行政院國家科學委員會專題研究計畫成果報告

電子商務交易協定之不可抵賴性研究

A Study on the Non-repudiation Requirement for Electronic Commerce

計畫編號：NSC 88-2416-H-009-N9
執行期限：87 年 10 月 1 日至 88 年 9 月 30 日
主持人：黃景彰　　國立交通大學資訊管理研究所

一、中文摘要

為確保電子商務交易的安全性，學術界與產業界許多專家學者相繼投入電子商務安全交易之研究。因而也制訂出許多與安全交易相關的國際標準與產業標準，諸如 CCITT X.509、SET、PKCS...等。在目前眾多電子交易安全的研究多著墨於身份鑑別、私密性與真確性，而對於交易行為的不可否認性則相對的較缺乏文獻的討論。然而在諸如訂購、付款、清算、契約、稽核...等商業行為中，不可抵賴性卻是不容忽視的。本研究計畫將廣泛蒐集相關文獻，對目前已提出之不可抵賴性機制加以研究，以歸納出在各種商業行為中所必須考慮的狀況。並對目前具有相當影響力的電子商務交易協定加以討論，評估其不可抵賴性的程度，並對其優缺點提出建議。
。

關鍵詞：電子商務、資訊安全、不可抵賴性

Abstract

Information security is an essential issue for the promotion of electronic commerce. Many scholars have studied the following security requirements: (1)authentication of business participants, (2)privacy protection of transaction data, (3)integrity assurance of transaction data, and(4)non-repudiation of transactional evidences. For fulfilling those requirements, in particular the requirements for authentication, privacy, and integrity, several international or de factor standards, such as CCITT X.509 and SET, have been proposed. In this research, we have focused on the non-repudiation requirement, which is essential for many business activities like purchasing, payment, clearance, contract negotiation,etc. We have conducted a comprehensive study on the non-repudiation issue. What are the standards that have been proposed and studied? What are the schemes adopted in well-known systems, such as SET? In this final report, we present a survey on the state of the art, and offer our assessments or extensions to existing standards and current practices.

Keywords: Electronic commerce, Computer security, Non-repudiation.

二、緣由與目的

隨著資訊科技與網際網路的迅速發展，越來越多的公司開始採用資訊網路系統處理與上游供應商及下游客戶間的交易，如訂貨、配銷、付款...等。同樣的在與消費者的交易行為中，運用網路作為商業交易的通路，進行傳統商業的各項行為，如廣告、議價、訂貨、付款及遞送交易憑證...等，亦將成為不可抗拒的趨勢。和傳統商業行為不同的是，電子商務中，每一筆交易的單據係以電子訊號的方式傳遞、儲存。因此如何確保交易資料的安全性，將成為所有交易伙伴重視的問題，也因此「交易安全性」成為推動電子商務所必須探討的核心議題之一。

何謂電子商務交易之安全性？首先，

在交易過程首先必須保證能達到交易資料的真確性（Integrity），確定交易中所有資料沒有蓄意或無心的被更改、取代、增加或刪除；其次則是交易對象的身份鑑別（Authentication），確認交易對象之身分及合法性；再者為交易行為的不可抵賴性（Non-repudiation），防止交易參與者否認交易行為曾經進行的事實；最後則是交易資料的私密性（Confidentiality），防止非法或未經授權者竊取交易內容及其相關資訊。對一個安全的電子交易系統而言，上述四項特性缺一不可。然而目前對電子商務交易的研究卻多著墨於身份鑑別、私密性與真確性，而對於交易行為的不可否認性則相對的較缺乏文獻的討論。然而在諸如訂購、付款、清算、契約、稽核...等商業行為中，不可抵賴性卻是不容忽視的。本文將以 ISO 相關國際標準所提出之安全服務架構為基礎，討論電子商務環境中的不可抵賴性安全需求。

二.相關國際標準簡介

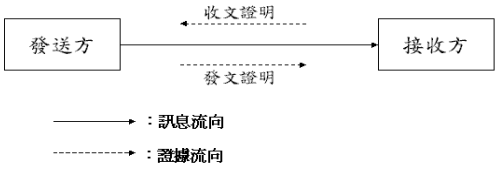
本節將簡述 ISO 7498[1]、ISO 10181[2]及 ISO 13888[3]等提供資訊安全服務架構的國際標準。其中 ISO 7498 為開放式系統間網路互連的國際標準；ISO 10181 則針對開放式系統的安全需求提出完整的架構；ISO 13888 則對不可抵賴性安全服務提出了更詳盡的定義。

2.1. 簡介 ISO 7498 中的不可抵賴性安全服務

在網際網路這樣一個由各種不同設備相互連接而形成的網路環境下，為確保網路間所有的設備都能相互連接，所有互連設備必須使用相同的通訊方式。而 ISO 7498 就是為了這個目的而制訂的網路通訊標準。在 ISO 7498 的第二部分（ISO 7498-2）則定義了網路通訊安全的通用架構，其中包含了以下五項主要的資訊安全服務：身份鑑別、存取控制、私密性、真確性、不可抵賴性。

在不可抵賴性安全服務方面，ISO 7498-2 定義了以下兩種不同型式的不可抵賴性安全服務：具有發文證明的不可抵賴性安全服務及具有收文證明的不可抵賴性安全服務。具有發文證明的不可抵賴性安全服務提供適當的證據（發文證明），以防止訊息發送方惡意的否認曾經發送訊息的事實；相對的，具有收文證明的不可抵賴性安全服務則提供適當的證據（收文證明），以防止訊息接收方惡意的否認曾經收到訊息的事實。圖一為使用上述不可抵賴性安全服務的實例。

圖一：使用發文證明與收文證明的實例



2.2. 簡介 ISO 10181 中的不可抵賴性安全服務

ISO 10181 根據 ISO 7498-2 所定義的各項安全服務，提出了一套完整的網路安全服務架構。包含各項安全服務的定義、各項安全服務的目的、可能的參與的角色.....等，至於安全服務的施行細節，則無詳細描述。該標準共分為以下七個部分：ISO 10181-1 : 安全架構綜觀
ISO 10181-2 : 身份鑑別
ISO 10181-3 : 存取控制
ISO 10181-4 : 不可抵賴性
ISO 10181-5 : 私密性
ISO 10181-6 : 真確性
ISO 10181-7 : 安全稽核

根據 ISO 10181-4，不可抵賴性安全服務應包含以下四個階段：1.證據產生、2.證據傳送、儲存與取回、3.證據查驗、4.爭議處理。圖二為 ISO 10181-4 提出的不可抵賴性服務參考架構。

圖二、不可抵賴性服務參考架構

* 資料來源：修改自 ISO 10181-4

圖二包含了不可抵賴性安全服務的前三個階段，其中第一階段為證據產生。這個階段由證據提供者向證據產生者提出產生證據的要求，在證據產生後，由證據產生者與證據提供者共同檢驗證據的合法性。根據不可抵賴性安全服務政策及其實際應用的環境，證據提供者與證據產生者可能為單一實體或個別實體。

第二階段為證據傳輸、儲存及取回。由證據產生者將證據送交證據驗證者，並由證據驗證者對證據的正確性、合法性進行驗證。在第二階段執行的過程中，可能需要由一被信賴的第三者介入，協助證據驗證者對證據的內容及其真確性進行驗證。同樣的，依據不可抵賴性安全服務政策及其實際應用的環境，證據可能直接由證據產生者傳送給證據驗證者，或是將證據儲存於特定儲存單位，再由證據驗證者在必要時取出。

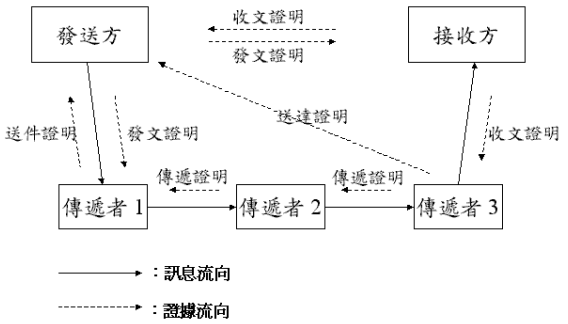
第三階段為證據驗證。證據使用者在有必要使用證據（用以證明某一行為確實曾經發生）時，可向證據驗證者提出驗證證據的要求。證據驗證者可經由適當的驗證過程（通常為單向雜湊函數、數位簽章等密碼方法），確認證據的合法性，並告知證據使用者。必要的時候，證據驗證者可要求被信賴的第三者的協助。根據不可抵賴性安全服務政策及其實際應用的環境，證據使用者與證據驗證者可能為同一實體或各別實體。

第四階段為爭議處理階段，這個階段將在發生爭議後展開。此時必須有一受爭議雙方共同信任的仲裁機關介入，由爭議雙方將所有已取得之證據送交仲裁機關，再由仲裁機關根據雙方所提出之證據，進行仲裁。

除了提出上述一般化的不可抵賴性服務架構外，ISO 10181-4 還補充了 ISO 7498-2 所定義的不可抵賴性服務的種類，其所擴充的不可抵賴性服務主要用於儲存—轉送（store and forward）的通訊架構。包括以下三種：具有送件證明的不可抵賴性安全服務、具有送達證明的不可抵賴性安全服務及具有轉送證明的不可抵賴性安全服務。

具有送件證明的不可抵賴性安全服務提供適當的證據（送件證明），以防止訊息傳遞者惡意的否認曾經接受傳遞訊息的事實；相對的，具有送達證明的不可抵賴性安全服務則提供適當的證據（送達證明），用以證明傳遞者確實已將訊息送交接收方。最後具有轉送證明的不可抵賴性安全服務則提供適當的證據（轉送證明），達成訊息在傳遞者間轉送過程的不可抵賴性。圖三為一使用上述不可抵賴性安全服務的實例。

圖三、儲存—轉送通訊架構中不可抵賴性服務的實例



*資料來源修改自 ISO/IEC 13888-3

圖三中每一項證據的處理過程皆可套用圖二所定義的參考架構。表一說明了 ISO 10181-4 所定義的各項證據在套用圖二所述之基本架構時的證據提供者及證據使用者。

表一、ISO 10181-4 所定義的各項證據的證據提供者及證據使用者

證據名稱	證據產生者	證據使用者
發文證明	發送方	接收方、傳遞者
送件證明	傳遞者	發送方
送達證明	傳遞者	發送方

傳遞證明	傳遞者	傳遞者
收文證明	接收方	發送方、傳遞者

＊ 修改自 ISO 10181-4 Annex C

2.3. 簡介 ISO 13888

ISO/ICE 13888 則由三個部分組成，它首先提供一個一般化的不可抵賴性架構，並分別提出以對稱式密碼系統及非對稱式密碼系統達成不可抵賴性服務的實施細節。共包含下列三個部分：

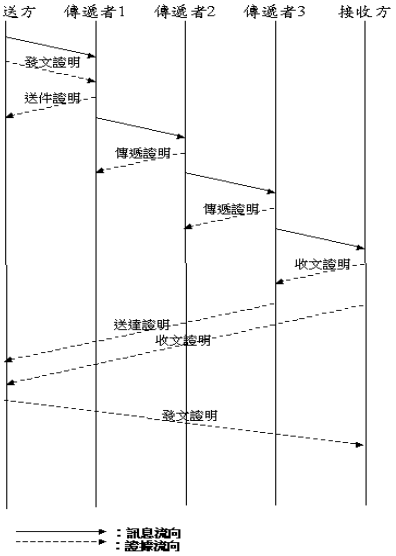
ISO 13888-1 : 安全架構綜觀

ISO 13888-2 : 使用對稱金鑰機制

ISO 13888-3 : 使用非對稱金鑰機制

ISO 13888-1 參考了 ISO 10181-4 所定義的一般化架構，並該架構有更詳盡的規範。根據 ISO 13888-1，圖三所描述的實例，在資料傳送的順序應該有圖四所描述的時間關係。

圖四、圖三的時序關係圖



除了 ISO 13888-1 所定義的不可抵賴性安全服務架構外，該標準並分別定義使用對稱式金鑰密碼系統達成該安全服務架構的方法及其細節與使用非對稱式金鑰密碼系統達成該安全服務架構的方法及其細節。分別定義於 ISO 13888-2 及 ISO 13888-3。在 ISO 13888-2 及 13888-3 所提出的實施方法中，為達成接收方與發送方雙向的不可抵賴性，均有協助證據產生、驗證工作的被信賴的第三者的參與。

至於 ISO 10181-4 中所提及，可能可以使用防竄改模組（tamper-resistant modules）、時戳（time stamping）、公證（notary）、介入訊息傳輸的被信賴的第三者（in-line Trusted Third Parity）等不可抵賴性安全服務的方法之實行細節，目前則尚無相關國際標準。

三. 電子商務環境下之不可抵賴性需求

綜合上節對相關國際標準的研究，我們可以歸納出不可抵賴性與身份鑑別相關，不同之處在於不可抵賴性需要更嚴格的證據力。一般來說身份鑑別機制主要在於防止非法的使用者冒充合法使用者進行資訊交換，以從中竊取資訊或獲取非法利益。而不可抵賴性則著重於防止合法使用者的欺騙行為。不可抵賴性機制保護交易行為之一方，在交易對象完成交易後，對方否認交易曾經進行的事實。因此在提供不可抵賴性安全服務之前，建立諸如 X.509 等適當的身份鑑別機制是必須的。本節將討論在電子商務環境下的不可抵賴性需求，並假設已有適當的身份鑑別機制。

3.1. 單向不可否認性安全服務

在電子商務環境中，附加數位簽章的商業文書的傳遞即可達成發送方的單向不可否認性安全需求。亦即經由數位簽章的驗證，發送方將無法惡意的否認曾經發送訊息的事實。

根據 ISO 10181-4 的建議，不可否認證據應包含：1.發送方的身份鑑別資訊、2.接收方的身份鑑別資訊、3.發送訊息、4.發送訊息之數位指紋、5.發送時間與日期。等五項資訊及其數位簽章即可達成發送方單向的不可否認性安全服務。但由於這種單向的不可否認機制對接收方完全沒有不可抵賴性的作用，因此僅適用於一些較不重要的商業文書、小額付款等對不可抵賴性要求較低的情況，或是當接收方具公信力，值得信賴的情況。

3.2. 雙向不可否認性安全服務

一般而言，目前研究所提供之不可抵

賴性機制多以設立被信賴的第三者的方式，提供不可抵賴性服務。此一被信賴的第三者涉入所有交易過程，並提供適當的證據給所有交易參與者，並在交易行為發生爭議時，根據適當的證據進行仲裁的工作。

被信賴的第三者的涉入勢必增加整個訊息傳遞過程的複雜度，然而在某些情況下交易雙方皆希望能擁有交易曾經進行的證據，但可能因為交易金額不大，不值得使用太複雜的訊息傳輸協定；或是沒有適當的被信賴的第三者可以協助訊息傳遞的進行。此時可以考慮採用沒有被信賴的第三者參與或僅於爭議發生時才加入處理的被信賴的第三者。由於並沒有被信賴的第三者對交易雙方進行監督，這類的不可抵賴性機制多半犧牲了交易雙方其中一方的不可抵賴性的強度，然而卻可以減少被信賴的第三者所可能造成的複雜性。因此又被稱為「弱公平」(weak fairness) 的訊息傳遞方式。

3.3. 電子支付行為的不可抵賴性

電子支付是電子商務相關研究中，最重要的課題。目前常見的支付方式可分為信用卡型(SET、iKP 等)、電子轉帳型(如 NetBill、Netcheque 等)及電子現金型(如 Ecash、Millicent 等)。信用卡型與電子轉帳型並不具有匿名性，而所謂的「線上支付」就是在網路上傳遞付款、轉帳所需使用的訊息，因此本文所提及之所有不可抵賴性服務及其實施行細節皆可應用於這類的付款過程。將原有的付款機制稍做修改，即可提供電子支付行為的不可抵賴性。

然而另一方面，電子現金型的線上支付系統，由於必須考慮付款人的匿名性，因此就很難兼顧支付行為的不可抵賴性了。使用電子現金的電子交易，若欲於交易同時留下相關的證據，以達成支付行為的不可抵賴性的需求，卻會因此破壞了電子現金的匿名性，失去使用電子現金的意義。

為同時達成電子現金的匿名性與支付行為的不可抵賴性，已有學者進行電子現金的可追蹤性（traceability）研究[4,5,6]。可追蹤的電子現金同時滿足了匿名與可追蹤兩個特性，在一般的情況下，電子現金是具有匿名性的，但經由適當公正機關的協助，卻可以去除電子現金的匿名性，以作為電子支付行為的不可抵賴性服務所使用的證據。

四. 結論

不可抵賴性相關的國際標準有 ISO/ICE 10181-4 及 ISO/ICE 13888，ISO/ICE 10181-4 對 ISO 7498-2 中提及的不可抵賴機制提出改進，並提供一個完整的不可抵賴性機制架構。而 ISO/ICE 13888 則由三個部分組成，它首先提供一個一般化的不可抵賴性架構，並分別提出以對稱式密碼系統及非對稱式密碼系統達成不可抵賴性服務的方法。

本計畫以電子商務為應用環境，探討電子商務中訊息傳遞所需的不可抵賴機制。包括了單向不可抵賴性、及雙向的不可抵賴性，及其適用環境。另外對支付行為的不可抵賴性也進行討論，在目前已提出的電子交易支付系統，如 iKP、NetBill、SET...等。對交易行為的不可抵賴性均有所討論，然而目前提出的支付系統大多只考慮到單向的不可抵賴性，亦即只對訊息的來源方有不可抵賴的機制，而無法達成雙向的不可抵賴機制。根據不同形式的支付工具，本文也討論提供不可抵賴性安全服務的可能方式。

五、參考文獻

[1] ISO 7498:1989. Information Processing Systems – Open System Interconnection – Basic Reference Model – Part 2: Security Architecture. 1989.

[2] ISO/IEC 10181: Draft International Standrad Non-repudiation Framework. Dec. 1996.

[3] ISO/IEC 13888. Information technology – Security Techniques – Non-repudiation – Part 1: General Model, Nov. 1997.

[4] Peter S. Gemmell, Traceable e-cash, *IEEE*

Spectrum, Feb. 1997.

[5] 葉士民, 電子現金之研究, *國立交通大學資訊管理研究所碩士論文*, Jun. 1996

[6] 李建宗, 電子現金的可追蹤性與使用者的隱密保障, *國立交通大學資訊管理研究所碩士論文*, Jun. 1998

（本成果報告著作人：宋振華，黃景彰）