IC卡安全網路下單系統的設計與實現

楊中皇、徐燕貞、王雪莉、葉鵬誌、高儷芳
國立高雄第一科技大學 資訊管理系
E-mail: chyang@ccms.nkfust.edu.tw
Web: http://www.nkfust.edu.tw/~chyang/

摘要

國內在民國八十六年七月准許券商開辦網路下單業務，至今單月成交總金額佔市場成交量的比例成長至6.42%，而開戶人數亦成長至一百三十萬餘人。而隨著證券網路下單的蓬勃發展，建立一個網路下單的安全環境，讓交易雙方有所參考依循，也就成為一個刻不容緩的議題。本研究裡我們以智慧IC卡為基礎，採用密碼學的理論，以公開金鑰密碼系統及私密金鑰密碼系統來達成網路下單系統的無可爭議、認證、責任性等網路安全功能。

關鍵字：網際網路、電子商務、證券業、網路下單券商、交易安全、IC卡、數位簽章、保密

一、前言

隨著網際網路的日興月盛，以網路進行交易的商業經營模式，逐漸地蔓延在世界各個角落，各行各業無不爭相採用這種經營模式來提高市場競爭力且拓展業務；而這種新興的交易方式包涵的內容林林總總，不勝枚舉，而其中又以電子金融為持續擴大電子商務的重要支撐，也是在企業對企業的電子商務時代跨入此領域最重要的切入點。因為所謂的金融商品，必須兼具流通與變現的特性，而配合電子化的系統使得金融商品無論在保管或交易的便利性上都達到了革命性的突破。電子金融其優點在於能以極低的經營成本就可獲得許多消費者的注意。然而，就像所有其他的行銷通路一樣，網路交易本身具有若干安全上的考量。

國內在民國八十六年七月准許券商開辦網路下單業務，投資人得經由網際網路委託方式買賣上市及上櫃證券。至八十九年七月為止，根據證交所統計，單月成交總金額佔市場成交量的比例從原本的 0.0071%成長至6.42%，其間開戶人數亦由一千零二十二人，至今累成長至一百三十萬二千五百七十四人[1-2]。而在網路證券交易中，關於投資人權益保護之議題，除隱私權保障外，投資大眾最主要考量即在於交易的安全性，所以確保證券交易系統與過程之隱密性及安全性，是整個證券交易系統成功與否的決定性關鍵，也是經營者在推動業務之初就應該考慮並設法排除的一大問題。本研究針對現今網路下單，提出以 IC 卡 [3-4] 的方式進行證券交易，並具體實現網路下單系統。

IC卡是植入晶片的塑膠卡，大小是如同平常的信用卡，非常容易攜帶。IC卡與傳統磁條卡或信用卡比較起來具有難以偽造與記憶空間較高的優點，然而價位也較磁條卡高。IC 卡一般可分為接觸式與非接觸式兩種，前者歷史悠久且功能強大，後者則目前功能較差且多為單一用途(例如高速公路電子收費系統用非接觸式記憶型 IC 卡)。接觸式 IC 卡又可分為記憶型(例如電話 IC 卡)與智慧型(例如金融 IC 卡)，前者安全性較差。

隨著網路技術的快速發展及應用，IC卡的應用日趨廣泛。例如：目前應用最多且被金融界視為塑膠貨幣新興的金融 IC 卡、由中國信託商業銀行與文化大學合作的金融卡與學生證結合的雙重功能之學生證智慧卡、中華電信推出之通話 IC 卡、十大書坊推出的租書 IC 卡、中央健保局在澎湖試辦的健保 IC 卡、中國信託商業銀行與中國石油公司和台北捷運局等將合作推出之卡票合一儲值金融卡、運用在停車場管理及收費的 IC 卡、以及政府大力推行之國民卡・・・等等。由以上實例可知 IC 卡的應用日趨重要亦是未來發展的趨勢。

二、IC卡網路下單

目前熱門的股票交易為了符合客戶的需求以及增加處理的速率已漸漸發展出另一套交易的模式，那便是從網路上來進行買賣。這種方式有別於以往傳統的電話通訊方式，讓客戶在自己的時間許可下，充分進行選擇與決策，而不受限於有限的人力與時間

期限，因此，受到廣大的投資者的歡迎並且期待它的多元化。

然而現行網路下單的網路安全措施以使用通行碼(password)為主。通行碼提供使用權限控制(access control)與基本網路稽核控管功能。這雖然可提供基本的資訊安全功能，但仍需要進一步的防護措施。例如網路沒有保密的功能便很容易為別有用心者在網路傳遞過程中擷取通行碼等相關訊息。無疑地，現有粗糙的網路下單防護措施，並不足以防止各式各樣的入侵、竄改和擅用。本研究是將 IC 卡應用於網路下單內，以低成本高安全性之可攜式 IC 卡裝置來提供證券交易資訊安全功能。

IC 卡記憶容量大，資料可重複多次寫入或更新，具有發展為多目的、多功能卡的潛力。相對於 IC 卡，目前市場上較普遍之而磁條卡的記憶容量僅約為 110 個位元組。本研究中使用 EEPROM 容量為 6K 位元組的 IC 卡；而 16K 位元組以上的卡片也已經進入量產階段。IC 卡的資料可重複上萬次的寫入或更新，使其應用領域大增。由於 IC 卡從製造到發卡的過程相當嚴謹；且 IC 卡是屬高科技的產品，一般人能偽造的機會不高，且其內部資料也是層層保護不易竊讀。因此從安全性的觀點而言，IC 卡實是比磁條卡安全多了，而這也正是 IC 卡吸引人的特點。基於以上幾點，我們可以利用 IC 卡特性，保護個人的憑證資料，增加系統的安全功能。

安全一直是網路下單的最高原則，不管在何種情形下，都希望能達到絕對保密防偽的程度。任何有心破壞或竄改資料內容的駭客者，即使攔截到傳輸的資料時卻無法瞭解內文或者是即使變更了內文而我們依然能憑著使用者本身的認證資料來加以辨識，成功的阻絕錯誤的資訊所可能造成的損失發生。在公開網路上我們不僅能夠以加密的方式確保其安全性，同時在硬體方面運用 IC 卡來加強確認工作，非但在網路證券商那裡下單資料有所存證，投資人自己也能有所記錄，雙方站在相同的立足點上，在公平、公開的原則下交易。在保障傳輸資料的安全性的同時，能做到使其中的交易資訊保持其同一性，不因傳輸而受到破壞，使雙方都能信任彼此所傳遞的內容是最初的也是最完整的。

在傳輸的資料當中，本研究加入了使用者個人身份的驗證，透過數位簽章的技術，使得投資人及網路證券商雙方都可以在個人隱私資料充分被保護下還能夠讓對方確認自己的身份，並也間接地為此份傳輸的資料做保證和聲明，保證資料的來源無誤和聲明作者為何人，因為這樣的特性而能使個人的身份擁有不可否認的本質。本研究的研究成果便可以使在網際網路上傳輸的內容和整個流動的過程，包括資訊的查詢和資料庫的存取都達到高度的私密性，讓網路上的資訊安全的問題得到一個最好的解決和應對之道。

三、系統架構

一套安全完善的網路下單系統可以防止駭客的破壞，下單資料在網路傳送時也不用擔心被洩露而造成嚴重的後果。本文採用 IC 卡做為系統之可攜式裝置，針對網路下單達到: (1). 提供保密性，僅有經過授權的單位能讀取出傳送的下單資料，(2). 提供認證性，下單投資人及網路證券商雙方的身份可經確認，(3). 提供無可否認性，不容許傳送的網路下單資料於事後加以否認。

如圖 1 所示，我們 IC 卡網路下單系統是以端對端安全架構為主，依據使用的下單軟體進行端對端資訊安全設計。使用時用戶端為配備 IC 卡讀卡機之個人電腦，而在伺服器端包括認證中心(certificate authority, CA)與網路下單伺服器。

認證中心為具公信力之機構，可對網路證券商及投資人提供公開金鑰憑證(certificate)管理服務。認證中心的基本功能如下列：

1. 憑證申請: 提供用戶申請其所屬的電子憑證。憑證是以 X.509 的格式儲存。
2. 憑證註銷: 註銷尚在有期間內用戶憑證。
3. 憑證查詢: 可以查詢自己或他人的憑證資料，以便取得到公開金鑰資料。
4. 憑證展期: 若因為其他因素必須延長憑證有效期限，CA 也提供憑證延期的服務。
5. CRL 列表: 當憑證註銷後，系統便會將憑證資料轉入此表中，讓使用者可以查詢。

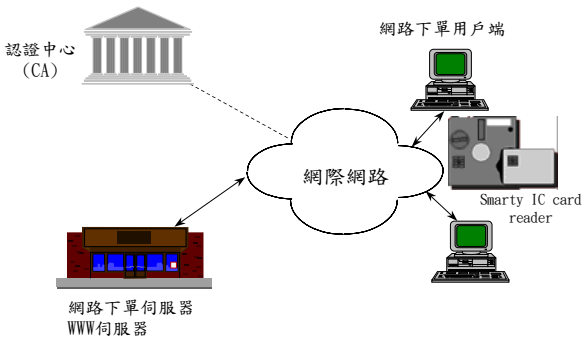

圖 1　IC 卡安全網路下單系統架構

投資人必須先在認證中心上面註冊自己的個人資料和自己的公開金鑰，然後取得憑證。用戶端與伺服器端的進行通信時，各自應用程式會對通信內容產生數位簽章（Digital Signature）[5]，用以防止內容遭到修改或仿造且提供寄信的證明。發文單位先將通信內容用使用 SHA 演算法 [6] 產生該郵件的單向雜湊函數值（One-way hash value）並使用寄件人的 RSA 私密金鑰（private key），產生數位簽章，附加於此郵件。同一發文單位發出不同資料時，各資料之簽章不同；相同資料由不同發文單位發出時，簽章也不同。為了保障傳輸時的隱密性，系統會先在傳送端產生一串 112 位元的隨機亂數作為將內容做 Triple-DES [7] 加密的會談金鑰（Session Key）[5]，然後從接受端的憑證中取出公開金鑰對會談金鑰作加密；這是所謂的數位信封(Digital Envelope) [5]。

雖然 DES 為一相當強的資訊保密演算法，但隨著電子科技的發展與電腦運算速度的提升，設計破解 DES 的特殊硬體或以多部電腦合作破解 DES 的構想與實驗近幾年來一再被提出，使得 DES 系統的安全性受到質疑 [8]。這也使得以 DES 為密碼演算法機制的 IC 之系統安全性堪虞。所以我們改用所謂的三重 DES (Triple-DES, TDES) [7]。在 TDES 系統可用兩組各 56 位元的金匙，使得加密或解密金匙總長度擴充到 112 位元，足以應付一般資料保密需求。

四、具體實現

我們採 C++Builder 4.0 [9] 作為軟體主要開發工具，並結合微軟公司 SQL 伺服器完成資料庫之建構。認證中心的數位簽章採用 2048 位元的 RSA 金鑰來製作，投資人與網路證券商的數位簽章則採用 1024 位元的 RSA 金鑰來製作，同時我們也採用 IC 卡來儲存與管理的憑證以及私密金鑰。憑證採用符合 X.509 的格式儲存，憑證內含有憑證所有人的姓名，電子郵件等資料，其中最重要的是憑證所有人的公開金鑰。

讀卡機係採用 Fischer 公司的 Smarty IC 卡讀卡機 ，它在形狀大小上跟 3.5 吋磁碟片一樣。只要將 IC 卡置入讀卡機後，再將此讀卡機插入電腦 3.5 吋軟碟機即可透過 PC 操作。用戶端系統是在 Windows 98 平台下發展，而認證中心及網路下單伺服器則是在 Windows NT4.0 平台。IC 卡安全網路下單系統功能基本上可分為用戶端(client)與伺服器端（server)兩部分。

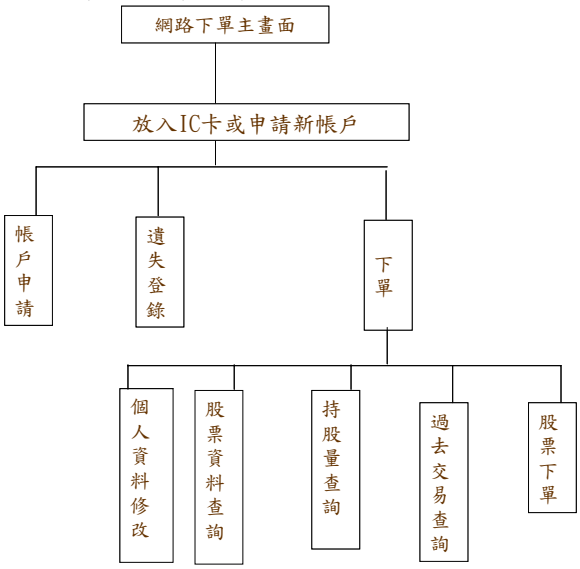

圖 2　客戶端網路下單主要功能

客戶端的主要功能如圖 2 所示。投資人先透過網際網路向證券商申請開戶，此時系統會將開戶欄位所輸入的資料加密，並傳送給伺服器，若開戶成功，伺服器會回傳開戶成功訊息，否則回傳開戶失敗。爾後客戶進行帳號登入時會檢查密碼是否正確，正確時系統會從 IC 卡中讀取客戶編號並將客戶編號加密及加數位簽章，傳送到下單伺服器，並等待伺服器回傳客戶基本資料。當客戶 IC 卡遺失時，則使用 “遺失登錄”，選擇以 “客戶編號” 或 “身份証字號” 來做遺失登錄。所輸入的客戶編號或身份証字號將加密及加數位簽章，並傳送給伺服器。遺失登錄成功與否，伺服器會回傳相關訊息。

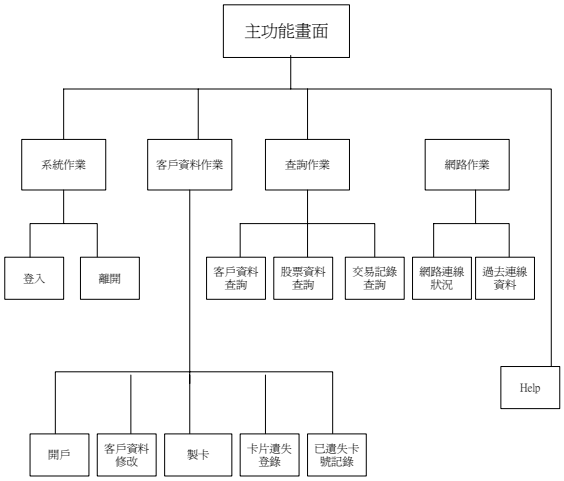

圖 3　網路下單伺服器主要功能

網路下單伺服器系統主要功能介紹如圖 3 所示，簡述如下：

1. 系統作業: 包含系統管理者登入、離開兩個子功能項。
2. 客戶帳號管理作業: 包含客戶帳號申請、客戶資料修改、IC 卡製作、遺失登陸、已登錄失卡清單等五項子功能項。
3. 查詢作業: 包含客戶資料查詢、股票資料查詢、網路下單資料查詢等三項子功能項。
4. 網路作業: 目前連線狀態、過去連線記錄、訊息顯示三項子功能項。
5. 說明: 包含關於我們一項子功能項

伍、結論

網際網路電子商務有著跨國界、跨地區、24 小時全年無休的效率以及卓越的分佈性，但是除非能建立一套安全且便捷的制度，否則網路商業將難以有突破性的發展。世界各大企業為了搶攻電子商務這塊大餅市場，無不爭先恐後地架設自身的電子商務站，但又紛紛面臨到資訊不安全的問題，於是又積極地研究有關資訊安全的環境，希望能拔得頭籌，搶得龍頭的寶座，獲取客戶的信心。雖然在現行制度下，有許多保護資訊安全的方法，但是卻沒有任何一種方法或制度可以完全確保電子商務的安全，通常都必須要兼採不同的方法，例如採取加密保護(使明文內容不易被更改)、線上認證（交易雙方能夠確定對方身分)、不易更改裝置（IC 卡）等方式來嚴格執行，才能確保電子交易的安全。

本研究依照上述的論點開發了網路下單雛形系統，在這樣的處理架構下，所有流通於投資人與證券商二方之間的資訊流，都使用密碼學技術將其保護，不論任何來自於投資人或證券商的要求或存取，都在其中受到保障，而這所有的訊息傳遞都被兩端系統所獨立記錄，以便日後比對，且在這樣的基礎架構之下，可彈性地依使用者的在網路安全的需求之下來建置系統，發展出屬於自身的特色。

致謝：

本研究承蒙企龍股份有限公司的贊助，特此致謝。

參考文獻

1. 台灣證券交易所，http://www.tse.com.tw/docs1/data01/trading/public_html/月統計表.doc.
2. 陳榮吉、黃俊豪，網際網路證券交易專題研究，88年11月，台灣證券交易所。
3. W. Rankl, W. Effing, R. Wolfgang, *Smart Card Handbook*, John Wiley & Sons, 1997.
4. M. Hendry, *Smart Card Security and Applications*, Artech House, Inc., 1997.
5. William Stallings, *Cryptography and Network Security: Principles and Practice*, 2nd edition, Prentice-Hall, Inc. 1999.
6. National Institute of Standards and Technology, *Secure Hash Standard*, Federal Information Processing Standard, FIPS PUB 180-1, April 1995.
7. National Institute of Standards and Technology, *Data Encryption Standard (DES)*, Federal Information Processing Standard, FIPS 46-3, October, 1999.
8. "Cracking DES code all in a day's work for security experts, " http://cnn.com/TECH/computing/9901/21/descrack.idg/index.html. See also " RSA Code-Breaking Contest

Again Won by Distributed.Net and Electronic Frontier Foundation (EFF) - DES Challenge III Broken in Record 22 Hours, " http://www.rsasecurity.com/news/pr/990119-1.html.

9. Borland C++Builder, http://www.borland.com/bcppbuilder/productinfo/.