行政院國家科學委員會專題研究計畫成果報告

電子商務產業標準之競爭、整合與應用(總計畫)

計畫編號：88-2416-H-009-025-N9
執行期限：87 **年** 10 **月** 01 **日至** 88 **年** 09 **月** 30 **日**
主持人：黃景彰　執行機構及單位名稱：國立交通大學資訊管理研究所

一、中文摘要

由於電子商務已經成為最具潛力的網際網路應用領域，如何在網路環境建造兼具公平性與整合性的商務系統攸關企業在網路時代的競爭力。本計畫的研究重點分為四部份：(1)**安全性：將具自我驗證性的密碼系統引用到金鑰交換以及會議金鑰分配協定中，提高此類協定的效率。**(2)**公平性：深入探討目前針對不可抵賴性安全服務的研究，並且以契約簽訂為例，設計了一個滿足公平性的網路簽約協定。**(3)**整合性：利用具有可擴充性的** XML **語言設計網路環境中跨組織的工作流程管理系統。**(4)**應用：為了探討使用者對於網路中電子資料交換的觀感，我們也針對花卉運銷組織主管進行實證研究，推論出網際網路** EDI **成功的關鍵因素。我們相信，本計畫的各項結果可以增進電子商務的安全性與公平性，並且為電子資料的交換與整合做了良好的示範。**

關鍵詞：電子商務、整合、公平性

Abstract

Electronic commerce is believed to be everywhere in the near future. For the competitiveness of enterprises, it would be critical to establish fair, secure, and efficient transaction systems that integrate its business systems in enterprises with their partners'. This project includes five sub-projects that have done the following tasks: (1) We have applied self-certified cryptosystems to key exchange and conference key distribution protocols so as to improve the efficiency in executing those protocols. (2) We have surveyed the state-of-the-art standards and development on the subject of non-repudiation, and have proposed a fair protocol for signing contracts over computer networks. (3) We have designed a workflow management system within organizations with the Extensible Markup Language (XML). (4) To explore users' attitude towards electronic data interchange (EDI), we have conducted an empirical study on managers in businesses for marketing channels and have discovered critical factors to the success of EDI over the Internet. This project, we believe, not only has improved security and fairness of electronic transaction systems, but has included a well-integrated system for electronic data interchange.

Keywords: Electronic Commerce, Integration, Fairness

二、緣由與目的

網際網路的普及促成了電子商務的流行，也使得在網路上進行商務活動所應該注意的議題紛紛被提出來。自從密碼學廣泛應用在機密性與真確性的保護之後，如何設計滿足公平性要求的系統已經成為密碼學的下一個挑戰。在本計畫中，我們在子計畫一中蒐集現有研究中針對不可抵賴性 [3,4,8]**的公平服務，並且在子計畫二中嘗試設計出在網路上簽訂契約的公平協定，讓公平性的研究更加完善。**

自從具有自我驗證性的密碼系統[1]**提出之後，驗證公開金鑰持有者的效率提高許多；由於不需要伺服器提供金鑰憑證讓驗證者下載憑證，所以也不需要擔心伺服器遭受主動攻擊。基於這些優點，我們在子計畫三中把具自我驗證性的密碼系統引用到金鑰交換以及會議金鑰分配協定中，讓金鑰交換的效率提高許多。**

除了安全性的研究之外，如何利用網際網路整合上下游產業的資料交換一直是十分熱門的研究主題。由於可以很容易的定義屬於自己的文件類型， XML **語言**[7]**被認為**

是一種十分具有擴充性的語言。所以，我們在子計畫四中用 XML 來描述跨組織工作流程(workflow)間的交換資訊。另外在子計畫五中，我們針對農產運銷通路設計一個應用雛型系統，並且針對花卉通路主管進行調查，以分析歸納影響 EDI 施行的關鍵成功因素。

關於上述五個子計畫的研究內容與成果，我們將在下一節中分別討論。

三、結果與討論

子計畫一、電子商務交易之不可抵賴性研究

電子商務已經從一項熱門的研究課題逐步進入我們的日常生活中。為了確保電子交易的安全性，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，也已經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[2]、SET[5]…等）。從這些與電子交易安全相關的標準中，我們可以歸納出以下幾個必要的電子交易安全因素：（1）交易參與者身份識別機制、（2）交易資料之私密性、（3）交易資料之真確性、（4）交易行為之不可抵賴性。對一個安全的電子交易系統而言，上述四項特性缺一不可。

在現有電子商務交易的研究中，身份識別、私密性與真確性的研究已經相當完備，但是對於交易行為的不可否認性則相對缺乏。由於不可抵賴性其實是訂購、付款、清算、契約、稽核…等商業行為中不容忽視的重要性質，本計畫先研究與不可抵賴性相關的國際標準，如 ISO/ICE 10181-4[3]及 ISO/ICE 13888[4]，然後再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。我們發現，目前提出的支付系統大多只考慮到單向的不可抵賴性，還無法達成雙向的不可抵賴機制。這將是不可抵賴性研究可以繼續努力的方向之一。

子計畫二、網路公平契約簽訂之研究

由於商務電子化的緣故，透過網際網路進行購物將成為十分普遍的交易行為。為了讓從事線上交易的雙方能夠處於公平的地位，也就是讓賣方能確定可以收到貨款，買方可以確定收到正確商品或服務，我們希望藉著密碼學的幫助，設計一套協定讓交易雙方在網路上共同擬定一份契約。

在這個子計畫中，我們先討論網路訂約所應滿足的需求。我們將傳統訂約種類進一步區分為單純訂約與包含預繳貨款和契約交換兩種。最後我們適當調整 J. Zhou 和 D. Gollman 所提出的公平與不可否認協定[8]，並將調整後的協定應用到上述兩類訂約環境中。

透過我們提出的兩種公平訂約協定，交易雙方可以各自留存交易證據。日後交易發生爭議時，雙方可以提出不可否認性證據來保障自己權利。我們相信這個研究可以補強目前線上交易過程中契約簽訂不足的部份，進而增加交易雙方對於線上交易的信賴感，提高使用者上網消費的意願。

子計畫三、適用於電子商務應用之具自我驗證公開金鑰密碼系統設計

為了在電子商務環境中建立安全通道，金鑰交換或會議金鑰分配協定是經常用到的核心技術。由於現有的金鑰交換與會議金鑰分配協定通常用公開金鑰密碼系統作為設計的基礎，對於公開金鑰的驗證都是以憑證或身分作為驗證的根據。在本計畫中，我們利用植基於離散對數困難度的具自我驗證(self-certified)密碼系統[1]，設計新的金鑰交換與會議金鑰分配協定。在我們所設計的系統中，使用者所持有的私密金鑰不需要被系統中心知道，而且公開金鑰的驗證能夠在一個邏輯步驟中達成。由於所有用來驗證使用者的資訊都內嵌於公開金鑰之中，使得本計畫所提出的新方法具有下列優點：(1) 系統並不需要額外的憑證以進行公開金鑰驗證；(2) 金鑰交換或會議金鑰分配的過程中可以同時驗證公開金

鑰的正確性；(3) 驗證公開金鑰所需的計算量與傳輸成本可以降低；(4) 系統不需要維護一個公開目錄或伺服器，所以不需要擔心遭受主動攻擊的可能性。

子計畫四、網際網路工作流程整合與標準之研究

除了上述企業與顧客(B-to-C)的電子購物應用之外，網際網路還能夠作為企業與企業間(B-to-B)的電子交易平台，進一步提供企業進行跨企業共同合作之流程管理。除了網際網路技術的成熟之外，虛擬組織觀念的興起也是促使組織與組織間更加緊密結合的重要因素。

在本計畫中，我們希望利用網際網路整合跨組織間的工作流程管理系統，以提升組織合作的工作效率，這將是未來企業成功的關鍵因素。所以，我們先探討工作流程系統在網際網路上之操作整合，分析工作流程管理制定協會 (WfMC,Workflow Management Coalition)所定義的提供工作流程操作整合性的主要應用程式介面，包括程序定義交換介面、工作流程客戶端應用程式介面、呼叫應用程式介面、工作流程操作整合介面、系統管理與監督介面等[6]。

此外，我們還應用 XML 來描述跨組織工作流程間的交換資訊，並透過 XML 攜帶主動規則之控制流程資訊，藉由主動規則所啟動的事件狀態來動態地決定工作流程的執行，使跨組織工作流程的執行更具彈性與效率。最後，我們用終端客戶的訂貨例子解釋這個流程如何與零售商以及製造商的流程相結合，使得上下游的廠商能夠透過整合性的工作流程系統與 XML 技術將資料與流程統合在一起。

子計畫五、XML/EDI 在農產運銷通路之應用雛型開發與實施關鍵成功因素之探討

本研究是以台灣花卉產品運銷通路的相關組織成員之主管為調查對象，分析歸納影響 EDI 施行的預期關鍵成功因素，並探討實施農產運銷通路網際網路 EDI 的應用架構及建立應用雛型。根據我們實證分析的結果，所獲結論為：(1)運輸公司與批發市場之實施網際網路 EDI 的預期關鍵成功因素有管理資訊系統的支持、資訊品質、組織之間的信賴關係及高階管理的支持；(2)農會、合作社場、產銷班之實施網際網路 EDI 的預期關鍵成功因素有資訊品質、訓練有無、高階管理的支持、系統輸出的結果、系統品質、職能劃分程度及專業技術；(3)銀行、農會信用部之實施網際網路 EDI 的預期關鍵成功因素有資訊品質、安全、高階管理的支持、管理資訊系統的支持、頻寬及系統輸出的結果；(4)農產運銷通路之實施網際網路 EDI 的共同預期關鍵成功因素有資訊品質、管理資訊系統的支持、高階管理的支持及系統輸出的結果。

四、結論

在計畫成果自評部份，我們的研究內容與計畫目標完全相符，並達成預期的目標—深入探討電子商務環境的公平性與整合性；另外，我們也針對金鑰交換與會議金鑰分配協定進行更有效率的設計。我們相信不論在學術上或實際應用上，本研究成果都深具潛力。

五、參考文獻

[1] M. Girault, Self-certified Public Keys, *Advances in Cryptology- EUROCRYPT' 91*, 1991.

[2] ISO/IEC JTC1/SC6, *ISO/IEC 9594-8, Information Technology-Open Systems Interconnection-The Directory: Authentication Framework*, 1995.

[3] ISO/IEC JTC1, ISO/IEC 10181, Draft International Standard Non-repudiation Framework, Dec 1996.

[4] ISO/IEC JTC1/SC27, *ISO/IEC 13888, Information Technology-Security Techniques-Non-repudiation-Part 1: General Model*, Nov. 1997.

[5] *SET: Secure Electronic Transaction Specification: Book 1: Business Description,*

verion 1.0, May 31, 1997.

[6] Workflow Management Coalition, *Workflow Management Coalition: Workflow Reference Model*. (http://www.aiim.org/wfmc/standards/docs/glossary.pdf)

[7] World Wide Web Consortium, *Extensible Markup Language (XML)*. (http://www.w3.org/XML)

[8] J. Zhou and D. Gollman, Observation on Non-repudiation, *Advances in Cryptology: Asiacrypto'96*, 1995.

(**本成果報告著作人：廖耕億，黃景彰**)