探討二維條碼資訊安全應用架構－以信用卡安全服務為例

楊子漢	呂新科	林芃君
中國文化大學推廣部資訊管理所研究生	中國文化大學推廣部資訊管理所教授	中國文化大學推廣部資訊管理所講師

摘要

一維條碼因應結帳速度效率的需求、大量產品整理計算運用，及掃描技術的出現，其快速及便利性迅速運用在各生活面上。然而隨著時代演進，產品訊息繁雜，簡易一維條碼已無法符合需求，二維條碼的出現開始逐漸在更大量訊息資訊讀取上的應用。伴隨資訊進步、智慧手機和數位影像的開始普及，加上二維條碼可容許訊息及字串量的龐大，許多衍生運用開始出現，不論食衣住行育樂，皆可以見到其應用方面。

不同於一維條碼僅能有英數字簡易稀少的符號，二維條碼可容納達 7000 多字元，並可接受各類符號資訊存取，3G 網路普遍，商店或廣告運用二維條碼方式，將宣傳網址存入二維條碼做快速連結上網運用。二維條碼存取符號字元多樣，因此可於條碼中做加解密運用，拓展條碼應用的範疇，可結合保密安全性的加值運用。高鐵除了用磁卡外，現在亦推行二維條碼票券，以加密方式確保各票券資訊不易外流被破解，運用手機搭配網路訂票方式，添增購票便利性及節省多餘磁卡紙類的消耗。

現今社會信用卡盛行，多張信用卡不同優惠模式已經是大部分民眾的生活必需，多張信用卡攜帶逐漸產生一種麻煩，且各張信用卡超過使用期限後，定期換卡所造成的成本及社會資源浪費不斷增長。隨著二維條碼加密安全模式成熟，兼且影像效果完善，本研究提出一個信用卡結合二維條碼之營運模式，運用二維條碼電子信用卡之特性與安全加強機制，以增加使用與匯整便利性、減少信用卡製作成本及縮短信用卡補卡生命週期，同時亦考量其安全性；在線上信用卡交易模式上，直接以二維條碼檔案取代直接線上輸入信用卡卡號訊息，增加線上交易安全性。研究中預定提出建構電子信用卡架構，以推廣漸進方式，逐步取代原先信用卡模式。

關鍵字：二維條碼、安全性、信用卡、線上交易

第一章　緒論

1.1 研究背景與動機

信用卡制度行之有年，隨著信用卡消費模式興盛，消費者人手多卡狀況逐漸普遍，每年換卡發卡數量漸漸接近百萬張，社會成本及資源的浪費逐漸浮現。人手多卡情形多為不同銀行發卡優惠不同造成，消費者往往在不同地方消費需要不同卡片，卡片管理及攜帶卡片不便性也常是消費者困擾因素之一。

二維條碼可以存放龐大資訊位元，並且產生容易，且可運用加密技術將資訊加密處理，目前已逐漸廣泛運用在不同行業，如高鐵的二維條碼感應過站模式，日本公車站增加 QRCode 提供公車路線及等候時間等資訊的運用。本研究採用目前便利並逐漸廣為應用的二維條碼，嘗試以二維條碼搭配加密機制逐步替代實體信用卡，節省信用卡生產資源，縮短信用卡生命週期增加安全性，並於線上信用卡購物時避免卡號等重要資訊外流情況產生。增加線上刷卡安全性。

第二章　文獻探討

2.1 信用卡

信用卡交易制度乃發軌於買賣雙方記帳消費的消費行為，而隨著業務漸次發展，逐步自地區性記帳消費工具訊速擴張成為全面性支付制度。台灣地區每年信用卡的累積發卡量與簽帳金額均呈現快速的成長，信用卡業務已成為銀行其中一個重要的業務來源。直到民國 94 年，卡債風波爆發，信用卡流通數量才逐漸下滑，但近年又開始逐年慢慢回升，如表 1。至民國 102 年 8 月主計處統計，台灣流通信用卡總數量達 3483 萬多張，單月發卡數也達到 72 萬多張，如表 2。[陳丘（2005）][陳金岳（1999）]

表 1 主計處信用卡各年流通數統計

單位：千張；百萬元

民國年月底	流通卡數	民國年月底	流通卡數	民國年月底	流通卡數
80年	927	90年	24 135	100年	32 855
81年	1 503	91年	31 591	101年	34 076
82年	2 051	92年	37 850	102年 1月	34 122
83年	2 709	93年	44 182	2月	34 177
84年	3 676	94年	45 494	3月	34 329
85年	5 467	95年	38 324	4月	34 489
86年	7 665	96年	36 437	5月	34 624
87年	10 640	97年	33 950	6月	34 689
88年	13 575	98年	30 567	7月	34 802
89年	18 276	99年	30 706	8月	35 024

表 2 主計處民國 102 年 8 月信用卡統計

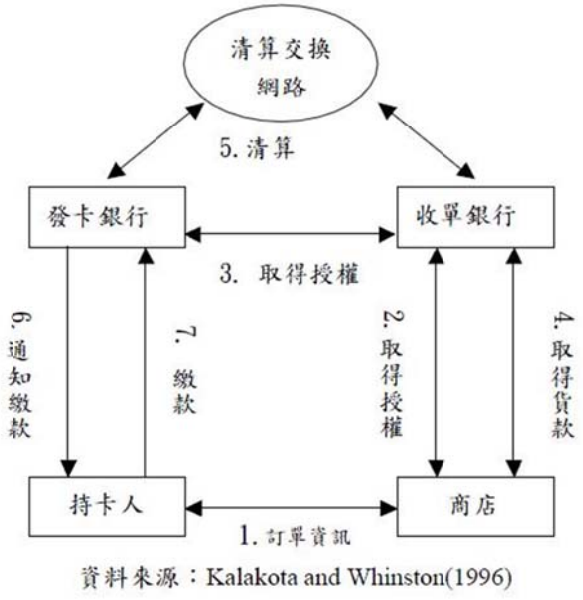
機構別 Issuer	流通卡數（張）Card in Force	有效卡數（張）Active Cards	本月發卡數（張）Monthly Issuing Cards	本月停卡數（張）Monthly Cancelled Cards
總計 Total	35,023,570	22,115,849	724,521	365,829
本國銀行小計 Domestic Banks	34,834,179	22,014,626	721,211	363,763

物流與工程管理中期刊中淺談信用卡製造企業物流風險成本核算中曾估算信用卡成本值約 2.5 美元，年產值 3000 萬張。光一家公司產製信用卡年成本消費金額達到約達 7500

萬美元，全球每年在製造信用卡成本上的消耗可以越見龐大。[胡萬里 （2010）]

2.1.1 信用卡交易流程分析架構

信用卡，是具有延展消費者信用的支付工具，其運作方式採用消費者在特約商店刷卡交易時，能延展其消費金額並於每月指定日結清或支付部分款項後採用循環信用計息方式遞延支付未償金額。信用卡付款方式如圖 1。[林鈴玉（2001）][張哲綸（2009）][曹壹登（2000）]



資料來源：Kalakota and Whinston(1996)

圖 1 信用卡交易流程

2.1.2 SSL 交易安全機制(Secure Scket Layer)

為 Netscape 公司在 1994 年 10 月提出的網路通訊協定，此協定內建於網頁伺服器中，提供資料加密、伺服器認證、資料完整性檢查功能，其主要目的為保護傳輸資料之安全。SSL 為介於原始 TCP/IP 協定和應用程式層中間的一個層級。TCP/IP 協定只負責傳送無誤的資料串流，SSL 則為這條串流加入多項特徵：

<1>用數位簽章達到伺服器端的身分認證和不可否認性

<2>用數位簽章達到客戶端的身分認證和不可否認性

<3>運用加密技術滿足資料保密性

<4>用訊息認證碼滿足資料完整性

使用 SSL 購物流程如下圖。運作方式如下：

(1) 消費者在網路上購買商品，輸入個人資料，授權之資料(消費者姓名、信用卡卡別、信用卡卡號、信用卡有效日期、驗證碼及交易金額)。並使用 SSL 網路安全機制將資料傳送到網路商店之伺服器

(2) 網路商店收到消費者交易資料後，會將消費者資料存到資料庫中，再將授權資料(消費者姓名、信用卡卡別、信用卡卡號、信用卡有效日期、驗證碼及交易金額)以 SSL 網路安全機制方式傳給付款閘門，付款閘門收到授權資料，轉換成 ISO8583 格式(目前一般信用卡格式)，再送到收單銀行的主機。

(3) 收單銀行將授權資料經由信用支付中心傳到發卡銀行進行授權要求。

(4) 發卡銀行經由支付中心傳送授權回應到收單銀行的主機

(5) 收單銀行主機將授權回應給網路商店

(6) 網路商店收到授權回應後，如果取得授權，便代表交易成功，會通知消費者並將貨物送出。

(7) 發卡銀行於結帳日寄送信用卡帳單給消費者。

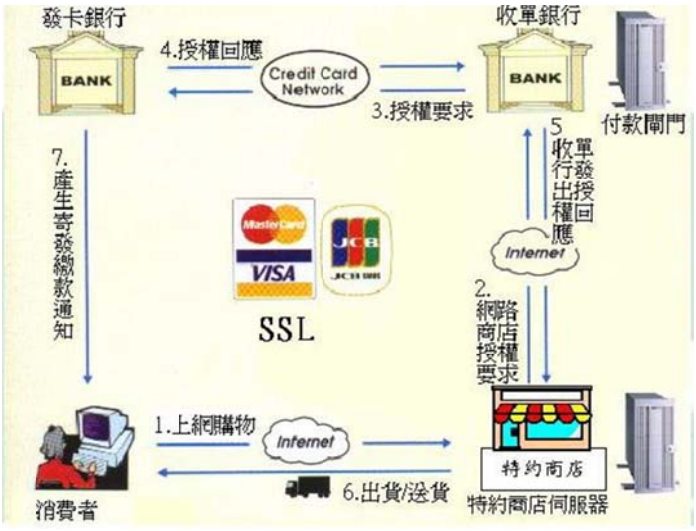


圖 2 SSL 交易機制流程圖

2.1.3 SET 安全電子交易協定(Secure Electronic Transaction)

為一種應用於網際網路上以信用卡為基礎的電子付款系統規範，用來確保線上信用卡交易的安全性。安全核心技術主要為三部分：

(1) 資料保密的加解密技術(Crytography)

(2) 維護資訊完整的數位簽章(Digital Signature)

(3) 交易資訊無可否認的電子認證機制(Certificate)

規格運用了公開鑰(RSA)、對稱式金鑰(DES)、電子信封、雜湊函數和電子數位簽章等安全技術，用以維護開放網路上交易的安全機制。主要特色為：

(1) 交易時交易身分的辨識

(2) 交易資料傳送過程的安全性

(3) 交易資料的完整性

(4) 交易的不可否認性

SET 的基本架構圖如下圖。交易流程如下：[邱筱雅，1997]

(1) 信用卡交易的前提在於，顧客必須向發卡銀行申請成為合法持卡人，擁有唯一的信用卡號碼，並且向發卡組織委託的認證中心申請身分識別。

(2) 持卡人發出[交易起始訊息]給商店，要求與商店進行線上信用卡交易。

(3) 特約商店回應持卡人起始訊息，將商品訂購資訊傳回給持卡人，包含經特約商店簽章過的證書，內含特約商店與收款銀行的公開金鑰，讓持卡人來加密正式交易訊息。

(4) 持卡人發出商品訂購的正式申請，其中[訂單資訊]為商家的公開金鑰加密，[付款指示][持卡人信用卡號碼]則以收款銀行的公開金鑰加密。

(5) 特約商店收到申請資訊，傳送[訂購回應訊息]給持卡人，並持續進行身分驗證工作。

(6) 持卡人向特約商店查詢訂購狀況，確認商品訂購是否接受。

(7) 商店按持卡人帳號的驗證狀況，答覆持卡人交易進行的時程。

(8) 特約商店將經過收款銀行公開金鑰加密過的付款指示及持卡人信用卡號碼，附上其簽章後的特約商店證書，成為[授權申請訊息]，再以收款銀行的金鑰加密所有的[授權申請訊息]，傳送給收款銀行進行持卡人驗證。

(9) 收款銀行核對身分無誤後，將持卡人資料傳送給發卡銀行，進行包含[持卡人身分]、[使用卡使用期限]、[信用額度]的確認。當合乎交易條件，則將結果通知收款銀行，並由收款銀行傳回[授權回應訊息]給特約商店。

(10) 特約商店收到收款銀行的授權回應後，交易商品給持卡人。

(11) 特約商店可於連線時或累積一定付款授權後，產生[取款申請訊息]，請求收款銀行進行付款。

(12) 發卡銀行與收款銀行進行帳務清算後，完成 SET 信用卡交易流程。

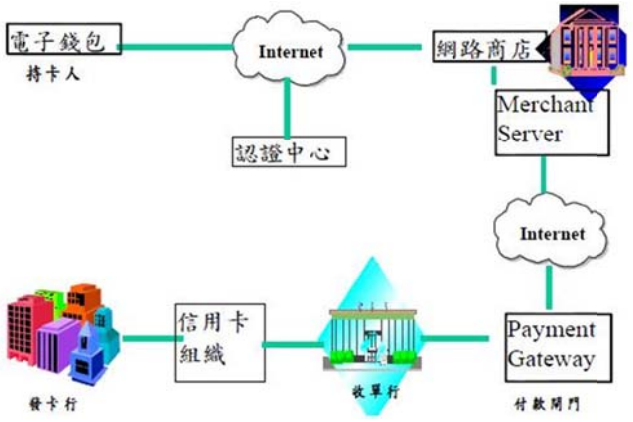


圖 3 SET 交易機制流程圖

SSL 交易機制與 SET 機制比較如下表。

表 3 SSL 與 SET 機制比較表

比較項目	SSL	SET
發表時間	1994年	1996年
制定組織	原爲Netscape公司所制定，目前被IETF組織列爲工業標準並更名爲TLS	由兩大信用卡公司Visa與MasterCard所制定
OSI架構	介於傳輸層與應用層之間	屬於應用層協定
公開金鑰架構	簡單公開金鑰架構	較爲嚴謹的公開金鑰架構
身份驗證方式	基本的密碼驗證(password)	數位憑證(Digital certificate)
啓動方式	內嵌於WEB瀏覽器	需事先安裝特殊軟體，如電子錢包
安全服務層級	低	高
資料防護	有	有
不可否認性	不具備	具備
專屬應用	無特定的專用方式，以資料的防護與機密性爲主	有特定的應用方式，主要用以信用卡的付款，而且有特定的付款閘道
交易認證方式	爲了方便起見，通常僅做單向認證，由消費者認證商家	消費者與商家之間可互相認證
主要演算法	RSA&DES演算法	RSA&DES演算法

[陳仕國（2008）][葉文熙（1997）][鄭美枝（2000）][盧銘仁（2000）]

2.2 二維條碼

條碼因應快讀取，產生容易等優點廣泛運用在物品記帳、紀錄等使用，隨著社會日益進步，物品多元化，一維條碼已無法提供充足需求。二維條碼因而產生，除了兼具一維條碼特點外，兼之具有大量位元資訊存取及不易受破損影響等特點，開始被廣泛運用在其他方面。表 3 為一、二維條碼比較表。[吳伊仕(2011)][陳相如(2012)][蔡志偉(2012)]

表 4 一維條碼與二維條碼比較

比較特性	一維條碼	一般二維條碼
儲存量	僅數十個文數字(無法顯示中文)	3079英文/平方英吋
抗損性	損壞時較難判讀資料	30%-50%容錯率
安全性	條碼資訊過少，無法做加密處理	條碼資料可作隱匿及加密動作
複製判讀性	經傳真或影印後，可判讀機率降低	經傳真或影印仍可使用
追蹤性	僅為代碼，需連結資料庫才可比對出產品資訊	包涵產品資訊，可與產品一起攜帶

二維條碼資訊量的增加，兼且網路資訊的發達，大幅增加其應用效能。除了原先傳統一維條碼運用外，其他產業也開始廣泛運用條碼搭配運用，食、衣、住、行、育、樂各方面都有產業上的運用，下表簡單列舉各類型上的運用。

表 5 二維條碼各類型運用列表

類型	條碼應用
食	1. 台灣農委會推廣生產履歷的機制，民眾可藉由生鮮產品上面所附有的QR Code標誌，用自己的照相手機一照，再藉由手機內建的QR Code解碼功能，便能看到生鮮產品的生產流程及商品資訊。
衣	1. asics在其產品-羽排球鞋的產品標籤上，印有產品介紹網頁連結的QRCode。
住	1. 房仲業者-台灣房屋使用QuickMark軟體技術，推出了具有QR Code的「物件資訊帶著走」服務供民眾使用。
行	1. 台灣高鐵公司的實體車票上，印有QR Code（指到便利商店領取之車票），當乘客到達高鐵車站閘門處感應後即可開閘門通行（2010/02）。 2. 中國鐵道部於2009/12/10開始改版鐵路車票，新版車票採用QR Code作為防偽措施，取代以前的一維條碼。 3. 在日本，許多公共汽車站牌都已增加QR Code，乘（旅）客只需使用手機解讀解條碼內資訊，就可以即時獲得該站牌的路線與班車時刻等許多資訊。
育	1. 壹傳媒是透過QRCode的連結方式，將實體的文字報轉向影音形式的新聞內容展現。 2. 公司/機關在其官網上（如：工研院學習服務網、台灣大學圖資系），放置紀錄著該網址資訊的QR Code，讓使用者可省時又省力的連結至該網站。 3. 個人名片或宣傳海報/DM。 4. 各種繳費通知、帳單或交易收據、憑證。 5. QR Code導覽。
樂	1. 中華電信的行動電話產品銷售DM上印有QR Code，用手機解碼後即可下載歌星音樂鈴聲。 2. 《超能量資訊》與金揚資訊QuickMark合作，將QR Code與旅遊業整合應用於宣傳海報上，用手機讀取QR Code後可看到台灣各地的觀光資訊，這讓QR Code展現另類的行動觀光應用。 4. 夢時代購物中心為台灣百貨界最先將QR Code做為行銷介面的購物中心。2010年8月25日推出專屬QR Code商品及相關應用，方便顧客能經由館內外、網站及DM上的QR Code，得到特別優惠。
其他	1. QR Code還可以變成招牌、交通情報、生日蛋糕和衣服的一部分（千言萬語都在蛋糕、衣服上的條碼中）。

2.2.1 條碼影像隱藏技術

浮水印是指將特定資訊嵌入特定訊號中，該訊號可能為音訊、圖片或是影片，主要可分為浮現式和隱藏式兩種，前者為可被看見的浮水印，所包含的訊息可同時被看見，而後者在一般的情況下是無法被看見的。有效浮水印需具備以下特質：

(1) 隱蔽性和透明性：不能降低或破壞原始影像的品質。

(2) 不易移除性：不容易或不可能被駭客移除。

(3) 強健性：透過雜訊、壓縮處理及影像處理等動作，所萃取的浮水印仍可以清楚的呈現以便於辨識或判斷。

(4) 明確性：經過攻擊後，失真不會過於嚴重，可以明確辨識或判斷。

[賴勇志（2003）][王梓勳（2012）][莊明奇（2009）]

2.3 密碼學

(1)基本的加解密流程：將需要加密的密文，透過加密金鑰，加密成密文，再藉由解密金鑰將密文解開，得到最初的明文。

(2)對稱式密碼金鑰：加解密都使用同一把金鑰，在加密的安全性與非對稱式密碼相比安全性較低。

圖 4 對稱式金鑰示意圖

(3)非對稱式密碼金鑰系統：每人可產生一對金鑰，為公開金鑰及私密金鑰，私密金鑰為個人妥善保管，公開金鑰為他人可任意獲得。非對稱式金鑰系統所用來加解密金鑰是不同的，不能直接由一把金鑰計算出另外一把金鑰。

圖 5 非對稱式金鑰示意圖

(4)雜湊函數：對任意可變長度之明文，經由雜湊函數計算後，會產生固定長度的雜湊值。在雙方通訊確認時，雜湊函數是最常被使用的重要工具之一。

(5)數位簽章：在對稱式金鑰密碼系統中，有兩把不同鑰匙分別為公鑰和私鑰，其中用私鑰加密的文件，別人要用其公鑰才能解密的文件，由此可以驗證此為目標所發之文件，也稱之為數位簽章。數位簽章具有資料完整性、資料來源辨識、資料之隱密性、不可否認性等特點。

[周韋伶（2006）][陳宗保（2001）][曾建豪（2007）]

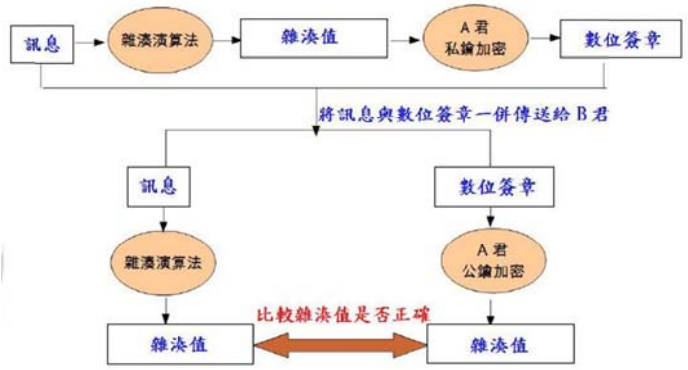


圖 6 數位簽章驗證示意圖

第三章　二維條碼信用卡架構

3.1 條碼信用卡架構及產製

實體信用卡每張卡片製作都需要成本，台灣目前一年信用卡流通卡數達到 3500 萬張，僅僅八月換卡數便達到 75 萬張驚人數字，在信用卡上成本消耗逐漸增加，部分信用卡有效年限也從原先 2、3 年調升到 5 年之久，對於信用卡的安全性威脅大幅提升。信用卡線上交易目前交易方式仍採用

輸入卡號、卡別、有效年限和驗證碼方式經由 SSL 和 SET 模式做消費，雖有線上加密機制，但卡號等資訊為自身輸入進去，難免會有外洩情況產生。

本研究運用二維條碼產生容易特點，構思於行動裝置上設計專屬信用卡程式方式，取代現有實體信用卡，每張信用卡資料存於信用卡程式中。如此方便信用卡整理，卡片亦不會造成攜帶負擔。

每張卡片預估會有卡別、卡號、卡片其他資訊(可加密)、銀行信用卡公鑰、個人私鑰，於刷卡付款時採用程式快速產生二維條碼供讀取，如此不僅節省了信用卡換卡消費成本，信用卡換卡時間亦可縮短為數月或是認為不安全及可做換卡動作，降低卡片被破解方式。於線上交易部分，採用匯入二維條碼做交易，避免信用卡訊息洩漏情況產生。

製作信用卡條碼程序為：

(1) 添加時間撮記將其和卡片其他資訊一同做個人私密金鑰加密。

(2) 將卡號和加密資訊作指定銀行公鑰加密後，輔以銀行代碼及卡別快速產製出二維條碼。示意圖如圖 7。

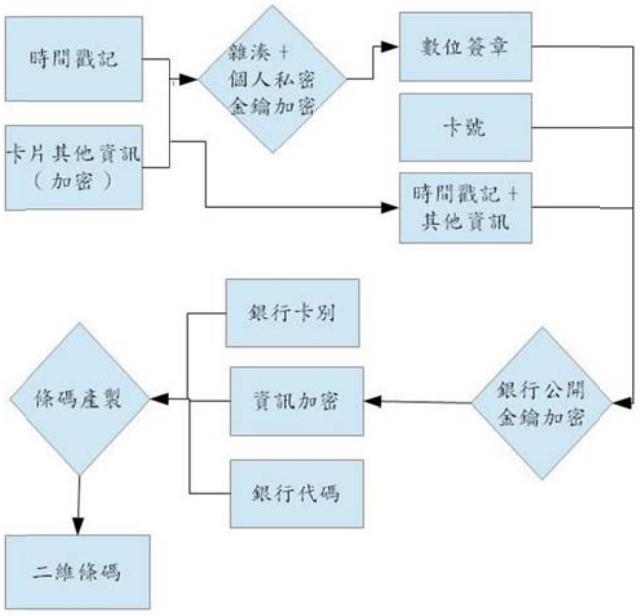


圖 7 信用卡刷卡時產製條碼過程

條碼產製時添增了時間戳記及戳記容許時間，且可避免條碼被複製後去做其他運用，避免條碼容易複製的為他人盜用的情況產生。如條碼匯出需做線上付款運用的話，戳記容許時間可給與較長，彈性方便使用。

3.2 條碼信用卡交易模式

信用卡交易模式類似圖 1，經由條碼讀取到資訊後，特約商店將送給收款銀行，再由收款銀行將授權資料送給發卡銀行，由發卡銀行做解密和辨識工作，做解析動作。流程圖如圖 8，說明如下：

(1) 將加密資訊以銀行私密金鑰解密，取得數位簽章、信用卡其他資訊及時間戳記和卡號。

(2) 由卡號取得信用卡個人公開金鑰，將數位簽章以公開金鑰解密，比對其雜湊值是否與信用卡其他資料及時間戳記雜湊值相符合，不符合表資料不正確。

(3) 確認相符合，比對時間戳記，在時間戳記容許值內，則通過時間驗證。分析比對信用卡其他資訊，如信用額度與消費金額是否容許。

(4) 條件比對符合，回傳准許授權，不符合，回傳拒絕授權。

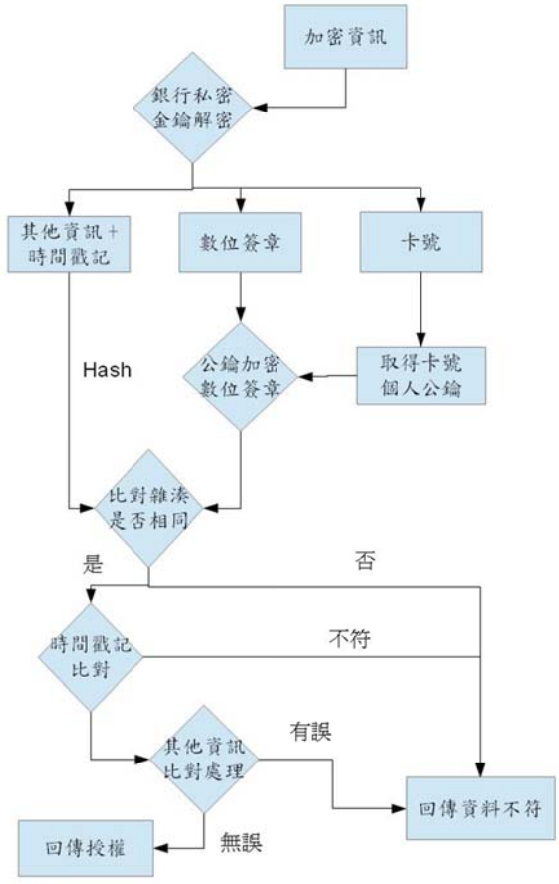


圖 8 條碼信用卡資料授權判斷分析

3.3 信用卡資料申請取得模式

信用卡資料皆由銀行發出，使用者初次申請條碼信用卡需去銀行做一次金鑰交換動作，後續要更換個人金鑰時，有，也皆需銀行做更換動作。更換動作如下圖。

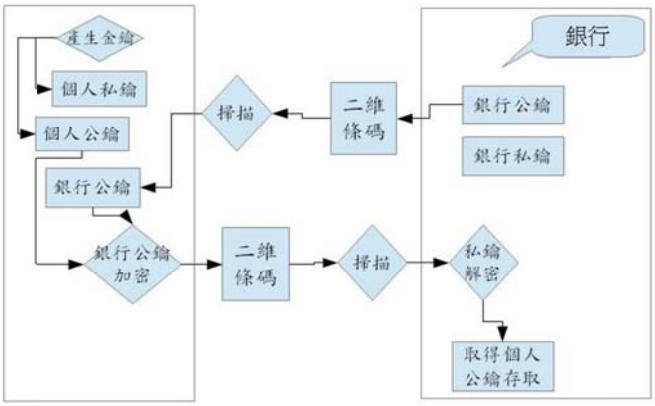


圖 9 初次申請信用卡金鑰交換流程

流程為：

(1) 由銀行將公鑰產製二維條碼供使用者讀取。

(2) 使用者產製個人該銀行個人公鑰和個人私鑰，私鑰保存。

(3) 讀取銀行公鑰保存，將個人私鑰以銀行公鑰加密，並產製二維條碼。

(4) 銀行讀取使用者產製二維條碼，取得個人公鑰，並將個人公鑰依照個人資料存放。

完成信用卡第一次申請後，銀行之後換卡模式可採用傳統模式將信用卡資訊以銀行私鑰加密做數位簽章，輔以個人公鑰加密產製的二維條碼，以現有信件寄送信用卡方式或電子寄送方式提供使用者更換信用卡，藉以完成信用卡換卡作業。

第四章　結論與後續探討方向

4.1　結論

科技進步往往會帶來技術轉變及演進，二維條碼產生加上行動裝置的興起，線上交易逐漸普及，信用卡線上交易安全性仍有些微不足。採用二維條碼電子信用卡模式，在不影響信用卡本身安全性下，增加信用卡線上交易安全性，並減少信用卡消耗成本及可簡短換卡時間，減少信用卡被破解情況產生。在此初步提出二維條碼信用卡架構，分析交易安全性流程與可行性，以其採用更為簡約社會成本消耗下，兼之不影響安全性狀態下，提供縮短週期性換卡時間，減少信用卡暴力破解機會，並增進線上交易流程安全。

4.2　後續方向探討

信用卡特點在於信任，在轉換為二維條碼電子信用卡過程中如何做到完善整個信用卡安全、且不影響信用卡使用便捷是個很大的問題。目前網路傳輸技術發達，假設傳輸二維條碼圖案是否會影響傳輸時間，及條碼讀取分析的問題，仍需詳細討論分析可行性。

實體信用卡具有簽名身分驗證效果，增加民眾對於持卡交易信任感，採用二維條碼電子信用卡是否減低了這層信任感？或許可以利用二維條碼隱匿功能，搭配個人圖象鎖定製作個人實體交易信用卡，但其不可複製性問題仍須探討研究。

參考文獻

1. 陳丘（2005）。**行動環境下匿名付款機制**。世新大學資訊管理所。
2. 陳金岳（1999）。**交易付款模式之資訊流分析**。國立東華大學。
3. 胡萬里 （2010）。 淺談信用卡製造企業物流風險成本的核算。**物流工程與管理， 32**（192），頁 3。
4. 林鈴玉（2001）。**國內網路銀行現況發展及交易安全之研究**。國立交通大學資訊管理所。
5. 張哲綸（2009）。**以隱匿信用卡卡號為基礎之改良式電子付款機制**。亞洲大學資訊工程所。
6. 曹壹登（2000）。**多樣化網際網路付款機制之設計與實作**。國立台灣大學電機工程研究所。
7. 陳仕國（2008）。**台灣小額付款之現況與未來發展－已有無銀行憑證電子錢包為例**。開南大學資訊及電子商務所。
8. 葉文熙（1997）。**預付卡式付費系統－流程、實作與安全分析**。國立交通大學資訊科學研究所。
9. 鄭美枝（2000）。**台灣電子付款機制之發展與消費者偏好結構調查**。國立臺灣大學商學研究所。
10. 盧銘仁（2000）。**信用卡安全交易伺服系統在電子商務之廣用性設計與實作**。中原大學電子工程所。
11. 周韋伶(2006)。**行動商務安全**。明新科技資訊管理所。
12. 陳宗保(2001)。**行動電子商務環境下安全協定之研究**。大葉大學資訊管理所。
13. 曾建豪（2007）。**WAP 行動銀行系統**。世新大學管理學系。
14. 吳伊仕（2011）。**QR Code 建置運動地圖行動導覽系統之應用**。佛光大學資訊應用所。
15. 陳相如（2012）。**結合 QR code 與彈性化網頁框架通訊平台之建置**。佛光大學資訊應用所。
16. 蔡志偉（2012）。**以架構導向法探討台灣無障礙協會行動網站導入 QR Code 之研究**。高苑科技資訊科技應用研究所。
17. 賴勇志（2003）。**結合二維條碼與定位方法之影像浮水印技術**。大葉大學資訊工程所。
18. 王梓勳（2012）。**大尺寸二維條碼的隱藏與應用**。國立雲林科技資訊工程所。
19. 莊明奇（2009）。**二維條碼之解碼及糾錯分析**。國立台

灣海洋大學電機工程所。

20. 王梓勳（2012）。**大尺寸二維條碼的隱藏與應用**。國立雲林科技資訊工程所。

21. 黃翔偉, 黃., 王旭正 （201210）。 QR code 雙重型態的高隱匿性資訊隱藏技術。**資訊管理學報， 19**（4），頁 15。