一個電子化商業交易的證據管理架構與應用於網路金融服務之研究

學生：沈曉芸　　指導教授：黃景彰

國立交通大學資訊管理研究所

中文摘要

電子商務是在二十世紀末期出現的新的商業活動方式，如同傳統的商業活動，電子化商業交易的「爭議」是無可避免的。因此，一個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，取出證據以為依循的爭議解決機制，是電子商務的環境所必須建立的。

「證據」是爭議解決機制中的關鍵要素。本論文以相關的國際標準與學術文獻為理論背景，歸納出一個解決電子化交易爭議所必需的證據管理之依據，提出本文的證據管理概念架構，並依據所應用的密碼學方法環境，與可信賴第三者參與的模式建構出證據管理的一般化模型。此外，基於前述證據管理的一般化架構，以最適合網路交易的行業之一的金融服務為背景，並參酌國情，以現行契約準則及電子簽章法為依據，針對臺灣網路證券下單作業、網路銀行的轉帳交易、與電子支票付款系統設計出合宜適用的交易證據管理機制。

其中，在電子支票系統部份，本論文自系統流程的角度重新思考，結合證券市場之有價證券的集中保管作業方式與電子化商業交易之證據管理模型，設

計出一個「集保型」的電子支票系統模型，避免支票在市場上流通，以降低電子支票因數位文件本身的可複製特性所帶來的風險，同時融合資訊安全觀點與現有支票業務流程，建構一個能支援多種商業模式的連線付款工具之基本流程與安全的模型，使企業與消費者皆能更便利且有效率地進行網路商業活動。

關鍵字： 電子化交易證據管理、爭議解決、網路下單、網路銀行、電子支票系統、集中保管

An Evidence Management Conceptual Framework in Electronic Commerce for Network Financial Banking Services

Student: Shen, Hsiao Yun Advisor:Hwang, Jing Jang

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, 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.

Since “evidence” is the key to resolve disputes, generalized from relevant international standards, an evidence management conceptual framework is proposed in this study for disputes resolution. Several proposed generic models in the framework are classified according to Trusted Third Party (TTP) involved and their underlying cryptography—symmetric or asymmetric cryptography. Then the models are applied to define three adapted schemes that would help to resolve disputes

arising from on-line trading in the Taiwan securities market, or network banking, or electronic payment systems.

For electronic payment systems, a “central-deposit” electronic check system model is proposed in this study. The basic idea was obtained from observing the central depository system for equity securities in Taiwan and the evidenceu management framework as above. By including a “Central Payment Center (CPC)” into the proposed model, electronic checks generated are registered and kept at a location instead of being circulated. The major benefits of the Central Depository Model include reduction of both cost and risk.

Keywords: Evidence management for electronic transactions, disputes resolution, network banking, network securities trading, electronic check, central depository model.

誌　謝

歷經漫長的研究過程，如今能夠完成我的論文，首先要感謝指導教授黃景彰老師的悉心指導。尤其是老師豐富的經驗、宏觀的視野、與嚴謹的治學態度讓我受益良多，使我在此期間學習到獨立、嚴謹的研究精神與寫作的技巧，從今而後也可以在寬廣的研究領域上自由發揮。在此謹致上我最誠摯的感謝之意。

也由衷地感謝論文口試委員吳壽山老師、王素華老師、陳安斌老師與劉敦仁老師對論文的詳細審閱與費心指導，並提供了許多寶貴的意見，讓我的博士論文得以更加完善。此外，感謝本所的各位老師在專業領域上之學術理論上的指導。

除了師長的教導與指正，我也要感謝本所諸位優秀同學們在研究期間於學業與生活上的相互支援。尤其是在多年的實驗室生活中一起進行學術討論、分享喜怒哀樂、與相互鼓勵的同窗夥伴們 — 鵬雲、怡鎮、鍾斌、俊龍、慈章、敏華、文宏等人，使得我得以在十分和諧與融洽的環境中進行研究。也謝謝本所助理淑惠在許多事務上的幫忙。

最後，更要感謝我的父母與家人一路上的支持。父母的照顧支援，姐妹的手足之情，尤其是我的先生碩源對我耐心的鼓勵與支持，讓我能夠無後顧之憂地攻讀學位。如今，完成學業，論文付梓，謹獻上最真誠的謝意給我親愛的家人，並與他們分享這喜悅的一刻。

目　錄

圖 目 錄

表 目 錄

第 1 章 緒論

1.1 研究背景、動機

進入二十一世紀，電子化商務已然成為人類社會新的商業活動方式，此種透過網際網路進行商業交易的模式也對許多產業造成了影響與衝擊。雖然 2000 年中開始發生的網路股災使得許多的網路公司 (dot-coms) 陷入經營上的重大危機，電子商務的發展似乎也陷入了低潮。但根據市場研究公司 Ipsos-Reid 以十二個國家為樣本的調查研究指出， 54% 受訪者有連網行為，在上網族群中 62% 曾經在網路上購買商品及服務 (劉芳梅，民 92)，這顯示人們已透過網際網路將生活與商務活動緊密地串接在一起，2003 年 5 月份的商業周刊也專文報導了電子商務的蓬勃生機 (Mullaney, 2003)。網路銀行、網路下單、線上購物、網路拍賣、企業快速回應系統、供應鏈管理、客戶關係管理等新的企業經營模式已經進入了人們的日常生活當中，而已在市場上具有一席之地的企業也必須透過電子化進一步地提升其競爭力。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，或是參與商業行為的任何一方對其行為加以否認，將會造成商業上的糾紛，再加上全球電子商務無地域國界的特性，使得商業交易的爭議處理較傳統更為複雜。因此，一套公平便利的爭議解決機制，在電子商務的環境中是不可或缺的。

為建立交易個體對網路交易的信心，美國聯邦貿易委員會 (Federal Trade Commission, FTC)、全球電子商務論壇 (Global Business Dialogue on Electronic

Commerce, GBDe)、經濟合作發展組織 (The Organization for Economic Co-operation and Development, OECD)、美國仲裁協會 (American Arbitration Association, AAA)、及美國律師協會 (American Bar Association) 等組織已積極支持並推動線上替代性爭議解決機制 (Online Alternative Dispute Resolution, ADR) 的發展 (FTC/DOC, 2000；GBDe, 2000；OECD, 2001)，以期在法庭之外，解決因商業行為而產生的紛爭。

要解決商業糾紛，交易行為的「證據」可以說是關鍵之鑰。依據留存的證據，可以在事後證明事件發生的真實性，而交易的參與者則可以引用證據來解決具爭議性的事項。目前實務上的電子商務系統對於電子化商業交易的爭議解決著墨並不多，因而引發本論文在電子化商業之交易證據管理的議題上深入研究的動機。

1.2 研究目的、方法

本論文的研究目的在於建構一個電子化商業的交易證據管理之概念架構。此架構中描述交易證據處理的工作階段、相關的參與者、以及證據的技述分類與內涵，並依據可信賴第三者的介入模式與所應用的密碼學方法環境 — 對稱式與非對稱式密碼學方法 — 針對交易證據處理的工作，提出基本的運作流程與參考模型。

而無論是傳統或是電子化的商業活動中，金融服務都是不可缺少的必備條件，如何使得金流能夠順暢的運轉，已成為重要的課題。再者，包括網路銀行、網路證券、電子支付系統 (electronic payment) 等金融服務亦可說是最適合網路

交易的行業之一。故以網路金融服務為背景，對網路下單、網路銀行交易與電子支票支付系統等相關領域提出證據管理的應用模式，也是本論文的研究重點。

本論文所採用的研究方法與步驟說明如下：

(1) 事件發生之不可否認服務 (non-repudiation) 的目的在於提供交易證據，以支援爭議的處理，故本論文廣泛蒐集並深入研究相關之國際標準與學術文獻；

(2) 研析事件發生之不可否認服務之特性與基本運作方法；

(3) 探討國內網路金融服務相關事項的作業模式、流程，與規範；

(4) 研析現行已發展之電子支票系統的運作架構與機制；

(5) 透過系統思考 (system thinking) 的方法，建構本論文所希望發展出來的架構與參考模型，並以網路金融服務為應用背景，設計證據管理之機制。

1.3 研究範圍與限制

本論文的研究範圍著重於電子化交易爭議解決機制中一系列證據處理的工作，設計交易證據管理之概念架構，而未涵蓋爭議解決機制中仲裁政策的制定與法律上的議題。

而在應用層面上，係以網路證券的下單作業、網路銀行之轉帳交易事項、及電子支票系統為應用背景，設計其所需的交易證據管理事項以及證據內容的建議。此外，本論文的研究係以概念化架構與系統化的思考為重點，故僅提出運作的模型，而未涉及系統的實作。

1.4 論文章節概述

本論文分為六章，各章的內容分別敘述如下：

第 1 章、緒論： 本章分別說明本論文之研究背景與動機、研究之目的與研究方法、研究的範圍、限制，以及論文之章節概述。

第 2 章、事件發生之不可否認服務：主要在於自技術面探討事件發生之不可否認服務的國際標準與相關文獻。

第 3 章、一個電子化商業交易的證據管理概念架構：本章提出一個電子化商業的交易證據管理之概念架構。此架構的內涵主要根據相關國際標準歸納出電子化商業交易證據處理的工作階段、列舉其參與的角色，並歸類網路上訊息往來所需要產生的證據類型。此外，在此架構下，取決於所使用的密碼技術，將證據分為「簽章式證據」與「封條式證據」，並依據所使用的密碼學技術與可信賴的第三者 (Trusted Third Party; TTP) 之介入模式分別提出一般化的參考模型。

第 4 章、網路金融交易的證據管理機制：本章主要探討國內網路證券與網路銀行的運作方式與網路金融相關事項的規範，並自爭議解決機制的觀點出發，參酌國情，針對網路證券下單與網路銀行轉帳交易事項，提出證據處理階段的相關事項與運作模型之建議，設計出合宜的交易證據管理機制。

第 5 章、集中保管的電子支票系統模型：本章之目的在於深入探討、研析現行已發展之電子支票系統的運作機制，自系統流程的角度重新思考，並延伸本論文所提出的證據管理概念架構中的模型，同時結合證券市場之有價證券的集中保管作業方式，設計一「集保型」的電子支票系統模型。同時，融合資訊安全之觀點，儘量避免支票在市場上流通，以

降低電子支票因數位文件本身的可複製特性所帶來的風險，以建構一個能支援多種商業模式的安全的連線付款工具之基本模型。

第 6 章、結論與討論：本章提出本論文之結論與未來研究之建議。

第 2 章 事件發生之不可否認服務

交易證據可為特定的事件或行為建立責任的歸屬 (accountability)，使得在網路環境中參與的個體無法否認其所從事的行為，因此，為商業交易或訊息傳遞行為提供證據的安全服務是不可忽視的。一系列證據處理的工作與提供證據解決交易紛爭的服務，即稱之為「事件發生之不可否認服務」 (non-repudiation)。本章的主要內涵即在於自技術面探討事件發生之不可否認服務的國際標準與相關研究文獻。

2.1 事件不可否認服務的基本概念

根據國際標準組織 (International Organization for Standardization ((ISO)) 與國際電工協會 (International Electrotechnical Commission (IEC)) 所制定的標準文件 ISO/IEC 10181-4 (ISO/IEC JTC 1, 1997a) 所述，不可否認服務的目的乃是在訊息傳遞的過程中產生、蒐集、記錄證據，並維持其可用性及有效性，並在爭議發生時，取出證據加以驗證以解決爭議。此標準文件同時定義了不可否認服務的基本架構 — 證據處理階段與爭議解決階段，並提出一些不可否認服務所需具備的安全資訊、管理功能、及可行的實施方法。

圖 2-1 及圖 2-2 分別為 ISO/IEC 10181-4 所定義的不可否認服務在證據處理階段以及爭議解決階段的基本架構。

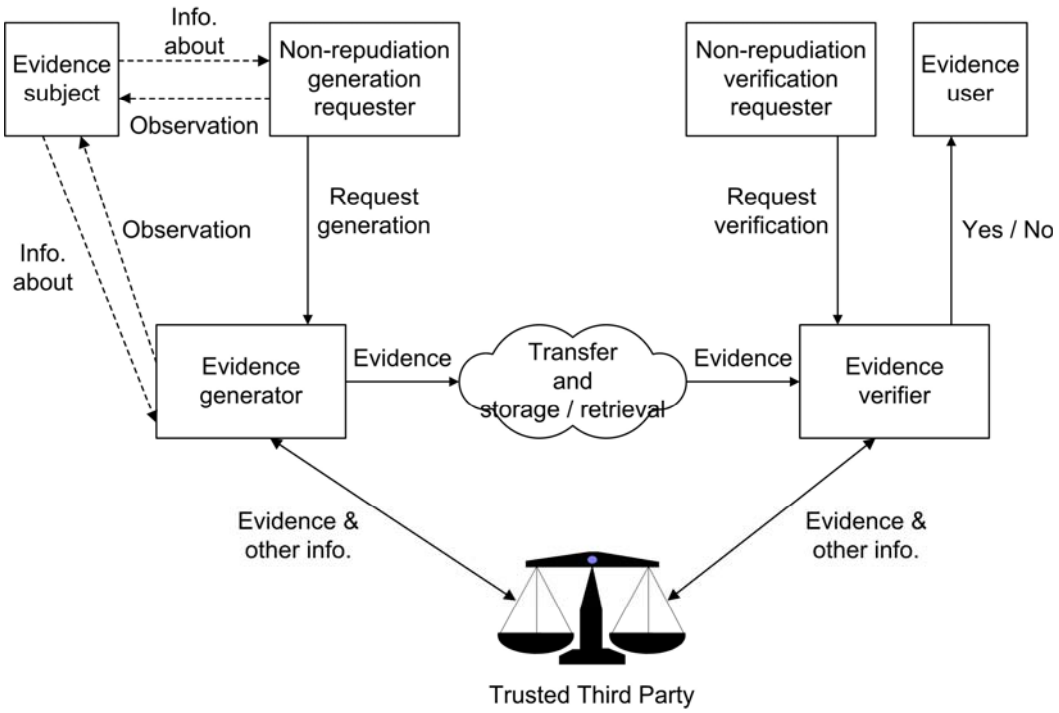

圖 2-1　不可否認服務的基本架構—證據處理階段

(資料來源: ISO/IEC 10181-4 (ISO/IEC JTC 1, 1997a))

基本上，不可否認安全服務由以下四個階段所組成：

(1) 證據 (Evidence) 的產生階段：在此階段，證據要求者 (Evidence Generation Requester) 要求證據產生者 (Evidence Generator) 產生證據以證明特定事件的發生。證據產生後，再由二者共同檢驗所產生的證據。

(2) 證據的傳遞、儲存及取回：證據產生者將證據送給證據驗證者 (Evidence Verifier)。在此階段，證據產生者可將證據直接傳遞給驗證者，或是將證據儲存起來，再由證據驗證者取出。

(3) 證據的驗證階段：此階段的主要目的是讓證據使用者 (Evidence User) 在必要時，可向證據驗證者提出驗證的要求，以證明所提供的證據是值得信賴的。在此，可信賴的第三者 (Trusted Third Party; TTP) 可以參與提供驗證證據所需的資訊。

(4) 爭議的解決：當有爭議發生時，由一受爭議雙方信任的仲裁者自爭議雙方或 TTP 處蒐集證據，並依照雙方共同接受之不可否認性服務政策進行仲裁以解決爭議。在沒有爭議時，此階段可以不必執行，但是所有的不可否認性安全服務機制都必須能夠支援爭議的解決。

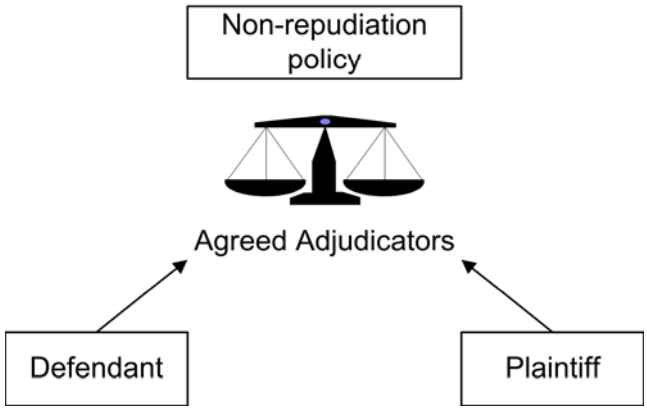

圖 2-2 不可否認服務的基本架構—仲裁階段
(資料來源: ISO/IEC 10181-4 (ISO/IEC JTC 1, 1997a))

除了 ISO/IEC 10181-4 之外，另一與不可否認服務相關的系列標準文件是 ISO/IEC 13888 (ISO/IEC JTC 1, 1997b, 1997c, 1997d) 。ISO/IEC 13888 共由三個部份所組成：

- ISO/IEC 13888-1 (General)：一般化的不可否認服務架構；
- ISO/IEC 13888-2 (Mechanism using symmetric techniques)：使用對稱式密碼技術實作的不可否認服務機制；
- ISO/IEC 13888-3 (Mechanism using asymmetric techniques)：使用非對稱式密碼技術實作的不可否認服務機制。

此系列文件更詳盡地定義與討論不可否認服務的種類、參與者、及其核心元件—證據，同時，也提出在不同密碼學環境下實現此服務的方法。其中，證

據產生階段的參與者包含了證據提供者、證據主體 (evidence subject) 以及證據產生者，證據使用者及證據驗證者則會參與於證據驗證階段，此外，在各個階段，皆可能有可信賴的第三者 (TTP) 協助證據的產生及驗證工作。

2.2 不可否認服務的種類

在不可否認服務的一般模式中，必須具備六項基本的服務 (ISO/IEC JTC1, 1997b; Bhattacharya & Paul, 1999)：

- 對於建立訊息無法否認的安全服務 (non-repudiation of creation)；
- 對於傳送訊息無法否認的安全服務 (non-repudiation of sending)；
- 對於收受訊息無法否認的安全服務 (non-repudiation of receipt)；
- 對於得知訊息無法否認的安全服務 (non-repudiation of knowledge) ；
- 對於傳遞訊息無法否認的安全服務 (non-repudiation of submission) ；
- 對於轉送訊息無法否認的安全服務 (non-repudiation of transport)。

根據此六項基本的服務，尚可延伸出其他的不可否認服務種類。以下為分四種特定常用的服務：

(1) 具有來源證明的不可否認性服務 (Non-repudiation of Origin)：此項服務旨在防止訊息建立者否認其建立及傳送訊息。

(2) 具有收文證明的不可否認性服務 (Non-repudiation of Delivery)：此項服務旨在防止訊息的接收方在收到訊息並得知其內容後卻加以否認。

(3) 具有傳遞證明的不可否認性服務 (Non-repudiation of Submission)：若有一個訊息的傳遞者 (delivery authority) 負責在收送雙方間傳遞訊息時，此項服務提供適當的證據，以防止傳遞者否認其曾經接受訊息傳遞要求的事實。

(4) 具有送達證明的不可否認性服務 (Non-repudiation of Transport)：當介入收送雙方間傳遞訊息的傳遞者確實已將訊息送交至接收方，此項服務可以提供適當的證明防止接收者對於其已收到訊息的事實加以否認。

為提供各項不可否認服務，必須透過提出適當的證據來達成 (Zhou & Gollmann, 1997a)。圖 2-3 說明可達成上述四項特定服務之實例。

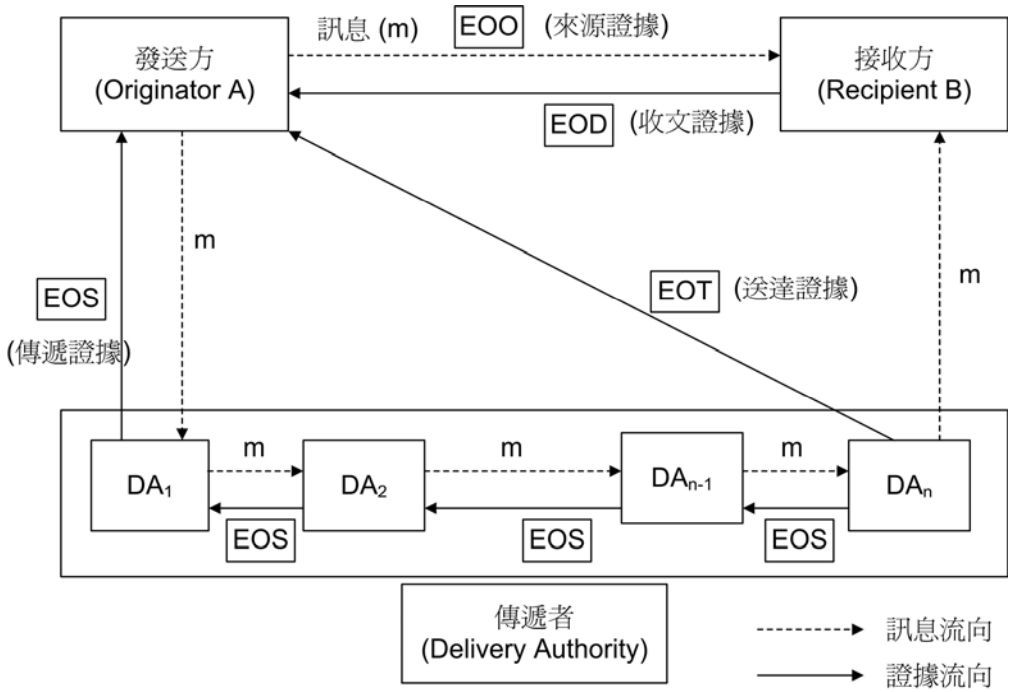

圖 2-3 四種特定不可否認服務示意
(資料來源: 修改自 ISO/IEC 10181-4 (ISO/IEC JTC 1, 1997a))

來源證據 (Evidence of Origin; EOO)、收文證據(Evidence of Delivery; EOD)、傳遞證據 (Evidence of Submission; EOS) 及送達證據 (Evidence of Transport; EOT) 分別用以提供具有來源證明、收文證明、傳遞證明、及送達證

明的不可否認服務。

各項服務所提供之證據的時序圖則如圖 2-4 所示。

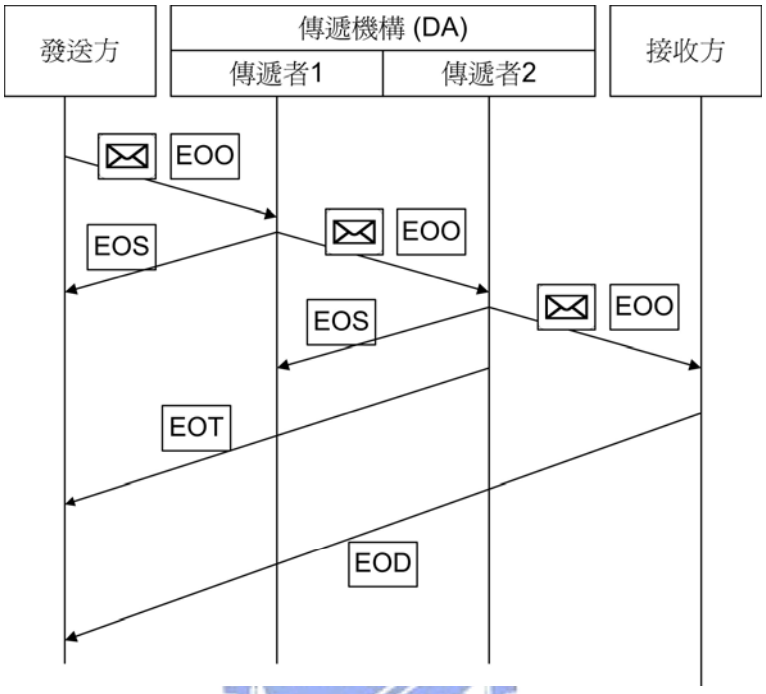

圖 2-4　不可否認服務證據傳遞時序圖
(資料來源: 修改自 ISO/IEC 10181-4 (ISO/IEC JTC 1, 1997a))

2.3　不可否認服務的核心元件 — 證據

在 ISO/IEC 13888-1 (ISO/IEC JTC 1, 1997b) 中分別描述了一般性的證據 (generic non-repudiation token; GNRT)、時戳證據 (time stamping token; TST) 及公證證據 (notarization token; NT) 等三種類型的證據。其中，一般性及其所衍生的證據 (如來源證據、收文證據等) 是由證據產生者所建立，而時戳證據是由時戳中心 (Time Stamping Authority; TSA) 所產生，公證證據則是由公證機構 (Notary Authority; NA) 建立。

1. 一般性證據 (GNRT)

在 ISO/IEC 13888-1 (ISO/IEC JTC1, 1998b) 中，一般性證據之定義為：

$$\mathbf{GNRT = text \| z \| CHK_X(z)}$$

其中，z = (Pol ‖ f ‖ A ‖ B ‖ C ‖ D ‖ E ‖ Tg ‖ Ti ‖ Q ‖ Imp(m))；$CHK_X(z)$ 為針對 z 所產生的密碼檢查值；而 text 則包含了不需要受到密碼保護的額外資訊，如一個憑證中心 (Certification Authority; CA) 的識別碼等。以下分別說明各個符號所代表的意義：

- Pol：表示應用於證據之不可否認性安全服務政策
- f：代表所提供之不可否認性服務的類型
- A：證據主題之識別碼 (distinguishing identifier)
- B：證據產生者之識別碼
- C：與證據主題互動之個體的識別碼（如訊息的發送者或傳遞者等）
- D：證據提供者的識別碼
- E：在訊息傳遞活動中，其他參與者的識別碼
- Tg：產生證據時的日期與時間
- Ti：訊息傳遞各個活動（如發文、收文）的日期與時間
- Q：一些需要受到保護的其他資訊
- Imp(m)：相關訊息的數位指紋，如以 Hash 函數產生的訊息摘要

2. 時戳證據 (TST)

時戳證據是用來更進一步地證明一般性證據的建立時間，而其乃是由可信賴的時戳中心 (TSA) 負責產生。時戳證據之定義為：

$$\mathbf{TST= text \| w \| CHK_{TSA}(w)}$$

text 與 $CHK_{TSA}(w)$ 所代表的內涵等同於一般化證據中所提及，而 w = Pol || f || TSA || Tg || Q || Imp(y)。各個符號所代表之意義分別說明如下：

- y：由要求時戳證據之個體所提供的相關資料。如發文者要求時戳中心為其所提供之來源證據 (EOO) 證明其產生的時間。
- Pol：表示應用於證據之不可否認性安全服務政策
- f：代表所提供之不可否認性服務的類型
- TSA：時戳中心之識別碼 (distinguishing identifier)
- Tg：產生時戳的日期與時間
- Q：一些需要受到保護（來源/真確性）的其他資訊
- Imp(y)：相關證據的數位指紋，如以 Hash 函數產生的摘要。

3. 公證證據

公證證據的服務係由一具有公信力的權威機構 (NA) 所提供。此機構可以負責儲存證據、管理證據的有效性及註銷證據等。公證證據之定義為：

$$\mathbf{NT= text \| w \| CHK_{NA}(w)}$$

其中，w= Pol || f || X || NA || Tg || Q || Imp(y)。

- y：由要求公證證據之個體所提供的相關資訊。其可以是一個訊息、一個不可否認性服務的證據、訊息摘要，或是任何服務要求者所希望由 NA 所簽證的資訊。
- Pol：表示應用於證據之不可否認性安全服務政策
- f：代表所提供之不可否認性服務的類型
- X：為要求公證服務的使用者識別碼
- NA：具有公信力的權威機構之識別碼 (distinguishing identifier)
- Tg：NA 執行公證服務的日期與時間。
- Q：一些需要受到保護（來源/真確性）的其他資訊
- Imp(y)：相關資訊的數位指紋，如以 Hash 函數產生的摘要。

安全信封 (secure envelope; SENV) 與數位簽章 (digital signature; SIG) 乃分別使用於對稱式及非對稱式密碼學方法來提供與驗證以上所述證據的基本方法。

2.4 不可否認服務的機制與協定

ISO/IEC 13888-2 (ISO/IEC JTC1, 1998c) 中建議了兩個使用對稱式金鑰密碼技術以達成具有強制性之來源及收文證明的不可否認服務的實施方法。Zhou & Gollmann (1996) 所提出的公平的不可否認性服務協定，旨在使得訊息發送雙方在協定執行的任一階段都不能夠取得任何可能具有否認性的優勢。Coffee &

Saidha (1998) 則提出之一具時戳之不可否認性安全服務的協定，其主要目的乃為達成具有強制性來源及收方證明的不可否認性服務。

2.4.1 ISO/IEC 13888-2 使用對稱式金鑰密碼技術實作之機制 (1)

圖 2-5 為 ISO/IEC 13888-2 所建議之使用對稱式密碼技術實作不可否認安全服務之機制(1)。

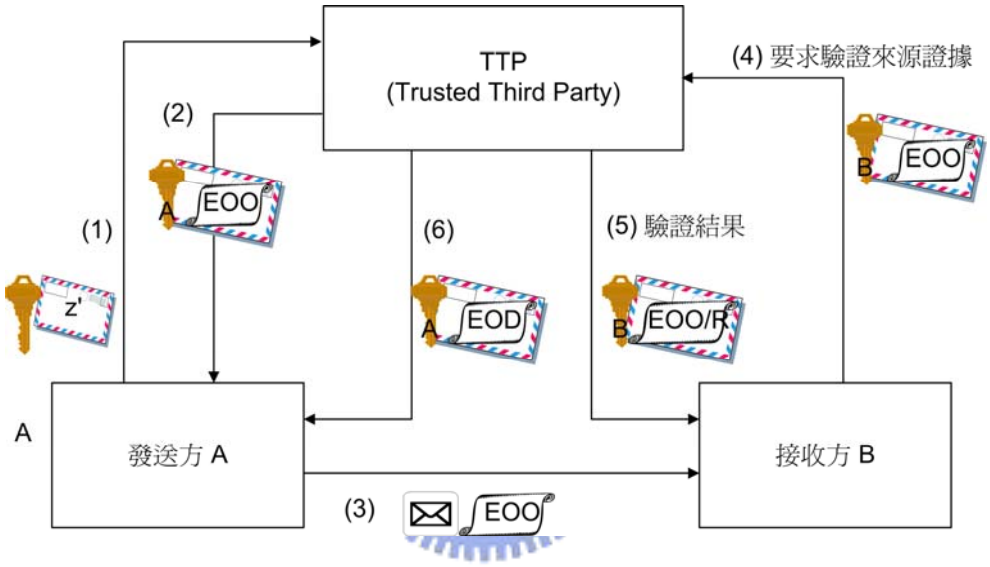

圖 2-5 ISO/IEC 13888-2 使用對稱式金鑰密碼技術實作之機制 (1)
(資料來源: 修改自 ISO/IEC 13888-2 (ISO/IEC JTC 1, 1997c))

其實施階段如下：

(1) 發送者 A 首先使用秘密金鑰 (secret key) 產生一個安全信封 $SENV_A(z') = y \| MAC_A(z')$，z'之格式如 1.3 節中所述，但在此處，z'中的 Tg 尚未形成。並將此信封傳送給 TTP，以要求產生來源證據。

(2) TTP 使用秘密金鑰與 MAC 重新計算 z' 的檢查值與信封內的 z' 互相比對，以檢驗此安全信封。驗證成功後，TTP 將 Tg 加入 z 中，並使用與發送方共同持有的秘密金鑰計算出一密碼檢查值 $MAC_{TTP}(z)$ 後，並產生來源證

據 EOO = text ‖ z ‖ MAC_{TTP}(z)，而後建立安全信封 $SENV_A$(EOO)，並傳送給 A。當 A 收到 $SENV_A$(EOO) 時，以同樣的方法檢驗信封。

(3) A 將訊息 m 及 EOO 一起送給接收方 B。

(4) B 收到 EOO 後驗證第三節所述之 Imp(m)，同時使用 secret key b 產生 $SENV_B$(EOO)，並傳送給 TTP，要求驗證來源證據 EOO 的合法性。

(5) TTP 接著會以 key b 檢驗信封，並以 key ttp 驗證 EOO。若兩者皆驗證成功，則 TTP 會產生並儲存收文證據 EOD 並將驗證結果 PON、EOO 與 EOD 一起放入安全信封 $SENV_B$(PON ‖ EOO ‖ EOD) 傳送給 B；假設 EOO 驗證無效，則 TTP 則傳回 $SENV_B$(PON ‖ EOO)。如果 B 接收到後者，則整個通訊就此結束。

(6) 一旦 TTP 傳送 EOD 給 B 後 (Step 5)，也會立刻利用 key a 傳送 $SENV_A$(EOD) 給 A。A 在收到此安全信封後，會進行檢驗的工作，若信封及 EOD 二者皆有效，則完成具有收文證明之不可否認性安全服務。同時，EOD 會被儲存以為將來所用。

2.4.2 ISO/IEC 13888-2 使用對稱式金鑰密碼技術實作之機制 (2)

圖 2-6 為 ISO/IEC 13888-2 所建議之使用對稱式密碼技術實作不可否認安全服務之機制 (2)。

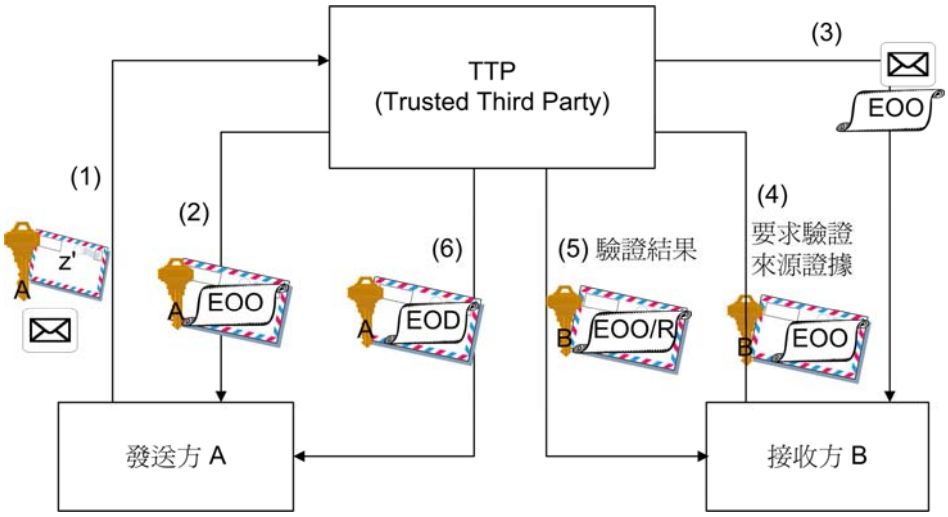

圖 2-6　ISO/IEC 13888-2 使用對稱式金鑰密碼技術實作之機制 (2)
(資料來源: 修改自 ISO/IEC 13888-2 (ISO/IEC JTC 1, 1997c))

其實施階段如下：

(1) 發送者 A 首先利用一 secret key a 產生一個安全信封 $SENV_A(z')= y \| MAC_A(z')$，z'之格式如第三節中所述，但在此處，z'中的 Tg 尚未形成。並將此信封傳送給 TTP，以要求產生來源證據。

(2) TTP 使用金鑰 a 與 MAC 重新計算 z'的檢查值與信封內的 z'互相比對，以檢驗此安全信封。驗證成功後，TTP 將 Tg 加入 z 中，並使用 secret key ttp 計算出一密碼檢查值 $MAC_{TTP}(z)$ 後，並產生來源證據 EOO= text ‖ z ‖ MACTTP(z)，而後將 EOO 放入 secret key a 產生安全信封 $SENV_A(EOO)$，並傳送給 A。當 A 收到 $SENV_A(EOO)$時，以同樣的方法檢驗信封。

(3) TTP 將訊息 m 及 EOO 一起送給接收方 B。

(4) 由於 EOO 並未以安全信封的方式傳送給 B，故 B 收到 EOO 後驗證第三節所述之 Imp(m)，同時使用 secret key b 產生 $SENV_B(EOO)$，並傳送給 TTP，要求驗證來源證據 EOO 的合法性。

(5) TTP 接著會以 key b 檢驗信封，並以 key ttp 驗證 EOO。若兩者皆驗證成功，則 TTP 會產生並儲存收文證據 EOD 並將驗證結果 PON、EOO 與 EOD 一起放入安全信封 $SENV_B(PON \| EOO \| EOD)$ 傳送給 B；假設 EOO 驗證無效，則 TTP 則傳回 $SENV_B(PON \| EOO)$。如果 B 接收到後者，則整個通訊就此結束。

(6) 一旦 TTP 傳送 EOD 給 B 後 (Step 5.)，也會立刻利用 key a 傳送 $SENV_A(EOD)$ 給 A。A 驗證成功後，則完成具有收文證明之不可否認性安全服務。此 EOD 會被儲存起來，以供未來使用。

2.4.3 一個公平的不可否認性安全服務協定

由 Zhou & Gollmann 所提出的公平的不可否認性服務協定，旨在使得訊息發送雙方在協定執行的任一階段都不能夠取得任何可能具有否認性的優勢。在這個協定中，需要有一個線上可信賴第三者的參與。圖 2-7 說明了這整個協定的實行步驟及方法。

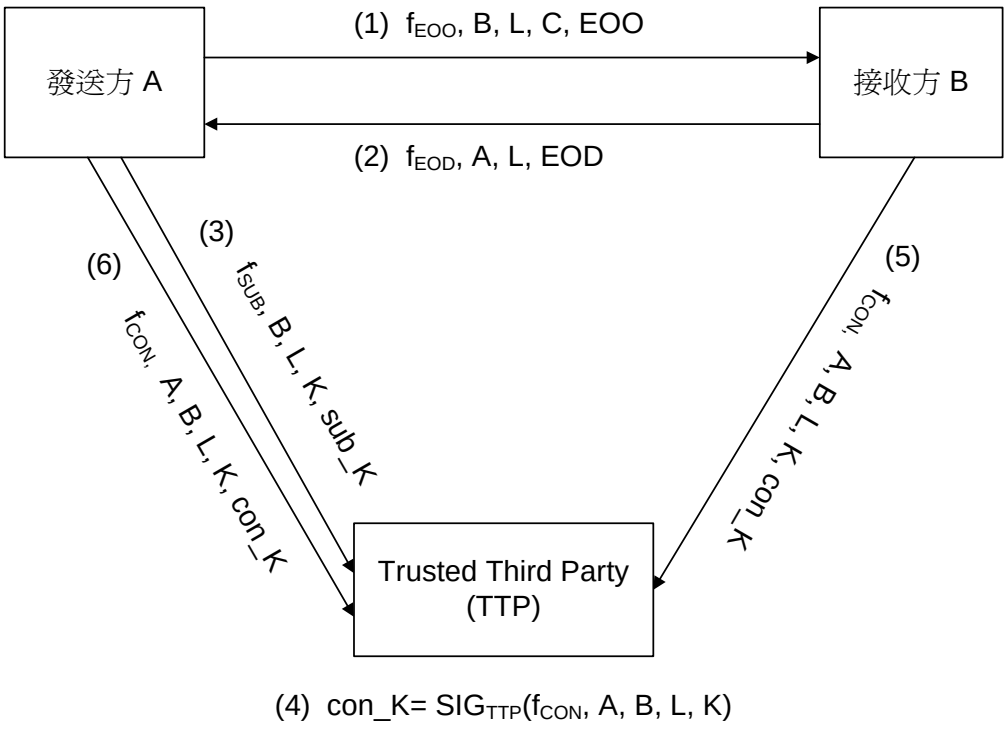

圖 2-7　Zhou & Gollmann (1996) 之公平的不可否認性服務協定

(1) A→B: f_{EOO}, B, L, C, EOO

(2) B→A: f_{EOD} A, L, EOD

(3) A→TTP: f_{SUB}, B, L, K, sub_K

(4) TTP 產生 con_k，以確認 K

(5) B←TTP: f_{CON}, A, B, L, K, con_K：B←TTP 表示 B 進行 “ftp_get TTP” 的活動。

(6) A←TTP: f_{CON}, A, B, L, K, con_K：A←TTP 表示 A 進行 “ftp_get TTP” 的活動。

以下說明在此協定中各個符號代表的意義：

- f_{EOO}, f_{EOD} f_{SUB}, f_{CON} 指示出在通訊協定中各階段訊息傳送的目的。

- A, B 分別表示訊息發送方 A 與接收方 B 的識別碼。
- K 為發送方 A 所產生之訊息金鑰 (message key)。
- C 為使用 K 將訊息 m 加密後的密文。
- L 為一連結 C 與 K 的標籤。其內容為 H (m, K)，H 表示 hash function。
- EOO 表示發文/來源證據；EOO= SIG_A(fEOO, B, L, C)，亦即使用 A 的私密金鑰 (private key) 對 (f_{EOO}, B, L, C) 簽章。
- EOD 表示收方證據；EOD= SIG_B(f_{EOD}, A, L, C)，亦即使用 B 的私密金鑰對 (fEOD, A, L, C) 簽章。
- sub_K 表示傳遞證據；sub_K= SIG_A(f_{SUB}, B, L, K) ，亦即使用 A 的私密金鑰對 (f_{SUB}, B, L, K) 簽章。
- con_K 為 TTP 所核發之確認 K 的證據；con_K= SIG_{TTP}(fCON, A, B, L, K)，即使用 TTP 的私密金鑰對 (f_{CON}, A, B, L, K) 簽章。

在此協定中，A 首先傳送訊息密文與發文證據給 B，B 收到密文後則傳送收文證據給 A，A 收到收文證據後則傳送傳遞證明 EOO 與訊息金鑰 K 給 TTP，一旦 TTP 收到 sub_K 與 K 後，則 TTP 將產生確認 K 的證據 con_K 並加以儲存。其後，B 以 ftp 方式至 TTP 處取得 K 解開密文取得訊息 m 並保有 EOO 以達成具有來源證明的不可否認性安全服務；而 A 也以 ftp 的方式至 TTP 處取得 con_k 並保有 EOD 以達成具有收文證明的不可否認性安全服務。

在這個公平的不可否認協定中，由 A 傳訊息金鑰 K 給 TTP 的過程可說是最

重要的，而在此協定中 K 的傳送過程欲沒有任何的保護。You, C. H., Zhou, J., 及 Lam, K. Y. (1998) 則針對此協定提出了一個改進的方法，說明如下：

(1) A→B: f_{EOO}, B, L, C, EOO：EOO= $SIG_A(f_{EOO}, B, L, C)$。

(2) B→A: f_{EOD} A, L, EOD：EOD= $SIG_B(f_{EOD}, A, L, C)$。

(3) A→TTP: f_{SUB}, B, $\{K\}k_{TTP}$, EOR, $Cert_B$, sub_K：在這個傳送階段，A 使用 TTP 的公開金鑰將訊息金鑰 K 加密，並加入 B 的公開金鑰憑證 (certificate) $Cert_B$，而 sub_K 的內容則改變為 $SIG_A(f_{SUB}, B, L, K, EOR, Cert_B)$。當 TTP 收到訊息後，使用其秘密金鑰解密 K，並產生 con_K= $SIG_{TTP}(f_{CON}, A, B, L, K, EOD, T_g)$，其中 T_g 為 TTP 產生 con_K 的時間。

(4) B←TTP: f_{CON}, A, B, L, K, T, con_K：B 至 TTP ftp (f_{CON}, A, B, L, K, T, con_K)，取得 K 後用以解密訊息 m。

(5) A←TTP: f_{CON}, A, B, L, K, T, con_K

在這個改善的協定中，所有的證據必須等到 con_K 產生後方才生效，而時間 T_g 也代表著訊息傳遞的時間，此外，當 $Cert_B$ 在時間 T_g 有效時，則 EOD 與 EOO 亦具有有效性。在爭議解決階段，只要 A、B 送收雙方都能夠提出 m、C、K、L、T、$Cert_A$、$Cert_B$、EOO、EOD 及 con_K 以供仲裁，則 B 將不能否認其已收到訊息 m，A 也無法否認其曾送出訊息。此外，Zhang & Shi (1996) 也曾提出一個類似的協定。

2.4.4 具有時戳之強制性收方證明的不可否認性安全服務協定

圖 2-8 為 Coffee & Saidha (1998) 所提出之具時戳之不可否認性安全服務的協定，其主要目的乃為達成具有強制性來源及收方證明的不可否認性服務。圖中之不可否認服務中心 (Non-repudiation Server; NRS) 為可信賴的第三者，會介入訊息的傳輸。其功能即在提供具有強制性具有來源及收方證明的不可否認性服務。

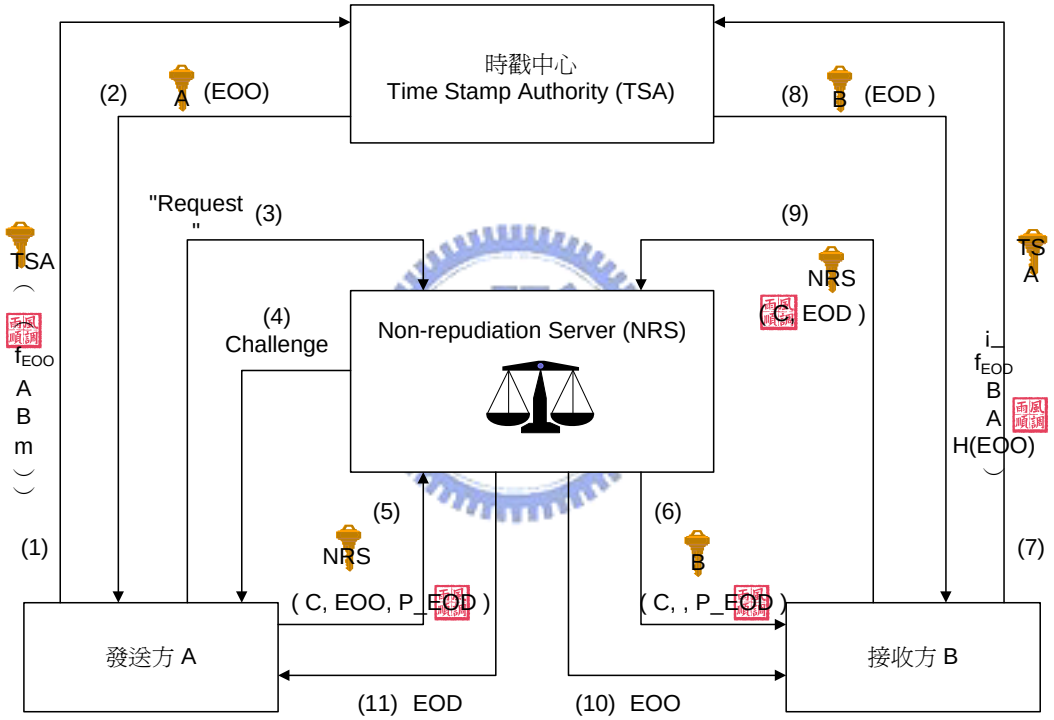

圖 2-8 Coffee & Saidha (1998) 之具時戳之不可否認性安全服務的協定

整個協定執行的步驟如下所示：

(1) A→TSA: { P_EOO} k_{TSA}：首先，A 用 TSA 的公開金鑰將部份發文證明 (Partial EOO; P_EOO) 加密後送給時戳中心 (TSA) 要求產生時戳，其中 P_EOO= $SIG_A(f_{EOO}, A, B, m)$，意即 A 用其私密金鑰對 (f_{EOO}, A, B, m) 簽章。f 用於指出不可否認性安全服務的類型，A、B 分別為發文者及收文者的識

別碼，m 則代表文件訊息。

(2) TSA→A: { EOO} k_A：TSA 在收到 A 的要求後，使用其秘密金鑰解密，並在 P_EOO 後附加一時戳 T_{g1} 然後加以簽章而形成完整的來源證據，並利用 A 的公開金鑰將此證據加密後傳送給 A。其中，EOO= SIG_{TSA}(P_EOO, TSA, T_{g1})。

(3) A→NRS: { "N_R_req" }：其後，當 A 收到加註時戳的完整來源證據 EOO 後，則送一個要求傳遞資訊服務的信息給不可否認服務中心 (NRS)。

(4) NRS→A: { challenge_A } k_A：當 NRS 收到 A 的要求時會以 A 的公開金鑰製作一個挑戰送給 A。只有真正的 A 能夠以其秘密金鑰解密並回應挑戰。

(5) A→NRS: { SIG_A(challenge_A, EOO, P_EOD) } k_{NRS}：當 A 收到 NRS 所傳送過來的挑戰時，以其私密金鑰解密，將來源證據 EOO 及部份的收文證明 (Partial EOD; P_EOD) 附於其後，並以其私密金鑰對整串訊息做數位簽章，而後以 NRS 的公開金鑰將簽章後的訊息加密，傳送給 NRS，故 NRS 在此階段會得到來源證據並加以儲存。其中，P_EOD= {f_{EOD}, B, A, H(POO) }，而 H 表示一個 hash function。

(6) NRS→B: { SIGNRS(challenge_B, P_EOD) } k_B：當 NRS 解開 P_EOD 後，將透過傳送一個挑戰及 P_EOD 給 B，以啟動收文證據 (EOD) 的產生階段。

(7) B→TSA: { SIGB(P_EOD) } k_{TSA}：當 B 收到 NRS 送來的挑戰時，必須以其私密金鑰解密，以達成身份的確認，同時可以得到 P_EOD。然後再對 P_EOD 簽章，並以 TSA 的公開金鑰加密送給 TSA 要求加註時戳。

(8) TSA→B: { EOD }k_B：TSA 在收到 B 的要求後，使用其私密金鑰解密，並在 SIG_B(P_EOD) 後附加一時戳 T_{g2} 然後加以簽章而形成完整的收文證據，並利用 A 的公開金鑰將此證據加密後傳送給 A。其中，EOD= SIG_{TSA}(SIG_B(P_EOD), TSA, T_{g2}))。

(9) B→NRS: { SIG_B(challenge_B, EOD) } k_{NRS}：接著，B 把 challenge_n2 及 EOD 共同簽章並以 NRS 的公開金鑰加密後傳送給 NRS。NRS 在此階段將得到完整的收文證據，同時將其儲存起來，以為將來所用。

(10) NRS→B: { EOO }k_B：NRS 將來源證據傳送給接收方 B。

(11) NRS→A: { EOD }k_A：NRS 將來源證據傳送給發送方 A。

根據此協定，表 2-1 說明了爭議仲裁的處理準則。表中明確指出，一旦 NRS 或傳送方可以提出收方證據 (EOD) 即認定有訊息傳遞的事實，若接收方可以提出 EOO，則認定訊息傳遞過程已經發生。因此任何的爭議將依據表 2-1 中準則進行裁決。

表 2-1　Coffee & Saidha (1998) 協定之爭議處理準則

參與者 / 提出	NRS		發送方 A	接收方 B
交易發生	EOO	EOD	EOD	EOO
是	×	是	×	×
是	×	×	是	×
是	×	×	×	是
否	×	否	否	否

下一節中將提出本論文有關於相關文獻的討論。

2.5 討論

在網路的環境中，證據是一種數位化形式的文件，有效的證據必須依賴密碼學的技術予以保證或檢驗。綜觀相關文獻所提到的不可否認服務機制的設計方法，可以就兩個層面來探討：一是公正的第三者介入程度，另一則是所使用的密碼學技術。然而，卻沒有同時將此二層面整合討論的相關文獻，本論文主要目的之一即是整合此二層面，設計電子化交易證據管理的一般化參考模型。

第 3 章 一個電子化交易的證據管理概念架構

本章提出一個電子化商業的交易證據管理之概念架構。此架構主要根據相關國際標準歸納出電子化商業交易證據處理的工作階段、列舉其參與的角色、同時歸類網路上訊息往來所需要產生的證據類型。此外，在此架構下，取決於所使用的密碼技術，證據可分為「簽章式證據」與「封條式證據」，同時依據所應用之密碼學環境與可信賴的第三者 (Trusted Third Party; TTP) 之介入模式分別提出一般化的參考模型。

3.1 一個電子化商業的交易證據管理之概念架構

圖 3-1 說明本論文所提出之電子化商業交易證據管理之概念架構。

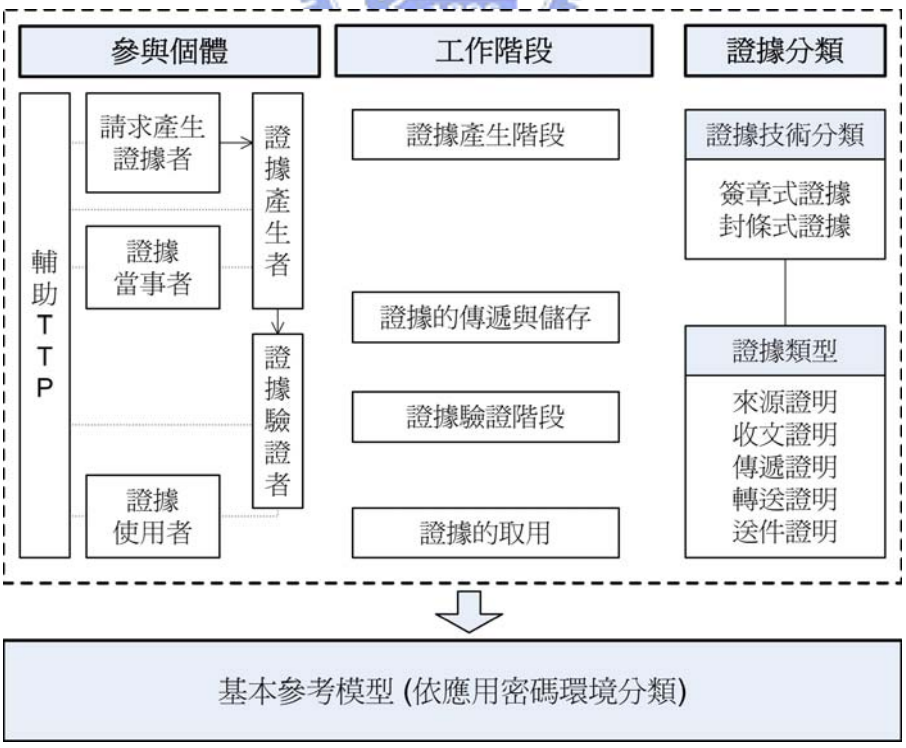

圖 3-1 電子化商業交易的證據管理概念

此架構中描述了交易證據處理的工作階段、相關的參與者、以及證據的技述分類與內涵，並依據所應用的密碼學方法環境建構一般化之參考模型。3.2 節中說明工作階段與各階段之參與者的角色，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，圖中的虛線部份即表示各種角色是可重疊的，而實線則表示實際上訊息或證據的流向。此外，證據的類型與技術分類詳述於 3.3 節，最後在 3.4 節則分別說明應用於公開金鑰與非對稱密碼學環境下的交易證據管理之一般化參考模型。

3.2 電子化商業交易證據處理的工作階段

本文歸納國際標準組織 (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)，將證據處理的工作分為四個階段：

(1) 證據產生階段：為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) 證據的取用：當有需要時，使用證據的個人或團體可由證據的儲存處取出證據來使用。

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。在爭議解決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，此階段的工作不會被執行，但是，上述的證據處理四階段的設計都是為了支援這一階段的工作。

依據以上的工作任務，並根據國際標準文件 (ISO/IEC JTC 1, 1997a) 之內容，本論文也歸納出電子化交易證據管理架構中的參與角色：

- 證據當事者：證據是為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，稱之為證據的當事者。以一般商業交易為例，發出購買請求的買方必須為他的動作負責任，「訂單」可以視為一項證據，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」為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：因為某種需求，而要求產生相關的證據，此要求者即為請求產生證據的個體。若事件的當事人為證明他的行為，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，或為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，或作為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。

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 介人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。

3.3 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，本論文將比較重要與常見的歸類於下，並分別加以說明。

- 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，來源證明可以視為訊息發送方的「創作證明」(proof of creation) 與「發文證明」 (proof of sending)，換句話說，來源證明可以作為訊息發送者建立了訊息的證據。

- 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，這項證據可以視為「接收證明」(proof of receipt)，同時也作為接收者已得知訊息內容的「獲知證明」(proof of knowledge)。

- 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。

- 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。

■ 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真確性 (integrity)；為保護數位化證明文件的真確性，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) 對真確性保護方法的評估，以「數位簽章」與「封條」作為安全資訊的真確性保護方法，方可用於數位化證明文件的真確性保護，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，依據前述的真確性保護方法，可將爭議解決機制中的證據分為「簽章式證據」與「封條式證據」；若以國際標準 (ISO/IEC JTC 1, 1997b-d) 常用的符號表示，則為：

(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。 $SGN_A(z)$ 是由 A 所簽署的數位簽章式的安全資訊； $SENV_{TTP}(z)$ 稱為安全信封，主要是為了保護事實陳述的真確性，$MAC_{TTP}(z)$ 則是由某一個被信賴的公正機構 (TTP) 所製作的封條。text 的使用相當有彈性，為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。

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，此證據為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 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，檢驗訊息的真確性，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 (參閱第 2 章 2.3 節)。

3.4 電子商業交易證據管理的基本模型

在電子商業交易的證據管理模型中，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，TTP 的介入方式可以分為：

- 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；
- 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；
- 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，金鑰的真實性與有效性必須被保證，在這裏，憑證機構 (Certification

Authority (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在證據處理的過程中所需要的資訊。另外，有效的時間戳記可說是各種證據中的重要項目，為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。

表 3-1 歸納出使用對稱式與非對稱式密碼學方法時，TTP 所扮演的角色與其所供的證據類型。

表 3-1　TTP 在爭議解決機制證據處理階段的角色

密碼學方法		對稱式密碼學方法	公開金鑰密碼方法
TTP 參與模式	強制參與	證據的產生者、證據的驗證者	憑證機構 (off-line)
	選擇性質	時戳服務中心、證據保管中心、傳遞機構等	時戳服務中心、證據保管中心、傳遞機構等
技術分類		封條式證據	簽章式證據
證據類型	來源證明	text || $SENV_{TTP}(z)$	text || z || $SGN_A(z)$
	送達證明	text || $SENV_{TTP}(z)$	text || z || $SGN_A(z)$
	送件證明	text || $SENV_{TTP}(z)$	text || z || $SGN_A(z)$
	傳遞證明	text || $SENV_{TTP}(z)$	text || z || $SGN_A(z)$

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 3-2 顯示出在使用公開金鑰密碼方法的技術條件下，交易證據處理的基本模型。

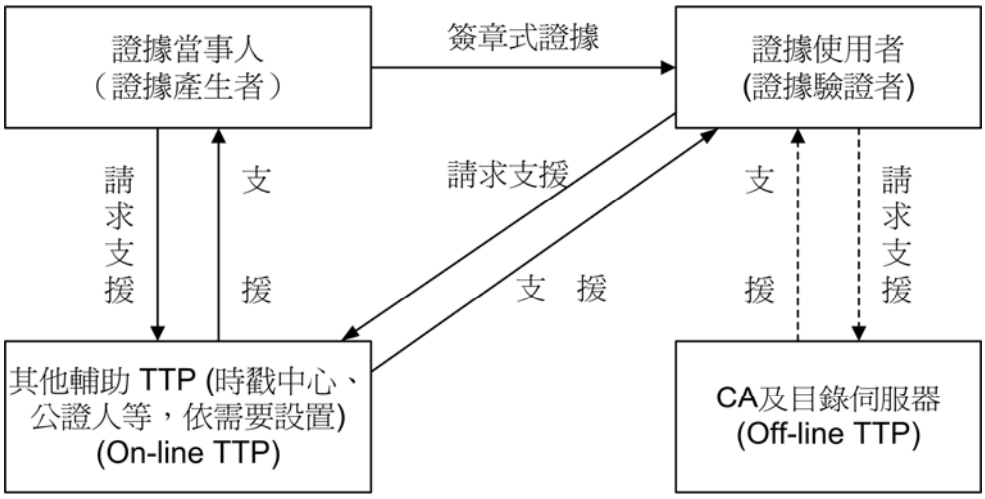

圖 3-2　電子化商業交易證據管理的參考模型 — 公開金鑰密碼環境

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 3-3 所示。

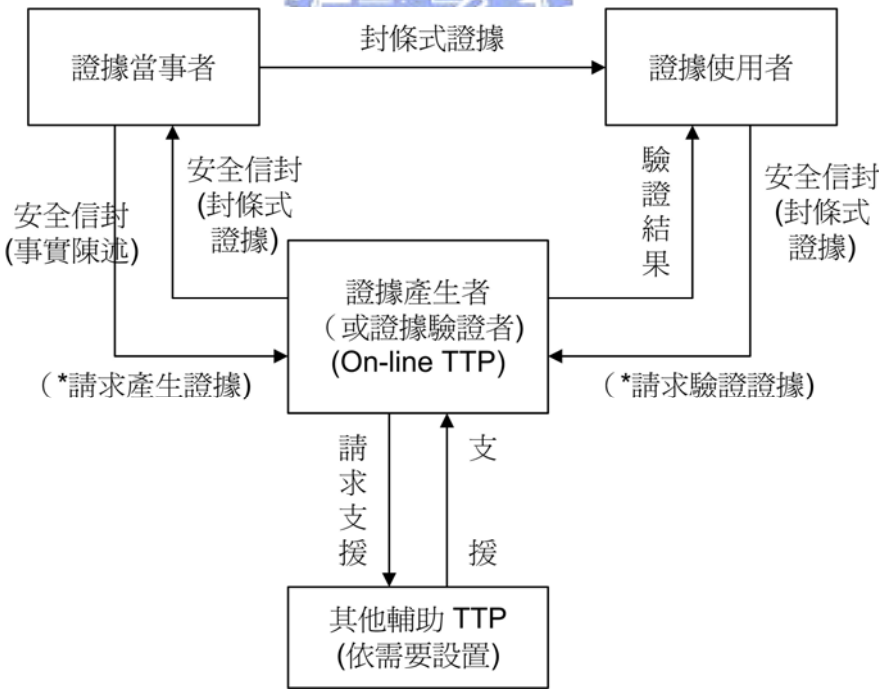

圖 3-3　電子化商業交易證據管理的參考模型— 對稱式密碼學應用環境

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為同一人時，他們彼此之間也會共享一把秘密金鑰。以圖 3-3 為例，證據的當事人會以他與證據產生者之間共享的秘密金鑰為「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產生封條式證據 (即 $z \| MAC_{TTP}(z)$) ，並製作安全信封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 3-4 所示即為 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。

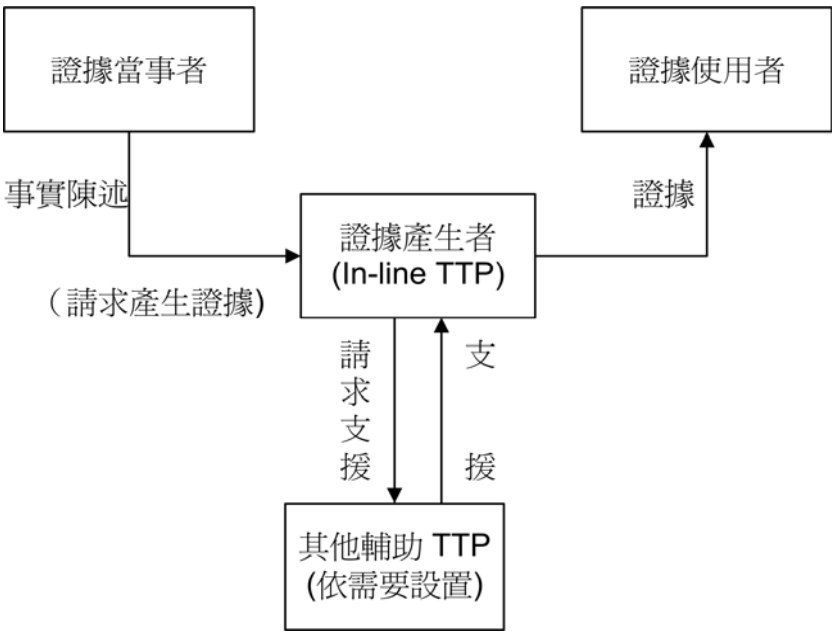

圖 3-4　電子化商業交易證據管理的參考模型— 介入 in-line TTP

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。

3.5 應用環境

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，因此，商業環境、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。尤其是，從法律與技術的觀點來看 (Mccullagh & Caelli, 2000)，必然也會有相異的解釋與做法。

已有研究針對不同的應用環境設計個別的不可否認服務或爭議解決機制。Asokan, Herreweghen, 以及 Steiner (1998) 建議了一個處理付款系統爭議事項的一般化架構，Liew, Lim, Tan, 與 Ong (1999) 針對以代理人為基礎的電子商務環境提出討論， Lee 等人則對付費電視系統提出一個可提供隱私保護與不可否認服務的協定 (Lee, Chang, Lin, & Hwang, 2000)。

本文所提出的交易證據管理架構與一般化的參考模型基本上可以適用於任何的電子化交易，但證據的內涵勢必會因不同的商業應用環境而有差異。

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為金融產業的時代課題。以銀行為例，在網際網路尚未盛行以前，距離一直都是消費者選擇銀行的重要決定因素，從信用合作社、農會、漁會、至各地郵局介入金融業務的事實，正說明了地緣因素與服務業的緊密關係。然而，隨

著網路人口的使用率呈指數成長趨勢，網路銀行的設立已打破地域、時間、空間的限制，它可說是延續自動櫃員機、電話銀行、無人銀行、以及專屬撥接等服務的新型態服務。此外，支付工具更是商務活動中不可或缺的元素，在電子商務這個發展迅速的領域中，已有不少連線付款系統可用於網路化的商業交易。其中，電子支票 (electronic check) 在近年來已逐漸發展，希望建立有效、安全、低風險的付款方式。

有鑑於此，也為進一步說明本架構的應用，本論文選擇網路金融服務為背景，更深入設計相關的交易證據管理模式。重點在於以我國網路證券下單作業與網路銀行之交易轉帳事項為例，依據本章的交易證據管理架構，提出相關建議。此外，融合此架構之概念於電子支票系統，發展一個集中管理的電子支票系統模型。

第 4 章　網路金融交易的證據管理機制設計

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為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為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為重要的議題。因此，本論文探討國內網路金融在相關事項的規範，自爭議解決機制的觀點出發，以網路證券下單與網路銀行為例，建議證據處理階段的相關事項與運作模型。

4.1　臺灣金融服務現況探討

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，委託紀錄確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為仲裁的依據。

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，並應確保紀錄之真實性及完整性。客戶如未保存者，推定以銀行所保存之紀錄為真正。」又，在第十七條中則註明電子訊息可為仲裁爭議的效力：「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

錄為一切證明的依據，有欠公允。也就是說銀行不必對他的行為提出證據。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。

4.2 網路證券下單交易的證據管理

目前，臺灣證券市場中，投資人可以當面委託、電話、書信、電報、IC 卡、語音或網際網路等方式委託證券經紀商買賣有價證券。其中，語音或網際網路兩種委託交易方式，為現有傳統委託方式 (附錄二) 全新的委託交易方式。附錄二也描述在受託買賣交易事項常見的糾紛類型。

委託買賣所依據之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的網路下單網頁，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：

- 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。
- 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。
- 儲存證據的規則：證據的存放地點、儲存媒體等相關事項。
- 證據的使用規則：誰是證據的使用人、證據的取用限制等。
- 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為應用環境，並以電子簽章法 (行政院，院臺經字第 0910080314 號令) 為執行時的法律依據。

在這個機制中，委託紀錄為「來源證明」，委託回報為「送達證明」。圖 4-1

為網路下單交易證據管理機制的示意圖。此機制乃為 3.4 節中介入 in-line TTP 的證據管理參考模型 (圖 3-4) 之應用。

投資人與網路證券商分別為來源證明與送達證明的當事者，亦分別為請求產者證據者。換句話說，投資人與網路券商亦分別為送達證明與來源證明的證據使用者。而為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) 為有效證據的產生者。在此，TSA 即為中介處理 (in-line) 的 TTP，亦為證據的產生者。此外，由於此下單的過程係於公開金鑰密碼環境中作業，故核發憑證的臺灣網路認證股份有限公司 (www.taica.com.tw) 則為此機制中的離線 (off-line) TTP。

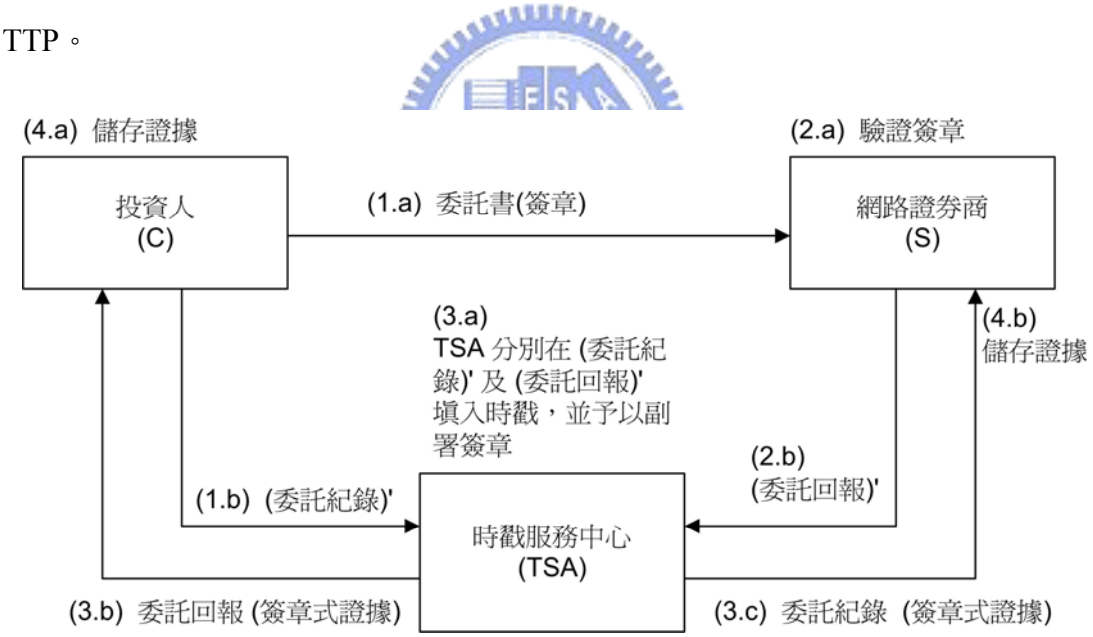

圖 4-1 網路下單爭議解決機制

此機制運作所遵行的詳細程序說明如下：

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

$(m, t_m) \| SGN_C(m, t_m)$。

(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'〉 $= z' \| SGN_C(z')$，$z' = (f_1, C, S, TSA, t_m, H(m, t_m))$；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，即驗證訊息的真確性。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'〉 $= r' \| SGN_S(r')$，$r' = (f_2, S, C, TSA, t_r, H'(m, t_m))$；其中，$f_2$ 指出此一證據代表的是送達證明， t_r 為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〉$= z \| SGN_{TSA}(z)$， $z = z' \| SGN_C(z') \| t_{g1}$

〈委託回報〉$= r \| SGN_{TSA}(r)$， $r = r' \| SGN_S(r') \| t_{g2}$

其中， t_{g1} 與 t_{g2} 即為由 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 負責為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為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。但如果為了方便、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。委託紀錄的內容為 $z \| SGN_C(z)$，$z = (f_1, C, S, t_m, t_{g1}, H(m))$。

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

一旦有委託行為上的糾紛發生時，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〉作為證據，使證券經紀商不得以未收到委託書為藉口。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為基本假設，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」，具備防偽、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。

4.3 網路銀行交易事項的證據管理

我國財政部已發佈「金融機構辦理電子銀行業務安全控管作業基準」，規範電子銀行交易與管理層面中安全的需求，以保障金融機構透過各種電子及通訊設與客戶業往來的安全。根據「金融機構辦理電子銀行業務安全控管作業基準」對電子銀行的業務分類，網路銀行的交易類別可概分為二種： (1) 電子轉帳及交易指示類 —— 係指與資金移轉有關或直接影響客戶權益之服務項目，例如，轉帳、付款、及網路交易等， (2) 非電子轉帳及交易指示類 —— 指與資金移轉無關或不直接影響客戶權益之服務項目，如申請服務、查詢服務及金融財經資訊的提供等。以我國的第一商業銀行的網路銀行為例 (http://nb1.firstbank.com/bbs/NetBankHelp.htm)，其網路銀行業務共分為 (1) 查詢類交易：包含帳戶餘額查詢、期貨入金明細查詢、信託業務查詢等； (2) 金融資訊類交易：以各類利率查詢、匯率查詢、基本淨值查詢服務為主； (3) 通知類交易； (4) 申請類交易：業務內容包括存款轉籍申請、掛失申請、領取支票簿申請等； (5) 授權類交易：如存款轉帳、代收款轉帳、預約轉帳、期貨入金交易等； (6) 其他交易類：如變更登入密碼等。依業務性質，其交易安全的需求亦有所不同，電子轉帳及交易指示類應確保訊息的隱密性 (confidentiality)、真確性 (integrity)、來源辨識 (original authentication)、不可重複性、與無法否認訊息的傳送與接收。

目前，國內網路銀行所採用的安全機制分為 SET (Secure Electronic Transaction)、Non-SET、SSL (Secure Sockets Layer) 三類。使用 SET 機制，用戶必須以銀行帳號為基礎申請電子憑證 (即每一帳號需要一張憑證)，並安裝電子錢包，進行交易時需輸入用戶名稱與通行碼，打開電子錢包 ；Non-SET 機制是由銀行業者自行建置的交易系統，用戶申請以身分證字號或公司統一編號為基礎的電子憑證，配合客戶端安控程式使用，必須同時使用電子憑證金鑰及密碼，才可進行交易；而 SSL 機制，則是以用戶身分證字號、網路代碼、網路通行碼為權限，進入網路銀行系統；在此機制的運作模式中，銀行客戶不需要申請電子憑證，使用上比較便利。依據交易事項，各類安全機制使用情形如表 4-1 所示。

表 4-1　臺灣網路銀行交易安全機制

交易類別 / 安全機制	非電子轉帳及交易指示類	電子轉帳及交易指示類	
		低風險性	高風險性
SSL	✓	✓	✓
SET	✓	✓	✓
Non-SET	✓	✓	✓

在表 4-1 中的「低風險性」交易係指同戶名或約定轉入帳戶、或非約定轉入帳戶小金額 (以每戶每筆不超過三萬元、每日最高三萬元、每月累積不超過二十萬元為限) 之各類電子轉帳。財政部乃是於 89 年 8 月方才開放金融機構可以採用 128 bits 以上 SSL 版本，從事此類型的交易。根據對網路銀行交易事項的討論，以即時轉帳、預約轉帳、與付款類的交易活動為主，設計交易時應紀錄的證據內涵，並探討使用不同安全交易機制時，交易事項的證據管理設計原則。

依據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，並應確保紀錄之真實性及完整性。客戶如未保存者，推定以銀行所保存之紀錄為真正。」又，在第十七條中則註明電子訊息可為仲裁爭議的效力：「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。」也就是說，在使用 SET/Non-SET 安全機制時，交易雙方是以契約簽訂的方式，強制電子簽章的效力，並經由此達成事件發生的不可否認性。

其證據的處理與傳遞方式如圖 4-2 所示。此證據管理機制所應用之模型為節 3.4 之所述的第一個基本參考模型 (如圖 3-2)。網路銀行客戶為來源證明的當事人，亦為證據產生者，而網路銀行伺服站則為送達證明的當事人與證據的產生者。核發憑證的臺灣網路認證股份有限公司 (www.taica.com.tw) 則為此機制中的離線處理 (off-line) TTP，但若在證據處的過程中，雙方需要即時要求驗證憑證的有效性，憑證中心亦可成為即時處理 (on-line) TTP。

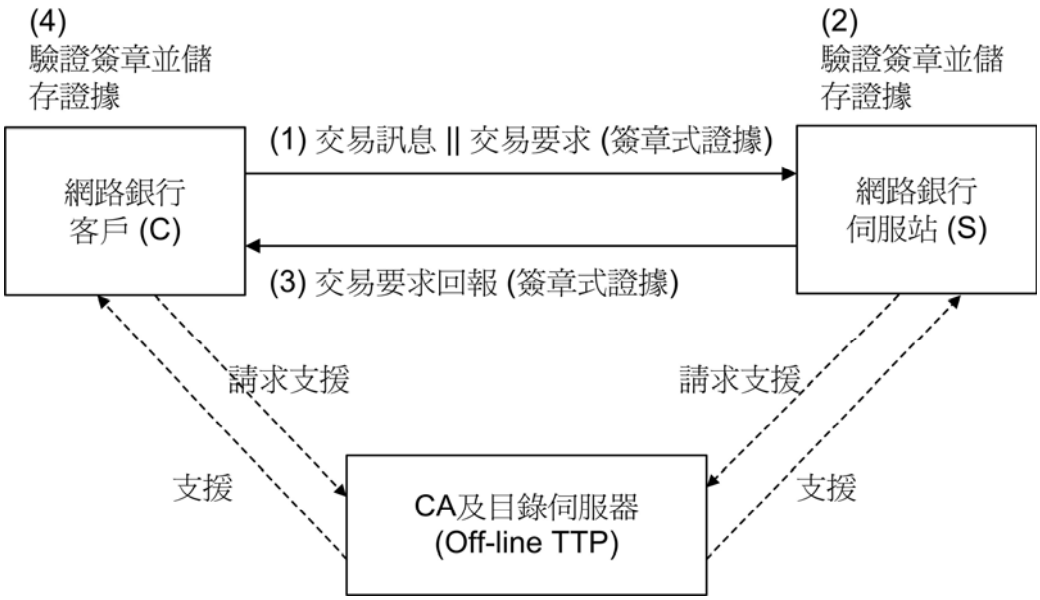

圖 4-2　網路銀行交易證據管理模型 — 使用於 SET/Non-SET 機制

「交易訊息」中所表達的為客戶所要求的交易事項。舉例來說，一個轉帳交易訊息至少應具備轉帳型態、轉出帳號、轉入帳號、轉帳日期、轉帳金額與交易序號等資訊；若在 90 年 1 月 5 日由帳號 822-012-34-5678 立即轉出 NT$10,000 帳號 855-987-6542，則交易訊息 (m) = 〈即時；send_822-012-34-5678；rcv_855-987-6542；2001/01/05；amt_10000；code_xxxx〉。

「交易要求」為用戶端 (C) 所建立傳送的來源證明，以符號表示為 z_C || $SGN_C(z_C)$。z_C 為事實的陳述，$SGN_C(z_C)$ 表示 z_C 的數位簽章，|| 則是連結的意思。其中，z_C 應具備的資料項目為 {證據的類型，證據當事人的唯一識別，訊息傳送的時間、證據產生的時間、SGN_C(交易訊息)}。若用戶王小明 (身份證字號為 A123456789) 於民國 90 年 1 月 5 日 10 時要求即時轉帳交易，則其事實陳述如表 4-2，即 $z_C = \langle f_O, S, C, T_1, T_{g1}, SGN(m) \rangle$。

表 4-2　來源證明 (交易要求) 中的事實陳述

資料項目	內涵	符號
證據類型	交易要求	f_O
訊息發送方唯一識別	A123456789 王小明	C
訊息接收者唯一識別	XX Bank 網路銀行系統	S
訊息發送時間	2001/01/05 09:00	T_1
證據建立時間	2001/01/05 09:01	T_{g1}
SGN(交易訊息)	交易訊息 (m) 的簽章	SGN(m)

當銀行伺服端 (S) 收到交易要求後，驗證用戶端的簽章，確認之後，建立「交易要求回報」作為網路銀行端 (S) 送達證明，傳送給用戶端。「交易要求回報」= $z_S \parallel SGN_S(z_S)$；

$z_S = \langle f_R, S, C, T_1, T_2, T_{g2}, m^*, SGN(m^*) \rangle$

其中，f_R 表示送達證明、T_1 為用戶端執行時間、T_2 為伺服端執行時間、T_{g2} 為證據產生的時間、m^* 表示交易訊息。與前述交易訊息內涵不同之處在於，m^* 可以加入可加入轉帳成功的通知與帳戶餘額等相關資訊。如果此筆轉帳交易的類型為「預約轉帳」，則 $m^* = m$。

在這一個交易證據管理機制中，有關於紀錄儲存的部份，並未強制銀行業者必須傳送適當的證據給用戶，而無法達成證據傳遞的「公平性」(fairness)；此外，本研究發現，多數的網路銀行均未提供爭議處理的安全政策 (security policy) —— 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。對此，

本研究建議，銀行業者應明訂其爭議處理的安全政策，以進一步保障客戶的權益。

至於使用 SSL 機制從事低風險性的交易 (也就是金額較低的交易) 時，並沒有強制達成「無法否認傳送/ 接收訊息」的安全需求。但是，電子商務交易有許多小額交易的情形，而這一類的交易不表示不會發生糾紛。故本研究認為，即使是低風險性的交易，仍應提供適當的交易證據管理機制，如此方能建構實際的商業環境，並建立消費者或企業跨區域交易的信心。

為了在以 SSL 機制為基礎的交易環境中，也能提供適當的交易證據，本論文提出一個與 Online ADR 結合的交易證據管理機制。根據目前 Online ADR 現行的一些機制的運作來看，Online ADR 業者係以會員的方式發行安全標章 (seal) 給企業，而後在消費者與企業會員之間提供解決爭議的服務。但在一般 ADR 的處理程序中，通常未涉及證據的產生、傳遞等過程，延襲這樣的概念，本研究將產生證據的 TTP 與 Online ADR 業者二者的角色相互結合，由 ADR 業者提供建立證據的服務，圖 4-3 為本研究建議的交易證據管理機制。

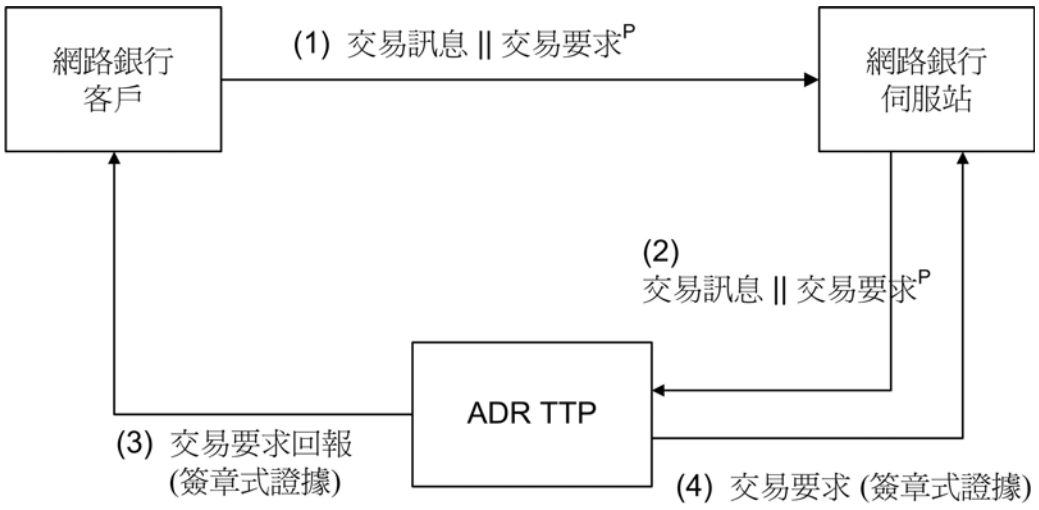

圖 4-3　網路銀行交易證據管理模型 — 使用於 SSL 機制

在這個模型中，三方的連線都受到 SSL 的保護，以保持資訊的機密性與真確性。此外，以 ADR/TTP 的簽章產生來源與送達證明，確保證據的效力。在此， ADR/TTP 亦為一 in-line TTP。其運作流程如下所述：

(1) 客戶端提出交易要求，傳送交易訊息 m 及 z_C，$z_C = \langle f_O, S, C, T_1 \rangle$，其中，$T_1$ 為交易訊息的時間

(2) 銀行端收到交易要求後，傳送 $m \| z_C \| SGNS(m, z_C)$ 給 ADR/TTP，請求產生「交易要求」。

(3) ADR/TTP 檢驗銀行的簽章後，產生「交易要求」(來源證明) 與「交易要求回報」(送達證明)，並將「交易要求回報」傳給客戶端。交易要求回報的內涵為 $z2_{TTP} \| SGN_{TTP}(z2_{TTP})$，此時，$z2_{TTP} = \langle f_R, S, C, TTP, T_1, T_2, T_{g2}, m, SGN_{TTP}(m) \rangle$；而交易要求 $= z1_{TTP} \| SGN_{TTP}(z1_{TTP})$，$z1_{TTP} = \langle f_O, S, C, TTP, T_1, T_2, T_{g1}, SGN_{TTP}(m) \rangle$。

(4) ADR/TTP 回傳「交易要求」給銀行伺服端。

由於基本的 SSL (basic SSL) 機制僅僅透過使用者唯一識別與通行碼進行身份鑑別，因此，其安全性必然低於公開金鑰憑證的使用。但經由制度的設計將可提昇安全強度，例如，可以使用雙重通行碼 (登入系統與執行交易需要不同的通行碼)，或是加強建構稽核線索等。如此，可以使得交易遭受偽造的可能性降低，也加強證據的可信賴度。

4.4 討論

在傳統的商業社會裏，已使用契約等方式規範商業行為的不可否認性，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，商業行為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。

本章根據第 3 章所提出之電子商業交易爭議解決機制中證據管理的概念架構及一般參考模型，以網路證券為例，提出可適用於網路下單的交易證據管理機制，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。

此外，網路銀行是一個有效率且低成本的金融服務通道，銀行業者莫不積極投入，如何建構安全、私密與可信任的應用系統，將成為客戶使用網路銀行的重要考量。除了符合高標準的資訊安全技術外，建構一套法庭之外的公平便利的爭議解決機制，將有助於提昇客戶的信心，也有利於銀行業務的拓展。尤其是，安全無法全然仰賴艱困的技術，而必須能與其他制度互相搭配，才能夠創造真正的價值。本論文亦以網路銀行的轉帳、付款交易事項為應用環境，自技術的觀點出發，探討爭議解決機制中，證據處理的過程與方法，並設計證據的內涵與證據處理的流程，將不可否認服務的機制納入其中。事實上，交易證據管理的內涵並非只具有技術上的特質，還牽涉到法律上的架構，線上替代性爭議解決機制即具有相當程度的法律意涵，本論文所提出的證據管理機制可作

為 Online ADR 解決紛爭的基礎，以期在不同的密碼學應用與商業環境中，均能建構出一個公平、有效率的電子交易的爭議解決機制。

第 5 章 概念應用—集中保管的電子支票模型

目前，在電子商務這個發展迅速的領域中，已有多樣化的連線支付工具可用於網路化的商業交易，包括由 Master 與 VISA 國際信用卡組織 (1997a, b, c) 共同提出的 SET 線上信用卡付款系統、用以保護信用卡付款資訊的 SSL 協定 (Freier, Karlton, & Koche, 1996; Direks & Allen, 1999)、電子現金 (Chaum, Fiat, Naor, 1990; www.mondex.com)、電子支票 (Stavins, 2003) 等等。其中，有將信用卡號碼連線傳送用於指示付款、有類似於傳統使用的現金、也有透過上網連線遞送訊息，指示銀行轉帳以支付水電、瓦斯等費用、或有類似於傳統的紙張支票等，另外有些方式被歸納為「小額付款系統 (micropayment systems)」(Manasse, 1995; Rivest & Shamir, 1996)，用以支付一些本身價值非常低、卻遍佈全世界的資訊商品。

在眾多的支付工具中，支票是企業間商業交易最常用的付款工具，它具有避免支付現金之煩擾以及減少通貨計算錯誤等優點，故使用數位化的電子支票作為企業間連線付款的工具或許會更符合傳統的商業習慣。此外，一般消費者也可以在信用卡之外，尋求另一個有效、安全、低風險的付款方式。有鑑於此，美國 FSTC (Financial Services Technology Consortium) 已於 1998 年發展 eCheck 計畫，試圖在美國原有的法律架構與商業實務之下，建構一個完全電子化的支票系統 (www.eCheck.org)。

而我國也在「知識經濟發展方案具體執行計畫」中規畫了「發展電子支票計畫」的子計畫 (行政院經濟建設委員會，民 89)，此計畫已在中央銀行與台北

票據交換所的積極投入下，從初始的研發進入實施的階段 (傅沁怡，民 92)。

一般來說，一張支票自簽發經背書 (轉讓) 到提示 (取款) 為止，會在付款人、收款人、與銀行之間流通，在流通的過程中，可能會遭受被盜用、複製、或遺失的風險。舉例來說，一份被複製的電子文件是肉眼、甚至是電腦系統無法察覺的，最終，一張電子支票是否有效必須由銀行來決定，無效的支票會被銀行退票，也就是說，支票持有人必須承擔支票遭盜用或複製的風險。因此，延伸本論文所提出的交易證據管理模型，本文深入探討、研析現行已發展之電子支票系統的運作機制，自系統流程的角度重新思考，結合證券市場之有價證券的集中保管作業方式，設計一個「集保型」的電子支票系統模型，儘量避免支票在市場上流通，以降低電子支票因數位文件本身的可複製特性所帶來的風險，並融合資訊安全觀點與現有支票業務，建構一個能支援多種商業模式的連線付款工具之基本模型，使企業與消費者皆能更便利且有效率地進行網路商業活動。

5.1 支票概述

臺灣之票據法對於支票有明確的定義與規範。根據票據法第四條：「稱支票者，謂發票人簽發一定之金額，委託金融業者於見票時，無條件支付與受款人或執票人之票據。前項所稱金融業者，係指經財政部核准辦理支票存款業務之銀行、信用合作社、農會及漁會。」票據法第一二五條則規定了支票應載之事項 — (1)表明其為支票之文字 (2)一定之金額 (3)付款人商號 (4)收款人姓名或商號 (5)無條件支付之委託 (6)發票地 (7)發票年、月、日 (7)付款地，並由發票

人簽名。(王毓仁，民 85)

一般支票流通的過程係由發票 (簽發) 經背書 (轉讓) 到提示 (取款) 為止，其流程如圖 5-1 所示。

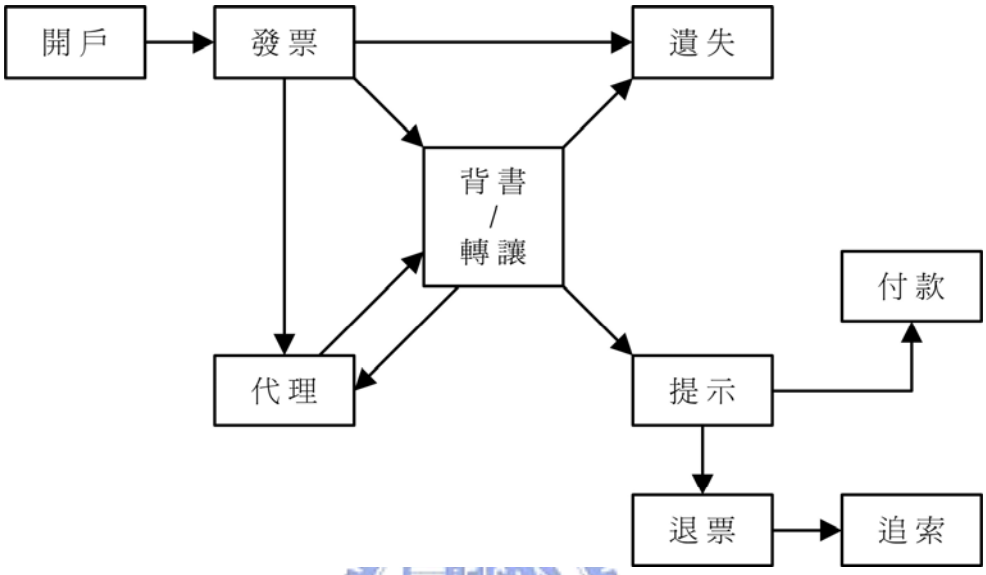

圖 5-1　支票流通過程 (王毓仁，民 85)

使用支票替代現金的收付，可以免除巨額現鈔點收之不便，減少處理錯誤的情形；其延遲付款的特性，可便利工商業資金週轉，作為企業的信用工具；此外，當支票遺失、遭竊、或損毀時，尚可申請掛失止付，較現金來得安全許多。然而，紙張支票在使用上仍然遭遇到許多難題，若能發展電子化支票，將可改善所面臨的問題。茲說明如下 (蕭曉玲、黃景彰，民 92)：

- 隨著社會進步，商業交易發達，支票使用量亦日益增加，使得紙張支票之作業疏失隨之增加。此外，支票交換量也因此不斷擴大，使得票據交換所負荷過重，而易產生管理漏洞。

- 企業以人工處理紙張支票，除了較費時費力，也無法將付款資訊與企業內部資訊系統整合。適當地使用電子支票，將可提昇 B2B 電子商務金流效率。

- 使用電子支票系統，應可大幅減少紙張支票的使用疏失、偽造、或遺失等多項導致退票的情況。

5.2 電子支票系統的運作流程

美國 FSTC 所發展的 eCheck 系統是電子支票系統的典型代表(Anderson, 1998; Gelinas, Gogan, & Wade, 2003)，此系統的架構完全模仿美國現有紙張支票的運作流程，因此可依循其現行的商法律規範與商業實務，而不必建立任何新的付款工具。 eCheck 的基本運作方式如圖 5-2。

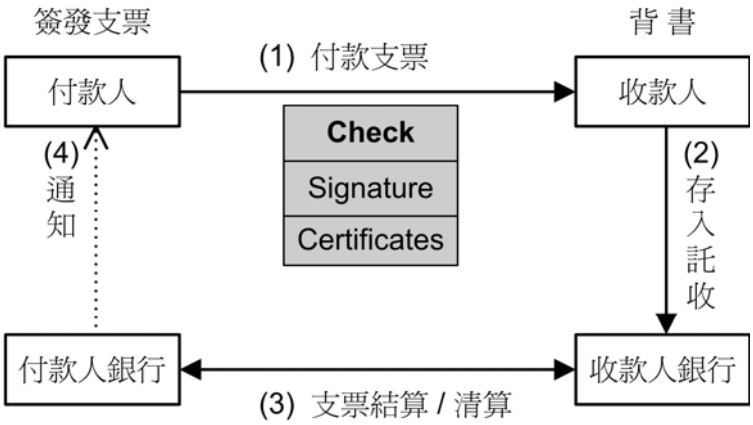

圖 5-2 FSTC eCheck 系統基本運作流程

系統中包括付款人、收款人、付款人的銀行、與收款人的銀行，使用 eCheck 系統的用戶，必須在銀行開立一個電子支票的存款戶，銀行會與此存款戶簽訂一個一般的定型化契約，明定電子支票所適用之現行有關於支票的法律依據。在技術上，eCheck 系統使用數位簽章以確保資料的來源，以及資料未遭受到非經授權的篡改或偽造。此系統發展過程中所遵循的文件發展技術是 FSML (Financial Service Markup Language)，透過這個標準的規範，不同的廠商、銀行都能夠理解支票的內涵。利用 FSML 所撰寫的支票是一個複合式的文件，其允

許支票本體加上其他相關的商業文件 (例如發票、信用狀等) 一併流通，再依情況適當地加以拆解。但就簽章來說，在流通過程中可以抽換的複合式文件會造成一些困擾，因此在技術上必須有一些創新，而複合文件的簽章技術正是這個系統的重要貢獻之一。此外，美國聯邦已於 2000 年 6 月通過「全球暨國家商務電子簽章法」(Electronic Signatures in Global and National Commerce Act)，可為系統使用之法律依據。

除了以數位簽章密碼技術為基礎的 eCheck 系統外，有一個更早的是美國南加大應用對稱式密碼方法所發展的 NetCheque 系統 (Neuman & Medvinsky, 1995)。NetCheque 的觀念是一個類似支票付款的分散式帳戶服務系統，在整個系統中，由若干個帳戶伺服器 (accounting server) 負責管理使用者帳戶，收付款雙方必須在系統中設立帳戶，付款人可以簽發一份包含付款人姓名、財務機構 (如銀行) 名稱、付款人帳戶名稱、收款人名稱、以及付款金額的電子文件，這份文件同時承載付款人所簽署的電子簽名；當收款人收到此份文件後，必須在文件上背書簽名，方可兌現。NetCheque 系統是以 Kerberos 鑑別系統 (Neuman & T'so, 1994) 的票證 (ticket) 為基礎進行簽名與背書，由於應用對稱式密碼學方法，節省了公開金鑰密碼系統所需的高昂成本，這個系統可用於小金額的商業交易及資金往來的活動，但它到目前仍然止於實驗室的學術研究計畫，並未發展成為實用的商業系統。此外，NetBill (Tygar & Sirbu, 1995; Cox, Tygar, & Sirbu, 1995) 則是用於支付低價商品的類似支票付款方式的系統。也有學者基於 FSTC e-Check 系統提出改善的模型 (Dani & Krishna, 2001).

我國中央銀行為解決電子商務金流問題，於民國 89 年 12 月提出「發展電

子支票計畫」，由台灣票據交換所與數家銀行共同規畫、建置電子票據各項業務規範與系統，希望能提昇全國支付系統的效率。在法令依據上，票據交換所依據我國「電子簽章法」第四條第二項及第九條第一項訂定「金融業者參加電子票據交換規約」與「電子票據往來約定書」(範本)，以及金融業者與客戶間相關之業務規範為電子票據系統之法律基礎 (臺灣票據交換所，民 92)。由於這個計畫所開發的系統之處理標的除支票外，尚包含了銀行擔付本票與銀行承兌匯票，故統稱為電子票據系統，本系統的特點在於空白票據置於銀行端，而已簽發之票據則由票據交換所採集中登錄之保管方式其基本交易流程如圖 5-3 所示。以支票為例，電子票據系統的使用者必須先至銀行辦理支存開戶，並取得以 IC 卡為載具的數位憑證 (digital certificate) 及私密金鑰 (private key)，簽發支票及存入託收的作業都是在銀行網站端進行作業。

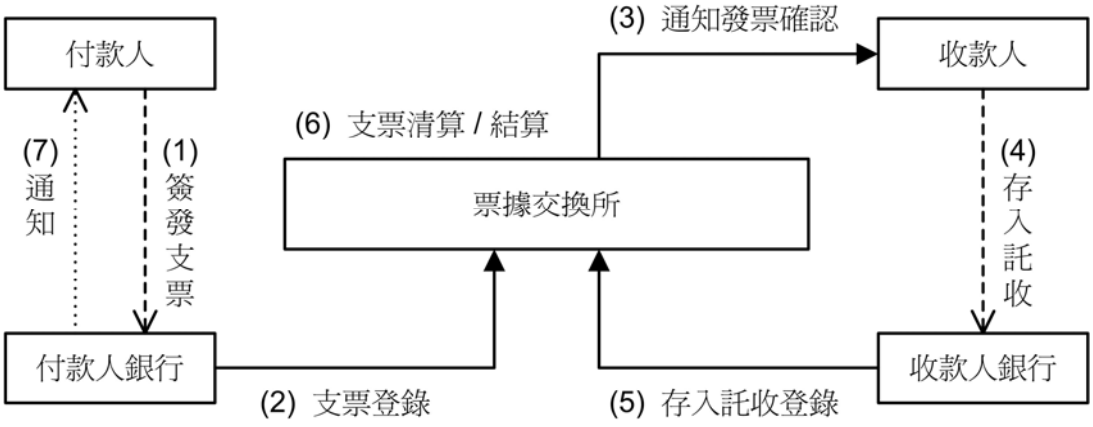

圖 5-3　臺灣電子票據系統基本運作流程

綜觀以上所述的幾個系統， Netcheque 系統使用之密碼技術為對稱式密碼學方法，但並未進入實用的階段。其餘二者皆是以使用數位簽章 (digital signature) 為基礎，且分別已經 (或準備) 進入實用的階段，表 5-1 為 eCheck 與臺灣電子票據系統的比較。

分析這兩個系統，可以發現兩者最大之差異在於 eCheck 系統使用的電子支票係以複合式的數位文件在收付款雙方及銀行間流通，未兌的支票由執票人保管，而臺灣電子票據系統中的電子支票則由票據交換所集中登錄與保管。前者的優勢在於系統中的參與者與紙張運作的模式完全相同，參與者扮演的角色也沒有任何的改變，符合一般使用者的使用習慣，但在收付款人之間流通的電子票據可能會有遺失或被複製之虞。而後者所開立的支票由票據交換所統一管理，不會在付款者與收款者之間流通，所要承擔的風險較低，但是票據交換所卻必須身兼票據交換與保管兩種角色，使得原參與者間彼此的互動與作業流程有所改變。故，本研究的目的在於設計出能兼具兩個系統優勢的電子支票系統模型。

表 5-1　eCheck 系統 與 臺灣電子票據系統

	eCheck 系統	臺灣電子票據系統
處理標的	支票	支票、銀行擔付本票、銀行承兌匯票
密碼技術	數位簽章	數位簽章
文件格式	FSML (Financial Markup Language)	XML (eXtended Markup Language)
開票方式	空白支票置於付款人的 IC Card，由付款者的系統端開票	空白支票置於銀行端，付款人登入銀行網站簽發支票
支票保管	執票人	票據交換所

5.3　一個加入公證第三者的集保型電子支票系統模型

要降低電子支票因數位文件本身的可複製特性所帶來的風險，集中保管模式是一個較佳的選擇，但是臺灣電子票據系統中的票據交換所卻缺乏角色的獨立性。比較圖 5-4 中同樣為集中保管模式的臺灣有價證券管理作業 (臺灣集保公

司，2003)，可以發現，臺灣證券集中保管公司只負責有價證券的管理，而未涉及與證券交易相關的參與角色 (如投資人、證券商、證券金融公司、或上市公司等)，也就是說，集保公司所扮演的角色是單一的。

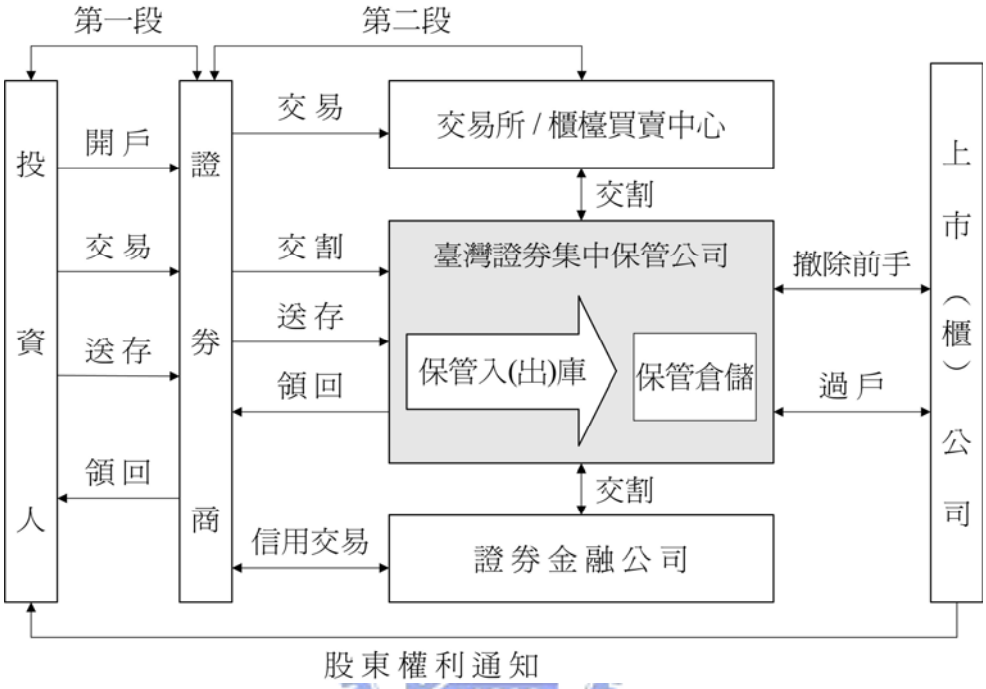

圖 5-4　臺灣有價證券管理之集保作業模式
(資料來源：臺灣集保公司)

為了能在降低風險的同時，也能維持系統中原有參與者角色之獨立性， 本研究參考臺灣有價證券管理之集保作業模式設計一稱為「集中支付管理中心」(Central Payment Management Center; CPC) 的可信賴第三者 (TTP, Trusted Third Party)，獨立負責支票的集中保管作業，以避免角色上的重複。圖 5-5 為參考 eCheck 系統、臺灣電子票據系統、與臺灣有價證券管理之集保作業模式所設計的集保型電子支票系統模型之示意圖。

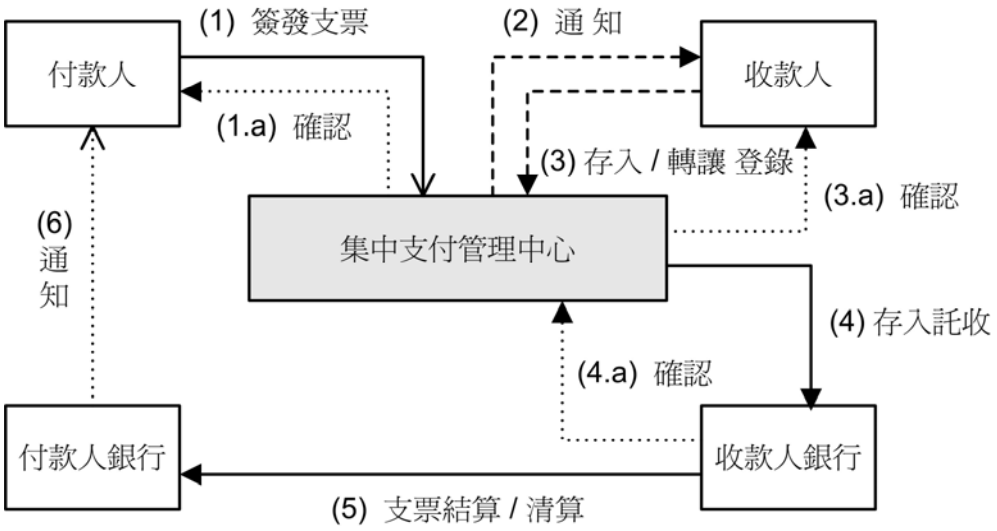

圖 5-5　加入集中支付管理中心之集保型電子支票系統模型

在本研究所設計的模型中，付款人必須先在付款人銀行開立支存帳戶，由付款人事先在銀行取得具有銀行識別碼的空白支票，儲存在 IC 卡中，也就是說，以 IC 卡作為電子支票簿。此外，收付款雙方皆必須登錄成為 CPC 的會員，由「集中支付管理中心」(CPC) 負責支票的集中保管作業，支票必須由 CPC 的簽證後，才具有支付的效力。

此系統模型之運作流程說明如下：

(1)　付款人由付款人系統簽發支票，傳送給 CPC。電子支票所記載的內容應與紙張支票應記載的事項相同，並附加收票人的電子郵件地址等資訊。

(1.a)　CPC 發送確認訊息給付款人。此確認訊息可作為發生爭議時的證據，故其內容應包涵依循的安全政策、CPC 與付款人的唯一識別、簽發票據的日期與時間等資訊，並由集中支付管理中心簽章。

(1.b)　CPC 在支票上附加其簽章，入庫保管。未來，銀行在支付款項時，必須驗證此簽章以確認支票的真實性。

(2) CPC 依據付款人所提示的收款人資訊 (如電子郵件地址或住址等) 通知收款人。

(3) 收款人登入 CPC 進行存入或票據轉讓登錄的作業。同樣地，收款人必須登錄成為 CPC 的會員。在此，先簡單地以存入登錄為例。在這個處理過程中，收款人會在支票上加上他的簽章。

(3.a) CPC 發送確認訊息給收款人。這個訊息是由 CPC 簽章的一項證據。其內容包涵依循的安全政策、CPC 與收款人的唯一識別、存入託收的日期與時間等資訊。

(3.b) CPC 進行支票所有權移轉的維護作業

(4) CPC 針對各個銀行，整理出存入託收的清單，並將支票存入收款人銀行。

(4.a) 收款人銀行開立收到支票的證明給集中支付管理中心。

(5) 收款人銀行與付款人銀行之間透過票據交換所進行票據交換與清算的作業。

(6) 付款人銀行對付款人帳戶進行扣款，並通知付款人。

在此模型中，支票自付款人開票後即由 CPC 集中保管，支票本身不會在收款人與付款人之間流通，因而可避免其在流通過程中可能遺失、損毀、或被複製的風險。同時，由於票據集中處理，可以提高票據的處理速度。就系統的實際應用面來看，由於本模型使用之密碼技術為數位簽章，故可以相關的電子簽章法案為法律依據，使原來應簽名或蓋章之處，由相對人同意後，以數位簽章

為之；此外，由於在本模型中，票據交換所與銀行之間之作業程序完全與紙張支票相同，故不需要另外訂立新的法規，惟應就集中支付管理中心之作業加以規範。

另外，由集中支付管理中心作為獨立的公正的第三方機構 (可信賴的第三者)，可以同時建立、紀錄與管理交易證據，當有因交易而引起的糾紛或爭議發生時，集中支付管理中心還可以作為爭議解決的機構。使得支票的支付處理可以更安全、更快速的進行。

5.4 分析與討論

本文所提出之集保型電子支票系統模型乃是深入研析美國之 eCheck 系統、臺灣電子票據系統，就系統與作業流程的角度重新思考後建立。茲就以下幾個方向與前述兩個系統作一比較與分析。

- 安全性：

  在本模型中，電子支票的真確性可以透過數位簽章來達成，與其他兩個系統相同。再就支票在流通的過程可能遭受的各項風險來看，由於支票是由 CPC 集中保管的「集保型」系統，而 eCheck 系統是屬於「流通型」的系統，因此，所承擔的風險將較 eCheck 為低。相較於同於集中保管型的臺灣電子票據系統，雖然本模型電子支票簿是由付款人自行保管，但是由於支票必須由 CPC 簽證後才具有支付的效力，因此不必擔心支票由付款人流向 CPC 時可能遺失或被複製的問題。此外，透過本模型所設計的集中支付處理中心，尚可提供「爭議解決」的資訊安全服務。故，本系統模型的安

全性是優於 eCheck 系統而與臺灣電子票據系統相同的。

- 責任分工：

eCheck 系統基本上完全仿照紙張支票系統的運作模式，因此，在 eCheck 系統中，支票處理過程中的各個參與角色的互動與原來完全一樣，並沒有任何的更動。而在臺灣電子票據系統中則有較大的變革 — 票據交換所除票據交換的業務外，同時要負責支票的集中登錄與保管，此作業範圍的變革，使得銀行與票據交換所之間的互動也有所不同，因而使得角色之間比較缺乏獨立性。由於票據交換所本來就是支票交易過程中的參與個體，本文認為其應維持角色的單一功能，透過集中支付處理中心的設立，可將票據交換與支票保管的業務各自獨立，原本銀行與票據交換所之間的作業體系也不必有任何變動。故就責任上的分工來看，本模型是優於臺灣電子票據系統的。

- 成本：

本模型與 eCheck 一樣，採用 IC 卡作為電子支票簿與金鑰的載具，因此各個參與者必須建置能夠使用的系統。付款人必須建置開票系統，銀行必須建置驗證系統。而在臺灣電子票據系統中，開票人必須登入銀行網站進行開票的動作，故付款人端僅需安裝簽章軟體，而不必建置開票系統，但是銀行端必除驗證的工作外，必須建置供客戶使用的開票系統，而收款人銀行也必須建置供收款人進行存入託收作業的系統。故就成本面來看，本文認為各個架構皆必須負擔一定的系統建置成本，差異應不是很大。

■ 企業機會：

只要能夠具有足夠的公正性，集中支付處理中心可以由私人機構來成立，也可以是一個營利事業。舉例來說，一些線上爭議解決機制 (Online ADR) 的公司，如 Cybercourt、BBBOnline 等，或是數位憑證機構，如 Verisign 等；這些機構皆是從事公正第三者業務的營利單位。故集中支付處理中心的設計，尚提供了新型商業模型的發展機會。

就以上的層面來看，本系統模型可以說是集合了 eCheck 系統與臺灣電子票據系統的優點，而改進了他們的缺點。

第 6 章 結論與討論

6.1 結論

在傳統的商業社會裏，已使用契約等方式規範商業行為的不可否認性，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，商業行為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。

但無論如何，「證據」都是爭議解決機制的核心要素，本論文提出一個電子化商業交易證據管理的一般化概念架構，以支援爭議的解決。此架構描述了證據處理的工作階段與參與個體，歸類證據的使用類型與證據的內涵，也依據使用的密碼學技術提出證據的技術分類。同時，在此架構中，本論文依據所應用的密碼學環境與可信賴第三者的介入方式提出證據處理之一般化參考模型。

而無論是傳統或是電子化的商業活動中，金融服務都是不可缺少的必備條件，如何使得金流能夠順暢的運轉，已成為重要的課題。其中，網路銀行與網路證券是一個有效率且低成本的金融服務通道，業者莫不積極投入，如何建構安全、私密與可信任的應用系統，將成為客戶使用網路金融的重要考量。除了符合高標準的資訊安全技術外，建構一套法庭之外的公平便利的爭議解決機制，將有助於提昇客戶的信心，也有利於銀行業務的拓展。尤其是，安全無法

全然仰賴艱困的技術，而必須能與其他制度互相搭配，才能夠創造真正的價值。

本論文並以網路金融服務為例，依據電子化商業交易證據管理之概念架構，在網路證券、網路銀行與電子支付系統三項金融服務中，參酌我國國情，分別針對臺灣證券集中市場之網下單作業、網路銀行使用 SET/Non-SET 以及 SSL 機制的轉帳作業以及電子支票系統，建議證據處理的過程與方法，提出合宜適用的證據管理機制，使得交易雙方可提出證據證明交易事實的發生。而本論文所規畫的集保型電子支票系統模型乃是透過深入研析現行的電子支票系統，並參考有價證券的集保作業模式，結合交易證據管理之基本模型所提出之一種新的作業流程。經由對電子支票的集中保管方式，避免了在流通型的 eCheck 系統可能遭遇的風險 — 數位文件本身的可複製性所帶來的風險，以及支票在流通過程中可能會遺失或毀損的風險。同時，透過設立集中支付管理中心，除了可以提供交易證據，也可以儘量不需更動銀行與票據交換所中的作業流程，解決了臺灣電子票據系統中所欠缺的參與角色的獨立性問題。在不需承擔較高成本的情形下，本模型可說為電子支票的運作提供了一個更佳的解決方案。

6.2 未來研究方向

在電子化的環境中，大量的交易與金額在網上流通，如何追蹤與檢驗企業外部交易與內部活動的有效性，可說是一個相當值得討論的議題。本論文所提出的證據管理架構著重於企業外部交易行為證據的控管，至於企業內部活動的管控則有賴於稽核系統建立「稽核線索」(audit trail)，兩者皆是企業資訊系統安全管理的重要工作，其特質有部份的重疊，卻分屬不同的領域。探討此二類資

訊安全工作所需要使用的證據，分析各種證據的內涵與其關連性，並研究其互相整合的可行性與應用空間，將是值得研究的議題。而為達成更具彈性與自動化的證據蒐集與稽核控管，在證據管理系統中整合智慧型系統也是值得思考的方向。

此外，在現行的實務系統中，通常僅以「數位簽章」做為傳遞文件、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，以證據管理為核心，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，也是未來進一步的研究議題。

而針對本論文所提出的集保型電子支票系統，將可經由進一步的規畫集中支付處理中心的資料庫設計等細部系統實作相關工作，以繼續朝實作本模型的系統雛型努力，使企業與消費者皆能更便利且有效率地進行網路商業活動。

參考文獻

王毓仁，民 85，*支票使用實務*。書泉。

行政院經濟建設委員會，民 89 年，*知識經濟發展方案具體執行計畫－發展電子支票計畫*，於民國 91 年 7 月 25 日由 http://www.aproc.gov.tw/kbe/3/0119/03.doc 取得。

財政部金融局，(民 88 年)，*個人電腦銀行業務及網路銀行業務服務契約範本*。於民國 89 年 4 月 25 日，由 http://www.boma.gov.tw/8872563-1.htm 取得。

傅沁怡，民 92 年 9 月 11 日，電子票據 29 日上路。*經濟日報*。於民國 92 年 9 月 25 日，由 http://archive.udn.com/2003/9/11/NEWS/FINANCE/FIN3/1555156.shtml 取得。

黃景彰，民 90 年，*資訊安全—電子商務之基礎*。華泰書局。

電子簽章法，院臺經字第 0910080314 號令，民 91 年，於民國 94 年 3 月 10 日，由 http://www.moea.gov.tw/~meco/doc/ndoc/s5_p05.htm 取得。

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。

臺灣票據交換所，民 92，*電子票據簡介*，於民國 92 年 9 月 20 日，由 http://www.twnch.org.tw/echeck/index.html 取得。

臺灣集保公司，*有價證券管理*，於民國 92 年 8 月 30 日由 http://www.tscd.com.tw/index_main_03service01.htm 取得。

臺灣證券交易所股份有限公司，民 90 年，*證券經紀商受託契約準則*，於民國 90 年 2 月 10 日，由 http://www.selaw.com.tw 取得。

劉芳梅，民 92 年，*線上金融服務逐漸普及*，於民國 92 年 8 月 25 日，由 http://www.find.org.tw/0105/news/0105_news_disp.asp?news_id=2480 取得。

蕭曉玲，民 92 年，*電子支票應用運作機制*。國立交通大學資訊管理研究所碩士論文。

Asokan, N., Herreweghen, E. V., & Steiner, M. (1998). *Toward a framework for handling disputes in payment systems*. IBM Research Division.

Bhattacharya, S., & Paul, R. (1999). Accountability issues in multihops communication. *Proceedings of Application-Specific Systems and Software Engineering and Technology*, 74-81.

Chum, D., Fiat, A., & Naor, M. (1990). Untracable electronic cash. CRYPTO 88', *LNCS 403*, 319-327.

Coffey, T., & Saidha, P. (1996). Non-repudiation with mandatory proof of receipt. *Computer Communication Review, 26*(1), 6-17.

Computergram International. (1998). *US Treasury makes first Internet payment with eCheck.* Retrieved September 15, 2003, from the World Wide Web: http://www.findarticles.com/cf_dls/m0CGN/n130/20851519/p1/article.jhtml

Cox, B., Tygar, D. & Sirbu, M. (July 1995). Netbill security and transaction protocol. *Proceedings of the First USENIX Workshop on Electronic Commerce*, 77-88. Retrieved September 5, 2002, from http://www.usenix.org/publications/library/proceedings/ec95/cox.html

Dani, A. R., & Krishna, P. R. (2001). An E-check framework for electronic payment systems in the web based environment. EC-Web 2001, *LNCS 2115*, 91-100.

FTC/DOC. (2000). *Summary of public workshop: Alternative dispute resolution for consumer transactions in the borderless online marketplace*. Retrieved May 25, 2001, from the World Wide Web: http://www.ftc.gov/bcp/altdisresolution/index.htm

GBDe. (2000). *Alternative dispute resolution*. Retrieved May 15, 2001, from the World Wide Web: http://www.ftc.gov/bcp/altdisresolution/index.htm

Gelinas, U. J. Jr., Gogan, J. L., & Wade, C. (2003). The U.S. Treasure tests a new payment mechanism. *Journal of Information Systems Education, 14*(3), 259-269.

ISO/IEC JTC 1. (1997a). Information technology — *Open systems interconnection – Security frameworks for open systems: Non-repudiation framework* (ISO/IEC

10181-4).

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

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

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

Lee, J. K., & Yoon, H. S. (2000). An intelligent agents-based virtually defaultless check system: The SafeCheck system. *International journal of Electronic Commerce, 4*(3), 87-106.

Lee, N. Y., Chang, C. C., Lin, C. L, & Hwang, T. L. (2000, Feb.). Privacy and Non-repudiation on Pay-TV Systems. *IEEE Transactions on Consumer Electronics, 46*(1), 20-27.

Liew, C. C., Ng, W. K., Lim, E. P., Tan, B. S., & Ong, K. L. (1999). Non-repudiation in agent-based electronic commerce system. *Proceedings of 10th International Workshop on Database and Expert Systems Applications*, 864 -868.

Manasse, M. (1995). The Millicent protocols for electronic commerce. *Proceesings of 1st USENIX Workshop on Electronic Commerce*. Retrieved February 20, 2000, from the World Wide Web: http://www.millicent.com/

MasterCard and VISA. (1997a). *Secure Electronic Transaction (SET) Specification, Book 1: Business Description*, version 1.0.

MasterCard and VISA. (1997b). *Secure Electronic Transaction (SET) Specification, Book 2: Programmer's guide*, version 1.0.

MasterCard and VISA. (1997c). *Secure Electronic Transaction (SET) Specification, Book 3: Formal Protocol Definition*, version 1.0.

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

Mondex Electronic Cash. Retrieved from the World Wide Web: www.mondex.com

Mullaney, T. J. (2003). The E-BIZ surprise. Business Week, 3832, 60-60.

Neuman, B. C., & Medvinsky, G. (1995). Requirements for network payment: The NetCheque perspective. *Digest of Papers on Technologies for the Information Superhighway, Compcon '95*, 32-36.

Neuman, B. C., & T'so, T. Y. (1994). Kerberos: an authentication service for computer networks. *IEEE Communications magazine, 32*(9), 33-38.

Newsbyte PM. (1999). *Asia's first electronic check service pilots in Singapore.* Retrieved September 25, 2003, from the World Wide Web: http://www.findarticles.com/cf_dls/m0HDN/1999_Feb_15/53888630/p1/article.jhtml

OECD. (2001). *Building trust in the online environment: Business to consumer dispute resolution.* Retrieved July 25, 2001, from the World Wide Web: http://www1.oecd.org/dsti/sti/it/secur/act/Online_trust/documents.htm

O'Mahony, D., Peirce, M., & Tewari, H. (2001). *Electronic payment systems for E-Commerce*. ArtTech House.

Rivest, R., & Shamir, A. (1996). Payword and microMint: Two simple micropayment schemes. *Cryptobytes, 2*(1), 7-1.

Schneider, S. (1998). Formal analysis of a non-repudiation protocol. *Proceedings of 11th IEEE Computer Security Foundations Workshop.* 54-65, 1998

Sirbu, M., & Tygar, D. (March, 1995). NetBill: An Internet commerce system pptimized for network delivered services. *Proceedings of the IEEE CompCon*.

Stavins, J. (2003). Network externalities in the market for electronic check payments. *New England Economic Review*, 19-30.

Sung, W. T., & Eun. K. P. (2004). A softward framework for non-repudiation services based on adaptive secure methodology in electronic commerce. *Information Systems Frontiers, 6*(1), 47-66.

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

Zhang, N., & Shi, Q. (1996). Achieving Non-repudiation of Receipt. *The Computer Journal. 39*(10), 844-853.

Zhou, J., & Gollmann, D. (1996). A Fair Non-repudiation Protocol. *Proceedings of 1996 IEEE Symposium on Security and Privacy*, 51-61.

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

附錄：傳統證券交易下單流程與常見糾紛

傳統證券委託交易流程如下：

(1) 投資人至證券經紀商營業處開立交易帳戶。

(2) 投資人填寫委託單後以當面委託、書信、電報、傳真等方式或直接以電話委託證券經紀商買賣有價證券 (買進有價證券時應填寫紅色買進委託書；委託賣出時則應填寫藍色賣出委託書)。

(3) 營業員確認委託資料後，將委託買賣事項轉知證券商場人員。證券商場人員依證券集中交易市場作業程序 (臺灣證券交易所股份有限公司，民 70 年，臺證業字第 2031 號公告訂定發布) 申報買賣有價證券。

(4) 證券交易所接受買賣資料，進行交易撮合。證券交易所專櫃執行人員將交易撮合結果提供給證券商。證券商將交易撮合結果回報給投資人 (或由投資人自行查詢是否成交)。

根據臺灣證券交易所股份有限公司統計(民國 94 年 11 月由 http://www.tse.com.tw/ch/investor/investor_protection/dispute.php 取得)，在受託買賣部份，常見之投資交易糾紛類型如下：

(1) 投資人於電話委託時，未說明委託價格，而營業員卻接受其委託，且自行決定價格。

例：投資人甲因與某證券商之營業員乙熟識，常電話委託下單時未敘明交易價格，而營業員乙亦自作主張自行決定交易價格，後因買賣價格不理想，致造成甲損失，引發甲乙間之交易糾紛，故投資人委託買賣應敘明交易價格，營業員亦不得自作主張，決定交易價格，方可避免類似情形之發生。

(2) 投資人當面委託之委託書未簽章，致事後無法判別交易糾紛責任歸屬。

例：某營業糾紛案例係因投資人甲委託書所勾選之買賣方式為電話委託，惟本公司查核人員檢視電話錄音紀錄時卻發現無錄音資料，但營業員乙堅持係甲當面下單，祇是未當面簽章而已，由於事後相關資料無法勾稽，致造成屬何人下單之爭議及交易之糾紛，故投資人當面委託時應填妥委託方式並於委託書上簽章，營業員亦應檢查委託書上委託方式及簽章，方可避免交易之爭議。

(3) 投資人對買賣有價證券之種類、數量、價格及買進或賣出全權委託營業員辦理。

例：投資人甲於證券商開戶下單委託買賣，後來由於投資人甲工作繁忙或其他因素無法親自看盤與委託下單，在與營業員乙熟識之情形下，且營業員乙為衝業績遂對投資人甲作盈利之保證並提議甲將其資金存入交割銀行帳戶內，並言明由營業員乙全權代為決定買賣有價證券之種類、數量、價格。後因市場行情變動造成虧損而營業員乙為增加業績及平損仍持續代客操作，而甲聽從乙之勸說陸續匯入資金增加投資金額，最後於總結算時造成甲鉅額虧損，進而衍生雙方之糾紛，此行為為法令所禁止，故投資人買賣股票應自行決定有價證券之種類、數量、價格及買進或賣出時機。

(4) 投資人未台具委任書委託他人代為下單買賣，而營業員卻逕自接受非本人且未具委任書之他人委託買賣。

例：投資人甲因長期向某證券公司營業員乙電話委託而日漸熟識，某日乙接到投資人甲女友丙電話表示因甲工作繁忙，委請丙賣出甲帳戶內之部分股票，因甲與乙平日閒聊時，知其有位女友丙，不疑有他而接受該筆委託，但事後發現係在甲毫不知情下被丙盜賣，因甲未簽具任何委任授權書或委託書，乙最後不僅賠償甲損失亦被本公司查知而受行政處分，故營業員在接受此類委託買賣時，應要求代理人台具委任授權書方可接受下單買賣。

(5) 投資人台借帳戶供營業員買賣股票。

例：某證券商投資人甲與營業員乙為朋友關係，乙為增加業績，乃向甲借用帳戶買賣股票，後因操作不利，乙甚至挪用甲帳戶內原有之款項，而引起投資人甲與營業員乙兩造間之糾紛，不但使投資人甲損失慘重，而營業員乙亦違反相關規定遭到處分，故為避免此類糾紛，投資人應避免台借帳戶供他人使用，營業員亦不得借用他人帳戶買賣股票。