線上信用卡付款：技術發展的回顧與評估

薛夙珍 黃景彰
交通大學資訊管理研究所

摘 要

在 Internet 線上使用信用卡付款，於提供信用卡付款資訊之後，眞正的貨款轉移及隨後的銀行間清算，是以現有信用卡付款的組織體系爲基礎。此類系統較易與現行的體系整合，故發展的速度較快，所以我們預期它是各種電子支付協定中，是最廣爲社會所接受的方式。這一篇文章回顧了最近幾年來 Internet 線上信用卡付款系統技術的發展；我們回顧了以卡號加解密爲主的「傳輸加密 (channel encryption)」方式、IBM 蘇黎士實驗室的 iKP 協定 (Internet Keyed Payment Protocol)、提供「持卡人證書 (cardholder certificate)」作爲個體識別的 SET、與以「信用卡證書 (credit card certificate)」取代「持卡人證書」的 Revised SET、匿名信用卡協定五種方法。經過對各種線上信用卡付款系統詳細的分析與討論，我們知道由於在設計上對交易個體間彼此信任關係的基本假設不同，各種協定採行了不同的安全保障方法，也因此有了不同程度的隱私保護。最後，我們也預測未來的發展趨勢。

關鍵詞：線上付款、信用卡、安全、隱私權、電子證書

On-line Payment by Credit Card : A Review and an Assessment of the State-of-the-Art Technology

Sue-Chen Hsueh Jing-Jang Hwang
Institute of Information Management
National Chiao-Tung University

Abstract

It is anticipated that on-line payment by credit card will be quickly accepted by electronic payment protocols. Fund transfers and clearings that follow the transmission of information about payment by credit card over the Internet are based on the current credit card payment infrastructure. Due to easy integration with current banking systems, on-line payment systems using credit cards have been quickly developed. This paper reviews

several techniques that facilitate on-line payment by credit card over the Internet. Included are the "channel encryption" method that relies on the encryption of credit card numbers; Internet Keyed Payment (iKP) protocol developed by IBM Laboratory at Zurich; SET that provides "cardholder certificate" as individual identity; revised SET that substitutes "cardholder certificate" by "credit card certificate"; and anonymous credit card protocols. The distinct protocols make different assumptions about trust between transaction parties, and apply diversified security protection mechanisms. As a result, they induce different degrees of privacy protection. Future trends of this technology are also predicted.

Keywords: On-line Payment, Credit Card, Security, Privacy, Digital Certificate

壹、簡介

網際網路 (Internet) 的蓬勃發展，提供了一種新形態的商業環境，形成了電子商務 (electronic commerce)。網路上的電子商務，由於買賣雙方並不是直接面對面進行交易，有關交易過程所衍生的安全問題格外重要；尤其是牽涉到資金移轉的付款時，對於安全的要求更需嚴謹。如果交易的安全受到了質疑，便無法營造買賣雙方互相信賴的環境，電子商務也就不可能成功地發展。

以信用卡付費是目前相當普遍的付款習慣，如果可以將原有的支付方式修改以適合網際網路的交易環境，預估將比其他支付工具更容易被大衆接受。因此線上信用卡付款有可能成爲最主要的電子式支付方式。

在本篇文章中，我們首先對各種不同支付工具的付款系統作一簡單的分析，說明線上信用卡付款系統最具發展潛力的理由。其次，我們回顧各種線上信用卡付款系統，並且分析比較幾個主要的線上信用卡付款協定。然後，我們探討其基本假設之異同，評估其發展的限制，並展望未來的發展趨勢。

貳、主要的電子支付系統

依據所使用付款工具的不同，電子支付系統 (electronic payment system) 大致可分爲線上信用卡付款 (on-line payment by credit card)、電子現金 (digital cash) 形式、以及借貸模式 (debit-credit model) 的電子支票 (electronic cheque) 三類 (Neuman 1995)。以電子現金來說，它提供的付款工具，乃是模擬一般傳統現金的方式，其理論基礎是根據 1982 年 David Chaum 所提出的盲目數位簽章 (blind digital signature) (Chaum 1983 ; Chaum et. al. 1990)；它是以一串數字代表一筆現金，利用密碼機制，使其具有一般現金的不易僞造及匿名的特色，而且是安全、可分割、可交換與可儲存的 (Okamoto & Ohta 1992)。爲了防止重覆使用，電子現金發行單位必須維護一個大型資料庫，以提供線上檢查，或是採用無法開啓的裝置 (tamper-resistant device) 來進行離線式 (off-line) 的重複使用查核；無論是線上檢查所需的資料庫之維持，或是離線查核所必須的額外裝置，都需要付出不成比例的成本。另外，雖然電子現金具有匿名的特性，但也因而沒有了可追蹤的記錄，有可能成爲洗錢與電腦犯罪的工具；就流通的需要而言，也還沒有完備的清算體系。雖然歐美已有若干實驗性的或小規模使用的系統 (Okamoto & Ohta 1992 ; Chaum 1983 ; Chaum et. al. 1990)，但大部份的金融單位與消費者均處於觀望階段，這種新式的支付工具是否有可能成爲法定貨幣 (legal tender) 仍是值得存疑的，未來發展仍然有待觀察。

第二種以電子支票爲基礎的電子付款系統，實際上是現有銀行紙張支票體系的網際網路化。電子支票可以取代傳統的支票，此種支票上的簽章或背書一般是使用數位簽章技術來取代筆或印鑑的簽章方式，以簽章卡 (signature card) 來執行；紙張的支票簿則是利用電子支票簿 (electronic checkbooks) 來代替 (Doggest 1995)。付款系統本身必須提供身份驗證、數位簽章以及安全通訊傳輸的功能，其中數位簽章的執行一般需配合智慧卡形式的簽章卡，以妥善保護簽章所使用的私密金鑰，並利用讀卡機輔助計算及資料傳輸。雖然電子支票的作業是模仿現行支票的運作，但簽發支票所涉及的法律規定甚多，且在金融法規的規定裡對開立支票帳戶有一定的限制，也因此限制了網路上電子支票的

使用範圍。我們認爲，電子支票付款系統的發展必須先建立合宜的法制環境，是否可以將現有的票據法（鄭玉波 1995）及一般的商業慣例延伸於網路環境中，或是需要另行立法等，仍是有待深入研究的議題。

至於以信用卡在網際網路上付款，則只是傳統信用卡付款方式的一個延伸應用，類似於利用信用卡郵購付款或電視購物。我們認爲在三種不同類型的線上付款方式中，信用卡付款比較容易被市場所接受。對於接受信用卡的商店而言，因爲有信用卡發卡組織代爲查詢付款信用，以及原有完善的銀行之間的清算體系，他們無需特別顧慮網路交易可能無法取得貨款的風險。雖然以信用卡爲基礎的電子付款系統，消費者必須申請信用卡，而商店必須申請成爲信用卡組織的特約商店，但因信用卡的普及，事實上已經有遍佈世界各地的使用者與特約商店。我們可以說利用信用卡的線上付款，已經有廣大的顧客基礎，以及完備的組織運作體系（infrastructure）。我們所欠缺的是交易安全的保証以及消費者的隱私保護，而安全與隱私可以仰賴密碼技術（cryptography）來達成。

線上信用卡付款系統，在本質上不同於電子現金或電子支票，後二者是攜帶價值的有價証券，不過是以數位化的方式來儲存價值而已；因爲本身是有價的，電子現金及電子支票的使用似乎較難延用現有的法律規範。不同的，線上使用信用卡所需的法制環境或商業習慣可以自郵購商業移植而來，不必要另行立法或建立全新的商業契約模式。所以，我們預期在各種電子支付協定中，線上信用卡付款將是最容易被社會所接受的方式。

參、線上信用卡付款

顧客使用信用卡在線上付款時，只要輸入其卡號及有效期限，透過網際網路傳送至進行交易的商店，商店再將該資料傳送至往來的信用卡收單銀行請求交易授權；如果經過許可，商店便可循原有信用卡的銀行體系間的往來取得貨款。因此利用以信用卡爲基礎的電子付款系統來進行支付時，消費者必須至發卡機構申請合法的信用卡，網路上的廠商必須與發卡機構簽約成爲特約商店，提供能夠收受顧客信用卡支付的伺服器系統（service server）；而電子付款系統本身必須能夠確保客戶資料、信用卡號碼、交易內容等具有個人隱私性質的資料在網際網路上傳輸過程的安全。

線上信用卡付款系統內參與的個體包括持卡人（cardholder）、發卡銀行（issuer）、收單銀行（acquirer）、特約商店（merchant）。持卡人是擁有發卡銀行發給信用卡的人，透過網際網路以信用卡在特約商店購買商品或服務。特約商店則是向信用卡發卡組織提出申請提供銷售商品或服務的企業組織，與發卡組織約定可接受消費者以信用卡作爲線上交易付款的方式，並透過收單銀行取得持卡人付款。收單銀行則負責爲特約商店查詢交易授權，及協助特約商店取得貨款，進行收取信用卡交易付款的業務。發卡銀行則是根據各種授權規定來發行信用卡，授權的內容包含有對持卡人的身份辨識、信用卡的有效期限、以及信用額度等，且發卡銀行必須負責寄發帳單予持卡人，並從持卡人取回交易的款項。線上信用卡付款系統的基本系統概念如圖 1 所示（Janson & Waidner 1995）。

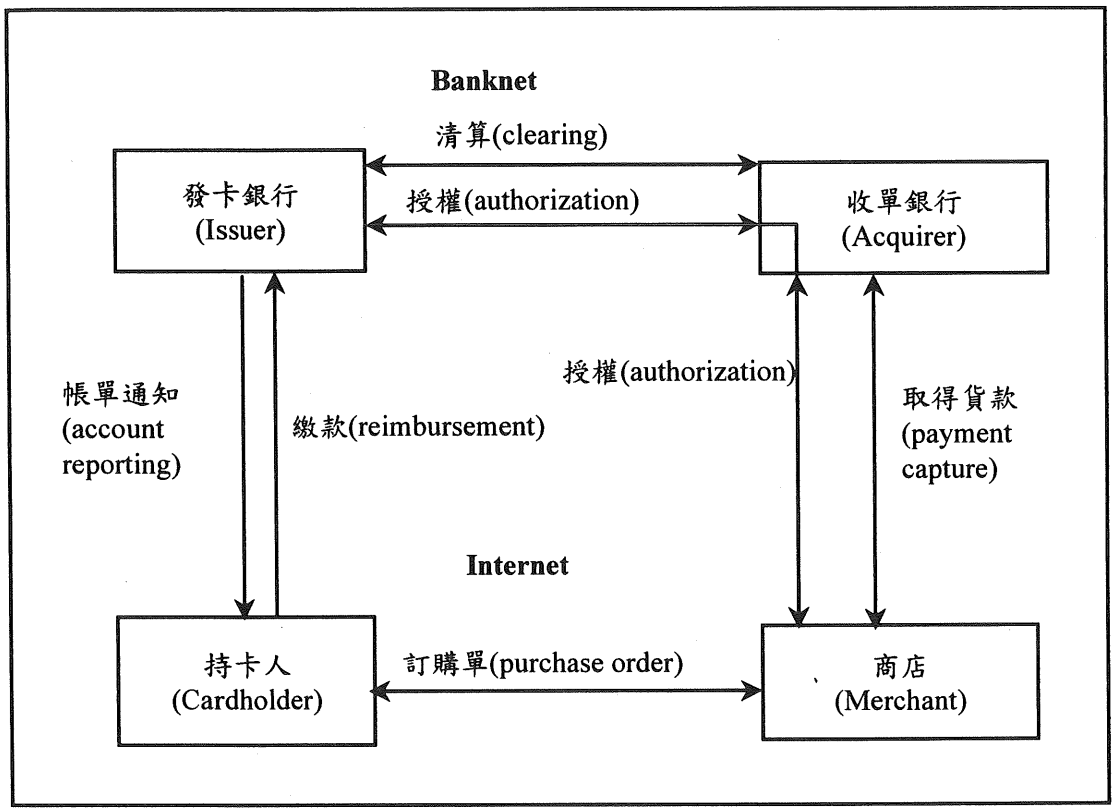


圖1：線上信用卡付款系統之系統概念圖

線上信用卡付款系統的安全需求相當的嚴謹，如何提供一個安全而方便的使用方式，是重要的研究課題。現行的各種線上信用卡付款協定可依技術發展及安全程度的不同分成對卡號加解密爲主的「傳輸加密 (channel encryption) 」方式與提供「證書 (certificate) 」作爲個體識別的 SET(Secure Electronic Transaction) 兩大類。其中廣被討論的 SET 規格值得詳細的說明其發展過程與設計理念，並分析其優缺點。除此之外，本文作者曾提出了 SET 之修訂協定 (Hwang & Hsueh 1998)，在此稱爲 Revised SET 。Revised SET 對線上購物者隱私權作了更宏觀的思考，它將 SET 的個體識別證書之一的「持卡人證書 (cardholder certificate) 」以「信用卡證書 (credit card certificate) 」取代之。另外也有學者設計了以公正的第三者銀行提供匿名帳戶爲基礎的線上信用卡付款機制。

以下各節將分別論述上述五種信用卡付款技術。然後，我們將比較討論五種技術所提供的隱私保護。

肆、傳輸加密的方法

傳輸加密 (channel encryption) 是最早被引進於 WWW 的付款方式；這種方式採較簡單的作法，透過對交易資訊在傳輸過程予以加密，來符合基本的安全需求。在以信用卡爲支付工具的交易過程中，對持卡人的識別，仍依據傳統的信用卡號碼。爲避免卡號在網路傳輸時被竊取或竄改，持卡人使用 WWW 環境的通訊安全協定，如 S-HTTP 或 SSL ，利用這些協定所提供的安全機制，先以非對稱金鑰密

碼法 (asymmetric cryptography) 取得通訊金鑰 (session key)，再以該通訊金鑰對信用卡號碼進行加密後再傳送，因此僅有商店以及提供收款處理服務的收單銀行或其代理人可以讀取卡號。

SSL(Secure Sockets Layer Protocol，簡稱 SSL) 及 S-HTTP(Secure HyperText Transfer Protocol，簡稱 S-HTTP) 是適用於 WWW 環境的兩個主要的通訊安全協定，使往來的商業交易訊息在通訊時能夠達到基本的安全需求。這二個協定提供了端點系統的識別、秘密通訊、資料完整性與訊息發送來源的確認等服務。

SSL 協定由 Netscape 公司在 1994 年 10 月提出，它使用對稱式密碼系統，例如傳統的 DES 或 RSA Data Security 公司發展的 RC4 等，對網路中傳遞的訊息進行加密處理，以確保傳輸資料的私密性。另外 SSL 還使用非對稱式密碼系統，例如 RSA 公開金匙演算法，並結合 X.509 的電子證書，以識別交易雙方的身份。在 SSL 協定中，伺服端的身份必須經過驗證的，用戶端則可由伺服端自行決定是否加以驗證；傳輸的訊息則透過安全的赫序函數，例如 MD-5 或 SHA 等，計算產生訊息驗證碼 (message authentication code，簡稱 MAC)，來檢查訊息的完整性。

EIT(Enterprise Integration Technologies) 公司在 1994 年 7 月提出 S-HTTP，它是一種以文件爲處理單元的安全管制方法，用以提供 WWW 分散式環境中的用戶端與伺服端在進行文件交換時所需的安全服務。S-HTTP 針對 HTTP 所傳輸的文件內容直接增加安全性的功能，所提供的安全服務包括交易訊息的私密性、完整性的保護，以及可驗證訊息來源的功能。S-HTTP 安全機制的運作主要由數位簽章、完整性的驗證和加密三個技術來達成，另外還提供了一種簡單的盤問 / 回應 (challenge/response) 的機制，讓交易雙方能夠確定交易是新產生的，而非被複製或僞造的訊息。S-HTTP 以對稱式密碼系統加密傳輸資料，使用訊息驗證碼 (MAC) 來查證訊息的完整性，也使用公開金鑰密碼技術來對訊息的發送來源進行身份的識別。另外，S-HTTP 提供數位簽章的功能，一旦發送方使用了數位簽章功能對訊息進行簽章，則有關發送方身份的證書資料 (certificate) 或一個可提供證書來源驗證的證書串列 (certificate chain) 便會附在訊息後面，讓接收方可以根據證書內的公開金鑰或證書串列上一系列的公開金鑰來檢查發送方簽章的正確性。S-HTTP 不要求用戶端的公開金鑰證書 (public-key certificates) 來支援對稱式通訊金鑰的交換，也就是說個別的用戶不需要建立一個公開金鑰，亦不需要在特定的證書管理體系下，便能夠利用 S-HTTP 在 WWW 上與特定的伺服端進行安全通訊。S-HTTP 對所使用的密碼演算法、通訊方式和其參數提供相當大的彈性，可依需要作不同的選擇。

CyberCash、Netscape 的商業伺服器 (commerce server) 以及 Secure Mosaic 是採行這種傳輸加密作法的典型例子。但這些採用 SSL 與 S-HTTP 協定的 WWW 相關應用系統，都是屬於美國公司所發展的系統，由於牽涉到美國政府所管制的密碼技術，必須接受美國出口管制法的限制，因此不是禁止出口，就是外銷的系統所使用的密碼機制必須受到限制。其中採用 S-HTTP 的 Secure NCSA Mosaic 系統僅供美國境內使用；採用 SSL 協定的 Netscape 商業伺服器系統則是分成美國國內版與國際版 (Netscape 1995；Hickman & Elgamal 1995；NCSA 1995；Rescorla & Schiffman 1994)。美國國內版遵循了 SSL 協定完整的設計，可視需要選擇安全程度較強的演算法，或是長度較長的金鑰 (最長爲 128 bits)；而美國境

外所使用的國際版不但加密演算法受限，且金鑰長度限制爲 40 bits 。這兩個版本在安全程度上相差甚多。

伍、IBM的iKP協定

IBM 蘇黎士實驗室設計了一系列的付款協定-iKP (Internet Keyed Payment Protocol)，透過使用公開金鑰密碼法(public-key cryptography)，來保障線上交易的安全。此系列協定(a family of protocols)是最早使用公開金鑰電子證書並以現行金融體系爲基礎的付款協定，往後許多電子支付均參考它作爲發展的基礎。

iKP 使用現存的金融體系中的清算與授權系統，設計了在網路上持卡人與商店之間的信用卡交易協定。iKP 因爲考慮不同程度的識別需求與金鑰管理的複雜度，且允許漸進的使用 iKP 系統，因此以擁有公開金鑰證書的個體種類之數目不同來區分複雜等級，其中 iKP 的 i 即代表擁有公開金鑰證書的個體種類數目。1KP 提供了最基本的個體識別，只有收單銀行在系統中的代理者(agent)，即所謂的通訊閘道(acquirer gateway)，才有公開金鑰電子證書；交易的參與者經由檢查該證書而信任收款者的伺服器，但 1KP 對於持卡人與商店並不提供證書，商店對持卡人的個體識別仍依據信用卡卡號。在 2KP 中，則除了代表收單銀行的通訊閘道外，商店也有公開金鑰電子證書，因此對商店所發出的訊息也提供了電子簽章的驗證，持卡人不需與第三單位連線接觸，即可透過證書來驗證商店的身份。至於 3KP ，則每一個參與個體包括代表收單銀行的通訊閘道、商店、持卡人，均擁有公開金鑰，故此種系統可提供多個體的識別、及所有訊息的來源確認的服務。

iKP 使用了公開金鑰密碼技術，擁有公開金鑰的參與個體，必須向可信賴的第三者(Trusted Third Party)申請提供身份識別所需的公開金鑰電子證書。iKP 採行 ITU (International Telecommunication Union)與國際標準組織 ISO (International Standards Organizations) 所共同提出的 X.509 個體識別架構。X.509 建議採用 X.500 所規範的目錄驗證要點（ Directory Authentication Framework ），可用來管理、傳佈參與個體的公開金鑰證書，讓各個參與個體不需要儲存個別往來交易夥伴的公開金鑰，來簡化使用公開金鑰密碼法的程序，並加強金鑰之管理。

X.509 的運作主要是利用公正可信賴的電子證書管理機構(Certificate Authority ，簡稱 CA) 發給每個用戶證書。CA 對證書的內容作簽章，將證書中的公開金鑰與使用者的識別名稱結合在一起；驗證時，取證書上的公開金鑰來檢驗送來文件所附的簽章。X.509 中的電子證書的內容包括證書所有人的識別名稱、公開金鑰、有效期限、及電子證書管理機構的簽章等。

iKP 協定中使用可信賴的 CA 所簽證的“公開金鑰證書”以及數位簽章來作爲身份識別。發送方在要求與接收方開始交易時，必須將發送的訊息利用其私密金鑰加密成數位簽章後，隨著證書傳送給接收方。接收方收到後，取出發送方的證書，以 CA 的公開金鑰驗證證書上的 CA 簽章來檢驗證書是否是經過 CA 認證過的合法證書（註：假設CA的公開金鑰已可取得），然後取出證書中發送方的公開金鑰對發送方的簽章訊息進行驗證（見圖 2）。如此可達到辨識身份與檢驗訊息完整性等二項功能。

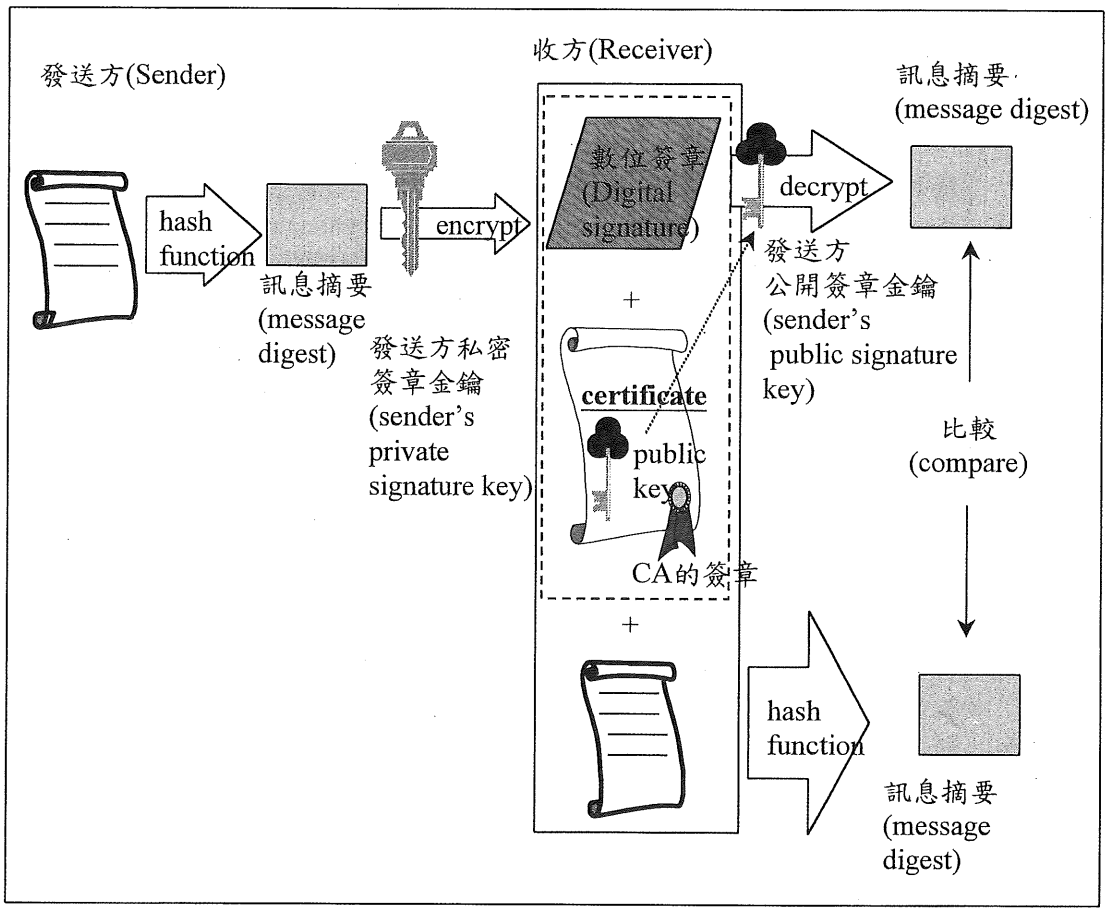


圖2：利用數位簽章的驗證來檢驗文件的來源及完整性

iKP 除了使用了公開金鑰密碼法的證書與數位簽章作爲身份識別外，爲免除持卡人將信用卡卡號直接揭露給商店之必要以及避免收單銀行取得交易商品的資訊，可用單向赫序函數的運算產生訊息摘要(message digest)，來隱匿信用卡卡號與交易商品的資訊。另外，爲了保障傳輸的安全，對部份隱私的資料，如帳號等，可使用收方的公開金鑰對傳送的訊息予以加密，在傳送予收方。

在 iKP 協定中每個參與個體擁有一對金鑰，對數位簽章與訊息私密性的保護都是使用公開金鑰密碼法。在作數位簽章時，發送方以自己的私密金鑰對訊息加密後產生簽章，收方在收到訊息後，以發送方的公開金鑰來驗證簽章。若欲保障交換訊息的私密性，在 iKP 協定中是以收方的公開金鑰對訊息加密，再傳送予收方；收方收到加密的訊息後以自己的私密金鑰將訊息解密。因此在 iKP 協定中，數位簽章與訊息的解密，是使用同一對金鑰中的私密金鑰。

iKP 的設計理念相當簡單，以 X.509 的電子證書作爲個體識別的基礎，由發卡銀行或可信賴的機構來核發證書。並且可針對實際上安全的需要選擇採行 1KP 、2KP 或 3KP ，在執行上相當有效率；因具有相當大擴充的彈性，在未來可視需求的改變進行擴充。

陸、使用持卡人證書作爲個體識別的SET

SET 協定所規範的是一種線上信用卡的付款系統，目前在網際網路上以這種系統的發展進度最爲快速。SET 協定的前身，分別是世界上最大的兩家國際性的信用卡發卡組織 Visa 和 MasterCard 在 1995 年九月與十一月分別提出的安全電子付款交易協定。Visa 和 Microsoft 公司聯合發展了 " 安全交易技術協定 "(Secure Transaction Technology Protocol ，簡稱 STT) (VISA 1995) ；MasterCard 則和 IBM 、 Netscape 、 GTE 及 Cybercash 等公司，以 iKP 爲基礎共同提出了 " 安全電子付款協定 "(Secure Electronic Payment Protocol ，簡稱 SEPP) (MasterCard, 1995; Visa & MasterCard, 1996) 。由於兩種協定所使用的安全機制相當接近，而且爲了與未來客戶終端系統相容起見， Visa 和 MasterCard 與 IBM 、 GTE 、 Microsoft 、 Netscape 、 SAIC 、 Terisa 、 Verisign 合作，在 1996 年 2 月 23 日提出一個結合 STT 與 SEPP 兩個協定的新付款協定 - SET 協定，並且預計在 1997 年進行測試 (Visa & MasterCard 1996) 。

參與 SET 的個體有持卡人、發卡銀行、商店、收單銀行、以及電子證書管理機構。下圖表示 SET 的系統概念 (Visa & MasterCard 1996) ：

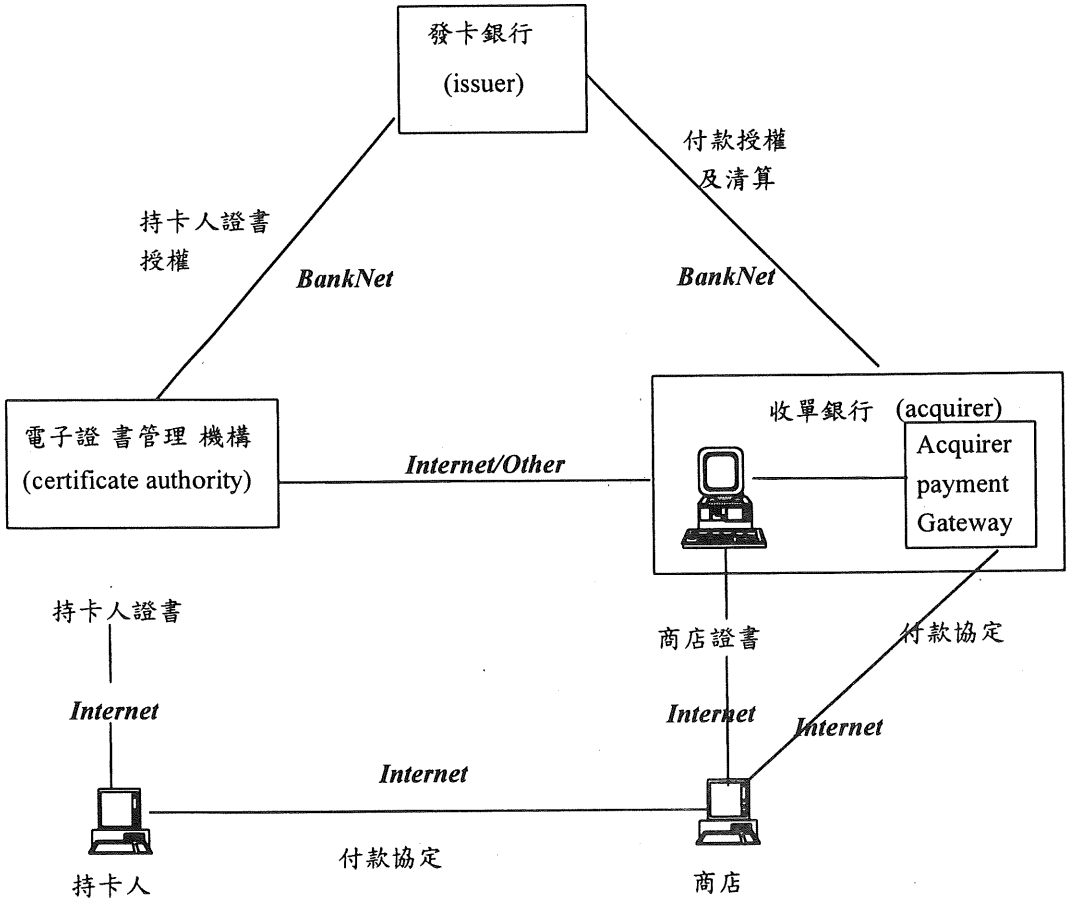


圖3：SET的系統概念圖 (Visa & MasterCard 1996)

SET 的安全機制，主要是運用密碼學的技術來保障交易的安全。首先在資料私密性的保護方面，SET 協定使用 " 數位信封 "(digital envelope) 的加密方式，來防止私密的資訊遭蓄意竊取或無意中揭露。其方式是發送方先使用對稱式金鑰密碼演算法 (例如 DES) 隨機產生一個 " 通訊金鑰 "，將欲保密的資料加密，再使用非對稱式金鑰密碼演算法 (例如 RSA) 以接收方的 " 金鑰交換公開金鑰 " (public key-exchange key) 對該通訊金鑰加密，然後將經該通訊金鑰加密後的資料，以及經接收方 " 金鑰交換公開金鑰 " 加密後的通訊金鑰一併傳送至接收方。接收方在收到後，首先使用自己的 " 金鑰交換私密金鑰 " (secret key-exchange key) 解密出通訊金鑰後，再利用該通訊金鑰進一步解密出被加密的資料。如此不僅可達成安全的金鑰交換，而且也能有效率傳遞私密資訊。

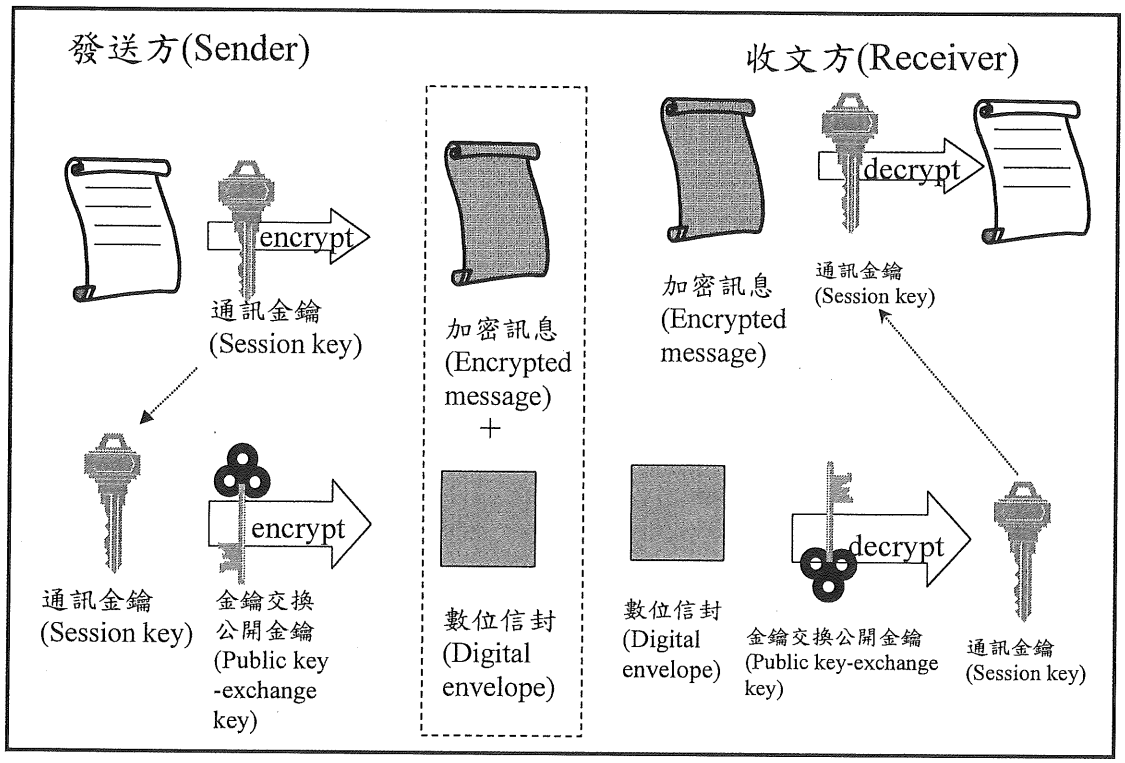
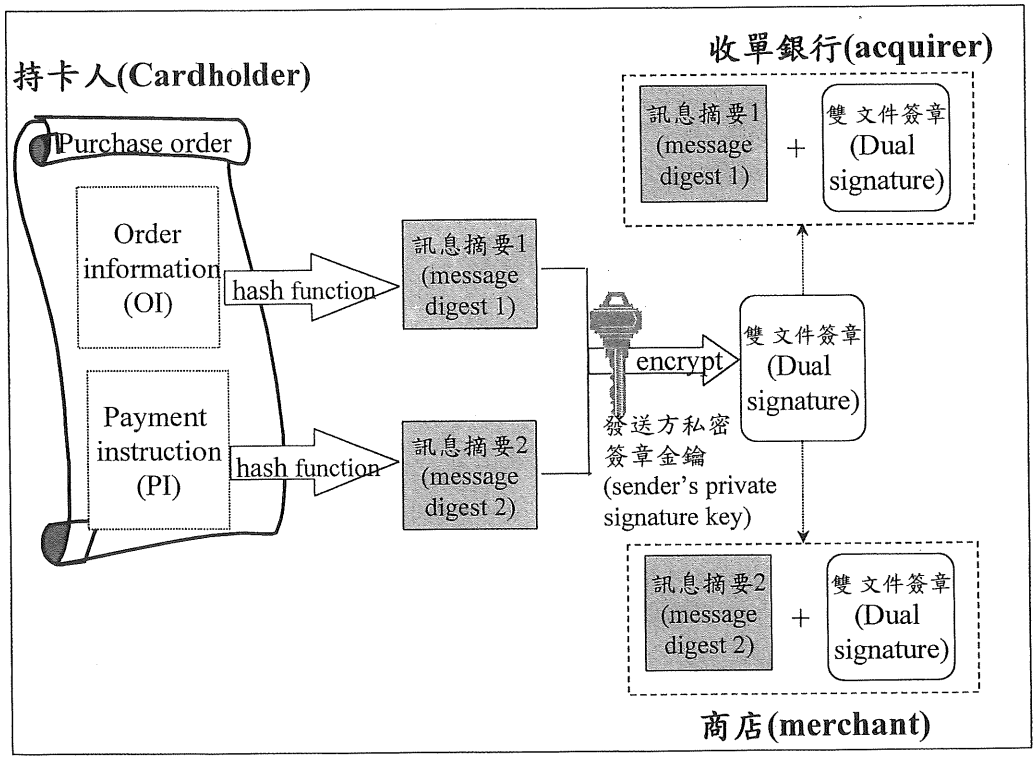


圖4：數位信封(digital envelope)示意圖

其次在提供資料完整性 (integrity) 檢驗的部份，SET 使用赫序函數 (hash function) 及數位簽章技術來達成。發送方將欲傳送的資料先以赫序函數產生一個訊息摘要，然後再將訊息摘要用發送方的 " 簽章用私密金鑰 " (private signature key) 加密產生數位簽章，以備接收方檢驗來源及資料完整性之需要。所傳送資料包含原始資料、演算法識別值 (Algorithm Identifier) 以及數位簽章，另外亦可包含發送方的公開金鑰證書，讓接收方可以從發送方的證書中取得驗證簽章用的公開金鑰。接收方驗證結果無誤，即可對該交易繼續進行處理。雖然 SET 與 iKP 協定都一樣是

使用赫序函數及數位簽章的技術來提供資料完整性的檢驗，但 iKP 協定中每個個體只有一對金鑰 (key pair)，SET 則設計了兩對金鑰。這二對金鑰中的一對是作爲產生與驗證數位簽章用，另一對則是作爲金鑰交換之用，用來加解密通訊金鑰，因此 SET 在作數位簽章時所使用的是 "簽章用" 的金鑰，所使用的證書也是簽章用的公開金鑰證書，與 iKP 協定不同。

在持卡人帳戶資訊隱私的保護方面，SET 協定使用了的一種數位簽章技術，稱爲雙文件簽章 (dual signature) 來達成。在信用卡付款交易的過程中，持卡人必須將訂單資料 (Order Information) 與付款指示 (Payment Instruction) 一起傳送給商店，商店收到後再將付款指示交給收單銀行申請付款授權。其中付款指示中包含了持卡人的帳戶資訊，如持卡人姓名、信用額度、信用卡有效期限等，這些資訊是持卡人的個人隱私，沒有必要對商店揭露，所以必須以收單銀行的公開金鑰加密，如此商店收到後亦不能得知付款指示的內容。然而付款指示與訂單資料是互相關連的，爲讓商店與收單銀行相信持卡人發出的訂單資料係配合了對應的付款指示，SET 以所謂雙文件簽章的應用來達成。雙文件簽章的處理方式是發送方將兩份文件分別使用赫序函數產生訊息摘要，將兩份文件的訊息摘要連結 (concatenate) 起來，以發送方的私密金鑰進行簽章，作爲兩份文件單一的雙文件簽章。兩份文件分別以不同接收者的金鑰加密後再傳送，並附上另一份文件的訊息摘要及雙文件簽章送到接收方，接收方收到上述資料後，以發送方的公開金鑰解出簽章，得到原始的連結訊息摘要，計算出自己可以取得的文件的訊息摘要及所附的另一份訊息摘要連結，與所收到的雙摘要連結互相比較後便可辨認該雙文件簽章是否正確。



SET 與 iKP 都是以使用公開密碼法爲主，但 SET 協定更結合了對稱密碼法 (symmetric cryptography) 與非對稱密碼法。SET 必須建立公開金鑰組織體系 (public-key infrastructure，簡稱 PKI)，使公開金鑰可以作爲個體識別及檢驗資料完整性之工具，並且利用公開金鑰密碼法來交換通訊金鑰。對於交換訊息的私密性，則使用對稱密碼法，以金鑰交換中所取得的通訊金鑰對訊息進行加解密。iKP 對訊息加密與數位簽章均使用公開密碼法，並且加密與簽章都使用同一對金鑰。由於使用公開密碼法對訊息的加解密，速度較爲緩慢，因此 iKP 僅在持卡人要送出帳號時，才以收單銀行的公開金鑰對帳號加密，其餘的資訊若須保持私密性，只以赫序函數保護。因此，iKP 在交換訊息加解密的速度上比較慢，在安全的保護的方面也不如 SET 的嚴謹。

SET 對個體識別，與 iKP 一樣採行 X.509 所規範的電子證書作爲識別基礎，證書的核發與管理的 CA，則建議採用如圖 6 的階層式組織體系。電子證書管理當局 CA 的功能在發行作爲身份辨識的證書，由信用卡發卡單位共同委派的公正組織，主要功能是提供產生、分配與管理所有持卡人、特約商店以及參與銀行所需的電子證書。CA 組織體系中每個層級的 CA 的證書必須經過上層 CA 的簽章認證，並且負責簽發下層的證書。最上層的「根電子證書管理機構 (Root Certificate Authority，簡稱 RCA)」，擁有唯一的 Root 私密金鑰，用以簽發其本身 (RCA) 與下一層依信用卡種類不同來區分的 BCA 級的證書。檢驗「根」CA 簽發的證書 (例如圖 6 的 BCA 的證書) 需要 Root 的公開金鑰；這個金鑰可以經由公開的、可信任的管道獲得，例如公開的新聞報導、Root CA 的公報或公開的刊物。根電子證書管理機構下一層的 Brand Certificate Authority(簡稱 BCA) 以信用卡的種類來區分，不同的信用卡發卡組織會建立不同的 BCA，例如，Visa 和 MasterCard 兩個發卡組織便可設立各自的 BCA。Geo-Political Certificate Authority(簡稱 GCA) 則是以地區或國家爲設立單位的機構，可視地區使用人數的多寡而決定是否成立或成立的個數。個體識別階層式組織體系中最主要的 CCA(Cardholder CA)、MCA(Merchant CA) 及 PCA(Acquirer Payment Gateway CA)，分別負責持卡人、特約商店與收單銀行通訊閘道的證書管理。

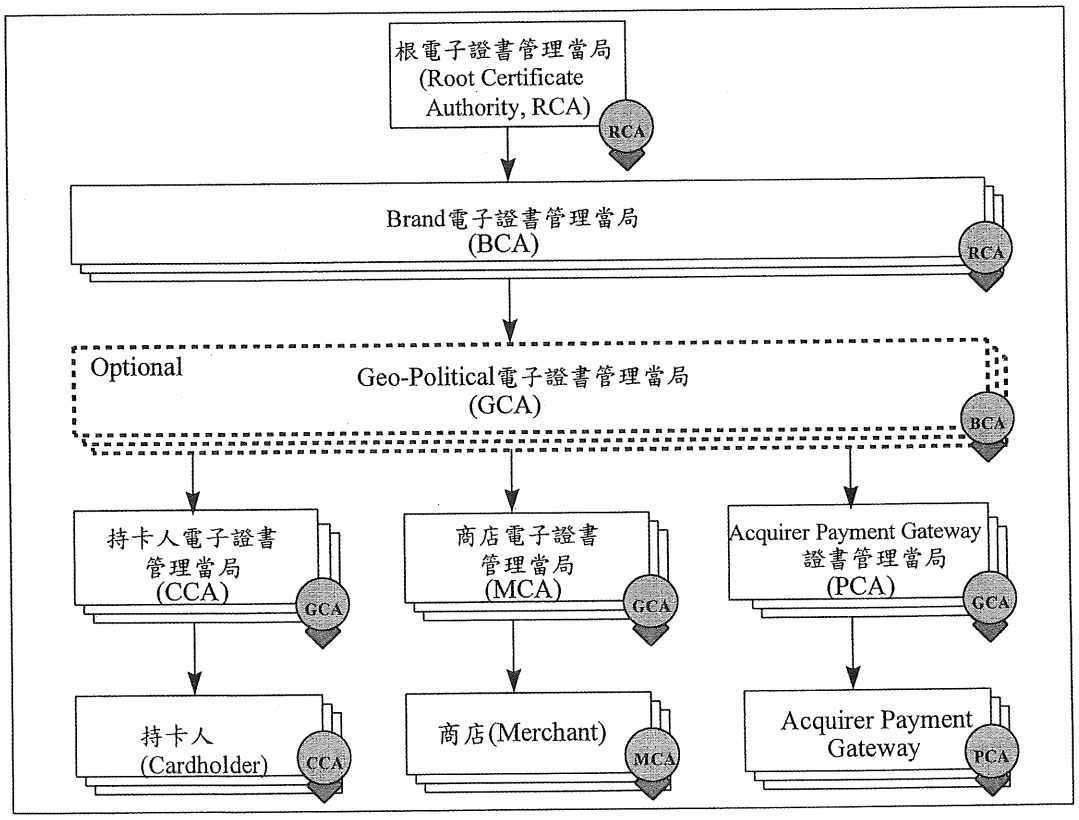


圖6：SET協定的證書管理系統概念圖 (Visa & MasterCard 1996)

SET 協定中所有參與的個體，在實際進行交易前都必須先自特定的 CA 申請電子證書。SET 所使用的電子證書包括“數位簽章所使用的公開金鑰證書”(public key certificate for digital signature) 與“金鑰交換公開金鑰證書”(public key-exchange key certificate)，二類各有不同用途的證書。“公開金鑰證書”中的公開金鑰是用來驗證發送方的數位簽章，而“金鑰交換公開金鑰證書”上的公開金鑰則是用以加密通訊金鑰，藉此來交換通訊金鑰。

SET 採行簽證管理系統 (Certificate Management System，簡稱 CMS) 負責證書的發行及管理，提供確實的公開金鑰證書給持卡人、特約商店、銀行以及 CA 等所有參與的個體。公開金鑰證書中主要包含了證書持有者的識別資訊以及一個公開金鑰，並經過上層可信賴 CA 的簽章認證後，才能成爲具有公信力的合法簽證。SET 協定中規劃了完整的證書管理體系，可將各地區的證書管理系統整合成完整的運作體系，讓消費者在世界各地都可以利用網際網路使用信用卡付款，並透過目前的連線清算機制便可完成帳務的處理。

SET 與 iKP 都使用了公開密碼法，也都一樣使用 X.509 所規範的電子證書作爲識別基礎，但 SET 比 iKP 協定更進一步強調公開金鑰組織體系的建立，建議 CA 採行階層式組織體系，並規劃了電子證書管理系統的功能。

SET 的設計是以符合安全上的基本需求爲目標，所提供的安全機制已能夠滿

足一個網際網路電子付款交易所需的資料保密性、資料完整性、識別交易個體身份、防止發送方拒絕負責等安全需求。它是目前最充分討論的協定，這個標準延伸至目前的信用卡付款體系，雖然，SET是否會成爲業界標準仍未可知，但它必定是未來發展的基礎。

柒、使用信用卡證書作爲個體識別的Revised SET協定

SET規範了客戶與商店間以信用卡爲基礎的交易，但仍然採行現有之財務網路作結算與授權，主要是爲銀行業與信用卡廠商所作的。然而對於銀行對客戶交易資料做資料匯集(data aggregation)的威脅缺乏考量適度的預防，這可能是相當嚴重的問題。曾有某位學者就曾經說到“電子商業環境最主要的風險不在於是否有處理不當之交易，而在於資料匯集與監視(surveillance)”(Geer 1995)。SET確實是可以在個別交易的層次保護個別資料的私密，但卻未曾考慮資料匯集可能侵犯個人隱私的問題。

對一個在網際網路上的購買者而言，安全保障與隱私保護是兩個重要的要求，缺一不可。SET應用了密碼學的技術滿足了個體識別、資料確認與隱密性保護的要求；對於隱私的保護，SET考慮到商店的可信賴問題，所以根據資訊分離的方式將購買的訂單分爲訂購資訊與付款資訊來達成對商店隱匿信用卡帳號的目的。但是，收單銀行卻可在交易過程取得信用卡號碼；從實際處理交易的過程來看，收單銀行的工作是從發卡銀行安全地取得付款，而非從信用卡的帳號收取款項，因此無需取得信用卡號碼才能向發卡銀行提出付款的授權。Revised SET的基本想法就是：收單銀行所需要的是信用卡的匿名代理證書(surrogate)，並不需要知道信用卡本身的資訊，也就是說，它不必知道信用卡號碼。

在Revised SET中，商店或收單銀行都無法從代理證書取得信用卡號碼，但持卡人與發卡銀行卻也都不能否認代理證書等於提示信用卡號碼。根據這個準則，Revised SET設計了一個信用卡證書(credit card certificate)作爲信用卡號碼的代理證書(Hwang & Hsueh 1998)，如圖7所示。信用卡代理證書如同SET的各種電子證書一樣採行X.509的格式(ISO 1996)，包括二個部份。第一部份是帳戶憑證(account credential)的相關資訊，有持卡人的公開金鑰、序號(serial number)、個體的命名(subject name)、有效期限及發卡銀行的名字，其中Subject Name就等於信用卡號碼的匿名代理；第二部份則是CA的簽名。發卡銀行必須能透過辨識CA的簽名眞僞與否來決定是否接受該電子證書爲一合法的信用卡代替品(substitute)。在交易進行時，信用卡證書包含在付款指示中，就如同在SET的設計中一樣，付款指示經過加密後只有收單銀行可以看到，但商店無法看到憑證的內容。收單銀行藉著個體的命名來辨識證書。由於個體名稱與卡號之間的關係只有持卡人與發卡銀行知道，所以，收單銀行是不知道卡號的；並且因爲收單銀行在沒有購買的資訊與信用卡號碼的情況下可以彙集的資訊有限，如此一來可以進一步保障持卡人的隱私。

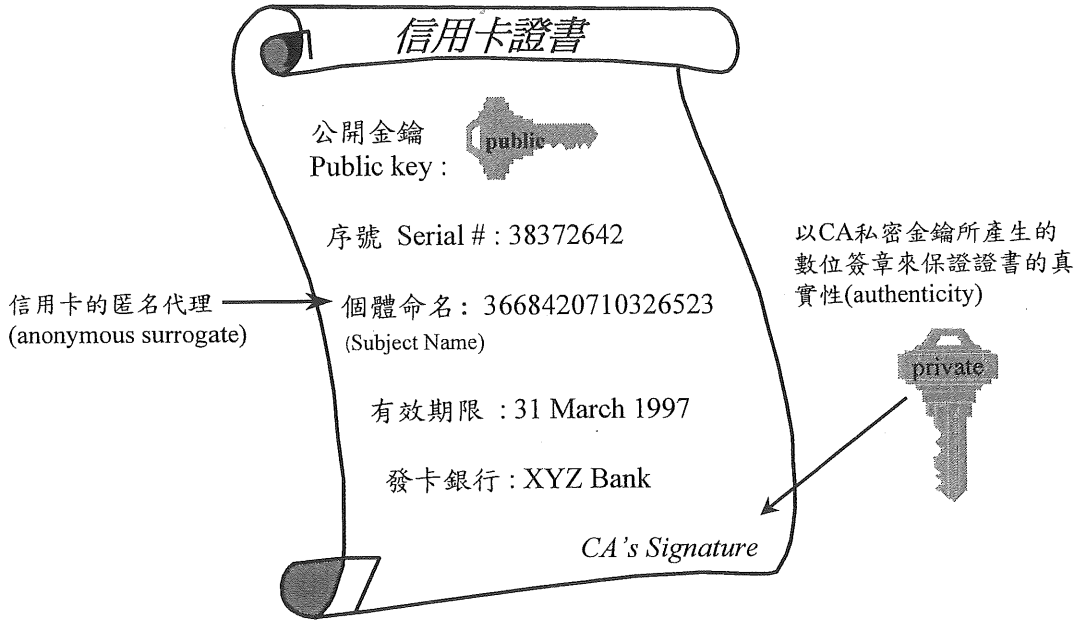


圖7：信用卡証書(Credit card certificate) (Hwang & Hsueh 1998)

另外，Revised SET 還利用了 SET 中的 Transaction ID 作爲資訊的連結，提供作爲持卡人產生月結單的工具（見圖 8）。持卡人在每筆交易後留有消費存根(customer copy)，存根中包含有該筆交易的購買資訊，例如購買的商品說明、購買的地點等。在發卡銀行在進行定期結帳作業時，僅須提供予持卡人 Transaction ID 與交易金額，持卡人即可透過 Transaction ID 的連結產生所需月結單。在 SET 的程式設計說明書中 (Visa & MasterCard 1996)，Transaction ID 是幾個身份辨識碼的組合，發卡銀行可運用其中用以辨識持卡人的 LID_C(local ID) 或以作爲全球唯一識別碼的 XID 予持卡人作爲資訊的連結。如此一來，由於月結單由持卡人自行產生，免除了發卡銀行彙集資訊之需要，因此加強了保障消費者的消費隱私。因此藉由資訊分離與隱匿的使用，這個 Revised 的 SET 版本可以有效地強化對消費者隱私的保護。

捌、匿名信用卡協定

由於傳統的信用卡交易對每一筆交易均有詳細的記錄，因此不具有現金的匿名性。Steven H. Low 等學者針對信用卡號碼的匿名性作研究，提出了一個利用通訊網路的匿名性信用卡付款協定 (Low et. al. 1994)。這個協定結合現金交易中保障消費隱私的特性，與信用卡交易中對安全保護、記錄交易與收費的機制，使得匿名信用卡協定除了具備信用卡交易安全、清算方便與交易可追蹤的特色外，也能防止對消費者隱私權的侵犯。

在匿名的信用卡協定中，對訊息加密以及數位簽章均使用公開密碼法，每一個交易個體都擁有一對公開與私密金鑰。進

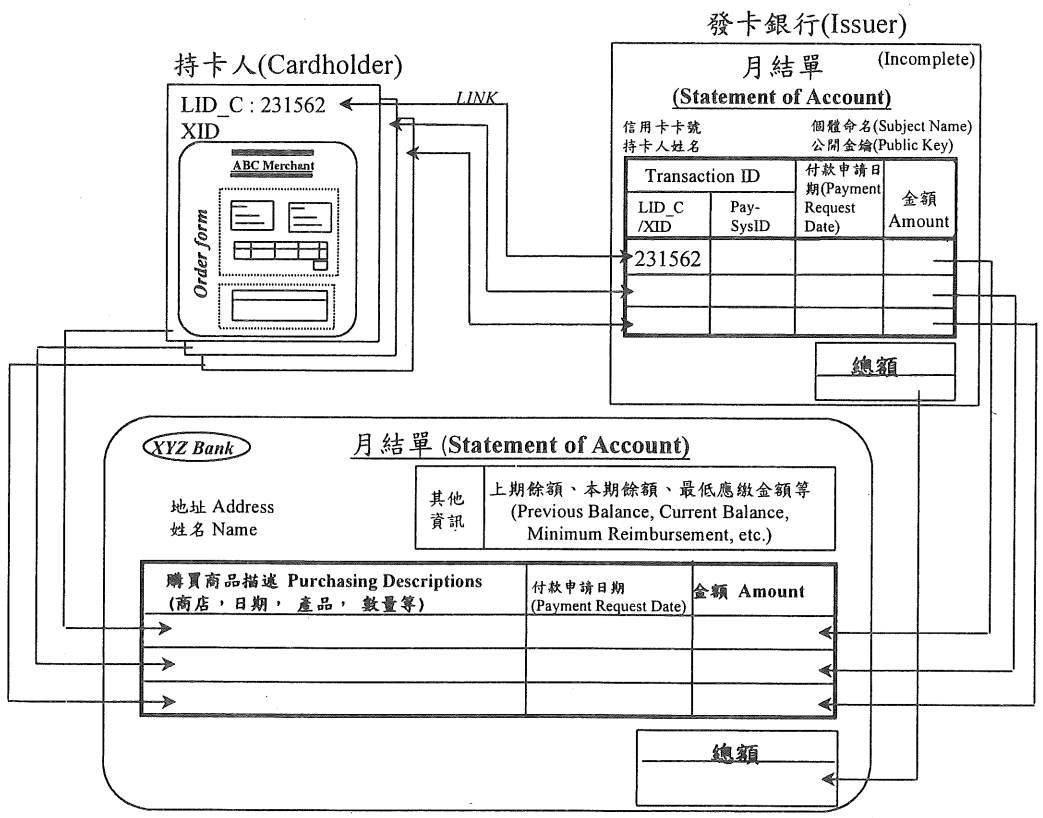


圖8：Revised SET月結單產生之示意圖 (Hwang & Hsueh 1998)

行匿名信用卡的付款時，參與的個體包含了持卡人、發卡銀行、第三者銀行、商店、商店之代理銀行等。在這個協定中，持卡人在不同的兩家銀行擁有兩個帳號，除了在發卡銀行有一個信用卡帳號外，另外在第三者銀行還有一匿名的帳號。發卡銀行知道持卡人的眞實身份，負責將持卡人的信用延伸到第三者銀行；也就是說，在交易進行之前，發卡銀行會將持卡人所擁有的信用額度授權給第三者銀行。第三者銀行透過持卡人的假名 (pseudonym)、匿名帳號與發卡銀行授權的消費信用額度，來確認持卡人所提出的交易是否可予以許可。當持卡人欲在商店購買某樣商品時，他要先向第三者銀行以自己的假名證明自己的身份，第三者銀行確認信用卡與持卡人的身份無誤後，第三者銀行透過代理收款銀行將貨款轉入商店的帳號。每隔一段時間，第三者銀行會將持卡人交易帳單寄給發卡銀行，發卡銀行將帳單交給持卡人進行付款。一旦持卡人完成帳單的付款後，發卡銀行再通知第三者銀行增加持卡人的匿名帳號中的信用額度。協定的基本流程如圖 9 所示。

除了上述的設計外，Steven H. Low 等也將 David Chaum 所提出的 mixer (Chaum 1981) 觀念應用在這個匿名信用卡消費機制中，在協定中設計了一個通訊交換機制 (communication exchange，簡稱 cx)。當任兩個角色之間要互相傳遞訊息時，都要先經過 cx 這個中間角色，這樣的設計藉由 cx 來達成資訊分離的目

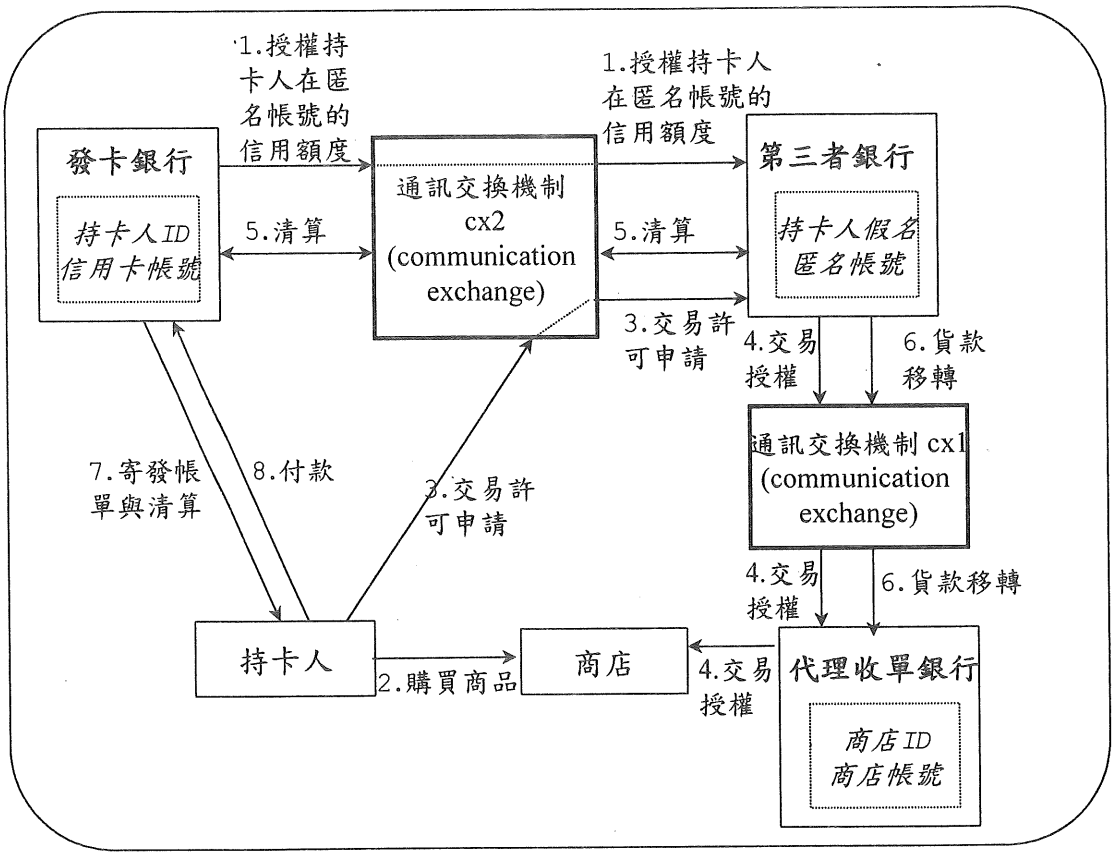


圖9：匿名信用卡協定基本流程圖

的，使得兩個銀行彼此間無法將收到的訊息與送出訊息者之關聯性建立起來。只有在商店、發卡銀行、商店之代理銀行、第三者銀行以及 cx 等五個角色共同合作，才可能知道持卡人身份和他所付款購買的商品的完整資訊。

雖然 Steven H. Low 等提供了一個安全性高的匿名信用卡交易協定，但是仍有一些問題待解決。在協定中，第三者銀行本身不僅是一個一般性的銀行外，它還要提供持卡人一個匿名性的帳號，要如何提供一個匿名性的帳號，文章中並未對其可行性有清楚的說明。從法律的角度來說，銀行提供一個匿名性帳號的可行性，和目前的銀行經營現況有所不同。這個協定未來的發展，仍有待在法制層面先予以釐清。

玖、隱私保護的比較分析

上述所介紹的五種線上信用卡付款的方法，對參與個體之間的信任關係作了不同的假設，根據這些基本假設的不同，對安全的保障亦採取不同的作法，也因此有了不同層次的隱私保護。

以傳輸加密的方式來說，是模仿現行郵寄或電話訂購的信用卡付款方式，由於持卡人對商店的商標與信譽有事先的了解，或持卡人透過其他管道確認網路商店的眞實性，所以持卡人願意信任商店，信

任商店不會冒充持卡人；所以，只有網路上的惡意第三者才是不可信賴的。這種方式的設計理念在於保障信用卡卡號在傳輸過程的安全，避免卡號在傳輸時被竊取或竄改。由於是在商店是可信任的假設下，信任商店不會因爲在交易的過程中知道了信用卡號碼，就冒名持卡人進行交易；也信任商店不會隨意洩露個人的消費資訊，因此在傳輸加密的方式中，從信賴商店的角度考慮，以簡單的加密方式達成對信用卡號碼最基本的安全保障。

傳輸加密的方式，以信用卡號碼作爲持卡人的身份辨識，但由於網路的開放特質及電子商務的發展，在未來有許多的電子商店，持卡人無法再像傳統的信用卡交易一般，可從商店的眞實存在或商譽來判斷商店的可信任程度，因此在傳輸加密的方式中對信任商店的假設，在網際網路的交易環境中，有其發展的基本限制。

雖然這類方式保證傳輸卡號之隱密性，且對已採行這種方式的商店而言，可獲得較廣泛的顧客基礎。但因網際網路開放的特性，任何知道信用卡號碼的人都可以仿冒持卡人進行付款，尤其是惡意的商店更可盜取信用卡號碼，可能冒充持卡人、或洩露給他人來冒充持卡人。謹慎的使用者將不信任網路的安全性，怕個人信用卡被盜用，也怕個人的隱私被侵犯，不願意將自己的信用卡號碼透過網路傳輸；所以，在網路上使用信用卡，其安全需求相當高，若只是單純的將卡號加密，無法被謹慎的使用者所信任。

從下圖中 VISA 對未來線上信用卡付款的發展所作的預測 (Lewis 1996)，他們知道這種傳輸加密的作法不能滿足網際網路交易的安全需求，也因此突顯了安全的信用卡付款協定的需求。

iKP 主要使用公開金鑰密碼法，因此以採行 X.509 的電子證書作爲個體識別，交易的確認除了透過確認電子證書是由合法的 CA 所核發外，並由證書中取得公開金鑰來驗證數位簽章。 iKP 在執行上相

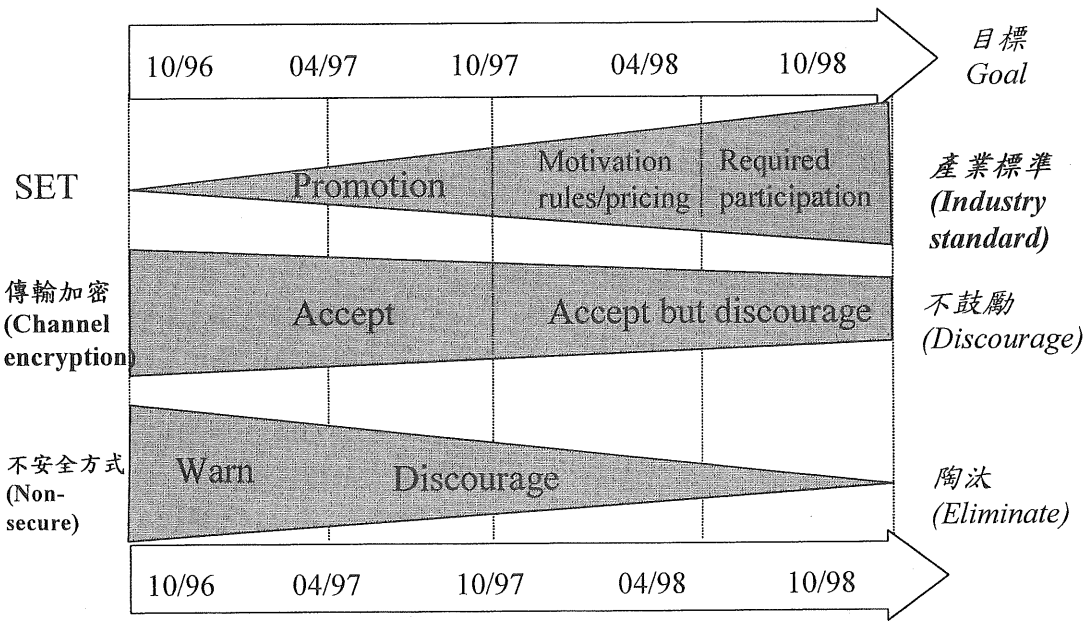


圖10：安全電子商務之市場策略 (Lewis 1996)

當方便，以現行的授權清算體系爲基礎，參與個體間的信賴假設與現行一般信用卡付款相同。所以是假設銀行是可信任的，在設計上，要求商店不可直接取得信用卡卡號以及收單銀行不需知道交易商品內容，以單向赫序函數對商店與收單銀行分別隱藏信用卡卡號與交易商品內容。

iKP 是信用卡付款協定 SET 的前身。在 iKP 中所使用的電子證書，以作爲驗證數位簽章用的電子憑證爲主，參與個體在需要時，可取得電子證書管理機構所簽發的電子證書。SET 使用兩種電子證書，一種是與 iKP 所使用的電子證書相同，用來驗證數位簽章，另一種則是作爲交換金鑰用的電子憑證。至於在消費隱私的保護方面，iKP 使用單向赫序函數來保護信用卡卡號與交易商品內容，SET 則設計了雙文件簽章達成更進一步的保障。

SET 是從銀行的角度來考慮，不管是發卡銀行或是收單銀行都是可以信任的，所以除了以持卡人證書作爲個體識別外，並藉著密碼學的方式，分別以資訊擁有者的公開金鑰加密通訊金鑰，來達成將「訂購資訊」及「付款資訊」對商店及收單銀行作區隔分離。這樣的作法，防止商店取得卡號冒充持卡人，也避免了商店或收單銀行對消費資訊的匯集。使用 SET 系統，發卡銀行可取得個人所有消費相關訊息，對隱私的保護是建立在信賴發卡銀行的假設上，發卡銀行仍能匯集所有的消費資訊，在每個月持卡人所收到由發卡銀行所寄發的月結單中，明列每筆交易的時間、地點、消費的商品內容等，這種對消費資訊的匯集仍然侵犯了個人隱私權。

Revised SET ，依據＂資訊僅讓處理交易眞正需要的人才知道 (need to know) ＂的準則，在不特別假設信任關係下，儘量減少交易資訊的揭露。以信用卡證書作爲信用卡號碼的代理證書，取代了在 SET 中所使用的持卡人證書；這樣的設計，不僅使商店無法冒充持卡人，也解決了資料彙集的問題，避免了對消費隱私的侵犯。而且在 Revised SET ，持卡人可透過使用 Transaction ID 自行產生月結單，減低發卡銀行在編製月結單時同時彙集個人資訊之必要。這個 Revised 版本，確實可以改善 SET 對隱私保護所不足的地方。

iKP 與 SET 都是對現有的信用卡授權清算體系作延伸，所以對消費者的隱私權保護是以銀行是可以信賴的角度來設計，對銀行的客戶保護隱私是以個人資料保護法來規範 (行政院法務部 1995) 。個人資料保護法不允許銀行將彙集消費者的資訊作進一步的利用，因此在 iKP 及 SET 的環境中，持卡人可以引用法律來保護個人的隱私。但這樣透過法律的方式來保障消費隱私是一種被動式的防禦方式，且若銀行網路受到攻擊或銀行內部不法人員侵犯個人消費隱私，就只能尋求法律途徑來保障。 Revised SET 所提供的是主動式的防禦，因爲持卡人可自行產生月結單，在整個交易過程中，除了持卡人本身之外，每個交易個體僅取得處理交易所需要的資訊，因此可避免資料彙集的必要。

SET 協定有工業界的推動，在 1997 年 6 月台灣的 VISA 與 MasterCard 也分別推出 SET 的實驗計畫，未來相當具發展潛力，但發展的成功則取決於 CA 的組織體系之建立。至於 Revised SET 由於特別強調消費隱私，必須視未來電子商務的發展，消費者隱私權重視的程度而定，市場的需求將決定 Revised SET 是否值得商品化。

至於匿名信用卡協定，設計了一個在第三者銀行所開立的匿名帳號，來達成消費隱私保護的目標；而且透過 mixer 的機制，使得商店的代理銀行與第三者銀行無

法取得資訊的關連性。由於只有商店、發卡銀行、商店之代理銀行、第三者銀行以及 mixer 等五個角色共同合作，才可能知道持卡人身份和購買商品資訊，因此我們可知在匿名信用卡協定中，無需與任一交易個體建立可信賴的關係，這樣的設計能夠滿足保護消費的隱私。但是在這個完整的機制中，匿名帳號從法律的觀點來看則尚未有完備的法制環境，有實際執行上的困難。

壹拾、結論

在網際網路上以信用卡作爲付款工具，已成爲未來線上交易支付的主要潮流。對目前普遍使用的傳輸加密的方式來說，由於美國出口管制的限制，較原先的安全性設計薄弱；未來，如果能增強其保密能力，對持卡人而言，這種方式是一種方便而有效的方式，商店也可以擁有原先的顧客基礎。因爲容易建構，傳輸加密方式將能繼續存在；但是長期的發展，仍以 SET 的發展較爲看好。由於 SET 的架構較爲複雜，需要有 CA 的設立以及軟體的提供，所以建構的速度較爲緩慢，測試時程已由原本的 1996 年年底延後至 1997 年第三季，甚至有學者認爲 SET 整個組織體系可能必須要到 1998 年才可能完成 (Clark 1996)。除此之外，由於 SET 主要是藉著電子證書的使用來達成各種安全需求，因此未來極可能會結合 IC 卡來存放持卡人證書，以取代現有的塑膠信用卡，才能讓持卡人更方便地使用。本文作者在另一篇文章提出的 Revised SET ，則是在更進一層思考之後，所延伸之設計，它提供了新一代 SET 的若干思考。總之，安全、隱私與方便三大因素將決定各種協定是否符合電子商務的需要。

參考文獻

1. 鄭玉波， 1995 ，票據法，台北：三民書局。
2. 行政院法務部編， 1995 ，電腦處理個人資料保護法。
3. M. Bellare, et al, iKPoA family of secure electronic payment protocols, in Proceedings of Usenix Electronic Commerce Workshop, July 1995.(http : //www.zurich.ibm.com/Technology/Security/extern/ecommerce/)
4. D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, pp. 84-88, Feb. 1981.
5. D. Chaum, "Blind Signatures for Untraceable Payment," Advances in Cryptology – CRYPTO 82, pp. 199-203, 1983.
6. D. Chaum, A. Fiat and M. Naor, "Untraceable Electronic Cash, "Advances in Cryptologyo-CRYPTO 88, pp. 319-327, 1990.
7. T. Clark, "Secure standard not set in stone", Dec. 24, 1996. (http : //www.news.com/News/Item)
8. John Doggest, Electronic Check Project, Financial Services Technology Consortium (FSTC). (http : //www.llnl.gov/fstc/projects/echeck/index.html)
9. D. E. Geer, "Electronic commerce, banking and you," Computer Security Journal, pp.55-62, vol. XI, no. 2, 1995.
10. Kipp E. B. Hickman, Taher Elgamal, INTERNET DRAFT : The SSL Protocol, Netscape Communications Corp., June,1995.
11. Jing-Jang Hwang and Sue-Chen Hsueh,

"Greater protection for credit card Holders: A revised SET protocol," Computer Standards & Interfaces, Vol. 19, pp. 1-8, 1998.

12.ITU Rec. X.509 (1993)|ISO/IEC 9594-8: 1995, Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, including Draft Amendment 1: Certificate Extensions (Version 3 certificate), ISO/IEC JTC1/SC21/WG4 (April 1996).

13.P.Janson and M. Waidner, Electronic Payment over Open Networks, IBM Zurich Research Laboratory, March 1995. (http : //zurich.ibm.com/Technology/Security/publications/1995/JaWa95.dir/JaWa95e.html)

14.T. Lewis, Lecture Notes in SET Technology, VISA International (November 1996).

15.Steven H. Low, Nicholas F. Maxemchuk and Sanjoy Paul, "Anonymous credit cards," Proceedings of the Second ACM Conference on Computer and Communications Security, pp. 108-117, Nov. 1994.

16.Secure Electronic Payment Protocol (SEPP), MasterCard, Draft Version 1.1, Nov. 1995.

17.Secure NCSA Mosaic Manual, , NCSA,1995.(http: //www.commerce.net/software/SMosaic/Docs.win/Smosaic.version.html)

18.On Internet Security, Netscape Communications Corporation, 1995. (http: //home.netscape.com/newsref/ref/internet-security.html)

19.B. Clifford Neuman, "Security, Payment, and Privacy for Network Commerce," IEEE Journal on Selected Areas in Communications, vol. 13, no. 8, pp. 1523-1531, Oct. 1995.

20.T. Okamoto, K. Ohta, "Universal Electronic Cash," Advances in Cryptology oCRYPTO91, pp. 324-337, 1992.

21.E. Rescorla, A. Schiffman, The Secure Hypertext Transfer Protocol, Internet Draft, Dec 1994.

22.Secure Transaction Technology (STT), VISA, Sep. 1995.

23.Secure Electronic Transaction(SET) Specification : Book 1. Business Description (draft for testing),Visa International & MasterCard International, June 1996.

24.Secure Electronic Transaction(SET) Specification : Book 2. Programmer's Guide (draft for testing), Visa International & MasterCard International, June 1996.

25.Secure Electronic Transaction(SET) Specification : Book 3. Formal Protocol Definition (draft for testing), Visa International & MasterCard International, June 1996.