電子商業交易的爭議解決機制*

黃景彰、沈曉芸
交通大學資訊管理研究所

摘 要

電子商務是在二十世紀末期出現的新的商業活動方式，正如同傳統的商業活動，商業交易的「爭議」是無可避免的。因此，一個可以解決交易爭議的機制，是電子商務的環境所必須建立的。由於「證據」是解決爭議的關鍵要素，故爭議解決機制必須能夠在交易事件發生時，產生、記錄、傳遞、儲存與檢驗證據，並在有爭議發生時，取出證據以爲依循。本文以相關的國際標準與學術文獻爲理論背景，依據所應用的密碼學方法環境 ?? 對稱式與非對稱式密碼方法 ?? 歸納得到二類電子商業交易中爭議解決機制的一般模型 (generic model)。此外，基於該模型，以臺灣網路證券交易市場爲例，並以現行契約準則及正在立法院審議的電子簽章法草案爲依據，設計適用的交易爭議解決機制。

關鍵字：電子交易爭議解決機制、不可否認服務、證據、資訊安全、網路證券

*本文係國科會專題研究計畫「網路銀行交易事項的不可否認服務之研究」(89-2416-H-009-038) 補助之研究

Dispute Resolution Mechanism for Electronic Transaction

Jing-Jang Hwang, Hsiao-Yun Shen
Institute of Information Management
National Chiao Tung University

ABSTRACT

Closing to the end of last century, electronic commerce emerged as a new way of doing business. As in the old commerce, disputes are inevitable; therefore, mechanisms for disputes resolution are essential even in the world of cyberspace. Since evidence is the key to resolve disputes, those mechanisms must entail procedures defining the generation, record, transfer and verification of evidence about the occurrence of an e-commerce event, and the retrieval of this evidence if disputes arise later on.

Generalized from relevant international standards, two generic models are proposed in this paper for disputes resolution. The models are classified according to their underlying cryptography-symmetric or asymmetric cryptography. Then the models are applied to define a scheme that would help to resolve disputes arising from on-line trading in the Taiwan securities market. The scheme complies with the current regulations and the draft of the digital-signature law, which is now under review in the Legislative Yuan of the government.

Keywords : disputes resolution, non-repudiation service, evidence, information security, on-line trading on securities

壹、前　言

隨著網際網路時代的開啓，電子商務亦隨之快速發展，成爲人類社會新的商業活動方式，並且對許多產業造成了影響與衝擊。網路商店、網路下單、網路銀行、企業間電子商務等新的企業經營模式已經進入了人們的日常生活當中；在這些以電子化方式進行的商業活動當中，若是交易訊息的傳遞有所疏漏，或是參與商業行爲的任何一方對其行爲加以否認，將會造成商業上的糾紛。因此，一個可以產生、蒐集、記錄交易證據，並確保證據的可用性，有能力在糾紛發生時，將證據取出以供仲裁的爭議解決機制，是在電子商務的環境中不可或缺的。

「證據」是電子商業交易爭議解決機制中的核心觀念。依據留存的證據，可以在事後證明事件發生的眞實性，而交易的參與者則可以引用證據來解決具爭議性的事項。爲佐證事實，證據中必須記錄交易的當事人、交易事件、事件發生的日期、時間等相關資訊。同時，也必須制定產生、驗證、儲存及使用證據的安全政策；針對那些交易訊息必須產生證據，證據由誰建立、由誰負責保管、由誰來檢驗、使用上有何限制，以及每一項工作的程序都應當有明確的規範。此外，一個週全的爭議解決機制還需要涵蓋由交易雙方所共同接受的仲裁政策，也就是說，當有糾紛發生時，當事者或仲裁者引用證據時，要有依循的準則，以處理爭議。一般說來，由於證據是用來證明事件是否曾經發生的資訊，使得參與事件的當事人無法否認他的行爲，故此一系列證據處理的工作，也稱之爲事件不可否認服務 (non-repudiation)。

目前，實務上的電子商務系統對於電子商業交易的爭議解決機制著墨並不多。本文探討相關國際標準與學術文獻，依據所應用的密碼學方法環境 ?? 對稱式與非對稱式密碼學方法 ?? 歸納出電子商業交易中爭議解決機制的一般模型。此外，討論現有網路金融（如網路下單與網路銀行）的相關規範，並基於一般化的模型，以臺灣網路證券交易市場爲例，設計適當的交易爭議解決機制，以期建構更完善的電子商務環境。

貳、電子商業交易爭議解決機制的工作階段

國際標準組織 (International Organization for Standardization ((ISO)) 與國際電工協會 (International Electrotechnical Commission (IEC)) 制定的標準文件 ISO/IEC 10181-4 (ISO/IEC JTC 1, 1997a) 自證據處理的角度出發，將事件發生的不可否認服務分爲四個階段：

(1)證據產生階段：爲證明特定事件的發生，可以由事件參與的當事人或是公正的、被信賴的第三者 (Trusted Third Party (TTP)) 負責產生證據。證據中必須載明事件發生的事實、涉入事件的當事人、證據產生者、及事件發生的日期、時間、或地點等相關資訊。

(2)證據的儲存、傳遞與取用：主要是處理已產生的證據，包括證據的儲存與傳遞。例如，由證據的產生者將證據傳遞至證據的保管處，或是傳遞給證據的檢驗者；另外，也可能是由請求產生證據的當事人取用已儲存的證據。

(3)檢驗證據的有效性：在必要時，使用證據的個人或團體可以要求檢驗證據，以證明使用的證據是值得信賴的。如此一來，證據的使用者可以獲得信心，相信爭議發生時，可以提出具有可信度的證據。

(4)爭議解決階段：當爭議發生時，仲裁者

自原告、被告、或被信賴的公正機關蒐集證據，並依據仲裁政策來解決爭議，或者，爭議的雙方也可以自行引用證據來處理，不一定會需要仲裁者的介入。這個工作階段的作法與法制環境有相當程度的關係，比較沒有標準的程序可以依循。如果沒有爭議發生，最後這個階段的工作不會被執行，但是，前面三個階段的設計都是爲了支援這一階段的工作。

依據上述四個階段的工作任務，國際標準文件 (ISO/IEC JTC 1, 1997a) 中列舉出幾種在電子商業爭議解決機制參與的角色：

※證據當事者：證據是爲了證明某一事件確實發生過，故涉入事件的個體而應該在證據中予以記錄者，稱之爲證據的當事者。以一般商業交易爲例，發出購買請求的買方必須爲他的動作負責任，「訂單」可以視爲一項證據，此時買方即是證據的當事者；買方付款後，賣方必須開立「收據」爲他確實收到款項這個事件負責任，則賣方是「收據」的當事者。

※請求產生證據者：因爲某種需求，而要求產生相關的證據，此要求者即爲請求產生證據的個體。若事件的當事人爲證明他的行爲，可以請求產生證據；需要使用證據的利害關係人、團體、或第三者，也可以提出產生證據的請求。例如，交易雙方、電子商務中代收或代付的金融機構、政府的課稅機關、或是他們委託的代理人等都可能發出請求產生證據。

※證據的使用者：是指使用證據的個人或團體，通常是與證據當事人有相對的權利義務的關係人，或是受到事件影響的個體。舉例來說，發送文件的「發文證據」的當事者是發文方，「發文證據」的使用者，則是受事件影響的收文方。另外，證據的使用者也可以是必須對事件負責的主管、機構，或爲後續活動採取因應行動的工作者，爭議處理仲裁者即是一例。

※證據的產生者：產生證據的個體。通常，證據的產生者可以是證據的當事者，也可以是公證的、可信賴的第三者。

※證據的驗證者：證據的使用者可以自行擔任證據的驗證者，或請求 TTP 檢驗證據的有效性。

※輔助 TTP：在證據產生階段，TTP 可以在記載事實的證據之中加入更多佐證事實的資訊，或額外附加所需的輔助證據。此外，TTP 可以在傳遞證據時擔任類似郵局的傳遞者，或作爲保管證據的特定機構。而使用密碼學工具所需要的憑證機構，或金鑰的分配者 (key distributor) 等也都可以是爭議解決機制中的輔助 TTP。

※原告、被告、與仲裁者：此三者是當有紛爭發生時，在爭議仲裁階段時涉入的三種角色。

這裏所列舉出的各種角色，彼此之間並不是互斥的，不同的角色功能可以由同一個體執行。證據的當事人可以是證據的產生者，也可以是證據的使用者；而證據的驗證者可能是證據的使用者，也可能是受託付的 TTP；同一個 TTP 可以同時擔任證據的產生者、驗證者，或許此 TTP 也可執行時戳服務的工作。TTP 介入爭議解決機制的模式相當有彈性，系統設計者必須考慮法制環境、系統參與者彼此之間的互信程度、與使用的密碼學方法等因素來建置 TTP。角色的合併或分割，取決於電子商業交易爭議解決機制的資訊安全政策，及由這些政策所規範的系統運作的需要。

參、證據的技術分類與內涵

在商業交易過程中所傳遞的某種承諾，像是經由網路傳遞的訂購單、網路下單的委託書、信用卡付款指示等，都是有必要留下證據的通訊事件。在 ISO/IEC 13888-1 (ISO/IEC JTC 1, 1997b) 標準文件中，定義了網路上訊息往來所需要產生的證據，以下幾類是比較重要與常見的。

(1)來源證明 (proof of origin)：用來證明訊息是由誰建立與傳送的，以反制訊息來源的否認。在標準文件中指出，來源證明可以視爲訊息發送方的「創作證明」(proof of creation) 與「發文證明」(proof of sending)，換句話說，來源證明可以作爲訊息發送者建立了訊息的證據。

(2)送達證明 (proof of delivery)：用來反制訊息的接收者在收到訊息並獲知訊息的內容後卻加以否認。換言之，這項證據可以視爲「接收證明」(proof of receipt)，同時也作爲接收者已得知訊息內容的「獲知證明」(proof of knowledge)。

(3)送件證明 (proof of submission)：在網際網路的訊息傳遞統中，可以透過一個訊息的傳遞機構負責在交易的雙方之間傳遞訊息，因此必須提供適當的證據，以防止傳遞機構否認其曾經接受訊息傳遞要求的事實。

(4)傳遞證明 (proof of transport)：當傳遞機構確實協助訊息傳遞之後，必須建立適當的證據，以證明傳遞機構已將訊息傳遞給訊息接收者。因此，傳遞證明可用來反制傳遞機構否認他已經送出訊息給接收方。

(5)轉送證明 ((proof of transfer)：若有二個或更多的傳遞機構介入訊息的傳遞過程時，其中一個機構接收到前一個傳遞機構轉送來的訊息，他有必要產生轉送證明，並交付給前一機構，以證明自已確實接受了傳送訊息的工作，而無法否認曾經接收其他傳遞機構所轉送的訊息。

送件證明與傳遞證明僅適用於有傳遞機構 (delivery authority) 協助訊息傳遞的環境，另外，如果有二個或多個傳遞機構介入訊息傳遞的過程，則會有轉送證明的需要。而不論是否有傳遞機構介入，來源證明與送達證明皆可適用於訊息傳遞的環境，且此二類型的證據可說是電子商業交易中的主要證據。以下，將自密碼學的角度來討論證據的技術分類與內涵。

由於在電子商業交易中的證據是數位化的證明文件，而數位化文件是否有效的條件是必須維持文件的資訊眞確性 (integrity)；爲保護數位化證明文件的眞確性，必須要使用保護程度較高的密碼學方法。根據黃景彰教授（民 90 年）對眞確性保護方法的評估，使用非對稱式密碼學方法的「數位簽章」與對稱式密碼學方法「封條」作爲安全資訊的眞確性保護方法，方可用於數位化證明文件的眞確性保護，以提供足夠的證據力。

法律上，證據可以是各種形式的，但以數位化的觀點來看，證據的類型主要取決於所使用的密碼技術，因此，依據前述的眞確性保護方法，可將爭議解決機制中的證據分爲「簽章式證據」與「封條式證據」；也就是說，簽章式證據是應用在對稱式密碼學（或公開金鑰）環境中，而封條式證據則是用於使用對稱式密碼學方法的環境。若以國際標準 (ISO/IEC JTC 1, 1997b-d) 常用的符號表示，則爲：

(1)簽章式證據 = text ‖ z ‖ $SGN_A(z)$

(2)封條式證據 = text ‖ z ‖ $MAC_{TTP}(z)$ = text ‖ $SENV_{TTP}(z)$

其中，‖是將前後的資料項目予以連接的符號；z 是事件的事實陳述，其中可能包含證據的當事人、產生者、證據產生的時間等不同項目，這些具體的內容會依事件的性質而有所差異；text 則是用於補充事實陳述的額外資訊，例如傳遞訊息的唯一識別或儲存位置等，text 的使用相當有彈性，爲非強制性的資料項目，並不納入數位簽章與封條的保護之中。

$SGN_A(z)$ 是由 A 所簽署的數位簽章式的安全資訊；$MAC_{TTP}(z)$ 則是由某一個被信賴的公正機構 (TTP) 利用他的秘密金鑰 (secret key) 所製作的封條，這是應用於對稱式密碼學環境中的方法，若將 z 與 $MAC_{TTP}(z)$ 連結起來，稱之爲安全信封 ($SENV_{TTP}(z)$)，以保護事實陳述的眞確性，。

一般來說，證據中的事實陳述 z 會包括以下的項目：

※爭議解決機制中所依循的安全政策
※證據的類型，也就是說，此證據爲來源證明或送達證明等
※證據產生者的唯一識別、事件當事人的唯一識別
※若有傳遞機構介入，則必須記錄證據傳遞機構的唯一識別
※事件發生的日期時間、證據產生的日期時間
※傳送的訊息本身，或可代表訊息的訊息摘要

舉例來說，若訊息發送方在 A 於 2001/02/01:0930 傳遞訊息 m 給接收方 B，並由 TTP 於 2001/02/01:0931 產生封條式的來源證明時，證據的格式如下：

來源證明 = text ‖ z ‖ $MAC_{TTP}(z)$

其中，z =（安全政策，"來源證明"，A，B，TTP，2001/02/01:0930，2001/02/01:0931，H(m))，其中 H(m) 是訊息 m 的訊息摘要（即赫序值）。MAC (Message Authentication Code) 是用 TTP 與證據驗證者共享的祕密金鑰 (secrete key) 對 z 所產生的保護封條，在證據檢驗階段，驗證者必須用同樣的赫序函數產生 H(m')，並與 z 中的 H(m) 加以比對，檢驗訊息的眞確性，並由 TTP 以其祕密金鑰對安全信封中的 z 產生一個新的檢查值 $MAC_{TTP}(z')$，然後與 $MAC_{TTP}(z)$ 互相比對來檢驗此封條式的證據。

在 ISO/IEC 13888 (ISO/IEC JTC 1, 1997b-d) 系列的標準文件中分別描述了一般性證據、時戳證據及公證證據等三種類型的證據，依據不同的證據，前述的 z 即會包含不同的資料項目。

肆、電子商業交易爭議解決機制的基本模型

在電子商業交易的爭議解決機制中，公正可信賴的第三者 (TTP) 扮演相當重要的角色，依據所使用的密碼學方法以及爭議解決機制的安全政策，TTP 可以在不同的工作階段適當地介入。一般來說，都是假設 TTP 是安全且可以信任的，TTP 的介入方式可以分爲 (1) 離線作業 (off-line)，也就是說，TTP 並不涉入證據的處理工作，而僅僅是支援的角色；(2) 即時線上作業 (on-line)，在這種情況下，TTP 可以是證據的產生者，或是輔助證據處理的相關機構；(3) 中介處理 (in-line)，一個 in-line TTP 負責證據的產生、驗證及傳遞，此時，訊息的收發雙方不會直接通訊，所有的通訊都必須透過 TTP。

舉例來說，在使用公開金鑰密碼系統

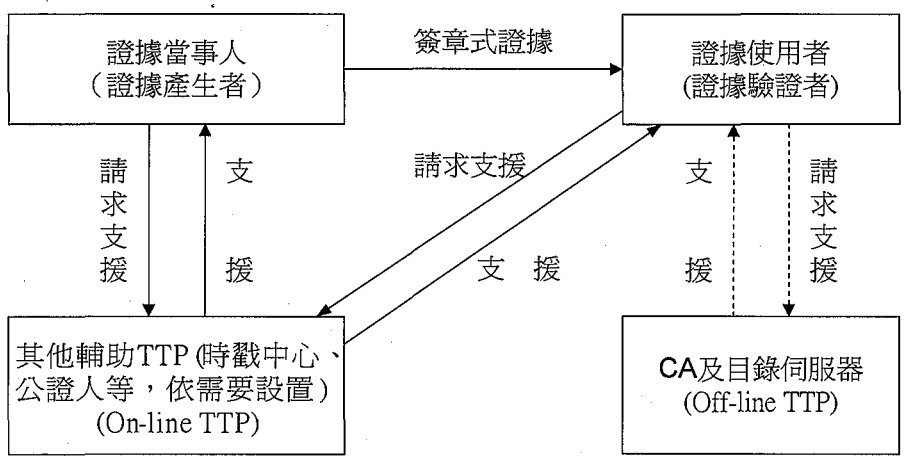

圖1 電子商業交易的爭議解決機制的參考模型－公開金鑰密碼環境

的環境中，證據的當事人可以使用他的私密金鑰產生簽章式證據，因此，在證據的產生階段，沒有必要假手 TTP；但是，金鑰的眞實性與有效性必須被保證，在這裏，憑證機構 (CA) 或目錄伺服器即扮演了一輔助性的 off-line TTP，他們以離線作業的方式提供不可否認服務所需要的資訊。另外，有效的時間戳記可說是各種證據中的重要項目，爲了在證據上加上可以信賴的時戳，扮演「時戳服務中心」的 TTP 將依需要設置，並即時地在線上提供服務。許多相關研究都是將不可否認服務工作建立在使用公開金鑰密碼方法的環境架構中 (Coffey & Saidha; ISO/IEC JTC 1, 1997d; Zhou & Gollmann, 1997a, 1997b; You, Zhou, & Lam, 1998)。圖 1 指出在使用公開金鑰密碼方法的技術條件下，爭議解決機制的基本模型。

而在使用對稱式密碼學架構的限制下，產生及驗證證據 on-line TTP 是必要的，產生證據與驗證證據的 TTP 可以是同一者，也可以是不同的二個機構。此時，證據處理系統中的主要角色及基本模型如 圖 2 所示。在這一類型的機制中，證據的當事人（以 A 表示）與證據的產生者之間共享一把秘密金鑰 (secret key)，而證據的驗證者與證據使用者 (B) 之間共享另一把秘密金鑰；如果證據產生者與驗證者非爲同一人時，他們彼此之間也會共享一把秘密金鑰。以 圖 2 爲例，證據的當事人會以他與證據產生者之間共享的秘密金鑰爲「事實的陳述」（即前文所述的 z）製作一個安全信封 ($SENV_{A,TTP}(z^*)$) 傳送給產生證據的 TTP，要求產生證據；而證據的產生者會依事實陳述 z^*，加入適當的證明，產生封條式證據，製作安全信封（即 $SENV_{TTP,A}(z)$，也就是 $z \| MAC_{TTP}(z)$) 回傳給證據的當事人，再由證據當事人送交給證據使用者。由於證據的當事者與使用者是利益衝突的兩種角色，因此他們之間並沒有共享的金鑰，而是由證據使用者要求驗證者進行檢驗的工作。

此外，如果進行商業交易的雙方之間欠缺信任，或者溝通不便時，也可以採用完全依賴 TTP 介入的 in-line 模式 (Coffey & Saidha, 1996; ISO/IEC JTC 1, 1997c)，或部份 in-line TTP、部份 on-line 的模式。圖 3 所示即爲 in-line TTP 的模型，在這種情況下，TTP 除了產生、驗證證據之外，證據及交易雙方所有的訊息往來都必須透過 TTP 來傳遞。有 in-line TTP 參與的爭議解決機制並沒有限定在特殊的密碼學應用環中建構，事實

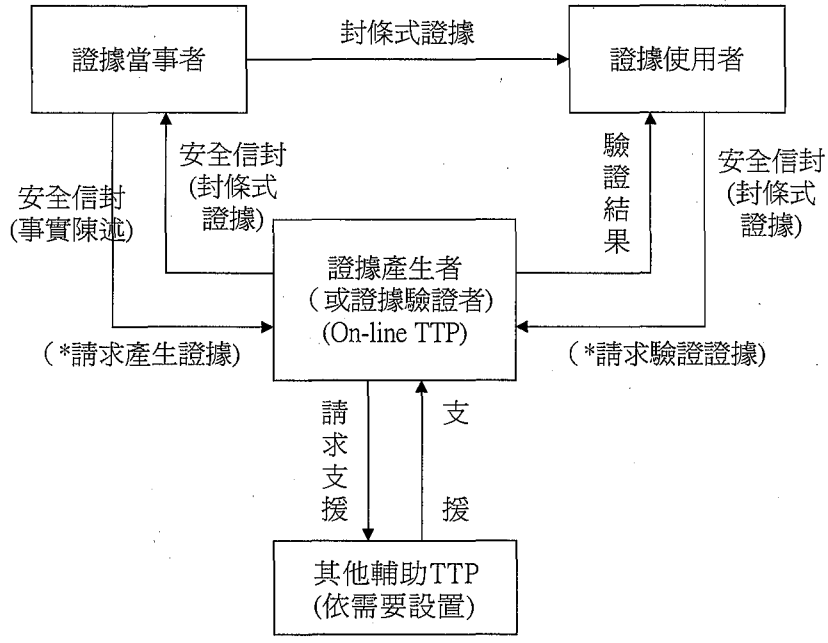

圖2 電子商業交易的爭議解決機制的參考模型－對稱式密碼學應用環境

上，不論是使用非對稱式或對稱式密碼學方法的應用系統，皆可能會有 on-line 或 in-line TTP 參與其中。

電子商業交易的爭議解決機制是一種應用導向的安全服務，尤其是，從法律與技術的觀點來看 (Mccullagh & Caelli, 2000)，必然會有相異的解釋與做法。故商業行為的特性與規範、法制環境、使用者等都是設計機制與制定相關安全政策時不可忽略的重要考量因素。

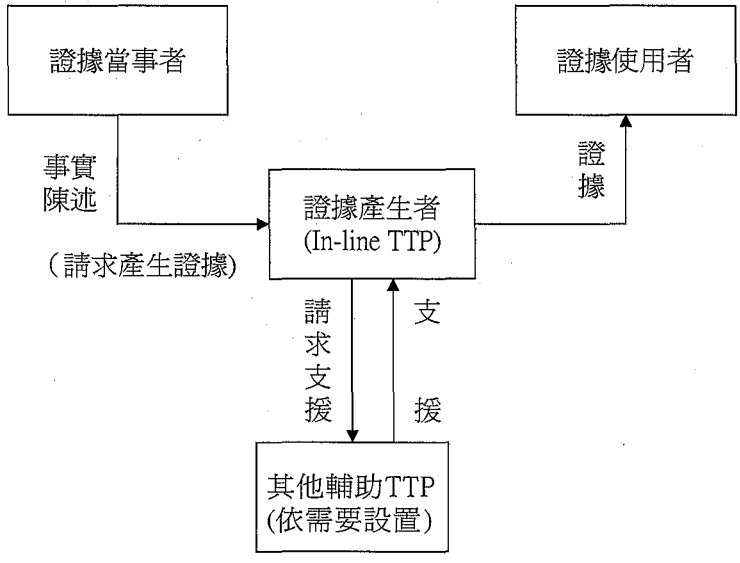

圖3 電子商業交易的爭議解決機制的參考模型－介入 in-line TTP

伍、網路金融交易的爭議解決機制

網際網路與電子商務的快速發展，已經衝擊了全球的金融市場，在成本、速度、服務的需求及網路發展的趨勢下，金融交易市場的網路化已成爲金融產業的時代課題。不論是銀行、證券、期貨、保險業者，對於現有服務或新的產品都必須朝向網路化、資訊化發展；在國外，純虛擬的網路銀行、網路證券商甚至已成爲新興的企業經營模式，例如安全第一網路銀行(Security First Network Bank)、網路券商 E*TRADE (www.etrade.com) 等。因此，網路金融交易的安全問題也成爲重要的議題，本文將自爭議解決機制的觀點出發，探討國內網路金融在相關事項的規範，並以網路證券下單爲例，提出本研究的建議。

一、國內現況探討

目前，在網路金融環境中，網路銀行與網路下單已時有可聞，本文先以現行與此二者相關的使用準則與規範，探討爭議解決機制的必要性。

就網路下單委託契約相關規定來看，臺灣證券交易所股份有限公司證券經紀商受託契約準則（民 89）第 4 條中規定：「委託人以 IC 卡、網際網路等電子式交易型態委託者，證券經紀商得免製作、代填委託書，但應依時序別即時列印買賣委託紀錄，並於收市後由經辦人員及部門主管簽章，委託紀錄應含委託人姓名或帳號、委託時間、證券種類、股數或面額、限價、有效期間、受託買賣業務人員姓名或代碼、委託方式等；」「證券經紀商與採行 IC 卡、網際網路等電子式交易型態之委託人間，其有價證券買賣之委託、委託回報及成交回報等電子文件之傳輸，應使用憑證機構所簽發之電子簽章簽署，憑以辨識及確認。」

從以上條文的內容來分析，可以發現，「委託紀錄」應是用來反制投資人在事後否認曾經傳送委託單的證明，而「委託回報」則是證券商確實曾接受委託的證據。但是，委託紀錄卻是由證券商自行列印，而非由投資人產生的來源證明，另一方面，由投資人以私密金鑰數位簽署的「委託書」的證據效力如何，也應當是要明確規範的。此外，在委託書的送達證明（即委託回報）的部分，也沒有適當的設計，許多網路證券商並不會簽署委託回報回傳給投資人，而是要求投資人自行上網查看委託是否成功，對於投資人來說，即無法取得適當的送達證明。如此一來，一旦交易發生紛爭，將無法有足夠的證據資料作爲仲裁的依據。

在網路銀行方面，個人電腦銀行業務及網路銀行業務服務契約範本（財政部，民 88 年）第十六條指出「雙方應保存所有含數位簽章之電子訊息及經由網路所提供相關電子訊息之紀錄，並應確保紀錄之眞實性及完整性。客戶如未保存者，推定以銀行所保存之紀錄爲眞正。」又，在第十七條中則註明電子訊息可爲仲裁爭議的效力：「雙方同意依本契約交換之電子訊息，其效力與書面文件相同，雙方就所生之任何糾紛，於審判、仲裁、調解或其他法定爭議處理程序中，均不得主張該電子訊息不具書面或簽名要件而歸於無效或不成立。於前項之審判、仲裁、調解或其他法定爭議程序中，雙方同意相關之訊息推定以銀行保存之電子訊息紀錄證明之。銀行不得拒絕提供。」

以上的條約雖然有仲裁政策明定電子訊息的效力，在仲裁時卻以銀行的記錄爲一切證明的依據，有欠公允。也就是說銀行不必對他的行爲提出證據。在紀錄保存

的部份，也未制定交易爭議解決的安全政策；也就是說，電子訊息的證據力仍需要更明確的規範。

二、網路金融交易爭議解決機制之探討—以網路下單爲例

臺灣證券交易所股份有限公司證券經紀商受託契約準則只是供證券商參考依據的準則，各證券商對於電子交易帳戶可能會有另外簽定同意書等不同的作法。目前，網路下單的一般流程如下所示：

(1)投資人向網路證券商申請數位憑證及私密金鑰。

(2)投資人進入網路證券商網站隨網路下單網頁，在網頁中填寫買賣委託單，包括股票代號、股票種類、交易性質、買賣張數等資料，並對買賣委託單進行數位簽章。

(3)前項資料經由網際網路傳輸至網路證券商之網路下單伺服器。

(4)網路下單伺服器檢查傳輸之下單資料、憑證及金鑰資料是否正確。

(5)正確下單資料傳輸至證券交易所連線下單端末機，向證券交易所申報買賣有價證券。

(6)證券交易所接受買賣資料，進行交易撮合。證券交易所將交易撮合結果傳輸網路證券商，完成網路下單交易。證券商將交易撮合結果回報投資人。

根據目前的流程來看，本文建議證券經紀商首要應制定爭議解決機制所應依循的安全政策：

(1)收集證據的規則：何種事件必須紀錄證據，由誰產生證據，產生證據的程序等皆需要明確訂立。例如，投資人委託交易是必須建立證據的事件，此證據由委託人自行產生或要求第三者的協助也必須明確規範。

(2)驗證證據的規則：明確規範負責檢驗證據的機構、檢驗的程序、有效證據的要件等。

(3)儲存證據的規則：證據的存放地點、儲存媒體等相關事項。

(4)證據的使用規則：誰是證據的使用人、證據的取用限制等。

(5)仲裁政策：當有爭議發生時，證據的效力如何（即那一種證據可以證明什麼事件），由誰負責仲裁等均應加以適當的確立。

除此之外，證據的內涵也應適當地設計。必須使得投資人在事後無法否認其曾經提出委託，證券經紀商也不能否認他未接收委託，而未盡其責。由於現行的網路下單是應用公開金鑰密碼學方法，參與的個體必須申請數位憑證 (digital certificate)，故此機制以非對稱式密碼學方法爲應用環境，並依循正在立法院審議的電子簽章法草案（民 88 年）。

在這個機制中，委託紀錄爲「來源證明」，委託回報爲「送達證明」。圖 4 爲網路下單爭議解決機制的示意圖。

圖 4 網路下單的爭議解決機制

爲了強制產生來源證明與送達證明，並達成證據傳遞的「公平性」(fairness)，在這個機制中引入時戳服務中心 (Time Stamping Authority, TSA) 爲有效證據的產生者。以下說明 圖 4 機制運作所遵行的詳細程序：

(1.a) 投資人 (C) 以其私密金鑰數位簽署委託書 (m) 與發出委託書的時間 (t_m) 給證券經紀商 (S)。延用標準的符號表達方式，可表示爲 $(m, t_m) \| SGNc(m, t_m)$。

(1.b) 投資人將他發出委託書的事實傳送給時戳服務中心 (TSA)，要求產生具有效力的來源證明。〈委託記錄'〉 $= z^* \| SGNc(z^*)$，$z^* = (f_1, C, S, TSA, t_m, H(m, t_m))$；其中，$f_1$ 指出此一證據代表的是來源證明，$H(m, t_m)$ 則是委託書與委託時間的

訊息摘要。

(2.a) 網路證券商驗證 C 的簽章，即驗證訊息的眞確性。並取得 $H(m', t'_m)$。

(2.b) 網路證券商將委託回報 (R) 提供給 TSA，要求 TSA 對委託回報附加時戳，並副署簽章。〈委託回報'〉 = $r^* \| SGNS(r^*)$，$r^* = (f2, S, C, TSA, tr, H(m', t'_m))$；其中，f2 指出此一證據代表的是送達證明，tr 爲證券商收到委託書的時間。

(3.a) TSA 收到證券經紀商的〈委託回報'〉後，取得 $H(m', t'_m)$，與先前由投資人處傳送過來的 $H(m, t_m)$ 加以比對，若二者相同，則填入時戳，並予以簽章，產生具有證據效力的〈委託紀錄〉與〈委託回報〉。

〈委託紀錄〉 = $z \| SGNTSA(z)$，$z = z^* \| SGNC(z^*) \| t_{g1}$

〈委託回報〉 = $r \| SGNTSA(r)$，$r = r^* \| SGNS(r^*) \| t_{g2}$

其中，t_{g1} 與 t_{g2} 即爲由 TSA 分別在〈委託紀錄'〉與〈委託回報'〉填入的時戳。

(3.b) TSA 將已完成的〈委託紀錄〉傳送給網路證券經紀商。

(3.c) TSA 將已完成的〈委託回報〉傳送給投資人。

(4.a) 投資人檢驗〈委託回報〉的有效性。

(4.b) 網路證券商檢查〈委託紀錄〉的有效性。

以上程序中，步驟 3.b 與 3.c 必須同時執行，方可達到公平性的要求。

在這個機制中，TSA 負責爲交易雙方的證據加上時戳，並負責傳送有效力的證據給交易的雙方，但證據應由交易雙方自行負責儲存與保管。

以上所提出的機制是爲了達到強制發送來源證明與送達證明，以及公平的證據交換。但如果爲了方便、簡單，也可以由交易雙方自行交換證據；則流程可以簡化如下：

(1)投資人將委託書 (m) 連同〈委託紀錄〉傳送給網路證券商。委託紀錄的內容爲 $z \| SGNc(z)$，$z=(f_1, C, S, t_m, t_{g1}, H(m))$。

(2)網路證券商製作〈委託回報〉回傳給投資人。〈委託回報〉 = $r \| SGNs(r)$，$r = (f_2, S, C, tr, t_{g2}, H'(m))$

若以不可否認服務的四個工作階段來說明，圖 4 中的第(1)、(2) 步驟乃是證據的產生階段，而 (3)、(4) 步驟則是證據的傳遞與儲存階段。一旦有委託行爲上的

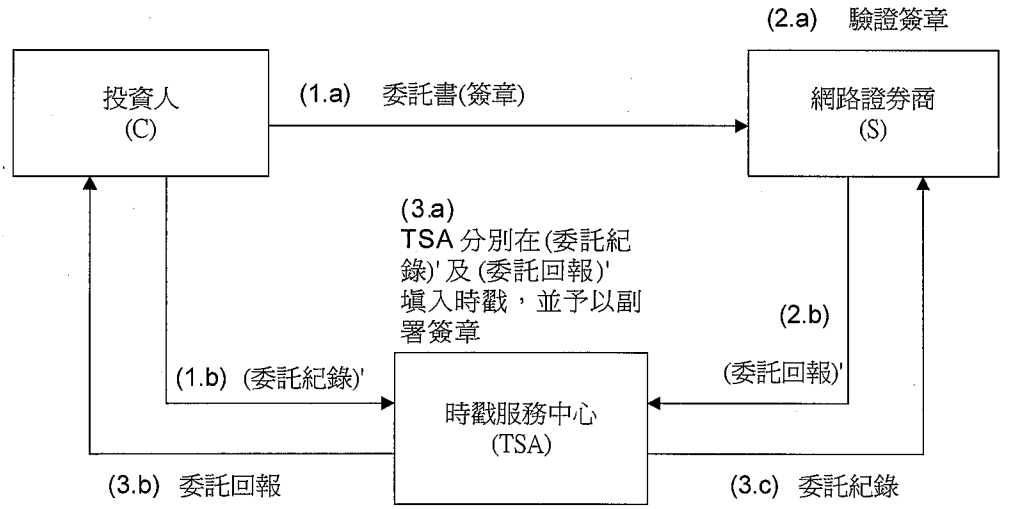

圖4 網路下單的爭議解決機制

糾紛發生時，交易的雙方可以要求提出彼此所持有的證據（若是證據由第三者保管儲存，則進入證據取用的階段），並要求檢驗證據的有效性（此即證據檢驗的階段），最後，再依據證據，進入仲裁爭議的程序。在本例中，證券經紀商可以提出〈委託紀錄〉證明投資人確實曾經進行證券交易的委託，使投資人無法否認；另外，證券經紀商如果沒有依據投資人的要求，將正確的下單資料傳輸至證券交易所連線下單端末機，則投資人可以提出〈委託回報〉作爲證據，使證券經紀商不得以未收到委託書爲藉口。也就是說，只要投資人或經紀商任一方有能力提出〈委託回報〉或〈委託紀錄〉，即可仲裁此筆證券交易委託是成立的。

以目前的應用來看，投資人與網路證券經紀商、或網路銀行與其客戶之間是以存在相當程度的信賴感爲基本假設，這樣的假設對投資人或銀行客戶來說，卻比較不公平。本文提出的機制可以在交易雙方有爭議時，提供明確的證據，保障彼此之間的權益，並增進交易的公平性。如果採用本文的建議，TSA 可以是一個經過權責機構檢驗合格的「時戳服務器」，以保證它的安全性與可信賴性，它具備防僞、防破壞之硬體裝置，就像是飛機上的飛行記錄器（俗稱黑盒子），可用於記錄飛行事過程的事件。

陸、結論

在傳統的商業社會裏，已使用契約等方式規範商業行爲的不可否認性，提供交易的爭議解決機制。同樣地，在新的電子商務的環境中，商業行爲的有效運作也必須依賴一套爭議解決機制，然而，電子商業交易的爭議解決機制是應用導向的，與商業環境的特性、法律規範等有相當程度的關連。設計這樣的機制時，不僅要考慮法律層面的規範，也要考量商業習慣、證據當事人與證據使用者之間信任關係等議題。本文依據相關的國際標準與研究文獻，提出電子商業交易爭議解決機制的系統概念與一般參考模型；並以網路金融爲例，提出一可適用於網路下單的爭議解決機制，使得交易雙方可提出證據證明對方已收到資訊，也確保網路證券經紀商「通知」及「投資人取得資訊」的要求獲得滿足。

在現行的實務系統中，通常僅以「數位簽章」做爲傳遞文件、訊息時的證據，但缺少安全政策的制定，則其所具備的證據力將略顯不足。因此，如何衡量速度、效率、成本、公平性及前述的相關重要考量，制定適當的安全政策，設計實用的爭議解決機制，將其整合於現有電子商務環境的交易流程之中，可說是未來進一步的研究議題。

參考文獻

1. 財政部金融局，民 88，『個人電腦銀行業務及網路銀行業務服務契約範本』，4 月 25 日，http://www.boma.gov.tw/8872563-1.htm。
2. 黃景彰，民 90，資訊安全？電子商務之基礎，華泰書局：即將出版。
3. 電子簽章法草案，中華民國行政院第 2611 次院會，民 88 年 12 月 23 日。
4. 臺灣證券交易所股份有限公司，民 90，『證券經紀商受託契約準則』。2 月 10 日，http://www.selaw.com.tw。
5. Coffey, T., & Saidha, P. 1996. Non-repudiation with mandatory proof of receipt. Computer Communication Review, 26(1), 6-17.
6. ISO/IEC JTC 1. 1997a. Information technology - Open systems interconnection - Security frameworks for open

systems: Non-repudiation framework (ISO/IEC 10181-4).

7. ISO/IEC JTC 1. 1997b. Information technology - Security techniques - Non-repudiation - Part1: General. (ISO/IEC 13888-1).

8. ISO/IEC JTC 1. 1997c). Information technology - Security techniques - Non-repudiation - Part2: Mechanisms using symmetric techniques. (ISO/IEC 13888-2).

9. ISO/IEC JTC 1. 1997d. Information technology - Security techniques - Non-repudiation - Part1: Mechanisms using asymmetric techniques. (ISO/IEC 13888-3).

10. McCullagh, A., & Caelli W. 2000. Non-repudiation in the digital environment. First Monday, 5(8). Retrieved February 15, 2001, from the World Wide Web: http://www.firstmonday.dk/issue5_8/mccullagh/index.html

11. You, C. H., Zhou, J., &Lam, K. Y.1998. On the efficient implementation of fair non-repudiation. Computer Communication Review, 28(5), 50-60.

12. Zhou, J., & Gollmann, D. 1997a. Evidence and non-repudiation. Journal of Network and Computer Applications, 20(3), 267-281.

13. Zhou, J., & Gollmann, D. 1997b. An efficient non-repudiation protocol. Proceedings of 10th IEEE Computer Security Foundations Workshop, 126-132.