第一章 緒論

第一節 研究背景

在這資訊及科技爆炸的時代電腦的使用率越來越普及，漸漸的將商業模式搬出檯面來，聰明的業者運用了網路作為交易的媒介與顧客進行網上交易，發展出所謂的電子商務。因此，在發展電子商務的過程中思索如何運用現有之經營模式，企業之長處與優勢去創造新的電子商務模式，而成為電子商務時代之佼佼者。然而電子付款系統在其中扮演著核心的角色，因為它掌握整個交易之帳務出入的重務，所以它的系統架構需要非常嚴密才能使消費者安心的上網購物，這也是電子付款中最難進行的一步;要做到不會將顧客資料外洩、交易過程中不會有錯誤，如此才能解除消費者心中的擔憂，進而有上網訂購物品的可能，因為時代的變遷逐漸地將傳統市場交易轉成線上交易，這也表示著咱們社會的進步及現代人們知識增長、水準的提高。

電子商務係近年來最新興最熱門之議題，藉由網際網路與無線

通訊之發展，改變了傳統的交易模式，更創造出眾多的新興科技與工業，提供比傳統商業模式下多出數十倍的商業貿易與工作機會，更促進國際間貿易的快速發展，真正達成地球村之理想。電子商務使傳統主要的商業或組織活動，不論是所謂的 B2B（業者對業者之交易）或是 B2C（業者對消費者之交易）、抑或 B2G（業者對政府之交易）的交易模式與運作皆產生劇烈變革。在這一波電子商務模式下，係以所謂資訊流、物流、金流等三方面主軸，凡能主宰此三大領域者，即主導了未來商業的發展趨勢。而在此其中，關於電子商務各種資金之流動、移轉，例如付款、轉帳及其他交易等，除仰賴傳統人工及自動化機具設備（如 ATM）等方式外，亦應運而生各種新的付款方式，例如透過網路信用卡、網路銀行、各種儲值卡、電子支票及銷售點系統（POS）.....等等，且隨著技術的不斷創新，新的支付方式亦不斷地產生與實施運用。

第二節　研究動機

在形形色色的電子商務系統中，電子付款系統往往是整個系統中最重要也最複雜的一個環節。有許多網路商店礙於規模及經濟上

的限制，無法提供給消費者安全的電子付款交易環境，變成其業務發展上的一個瓶頸，或者其維護成本較高，成為網路商店極大的負擔。

我們之所以研究電子付款系統之安全性及理論探討這個題目，是因為在 Internet 的風潮盛行之後，網路購物的效益及優越性已逐漸獲得大家的肯定，而網路購物模式的建立，不僅是企業流程再造及企業競爭的重要利器，也是攸關國家生產力及國家貿易競爭力提昇的重要管道。而未來在國家法令、網路安全標準制定，認證標準及國家網路頻寬解決後，將可解決網路上交易上現有的障礙，況且現代人也越來越注重時間的運用，希望能越短的時間取的物品越有經濟上的效益，所以用最節省時間的方式取得他們所想要的東西，為了迅速及便利故而採用線上購物，也就如此讓我們有了這個念頭，就是將電子付款系統作為理論性的研究及探討。

第三節 研究目的

本專題主要是現在網路上電子付款盛行，所以針對大家是否會怕交易安全方面及付款系統為何在國內依然無法普遍等問題一一探

討。然而我們想藉此主題的專題研究來讓大家對電子付款系統做更深入的了解，而另一方面也想加入我們本身對電子付款系統未來展望與安全機制還有加、解密技術的一些見解，我想這就是我們這一組所要研究的目的。

隨著網際網路商務應用的蓬勃發展，線上交易也衍生出許多安全性問題，目前電子商務上安全技術的發展已漸趨成熟，但是個人心理層面卻仍存在著對於商業關係的不信任。在電子商務交易關係中，企業可以藉由訂定合約、聲譽保證或社會契約來提高顧客信任感，至於個人對個人的交易關係，網路上的匿名性和非面對面的接觸方式，加上交易關係並無任何承諾約束，對於交易關係的信任更難建立。主要探討個人信任傾向和信任機制在個人對個人線上交易關係中的影響效果。結果發現，(1)消費者在個人對個人線上交易關係中，對於交易夥伴關係之信任感取決於個人信任傾向，此特質亦影響消費者對於交易滿意度之體貼性。(2)網站提供信任機制的服務，可以提高消費者對於交易夥伴之信任感和對於網站服務之滿意度。(3)網站提供不同的信任機制服務，對於使用者滿意度之有形性、保證性和體貼性具有顯著影響。(4)在不同信任機制服務下，高信任傾向的消費者對於交易之滿意度低於低信任傾向的消費者。(5)

個人信任傾向和信任機制之間並不具有顯著的交互作用。(6)信任傾向和信任機制對於交易信任感和滿意度之影響並不會受到個人電腦素養所調節。本研究之研究結果可以做為電子仲介提供加強消費者信任之機制的服務建議，以及個人線上交易信任的衡量與建立方式之參考。

第四節 研究範圍

這一波的資訊革命正在不斷地加溫中，能生逢此一關係人類文明發展的大時代裡，誠然令人興奮，但是如何創造出為我們所用的網路時代，正是我們所必當關切的重要議題。我們希望透過本篇論文，能了解在電子付款系統的內容和架構，並導引出付款系統未來發展的藍圖，所以首先在資料蒐集上我們大多採用直接資料，也就是在現有網路上所能蒐集到的第一手資料為主，而以間接資料和相關資料為輔助，畢竟真實地記錄並呈現網路的現況才能與網路發展同步，也才能更貼切地指出付款系統在未來網路應用上的方向，以網路為應用的當代或下個世代的電子付款系統，便極有可能成為安全的線上交易的最佳系統。

第二章 文獻探討

第一節 何謂電子付款及付款方式

2.1.1 何謂電子付款

電子付款是電子商業不可或缺的一部份。廣義而言，電子付款就是以線上方式進行買賣雙方的金融交換。這種交換的內容通常是由銀行或中間仲介或被法定貨幣所背書的數位金融工具（譬如加密過的信用卡號碼、電子支票或者是數位現金。電子付款之所以能引起金融機構的興趣原因有三：降低技術成本；減少營運和處理費用以及增加線上的商機。）電子付款之所以大量成長的主因就是渴望降低成本。

電子商務最重要之處不外乎顧客如何得到產品和服務，並在線上付款。目前，顧客可以在網際路上瀏覽到各個廠商所提供的產品和服務，可是可靠和安全的付款能力卻並不存在；正因如此，不相容的電子付款方法也激增抑制了電子商務的發展一小套可以廣為客戶使用且能廣為商店和銀行採行的付款方式。

2.1.2 電子付款的類型

(一)現金付款系統：由於現金的使用非常方便，即使在今日受塑膠貨幣及電子貨幣之衝擊，現金依舊是人們的最愛。

(二)銀行付款系統：支票付款系統、劃撥付款系統、跨行匯款系款、自動清算所（ACH）付款系款、電話語音轉帳與 ATH 轉帳。

(三)使用卡片付款：早在本世紀初，美國的百貨公司已發行顧客付款卡片。如：信用卡。

(四)郵購及電購（MOTO）：購買人通常僅須告知持卡人姓名、信用卡編號、信用卡有效日期及貨品送達地點等資訊，該筆消費即併入一般信用卡帳務系統處理。

2.1.3 依交易的付款方式可分為三大類

當消費者在家中利用 Internet 到全球的網路商店進行購物消費時，網路商店用來像消費者生取費用的付款系統。目前的發展方向是將傳統的支付方式(如支票、現金、信用卡)轉換成可利用網際網路的方式來進行支付。依交易的付款方式可分為三大類:

(１)中/大額付款(美金$10~數千元)：多以「信用卡」支付。

(２)小額付款(美金$10 元以下)：一般除了以會員方式收費外，目前 W3C 組織已經發展出「小額交易支付協定」(MPTP：Micro Payment Transfer Protocol)。並已經被美國 First Virtual 網路銀行採用。

(３)數位鈔票(Digital Cash)：由於使用信用卡消費容易留下個人消費記錄，且店家的收支也容易被稅務人員知悉，基於消費記錄保密的原因，數位化的電子現金亦開始被運用在網路上。目前發展中的系統如 Microsoft 的 MS-cash、Digicash、Netcash。

2.1.4 電子付款系統的種類

電子付款系統正逐漸被銀行界、流通業、線上商場、網路資料庫業者、政府單位甚至是進行線上情色會員交易的業者所廣為使用。上述我們提到的皆是電子交易系統的概念項目，而實際的電子交易系統種類到底有哪些？根據使用的支付工具來分類，而代幣式付款系統分為下列三種：

(一)電子現金(e-cash)

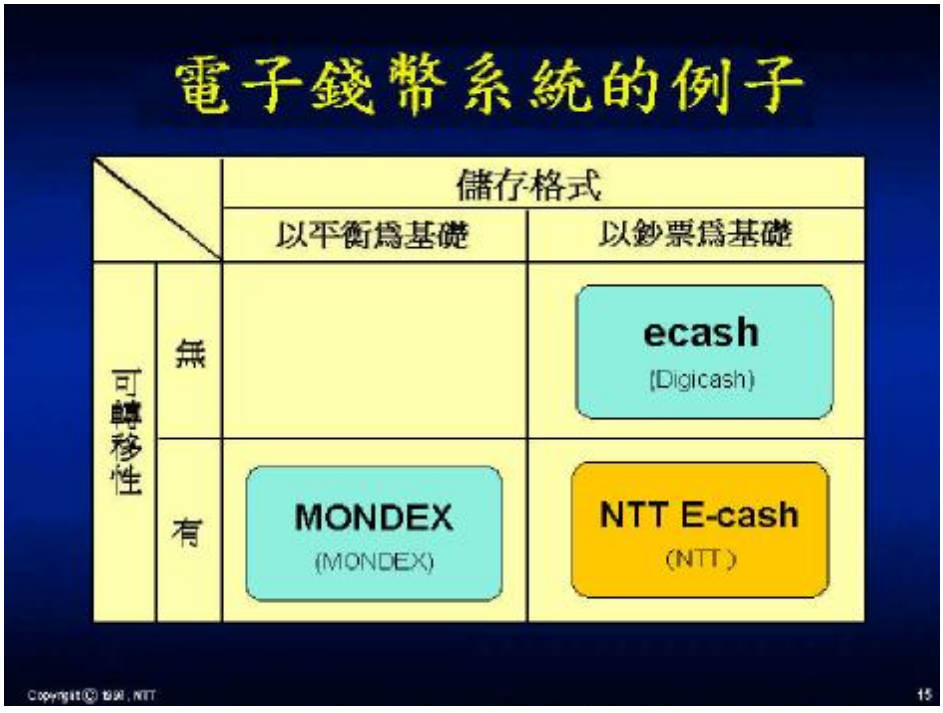
1.電子現金的現況

目前世界上晶片卡電子現金最著名的品牌首推 VisaCash 與 Mondex，分別由 VISA 與 MasterCard 兩大信用卡組織所推動。雖然兩者於 SET 安全交易的攜手合作，但在電子現金的競賽正方興未艾。VisaCash1996 年亞特蘭大奧運進行大規模的測試，並積極於美洲、歐洲推廣。目前正極力將 VisaCash 的系統功能加到信用卡、轉帳卡與金融卡上。至於 MasterCard，該公司自行研發的電子現金原本稍具劣勢，故購併 Mondex51%股份。Mondex 系統原來是由英國西敏寺為首的四家銀行所開發的，已在英國、香港等地完成測試；其特點包括可儲存五種不同的貨幣、准許個人與個人（Peer-to-Peer）的轉帳與資金轉移等。據聞統一超商擬與 VisaCash 配合，推動第一階段比較單純的 Pre-paid 卡在 7-11 店面來推動。Mondex 由於可以在個體之間直接轉換金流，央行與財政部正在了解這種做法對國家貨幣政策以及對金融環境的影響。

而在國內方面，財政部金融資訊服務中心自八十一年底推出 IC 卡銷售服務業務，提供匯集提款、一般轉帳、小額轉帳、信用及電話預付等功能於一卡，共有二十家公民金融機構參

與；但是推展經年後，遇到卡片功能太多、POS 設備操作複雜、圈存不方便等障礙，曾一時面臨曲高和寡的狀態。面對這樣的瓶頸與外商銀行和國際品牌 IC 卡的夾擊，金資中心計畫擴大本土 IC 卡的用途，增加預付卡的功能，選定台北博愛商圈及新竹科學園區為重點地區重新出發。在這場電子錢的競賽中，有心發展消費金融的銀行與軟硬體廠商勢必不可以掉以輕心。目前研考會、工業局、內政部、資策會已在正式的配合財政部推動金資中心金融 IC 卡的工作，引起民間公協會與廠商的熱烈參與。

表 1 電子錢幣系統之儲存格式表



2.電子現金主要用於小額的消費，可以節省平時像是使用信用卡的交易費用。電子現金具有下列幾項特性：

（1）電子現金可於個體之間交換、移轉，就如同現金一般。所不同的是，電子現金每一次移轉都要回到原發行機構，經過再重新發行才完成所有人轉換的動作。這也就是現金流和電子現金流之間的差異。

（2）電子現金和現金一樣，具有匿名的特性，無法追蹤到使用的身分，可以保障消費者的隱私權。換句話說，使用電子貨幣不必像信用卡簽帳般必須留下簽名以及個人資料。也因為如此，一旦電子現金遺失，便很難追回來。

（3）電子現金在使用時是獨立的，與銀行帳戶沒有直接的關連。不像信用卡直接傳輸卡號，有被截取的風險。然而，電子現金發行銀行或機構就必須維護一個大型資料庫，記錄已經使用過的電子現金，防止重複花用的弊端。

（4）電子現金與現金同是現付付款系統（pay-now Payment System），對銀行而言其性質是有所不同的。

電子貨幣的交易是無國界的，卡片上的 IC 晶片，可以同時設定不同的匯價，方便持卡人做跨國的交易。未來也可以發展到在 IC 晶片上設定用途。雖然使用電子貨幣是如此的便利，但相同的其擁有許多潛在的問題，首先，電子貨幣視同現金，卡片丟了，IC 晶片上原來以預付方式圈存的錢也就沒有了，不像信用卡遺失了可以馬上通知銀行掛失。二、如果卡片損壞了，儲存在卡片上的的錢也就消失了。三、由於電子貨幣交易無記名且沒有金額的限制，歹徒可以利用此特點進行洗錢等不法活動。

2.電子現金的美好未來?--由 DigiCash 實例來看

一、DigiCash--先鋒??先烈??

理論上網路上電子金錢是具有很大的發展與可能性，因為它是真正與現實生活中的「金錢」有相類似的特性，有相似的功能：可自由的交換、不記名、不需麻煩的簽章、可支付微小的付款、即時的完成交易等等，期望電子現金能夠藉著符合實際「金錢」的特性產生新的付款機制，創造出新一代的交易方式。然而，現實的生活所展現出來的事實卻不是

如此，DigiCash－第一家實行這個構想的公司，在不久前宣布破產保護，這和我們所期許的電子現金的美好遠景大相逕庭，相關的報導提到其失敗的原因有以下幾個重點：

（1）消費者和商家接受度不高

在 Digicash 慘遭破產之際，電子付款系統的前景似乎又受到重大打擊與考驗。電子付款系統並不像之前預期般盛行，消費者對其接受度不高的原因是並沒有很多商家採用電子付款系統，而商家卻認為消費者對於這種付款方式興趣不大且需求也不高，消費者與商家兩方面參與度都不高造成了電子付款沒有被廣泛採用。

而消費者也認為信用卡方式也比電子現金付款方式來得好。例如 Amazon 在信用卡付款的安全性上採用加密安全伺服器來保證交易安全，且對消費者蒙受未經授權付款的損失也予以保險補償；CDNow 信用卡付款在信用卡號傳送方面，不論是線上傳送或是 e-mail 訊息傳送都透過 PGP 方式加密。在線上傳輸信用卡號，雖然經過安全加密，但是消費者可以對此機制

放心，卻無法完全信任電子現金付款系統，這也是值得探討的地方。

（2）信用卡交易處理公司較為成功

目前而言，信用卡交易處理公司都較電子錢包交易處理公司來得成功，明顯對比的例子就是 Digicash 和 Ibill。對於 Ibill 採用 SSL 機制來保護使用者直接線上傳送信用卡資料，使用者的接受度比起同樣是安全性上設計良好的電子錢包卻高多了，Cybercash 發展 SSL 信用卡交易所獲得的利潤也比開發電子錢包系統來得多，可見消費者對於電子現金和電子錢包系統仍抱持懷疑的態度和強烈的不信任。

另外，一些先前發展電子現金系統的公司也紛紛轉向，如 FirstVirtual，已經停止電子現金交易而將重點轉向互動訊息傳送；CyberCash 目前主要收入來源也變成信用卡交易處理。

（3）電子現金的特點仍待發掘

在電子現金優點之一—小額付款的便利性也尚未彰顯出來。Powar 指出小額付款並非網際網路未來的發展重點，這也

降低了採用電子現金系統的需求和意願。但是電子付款系統也未到窮途末路的地步，例如其具匿名性的特點就非常值得關注。

在電子交易處理業者正把焦點轉移到其他目標上，如信用卡公司、公營機構和電話公司正採用線上支付帳單的方式。例如 Netscape 採用了 CyberCash 設計的機制發展了一個 Web 上支付帳單的系統—BillerXpert ，對採讓消費者在線上支付帳單的公司而言，不但可以節省郵寄費用且可以提供額外服務如個人化的內容等。

二、商家的看法

針以上的現象，產業觀察家則提出了另一個可能的見解：『消費者覺得使用信用卡，是較方便而舒服的。』

Amazon 的發言人 Bill Curry 認為：信用卡被過半數的人所使用，而我們也提供安全上的保障；這些都使得消費者對信用卡使用，信心增加。

CDNow 的客服部經理 Bill Trevor 則說：CDNow 的客戶們現在多半使用信用卡來進行交易。CDNow 的作法是：消費者可以送包含有信用卡號碼的 E-mail 給公司，而這 E-mail 是使用 PGP 的安全機制（Pretty Good Privacy:一種網路交易安全機制）。

事實上，很多採用信用卡交易的公司都發現，信用卡交易比電子錢包式的交易還來得成功，Ibill 公司的副總裁就說：現在已經有一種簡單、方便、快速的交易方法了，我們何必再去發明另一種類似的東西呢？（Ibill 公司業務是處理信用卡交易相關事項）

就 Ibill 來說，信用卡的交易使用 SSL（Secure Socket Layer）的安全機制，而這交易模式較容易成功。Cybercash 也正使用同樣的技術來運作。

Paul Kocher，一位編碼學的專家則說：「若是 Visa 或 IBM 來做 E-cash 的系統研發，那麼基於其背景的強硬，則很有成功的可能，但是今天發展這技術的是一家小公司－DigiCash，那麼要成功便是很難的一件事。」

然而，DigiCash 所發展出來的概念，對未來的貨幣型式，會有什麼影響，沒人可以預料，不過，很多公司及專家都很重視它所發展出來的新付款觀念，而 E-cash 的匿名性，更方便了消費者的交易，更顯出 E-cash 的價值。

在信用卡付款方面，為了要使線上付款成功及確認它的安全傳遞，必須使用密碼編碼及身份驗證的方法來確保付款的安全性。而其他線上付款工具，如數位現金、數位支票、電子錢包、智慧卡…等，同樣是在安全性、便利性、經濟性上經過良好設計過的付款方式，卻無法迎得消費者青睞，反而在網路公開環境下傳輸信用卡資料，消費者接受度反而較高，是消費者完全信任安全傳輸機制和標準，如 SSL 和 SET 以及其他信用卡處理公司開發或採用的安全機制?還是相較之下，消費者比較不能接受像數位現金、電子錢包…等這種看不見的東西，相對地也比較沒有安全感和信心?這不但是個有趣的問題，也是探討電子付款未被廣泛採用的關鍵之一，是什麼原因讓消費者和商家兩者的參與度和接受度都不高呢?

以智慧卡為例，對商家而言，以長期眼光來看，智慧卡應該是對於處理現金的替代方式。由於現金的計算、儲存及防止

竊取或誤置的處理費用很高，儲存的現金價值約有 4%被處理現金的手續所消耗。同時 IC 也較磁卡技術更難仿造。銀行也將長期眼光放在小型企業及消費者對現金的摒棄，最後由電話線路以 ATM、PC 代為處理所有業務。

我們以長遠眼光來看電子付款系統和工具，並且為其打造一片美好遠景，但是結果似乎不如預期中完美，消費者的接受度低是最大障礙。Digicash 的破產成了電子現金系統的重大打擊，諷刺的是先前開發電子現金系統的公司的最大收入來源並不是電子現金系統，而是信用卡交易處理系統，同時許多公司也紛紛轉向，連業者都不再努力甚至放棄了繼續開拓電子付款工具的新時代，消費者要重拾對其之信心想必更加困難了。

其實理論上，電子現金的匿名性和小額付款的便利性都是值得繼續發揚光大的，從 Digicash 針對其系統的匿名性申請專利權可見一般。其實電子付款工具，如電子現金、電子錢包、智慧卡…等發展潛力仍不容忽視，只要業者可以正視其背後的機制和意義，能讓消費者建立信心且真正享受到其好處。除此之外，消費者的行為，我們也應該加以探索，像

是目前一般的消費者都習慣於使用信用卡，也間接地造成了電子現金無法普行的因素之一，所以掌握消費者的心理及行為這方面，我們必須做更深入的探討，不可以貿然的投入市場之中。

(二)電子支票（Mondex）

Mondex 即是電子現金，它的主要用途在於取代日常小額消費的鈔票及硬幣。Mondex 卡擁有現金的特性，例如：人與人之間的轉值；人與商家的轉值；人對銀行的提款轉帳等功能。此外，Mondex 卡還有一個比現金更優良的特點，即是它能安全地通過電子管道（如：電話、網際網路等）來作人對人、人對商家、人對銀行的遠距轉值。

Mondex 卡的現金是儲存在晶片上，每一張卡就有如一個錢包，用來保存電子現金。每位持卡人都會由發卡銀行處取得一張 Mondex 卡，此卡會與持卡人的銀行帳戶連結以便讓持卡人作循環儲值。Mondex 卡是目前唯一在現實與虛擬世界都具有現金功能的 IC 卡 。

1.使用 Mondex 卡有什麼好處？

（1）Mondex 卡省卻找零的麻煩，縮短購物排隊等候的時間

（2）Mondex 卡能透過 Mondex 設備作循環儲值使用

（3）Mondex 卡能利用 Mondex 設備作近距離或遠距離的轉值

（4）Mondex 卡能上鎖，比現金安全

（5）Mondex 卡是電子商務（EC）上 B-to-C、C-to-C 最好、最安全的支付工具，有益公司發展 EC。

2.Mondex 的發展及國外使用狀況如何？

Mondex 目前是 MasterCard 公司旗下的一關係企業。Mondex 係 1990 年由英國西敏寺銀行（Natwest Bank）首創的付款體系。經多年發展，於 1995 年首先在英國 Swindon 地方測試，之後逐漸擴大到加拿大、澳洲、紐西蘭、香港、愛爾蘭、以色列、法國、美國、日本、韓國等。台灣亦由宏碁集團及富邦銀行於今年引進，在汐止東方科學園區測試。

3.如何使用 Mondex 卡消費？

在 Mondex 特約商店購物消費的步驟如下：

（1） 將您的 Mondex 卡插入商家的終端機中

（2） 商家的店員會將您該次的消費金額輸入終端機中

（3）您僅需核對終端機上的金額是否相符

（4）若您的 Mondex 卡已上鎖，則需再輸入您的 Mondex 密碼

（5）Mondex 交易即告完成，您該次的消費金額將自 Mondex 晶片中自動扣除

4.個人密碼（PIN）有何用處？

個人密碼（PIN）係保密號碼，讓您可為 Mondex 卡上鎖，如此其他人就無法使用 Mondex 卡裡的現金。當您初次領取 Mondex 卡時，服務人員會請您為 Mondex 卡設定一個私人密碼。您可自行設定一個四至八位數字的密碼。 當使用 Mondex 自動櫃員機時，您需要輸入個人密碼；將 Mondex 現金由帳戶轉入 Mondex 卡時，亦需輸入私人密碼。此外，當您想用 Mondex 現金時，您就需要用密碼將卡解鎖（假如您之前已將卡上鎖）。 您可利用 Mondex 自動櫃員機或您自己的 Mondex 餘額顯示器將卡上鎖或解鎖。

5.除提存 Mondex 現金外,Mondex 自動櫃員機還可以提供何種服務？

利用 Mondex 自動櫃員機可查詢聯繫帳戶的結餘，將 Mondex 卡上鎖或解鎖，查詢結單，查詢卡的結餘，還可以更改私人密碼。

(三)智慧卡（IC）

1. 信用卡式付款系統

（1）加密信用卡(SET.SSL)

（2）第三類認證(CA)

第二節 電子付款之優點

優點：以現有最高階的加密方法所建立的穩固系統，以及自由使用的亂碼函數可以確保沒有任何一方可以改變訊息，所以每一方都可確認訊息的正確性。類似代幣的現金，可以用於許多類似代理程式的網路應用程式中。系統提供有限的匿名性給買方與賣方。雖然對銀行而言，要監控顯示出大量交易的帳戶是有可能的，但是沒有人可以追溯顧客的電子現金到底花到哪裡去了。儲值智慧卡是批發的，不需要中央的核准，這可以大大地降低中央管理的費用。

第三節 電子付款的缺點

缺點：採用多重認證的方法固然不錯，但是沒人有充足經驗將其分發給廣大群眾，所以此標準可以在客戶沒有證明時處理付款，很明顯地此標準與要求付款一致，只有時間可以證明這是否可行。即使是部份的匿名，亦會使得有些人緊張。儲值智慧卡是批發的，

如果有人發現可以複製的方法，那麼可能會造成很嚴重的後果。

第四節 安全機制

2.4.1 安全機制

目前較常探討的安全機制包括 SSL、SET 等方式

（一）SSL（Secure Socket Layer）

SSL 的主要功能，是經由使用者的瀏覽器及主機端的 Web 伺服器，所共同提供的一套安全機制，其主要目的是要讓使用者在網路上所傳輸的每一份資料，都能受到安全的保護，例如：

（1）資料加密：提供資料加密功能。

（2）身分識別：瀏覽器連上 Web 伺服器後，伺服器會核發憑證給使用者以確認身份。

（3）資料檢核：當資料被人修改或攔截時，Web 伺服器可以偵測到此資料是否被動過手腳。

雖然 SSL 是目前電子商務網站上較常用的一種安全資料傳輸形式，但是它還是有一些問題有待克服，例如：

（1）缺乏認證機構。

（2）無法確認消費者是否為持卡本人。

（3）店家與收單銀行缺乏標準傳輸介面，資料不易整合。

（4）信用卡資料是傳給店家，因此資料有可能會被店家非法使用。

SSL 通訊協定提供連線安全（Connection Security）的通訊服務，有以下幾個特性：

（1）通訊雙方所建立的連線（Connection）是隱密的，加密的動作會在通訊雙方完成協商的程序後，依據協商後只有雙方才知道的加密金匙（key）對傳送資料作加密。對稱性保密系統將用來作資料的加密，所採用的演算法有 DES、Triple Tripl、DES、IDEA、RC2、RC4 等。

（2）通訊者的身分（Identity）識別（Authentication）是採用公開金匙保密系統，所採用的演算法有 RSA、DSS

等。

（3）通訊是可信賴的（Reliable），訊息傳遞時會同時跟隨著傳送「資料完整性檢查」的「資料辨識碼（MAC Code）」，資料辨識碼的計算是採用 MD5、SHA 演算法。

SSL 是位於傳輸層（Transport）之上的通訊協定，在 SSL 之上可以執行 Telnet、FTP、HTTP 等應用程式(如下圖)。

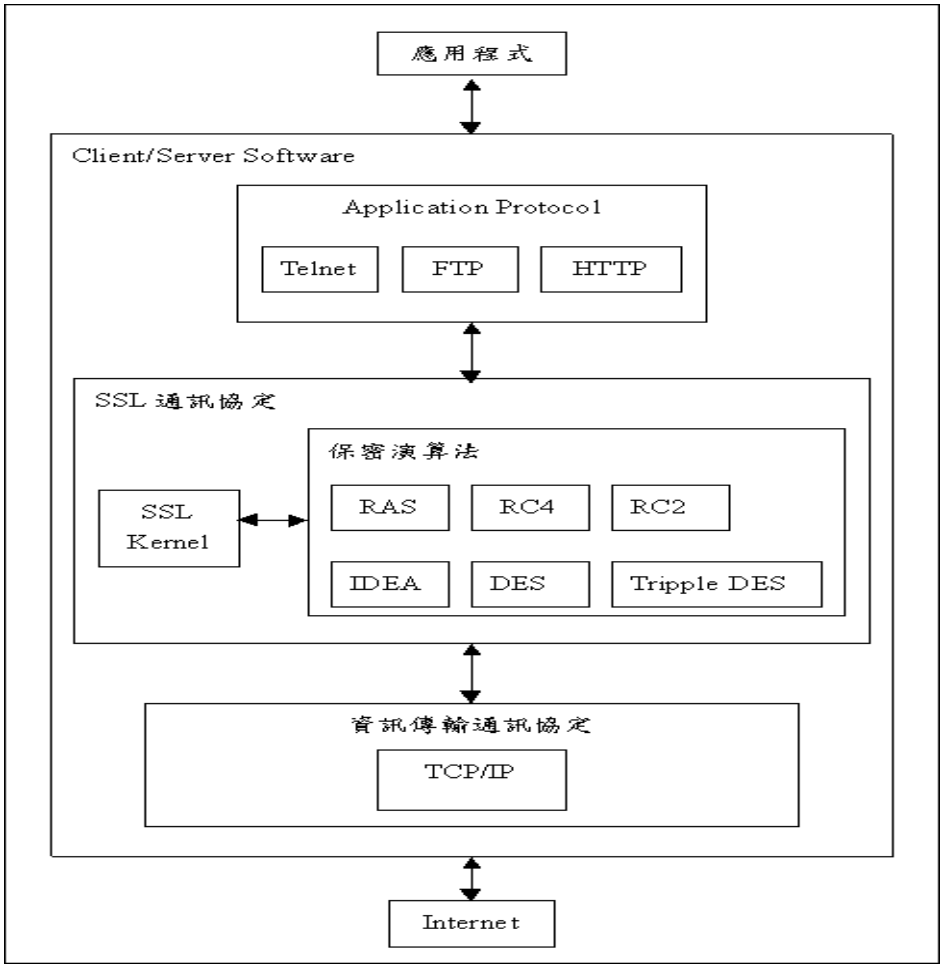


圖 1 SSL 之通訊協定

在發送端，所有要送出去的資料會先用一個只有在接收端才知道的加密金匙對資料做加密。在接收端，先對資料作解密動作後再傳回給預期的接收者。

1. SSL 的通訊協定包含兩個部份：通訊協定包含兩個部份。

（1）SSL 協商處理通訊協定：負責協商決定加密的方法與執行身分的識別。

（2）SSL 記錄處理通訊協定：對資料實施「加/解密」與「包裝/還原」的服務。

2. SSL 記錄處理通訊協定

SSL 記錄處理通訊協定（SSL Record Protocol）在發送端是將資料加密後包裝固定格式的 SSL 資料錄(SSL Record)，在接收端是將資料解密並還原。一個 SSL 記錄其格式分成記錄檔頭（Record Header）與記錄資料（Record Data）兩部分。

（1）記錄檔頭：用來指明訊息的種類（一般訊息、SSL 協商訊息或錯誤訊息等)、訊息的版次、記錄的長度。

（2）記錄資料：包含實際要傳送的資料、訊息辨識碼（MAC Code）、填充資料（Padding Data）與填充資料的長度。填充資料室使用區塊加密法時才會用到，目的是讓資料的總長度符合區塊加密法所需要的長度。以上資料準備完成後，將依通訊雙方同意的加密演算法予以加密。「訊息辨識碼」的目的是讓接收者可以檢查資料的內容在傳送的過程是否遭到篡改，資料傳遞次序是否正確等。計算方法勢將途中資料準備完成後，做一個雜湊函數的運算，得到 16-20bytes 的訊息摘要（Message Digest）。

接收端接收後，依相反的次序先行解密，檢查訊息辨識碼後還原資料的內容。

SSL 協商處理通訊協定（SSL Handshake Protocol）的目的是讓通訊雙方交談協商，決定要採用哪一種加密演算法、加密用的加密金匙與辨識通訊者的身分。SSL 提供三種身分辨識的模式，分別為：

（1）全匿名式通訊(Total Anonymity):Server 端與 Client 端未持有經過「公開金匙認證中心」認證過的「憑證

資料」，所以雙方的身分無法確實確認，不過依舊可以與匿名者建立安全的通訊管道。

（2）伺服主機單方辨識通訊（Server Authentication With An Un-authentication Client）：Server 端持有經過「公開金匙認證中心」認證過的「憑證資料」，所以 Server 端的身分可以確認。

（3）通訊雙方身分辨識通訊（Total Authentication）：Server 與 Client 端都持有經過「公開金匙認證中心」認證過的「憑證資料」，雙方的身分可以確認。

3. SET 的源起

安全電子交易(Secure Electronic Transaction，簡稱 SET)是一個用來保護在任何網路上信用卡交易的開放式規格，SET 協定融合了從 RSA 資料安全的公開鑰匙編成密碼文件的使用，以保護任何開放性網路上個人和金融資訊的隱密性。

SET（Secure Electronic Transaction）：SET 協定主要是由 VISA 和 MasterCard 信用卡發卡組織及 IBM 等公司提

出，交易是以信用卡為基礎的網際網路安全電子付款協定，目的是將信用卡在店家刷卡的交易方式， 轉移到消費者的電腦上。在 SET 的機制中，一個完整的線上購物交易包括訂購申請、身份認證、付款授權、付款取得及交易狀況查詢。經由上述的機制，可以讓消費者、網路店家及銀行放心地在網路上進行電子商務活動。目前 SET 交易模式中會牽涉到的個體包括：

（1）持卡人：一般消費者；擁有發卡銀行的信用卡，並向認證管理中心取得電子證書。

（2）特約商店：在網路上提供商品的業者，須與收單銀行簽約，並接受消費者透過網路來付款的商店。

（3）收單銀行：負責授權與管理特約商店的銀行，並提供交易的信用卡付款授權申請和付款取得。

（4）發卡銀行：發卡銀行與收單銀行須進行交易的付款授權、帳務清算等訊息之交換。

（5）認證中心(Certificate Authority;CA)：負責管理電子證書的認證。

SET 是 Visa 與 MasterCard 兩大信用卡發卡中心與 IBM、Microsoft、Netscape 等公司於 1996 年所提出的，它是由 VISA 國際組織與 MasterCard 國際組織，於 1996 年 2 月共同宣佈制定安控規格於網際網路上的交易協定(Protocol)。隨即美國運通(American Express)，HP，Microsoft，IBM，Netscape，VeriSign 等公司紛紛表示加入並支持此一標準。時至今日，SET 已成為國際上所公認在 Internet 電子商業交易的安全標準。

這個協定是以信用卡的交易為起始點，從商店透過網際網路進一步擴展到消費者的個人電腦上面，在新的交易方法中，以網際網路取代傳統面對面的溝通。因此持卡人、商店，及透過網路交易的消費者的角色認定，以及如何確保交易訊息的正確性、完整性，並且能保有私密性，就是 SET 協定規範的重點。

（二）為什麼需要 SET ？

（1）線上欺騙行為—很難確認使用者的真實身份

（2）web 認證—在要求服務之前，使用者必須證明自己的身份。

（3）EC 商家希望有更容易、更安全、可靠和有規模的認證方法。

（4）第三方—收送雙方相互確認身份

1.SET 的特色

（1）可信的資訊—由商家和銀行保証交易資訊的安全，防止被攔截修改。

（2）完整的資訊—確認資訊在傳送過程中沒有被修改。

（3）使用者帳號的認證—確認使用者是有效帳號的合法使用者

（4）商家的認證—確認商家身份，才允許他們接收銀行卡付款。用數位簽名和商家認證

（5）相互操作性—set 標準適用在許多軟、硬體上，消費者可和商家軟體相溝通，如果標準相同的話。用標準協定和訊息格式。

1.SET 的架構

SET 的架構是由幾個成員所共同組合起來的。分別是 Electronic Wallet(電子錢包)，Merchant Server(商店端伺服機)，Payment Gateway(付款轉接站)，和 Certification Authority(認證中心)。而運用這四個成員，即可構成於 Internet 上符合 SET 標準的信用卡授權交易。而欲落實 SET，則須靠 SET 所規範的交易模式中參與的各個個體。

一般來說，SET 所規範的交易模式中，所參與的個體包括：

（1）持卡人（Cardholder）：即擁有發卡銀行授權許可的信用卡，而且必需要先向認證管理中心（Certificate Authority）註冊登記並且取得簽張認證（Signature Certificate），以便進行交易。

（2）特約商店（Merchant）：在網路上提供商品的商店或者服務的機構一定要和收單銀行簽約，而成為可以接受客戶信用卡電子付款的特約商店。

（3）收單行（Acquirer）：主要是負責授權與管理往來的特約商店，並且負責在交易進行的時候，提供信用卡付款的授權（Payment Authorization）申請及付款取得（Payment Capture）的服務。為了完成付款取得的服務，所以在電子商務中通常會增設一個付款通路（Payment Gateway），這個付款通路分別透過網際網路與特約商店連線，並且透過原先已經存在的金融網路與發卡銀行交換訊息，取得交易的授權。

（4）發卡行（Issuer）：在每一筆交易進行之前，發卡行就會先代理接受持卡人簽章認證的申請，並且經由發卡行發出一張含有 CA 簽章的電子信用卡，這張卡可以是 Visa、MasterCard、AE 或是 JCB，依照持卡人的申請而定。當收款行透過金融網路要求付款授權的時候，發卡行就應該回應付款授權的申請，等到交易完成後再與收單行進行帳務清算並且交換訊息。

（5）簽字管理中心或稱數位簽字認證機構

（Certificate Authority，簡稱 CA）：負責所有電子認證的工作。原則上持卡人只須要一對金鑰，用來申請簽章認證，但是其他參與個體則需要兩對金鑰，分別用來申請簽章認證和換鑰認證。而認證的管理與運用就是 SET 協定是否可以安全的在網上交易的關鍵，故通常由公正可信的組織擔任此一角色，以求線上交易的安全性。

（6）VISA 國際組織：其主要的任務、公能是協助各國或各區建立電子數位證書的系統。並且協助各國或各區建立支付通路服務及支援方式；發展有關安全電子商業的基本教育及訓練素材，此外，更可協助會員銀行發展安全電子商業的網路架構及主機系統，以支援安全電子商業交易。由上述可知，VISA 國際組織實是電子商業參與者以及 VISA SET 科技小組的居中橋樑。

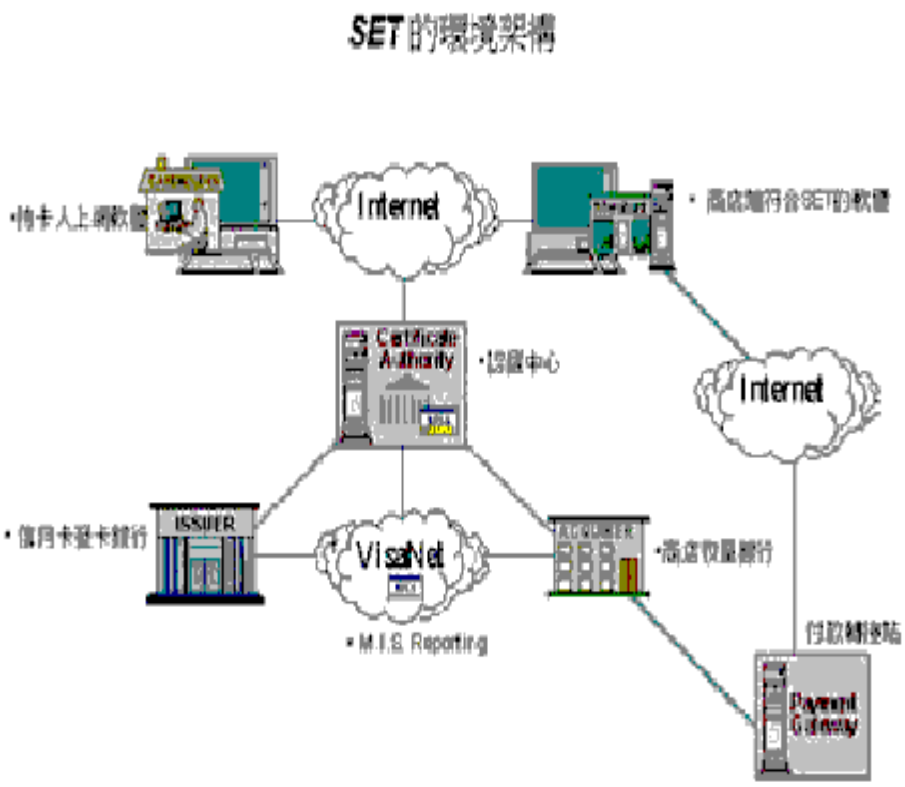


圖 2 SET 的環境架構

3.SET 線上交易流程

在 SET，一個完整的線上購物交易可細分為四部份：訂單申請、付款授權、付款取得以及交易狀況查詢。

4.SET 線上交易流程如下圖所示：

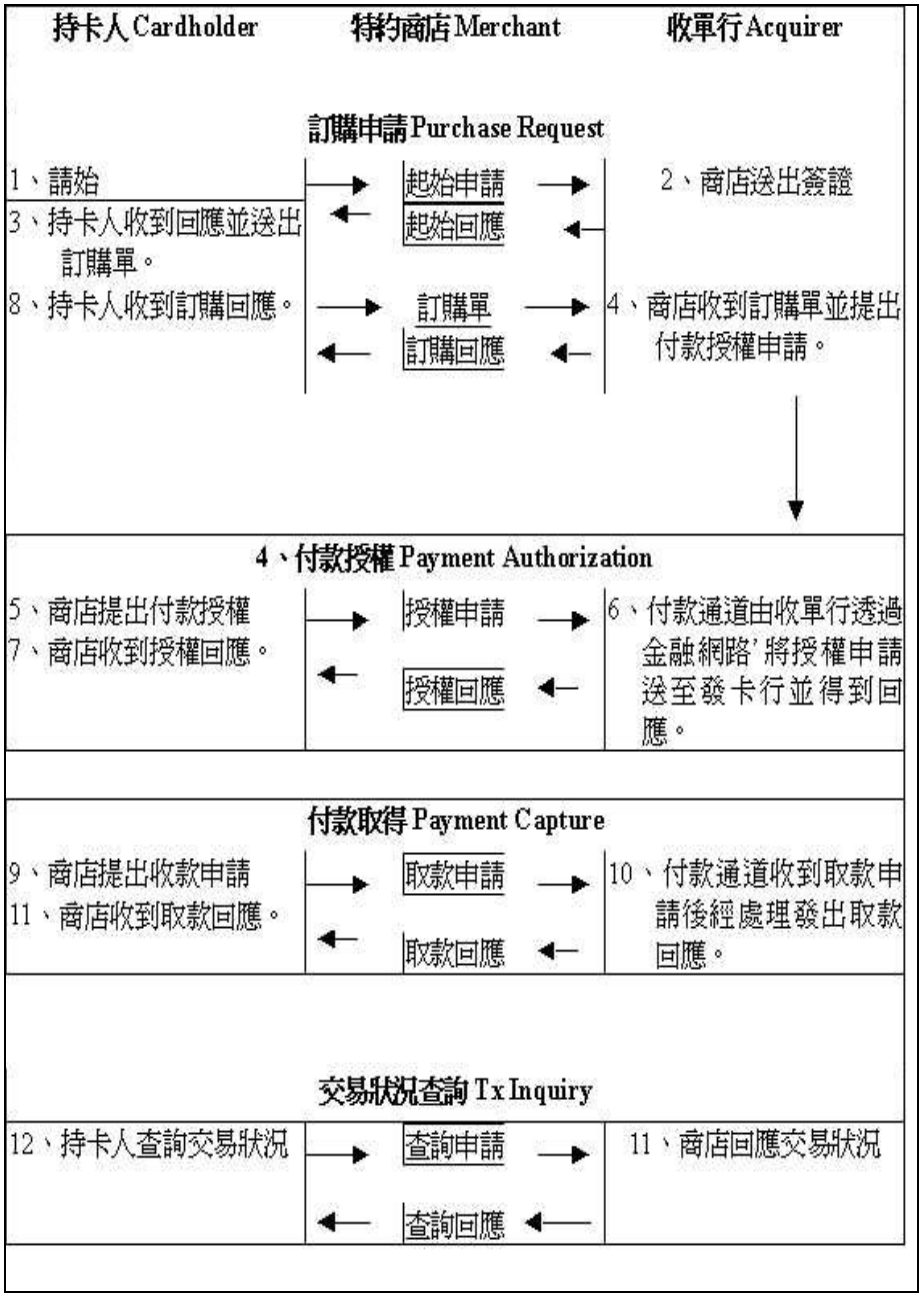


圖 3 SET 線上交易流程

交易/授權流程

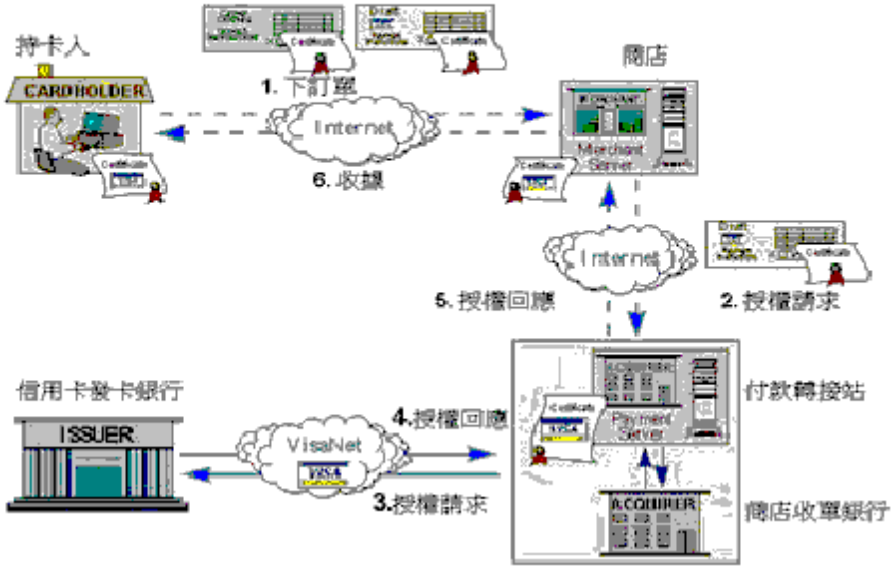


圖 4 交易/授權流程

4. SET 所採取之安全機制

歸納整理出 SET 所採取之安全機制如下：

（1）在認證方面：認證的交換驗證配合數位簽章以確認交易進行時雙方身份，進一步提供不可否認的功能。

（2）在密碼演算法方面：DES 與 RSA 互用以確保資料的秘密性。

在數位簽章方面：函數與 RSA 密碼演算法構成數位簽

章，以保護資料的完整性，防止偽造；並以數位信封、雙重簽章確保資料的隱私性與關連性。

5. SET 線上購物如何運作

雖然以下的 SET 交易過程十分複雜，但是一項網路購物的交易處理進行、授權與完成僅是花費幾秒鐘時間而已。請瀏覽 Visa Secure Electronic Commerce 的世界，看一看範例，為您示範 SET 如何運作——以及您要如何使用它來安全購物。

（1） 首先，持卡人取得電子錢包（digital wallets）

持卡人的電子錢包軟體自動地與特約商店的 SET 軟體溝通，確認商店的證書與銀行的往來關係。SET 規格的電子錢包可以在線上向幾個授權的廠商取得、在幾個受歡迎的瀏覽器新版本、或是由銀行提供軟體。

（2） 其次，持卡人取得電子證書.

持卡人必須先與其發卡銀行聯繫，完成註冊程序。Visa 國際組織提供電子證書給發卡銀行，讓發卡銀行提供電子證書給其持卡人。當交易進行與交換資料之前，每一方的 SET 軟體會確認特約商店與持卡人雙方的電子證書。

（3）第三，持卡人與特約商店進行購物對話

當您決定要在線上購買某項商品，特約商店會將訂購單與商店證書一併發送。只需要選擇所要使用的支付卡片，在您訂購時，的軟體會自動地把相關的證書(持卡人可能只是運用SET 就能安全購物，而不必提出電子證書。只要特約商店有能力確認持卡人身分，SET 交易也可以根據規格加以完成。)寄出。軟體會附上持卡人的付款說明，寄給特約商店，全部資料使用公開鑰匙加密技術，特約商店無法看見支付卡片的資料，惟有特約商店的收單銀行可以解密。

（4） 第四，授權與清償（settlement）的過程

一旦購貨單與付款資料安全送達，特約商店的收單銀行會要求持卡人的發卡銀行授權，正如同現在一般的特約商店請款方式。授權之後，特約商店就會向持卡人確認交易。清算與清償也就是像現在一般的付款與交易過程。

6.SET 軟體規劃

給買方或賣方的 SET 軟體規格可以在網際網路的 www.setco.org 找到，以下分別是組成 SET 規格的四個要素：

（1）持卡人的「錢包」軟體：這個軟體讓持卡人能夠透過簡單的點選動作（point-and-click）進行安全購物，與特約商店的 SET 軟體自動溝通，確認特約商店的證書以及與銀行之間的往來關係。這個軟體管理與保存持卡人的電子證書，消費者的電子證書是卡片的電子形式，儲存持卡人的帳戶資料與發卡銀行相關資料。

（2） 特約商店軟體：這個軟體包含與持卡人以及發卡銀行溝通的技術，它管理交易前的電子證書交換。特約商店的電子證書取得特約商店的資料以及特約商店與 Visa 會員銀行的往來關係。

（3） 支付閘門伺服器（Payment Gateway server）軟體：這個軟體專責自動處理標準支付過程。它會將持卡人的付款說明加密，且支援特約商店要求認證的過程。支付閘門伺服器將特約商店收單銀行傳來的 SET 交易資料轉換為現在 Visa 卡交易所用的格式。

（4） 認證授權軟體：銀行會使用這個軟體同意持卡人或特約商店的個別帳戶註冊，並用以進行安全電子商務。這個

軟體也會用來核發「電子證書」（digital certificates）給持卡人或特約商店。這些證書包含一組電子資料、密碼鑰匙與其他資料，這些被儲存在持卡人個人電腦中的軟體內，每一次持卡人透過電腦上網購物的時候就會被使用。電子證書確保參與電子商務交易的雙方是可以互相信賴的，電子證書也包含 Visa 國際組織與發卡銀行的數位簽章（digital signature），使特約商店可以知道持卡人的卡號已獲許可使用 SET 交易。

整個 SET 的成功推行，實有賴於許多因素的配合，不是單純的要有買、賣雙方的參與而已，還必須有夠安全、夠快速的加密技術以確保資料安全；認證技術以及數位簽名技術以確認買賣雙方身分，達到合約中的不可否認性，而在這整個架構的落實推行上，則還需要一個在技術上、管理上夠公信力的組織 CA，來推動其中相關技術及個體的管理。在這個組合中，每個環節都必須健全，不然將危及所有參予的個體，也將使整個 Internet 交易不再被信賴，其影響之大將是不可估計的！

在 SET 於電子商務中所採用的安全技術裡，各種的加密演算法都已經經過了幾十年的發展改進並接受各方的考驗，相信在相

對的短時間裡，應用來保障一般人的資料應是夠安全的，不過隨著科技的日新月異，對於安全性的擔心，實在是不可或忘的，尤其得記住，在 SET 中，交易的個人也為其中一環，培養大眾擁有資訊安全的基本觀念，由每個人自己本身做起，相信才是最根本預防各種非法傷害的最根本之道。

隨著電子商務（EC）及電子資料交換（EDI）的日趨普及，在未來勢必發現傳統以紙張文件為憑證進行交易的模式，將演進到透過網路以電腦數位資訊為依據的新交易形態。但是無論紙本文件或數位電子文件，都同樣面臨如何辨識文件真偽及防止偽造或否認的問題。所以在網路上，認證中心的興起，便是為了提供網路上交易傳輸文件之保證。而電子商務的基礎結構便是要建立在有效管理的認證中心上。

表 2 SET 電子安全交易機制及 SSL 電子安全交易機制比較表

	SET 電子安全交易機制	SSL 電子安全交易機制
方便性	1.需持有提供 SET 服務銀行的信用卡 2.需申請電子交易認 3.需有電子錢包軟體 4.商家需向銀行提出認證申請 5.商家需有 SET 交易軟體	1.需持有信用卡 2.商家需向銀行提出信用卡刷卡加盟申請
安全性	1.公開鑰匙加密的製碼技術 2.無被破解紀錄	1.IBM 所研發之網路訊息加密技術 2.無被破解紀錄
使用率	測試推廣階段,持有人數僅有數千人	凡持有信用卡的用戶均可使用
認證機制	1.中華民國金融資訊中心可確認交易之三方（銀行、商家、消費者）之確	1.中華民國金融資訊中心可確認交易之三方（銀行、商家、

	實交易內容 2.電子證書及電子簽名確認交易	消費者)之確實交易內容 2.電子證書及電子簽名確認交易
未來發展	1.由銀行及政府主力推動 2.安全機制受商家肯定	民間業者自行發展

第五節 線上交易的安全

【線上交易的安全】

1. 五種 Internet 安全需求：

（1）隱私性：控制誰可以、誰不可以看

（2）驗證性：連線的對方身份驗證

（3）完整性：確保資訊在傳送中沒被修改

（4）可用性：資訊和連線服務的有效性、可用性

（5）封鎖性：封鎖不要的資訊和干擾

2. 線上交易資料類型：

（1）Public data：沒有安全限制，可被任何人閱讀；易可禁止修改。

（2）Copyright data：非機密的，需經本人同意才可使用。

（3）Confidential data：內容是機密的，但存放地點不是機密，如：銀行帳戶、個人檔案 。

（4）Secret data：內容機密，且存取需經嚴密監控和記錄。

3. 交易安全的基本需求

（1）Privacy：未經授權的網路窺探程式 packet sniffing，安裝窺探程式來監視網路活動，會針對網路資料交換中特定資訊，如 ftp、telnet、login…偷取使用者帳號、密碼…如果 backbone 上的電腦系統遭侵害，破壞者即可監視網路往來

的 node 的資料。

（2）Confidentiality：網路環境必須保障所有通過的訊息資料。當成功傳遞至目的地閘道器後，這些訊息必須從公共環境中移除。僅保留訊息資料長度、驗證資料、或稽核軌跡。所有訊息必須在安全保護完善的系統上進行。還需對尚未完成傳送的暫存訊息一旦發生無法復原的毀損時的應變措施。因為資訊常被攔劫或盜取情況愈來愈嚴重，所以加密變得很重要。

（3）Integrity：資訊在傳送前和收到後必須一致。傳遞時確保不會被修改、新增或刪除。未經權而擅自送出、核對、處理或傳遞，混合連接其他資料也都不可以。被動採用訊息保密方式，而資料完整的維護技術則在預防資料遭受修改的主動性攻擊。

第三章 研究架構

第一節　研究流程

近年來因為在網路上交易的人越來越多，所以交易的安全就是更為重要了，這也是我們想要研究的動機，既然有了個方向就開始收集相關的資料，為了要了解其進行步驟，所以在線上作實務的操作、測試，看看是否符合我們所要的東西再確定專題題目，接著開始規劃整個研究該往哪個方向進行，並且訂立明確的目標把整個文獻內容整合彙總。

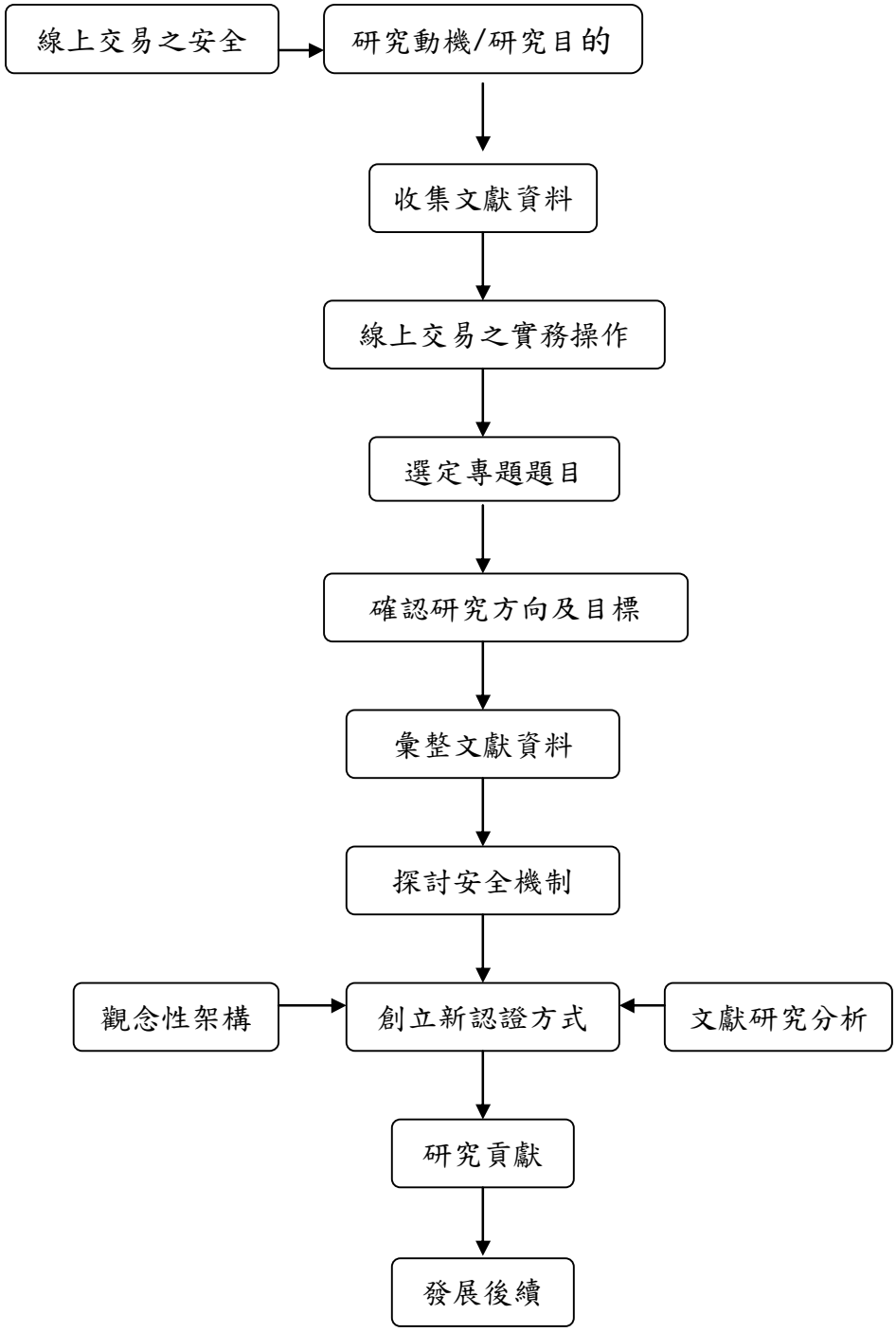

線上交易之安全
研究動機/研究目的
收集文獻資料
線上交易之實務操作
選定專題題目
確認研究方向及目標
彙整文獻資料
探討安全機制
觀念性架構
創立新認證方式
文獻研究分析
研究貢獻
發展後續

圖 5 研究流程圖

第二節　研究限制

在此研究當中所受的限制是目前手機並不是每個人都有,所以我們提出的用手機確認這項動作可能某些人就無法實行了,這也是目前的難處。還有另一點是因為要用手機確認,故等待時間增長或許消費者就不想採取此方法，故在未來應要加強這兩項缺失。

然而在網路的安全、法律、管理、技術標準等方面，尚待有很多問題待進一步克服，根據天下雜誌 1998 年網路調查報告指出網路安全性與網站真實性是台灣的網路使用者對網路交易的二大顧慮，因此如何建立用戶對網路安全信心，是國內發展電子付款的首要工作。

第四章　研究分析

第一節 電子系統付款之架構

電子付款系統必須要有硬軟體設備的支援，這些設備分別是電子錢包（Electronic Wallet），商店端伺服器（Merchant Server），付款轉接站（Payment Gateway），和認證中心（Certification Authority）。必須利用這四者才可構成於 Internet 上符合 SET 標準的信用卡授權交易。其架構如下圖 3-1-1 所示：

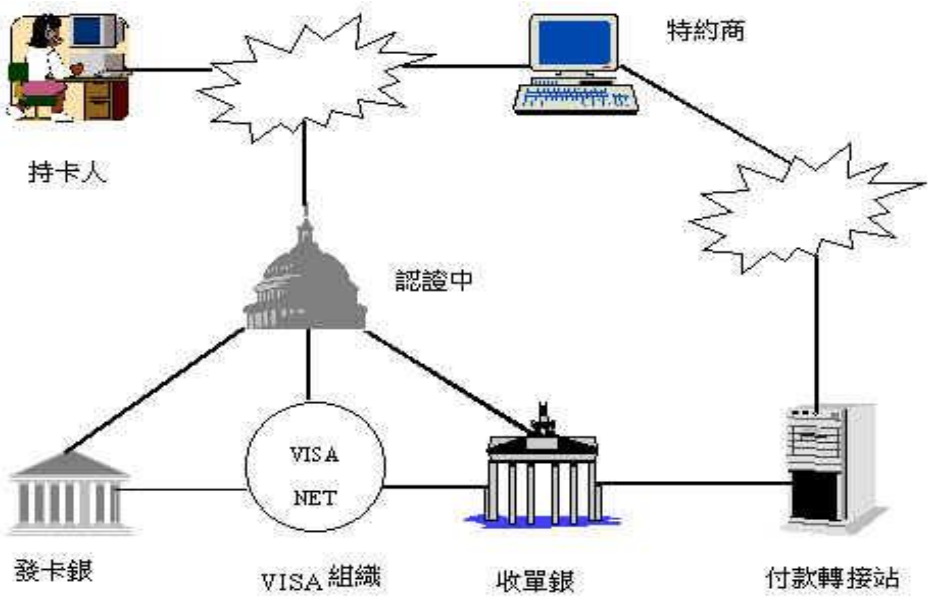


圖 6 電子付款系統的架構

以上便是電子交易的架構，其中還包含了一個組織是上述未提到的，即是 VISA 組織。VISA 國際組織的功能，是協助各國或各區建立電子數位證書的系統、支付通路服務及支援方式、協助會員銀行發展安全電子商業的網路架構及主機系統，以支援安全電子商業交易、回答任何有關 SET 規格的疑問、提供信用卡授權及清算網路系統。

但在電子付款技術中我們還需要一個技術提供者，他負責支援能在線上進行交易的安全軟體，並包含了消費者軟體提供者、特約商店軟體提供者和認證服務提供者。其功能分別如下：消費者軟體提供者開發符合 SET 規格、持卡人所需之上網軟體及瀏覽目錄軟體、特約商店軟體提供者發展應用 SET 規格的特約商店軟體、認證服務提供者發展應用 SET 規格的電子證書授與及認證軟體。

第二節 觀念性架構

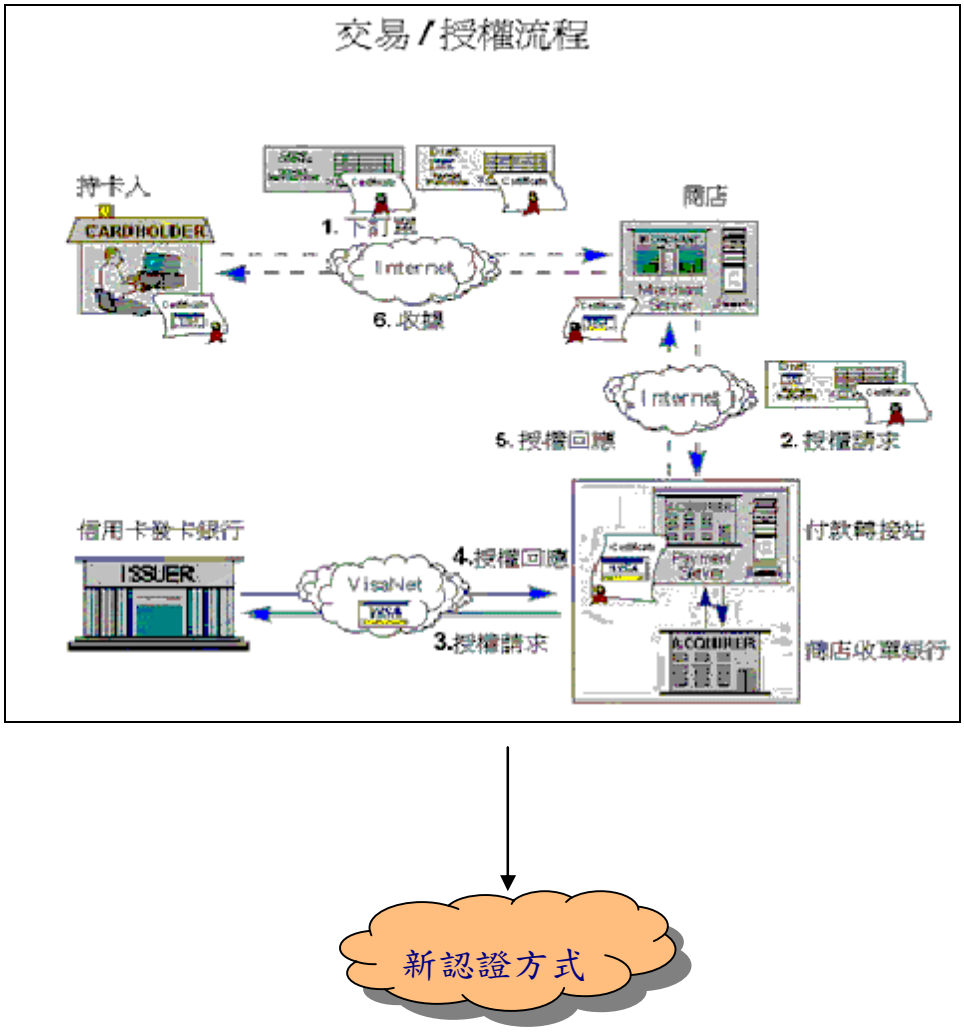


圖 7 觀念性架構圖

電子商務的環境中，認證已成為網路安全不可或缺的一個因素。但是什麼是認證(certification)呢？而 CA（Certification Authority）又為何？為什麼電子商務的交易環境需要這樣的機制？這些是本節所要討論的主題。

假若 A 與 B 欲進行秘密通訊時，資料要進行加密（Encryption）動作，先前必須要協調一把雙方都認可的加密金鑰（key），當 A 要

送訊息給 B 之前要以加密金鑰進行加密運算，而當 B 收到此一加密的訊息後，也要以加密金鑰進行**解密**（Decryption）運算將訊息還原，以達成秘密通訊的效果。因為加密與解密是使用相同的金鑰，因此這種方式稱之為對稱式加密法，其中以資料加密標準演算法（DES）最為著名。此種方式的演算法是公開的，因此其安全性的高低取決於金鑰的長度及隱密性。

非對稱式加密法是通訊的雙方，在通訊之前，雙方先產生一對金鑰，一把是私人金鑰（private key），另一把為公開金鑰（public key）。公開金鑰是必須要讓所通訊的對方得知的。例如當 A 與 B 要進行通訊時，A 要先將訊息以 B 的公開金鑰進行加密再傳送給 B，而當 B 收到 A 傳送的訊息後，則必須以 B 自己的私人金鑰加以解密才可以得到原始的訊息。由於訊息的加密是以 B 的公開金鑰加密的，所以也要 B 的私人金鑰才可以加以解密。因此非對稱式加密法可以產生數位簽章（digital signature），若訊息含有數位簽章，則此訊息的發送人將不可否認（non-repudiation）傳送訊息的動作，可以確保訊息的內容與來源是正確的，也不易遭到仿冒。

而非對稱式加密法在做訊息加密或是數位簽章時，雙方必須要取得對方的公開金鑰，而公開金鑰的取得可以透過雙方私下的交換

動作，也可以透過第三的公正團體來進行具公信力的認證與發送，不過以後者作為公開金鑰的取得在安全性方面來說是比較好的。此種為公開金鑰進行認證與發送服務的單位，就是一般所稱的認證中心（Certificate Authority, CA）。認證中心對於網路上交易具有不可否認性的業務，例如股票線上交易、網路銀行業務等，是重要的安全機制之一。

第三節　引入新認證方式之分析

之所以要有新的認證方式，主要是因為現在線上訂購系統發展的還不夠健全，怕有以下情況發生：

1. 國內金融犯罪。
2. 消費者最擔心的原因怕被盜刷。因為經濟的不景氣，造成高失業率，使得犯罪機率越來越高，其實信用卡的盜刷的問題一直存在著，只是最近越來越猖獗了，這就是消費者所擔心的原因之一。
3. 現金交易較不方便。說真的現金雖是大家一致認同的交易貨幣，但它有時攜帶並不方便，像是大筆交易的話總不能帶了

一大筆的現金在身上吧，因為這樣很引人注目的，而紙幣算是還好，說到硬幣那才是疼痛呢，因為它的重量太重了，所以帶出門並不方便呀，這就是現金交易不方便的地方了。

4. 信用卡怕被仿冒使用。這是只當你在線上交易時，可能被別人從中擷取你的帳號及密碼了，進而用你的信用卡直接在線上交易，因為網上所做的安全機制是防止個人的資料外洩，並不能預防帳號或密碼在傳輸時不被攔截呀，所以這正是將來要研究發展的方向。

第四節　新認證流程

【新認證流程－以信用卡為例】

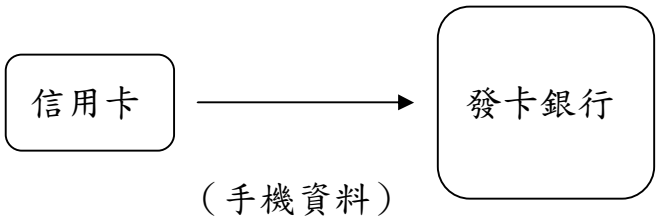


圖 8 簡易新認證流程圖

上列意思是指在申辦信用卡的同時要有當事人的手機號碼，方便在刷卡同時確認身分，預防他人盜刷信用卡。並且以手機傳訊方

式傳達給予信用卡持有人，等認證中心確認身份後交易就算完成。這就是我們認為未來可行且更安全的認證方式。

【當消費者在網路上消費時之流程】

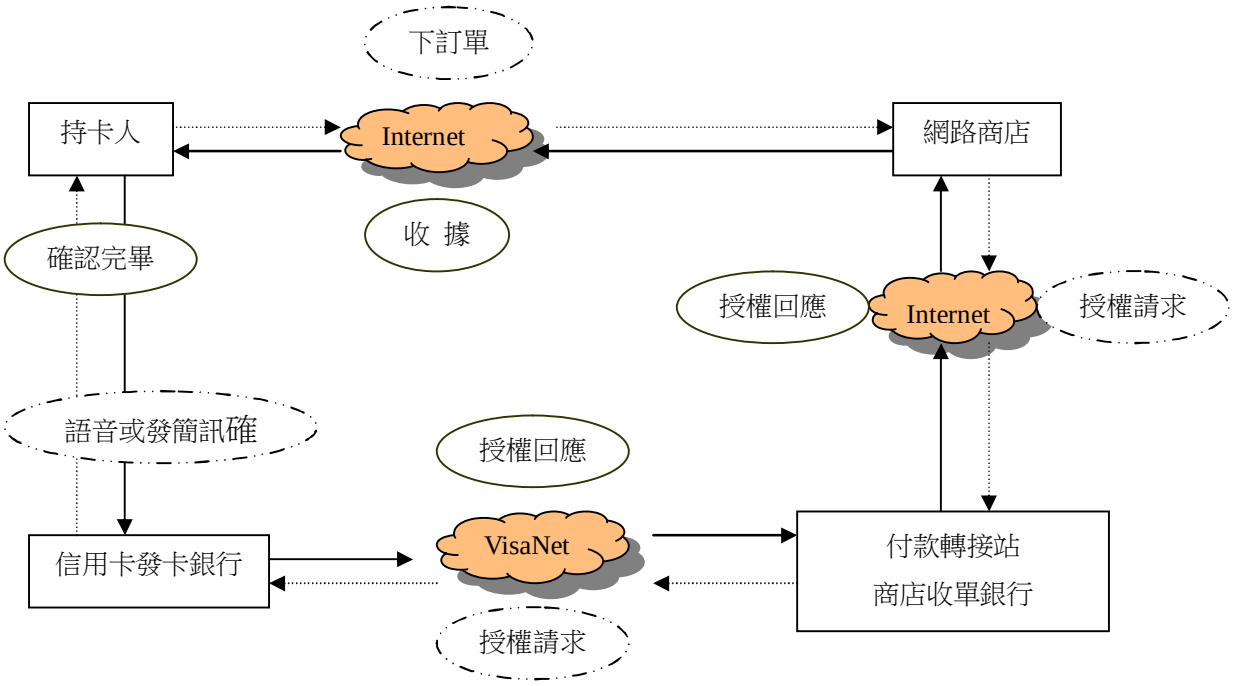


圖 9 新認證流程圖

以上的流程多了一項用手機確認身份的方式，以確保消費者的權益，因為網上訂購並不安全，因為別人要是知道你的卡號及密碼，那就能夠擅自利用你的名義下單了，而經過我們研究討論後，發現可以運用手機來做確認的動作防止別人冒用，因為 SET 或 SSL 他們只是防止資料不外洩，而並無核對身分此功能，所以在此加強。

第五章 結論

第一節 研究發現

經過本次專題研究，讓我們發現隨著科技文明的進步，電腦、通訊及其他結合電子智慧的科技產品與人類的食、衣、住、行緊扣在一起。付款系統隨著商業交易行為之演進而蛻變，也就是說，款項給付為交易行為重要之因素，款項給付完成之後，整個商業交易行為方為完成。

雖有安全機制的規範，但那只能保護資料不外流，並無法保證他人之冒用。所以我們在這個研究報告中發現有這項缺失故提出探討，且現在犯罪率節節上升，咱們更要做好防範措施避免不必要的困擾，因為現在人只會鑽漏洞，不管科技如何進步還是有人會突破，故要有事先的準備及防範才能降低損失。

第二節 未來展望

我們在未來的展望中，希望能夠確實地防止信用卡不被盜刷或冒用。現在手機越來越多人使用，而 WAP 也漸漸盛行，所以可以運用 WAP 的上網功能來做下單確認工作，降低傳輸時間的浪費。雖然現在還沒有業者這麼做，但相信不久的將來會有這樣的功能出現，讓消費者更願意上網購物，這也是我們最期待的發展趨勢。

參考文獻

1.中文部份

1. 尹章華、潘秀菊、馮震宇、陳連順，「商事法入門」，月旦出版社，1993 年 9 月。
2. 林建宏，「網路安全與電子交易」，工研院電通所系統技術部，資訊安全通訊第五卷第二期，1999 年 3 月。
3. 邱筱雅，「電子商務中的付款機制-研究文獻回顧與評述」，交通大學資訊管理研究所未出版碩士學位論文，1997 年 6 月。
4. 璠，謝清佳，「資訊管理-理論與實務」，智勝文化事業有限公司，2000 年 5 月。
5. 周冠中，郭美懿，蘇筱媛，「電子商務挑戰 N 世代商機」，博碩出版社，1999 年 12 月。
6. 黃景彰、薛夙珍、李鐘斌、秋筱雅，「電子支付系統的分類與實例」，資訊安全通訊第五卷第二期，1999 年 3 月。
7. 黃梓峰，「以仲介者為基礎之彈性化電子商務架構」，交大資訊管理研究所未出版碩士學位論文，1998 年 6 月。
8. 郭玉群，「電子市場中消費者與其他參與角色互動模式之探

討」，國立交通大學傳播研究所未出版碩士學位論文，1997 年 6 月。

9. 張勝富，「網際網路電子交易系統之分析與設計」，成大工業管理科學研究所未出版碩士學位論文，1998 年 6 月。

10. 葉慈章，黃景彰，「網際網路上的小額支付系統」，資訊安全通訊第五卷第二期 ,1999 年 3 月。

11. 經濟部技術處，「中華民國八十八年網際網路年鑑」，1999 年 6 月初版。

12. 經濟部商業司，「電子商務發展觀察與展望」，電子商務導航第二期，1998 年 11 月。

13. 經濟部商業司，「從 e-Commerce 到 e-Business」，電子商務導航第六期，2000 年 1 月。

14. 廖彗如，蔡靜芬，蔡國裕，「數位付款與澳洲電子付款演講紀要」，資訊安全通訊第五卷第二期，台灣科技大學資管系，1999 年 12 月。

15. 薛夙珍，「電子商務付款系統之研究」，交通大學資訊管理研究所未出版博士學位論文，1998 年 6 月。

16. 網際網路商業應用計畫，「電子商務市場與趨勢篇」，經濟部商

業司電子商業協盟 ，1999 年 2 月。

17. 網際網路商業應用計畫，「電子商務市場與趨勢篇」，經濟部商業司電子商業協盟 ，1998 年 2 月。

18. 網際網路商業應用計畫，「電子商業答客問手冊-資訊技術常見問題及解答」，經濟部商業司與資策會，1999 年 1 月，網址：www.org.tw/faq/index, 2000 年 3 月 20 日。

19. 嚴紀中，陳鴻基，「管理資訊系統—理論、科技、實務與應用」，松崗電腦圖書資料股份有限公司，1999 年 8 月。

20. 蕭清，「中國古代貨幣思想史」，台灣商務，1992 年。

2.中文翻譯

1. Shapiro, Carl and Hal R. Varian, “Information Roles”，張美惠譯，1999，「資訊經營法則」，時報文化出版社。
2. Garfinkel, Simson and Gene Spafford, “Web Security and Commerce”，李國熙、陳永旺譯，1999，「電子商務與網路安全」，美商歐萊禮台灣分公司。
3. Weatherford, Jack, “The History of Money-from Sandstone to Cyberspace”，楊月蓀譯，1998，「金錢簡史」，商周出版社。
4. Treese, G. Winfield and Lawrence C. Stewart, “Designing System forInternet Commerce”，黃彥憲譯，1999，「系統設計 DIY-電子商務系統設計實務」，跨世紀電子商務出版社。

3.網站資料

1. SET 相關網站

(1). SET 服務提供者 First Virtual Holding Company，網址：www.fv.com(1999 年 12 月 5 日) 。

(2). SET 服務提供者 Cybercash Company，網址：www.cybercash.com(1999 年 12 月 5 日)。

(3). 台灣威士卡，網址：www.visa.com.tw(1999 年 11 月 25 日)。

(4). 國際 MasterCard 信用卡組織，網址：www.mastercard.com(1999 年 11 月 25 日)。

(5). 台灣 SET 先導計畫組織，網址：www.set.com.tw(2000 年 1 月 5 日)。

2. 電子現金(e-Cash)

(1). 數位現金發行組織，網址：www.digicash.com(1999 年 12 月 3 日)。

(2). 英國 Mondex 智慧卡系統，網址：www.mondex.com(1999 年 12 月 3 日)。

3. 其他

(1). 行政院研考會，「政府憑證管理中心(GCA) 」，網址：

www.pki.gov.tw(2000 年 2 月 5 日)。

(2). 台灣網路認證公司，網址：www.ca.fisc.org.tw(2000 年 2 月 5 日)。

(3). 財團法人聯合信用卡處理中心，網址：www.nccc.com.tw(1999 年 12 月 5 日)。

(4). 財政部金融局，網址：www.boma.gov.tw/index.htm(2000 年 3 月 5 日)。

(5). 財金資訊公司，網址：www.fisc.com.tw(2000 年 2 月 10 日)。

(6). 資策會網路安全認證服務中心，網址：www.mic.iii.org.tw(2000 年 3 月 6 日)。

(7). 資策會市場情報中心，網址：www.mic.iii.org.tw(2000 年 3 月 5 日)。

(8). 經濟部網際網路商業應用計畫，網址：www.ec.org.tw/default.asp(1999 年 11 月 24 日)。

(9). 網際網路資訊情報中心，網址：www.find.org.tw/home.asp(2000 年 3 月 24 日)。

(10). 郵政儲金匯業局，網址：www.prsb.gov.tw(2000 年 4 月 5 日)。

(11). 聯合信用卡處理中心，網址：www.nccc.com.tw(2000 年 3 月 20 日)。

(12). 美國聯邦貿易委員會(FTC, Federal Trade Commission, 1997 年)，網址 ： www.ftc.gov/bcp/coline/pubs/credit/card.htm(2000 年 6 月 19 日)。

附錄一　專題製作會議記錄

專題製作第一次會議記錄

時間：89 年 9 月 20 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：無 (尚未決定)

目前進度：蒐集相關線上交易之資料

下次預定進度：訂立專題題目

指導老師建議： 要廣泛的蒐集資料，方便製訂題目。

專題製作第二次會議記錄

時間：89 年 9 月 27 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：蒐集資料

下次預定進度：先勾勒出大綱

指導老師建議：蒐集有關線上交易之探討與研究的資料並整合

專題製作第三次會議記錄

時間：89 年 10 月 4 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：專題大綱雛型已可

下次預定進度：將文獻資料做個整合

指導老師建議：文獻資料內容要完整最好有個架構出來

專題製作第四次會議記錄

時間：89 年 10 月 11 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：撰寫文獻探討的內容

下次預定進度：計劃書的撰寫

指導老師建議：計劃書的撰寫要完整內容須加強

專題製作第五次會議記錄

時間：89 年 10 月 18 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上研究之探討與研究

目前進度：撰寫計劃書

下次預定進度：將計劃書修飾的更完整

指導老師建議：計劃書內應放重點的大要即可，方便口試報告。

專題製作第六次會議記錄

時間：89 年 10 月 24 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：計劃書的訂正與修飾

下次預定進度：討論書面審查的口試部份

指導老師建議：書面審查及口試快到了要努力呦！

專題製作第七次會議記錄

時間：89 年 11 月 8 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：計劃書已完稿、正在製作計劃書的 PowerPoint

下次預定進度：探討書面審查的內容

指導老師建議：製作 PowerPoint 重點提出就好

專題製作第八次會議記錄

時間：89 年 11 月 15 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：PowerPoint 已製作完成、準備上台演練

下次預定進度： 上台報告

指導老師建議： 進度許可，希望能加緊腳步。

專題製作第九次會議記錄

時間：89 年 11 月 29 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：1.已完成期初口試

2.研究架構及內容的探討

3.加強蒐集資料

下次預定進度：確定架構內容

指導老師建議：資料要多方面蒐集，不然內容過少。

專題製作第十次會議記錄

時間：89 年 12 月 6 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：研究架構之編寫

下次預定進度：將主要架構完成

指導老師建議：對於架構有不懂之處要提出，避免有出入。

專題製作第十一次會議記錄

時間：89 年 2 月 21 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：研究架構已完成

下次預定進度：自己發展交易新流程

指導老師建議：多方面研究新流程的架構

專題製作第十二次會議記錄

時間：89 年 2 月 27 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：新流程已經有雛型了

下次預定進度：完成新流程

指導老師建議：可多參考其他流程，加強新流程的功能。

專題製作第十三次會議記錄

時間：89 年 3 月 7 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：1.新流程已完成，正進行內容的排版。

2.第二次口試報告的準備

下次預定進度：能將初稿完成

指導老師建議：雖然已經做的差不多，但些許部分能要增加。

專題製作第十四次會議記錄

時間：89 年 3 月 21 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：撰寫書面內容

下次預定進度：撰寫安全機制的分野

指導老師建議：將零星的資料的整合完整

專題製作第十五會議記錄

時間：89 年 4 月 24 日

地點：資管科圖書館

組別：第 18 組

組員：石佳敏、趙珮芬、張珮綺、蔡佳伶

題目：線上交易之探討與研究

目前進度：已將安全機制的差異分別出來了

下次預定進度：專題撰寫完成

指導老師建議：專題的製作已接近尾聲，希望各組員繼續加緊腳步將成品完成。恭喜妳們能順利畢業！！

附錄二　甘特圖

	月次								
預定項目	9 月	10 月	11 月	12 月	1 月	2 月	3 月	4 月	5 月
研習相關主題									
收集文獻資料									
訂立專題題目									
訂立專題大綱									
整合文獻資料									
撰寫計劃書內容									
撰寫第二章									
撰寫第三章									
確定研究架構									
收集相關流程									
討論線上交易的難處									
安全機制的差異									
探討觀念性架構及新流程									
撰寫第四章									
撰寫第五章(結論)									
修改和準備期未口試									
排版和內容最後修改並定裝訂									

附錄三　需求環境

軟體方面

Microsoft Word

Microsoft Excel

Microsoft Power Point

硬體方面

IBM	15.3 硬碟
音效卡	一般相容之音效卡
光碟機	32X CD-ROM
數據機	56Ｋ數據機
掃瞄器	Plug-N-Scan 1200 CU
印表機	EPSON Color 670
螢幕	View Sonic G653
鍵盤	BTC 8113
滑鼠	羅特　Logitech 旋豹
記憶體	64MB