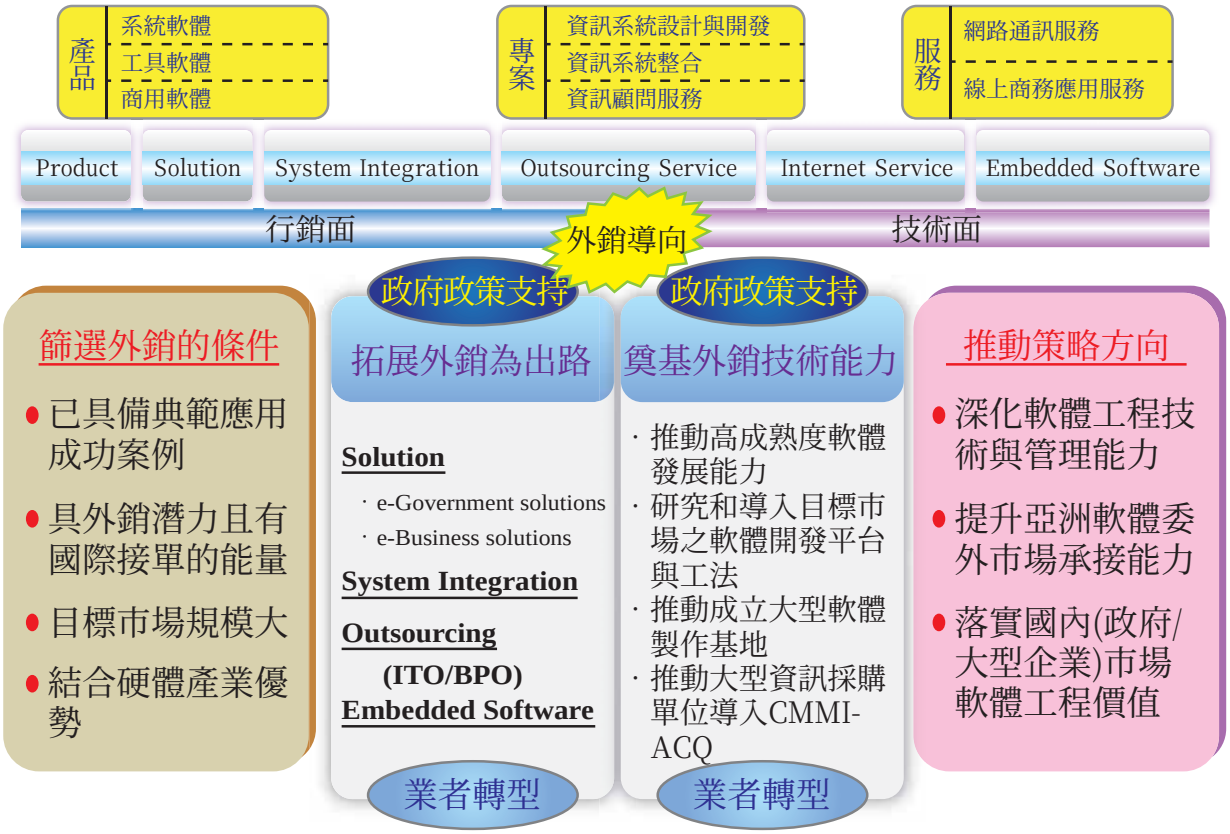


圖 6　2009~2012 年發展機會

金融服務業資訊安全指導方針概述

本篇摘自 2001 年 12 月出刊之財金資訊季刊第 19 期，由時任交通大學資訊管理所樊國楨兼任副教授、方仁威博士研究生、國防部通信電子資訊林勤經局長撰寫。

訂定適當的資訊安全計畫並落實其管理，已成為今日企業邁向虛擬世界所必須面對的課題。植基於此，本文謹以金融服務業為例，為讀者淺介「資訊安全指導方針」的內涵。

資訊安全指導方針

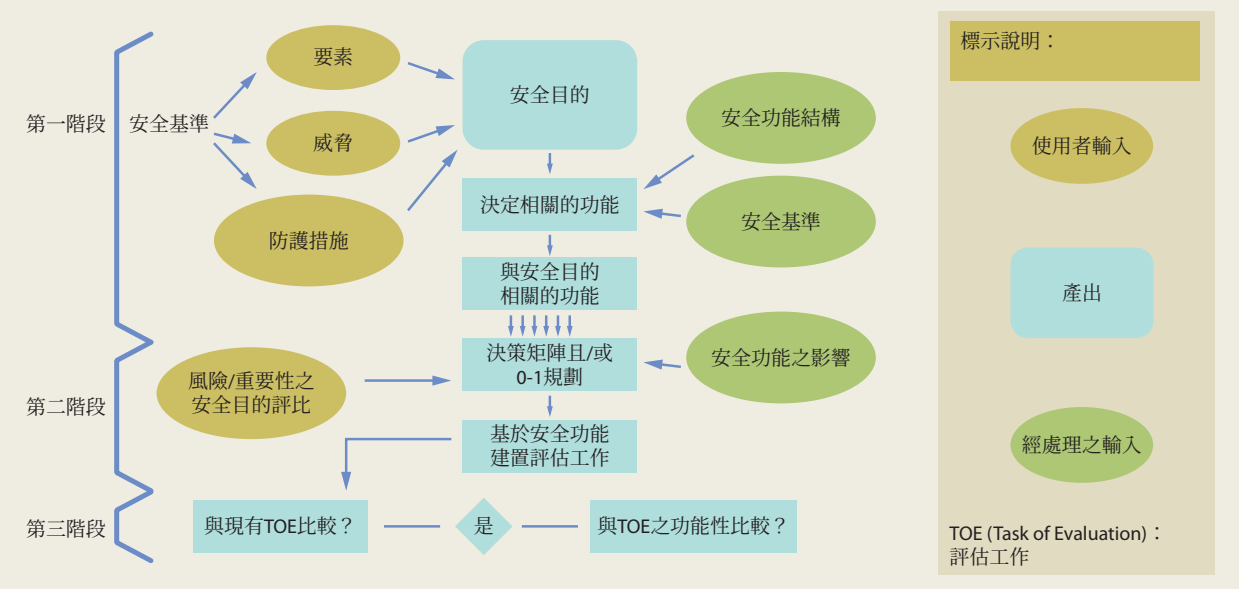
通常企業在訂定資訊技術安全計畫時，均先行規範資訊安全指導方針，以確立資訊安全計畫需求、資訊安全計畫構成要素與資訊安全控管目標及建議之控管方法，植基於國際標準組織（ISO）頒布之「銀行業、證券業及其它金融服務業之資訊安全指導方針。」茲分述於下：

一、資訊安全計畫需求

資訊安全計畫需求主要是在建立一個資訊安全計畫的起始點，同時陳述一個適當的資訊安全計畫之最低需求，也可以作為一個機構評估其資訊安全計畫現況的度量基準。（圖一）資訊技術安全評估共通準則之評估過程，是植基於資訊技術之安全需求及其評估準則產生過程的示意說明，其中之第二階段的評比方案選擇，可以參考（圖二）資訊安全管理概觀架構圖中風險管理部分內的四種不同方案。

二、資訊安全計畫構成要素

資訊安全計畫應該如何運作，各類主管（包括：董事、最高行政主管、管理人員、法務部門、資訊安全主管、員工、廠商及承包商）的特定責任，以及有助於健全安全實務功能（包括：風險接受度、保險、稽核、法令遵循、災害復原計畫、資訊安全認知、外部服務提供者、密碼運作及隱私）與溝通管道均在此討論。高階主管可以利用本規定來確保並降低安全實務的結構障礙，資訊安全人員也可以利用本規定來評估資訊安全計畫的有效性。



圖一　資訊技術安全評估共通準則之評估過程

三、控管目標及建議的控管方法

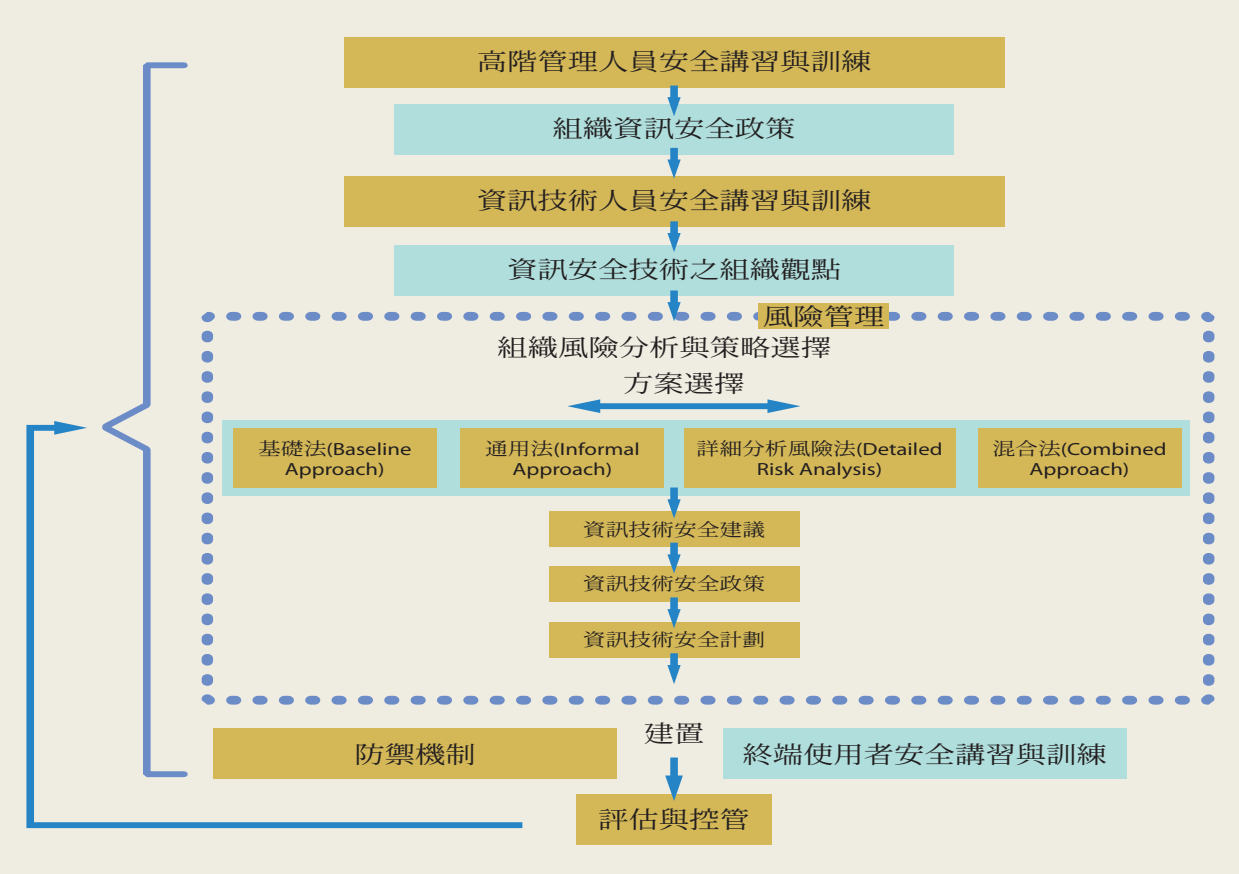
此部份是資訊安全指導方針的核心，此部份規定之控管功能是用來確保資訊及資訊處理的可用性，以及防制未經授權修改、揭露或是故意或意外的資訊破壞。金融人員可在他們的機構中以是否存在問題的角度來討論針對資訊的威脅。以下是四種用以支援其他控管重複出現的方法，以及電腦、網路、軟體、人為因素及特殊服務平台的控管與其適用性：

1.　安全控管之基礎方法：

- 資訊分類：並非所有在金融機構內的資訊都需要最高等級的安全控管，金融機構可將資訊分做重要性與敏感性來考慮不同的控管方式。
- 邏輯上的存取控制：利用一些存取控制方法，例如：使用者的識別控管、使用者鑑別控管、限制登入企圖控管、限制未授權終端機控管、作業系統存取控制特性控管、警告控管等，來確保只有被授權者在被授權的範圍下存取資訊或資訊處理設施。
- 稽核軌跡：稽核軌跡是一連串動作的紀錄。使用稽核軌跡可用來重建事件以及釐清責任歸屬。
- 變更控管：為了保護資訊處理系統的真確性，需要一個改變控管程序。當硬體改變、軟體改變及手動程序改變時，也必須配合改變控管程序。為了能達到效果，控管程序也具備處理緊急改變的能力。

2.　安全控管之一般方法：

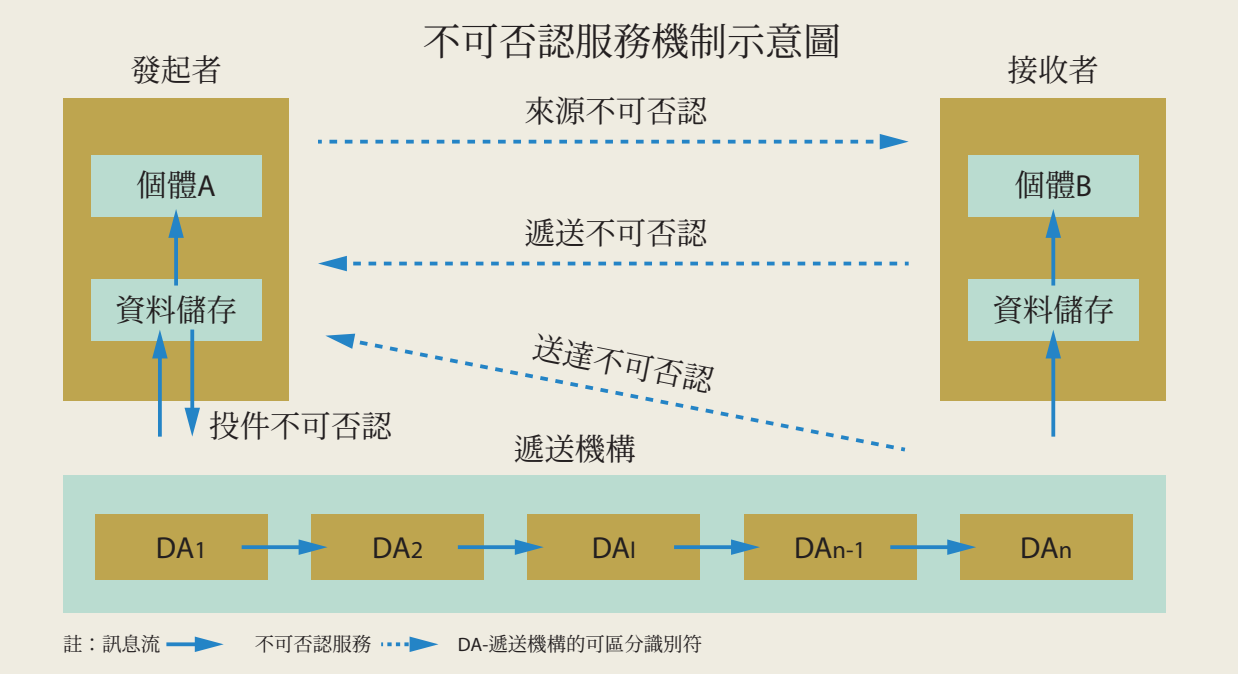
- 電腦：電腦是資訊安全討論的重心之一，其計算能力提供金融機構比以前更高的彈性，以及更強的處理能力。機構必須建置一些控管程序，例：實體保護控管、邏輯上的存取控制控管、系統改變處理控管、設備維護期間控管、電腦螢幕上的資訊揭露控管、自然災害或電力缺乏時控管、設備的報廢控管、分散式處理的控管…等等，來保護電腦的真確性。



圖二　資訊安全管理概觀架構圖

- 網路：網路是資訊處理資源與通訊資源的結合，它可能是簡單到兩個人電腦的連結，也可能複雜到全球性、多重機構、基金轉換的網路。保護網路之真確性的控管程序應該包括：網路真確性控管、存取控制控管、撥入控管、網路設備控管、網路改變期間控管、和其他網路連結時的控管、網路監督控管、資料傳輸保護控管、侵入偵測控管、自然災害或電力缺乏時的網路可用性控管、稽核軌跡…等等。
- 軟體：在金融範圍所使用的軟體是有高真確性的需求，因此也必須建置控管程序來保護軟體及該軟體所處理的資訊。這些控管程序包括：應用系統控管、資料庫控管、人工智慧技術控管、系統軟體控管、應用測試控管、有缺陷的軟體控管、軟體改變時的控管、軟體碼的可用性控管、非法軟體控管、軟體智慧財產權控管、病毒控管、記憶體常駐程式控管、遠端控管、提供給客戶的軟體控管…等等。
- 人為因素：任何的資訊安全計畫是否成功，人是相當重要的因素。因此如何控管員工也是相當重要的。員工的控管應包括：認知控管、管理人員控管、資訊資源的使用控管、員工雇用控管、資訊倫理政策控管、懲戒政策控管、詐欺偵測控管、早期的員工控管…等等。

- 聲音、電話及相關設備：聲音、電話及相關設備都是很容易暴露資訊，使之造成服務損失的設備，因此，應該使用控管程序來防止這些設備暴露語音及相關資訊。此類控管程序包括：存取語音郵件系統的控管、私人交換機控管、口語音信的控管、截聽控管、文件控管、語音回應單元控管、傳真與影像控管…等等。
- 電子郵件：由於電子郵件可在公眾或私人網路上運作，所以必須使用控管保護電子郵件。這一類的控管程序包括：使用者控管、電子郵件服務的實體設備控管、交易的真確性控管、資訊揭露控管、訊息保留控管、接收訊息控管…等等。
- 紙張文件控管：許多的決策製作資訊以及金融業的運作都是先透過紙張來進行的，所以紙張文件也必須控管。此類控管程序包括：資訊修改控管、未授權檢視控管、儲存設備控管、銷毀控管、企業永續性控管、保存證據控管、標示控管、偽造文件的控管、輸出分配方法控管…等等。
- 微縮影片及其他儲存媒體：微縮影片、縮影膠片以及大量儲存媒體可以儲存大量的資訊，因此應對微縮影片及其他儲存媒體進行控管以防止相關資訊的暴露。此類控管程序包括：資訊揭露控管、媒體破壞控管、企業永續性控管、儲藏環境控管…等等。
- 金融交易卡：使用金融交易卡的機構應該使用以下的金融交易卡控管：實體安全控管、內部人員的濫用控管、個人識別碼的傳送控管、人員控管、稽核控管、強制性的控管、防制偽造控管…等等。
- 自動櫃員機：自動櫃員機是允許客戶檢查帳戶餘額、提取現金、存款、支付帳單或執行其他一般與銀行出納人員相關功能的設備。自動櫃員機的控管包括：使用者識別控管、資訊傳輸控管、資訊揭露控管、詐欺預防控管、維護及服務期間的控管…等等。



- 電子資金移轉：電子資金移轉的控管包括：未經授權的來源控管、未經授權的改變控管、訊息重送的控管、記錄保留的控管、付款法律基礎的控管…等等。
- 金鑰管理：金鑰管理的良莠，攸關電子商務等使用上的安全，所以必須遵照國際標準的安全規範加以控管。金鑰管理的控管包括：金鑰的生成和啟始向量、金鑰的儲存與備援、秘密金鑰值與回復、金鑰分送、安全稽核日誌、秘密金鑰的保護、金鑰驗證、金鑰交換、金鑰的儲存、金鑰的歸屬、金鑰回復、金鑰使用結束…等等。
- 安全協定：密碼協定於設計之前，必須遵照結構化設計準則，完成之後，必須通過正規化分析證明，方能建置；有關存證的需求，必須遵照（圖三）及其說明之國際標準的安全規範。
- 敏感性資料：「無隱私、無貿易；事情就是如此單純 (No privacy, no trade. It's that simple.)。」，有關個人資料隱私，商業團體營業機密等敏感性資料均須遵照國際標準的安全規範加以控管。敏感性資料的控管包括：用途限制、資料品質、安全性、授權程序、獨立監督機制與救濟等。
- 法令遵行：遵守相關法令規範，並定期認證稽核。

結語

資訊安全指導方針的內容製訂了在建立及維護資訊安全措施時，必須遵循的一般方法，是資訊安全管理作業的基礎。植基於資訊安全指導方針，規劃、推動、控管資訊安全計畫將是通往可信賴的虛擬世界旅程中的必要工作。此外，於 ISO/TR 13569 1997(E) 中對於資訊隱藏學（Steganography）之圖像疊加、隱跡協議、浮水印等技術日益普及帶來之新的資訊安全風險特別要求加以考慮。

ISO/IEC 13888(1997)之存證證明示意：

1. 定義6個基本存證證明：
   - 1.1 產生存證 (non-repudiation of creation)。
   - 1.2 送件存證 (non-repudiation of sending)。
   - 1.3 收件存證 (non-repudiation of receipt)。
   - 1.4 知悉存證 (non-repudiation of knowledge)。
   - 1.5 投件存證 (non-repudiation of submission)。
   - 1.6 送達存證 (non-repudiation of transfort)。

2. 來源存證 (non-repudiation of origin) 可由結合產生存證與送件存證產生。

3. 遞送存證 (non-repudiation of delivery) 可由結合收件存證與知悉存證產生。

圖三　ISO/IEC 13888(1997) 之存證作業示意圖及其說明

個人資料保護法上路－我們準備好了嗎？

本篇摘自 2012 年 06 月出刊之財金資訊季刊第 71 期，由財金資訊公司安控部廖君美經理、安控部資訊安全組黃偉倫副組長（現任為組長）、稽核處檢查組許勇信高級管理師撰寫。

一、前言

鑒於科技日新月異，利用電腦蒐集、處理、利用個人資料之情形日漸普遍，再加上各類商務行銷廣泛大量蒐集個人資料，對個人隱私權之保護，造成莫大威脅。為規範個人資料之蒐集、處理及利用，以避免人格權受侵害，並促進個人資料之合理利用，電腦處理個人資料保護法修正案已於 99 年 5 月 26 日經總統公布，名稱則修正為「個人資料保護法」（以下簡稱「個資法」）。

個資法公告已屆滿兩年，施行細則之修正仍尚未定案，施行日期亦待行政院公告。然古有明訓：凡事豫則立，不豫則廢，本公司利用此過渡期間，面對個資新法之挑戰與衝擊，積極規劃執行相關因應措施與強化機制，並於 101 年 3 月通過 BS 10012:2009 個人資料管理系統驗證。期望在新法正式上路時，我們可以胸有成竹地說：我們準備好了！

二、「個資法」修正重點

「電腦處理個人資料保護法」係參酌「經濟合作暨發展組織」（OECD）所揭示之保護個人資料八大原則，於 84 年 8 月 11 日公布施行。而新版「個資法」則係因應急速變遷之社會環境，經彙集國內各方意見，並參酌各國立法案例所修正完成的，其修正重點簡述如下：

(一) 擴大保護客體：落實對個人資料之保護，不再以經電腦處理為限。

(二) 普遍適用主體：刪除行業別限制，涵蓋任何自然人、法人或團體。

(三) 增修行為規範：嚴格限制醫療、基因、性生活、健康檢查、犯罪前科等五類特種資料之蒐集、處理及利用；明訂個人資料蒐集、處理與利用之特定目的、合法要件、應告知事項及書面同意等規範。

(四) 強化行政監督：明訂中央目的事業主管機關與地方政府之行政檢查權，違法者得裁處罰鍰與行政處分。

(五) 促進民眾參與：增訂財團法人與公益社團法人提起團體訴訟之相關規定。
(六) 調整責任內涵：非公務機關之代表人、管理人或其他有代表權人，除能證明已盡防止義務者外，應並課以同額罰鍰，以加強其監督之責任。

法務部為順利推動「個資法」之施行，依據新法第 55 條，配合「個資法」修正內容，擬具「電腦處理個人資料保護法施行細則」（以下簡稱「施行細則」）修正草案，增修後共 28 條，於 100 年 10 月預告供各界表達意見或修正建議。法務部揭示「施行細則」之修正重點如下：

(一) 建立間接識別個人資料之標準。
(二) 界定敏感性個人資料之概念。
(三) 界定委託機關之權責。
(四) 界定書面意思表示之方式。
(五) 界訂單獨所為書面意思表示之方式。
(六) 告知義務之方式。

目前各界咸認新法仍有窒礙難行之處，對於「施行細則」部分內容亦有爭議待解，因此施行日期遲未定案。凡此種種，均有待行政院之衡酌與裁奪。

三、現況評估與差異分析

財金公司原本即受「電腦處理個人資料保護法」之規範，屬主管機關登記核准得電腦處理個人資料之非公務機關，並依據主管機關訂頒之「金融業個人資料檔案安全維護計畫標準」，訂有個人資料安全維護計畫書，分別就電腦處理個人資料之作業環境、存取權限、資料異動與輸出入之管理作業，採行各項安全維護措施。

「個資法」修正公告後，財金公司即全面清查各單位日常業務所可能接觸的個人資料，並檢視相關防護措施是否符合新法要求，同時評估現行個人資料保護機制與新版「個資法」要求之差異，以作為研擬相關因應對策之參考。此項評估作業於 99 年第四季完成，評估結果一如預期，多與新法之修正重點相關，摘要說明如下：

(一) 對於新法強調之個資蒐集、處理、利用應經當事人書面同意，並盡告知義務等事宜，應研訂相關規範與管理方式。
(二) 現有業務營運系統並無個人資料大量外洩之風險，未來將針對個人資料之儲存、內部處理或傳遞，視需要採行加密或遮罩等安全強化措施。
(三) 業務營運系統之個資保護措施相對完備，然而辦公室日常作業亦可能接觸個人資料，須進一步檢討並強化其保護管理機制。
(四) 現行防護措施多係對電子資料而訂，對於紙本型式之個人資料，亦應建立安全管理與維護機制。
(五) 因應舉證責任倒置，除建立良善之管理機制外，必須加強相關證據與軌跡紀錄之保存，以利事件追查與無故意或過失之證明。

四、因應措施與強化機制

因應「個資法」之修正公告，財金公司除邀請政府及業界專家，舉辦多場講座或研討會，以提升全公司同仁對新版「個資法」之認知外，並依據前述「個資法」符合性之差異分析評估結果及改善方向，自 100 年起陸續啟動多項專案，於技術面強化資料防護措施，於制度面建立個人資料管理系統（詳參下節），致力於符合「個資法」之各項要求。

有關強化資料防護措施之專案規劃，係考量以下作業原則：

- 資料去識別化：資料蒐集應以最小必要為原則，人員存取應以職務所需為準據，針對非必要揭露之個人資料欄位，應用系統程式或使用者介面應採行遮罩或刪除等去識別化之作為。
- 存取軌跡紀錄：個人資料存取之軌跡紀錄應可明確識別存取行為之人、事、時、地、物，並考量軌跡紀錄留存之完整性，以確保其證據能力。
- 資安產品輔助：採購資安產品並非因應「個資法」之必要選項，惟仍應與時俱進，適時考量作業風險，選用適當且必要之解決方案，以提升整體安全強度。

自 100 年至今陸續執行的各項專案（如下所列），除部分將於 101 年 6 月完成外，其餘均已完成，對於提升個人資料安全防護強度，應具相當成效：

(一) 針對使用者介面與資料庫存取作業，建立資料遮罩機制，並推動應用系統軌跡資料留存之改善作業，以強化營運資料存取控管，降低個人資料外洩之風險，並提高證據保存的有效性。

(二) 建置個人電腦作業環境之端點防護系統，加強可攜式儲存媒體與無線通訊設備等輸出介面之存取控管，以申請覆核、資料加密、軌跡記錄等多重措施，降低個人資料不當輸出之風險。

(三) 導入點對點之資料保護機制，針對有內、外部傳輸需求之機敏資料，進行加密保護，僅限指定之接收者可解密取得資料。

(四) 強化網路出入口防護，提升對外存取網際網路閘道設備之管理效能，針對惡意或不安全網站（如：釣魚、社交或網路郵件網站等）設置過濾機制，降低公司同仁因誤入惡意網站而可能導致之資料外洩風險。

(五) 設置紙本個人資料實體保管設施，並指定專人保管。另於業務營運區建置印表機管控系統，針對營運資料之列印輸出，建立覆核放行機制，並留存列印紀錄，以強化紙本資料之管控。

(六) 持續改善強化各項主機及資料庫系統之存取控管，包含系統權限調整、軌跡紀錄自動化比對、資料庫軌跡紀錄強化、伺服器檔案自動清整、資料輸出入執行監控等作業。

五、個人資料管理系統之建立

財金公司規劃個人資料管理制度之初，曾參考國內外相關標準規範，包含經濟部商業司推動之臺灣個人資料保護與管理制度（簡稱 TPIPAS），惟囿於業務性質並不適用。最後決定以「個資法」與 BS 10012 為建立管理制度之圭臬，係考量二者擬訂之初，均參照 OECD 揭示之個人資料保護八大原則為其法理基礎，

PDCA 之循環運作機制亦與本公司現行各管理系統（包含資訊安全、品質與業務持續運作等）類似，應有助於各項作業之推動或整合。

而法務部針對「個資法」所稱之適當安全維護措施之事項內容，於「施行細則」修正草案第 9 條第 2 項明確指出係參考 BS 10012 及日本 JIS Q 15001 等個人資料管理規範，以 PDCA 方法論予以建立，正與本公司之決定不謀而合。

財金公司自 100 年第二季起開始辦理個人資料管理系統導入專案，比照 ISO 27001 資訊安全管理系統，適用範圍涵蓋全公司所有服務與業務活動，歷經九個多月，於 101 年 3 月 16 日修成正果，經英國標準協會（BSi）台灣分公司審查通過 BS 10012:2009 驗證，開創我國金融機構之首例。

個人資料管理系統之建置過程與其他管理系統大同小異，以下僅就個人資料管理系統較為專屬特有的事項，簡單介紹工作內容。

(一) 確立管理組織：

參考個人資料保護法及國際標準之要求，建立個人資料管理組織，並明確定義權責。財金公司之管理組織原則上參照現行其他管理系統，以利日後相關作業之整合。

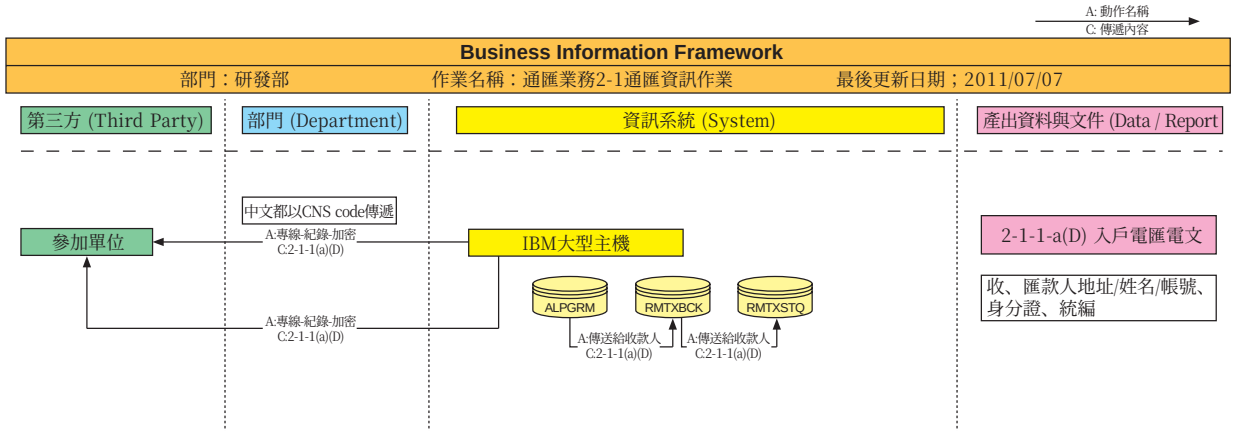
(二) 個人資料檔案清查：

清查個人資料檔案是個人資料管理作業最基本、也最耗時費心的工作項目，面對可能隱身於業務流程背後深處的個人資料，如何有效清點、分級與造冊列管，成為專案過程必須持續面對的挑戰。

財金公司係經由各單位業務流程，分析個人資料之生命週期，釐清蒐集、處理、利用及傳輸等作業現況，包含相關內外部單位、資訊系統及衍生之電子檔案及紙本文件等，以作為建立個人資料檔案項目清單之基礎。

個人資料之敏感性與識別程度各有不同，為規劃合理而符合實務需求的控管方式，財金公司考量法規要求及資料組合之可識別程度，將個人資料分為二種等級：含「個資法」所列之特種資料或可直接識別特定當事人者，均視為機密資料；而公務聯繫資料或可間接識別特定當事人者，則視為一般內部使用資料。

綜合前述分析與分級結果，各單位即可針對其管理範圍內之個人資料檔案建立項目清單，記載以下資訊：



- 基本資訊：作業項目、檔案名稱與型態（電子、紙本）、個人資料內容（如：姓名、帳號）與等級、特定目的及依據、管理單位等。
- 蒐集現況：資料來源、蒐集之類型（直接或間接）、方式（電話、傳真等）及當事人告知辦理情形等。
- 處理利用及傳輸現況：存放位置、保存期限、存取控管現況、外部傳輸、傳輸方式及保護機制等。

(三) 衝擊分析與風險評鑑

針對全公司個人資料管理之現況，分別就制度面之法令遵循與管理需求及技術面之安控防護措施，依據個資保護相關法規及管理標準之符合性，進行衝擊分析與風險評鑑，針對風險值超過風險可接受水準之項目，擬定處理計畫，實施各項改善方案。

(四) 作業流程與文件增修

財金公司已建立品質、資訊安全及業務持續運作等管理系統，管理作業與文件框架相對完備，惟個人資料管理系統首重「個資法」之遵循性，BS10012 對於個資保護亦有深入而廣泛的要求。財金公司除增訂個人資料管理之政策、目標、組織權責等必要項目外，並針對個人資料檔案項目清單之日常管理維護、個人資料當事人依法行使相關權利之處理、個人資料侵害事件之應變處理及鑑識等重要作業增修相關程序文件。

(五) 教育訓練

人員是所有管理系統共通的核心環節，提升人員對於個資保護的認知，了解相關權責及作業規範，可有效避免違法異常事件之發生。財金公司於專案期間針對基礎認知（「個資法」之衝擊與因應、個資管理標準、個資法令宣導等）、管理作業（個人資料清查辨識、風險評鑑、內部稽核等）及專業技術（事件鑑識與證據保全、系統安全稽核記錄等）等主題，辦理多場教育訓練，對象涵蓋全公司員工及保全、清潔等委外人員。專案結束後，重要基礎課程將列入每年度教育訓練計畫之規劃範圍。

個人資料之取得利用必須合理適當並揭露給當事人，以保障人格權與隱私權，這是先進國家個資保護的法理基礎，亦是新版「個資法」的核心價值。財金公司於新法正式實施前，積極導入個人資料管理制度，逐步落實各項管理作業，並在高層支持與全員投入之下，順利通過 BS 10012:2009 驗證，實具有多重效益：

- 提升全體同仁之個資保護認知，及早因應新法要求，並與國際標準接軌。
- 具體展現對人格權與隱私權之尊重，符合社會大眾對於企業保護個人資料之深切期待。
- 預先完成「施行細則」修正草案所要求之安全維護措施事項，可視為善盡良善管理責任之具體實績。

六、結語

本次「個人資料保護法」修正的涵蓋範圍極廣，影響層面極深，雖然修法單位已蒐集各界意見與建議，字斟句酌，各產業對於條文內容仍多所疑義，故施行時點、相關法規及配套措施均有待確立。

個人資料管理制度之建立與安全防護措施之強化，不應只是因應「個資法」修正的權宜措施，而階段性任務的達成也不代表從此萬無一失。個人資料管理不是企業中某一單位的責任，每位員工對於日常作業所接觸的個人資料，均應謹慎處理，妥善保護。唯有秉持持續改善的精神，落實 PDCA 的維運機制，將個人資料保護的觀念深植在企業文化中，才能因應環境、技術與法規之變遷，確實保障人格權，促進個人資料之合理利用。

※ 參考文獻 / 資料來源：

1. 法務部，電腦處理個人資料保護法修正草案總說明，2006/10/13。
2. 法務部新聞稿，預告「電腦處理個人資料保護法施行細則」修正草案，2011/10/26。

從「電子支付機構管理條例」展望國內電子金融服務發展

本篇摘自 2015 年 07 月出刊之財金資訊季刊第 83 期，由財金資訊公司業務部范姜群暐經理撰寫。

一、前言

鑒於資通訊技術與行動裝置的成熟普及，電子商務與行動商務隨之快速發展，新興的網路服務在不同領域、不同層面強勁擴展，消費大眾的付款情境也因而跳脫原有的固定模式，支付型態更面臨快速改變的衝擊與挑戰，各式各樣、五花八門的支付方式，琳琅滿目令人目不暇給，國際上非金融機構紛紛推出以網路做為金融輔助工具的「互聯網金融」(註 1) 服務，以突破性巧思搶食傳統金融市場，熱門的「第三方支付」更是異軍崛起、蓬勃發展，尤其美國 PayPal (註 2) 與中國大陸支付寶 (註 3) 呈星火燎原之勢，藉由網路第三方信賴功能，提供安全、快速、便宜的網路支付機制，取得爆發式的傲人業績。

面對第三方支付來勢洶洶的發展影響，國內相關網路電子商務供應商 (以下稱網路電商) 百花齊放、蓄勢待發，為達成「銀貨兩訖、完成交易」的市場需求，網路電商顛覆傳統金融服務市場區隔，企圖跨界扮演買賣雙方金流服務的角色，從單純代理收付的灰色地帶切入，或增加提供類似履約擔保功能的中介平台，或發展足敷交易扣款需求之儲值帳戶，期望建立保障網路交易雙方的信任關係，因此被迫應戰的金融機構與應運而生的網路電商紛紛加強創新變革，改善作業流程，整合資訊流、金流與物流，藉由滿足「交易保障及網路信任」的市場需求，期待在電子商務發展的浪潮中，能夠搏得先機且開花結果。

然而因為網路電商提供線上金流服務，違反銀行法第 29 條「除法律另有規定者外，非銀行不得經營收受存款、受託經理信託資金、公眾財產或辦理國內外匯兌業務。」因此，為保障消費者權益，金融監督管理委員會 (以下稱金管會) 102 年 3 月准予備查「信用卡收單機構簽訂提供網路交易代收代付服務平台業者為特約商店自律規範」，102 年 8 月准予備查「銀行受理客戶以網路方式開立儲值支付帳戶作業範本」，103 年 1 月修正「信用卡業務機構管理辦法」，雖然促使相關電子商務支付市場獲致一些進展，但國內網路電商服務品質參差不齊，而且提供第三方支付沒有法律可依據，國內金融機構面對新種型式的支付也欠缺明確的規範，致國內電子支付發展步履蹣跚，因此在各界殷切期盼中，「電子支付機構管理

條例」(俗稱第三方支付專法，以下簡稱本條例)歷經篳路藍縷，終於在104年1月16日經立法院三讀通過，並經 總統於2月4日公布，5月3日正式生效施行，期提供民眾安全便利之資金移轉服務，以建立消費者使用電子支付之信心，降低小額交易支付成本，營造小型及個人商家發展之有利經營環境。

二、「電子支付機構管理條例」摘述

(一) 本條例計58條，分為六章，如下表所列：

章次	名稱	條次	內容重點
第一章	總則	第1條至第6條	立法目的、主管機關、定義及規範對象、經營業務項目、收受使用者支付款項之範圍
第二章	申請及許可	第7條至第14條	最低實收資本額、不得經營之業務、得兼營電子票證業務、申請應檢具之書件與應及不得記載事項、主管機關得不予許可之事由、執照核發與開業及廢止、與境外機構合作之管理
第三章	監督及管理	第15條至第41條	款項移轉限額及交易金額限制、支付款項管理、款項支付方式、提領及存撥、準備金繳存、履約保證、優先受償權、結清算幣別、交易紀錄留存、建置客訴處理及紛爭解決機制、定型化契約之管理規範、資料保密、安全控管作業基準、建立內控內稽制度、申報及公告文件、金融檢查、違法之處分、退場機制、清償基金、兼營之電子支付機構
第四章	公會	第42條至第43條	加入公會始得營業、公會業務規章及自律公約
第五章	罰則	第44條至第53條	相關罰則
第六章	附則	第54條至第58條	日出條款、施行日

(二) 本條例相關授權法規命令(俗稱子法)如下：

1. 對於僅經營代理收付實質交易款項業者，規範排除適用對象之一定金額。
2. 與境外機構合作或協助境外機構於我國境內從事電子支付機構業務相關行為管理辦法。
3. 電子支付機構使用者身分確認機制及交易限額管理辦法。
4. 電子支付機構專用存款帳戶管理辦法。
5. 電子支付機構支付款項信託契約應記載事項及不得記載事項。
6. 規範儲值款項得運用及支付款項運用收益應計提之一定比率，於專用存款帳戶銀行以專戶方式儲存，作為回饋使用者或其他主管機關規定用途使用。
7. 電子支付機構業務定型化契約範本、應記載事項及不得記載事項。
8. 電子支付機構提供使用者往來交易資料及其他相關資料要點。
9. 電子支付機構資訊系統標準及安全控管作業基準辦法。

10. 電子支付機構內部控制及稽核制度實施辦法。
11. 電子支付機構業務管理規則。
12. 電子支付機構清償基金組織及管理辦法。
13. 非銀行支付機構儲值款項準備金繳存及查核辦法。

三、規範對象與經營業務範圍

(一) 本條例以「電子支付機構」為規範對象，重要定義如下 (第三條、第五條)：

1. 電子支付機構：限以「網路或電子支付平臺為中介」方式提供服務，接受使用者註冊及開立記錄資金移轉與儲值情形之「電子支付帳戶」，並利用電子設備以連線方式傳遞收付訊息，於付款方及收款方間經營資金移轉、儲值業務之「股份有限公司」。
2. 非透過以「網路或電子支付平臺為中介」方式提供服務者，非本條例規範之對象。
3. 利用電子設備以連線方式傳遞收付訊息：本條例所謂電子設備不限於傳統桌上型電腦，亦包含行動載具，例如平板電腦、行動電話等可攜式設備，或其他得以連線方式傳遞訊息之設備亦屬之。
4. 電子支付帳戶：指電子支付機構接受使用者開立記錄資金移轉及儲值情形之網路帳戶，俗稱「網路虛擬帳戶」，與金融機構所開立實體活期性存款帳戶不同。
5. 專營之電子支付機構與兼營之電子支付機構：因電子支付機構得兼營電子票證業務 (第九條)，故本條例所稱電子支付機構包含「專營之電子支付機構」、「兼營之金融機構」(銀行、中華郵政股份有限公司) 及「兼營之電子票證發行機構」。(第三十九條、第四十條、第四十一條)
6. 管理銀行與合作銀行：電子支付機構僅得選擇一銀行為「專用存款帳戶管理銀行」，各幣別管理帳戶以一戶為限，並得視業務需要選擇「專用存款帳戶合作銀行」，於單一合作銀行之各幣別合作帳戶以一戶為限。(「電子支付機構專用存款帳戶管理辦法」第七條、第八條)
7. 專用存款帳戶：指電子支付機構應依法於銀行開立，專用以儲存使用者支付款項之活期存款帳戶。專用存款帳戶名稱應敘明為「專用存款管理帳戶」、「專用存款合作帳戶」、「受託信託財產專用存款管理帳戶」或「受託信託財產專用存款合作帳戶」，並標明該電子支付機構名稱。(「電子支付機構專用存款帳戶管理辦法」第十三條)

(二) 「電子支付機構」之經營業務範圍為下列四項 (第三條、第四條、第六條)：

1. 代理收付實質交易款項

基於實質交易之代理收付款項，或稱為「實質交易基礎之資金移轉」，係指付款方及收款方因資金移轉而記錄於電子支付帳戶內之款項，意即以實質商品或服務交易為基礎之交易金額。

電子支付機構以代理收付實質交易款項為必要業務項目。本條例所規範之附隨業務項目係以有經營代理收付實質交易款項為限，故其餘三項業務 (收受儲值款項、電子支付帳戶間款項移轉、其他經主管機關核定之業務) 均屬必要業務所衍生之附隨業務項目。

電子支付機構獨立於實質交易之付款方及收款方以外，依交易雙方委任，接受付款方所移轉實質交易之金額，並經一定條件成就、一定期間屆至或付款方指示後，將該實質交易之金額移轉予收款方（「電子支付機構業務定型化契約範本」）。

本條例所規範經營業務項目均包含實體通路交易（線下交易）之支付服務（即 O2O, Online To Offline）型態，但涉及外匯部分，仍應依中央銀行規定辦理。（第四條）

基於監理重要性原則，避免對既有單純僅提供代理收付款項業者造成過大影響，依本條例第三條第二項之子法，僅經營代理收付實質交易款項業務，且所保管代理收付款項總餘額未逾新臺幣十億元，即非屬本條例所規範之電子支付機構。既然非屬本條例適用對象，即應回歸一般商業管理，由經濟部依現行既有機制進行管理。前述總餘額係指經營代理收付實質交易款項業務所保管使用者代理收付款項之一年日平均餘額。（「電子支付機構管理條例第三條第二項授權規定事項辦法」第二條及第三條）

2. 收受儲值款項

預先接受社會大眾資金，存放於電子支付帳戶之儲值款項，以供與電子支付機構以外之其他使用者進行資金移轉使用之款項，意即付款方於資金移轉前，先行預儲並記錄於電子支付帳戶內之款項，俗稱「網路帳戶儲值」，本業務屬衍生之附隨業務項目。

3. 電子支付帳戶間款項移轉

非基於以實質交易資金移轉為範圍之電子支付帳戶間款項移轉，俗稱「無實質交易之資金移轉」或「無實質交易的轉帳」，意即電子支付機構依使用者非基於實質交易之支付指示，將其電子支付帳戶內之資金，移轉至電子支付機構其他使用者電子支付帳戶，本業務屬衍生之附隨業務項目。

4. 其他經主管機關核定之業務

因應未來創新與發展之保留空間，本業務屬衍生之附隨業務項目。

四、電子支付機構之資本額與業務限額

（一）最低實收資本額

電子支付機構之最低實收資本額為新臺幣五億元，發起人應於發起時一次認足，主管機關得視未來社會經濟情況及業務實際需要適時衡酌調整之。但僅經營代理收付實質交易款項業務，且所保管代理收付款項總餘額未逾新臺幣十億元者，最低實收資本額為新臺幣一億元。（第七條）

（二）儲值限額

每一使用者於電子支付帳戶中收受儲值款項之餘額上限不得超過等值新臺幣五萬元，係指每一使用者新臺幣及外幣儲值之餘額合併計算，超過該限額即無法進行儲值。（第十五條）

使用者得透過電子支付機構同意之方式，於電子支付帳戶存入儲值款項，且儲值限額應明訂於「電子支付機構業務定型化契約」。電子支付機構不接受使用者以信用卡方式進行儲值。（「電子支付機構業務定型化契約應記載事項」第四點）

(三) 電子支付帳戶間款項移轉限額

電子支付帳戶間款項移轉之每筆上限等值新臺幣五萬元，係指每一使用者新臺幣及外幣電子支付帳戶間款項移轉之每筆金額併計不得超過等值五萬元。(第十五條)

使用者依電子支付機構指定方式進行支付指示，電子支付機構應於支付完成前，由付款方再確認；支付指示完成後，應以雙方約定之方式通知使用者。電子支付帳戶間款項移轉限額應明訂於「電子支付機構業務定型化契約」。電子支付機構不接受使用者以信用卡方式辦理電子支付帳戶間款項移轉。(「電子支付機構業務定型化契約應記載事項」第四點及第五點)

(四) 依不同身分認證等級之電子支付帳戶交易限額

因為電子支付機構之業務主要屬小額零售支付及資金移轉性質，且基於防制洗錢考量，電子支付機構依身分認證等級嚴謹程序之不同，而對使用者每月累計付款金額、每月累計收款金額及帳戶餘額，分別訂定不同金額上限。(「電子支付機構業務定型化契約應記載事項」第四點)

1. 第一類電子支付帳戶

(1) 限個人使用者。
(2) 以行動電話號碼及電子郵件信箱或社群媒體帳號，並輔以向相關機關查詢身分證明文件資料之真實性作為身分確認之程序；無法依後者確認使用者身分證明文件資料者，其電子支付帳戶不具儲值功能。
(3) 此類帳戶得具代理收付實質交易款項之付款及儲值功能，無收款及電子支付帳戶間款項移轉之付款功能，每月累計代理收付實質交易款項之付款金額，以等值新臺幣三萬元為限；儲值餘額以等值新臺幣一萬元為限。

(「電子支付機構使用者身分確認機制及交易限額管理辦法」第六條、第八條及第十七條)

2. 第二類電子支付帳戶

(1) 含個人使用者及非個人使用者。
(2) 由於非個人使用者多屬收款方角色，除第一類之身分確認程序外，應確認使用者本人之金融支付工具。
(3) 此類帳戶得具收款、付款及儲值功能，每月累計收款及付款金額，分別以等值新臺幣三十萬元為限。

(「電子支付機構使用者身分確認機制及交易限額管理辦法」第六條、第九條及第十七條)

3. 第三類電子支付帳戶

(1) 含個人使用者及非個人使用者。
(2) 除第二類之身分確認程序外，增加以臨櫃審查或符合電子簽章法之憑證確認使用者之身分。
(3) 此類帳戶得具收款、付款及儲值功能，每月累計代理收付實質交易款項之收款及付款金額，由電子支付機構與使用者約定之；個人使用者每月累計電子支付帳戶間款項移轉之收款及付款金額，分別以等值新臺幣一百萬元為限；非個人使用者每月累計電子支付帳戶間款項移轉之收款及付款金額，分別以等值新臺幣一千萬元為限。

(「電子支付機構使用者身分確認機制及交易限額管理辦法」第六條、第十條及第十七條)

茲整理不同身分認證等級之電子支付帳戶交易限額如下表：

電子支付帳戶	使用者	實質交易款項	電子支付帳戶間款項	儲值餘額
第一類	限個人	每月累計付款限額 3 萬元	無付款功能	限額 1 萬元
		無收款功能	無收款功能	
第二類	含個人及非個人	無每筆交易限額	每筆交易上限 5 萬元	限額 5 萬元
		每月累計付款限額 30 萬元		
		無每筆交易限額	每筆交易上限 5 萬元	
		每月累計收款限額 30 萬元		
第三類	個人	由電子支付機構與使用者約定每月累計付款金額	每筆交易上限 5 萬元，每月累計付款限額 100 萬元	限額 5 萬元
		由電子支付機構與使用者約定每月累計收款金額	每筆交易上限 5 萬元，每月累計收款限額 100 萬元	
	非個人	由電子支付機構與使用者約定每月累計付款金額	每筆交易上限 5 萬元，每月累計付款限額 1,000 萬元	
		由電子支付機構與使用者約定每月累計收款金額	每筆交易上限 5 萬元，每月累計收款限額 1,000 萬元	

註：同一使用者於同一電子支付機構開立一個以上之電子支付帳戶時，各帳戶收款及付款金額不得超過該帳戶類別之限額，歸戶後總限額不得超過該使用者註冊及開立電子支付帳戶中最高類別之限額。(「電子支付機構使用者身分確認機制及交易限額管理辦法」第十八條)

五、電子支付機構相關六項管理方法

(一) 採許可制，屬金融特許行業

1. 「本條例所稱電子支付機構，指經主管機關許可」，採「許可制」，賦予非金融機構經許可後，以電子支付帳戶方式辦理儲值及資金移轉業務。(第三條)
2. 申請經營電子支付機構業務許可應檢具之書件。(第十條)
3. 主管機關於電子支付機構營業執照載明得經營之業務項目，涉及跨境者，一併載明之；電子支付機構不得經營未經主管機關核定之業務。(第八條)
4. 為維護我國人民及業者權益，並確保我國金融市場秩序及有效監督管理，境外機構非經申請許可，不得於我國境內經營電子支付機構業務，換言之，境外機構如果要在我國經營電子支付業務，必須依本條例申請許可設立電子支付機構；且非經主管機關核准，任何人不得有與境外機構合作或協助其於我國境內從事電子支付機構業務之相關行為；涉及陸資部分，則須符合「臺灣地區與大陸地區人民關係條例」規定，故規範「與境外機構合作或協助境外機構於我國境內從事電子支付機構業務相關行為管理辦法」。(第十四條)

(二) 確保支付款項安全

1. 電子支付款項之管理 (第十六條)

因為電子支付機構收受使用者之支付款項應與其自有資金分別管理，以保障使用者權益，故專營之電子支付機構收取使用者之支付款項，應存入其於銀行開立之相同幣別專用存款帳戶，並確實於電子支付帳戶記錄支付款項金額及移轉情形。

對於專用存款帳戶開立之限制、管理與作業方式及其他應遵行事項，以「電子支付機構專用存款帳戶管理辦法」規範之。

2. 專營之電子支付機構支付款項之方式 (第十七條)

為確保支付款項之安全，專營之電子支付機構應依各方使用者之支付指示，進行支付款項移轉作業，不得有遲延支付之行為。

3. 支付款項應交付信託或取得銀行十足之履約保證，並設置清償基金 (第二十條、第三十八條)

為避免電子支付機構未將支付款項交付信託，或未取得銀行十足履約保證，導致日後違約影響消費者權益，基於專營之電子支付機構及兼營電子支付機構業務之電子票證發行機構所收儲值款項性質類似，故參酌「電子票證發行管理條例」第十八條規定，要求專營之電子支付機構對於儲值款項扣除應提列準備金之餘額，併同代理收付款項之金額，應全部交付信託或取得銀行十足之履約保證。採交付信託方式者，其信託銀行即為專用存款帳戶銀行，並以專用存款帳戶為信託專戶。(第二十條)

為避免電子支付機構未依第二十條交付信託或取得銀行十足履約保證，而損及消費者權益，電子支付機構應提撥資金設置「清償基金」，若電子支付機構因財務困難失去清償能力致違約時，清償基金得以第三人之地位向消費者進行清償，至於清償基金之提撥比率，由金管會訂定。(第三十八條)

4. 支付款項動用與運用方式、運用所得孳息或其他收益計提一定比率之金額及使用者之優先受償權 (第二十一條)

規定專營之電子支付機構可動用支付款項之條件及運用方式。

專營之電子支付機構對於代理收付款項，限以專用存款帳戶儲存及保管，不得為其他方式之運用或指示專用存款帳戶銀行為其他方式之運用。

專營之電子支付機構對於儲值款項之運用方式，參考「電子票證發行管理條例」第十九條規定，於一定比率內容許從事低風險之投資運用。

(三) 落實使用者身分確認

專營之電子支付機構應建立使用者身分確認機制，並留存確認使用者身分程序所得之資料範圍；有關使用者身分確認機制之建立方式、程序、管理及該程序所得資料範圍等相關事項，規範於「電子支付機構使用者身分確認機制及交易限額管理辦法」。(第二十四條)

(四) 執行洗錢防制

1. 電子支付款項之提領與儲值 (第十八條)

專營之電子支付機構保管支付款項非屬存款業務性質，且基於洗錢防制目的，為使實際資金流向及歸屬得以確認，於使用者提領電子支付帳戶款項時，不得以現金支付，應將提領

款項轉入該使用者之銀行相同幣別存款帳戶。

鑒於幣別兌換涉及匯率訂定及外幣交易等事宜，非屬電子支付機構業者所承辦業務之內容，為不涉及幣別之兌換，應由使用者以其本人在銀行外匯存款帳戶之相同幣別存撥之；即所規範之「使用者辦理外幣儲值時，儲值款項非由該使用者之銀行外匯存款帳戶以相同幣別存撥者，不得受理。」

2. 應建立使用者資料留存期限（第二十四條）

使用者身分確認程序所得資料之留存期間，係自電子支付帳戶終止或結束後至少五年。

3. 交易紀錄資料之留存（第二十五條）

留存使用者電子支付帳戶之帳號、交易項目、日期、金額及幣別等必要交易紀錄，於停止或完成交易後，至少應保存五年。

（五）保護消費者權益

1. 客訴處理及紛爭解決機制

為確保消費者之權益，提升支付服務品質，專營之電子支付機構應建置並於其網站公告客訴處理及紛爭解決機制。（第二十六條及「電子支付機構業務管理規則」第四條）

2. 電子支付機構業務定型化契約之管理規範（第二十七條）

規範「電子支付機構業務定型化契約應記載事項」，明訂電子支付機構資訊、同意及確認事項、身分資料留存及再確認、依身分認證等級對不同類型電子支付帳戶所提供服務之交易限額、儲值餘額及每筆款項移轉最高限額、核對機制、錯誤之處理、帳號安全性與被冒用之處理、資訊系統安全控管與舉證責任及損失責任、費用說明、匯率計算、履約保證機制、使用者義務、收款使用者特別約定事項、紀錄保存、客訴處理及紛爭解決機制、使用者資料之蒐集處理及利用、服務暫停事由與處理、因使用者事由所致之服務暫停、契約終止、契約條款變更、定型化契約解釋原則、通知、作業委託他人處理等應記載事項。

規範「電子支付機構業務定型化契約不得記載事項」，明訂不得約定拋棄契約審閱期間、不得記載使用者因其帳戶遭不法使用所生之損失一律由使用者自行負擔、不得就其提供服務所生爭議不負任何責任、單方變更契約之禁止、不得任意解除或終止契約及免除賠償責任、不得約定使用者拋棄或限制使用者依法享有之契約解除權或終止權、不得以契約約定排除有利於使用者之廣告應為契約之內容、不得為其他違反法律強制、禁止之規定或其他違反誠信、顯失公平之約定、不得記載電子支付機構僅負故意或重大過失責任等不得記載事項。

（六）完善資訊系統及安全控管作業

為確保電子支付機構之交易資訊安全及業務健全運作，避免因資訊系統運作、傳輸或處理錯誤，影響服務之穩定與安全，衍生相關糾紛，故規範「電子支付機構資訊系統標準及安全控管作業基準辦法」。（第二十九條）

六、電子支付機構相關七項風險控管機制

(一) 銀行協助管理專用存款帳戶運作

1. 電子支付款項之管理 (第十六條)

銀行對專營之電子支付機構所儲存支付款項之存管、移轉、動用及運用，應予管理，並定期向主管機關報送其專用存款帳戶之相關資料。

對於專用存款帳戶開立之限制、管理與作業方式及其他應遵行事項，以「電子支付機構專用存款帳戶管理辦法」為規範。

2. 業務資料之申報與提交 (第三十一條)

專營之電子支付機構應向主管機關及中央銀行申報業務有關資料，以應監理之需。

專營之電子支付機構應定期提交帳務作業明細報表予專用存款帳戶銀行，供銀行核對支付款項之存管、移轉、動用及運用情形，以協助主管機關監督專用存款帳戶之運作情形，確保使用者支付款項安全。

(二) 收受儲值款項達一定金額應繳存準備金

收受新臺幣及外幣儲值款項達一定金額以上者，應繳存足額之準備金。(第十九條)

專營之電子支付機構收受新臺幣及外幣儲值款項雖非銀行法等法令所稱銀行存款，但仍屬多用途支付工具，具有交易中介、替代通貨之功能。為保持儲值款項之高度流動性，合計達一定金額者，應繳存足額之準備金，故規範儲值款項超過 50 億元者，依新臺幣及外幣繳存比率計算產生之合計數，以新臺幣繳存準備金。(「非銀行支付機構儲值款項準備金繳存及查核辦法」)

(三) 支付款項運用收益應計提一定比率金額作為回饋會員及其他主管機關規定用途使用

專營之電子支付機構對於運用支付款項所得之孳息或其他收益，應計提一定比率金額，於專用存款帳戶銀行以專戶方式儲存，作為回饋使用者或其他主管機關規定用途使用。(第二十一條)

(四) 於必要時，得就電子支付機構收受款項總餘額與該公司實收資本額或淨值之倍數，予以限制

為健全專營之電子支付機構業務經營與財務基礎，主管機關得限制電子支付機構收受使用者之支付款項總餘額與該公司實收資本額或淨值之倍數，不符者，主管機關得命其限期增資或降低其所收受使用者之支付款項總餘額，並為其他必要之處置或限制。(第二十三條)

(五) 建立內部控制及稽核制度

為健全專營之電子支付機構經營管理，強化其內部控制及稽核制度，專營之電子支付機構應建立內部控制及稽核制度。(第三十條)

主管機關參酌金融控股公司及銀行業內部控制及稽核制度實施辦法、信用卡業務機構內部控制及稽核制度應注意事項、公開發行公司建立內部控制制度處理準則等規定，規範「電子支付機構內部控制及稽核制度實施辦法」，明訂目的、原則、政策、作業程序、內部稽核人員應具備之資格條件、委託會計師辦理內部控制查核之範圍及其他應遵行事項。

(六) 會計師查核及金融檢查制度

1. 專營之電子支付機構應委託會計師每季查核「支付款項應交付信託或取得銀行十足之履約保證」之辦理情形，並於每季終了後一個月內，將會計師查核情形報請主管機關備查。(第二十條)
2. 專營之電子支付機構應委託會計師每半營業年度查核其對於「支付款項」、「代理收付款項」、「儲值款項」、「運用支付款項收益之計提」、「運用支付款項總價值之評價及補足」等辦理情形，並於每半營業年度終了後二個月內，將會計師查核情形報請主管機關備查。(第二十一條)
3. 專營之電子支付機構應每年委託會計師辦理內部控制制度之查核。(第三十條及「電子支付機構內部控制及稽核制度實施辦法」第二十六條)
4. 專營之電子支付機構之財務報告或其他經主管機關指定之財務文件，應經會計師查核簽證，並定期公開。(第三十二條)
5. 主管機關之金融檢查及查核。(第三十四條)

主管機關得隨時派員或委託適當機構檢查專營之電子支付機構之業務、財務及其他有關事項，或令專營之電子支付機構於限期內提報財務報告、財產目錄或其他有關資料及報告。並於必要時，得指定專門職業及技術人員檢查專營之電子支付機構之業務、財務及其他有關事項。

(七) 累積虧損逾實收資本額二分之一之因應措施及退場機制

1. **累積虧損逾實收資本額二分之一之因應措施(第三十六條)**

為避免專營之電子支付機構因財產、業務顯著惡化發生經營危機，而影響使用者權益，專營之電子支付機構累積虧損逾實收資本額二分之一者，應立即將財務報表及虧損原因，函報主管機關。主管機關得限期令其補足資本，或限制其業務；專營之電子支付機構未依期限補足資本者，主管機關得勒令其停業。

2. **退場機制(第三十七條)**

專營之電子支付機構因業務或財務顯著惡化，不能支付其債務或有損及使用者權益之虞時，為維護使用者權益，並避免專營之電子支付機構負責人或職員潛逃出境或脫產，主管機關得採取相關防範、限制措施。

專營之電子支付機構因解散、停業、歇業、撤銷或廢止許可、命令解散等事由，致不能繼續經營業務者，應洽其他電子支付機構承受其業務，並經主管機關核准。

七、相關授權法規命令(子法)

1. 為避免對既有單純提供代理收付款項業者造成過大影響，故規範對於僅經營代理收付實質交易款項業務，且所保管代理收付款項總餘額未逾新臺幣十億元者，非屬本條例所規範之電子支付機構。(第三條)
2. 境外機構非經許可設立電子支付機構，不得於我國境內經營電子支付機構業務；且非經主管機關核准，任何人不得有與境外機構合作或協助其於我國境內從事電子支

付機構業務之相關行為，故規範「與境外機構合作或協助境外機構於我國境內從事電子支付機構業務相關行為管理辦法」，以明訂主管機關核准之對象、條件、應檢具書件、與境外機構合作或協助其於我國境內從事電子支付機構業務相關行為之範圍與方式、作業管理及其他應遵行事項。(第十四條)

3. 為落實執行防制洗錢之要求，以及合理控管專營之電子支付機構作業風險，並符合其業務主要屬小額零售支付及資金移轉性質，故規範「電子支付機構使用者身分確認機制及交易限額管理辦法」，以明訂使用者身分確認機制之建立方式、程序、管理、確認使用者身分程序所得資料範圍、留存必要交易紀錄之範圍與方式及電子支付機構業務之交易限額等事項。(第十五條、第二十四條、第二十五條)
4. 為確保專營之電子支付機構、兼營電子支付機構業務之電子票證發行機構及所收取使用者之支付款項安全，並有效監督管理電子支付機構存管、移轉、動用及運用支付款項等情形，故規範「電子支付機構專用存款帳戶管理辦法」，以明訂專用存款帳戶開立之限制、管理與作業方式及其他應遵行事項。(第十六條)
5. 為確保使用者支付款項之安全，對於專營之電子支付機構及兼營電子支付機構業務之電子票證發行機構，其儲值款項扣除應提列準備金之餘額，併同代理收付款項之金額，應全部交付信託或取得銀行十足之履約保證，故規範「電子支付機構支付款項信託契約應記載事項」及「電子支付機構支付款項信託契約不得記載事項」。(第二十條)

主管機關規範「電子支付機構支付款項信託契約應記載事項」，明訂信託財產之種類、名稱、數量及價額，以及明訂信託財產管理及運用方法、信託財產結算及差額補足之作業、信託收益計算、分配之時期及方法、信託契約之變更方式、信託契約之解除或終止事由、信託關係消滅時信託財產之處理、信託相關報表之報送、各項費用之負擔及其支付方法、保密之約定、受益權轉讓限制、避免使用者誤認之約定等應記載事項。

主管機關規範「電子支付機構支付款項信託契約不得記載事項」，明訂不得約定由受託人保證信託本金之安全或最低收益率、不得有使使用者誤認受託人係為其受託管理信託財產之內容、受託人除為共同受益人外，不得約定享有信託利益、不得為其他違反法令強制或禁止規定之約定等不得記載事項。

6. 為保障使用者權益及執行使用者資金移轉之需要，專營之電子支付機構及兼營電子支付機構業務之電子票證發行機構對於儲值款項之支應維持一定之流動性，限制僅得於一定比率內從事相關低風險投資，並訂定電子支付機構運用儲值款項之比率，合計不得逾百分之六十。另為衡平使用者與電子支付機構間權益，並使電子支付機構對於運用支付款項所得孳息或其他收益之歸屬合理，電子支付機構應計提孳息或其他收益之比率，不得低於百分之五十，於專用存款帳戶銀行以專戶方式儲存，作為回饋使用者或其他主管機關規定用途使用。(第二十一條及「電子支付機構管理條例第二十一條第六項授權規定事項辦法」第三條及第四條)

7. 為維護使用者權益並利相關業者遵循，故規範「電子支付機構業務定型化契約範本」、「電子支付機構業務定型化契約應記載事項」及「電子支付機構業務定型化契約不得記載事項」。(第二十七條)
8. 為明確規範電子支付機構提供使用者之往來交易資料及其他相關資料予各機關 (構) 等事項，特制訂「電子支付機構提供使用者往來交易資料及其他相關資料要點」，以保障電子支付機構使用者之隱私權及尊重使用者對其資料之控制處分權。(第二十八條)
9. 為確保電子支付機構之交易資訊安全及業務健全運作，避免因資訊系統運作、傳輸或處理錯誤，影響服務之穩定與安全，甚或衍生相關糾紛，爰參酌「CNS 27001 資訊安全管理系統」國家標準、金管會指定「非公務機關個人資料檔案安全維護辦法」、銀行公會「金融機構資訊系統安全基準」、「金融機構辦理電子銀行業務安全控管作業基準」等，規範「電子支付機構資訊系統標準及安全控管作業基準」。(第二十九條)
10. 為確保專營之電子支付機構及兼營電子支付機構業務之電子票證發行機構之健全經營與管理，強化其內部控制及稽核制度，故規範「電子支付機構內部控制及稽核制度實施辦法」，明訂電子支付機構內部控制及稽核制度之目的、原則、政策、作業程序、內部稽核人員應具備之資格條件、委託會計師辦理內部控制查核之範圍及其他應遵行事項。(第三十條)
11. 為確保電子支付機構業務之順暢運作及發展，規範「電子支付機構業務管理規則」，明訂電子支付機構之業務管理與作業方式、使用者管理、使用者支付指示方式、營業據點、作業委外、投資限制、重大財務業務與營運事項之核准、申報及其他應遵行事項。(第三十三條)
12. 為確保使用者支付款項之安全，避免專營之電子支付機構及兼營電子支付機構業務之電子票證發行機構，對於儲值款項扣除應提列準備金之餘額，併同代理收付款項之金額，未全部交付信託或取得銀行十足之履約保證，損及消費者權益，故規範「電子支付機構應提撥資金，設置清償基金」，並制定「電子支付機構清償基金組織及管理辦法」，明訂電子支付機構清償基金之組織、管理、清償及提撥比率等事項。(第三十八條)
13. 為保持儲值款項之高度流動性，基於專營之電子支付機構及兼營電子支付機構業務之電子票證發行機構所收儲值款項性質類似，其儲值款項應繳存準備金之門檻宜有一致性，故修正「非銀行發行機構發行電子票證預收款項準備金繳存及查核辦法」為「非銀行支付機構儲值款項準備金繳存及查核辦法」，採相同之計提比率，惟為順應電子商務快速成長，以及配合政府鼓勵電子支付業務發展，應繳存準備金標準由原訂 30 億元提高為新臺幣 50 億元；超過 50 億元者，始須就超過部分計提準備金，俾協助業者於開辦初期順利推展業務，減低營運負擔。(第十九條)

八、「電子支付機構管理條例」對國內金融業之衝擊

全球電子商務快速發展的利基，就是打破實體商店營業時間及交易地點的限制，在網路上買賣商品或勞務，賣方節省店租、人力成本，買方則足不出戶，即可隨時享受購物樂趣。針對現行的電子商務基本模式，不論企業對企業 (Business to Business，B2B)、企業對個人 (Business to Customer，B2C) 或個人對個人 (Customer to Customer，C2C)，剖析其運作架構，不外乎金流、物流、資訊流三大部分，目前國內各網路商城之資訊流及物流的作業機制已經相當成熟，惟適用於網路交易之金流作業機制則呈現多元面貌，包括貨到付款 (現金)、支票、匯款、ATM 轉帳、信用卡等方式，其中現金、支票、匯款等支付方式逐漸無法滿足網路 24 小時的交易模式，傳統銀行所提供的支付服務，在電子商務的世界顯得力不從心。

即便國內超商密集，超商取貨方便熱門，但考量貨款延後收取及手續費過高，很多賣方不願參與，C2C 的個人賣方基礎薄弱，更是無法達到超商代收門檻；而信用卡雖然被普遍使用，但由於網路商店素質參差不齊，且營業規模往往不高，不易取得申請受理信用卡的特店資格，消費者對於在網路上輸入卡號、效期、卡片背面 3 位驗證碼，有資料外洩的疑慮，加上信用卡在網路支付要求 3D 認證、動態密碼等安全機制，由於操作較為複雜，致使交易失敗率高，而且跨國刷卡面臨偽卡、無法分期付款等問題，亦無法滿足電子商務之需要。

綜上，如何強化買賣雙方對網路交易的信任度，使用自動化 (e 化)、行動化 (M 化) 的工具協助商店或個人處理收付款項，成為促成電子商務成功的關鍵因素。就消費者而言，勢必擔心已支付款項，卻無法保證取得商品，或在鑑賞期限內退貨，無法取回貨款；就網路賣家而言，則擔心依約交付商品，無法取得貨款；未來透過「第三方支付交易機制」，電子支付機構先以電子支付帳戶代收買方應支付的款項，就可以通知賣方出貨，等到買方收到商品同意撥款後，再將貨款轉付給賣方的電子支付帳戶，如此將可大幅提高網路交易買賣雙方的信任度，進而增進網路交易的健全發展，爰此，本條例可解釋為賦予非金融機構以電子支付帳戶方式辦理儲值及資金移轉業務之法源，用以解決銀行法第 29 條對於網路電商提供線上金流服務的限制，加上電子票證發行機構可兼營電子支付機構，尤其對於市占已有 4,000 萬張的悠遊卡、1,200 萬張的愛金卡 (icash)，突破單一功能的限制，提升為多用途支付及多元支付範圍，均顯示信心滿滿、躍躍欲試，將對國內金融機構帶來顛覆式的衝擊，強力侵蝕國內金融機構原有代收代付金流服務市場。

九、國內金融服務的趨勢與建議

金管會於 104 年 1 月 22 日新聞稿中表示，「本條例之施行，將健全電子商務金流支付服務，提升民眾對網路交易之信賴度，降低小額交易支付成本，有利青年網路創新環境，協助青年創業及企業開發商機。目前我國個人及網路商店約 10 萬家，市場預估 104 年度個人及網路商店應可成長 1 至 2 成，約 1 至 2 萬家，103 年電子商務市場交易規模達新臺幣 8,800 億元，本條例施行後，預估將增加新臺幣 1,200 億元至 2,000 億元，整體電子商務產業將躍升為兆元產業。」

由於不同產業有不同專長優勢，未來最佳的電子商務支付工具須結合電子支付業者、金

融機構、電信業者等多元產業，以產生「異業結合、互利共生」的跨業綜效，尤其不少民眾對於網路電商從事儲值等相關業務仍有吸金、洗錢之疑慮，而銀行產業為民眾高度信賴之機構，且支付服務屬金融機構固有之金融服務項目，並受高度金融監理，金融機構具有完善的金融帳戶管理系統及相關對帳、銷帳機制，可協助電子支付業者建構電子支付帳戶，並維運會員儲值帳戶、會員儲值卡，目前各金融機構已發行數千萬張晶片金融卡，市場運作成熟，正可透過網路 ATM 申請開立電子支付帳戶，並提供網路購物、轉帳儲值等跨行功能。電子支付業者與金融機構合作，可節省開發、建置儲值帳戶系統成本，以及需要取得金融機構信託或履約保證的手續費用，達到雙贏的實質效益。

由於平板顛覆了 PC，智慧型手機顛覆了傳統手機，民眾使用的終端已被顛覆，所以這些行動設備將消除民眾在時空使用上的限制，只要能上網，不論身在何處，甚至移動時都可使用，較坐下來使用 PC 的時間及空間更無限制，因此透過行動載具所發展之新興電子支付模式將不斷推陳出新，電子支付業者可透過金融機構與電信業者的合作，藉由手機的電子錢包作為支付工具，或以手機連結電子支付帳戶的消費方式，提升手機上網購物的方便性，有效簡化消費者的支付流程。未來行動支付將不限於網路的虛擬應用交易，尚可結合線上營銷購買以帶動線下消費體驗，或提供線下互動促銷以引領線上便捷交易，藉由「虛擬網路」與「實體通路」兩者交易相互結合，達到虛實整合應用 (O2O, Online To Offline 或 Offline To Online)，以提高消費者交易黏著度，更可將電子商務發展提升至行動商務，因此，行動支付前景遼闊，各方爭奪已點燃戰火，臺灣電子商務金流產業將進入百家爭鳴、爭芳鬥艷的戰國時代。

註 1：互聯網金融係指非傳統金融機構的網路電商以 Internet 及行動通訊等技術，利用巨量資料分析、雲端儲存運算、社群網路關係、app 內容運營等工具，高效能整合資訊流、物流與資金流，以網路電商平台優勢，突破傳統金融機構的思維架構，挑戰現行金融業務的服務模式，實現資金支付、資金融通與資訊中介的新興金融模式，尤其對於營業規模不高、無法提供抵押擔保、找不到信用保證人、缺乏信用紀錄的小型微利企業或個人而言，可有效紓解其金流不足之窘境，但也突顯傳統金融機構缺乏經由傳統通路提供低端用戶有效即時的金融服務。

註 2：PayPal 係 1998 年底成立，2002 年 10 月當時全球最大拍賣網站 eBay 以 15 億美元併購 PayPal，PayPal 便成為 eBay 的主要付款途徑之一，PayPal 突破傳統金融機構匯款手續太複雜、繁瑣的困境，是目前全球幣別轉換種類最多的新興線上跨國金流供應商。

註 3：支付寶係中國大陸阿里巴巴集團於 2004 年 12 月創辦，結合淘寶網、天貓商城擔保交易的第三方支付平台，支付寶提供有效的網路交易履約擔保機制 (Internet Escrow Agent)，確保交易完成，是目前全球註冊用戶數最多的新興線上跨國金流供應商。

※ 參考文獻 / 資料來源：

1. 電子支付機構管理條例－總說明及逐條說明，金管會。
2. 電子支付機構管理條例第三條第二項授權規定事項辦法－總說明及逐條說明，金管會。
3. 與境外機構合作或協助境外機構於我國境內從事電子支付機構業務相關行為管理辦法－總說明及逐條說明，金管會。
4. 電子支付機構使用者身分確認機制及交易限

額管理辦法—總說明及逐條說明，金管會。
5. 電子支付機構專用存款帳戶管理辦法－總說明及逐條說明，金管會。
6. 電子支付機構支付款項信託契約不得記載事項－總說明及逐點說明，金管會。
7. 電子支付機構支付款項信託契約應記載事項－總說明及逐點說明，金管會。
8. 電子支付機構管理條例第二十一條第六項授權規定事項辦法－總說明及逐條說明，金管會。
9. 電子支付機構業務定型化契約不得記載事項－總說明及逐點說明，金管會。
10. 電子支付機構業務定型化契約範本－總說明及逐條說明，金管會。
11. 電子支付機構業務定型化契約應記載事項－總說明及逐點說明，金管會。
12. 電子支付機構提供使用者往來交易資料及其他相關資料要點－總說明及逐點說明，金管會。
13. 電子支付機構資訊系統標準及安全控管作業基準辦法—總說明及逐條說明，金管會。
14. 電子支付機構內部控制及稽核制度實施辦法－總說明及逐條說明，金管會。
15. 電子支付機構業務管理規則－總說明及逐條說明，金管會。
16. 電子支付機構清償基金組織及管理辦法－總說明及逐條說明，金管會。
17. 2015 年 4 月 10 日新聞發布修正「非銀行發行機構發行電子票證預收款項準備金繳存及查核辦法」，中央銀行。
18. 2015 年 1 月 22 日「電子支付機構管理條例之制定與施行事宜」新聞稿，金管會。
19. 2015 年 4 月 23 日「為增進電子票證發展，行政院通過電子票證發行管理條例修正草案」新聞稿，金管會。

Focus 專注·專業 @ **Innovation** 創新·引導 @ **Security** 安全·穩健 @ **Convenience** 便捷·服務

財金資訊股份有限公司
Financial Information Service Co., Ltd.
http://www.fisc.com.tw