行政院國家科學委員會專題研究計畫　期中進度報告

子計畫四：行動電子商務之安全代理人交易模式設計與平台實作(2/3)

計畫類別：整合型計畫
計畫編號：NSC91-2213-E-002-047-
執行期間：91 年 08 月 01 日至 92 年 09 月 30 日
執行單位：國立臺灣大學電機工程學系暨研究所

計畫主持人：雷欽隆

計畫參與人員：尤焙麟　邱允鵬　蘇文鴻　江彬榮

報告類型：精簡報告
報告附件：出席國際會議研究心得報告及發表論文
處理方式：本計畫可公開查詢

中　華　民　國 92 年 5 月 26 日

行政院國家科學委員會專題研究計劃執行進度報告

行動電子商務之安全代理人交易模式設計與平台實作 (2/3)

Design and Implementation of Secure Agent-Assisted Transaction Model in Mobile Commerce (2/3)

計劃編號：NSC-91-2213-E-002-047

執行期限：91 年 8 月 1 日至 92 年 7 月 31 日

主持人：雷欽隆　台大電機系教授

一、中文摘要

由於行動商務讓使用者可以在任何時間、任何地點從事買賣交易、休閒娛樂、線上工作等事項，行動商務勢必大幅改變人們的生活型態。而且行動商務所提供的通路可以到達原本網際網路電子商務所不能涵蓋的族群。因此行動商務的發展不僅會讓整體電子商務更加蓬勃，也會為人類的生活帶來無限的便利。然而，行動裝置具有先天性的限制，如果一昧將網際網路電子商務模型套用在行動商務上，將嚴重阻礙行動商務的推展。本計畫的目標即在於行動電子商務中軟體代理人平台之研發與建置，研究主題包括通用軟體代理人基礎架構、行動付款系統及安全交易機制三大部分。本報告中將描述本計畫在第二年度中的執行進度與發展成果、以及未來一年的計畫與展望。

關鍵詞：行動電子商務、軟體代理人、電子付款系統、安全機制、智慧卡

Abstract

As the technologies of wireless communication are getting matured, the original transaction model in the electronic commerce is moving forward to a new generation. To successfully shift to the new paradigm of mobile commerce, it is important to design revolutionary transactional mechanisms as well as automated user interfaces. Under such circumstances, software agents are introduced to replace the traditional

human-driven operations and simplify the process of transactions. Mobile commerce will benefit a lot from the agent technology because of its autonomy and flexibility. In this project, we are going to design and implement a secure platform for agent-assisted transactions in mobile commerce. Three important issues will be addressed and researched extensively, including the construction of a generic infrastructure for software agents, the deployment of a mobile payment system, and the design of a secure transaction model. In this report, we briefly describe the progress of our research and implementation in the second year as well as our prospection of the coming year.

Keywords: Mobile Commerce, Software Agent, Electronic Payment System, Security, Smart Card

二、緣由與目的

在 2.5G、3G 甚至 4G 行動網路陸續進入市場之後，行動網路的頻寬已經能夠滿足大部分應用的需求。結合行動網路與網際網路將可提供主動，即時隨地以及個人化的服務，這些優勢將隨著電子商務交易的普及，使得行動電子商務在未來數年有驚人的成長。全球產業分析顧問公司 IDC [15] 在報告中預測美國行動電子商務(Wireless M-Commerce)金額在西元 2004 年將成長至二百億。歐洲更是在西元 2003 年前就可達到百三十億，Wireless Week [16] 週刊也預測，在西元兩千零三年以前，手機連上網際網路會超過個人電腦，專業顧問研究公司 Gartner Group [17] 同時也指出，除北美 Internet 普及的國家外，行動電子商務將占 C2B 電子商務市場的百分之四十。

然而，無線通訊有著低頻，高費率與通訊品質不穩定的缺點，所以如果想要將網際網路付款機制實際在無線網路上，就必須修改使其適應無線網路特性，舉例來說， SET [18][19] 付款系統在安全性上雖具公信力，但若將它原封不動地使用在行動電子交易時，使用者就必須花費昂貴的通訊費取得商品資訊、商家資訊、比價、議價以及達成協議後所進行的 SET 付款程序，這又包括取得商家與付款柵門(Payment Gateway)的憑證、在計算量有限的無線通訊設備上認證憑證、付款簽證、等候商家與付款柵門證認，如此冗長的交易過程，使用者都必須線上完成，龐大的通訊費令人望之卻步。

消費者購買行為(Consumer Buying Behavior)可分為以下六個階段：認知需求、搜集商品資訊、搜集商店資訊、決策與議價、付款與交貨以及評價與售後服務。未來的交易平台應對這六階段提出整合性的解決方案，因此我們視付款為交易系統的一部份而非獨立程序，基於這樣的觀點，我們提出以行動軟體代理人為基礎的行動電子商務平台，以解決無線網路低頻寬、低穩定度、高通訊費與行動裝置電力有限、計算量有限的問題，甚至在不用修改現有網際網路付款系統，就

可讓行動消費者以最經濟簡便的方式使用現行電子付款系統。

以前述 SET 付款交易流程為例，行動軟體代理人可藉由過去的經驗及行動用戶直接的命令作為搜集資訊與購買決策的依據，行動用戶離線設定欲購買商品或服務，傳送行動軟體代理人至網際網路後仍保持離線，行動軟體代理人開始搜集資訊、下購買決策，取得商家與付款柵門購買與身份憑證後返回行動裝置，返回動作可由行動軟體代理人發送短訊給使用者，由使用者上線取回行動軟體代理人或者由我們設計的系統本身提供主動返回(Server Push)的功能，使用者在同意購買後，在行動裝置上驗證行動軟體代理人所帶回的商品購買憑證與付款柵門身份憑證、簽署付款憑證、傳送行動軟體代理人至商家完成付款，行動軟體代理人在取得收據後返回行動裝置報告交易結果。如此一來，行動消費只需四次短暫上線即可完成，對使用者而言，若系統提供行動軟體代理人主動返回的功能，則只需處理二次的傳送動作，有效解決無線網路低頻寬、低穩定度、高通訊費等問題，至於行動裝置有限電力與計算量的問題，我們將設計一套低運算與通訊量的高效率的安全付款機制，參考 Schnorr [21] 在西元一九八九年所提出計算量、通訊量均少且能預先計算的認證協定，並採用效率較高的電子簽章演算法[1] ，利用低運算量的雜湊函數鑄電子錢，避免使用高運算量的 RSA 公開金鑰系統，改採對稱式加密系統或運算量較低的橢圓密碼系統，這些都是行動付款協定設計的方向。

在我們的架構下，搜集資訊、比價與決策同屬交易系統的一部份，因此行動軟體代理人的安全性影響整個交易系統的安全性，舉例來說，當行動軟體代理人到各商家搜集商品資訊時，惡意的商家若篡改行動軟體代理人先前所取得其家商家的報價，則會導致行動軟體代理人在錯誤的資訊下作出錯誤的決策，造成消費者的損失，因此本計畫將架構出一套安全的行動軟體代理人交易平台，達成下列目標：

1. 保護行動軟體代理人交易平台本身不受外來行動軟體代理人的攻擊。
2. 保護行動軟體代理人不受其他行動軟體代理人的攻擊。
3. 保護行動軟體代理人不因平台本身的攻擊而導致不公平交易。

三、結果與討論

在第二年度的研究計畫中，我們已經規劃出適合行動裝置使用的付款系統以及代理人平台之架構，並且完成雛形的實作與安全性分析。我們將這些成果整理條列如下：

(1) 行動電子商務中付款系統的研究：由於行動商務用戶端系統通常運算能力較差、記憶容量較少、連線品質不穩定、顯示與輸入裝置較不方便，因此以往為網際網路電子商務所設計的電子付款系統並無法直接移植到行動的世界。我們目前研究努力的方向包括：

- 以 PDA 為平台的電子付款機制。PDA 的運用越來越普及，包括各行各

業的上班族、快遞人員、司機、醫護人員等等將來都可能人手一台 PDA，因此利用 PDA 作為電子付款用戶端平台或收款端平台都是非常可行的做法。但是 PDA 並不像智慧卡具有防竄改的功能，因此我們設計了一套適用於 PDA 的安全付款機制。此外，我們也設計了多套以 PDA 為平台的行動 POS 端末機，讓商店端可以透過無線通訊在任何時間任何地點進行線上付款授權申請。

- 以手機作為用戶端平台的付款機制。我國行動電話的門號數已經突破 2000 萬，使用人口更早已過半。手機是人們最有可能隨身攜帶的物品之一，因此使用手機作為用戶端平台是非常合適的選擇。我們已經設計出以手機作為電子付款時的身分鑑別工具。而且我們的付款機制可以同時用在實體商店、網際網路電子商務、行動電子商務等環境。在未來一年內，我們將積極完成安全性與不可否認性的分析與驗證。

(2) 研發軟體代理人系統：目前行動電子商務最大的限制在於有限的頻寬及昂貴的通訊費用。就算使用 GPRS 或 3G 等全時連線（always-on）的網路，行動裝置的高度移動特性仍然會是連線穩定度最大的不利因素。何況在手機侷限的螢幕上進行瀏覽本身就是非常不方便的事情。若我們在系統供應商端及商家伺服器中間，設置一代理人平台，讓軟體代理人可經由客戶端的授權負責商品搜尋比價、購買、甚至付款的動作，不但可以節省使用者的通訊費用，更可以讓使用者體驗方便無比的行動商務體驗。但是要實作一軟體代理人系統，並將其融入行動電子商務系統之付款機制中，用以維持使用者、通信業者、商家、銀行及認證機構間良好的透通性、及使用上的便利性，並不是一件簡單的工程。我們目前已經定義出需求與目標，並且規劃出行動代理人軟體與平台的架構，未來一年中我們將針對各個議題深入分析其安全性與可行性，並且完成實作。

四、成果自評

在第二年的計劃執行中，我們已經達成預計的目標。在以手機為用戶端平台的電子付款機制中，我們設計出了一套適用於多領域的付款模型，並且完成雛形的實作。如果能應用於現實生活之中，將會成為行動通訊的殺手級應用（killer application）之一。此外，我們對於行動代理人的應用也深具信心。行動代理人如果能順利應用在行動電子商務中，對於人類生活模式更是一大革命。因為人們可以真正隨時隨地利用隨身攜帶的行動裝置送出代理人軟體，並且隨後就可以得到商品與服務的最佳組合。因此，我們將在未來一年半內朝這個目標繼續努力。

五、參考文獻

1. C.-I. Fan, and C.-L. Lei, “A User Efficient Fair Blind Signature Scheme for Untraceable Electronic Cash,” Journal of Information Science and Engineering,

2000.
2. C.-L. Lei, and C.-I. Fan, “Low Computation Partially Blind Signatures for Electronic Cash,” IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, Vol. E81-A, No. 5, pp. 818-824, 1998.
3. C.-I. Fan, and C.-L. Lei, “User Efficient Blind Signatures,” IEE Electronics Letters, Vol. 34, No. 6, pp. 544-546, 1998.
4. C.-I. Fan, C.-L. Lei, C.-Y. Chang, and P.-L. Yu, “An Efficient Divisible Blind Signature Scheme,” Proceedings of 8th Conference on Information Security, pp. 215-224, 1998.
5. C.-L. Lei, and C.-I. Fan, “Low Computation Partially Blind Signatures for Electronic Cash,” Proceedings of National Computer Symposium 1997, Vol. 2, pp. C-101-C-106, 1997.
6. Sonera,ioSonera Mobile Pay, le Sonera Ltd.. http://www.sonera.fi/english/solutions/mobilepay/.
7. Ioannis Mavridis, George Pangalos, and Sead Muftic, “iuA Secure Payment for Electronic Commerce,” 10th International Workshop on Database and Expert Systems Applications Proceedings, pp. 832-836, 1999.
8. Yi Mu and Vijay Varadharajan, “A New Scheme of Credit Based Payment for Electronic Commerce,” 23rd Annual Conference on Local Computer Networks, (LCN ’98) Proceedings, pp. 278-284, 1998.
9. K.-C. Wu, “A Notational Payment Scheme for Mobile e-Commerce.”
10. Durlarcher Research Ltd., “Mobile Commerce Report.”
11. Upkar Varshney, Ronald J.Vetter, and Ravi Kalakota, “Mobile Commerce: A New Frontier,” IEEE Computer, Vol. 33, No. 10, pp. 32-38, 2000.
12. Chang Woo, “Vicarious Certification and Billing Agent Web Information Service,” Proceedings of Twelfth International Conference on Information Networking (ICION-12), pp. 344-349, 1998.
13. Dong Won Kim, Kyung Pyo Jun, Geun Teak Ryu, and Hyeon Deok Bae, “Development of an Infoshop Service System,” ICCE ’96, June 1996.
14. Berry Schoenmakers, “Security Aspects of the Ecash Payment System”, LNCS 1528, pp. 338-352, 1998.
15. IDC Web Site, http://www.idc.com/.
16. Wireless Week Web Site, http://www. wirelessweek.com/.
17. Gartner Group Web Site, http://www. gartner.com/.
18. X. F. Wang, K. Y. Lam and X. Yi, “Secure Agent-Mediated Mobile Payment,” PRIMA ’98, LNAI 1599, pp. 162-173, 1999.
19. William Stallings, “Cryptography And Network Security”, Prentice Hall.
20. Forrester Web Site, http://www.forrester.com/Home/0,3257,1,FF.html.
21. C. P. Schnorr, “Efficient Signature Generation For Smart Cards,” Advances in Cryptology, CRYPTO ’89, pp. 392-252, 1989.
22. C. Bryce and J. Vitek, “The JavaSeal Mobile Agent Kernel,” Proceedings of the Third International Symposium on Mobile Agents, pp. 103-116, 1999.
23. T. Sander and C. Tschudin, “Protecting Mobile Agents against Malicious Hosts,” G. Vigna (Ed.): Mobile Agents and Security, Springer-Verlag, pp. 44-60, 1998.
24. F. Hohl, “Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts,” G. Vigna (Ed.): Mobile Agents and Security, Springer-Verlag, pp. 92-113, 1998.
25. G. Vigna, “Protecting Mobile Agents through Tracing,” Proceedings of the Third ECOOP Workshop on Operating System Support for Mobile Object Systems, 1997.

26. Xudong Guan, Yiling Yang, and Jinyuan You, "POM-a Mobile Agent Security Model against Malicious Hosts", Proceedings of the Fourth International Conference on High Performance Computing in the Asia-Pacific Region, Vol. 2, pp. 1165-1166, 2000.