具便捷性與安全性之行動消費者主導交易協定

薛夙珍

朝陽科技大學資訊管理學系

陳星百

逢甲大學資訊工程學系

摘要

隨著無線網路基礎建設的日趨成熟與手持設備的普及，促進了行動商務的發展，使得行動網路上所呈現的商品與服務種類日益豐富。然而，受制於行動設備有限資源之行動用戶在運用以商家主導之商業模式，經常需花費大量的資訊蒐集時間與連線成本，此外，繁複的行動交易程序更將降低其參與之意願。本文提出兼具便捷性與安全性之全球化行動消費者主導交易協定，應用條件採購單交易模式於資源珍貴之行動商務環境，減少所需耗費的搜尋與交易成本，並降低對行動設備之輸出入與通訊等資源需求。協定的設計藉由採購條件之提出，賦予行動消費者主導商品樣式與價格之權利，與符合其消費需求的潛在商家進行交易，以提供消費者一個兼具個人化與最高購物效益的交易模式。此外，協定採用具效率之密碼技術，以適應於低運算資源的行動環境下運作，並建立安全與公平之全球化行動交易環境，進而保障買賣雙方之交易權益。

關鍵詞：行動商務、消費者主導、資訊安全、個人化

A Convenient and Secure Buyer-driven Transaction Protocol over the Mobile Internet

Sue-Chen Hsueh
Department of Information Management, Chaoyang University of Technology

Hsing-Bai Chen
Department of Information Engineering and Computer Science, Feng Chia University

Abstract

Wireless technology is boosting the accessibility of Internet services to mobile users. Having the easy-to-carry mobile devices, mobile users now may conduct transactions anytime and anywhere, but they also suffer from the restrictions like limited computing power, small storage space, poor input/output interfaces, etc. Using such resource-limited devices to search services/products in the traditional seller-driven commercial model is more time-consuming than ever. To reduce the search time and the connection costs of mobile users, this paper presents a secure and convenient buyer-driven commerce model. We adopt and improve the conditional-purchase ordering mechanism, which allows users to specify their unique requirements and filter the intended merchants on public servers. We also provide light-weight security mechanisms for confidential and undeniable transactions without demanding high-end mobile devices. Therefore, both buyers and sellers will benefit from the personalized mobile commerce model.

Keywords: mobile commerce, buyer-driven commerce model, undeniable transactions, personalization

壹、緒論

隨著通訊與無線網路技術的突破，使用行動設備上網的人口將日益增多，預估至2005年全球將會有3億消費者透過行動設備購買無線內容與服務(Varshney 2002)，並發展成為全新風貌的商業型態—行動商務(Mobile Commerce)。Durlacher研究機構對行動商務定義為，透過行動設備經由無線網路與有線的網際網路中之電子商務架構連結，以進行有價的交易行為(Durlacher 2000)。行動商務在各方一致看好之下，行動商務相關之基礎建設、技術標準與服務應用已被戮力地開發及實行。由於行動設備之高度普及與行動商務市場之逐漸擴展，大量現行電子商務廠商與傳統實體零售商無不積極推出相關的無線服務以吸引消費者，如日本NTT DoCoMo於1999年2月所推出的i-mode服務，至2004年1月為止所提供的行動官方網站(Official Sites)數已增加為409萬個，而非官方網站(Unofficial Sites)於同期亦擴增到7,270萬個(NTT DoCoMo 2004)。透過具個人化之行動設備，用戶將可以隨時隨地存取網路上提供的多元服務、區域資訊與個人化商品，以豐富其生活及便利工作模式(Barnes 2002；Kalakota & Robinson 2001；Senn 2000；Varshney et al. 2000)。

面對市場普及的商家主導(Seller-driven)商業模式下，即商品規格與售價皆由販售之商家所制定，消費者僅能蒐集商品資訊與比價。然而，隨著網路服務與資訊日益豐富，消費者要尋找預期的資訊顯得越漸艱難，且商品比價及下單程序所需耗費的時間與通訊成本亦隨之增加，而導致消費者於過程中放棄交易之機率更為提升。依據Durlacher研究機構發現，當交易程序每額外增加一次需由消費者點選或輸入的操作，其交易成功機率將會降低50% (Durlacher 2000)；以此經驗觀之，尤以侷限於不友善的輸出入介面、低資料傳輸率、有限運算能力與較小記憶空間的行動商務最明顯。其次，面對持有具個人化通訊設備之行動消費者，商家主導商業模式所提供之商品樣式與價格的彈性較低，無法符合特殊需求的應用程式或相容於該行動設備規格之特定商品或服務，如支援某廠牌型號行動設備的攝影程式撰寫或具差異性之特定曲目鈴聲編輯等，消費者卻無從依其喜好變更商品樣式或需花費更高單價訂做。另外，虛擬商業模式下因缺乏具安全性之交易與付款機制，致使網路交易糾紛與詐欺事件頻傳；依據消費調查發現，88%的消費者不願參與尚未建立完善安全制度之交易活動(Datamonitor 2000)。然而，以輕小且易於攜帶為目的所設計之行動設備在受限於運算資源不足下，採用傳統繁複的安全密碼技術將導致交易處理所需時間大幅拉長，甚至因不堪運算負荷過大而導致交易失敗。

因此，行動交易的便利性與安全性已成為消費者是否願意參與行動商務之關鍵。本文以獨具移動性、定位性與個人化等特性的行動網際網路(Mobile Internet)為背景，應用消費者主導(Buyer-driven)商業模式，允許行動消費者將包含個別消費策略，如選擇成交價格越低、交易時效最快、商家信用優良、商家距離最短或商品比價資訊查詢，以及欲購買商品之樣式描述、價格與交易有效期限等需求填寫於條件採購單

(Conditional Purchase Order, CPO)，透過張貼在公正單位所維護的公佈欄內，以供有興趣的賣方瀏覽並提出交易請求。此交易模式內，消費者無須經由資源受限的行動設備而花費大量時間與連線成本來收集商品資訊，且可藉由填具條件採購單之方式主導商品的規格及成交價，以達到交易便捷性與個人化等目的。此外，本文提出安全的資訊商品交易協定，採用具效率的密碼技術，確保付款資訊與資訊商品的隱密性，以及達到交易之不可否認性，以滿足行動商務之即時性、安全性與移動性等目標，進而吸引行動用戶參與。

本文架構如下：第貳節介紹相關文獻，第參節描述行動消費者交易模式之架構與條件採購單格式的制定等，並於第肆節提出包含漫遊身份鑑別、交易付款及結算處理之交易協定，第伍節則分析及探討協定之安全性與效率性，最後為本文做一總結。

貳、文獻探討

一、行動交易平台之探討

（一）行動身份鑑別機制

行動通訊網路提供用戶具可移動與立即收發特性的交易環境，無須受有線的束縛。而且，人手一機的行動設備，已成為電信網路提供業者推行個人化服務之主要終端媒介，更可搭配電信或無線網路的追蹤定位技術，適時提供用戶所在的區域服務(Durlacher 2000；Tsalgatidou & Pitoura 2001)。因為行動商務支援移動性，用戶攜帶行動設備而跨入陌生無線網路進行商務活動的機會增加，在行動商務獨具的跨區漫遊功能下，可以提供用戶跨區使用行動設備進行通訊並連線存取網路資源(Durlacher 2000)，如圖 1 所示。

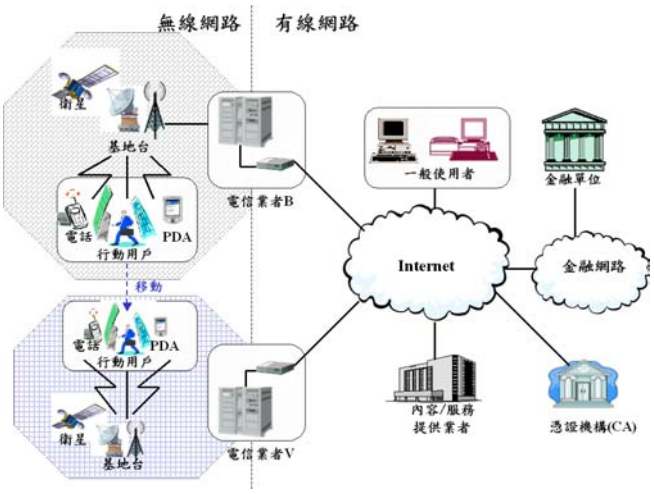

圖 1：行動用戶跨區交易示意圖

一般而言，與行動用戶建立契約關係之電信業者，稱之為註冊電信業者(Home Network Operator)，核發 SIM (Subscriber Identification Module)卡給契約用戶，SIM 卡內存有具唯一性的契約用戶識別碼 IMSI (International Mobile Subscriber Identity)、對應的身份鑑別金鑰(Authentication Key)與用戶目前所在之網域資訊 LAI (Location Area Identity)。為了鑑別用戶身份的合法性，註冊電信網路內的身份鑑別中心 AuC (Authentication Center)儲存有契約用戶的用戶識別碼 IMSI 與對應之身份鑑別金鑰。作法是當用戶使用插有 SIM 卡之行動設備，於註冊電信業者所提供的行動服務網路（以下稱為註冊電信網路(Home Network)）請求存取服務，註冊電信業者透過比對用戶傳送的 IMSI 與存於 AuC 內之 IMSI，鑑別用戶身份的合法性。若為合法用戶，則授權用戶存取內容／服務提供業者所供應之無線服務。

只要提供行動網路的電信業者彼此間提供漫遊服務，行動用戶即可於各城市間移動並連結上網，進而建構出全球化的交易平台。在支援漫遊服務的網路環境下，行動用戶因移動而跨入一個陌生的無線服務網路，本文稱此網路為漫遊電信網路(Visited Network)，而提供漫遊電信網路之業者稱為漫遊電信業者(Visited Network Operator)。一般而言，電信網路內之基地台(Base Station)每隔一段時間會自動發送其所屬的 LAI。因此，行動設備接收到漫遊網路所發送之 LAI 值，經由與 SIM 卡內之儲存值比對。若 LAI 值不同，則可判斷用戶已離開原註冊電信網路，便會發送區域更新請求。亦即，用戶之註冊電信業者的系統與漫遊電信業者的系統將會啟動換手(Handoff)作業，讓行動設備得以在漫遊電信網路內繼續享有行動通訊之服務。在換手的過程中，行動設備將會有短暫的訊號中斷，但行動用戶並不易明顯察覺。然而，當換手的過程因故而發生作業失敗，系統將會啟動回復(Rollback-recovery)機制使得換手作業可以順利完成。文獻(Lin & Dow 2001；Lin & Shin 1998；Park et al. 2002；Park et al. 2003)已分別提出回復的方法，其細節程序超出本文的介紹範疇，本文僅著重於區域更新之安全議題上。因行動用戶與漫遊電信業者之間未具信任之契約關係，必須執行所持行動設備之所在區域更新程序，完成用戶、漫遊電信業者與註冊電信業者三者間的身份鑑別作業後，方能在漫遊電信網路內參與商務活動。漫遊電信業者將區域更新請求轉送給用戶的註冊電信業者以驗證是否為合法用戶，若為合法用戶，註冊電信業者將核發用戶與漫遊電信業者間傳輸使用的通訊金鑰，以讓雙方鑑別彼此是否為合法交易對象，進而允許用戶於漫遊服務網路內存取加值服務，達到跨區交易之目的(Boman et al. 2002；Grecas et al. 2003；Pagliusi 2000)。

通常，電信業者扮演行動入口網站提供者的角色，與無線加值服務提供業者合作，以提供用戶更豐富的行動服務。另外，由於擁有用戶的個人資訊，用戶的註冊電信業者在行動商務交易上成為授權與索款負責單位。如日本電信巨擘 NTT DoCoMo 提供 i-mode 行動入口平台(NTT DoCoMo 2004)，授權用戶存取官方與非官方網站資源，並代收使用的加值服務款項。

（二）行動付款方式

隨著行動商務應用日益蓬勃，行動消費者所採購的商品包含低價之電話圖鈴、即時資訊或電影票等資訊商品，亦涵括高價的機票、消費性電子設備或飯店預約等。電子商務已提供各式付款系統以延伸交易模式之應用(Asokan et al. 1997；Sirbu 1997)，這些付款機制亦被移植至行動網際網路(Jin et al. 2002；Kim et al. 2002；Varshney 2002；Zheng & Chen 2003)，以促進行動商務更趨於完善。

自 1999 年成功推行 i-mode 行動服務後，日本市場已儼然成為行動商務推行之重要觀察指標。依據 InfoCom 研究機構調查發現，日本地區的行動用戶最喜歡使用之付款機制前二名依序為合併電信帳單(30.7 %)與信用卡(28.5 %)等付款機制。另外，南韓地區用戶最常使用的付款方式亦為合併電信帳單(55.2 %)與信用卡(26.8 %)等付款方式(Naruse 2002)。其中，合併帳單付款方式意指於固定期間，註冊電信業者彙整契約用戶於期間內所使用之加值服務費用，並結合語音帳單一併寄發予用戶。由電信業者代收加值服務費用，再分別將款項轉交給該內容供應商的付款方式。合併帳單付款機制允許用戶無須與個別加值服務供應商一對一進行繳款，僅需於固定期間內對註冊電信業者繳交合併費用。針對行動商務之小額付款，合併電信帳單付款已經提供便利的解決方案(Durlacher 2000)。另外，因為信用卡可以消費的額度高，適合高單價的商品交易。除了需要繁複的密碼技術以確保付款資訊之安全性與檢驗信用卡的有效性外，並需建立完善的信用管理，以避免電信業者之壞帳過高(Ginzboorg 2000)。

然而，支援漫遊服務之商務環境下，行動消費者於各電信網路內移動，將使得註冊電信業者無法立即得知消費者於各漫遊網路內之消費情形，通常需於固定期間後，由個別漫遊電信業者發出結算請求時才會得知。因此，行動消費者可能於漫遊電信業者與註冊電信業者間進行結算程序前，移動至多個漫遊電信網路並大肆消費，造成因無法繳清消費金額而導致的電信業者與金融單位壞帳增加之風險。另外，未建立不可否認性的交易機制下，行動消費者會質疑漫遊電信業者是否虛報消費金額或偽造交易記錄而超收交易費用，漫遊電信業者則擔心漫遊用戶否認交易記錄而拒絕支付交易款項(Herzberg 2003)。

（三）交易安全技術

商務活動為確保交易的安全性，包含私密資訊的隱密性、確認交易對象真偽之身分鑑別性與可釐清交易糾紛之責任歸屬的不可否認性等，多以密碼技術輔助。其中，採用不同金鑰對私密資訊加解密的密碼技術為非對稱式密碼法(Asymmetric Ciphers)，加解密使用金鑰對(Key Pair)，包含可對外公佈的公開金鑰與由金鑰持有者秘密保存之私密金鑰。應用於傳送方 A 以接收方 B 所公佈的公開金鑰 PK_B 對私密資訊 X 進行加密處理，產生密文 $E_{PK_B}(X)$傳送給接收方，以達到傳輸訊息的隱密性。唯持有對應私密金鑰的接收方 B 才可對密文 $E_{PK_B}(X)$進行解密運算，而推算出訊息原文。如此，可確認通訊對象非不法人士所偽裝，以達到訊息的身份鑑別性。此外，非對稱式金鑰密碼法支援數位簽章的功能。當訊息為交易資訊或需存證的文件時，訊息簽證

者 A 可使用所持有的私密金鑰 SK_A 對訊息 M 進行簽章處理，產生簽章摘要值 $S_A(M)$ 傳送給驗證方 B。以私密金鑰運算的文件可視為金鑰持有人對該文件進行簽章處理，驗證方 B 僅需以文件簽署者 A 的公開金鑰 PK_A 對該文件進行運算，即可確認該文件確實經由簽署者本人所簽章。此特性常被使用於交易處理上，以作為糾紛發生時的憑證，達到交易之不可否認目的。非對稱式金鑰密碼法可提供高階安全保護，缺點是需耗費大量運算資源。另外，當一把金鑰可同時用以訊息之加密與解密處理，稱之為對稱式金鑰密碼法(Symmetric Ciphers)，透過傳訊雙方事先協調的通訊金鑰對訊息加密或解密處理，可確保傳輸訊息的隱密性與身份鑑別性。對稱式金鑰密碼法相較非對稱式密碼法可以迅速完成運算處理，降低運算資源耗費，缺點為無法提供訊息不可否認性機制，與面臨如何安全協商傳訊雙方所使用的通訊金鑰之問題(Schneier 1996)。

目前已有許多研究機構與學者分別針對跨區交易之身分鑑別機制(Chen & Hsueh 2003；Horn & Preneel 2000；Samfat et al. 1994；Stach et al. 1999)與具不可否認性的交易付款方式(Chen & Hsueh 2003；Herzberg 2003；Horn & Preneel 2000；Dai & Zhang 2003)等議題進行探討。然而，大多數協定採行大量且繁複的公開金鑰加密系統，將難以順利運行於資源受限的行動商務上。另外，繁複的交易機制，使得著重付款效率性的小額付款發生作業延遲。因此，本研究將採用低運算資源耗費的密碼技術，建置具效率、高攜帶性與低成本的安全交易機制，保障買賣方之權益。

所採用之資訊傳輸方法(Chen & Hsueh 2003)以單向雜湊函數(One-way Hash Function)、XOR 運算與訊息鑑別碼 MAC (Message Authentication Code)密碼技術建構，這些密碼技術除了不受各城市國家進出口管制外，還具有快速產生運算結果與具固定資料長度輸出等特性，適合於運算與儲存資源有限的網路環境(Bird et al. 1995)。而且，單向雜湊函數與 MAC 密碼技術具有無法自輸出值 $H(m)$回推輸入值 m 之不可逆性(Schneier 1996)。訊息傳送方 A 將訊息 $\{Y, H(X), (X \oplus MAC_{AB}(Y, H(X)))\}$ 傳遞給接收方 B，其中 X 表示應被保密的資訊，Y 為一般可公開的資訊。於商務活動中，此私密訊息 X 可為包含具償贖能力之代幣值或信用卡號等電子付款資訊。當接收方 B 取得訊息後，可以利用與傳送方共同持有之通訊金鑰 K_{AB}，將訊息 Y 與單向雜湊值 $H(X)$透過 MAC 密碼技術計算出 $MAC_{AB}(Y, H(X))$摘要值，並可自 $\{X \oplus MAC_{AB}(Y, H(X))\}$中取出秘密資訊 X。換言之，因為通訊金鑰 K_{AB} 僅為傳送方 A 與接收方 B 持有，$MAC_{AB}(Y, H(X))$ 值只有合法傳送與接收雙方可計算產生，故可避免有心人士偽裝成合法單位，或從傳輸資訊中竊取並得知秘密值 X，達到通訊雙方之身份鑑別性與訊息隱密性的要求。另外，接收方只需將取出之秘密值 X 利用單向雜湊函數計算，比對其輸出值 $H'(X)$與傳輸訊息中接收的 $H(X)$值是否相同，若 $H'(X)=H(X)$，即可判斷秘密資訊 X 之真確性，以杜絕資訊於傳輸過程中遭受竄改或偽造。

為了達到不可否認性，雜湊鍊(Hash Chain)技術被採用。方法為：先產生隨機值 r_0 並秘密保存。以 r_0 為根(Seed)可以產生長度為 n 的雜湊鍊 $r_m = H^m(r_0)$ $(m = 1, 2, .., n)$。因為單向雜湊函數具備不可逆特性，任何人若取得 $r_i = H(r_{i-1})$ $(0 < i \le n)$，將可以求得 $r_i \sim r_n$ 的值，但無法反推得 $r_0 \sim r_{i-1}$；除了持有秘密值 r_0 的人。換言之，只有持有秘密值 r_0 的人才有能力產生合法的 $r_0 \sim r_n$ 值。運用此特性於商務交易上，持有 $r_0 \sim r_n$ 值的

消費者 透過公正單位授權即具有 n 消費額度。當商家收得 j 消費單位 r_{n-j}，只要符合 $r_n = H^j(r_{n-j})$ $(0 \le j < n)$，即可以驗證 r_{n-j} 的合法性，並可向該消費者索款，而消費者無從抵賴。

另外，為解決對稱式密碼法存在之通訊金鑰協調的問題，本研究採用 Diffie-Hellman 金鑰交換密碼法(Diffie & Hellman 1976)以安全地協調出傳訊方彼此間的通訊金鑰，作為後續傳輸資料加解密之用。Diffie-Hellman 金鑰交換密碼法的安全性，取決於計算離散對數的困難度。訊息傳送方 A 隨機產生 a 值，而接收方 B 產生 b 隨機值，雙方分別秘密保存。傳送方 A 以 a 計算 $x = g^a \bmod p$，而接收方 B 以 b 計算 $y = g^b \bmod p$，其中 p 為大質數，g 為 $\bmod p$ 之原根。通訊前，傳送方與接收方彼此交換以求得的 x 與 y 值。傳送方 A 取得 y 值後，可計算出 $K_{AB} = y^a \bmod p = g^{ab} \bmod p$ 做為與接收方秘密通訊用的金鑰；而接收方 B 取得 x 值後，亦可計算與傳送方之間的通訊金鑰 $K_{AB} = x^b \bmod p$。

二、消費者主導交易模式

網際網路上已提供相當多元的內容與服務，因此，使用者可以擷取豐富的資源以滿足工作、商務活動或興趣等需求。目前的商業模式依據商品規格及售價之主導權力歸屬，分為商家主導(Seller-driven)、市場主導(Exchange-driven)與消費者主導(Buyer-driven)等三類商業模式(Kelsey & Schneier 1997；Foo & Boyd 1998)，並分別簡要描述如下：

1. 商家主導商業模式：為目前最常見的交易模式。商品規格與定價均由販售之商家所掌控，而消費者必須自行詢價並比較商品規格。商店所販售的商品，價格已標示於商品本身，消費者只有選擇購買或不購買的權利，往往無法以自己目標價購買到想要的商品，或需花費大量的搜尋成本，才能購得用戶邊際效益最高的商品。
2. 市場主導商業模式：主要是由買賣雙方自行決定買賣標的與價格後，將委買單或委賣單送往第三公正單位，待委買與委賣標的與價格相符時即完成交易。於此交易模式下，公正單位僅提供買賣雙方價格與標的撮合動作。此類的應用如紐約股市。買賣雙方必須事先認知標的物之存在，買方無法購買具有個人化或客製之商品。
3. 消費者主導商業模式：消費者將想要購買的商品資訊及目標價填寫在條件採購單，再張貼於公正單位所提供的公眾伺服器。賣方可瀏覽伺服器上所公布之採購單，並針對有興趣的採購單申請配對授權(Binding Credential)以完成交易。消費者商業模式的交易程序如圖 2 所示，消費者僅需於張貼採購單與付款時主動連線，其餘交易程序皆無須參與，可有效降低消費者於交易期間所需的連線成本。

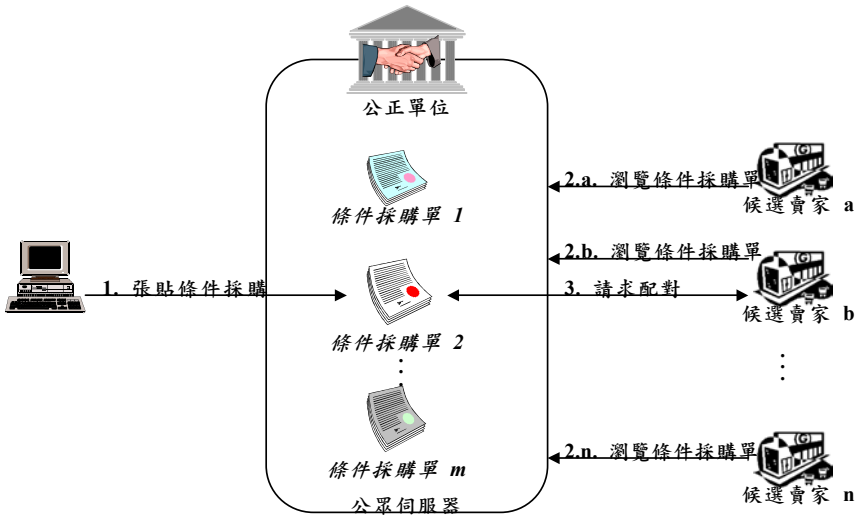

圖 2：消費者主導商業模式示意圖

面對日益豐富的商品種類與相關資訊，消費者勢必將花費更多搜尋成本，並經過漫長的操作程序才可以完成交易行為，如此將降低消費者的購買意願。因此，Kelsey & Schneier 提出透過張貼條件採購單方式，以大幅縮減消費者交易程序與成本，並授權商品規格與價格之主導權利予消費者，提升消費者的交易參與意願。

然而，除了消費者惡意張貼無效採購單，或商家惡意棄標而造成的交易失敗外，消費者對於採購單商品的描述資訊不齊全亦可能致使買賣間的交易糾紛發生。因此，條件採購單之設計應以能清楚表達商品之描述及消費者購買的目標價格資訊，但若過於詳實的採購單內容則需要消費者輸入大量資訊，如此可能反而讓消費者卻步。Kelsey & Schneier 針對條件採購單的內容資訊進行規劃，並定義包含的組成元素如下。圖 3 範例顯示條件採購單內包含的資訊。

1. 採購單編碼(ID)：為一個 160 位元的唯一隨機值，用以定義該條件採購單索引。
2. 公眾伺服器識別碼(Server ID)：公眾伺服器為張貼公布消費者的條件採購單，並進行管理。另外，公眾伺服器可處理賣方提出之競標或配對請求。
3. 仲裁者識別碼(Arbiter ID)：為一公正單位，仲裁者主要檢核消費者與賣方所持有之契約憑證是否具效力，並授權合法消費者張貼條件採購單於指定的公眾伺服器。
4. 商品資訊(Goods)：消費者描述欲購買商品的文字敘述。
5. 目標購買價(Price)：記載消費者願意購買該項商品的目標價格資訊。
6. 生效時間(Start Date)：具 32 位元長度，為消費者希望該採購單生效的時間資訊。
7. 截止時間(End Date)：具 32 位元長度，為消費者希望終止交易的時間資訊。
8. 備註(Terms)：可提供消費者針對購買的商品再行敘述，以確定商品特徵描述明確，避免消費者購買的商品與交付之商品不符。

9. 檢核碼(Checksum)：上述條件採購單內涵資訊的訊息摘要，採用單向雜湊函數計算之摘要值，用以檢驗條件採購單上資訊的真確性。
10. 契約憑證(Bond Certificate)：由公正單位發行。憑證上記載持有者的身份資訊與公眾伺服器識別碼。此憑證提供仲裁者驗證持有者身份，以允許合法消費者張貼條件採購單於公眾伺服器上，或授權賣方得以對公布之採購單提出配對請求。

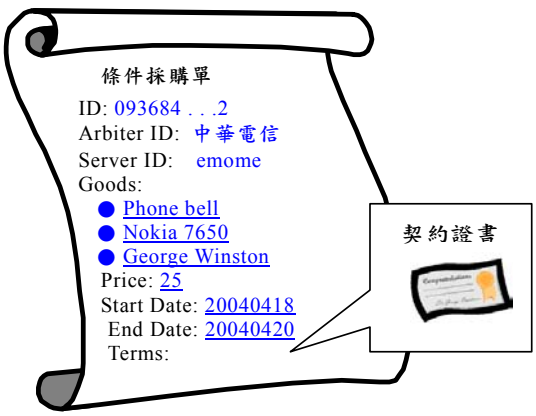

圖 3：條件採購單範例圖

綜觀上述討論，透過條件採購單內容的規劃讓消費者依據其採購需求填寫，以允許消費者具商品樣式與價格的主導權。此外，藉由公布採購條件讓有興趣的賣方瀏覽並提出交易請求之方式，有效縮減消費者所需的交易參與成本，包含減少採購之商品資訊蒐集與比價的時間花費、以及消費者主動參與之交易程序與連線成本等。此優勢將可應用於受限簡易輸出入介面與相對較高連線成本的行動商務。然而，面對簡易輸入介面與有限運算資源的行動交易平台，消費者主導商業模式仍面臨：(1)條件採購單所需輸入的資料量過多，易造成用戶放棄交易，或因資料誤植所導致之交易失敗或糾紛。(2) Kelsey & Schneier 所規劃的條件採購單無法滿足用戶多變的採購策略，如用戶購買某商品時考慮交易配對效率、成交金額或商家距離等因素。(3)漫遊用戶與服務網路內商家之交易糾紛的責任釐清，與行動設備執行繁複密碼技術以保障交易安全卻導致交易處理延遲等問題。因此，本文提出具便捷性與安全性之行動消費者主導商業模式，以解決上述問題。

參、行動消費者主導商業模式之架構規劃

面對數量急遽增加的行動服務，條件採購單交易模式可有效縮減消費者所需的交易參與成本。然而，直接應用於行動商務之條件採購單交易模式仍存在許多問題亟待

克服，如第貳節所探討。本研究將建立行動消費者主導商業模式之架構，並應用具效率的密碼技術以確保行動交易處理之即時性與安全性，此交易協定將於第肆節中敘述。

一、行動消費者主導商業模式之架構

行動消費者主導商業模式提供用戶一個具低成本、個人化與安全性的交易機制，商業架構中包含以下四個參與單位。

1. 行動用戶：與指定電信業者立有契約之行動商務使用者。用戶可自該電信業者處取得核發之 SIM 卡，並可使用插有此張 SIM 卡之行動設備，透過電信網路存取無線網路或網際網路內服務。
2. 電信業者：提供行動網路的服務業者。其中與用戶建立契約關係之註冊電信業者，擁有契約用戶之個人基本資料、與契約用戶間具有電信帳單收費以及代收行動數據服務款項的關係。另外，電信業者並可透過行動網路得知用戶所在區域位置。一般而言，電信業者扮演行動入口網站的角色，透過與眾多內容或服務提供業者合作的方式，進而提供多元且豐富的服務給網路內之用戶。因此，本系統利用電信業者同時擁有與用戶以及與加值服務提供業者之間的契約關係，提供公眾伺服器以公布用戶所填具的條件採購單，並允許商家瀏覽進而完成交易。此外，電信業者另提供檔案伺服器，儲存商務活動期間所產生之交易資訊，以降低行動設備的儲存負擔。
3. 商家：為可提供行動用戶所需商品與服務的商店、無線內容供應商或其他用戶。
4. 金融單位：負責處理交易後金流作業之金融機構。

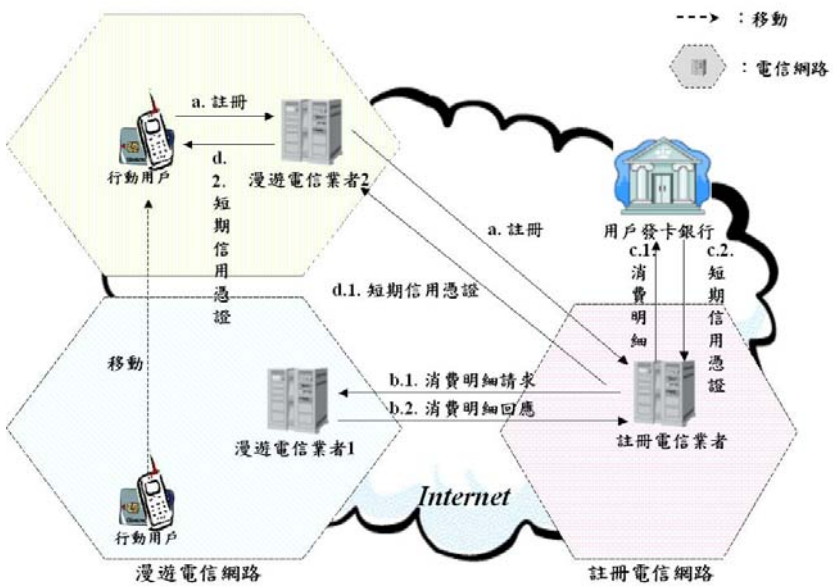

圖 4：行動消費者主導商業模式之信用管理程序

在支援跨區漫遊服務的行動交易平台下，行動用戶穿梭於註冊電信網路與漫遊電信網路內從事商業活動的機率大幅提昇，因而衍生已於第貳節描述之電信業者與金融單位壞帳增加的問題。本研究提出行動交易下之信用管理解決方案，如圖 4 所示。利用行動通訊的特性，當用戶離開所在之電信網路，用戶所持的行動設備會透過目前電信網路向註冊電信業者提出區域更新請求。註冊電信業者收到請求後，透過資料庫可取得對應之移動用戶剛離開的電信網路資訊，並向該漫遊業者請求用戶於區域內之消費總金額與明細。註冊電信業者可傳送消費明細給金融單位以核算用戶的消費情形，金融機構再依據用戶的信用額度核發短期之信用憑證，此憑證內含有允許用戶消費之信用額度。註冊電信業者將此信用憑證透過用戶目前所在之漫遊電信業者傳回行動設備後，註冊電信業者並於資料庫內更新用戶所在區域資訊。

透過此方式，當用戶進入新的電信網路，用戶持有的行動設備便會執行信用管理程序。因此，用戶移動至另一個電信網路內便擁有金融單位所核發之信用額度；另一方面，金融單位與電信業者並可掌握用戶之消費情況，有效地降低壞帳發生。

取得核發的信用額度後，行動用戶可以隨時隨地於各城市間從事商業活動，並視其需求與購買策略以填妥條件採購單。圖 5 顯示行動消費者主導商業模式之架構圖。

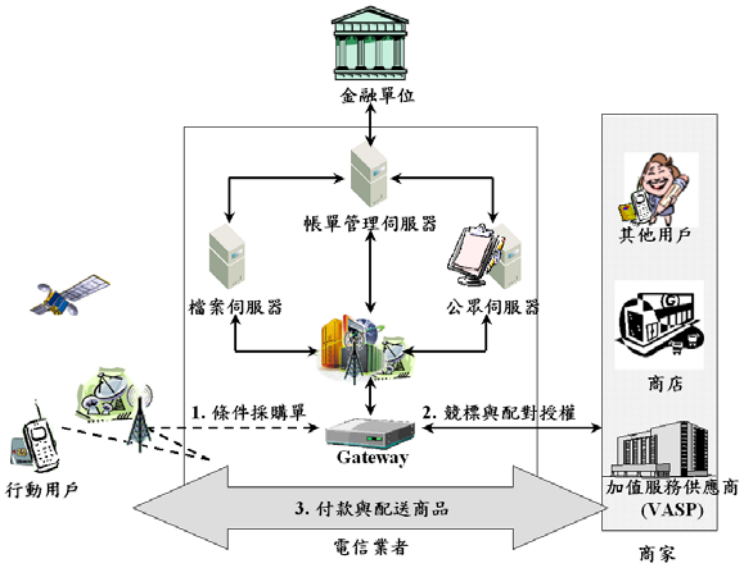

圖 5：行動消費者主導商業模式之架構圖

本研究將消費者的購買策略規劃為(1)取得提供商品最優惠價格的指定區域商家資訊之詢價策略，(2)與提供優惠價格且與用戶距離最短的商家交易之距離策略，(3)與具良好信用記錄且提供優惠價格的商家交易之信用策略，(4)與提供優惠價格的商家迅速完成交易之時間策略，(5)與願意提供最低價格的商家交易之價格策略，以及(6)購買低價資訊商品之預設策略等六類。表 1 說明各購買策略之要求對應關係。

表 1：購買策略與要求對應表

要求＼策略		詢價	距離	信用	時間	價格	預設
大額商品	指定區域	●					
	優惠價格	●	●	●	●		
	最短距離		●				
	良好信用			●			
	迅速交易				●		
	最低價格					●	
小額商品交易							●

依據用戶指定的購物策略，電信業者將條件採購單張貼於對應之策略伺服器。之後，電信網路或網際網路內之商家可瀏覽公布於公眾伺服器上的採購單內容，並針對感興趣的採購單提出競標與配對授權等請求。電信業者依據採購單對應之購買策略，遴選優勝商家以符合消費者交易預期，優勝商家並可取得配對授權而與採購單對應之用戶完成交易。圖 6 描述各策略伺服器之處理流程，以提供用戶最佳的購物滿足。

1. 『詢價』策略伺服器：當用戶想知道指定區域內那些商家正提供其欲購買的商品，且商家對該商品亦提供最優惠的售價。例如人們常有走在街上，突然腦中浮現想購買某項特定商品或所在鄰近商家的廣播電台傳來某個有致命吸引力之商品消息的經驗，然而卻無從得知目前所在區域附近何處可以購得該商品，以及鄰近何處能夠提供最優惠價格或最完整服務等資訊。尤當購買標的為實體商品時，能夠得到所在地鄰近商家位置、商品售價資訊及實地把玩商品，為消費者所主要關心情資。選擇此策略，用戶可依需求並規範競標時限，如 15 分鐘，甚至更短，滿足用戶自己所能接受的『立即』與『即時』的需求。詢價策略伺服器透過廣播方式將條件採購單內容告知指定區域內商家並開放競標，在競標期限後遴選指定區域內可提供最低價之前五名優勝商家。電信業者須發配對授權給優勝商家後，透過電信網路之定位功能將優勝商家的資訊與位置顯示予對應之用戶。透過此策略，用戶可以在既定路程上，到優勝的商家處實地觀賞並購買商品。

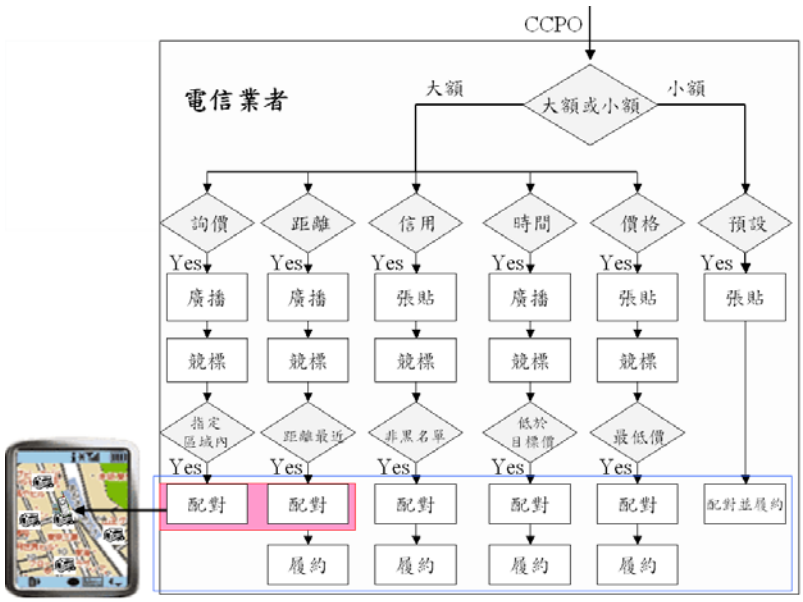

圖 6：策略公眾伺服器之處理流程圖

2.『距離』策略伺服器：當用戶希望與最靠近之商家進行交易。如以下情境：當商家對於有期限的商品，在將屆有效期限的情況下，商家會希望能順利出售商品以增加營收。如電影快開幕，商家期望能將剩下座位的票券賣出，而且願意大幅降低售價求售。當用戶有消費意願，即可以透過距離策略伺服器的輔助，伺服器將依據用戶所在區域廣播其條件採購單給附近商家。這些商家將樂意且立即釋出善意來完成交易。伺服器將自願意提供優惠價格的電影院中挑選出與用戶具最短距離之優勝商家，讓用戶可以在附近的電影院以較一般售價為低的成本觀賞電影。

考慮下列情景：當用戶因緊急事件必須馬上出差至某個城市，用戶若希望藉由有線網路辦妥運輸工具票券的訂購與下榻飯店之預約，除了必須花費尋找定點連線機器的時間成本之外，這些作業將可能拖延用戶處理緊急事件的時效，於現實情況下並不切實際。因此，在接獲緊急出差的指令後，用戶可在前往運輸工具搭乘站途中，以少於預估抵達搭乘站期間所需總時間做為條件採購單之交易處理可接受時限，透過行動設備連線發送條件採購單。同理，亦可在搭乘交通運輸工具期間，發送飯店預約的條件採購單至指定目的地鄰近區域內所有的飯店，以順利解決住宿問題。這些優勢並非有線網路商務所能比擬。由於交通運輸票券與飯店預約皆具有時效性，特性如上述之有期限的商品。面對此類商品，用戶可以依據自己所關心的交易考量因素，下達下列第 3 至第 5 購買策略來提高交易所得到的效益。

3. 『信用』策略伺服器：用戶注重售後服務，並以商家之交易信用程度作為交易的主要考量，降低交易糾紛的發生。信用策略伺服器將自競標候選商家中挑選信用良好的商家為優勝商家。
4. 『時間』策略伺服器：當用戶希望能以目標價迅速完成交易時，時間策略伺服器將配對授權給最早出價低於用戶目標價要求的商家。
5. 『價格』策略伺服器：當用戶以交易成交價錢之多寡為主要考量，價格策略伺服器將配對授權給提供最低成交價格的優勝商家。
6. 『預設』策略伺服器：當消費金額低於某標準，無須進行競標活動以降低交易成本，通常以低價資訊商品的交易居多。預設策略伺服器將條件採購單張貼公布，由感興趣之商家提出配對申請。

當商家取得電信者業者核發之配對授權後，於規定期間內將指定購買的商品配送給對應之行動用戶，而用戶付款給商家以完成交易。

二、條件採購單格式

為克服行動設備之簡易輸出入介面，避免用戶因必須大量操作所導致其降低使用意願。本研究以克服行動商務之限制為設計考量，將條件採購單的組成項目規劃如下：

1. 候選條件採購單(Candidate CPO, CCPO)編號 ID_O：以行動消費者之代名 CID_T 與張貼的時戳 T_C 等資訊結合而成，$ID_O = (CID_T, T_C)$。ID_O 為具唯一性的數值。
2. 條件採購單編號 TID：於公眾伺服器上公佈之採購單編號，由電信業者以 ID_O 與策略公眾伺服器辨識碼 ID_S 等資訊結合而成，$TID = (ID_O, ID_S)$ 具有唯一性。
3. 購買條件 $Condition$：行動消費者欲購商品之描述資訊。
4. 目標價 P：消費者心目中的購買價格。通常實際成交成本低於此價格且差距越大，消費者的交易滿意度越高。
5. 購買策略 $Policy$：消費者心目中的交易模式，包含詢價、距離、信用、時間、價格與預設等六個策略。
6. 交易期限 EXP_O：消費者指定之交易完成期限。於此期限前，取得配對授權的優勝商家必須依據採購單內容交付商品予消費者。
7. 競標期限 EXP_{BID}：公佈之採購單競標期限，此期限由電信業者依據交易期限而自動設定，避免消費者不當制定而造成因期間過長所導致的管理成本增加，或因時間太短致使流標。
8. 條件採購單張貼時戳 T_C：消費者將採購單上傳至公眾伺服器之時間戳記。

當行動消費者想要購買某特定商品時，僅需填寫採購單之內容如圖 7 所示，其稱為候選條件採購單 $CCPO = (ID_O, Condition, P, Policy, EXP_O)$。其餘訊息由行動設備與電信業者自動產生。如此，除了有效減少行動消費者輸入的訊息量外，並可避免因不當輸入而導致之交易失敗，如行動設備可依據填入的目標價格而自動切換大額或小額交易所對應的購買策略；另外，可以減緩無線頻寬負載不足而增加交易時間與成本。

圖 7：行動候選條件採購單範例圖

肆、行動消費者主導交易協定

本文以全球性行動商務為背景，支援行動用戶跨區並存取漫遊網路內所提供的服務。協定中包含行動用戶（消費者）C、商家 M、漫遊電信業者 V、用戶註冊電信業者 B 與發卡銀行等五個單位。對用戶而言，註冊電信業者與發卡銀行同為信用單位，為簡化協定之運作程序，協定內將不詳細探討用戶的註冊電信業者與發卡銀行之間之金流結算過程。表 2 描述協定所使用的符號列表。

表 2：行動消費者主導交易協定之符號表

符號	說明	符號	說明
C	行動用戶身份識別碼，包含 IMSI 資訊	V	漫遊電信業者身份識別碼
M	網路上商家身份識別碼	B	註冊電信業者身份識別碼
CID_T	用戶代名，$CID_T = H(C, Z_C)$	w	用戶產生的秘密隨機值
Z_X	單位 X 產生的秘密隨機值	LAI_X	電信業者 X 的區域資訊
K_L	匿名金鑰，$K_L = g^{bw} \bmod p$	$E_{K_X}(.)$	以通訊金鑰 K_X 對刮號內資訊加密
K_{XY}	單位 X 與 Y 共享的通訊金鑰	$E_{PK_X}(.)$	以單位 X 之公開金鑰對刮號內資訊加密
PK_X	單位 X 的公開金鑰，$PK_X = g^x \bmod p$	$S_X(.)$	以 X 之私密金鑰對刮號內資訊簽章，並包含明文與時戳
SK_X	單位 X 的私密金鑰，$SK_X = x$ $(1 < x < p-1)$	$MAC_{XY}(.)$	以通訊金鑰 K_{XY} 對刮號內資訊做 MAC 運算
T_C	行動設備送出候選條件採購單之時戳	$H(.)$	以單向雜湊運算對刮號內產生摘要值，具不可逆性
p	大質數，可公開	g	模 p 之原根，可公開
$(A \oplus B)$	資訊 A 與 B 的 XOR 運算結果	r_m	由單向雜湊函數 $r_m = H(r_{m-1})$ 產生的代幣值，$(m = 1, 2, \ldots n)$
r_0	雜湊鍊的根 $r_0 = MAC_{BC}(Z_C, Z_B)$	$Cert_X$	公正單位 CA 核發給 X 之數位憑證，$Cert_X = S_{CA}(PK_X, X)$
n	註冊電信業者核發之可使用代幣數目	δ	註冊電信業者核發之授權信用額度
EXP_{TC}	短期信用憑證之有效期限	ID_S	公佈採購單之對應策略公眾伺服器識別碼
ID_O	候選條件採購單之編號	$Policy$	包含詢價、距離、信用、時間、價格與預設等購買策略
β	協調 K_L 的公開因子，$\beta = g^w \bmod p$	TID	條件採購單編號，$TID = (ID_O, ID_S)$
P	用戶購買指定商品之目標價格	K_G	大額商品交易協定中商品金鑰
$Goods$	用戶指定購買之商品	$CCPO$	候選條件採購單，$CCPO = (ID_O, Condition, P, Policy, EXP_O)$
EXP_O	條件採購單之交易有效期限	EXP_{BID}	策略公眾伺服器制訂之指定採購單競標期限
Bid	商家提出之競標價格	CPO	公眾伺服器上公佈之條件採購單，$CPO = (TID, CCPO)$
BC	配對授權 $BC = S_V(CPO_L, PK_L, Bid, M)$	PC	付款授權 $PC = S_C(TID, Bid, V)$
$TCert_C$	註冊電信業者核發給用戶 C 的短期信用憑證 $TCert_C = S_B(CID_T, V, PK_C, PK_V, n, \delta, r_n, EXP_{TC})$		
$CCPO_L$	不含用戶目標價之候選條件採購單，$CCPO_L = (ID_O, Condition, EXP_O)$		
CPO_L	公眾伺服器上公佈之不含用戶目標價的候選條件採購單，$CPO_L = S_V(TID, CCPO_L, EXP_{BID})$		

假設存在跨國性的公正單位 CA (Certificate Authority)，此 CA 核發數位憑證給具法律規範的各城市 CA，憑證內含接收者之公開金鑰與身份等資訊。讓這些城市 CA 因而可以辨識彼此合法性，並能認證各 CA 發行給城市內各單位的數位憑證之有效性。在此階層式 PKI (Public Key Infrastructure)下，協定的參與單位：提供不同城市內的無線網路之電信業者，即漫遊電信業者 V 與註冊電信業者 B 能夠透過所屬城市 CA 以及跨國 CA 的輔助，取得彼此的數位憑證 $Cert_B$ 與 $Cert_V$，並以此兩個 CA 的公開金鑰驗證數位憑證之有效性，以確認對方身份的合法性。另外，城市 CA 分別核發予電信業者 V 與商家 M 數位憑證 $Cert_V$ 和 $Cert_M$；彼此可以使用該城市 CA 的公開金鑰檢驗憑證以確認彼此的合法性。本文假設漫遊電信業者 V 與商家 M 確信對方身份後，透過安全的機制以協調出一把共享的通訊金鑰 K_{VM}，作為日後驗證彼此間傳遞訊息的身份鑑別性與隱密性。

在協定的起始階段中，假設行動用戶與註冊電信業者建立契約關係後，行動設備內之 SIM 卡即存有用戶身份識別碼 C = IMSI、用戶與註冊電信業者之鑑別金鑰 K_{BC}、註冊電信業者之區域資訊 LAI_B 以及公開金鑰 $PK_B = g^b \bmod p$，其中 b 為用戶註冊電信業者 B 的私密金鑰並滿足條件 $1 < b < p-1$ (ElGamal 1985)。SIM 卡具有儲存、運算以及防止竄改等特性，並可確保行動用戶所持有之資訊的隱密性(Shelfer 2002)。

行動消費者主導交易協定可分為『區域更新』、『交易』與『結算』等階段，以下分別針對各階段運作程序進行說明。

一、區域更新階段

此階段程序僅於行動用戶移動至另一個電信網路時啟動。行動設備接收到漫遊電信網路所發送之區域資訊 LAI_V。行動設備比對 SIM 卡內儲有的 LAI_B 與接收 LAI_V 值，若兩者不相等，行動設備判斷用戶已經移動至另一個電信網路，故發出註冊請求訊息。此階段由行動設備自動發出區域更新請求，用戶並無須參與。

1. 用戶所持之行動設備傳送註冊請求訊息$\{\beta, CID_T, B, RR\}$。
   a、行動設備產生秘密隨機值 Z_C 與 w。Z_C 主要為產生後續與註冊電信業者共享秘密資訊之組成因子，並具有 challenge/response 之功用；w 值為協調 Diffie-Hellman 金鑰的秘密因子，而$\beta = g^w \bmod p$ 則為 Diffie-Hellman 金鑰的公開值。
   b、行動設備產生用戶於漫遊區域內使用之代名 $CID_T = (C, Z_C)$以達匿名性。並以註冊電信業者的公開金鑰 PK_B 利用 Diffie-Hellman 金鑰交換密碼法計算匿名金鑰 $K_L = PK_B^{\,w} \bmod p = g^{bw} \bmod p$。
   c、行動設備產生秘密註冊資訊 $RR = E_{K_L}(C, H(Z_C), (Z_C \oplus MAC_{BC}(\beta)))$，確保用戶身份 C 與秘密值 Z_C 僅可被註冊電信業者所取得。
2. 漫遊電信業者轉送$\{\beta, CID_T, RR\}$訊息給註冊電信業者。
3. 註冊電信業者完成用戶之信用管理後，核發其於新漫遊電信網路內可供交易付款使用的短期信用憑證 $TCert_C$ 與通訊金鑰 K_{VC}，並傳送 $\{RC, E_{PK_V}(K_{VC}), TCert_C\}$ 給

漫遊電信業者。註冊電信業者處理程序如下所描述：

a、使用私密金鑰 $SK_B = b$，依 Diffie-Hellman 金鑰交換密碼法產生匿名金鑰 $K_L=\beta^{\,b} \bmod p = g^{bw} \bmod p$ 後，可自訊息 RR 中取出用戶身份識別 C。

b、依據用戶身份識別 C，自 AuC 取得對應的身份鑑別金鑰 K_{BC}。

c、計算 $MAC_{BC}(\beta)$，並從 $Z_C \oplus MAC_{BC}(\beta)$導出秘密值 Z_C。

d、以 Z_C 做為 $H(.)$輸入值，比較輸出值是否相等於 $H(Z_C)$。若相等，則繼續執行以下程序。

e、依據電信資料庫取得對應用戶剛離開之電信網路資訊，並向此漫遊業者請求該用戶於區域內的消費總金額與明細。之後，依據用戶的信用額度與未償還之累積消費金額，決定其可於新的漫遊網路內使用之授權信用額度δ，以避免壞帳增加的風險。其中授權信用額度δ 包含可供小額交易的代幣數目 n。

f、產生用戶的短期金鑰對$(PK_C,\ SK_C)$。其中，簽章金鑰 SK_C 為允許用戶購買大額商品之交易付款使用。

g、隨機產生秘密值 Z_B，用以計算用戶 C 與漫遊電信業者 V 之間的通訊金鑰 $K_{VC}=H(Z_C, Z_B)$後，以漫遊電信業者 V 的公開金鑰 PK_V 加密 K_{VC}，產生 $E_{PK_V}(K_{VC})$ 以確保 K_{VC} 的隱密性。以及計算雜湊鍊的啟始值 $r_0 = MAC_{BC}(Z_C, Z_B)$，並以 r_0 為根產生 n 個代幣 $r_m = H^m(r_0)$ $(m = 1, 2, .., n)$，以供小額交易時使用。

h、核發短期信用憑證 $TCert_C = S_B(CID_T, V, PK_C, PK_V, n, \delta, r_n, EXP_{TC})$，供用戶 C 於漫遊網路 V 內使用。其中 EXP_{TC} 為短期信用憑證的有效期限。

i、產生註冊授權 $RC = \{B, E_{K_L}(Z_B, H(SK_C), (SK_C \oplus MAC_{BC}(Z_B)))\}$，以保障秘密值 Z_B 與簽章金鑰 SK_C 之隱密性與真確性，並更新電信資料庫中的用戶所在區域資訊。

4. 漫遊電信業者以註冊電信業者的公開金鑰 PK_B 驗證 $TCert_C$，以確認用戶 CID_T 是否為合法用戶，並可取得註冊電信業者所核發之與該用戶通訊用金鑰 K_{VC}、用戶於區域內被授權的信用額度δ與價值 n 單位之代幣驗證值 r_n 等資訊。漫遊電信業者傳送$\{RC, TCert_C\}$資訊給用戶。

用戶所持的行動設備驗證 $TCert_C$ 之有效性後，得知授權消費額度為δ，其中包含小額交易額度 n，並自註冊授權 RC 訊息中取出 Z_B 與 SK_C。行動設備分別計算出與漫遊電信業者之通訊金鑰 $K_{VC} = H(Z_C, Z_B)$，與雜湊鍊之根 $r_0 = MAC_{BC}(Z_C, Z_B)$，並以 r_0 為啟始值產生 n 個代幣 $r_m = H^m(r_0)$ $(m = 1, 2, .., n)$。

用戶所持的行動設備完成區域更新階段後，行動設備內即儲有可消費之 n 單位代幣 $r_0 \sim r_{n-1}$、δ單位信用額度消費用之簽章金鑰 SK_C 以及可於對應漫遊網路內交易之通訊金鑰 K_{VC}。行動消費者主導交易模式之區域更新階段運作程序如圖 8 所示。

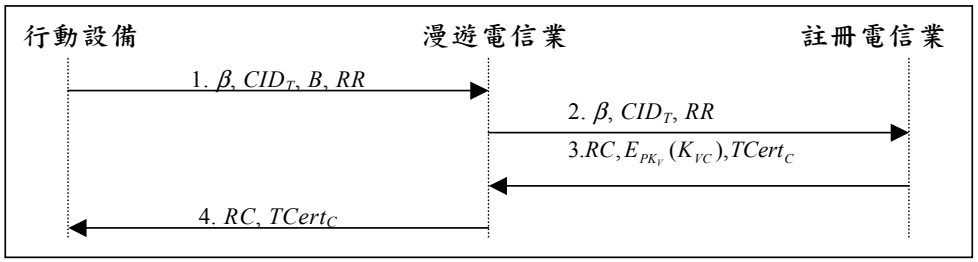

圖 8：行動消費者主導交易協定之區域更新程序圖

二、交易階段

當行動用戶取得核發之短期信用憑證 $TCert_C$、簽章金鑰 SK_C 與通訊金鑰 K_{VC}，即已被授權於漫遊電信業者 V 所提供之服務網路內消費。本交易階段主要應用於資訊商品之購買，各購買策略之運作程序將依消費金額多寡分別介紹如下。

（一）小額資訊商品交易

消費金額低於某標準，無須進行競標活動以降低交易成本之『預設』購買策略，通常應用於交易金額不大之資訊商品。此類交易型態下，用戶所關心的是交易成本與效率。

1. 用戶希望以 P 單位代幣值購買資訊商品，填寫採購條件後產生候選條件採購單 $CCPO$，再透過通訊金鑰 K_{VC} 產生 MAC 訊息摘要值 $MAC_{VC}(CCPO)$，以達讓漫遊電信業者因而判定用戶之合法性，以及順利張貼於公眾伺服器之目的。
2. 漫遊電信業者利用通訊金鑰 K_{VC} 驗證 $CCPO$ 的合法性，針對此 $CCPO$ 產生具唯一性的編號 $TID=(ID_O, ID_S)$，並於『預設』公眾伺服器上公佈條件採購單 $CPO=(TID, CCPO)$；之後，依用戶要求彈性回覆確認訊息 $\{TID, MAC_{VC}(TID)\}$ 給用戶。如此一來，用戶可隨時連線至『預設』公眾伺服器，查詢目前處理之進度。
3. 當條件採購單 CPO 張貼於公眾伺服器上，商家可上網瀏覽。商家可對有興趣的 CPO 提出配對請求，電信業者視 CPO 處理狀況而決定授權與否，以避免多商家同時生產同一 CPO 要求之商品。取得配對授權的優勝商家即可依對應 CPO 載明之條件生產指定資訊商品 $Goods$，並傳遞履約訊息 $\{TID, M, H(Goods), Goods \oplus MAC_{VM}(TID)\}$ 給漫遊電信業者。
4. 漫遊電信業者利用通訊金鑰 K_{VM} 取得資訊商品 $Goods$。驗證所接收訊息的合法性後，使用金鑰 K_{VC} 加密商品並傳送 $\{TID, H(Goods), (Goods \oplus MAC_{VC}(TID))\}$ 給用戶。
5. 用戶收到加密商品訊息後，利用通訊金鑰 K_{VC} 取得資訊商品 $Goods$，並透過單向雜湊運算驗證商品的真確性。用戶支付 P 單位有價代幣 r_{n-P} 的付款訊息 $\{TID, P, (r_{n-P} \oplus MAC_{VC}(TID, P))\}$ 給漫遊電信業者。

漫遊電信業者自付款訊息中取出價值 P 單位代幣 r_{n-P}，並透過 $r_n = H^P(r_{n-P})$ 檢查方

式以驗證代幣的有效性。漫遊電信業者可選擇性傳送成交訊息 $\{TID, V, P, MAC_{VM}(TID, P)\}$ 知會對應之優勝商家。圖 9 描述行動消費者主導商務模式之小額資訊商品交易協定運作程序，透過具效率的密碼技術與不可否認之代幣設計，提供用戶便利且公平的行動交易平台。

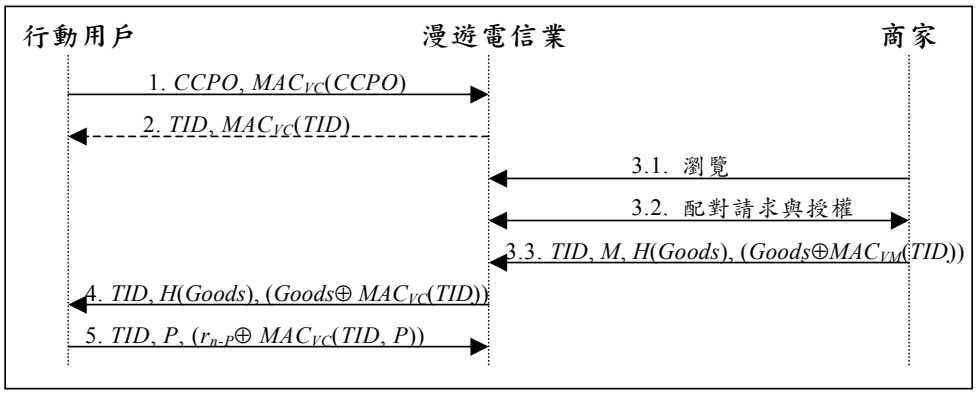

圖 9：行動消費者主導之小額資訊商品交易協定程序圖

（二）大額資訊商品交易

行動用戶面對欲購買之標的為高單價商品時，如機票、軟體執照(License)亦或其他高價值的數位資訊商品，因所支付金額較高，故用戶以交易付款之安全性為主要考量。此外，因屬大額交易，若成交所需花費的金額越低，用戶因交易而獲得之效益將越高，進而吸引其繼續參與行動商務活動。本協定對於大額交易除了提供『價格』策略外，亦分別支援『時間』、『信用』、『距離』與『詢價』等購買策略，以更貼近於現實消費者購物時之決策考量。大額資訊商品交易協定運作程序如圖 10 所示。

1. 用戶以簽章金鑰 SK_C 簽署包含目標價格的候選條件採購單 $CCPO$，以達下單之不可否認目的。並利用通訊金鑰 K_{VC} 加密產生 $\{E_{K_{VC}}(S_C(CCPO))\}$，保障目標價之隱密性。
2. 漫遊電信業者將未含用戶目標價的條件採購單張貼於對應之公眾伺服器，並開放給商家競價爭取該採購單。漫遊電信業者可選擇性傳送回條 $\{E_{K_{VC}}(S_V(TID, P))\}$ 給用戶。

a、漫遊電信業者驗證 $CCPO$ 上簽章之有效性後，依據其所指定的購買策略，決定對應之公眾伺服器 ID_S，如用戶選取購買策略為『價格』策略，則 ID_S 即指價格公眾伺服器的辨識碼。此 $CCPO$ 將具有唯一性之採購單編碼 $TID = (ID_O, ID_S)$。

b、為保護 $CCPO$ 上價格的隱密性以利商家競價投標，產生未含用戶目標價的候選條件採購單 $CCPO_L = (ID_O, Condition, EXP_O)$，並依據用戶指定交易期限決定競標截止日 EXP_{BID}。漫遊電信業者簽章並公布採購單 $CPO_L = S_V(TID, CCPO_L, EXP_{BID})$ 於對應之策略公眾伺服器上。

c、若用戶指定的購買策略為『時間』、『距離』或『詢價』等策略時，漫遊電信業者除了於策略公眾伺服器上公佈採購單 CPO_L 外，並對用戶所在區域或指定地區內進行廣播，以提升用戶與區域內商家的成交機率。

3. 商家可上網瀏覽採購單 CPO_L 所載明之採購條件，並於競價期限內，針對有興趣之採購單 CPO_L 發送競標請求 $\{M, E_{K_{VM}}(S_M(TID, Bid))\}$ 給漫遊電信業者。
4. 在對應採購單 CPO_L 的競標期限內，漫遊電信業者檢驗商家之競標請求是否已被商家所簽章，或競標價格 Bid 是否低於用戶目標價 P 等要求。若是，漫遊電信業者回覆競標收據 $\{V, E_{K_{VM}}(S_V(TID, Bid, M))\}$ 給商家。
5. 競標截止，漫遊電信業者依據對應的採購單上所選定之購買策略，找出最接近用戶心目中的理想賣方，稱之為優勝商家。各策略之優勝商家的決定條件已介紹於第參節。其中，當用戶選擇的購買策略為『時間』策略時，只要商家出價低於用戶目標價，則該商家即為此 CPO_L 的優勝商家，以滿足用戶迅速完成交易的需求。另外，若選擇『詢價』或『距離』策略時，漫遊電信業者會利用定位技術，在行動設備上顯示對應用戶所在區域內或指定區域內的優勝商家位置。漫遊電信業者將競標結果 $\{TID, H(Bid), (Bid \oplus MAC_{VC}(TID))\}$ 知會用戶，並核發給優勝商家一份配對授權 $BC=S_V(CPO_L, PK_C, Bid, M)$。若選擇『詢價』策略的用戶可持配對授權 BC 並親自到優勝商家所在位置察看商品，此商品可為數位或實體之商品，進而完成並結束交易。
6. 優勝商家可自配對授權 BC 訊息中取出用戶之公開金鑰 PK_C，並於交易截止日前，將包含有指定資訊商品的訊息 $\{M, E_{K_{VM}}(S_M(E_{PK_C}(Goods), BC))\}$ 傳給漫遊電信業者。
7. 漫遊電信業者儲存 $S_M(E_{PK_C}(Goods), BC)$ 以作為日後糾紛之裁決依據，並利用隨機產生的商品金鑰 K_G 與加密商品 $E_{PK_C}(Goods)$ 進行 XOR 運算後，傳送履約資訊 $\{S_V(TID, Bid, (K_G \oplus E_{PK_C}(Goods)))\}$ 給用戶，以達用戶付款後方能使用商品之目的。
8. 用戶接收訊息 5 和 7 後，驗證履約資訊上簽章之有效性。若簽章無誤，使用簽章金鑰 SK_C 簽署付款授權 $PC = S_C(TID, Bid, V)$ 後，傳送 $\{CID_T, E_{K_{VC}}(PC)\}$ 給漫遊電信業者。
9. 漫遊電信業者利用通訊金鑰 K_{VC} 解密以取出付款授權 PC，並檢驗付款授權 PC 上簽章的有效性。漫遊電信業者再檢查用戶支付金額 Bid 是否大於授權信用 δ 值，或已累積的消費金額是否超過 δ 值。若仍在信用額度內，表示此付款授權具清償效用，漫遊電信將傳送商品金鑰 K_G 給用戶。

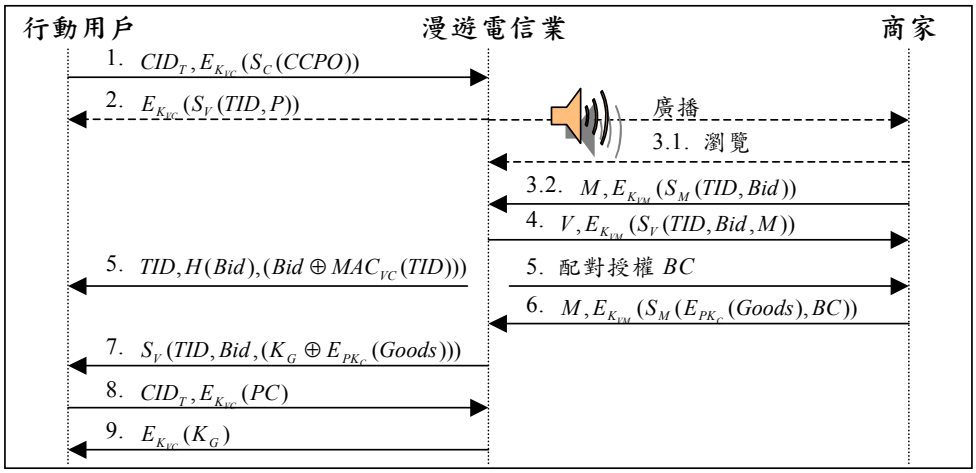

圖 10：行動消費者主導商務之大額資訊商品交易協定程序圖

用戶利用商品金鑰 K_G 與私密金鑰 SK_C 解密 $K_G \oplus E_{PK_C}(Goods)$，可順利取得所購買之資訊商品 $Goods$。若商品與採購單之購買條件不符，用戶可持漫遊電信業者對該採購單之簽章資訊 $\{S_V(TID,Bid,(K_G \oplus E_{PK_C}(Goods)))\}$ 為舉證依據，以保障消費權益。

三、結算階段

於固定期間或收到註冊電信業者傳送之消費明細請求訊息後，漫遊電信業者將用戶於期間所累積消費之代幣、簽章之付款授權與消費明細等資訊提供給註冊電信業者，以進行結算程序。註冊電信業者或金融單位依據用戶消費總金額產生帳單通知該用戶。

註冊電信業者與金融單位取得帳款後，依據消費明細與曾提供服務給用戶之漫遊電信業者進行結算，而漫遊電信業者再將收到之款項與提供商品的優勝商家們進行拆帳。

四、一個行動消費者主導交易的例子

當住在台灣的 Alice 必須前往日本開會，她可以在出發前填寫採購單購買小額的資訊商品，包括日本天候情況、交通乘車訊息、開會地點周邊飯店與當地文化名產等資訊。這些資訊將僅需少量代幣的價錢即可獲得，可省卻 Alice 需抽空且自行上網搜尋資料所耗費的時間與連線成本。甚至，Alice 可視行程的急迫性選擇『時間』策略，以迅速購買大額的電子機票與預約飯店住宿；若擁有較寬裕的準備啟程時間，可選擇『價格』策略以購買到低價的機票與飯店住宿。與傳統的交易方式相較，Alice 於交易期間並無須枯坐於電腦前花費大幅時間進行搜尋資訊、比價、下單與付款等程序。相反地，Alice 在接到開會指令後，僅需隨手填寫條件採購單並進行簽署動作，即可繼續手邊的工作，等候競標結果的回報。取得成交回報後，Alice 可在空閒（例如候車）時簽署付款證明，即可順利取得機票。

假設，台灣的電信業者為 Alice 的註冊電信業者，核發總額 80,000 元的授權信用額度，包含 5,000 元的小額代幣給 Alice。扣除 Alice 購買小額資訊商品 100 元與大額電子機票 15,000 元與飯店預訂 5,000 元，剩餘 59,900 元。當 Alice 搭飛機到日本，手持設備將自動執行區域更新程序。在此程序中，日本電信業者向台灣電信業者要求驗證 Alice 身份。確認無誤後，台灣電信業者進行信用管理，核發額度 59,900 元的授權信用額度，包含 5,000 元的小額代幣，以及可供簽署具法律效益之金鑰對給 Alice。此外，台灣電信業者將協調出 Alice 與日本電信業者間通訊用的金鑰。通關前，Alice 可選擇『距離』策略發送乘車條件採購單，日本電信業者將條件採購單發送給機場周圍的計程車業者。計程車業者可提供優惠價格以縮短排隊等候乘客的時間，因此，Alice 可以優惠的價格乘車至下榻飯店。同樣地，再次透過『距離』策略的使用，Alice 可用優惠價格從下榻飯店趕往開會地點。當會議結束，Alice 可選擇『信用』策略向信用良好的商家購買演唱會票券，或選擇『詢價』策略親自至商家購買電子產品，以避免因人生地不熟可能發生的交易糾紛。

於固定期間後，台灣電信業者結算 Alice 消費，並產生帳單通知 Alice 繳費。台灣電信業者取得費用後將 Alice 於日本期間消費金額轉帳給日本電信業者。爾後，日本電信業者再與提供服務的商家們進行拆帳。

若發生任何糾紛，將可依據交易雙方簽署之文件或不可否認之代幣，釐清責任歸屬。Alice 必須支付曾使用的代幣值與簽署之消費金額，而商家則必須提供承諾之服務。

伍、分析與討論

本文設計一個兼具安全性與便利性之商業模式，並支援全球性行動商務以允許行動用戶跨區消費。本節將分別以交易『安全性』與『效率性』兩個層面來檢視所提出之商務協定，並分別針對介面設計、行動運算與用戶的匿名性三部分做探討。

一、安全性分析

所提出的協定設計結合對稱式與非對稱式金鑰密碼技術，用以建構具安全交易平台的商務環境。以下將以『雙向身份鑑別』、『隱密性』、『真確性』以及『不可否認性』等四項需求來檢驗協定的安全性。

1. 雙向身份鑑別：提供服務的商家／電信業者必須能夠確認用戶身份的合法性，提供服務並計費，避免非授權人士假扮成合法用戶存取網路資源。對用戶而言，鑑別商家／電信業者的程序也是必要的，可以消除非法人士假扮商家騙取用戶的付款資訊，或假扮電信業者取得用戶的個人資訊與提供錯誤的服務，如提供受病毒感染的資訊。此外，電信業者在交易過程中扮演仲介的角色，商家必須確認電信業者身份，方能相信所授與的配對授權進而產生商品；而電信業者也必須確認商家身份的合法性，為用戶建立第一道安全防線，避免非法商家提供具惡意的資訊商品。

a、用戶與註冊電信業者：當非法人士想要冒充合法用戶向註冊電信業者申請更新所在區域，並取得價值δ額度的信用憑證，其必須產生合法的秘密註冊資訊$RR = E_{K_L}(C, H(Z_C), (Z_C \oplus MAC_{BC}(\beta)))$。然而，因為用戶與註冊電信業者彼此秘密持有相同的鑑別金鑰 K_{BC}，僅有合法的用戶可以產生有效的$MAC_{BC}(\beta)$。同理，唯有合法的註冊電信業者方能產生有效的註冊授權$RC = \{B, E_{K_L}(Z_B, H(SK_C), (SK_C \oplus MAC_{BC}(Z_B)))\}$。因此，此非法人士無法假扮成用戶或註冊電信業者來欺騙任何一方。

b、用戶與漫遊電信業者：若想要扮演用戶或漫遊電信業者，假冒者需要持有註冊電信業者的私密金鑰SK_V，以及自訊息$\{RC, E_{PK_V}(K_{VC}), TCert_C\}$中取得由註冊電信業者核發的通訊金鑰 K_{VC}。由於私密金鑰 SK_V 由漫遊電信業者秘密持有的情況下，假冒者無法從$E_{PK_V}(K_{VC})$中計算出 K_{VC}。因此，在小額資訊商品交易中，用戶可以透過履約訊息$\{TID, M, H(Goods), (Goods \oplus MAC_{VM}(TID))\}$來判斷訊息是否由漫遊電信業者端所傳遞。同理，對漫遊電信業者而言，當假冒者使用非法的K'_{VC}產生$\{CCPO, MAC'_{VM}(CCPO)\}$以試圖扮演成用戶，將可以因檢驗出非法的$MAC'_{VM}(CCPO)$而被偵測出來。另外，在大額資訊商品交易階段，用戶與漫遊電信業者可以透過檢驗彼此的簽章有效性來辨識對方。

c、商家與漫遊電信業者：在小額資訊商品交易階段，假使有心人士想要冒充為合法得標商家，他必須產生履約訊息$\{TID, M, H(Goods), (Goods \oplus MAC'_{VM}(TID))\}$，設法讓$MAC'_{VM}(TID)$通過漫遊電信業者的檢驗。然而，除非指定 TID 被授權的對應商家，否則無法持有效的K_{VM}產生合法之$MAC_{VM}(TID)$。在大額資訊商品交易階段中，漫遊電信業者除了可透過有效的K_{VM}外，還可以藉由檢驗$\{M, E_{K_{VM}}(S_M(E_{PK_C}(Goods), BC))\}$內含之配對授權 BC 的有效性，來確認商家的合法性。由此可知，漫遊電信業者有能力確實地鑑別商家身份的合法性。同理，商家可以透過檢驗競標收據$\{V, E_{K_{VM}}(S_V(TID, Bid, M))\}$與配對授權$BC = S_V(CPO_L, PK_C, Bid, M)$的有效性，達到鑑別漫遊電信業者身份之目的。

2. 隱密性：協定中，足以影響交易進行之安全性的秘密資訊，例如有價代幣、通訊金鑰、信用額度簽章金鑰與資訊商品等，必須確保其隱密性。以下就協定中安全關鍵的秘密資訊之隱密性進行分析。

a、由於秘密註冊資訊 RR 與註冊授權 RC 內含秘密值以匿名金鑰K_L加密保護，為了獲取加密資訊，竊聽者必須設法計算出$K_L = g^{bw} \bmod p$。然而，在無法取得被用戶與註冊電信業者所秘密持有的 b 與 w 值之情況下，根基於解離散對數問題的困難度(Schneier 1996)，竊聽者將無法順利計算出K_L。

b、秘密值Z_C與Z_B分別由用戶與註冊電信業者所產生，且希望秘密地被彼此所分享，讓雙方得以產生一致的通訊金鑰 $K_{VC} = H(Z_C, Z_B)$與雜湊鍊的啟始值$r_0 = MAC_{BC}(Z_C, Z_B)$。這意謂著，任何人只要窺視Z_C與Z_B值，即可獲取K_{VC}假扮為用戶或漫遊電信業者來欺騙另一方，也可以因取得r_0而計算得到 n 個有價代

幣 $r_m=H^m(r_0)$ $(m = 1, 2, .., n)$。然而，僅有持有鑑別金鑰 K_{BC} 與匿名金鑰 K_L 的用戶與註冊電信業者，才可以從註冊資訊 $RR = E_{K_L}(C, H(Z_C), (Z_C \oplus MAC_{BC}(\beta)))$ 與註冊授權 $RC = \{B, E_{K_L}(Z_B, H(SK_C), (SK_C \oplus MAC_{BC}(Z_B)))\}$ 中推算得到 Z_C 與 Z_B 值。由此可以得知，協定可以達到保障 Z_C 與 Z_B 值的隱密性之目的。另外，也因此，用戶代名 $CID_T = H(C, Z_C)$ 可以取代用戶身份 C，提供用戶身份的匿名性。

c、若想要從註冊授權 $RC = \{B, E_{K_L}(Z_B, H(SK_C), (SK_C \oplus MAC_{BC}(Z_B)))\}$ 中取得簽章金鑰 SK_C，竊聽者需要事先取得匿名金鑰 K_L 與鑑別金鑰 K_{BC}。由上述分析可得知，竊聽者並無從獲取 K_L 與 K_{BC}，表示 SK_C 的隱密性可被確信。

d、如果竊聽者想要從訊息 $\{RC, E_{PK_V}(K_{VC}), TCert_C\}$ 中取得通訊金鑰 K_{VC}，必須準備漫遊電信業者的私密金鑰。因此，這企圖將無法如願。

e、若竊聽者試圖分別自訊息 $\{TID, M, H(Goods), (Goods \oplus MAC_{VM}(TID))\}$、$\{M, E_{K_{VM}}(S_M(E_{PK_C}(Goods), BC))\}$ 或 $\{S_V(TID, Bid, (K_G \oplus E_{PK_C}(Goods)))\}$ 中得到資訊商品 $Goods$，需要準備秘密金鑰 K_{VM} 或用戶的私密金鑰 SK_C。因此，這攻擊無法成立。另外，竊聽者在無法獲得 $E_{PK_C}(Goods)$ 資訊的情況下，從 $(K_G \oplus E_{PK_C}(Goods))$ 取得商品金鑰 K_G 將不可能實現。

f、竊聽者在無法取得通訊金鑰 K_{VC} 的情況下，試圖自價值 P 單位之付款訊息 $\{TID, P, (r_{n-P} \oplus MAC_{VC}(TID, P))\}$ 導出代幣 r_{n-P} 的攻擊將會失敗。

g、若竊聽者試圖從競標請求 $\{M, E_{K_{VM}}(S_M(TID, Bid))\}$ 中獲取商家出價資訊，達到破壞採購單 CPO_L 的競標秩序之目的，需要事先取得對應的秘密金鑰 K_{VM}。在 K_{VM} 無法取得的情況下，每位商家的出價資訊 Bid 之隱密性將可受到保護，進而達到競標之公平性。

3. 真確性：協定利用眾所周知具有驗證訊息真確性能力的單向雜湊函數、訊息鑑別碼與數位簽章技術，防止訊息於傳輸過程中遭受惡意竄改或因網路不穩定產生之錯誤。

4. 不可否認性：為保證交易的公平性，必須達到用戶可確實取得購買之商品，商家則可順利取得貨款之目標。為此，必須讓交易方雙方持有具不可否認的憑據，當對方未依憑證內容履行義務，即可持此憑證做為法律上仲裁的依據。以下針對本文應用之數位簽章與單向雜湊鍊技術，檢視用戶、註冊電信業者、漫遊電信業者與商家之間交易的不可否認性，證明提出的商業協定可以支援用戶穿梭於各城市間進行交易。

a、數位簽章技術以簽章者的私密金鑰簽署資訊，具有不可否認的特性。因此，在 PKI 已建置的假設下，註冊電信業者簽章的短期信用憑證 $TCert_C = S_B(CID_T, V, PK_C, PK_V, n, \delta, r_n, EXP_{TC})$ 為用戶 CID_T 在指定的漫遊網路 V 內使用的公開金鑰 PK_C 與擁有總信用額度 δ 以及小額代幣總數量 r_n 背書，使其具有法律效益。用戶不可否認曾張貼的條件採購單 $S_C(CCPO)$ 與支付額度為 Bid 的付款授權 $PC = S_C(TID, Bid, V)$。同理，根基於 PKI 架構下，當糾紛發生時，核准競價的採購單 $S_V(TID, CCPO_L, EXP_{BID})$、競標請求 $S_M(TID, Bid)$、競標收據 $S_V(TID, Bid, M)$、配對授權 $S_V(CPO_L, PK_C, Bid, M)$、資訊商品

$S_M(E_{PK_C}(Goods), BC)$ 與履約資訊 $S_V(TID, Bid, (K_G \oplus E_{PK_C}(Goods)))$ 皆可視為責任釐清之依據。

b、因為 $r_0 = MAC_{BC}(Z_C, Z_B)$，只有用戶與註冊電信業者有能力產生，這意謂著代幣值 $r_m=H^m(r_0)$ $(m = 1, 2, .., n)$僅被用戶與註冊電信業者所知。在用戶與註冊電信業者間存在信賴關係的前提下，當漫遊電信業者出示 r_{n-P}，用戶不能否認曾於漫遊網路 V 內消費 P 單位之服務。

由以上分析可確信，提出之協定可以支援用戶於各電信網路內進行商業活動，並可達到交易之雙向身份鑑別、隱密性、真確性以及不可否認性等安全需求。

二、效率性分析

對參與行動商務的單位而言，除了行動用戶使用低運算與儲存能力的設備外，其他單位皆是透過高運算與儲存能力之伺服器來完成交易處理。因此，商務處理的效率性為行動用戶所密切關心的議題。當行動用戶漫遊至另一個電信網路，區域更新階段將在行動設備、註冊電信業者與漫遊電信業者等三單位交互作業下完成，行動用戶並不需要主動參與。因此，協定之效率性將著重於分析交易階段的運算處理量。

表 3 顯示協定中行動用戶端需要進行密碼技術的運算量與主動連線之次數。在小額資訊商品交易階段中，僅需分別使用 1 次的單向雜湊函數、3 次 MAC 與 2 次的 XOR 運算。根據 Schneier (Schneier 1996) 明確指出：使用相同運算能力的設備，每秒鐘可計算 20,000 次的單向雜湊函數，2,000 次的對稱式加解密，與 2 次簽章處理。因為 MAC 為包含金鑰之單向雜湊函數，可視為與單向雜湊函數一樣擁有高運算效能，加上 XOR 是眾所周知的高效率運算元，由此可明顯得知提出之小額資訊商品交易協定具有效率性。另外，由於單向雜湊函數與 XOR 皆具有固定長度的輸出資訊之特性(Bird et al. 1995； Schneier 1996)，可以有效降低協定所需之訊息的傳輸量。此優勢除了為用戶節省交易所需費用外，也使得協定可以適用於低資源的無線網路。

表 3：用戶端交易計算量統計表

作業階段 / 計算次數	行動用戶		
	區域更新	小額交易	大額交易
單向雜湊函數	n+4	1	1
MAC	3	3	1
XOR	2	2	2
對稱式金鑰加密	1	0	2
對稱式金鑰解密	1	0	0
公開金鑰加密	0	0	0
公開金鑰解密	0	0	1
簽章處理	0	0	3
指數運算	2	0	0
主動通訊	1	2	2

大額商品交易模式利用簽章技術，提供採購單內容、履約商品與付款授權等更高層級的真確性和不可否認性等能力，以及使用公開金鑰加密方法來達到訊息的身份鑑別性與隱密性，確保買賣雙方之交易權益。也因此，如表 3 所示，用戶除了需要單向雜湊函數、MAC 與 XOR 等高效率的密碼技術外，還必須計算 2 次對稱式加解密，1 次公開金鑰解密與 3 次的數位簽章。不過，由於買方主導商業模式具有讓用戶在交易期間無須全程處於線上的優勢，用戶除了請求張貼條件採購單與付款時必須連線，其餘交易時間皆處於被動且離線的狀態。因此，用戶可離線填寫條件採購單、簽署該條件採購單與簽署付款授權等高運算需求的作業後，方再連線發送訊息。相較於需要用戶線上全程完成高資源耗費之運算的傳統交易方法，本協定將可以舒緩交易時所需的運算負擔。

三、討論

以下分別介面設計、行動運算與用戶的匿名性三部分做探討。

1. 介面設計：隨著網路服務與應用的迅速開發，消費者將花費大量時間對網路上龐大的資訊進行搜尋，方能找到目標資訊。雖然，目前已提供搜尋引擎，提升消費者尋找資訊的效率，但是對於購買商品的消費者而言，仍須一一比較商家所提供之商品價格、配件、配送成本與商家信譽等考量因素，消費者依然需要耗費大量資訊蒐集的時間與成本，且只能妥協於商家所開立之交易條件。藉由對條件採購單的規劃，提供用戶更便利的輸入格式；並透過用戶購買策略處理機制之設計，致使系統更精確地尋找消費者理想的交易商家。因此，本協定除了可有效減緩行動設備運算處理負擔，以及幫助用戶節省可觀的通訊傳輸費用等實質利益外，更可因簡化用戶所需的操作次數而提升協定的使用率，以促進行動商務之發展。

   行動用戶之消費額度的核發，取決於其信用額度再扣除目前已消費之金額，即用戶目前所剩的信用額度。於全球化行動商務模式下，註冊電信業者於用戶的行動設備發出區域更新請求時，發送用戶消費明細請求訊息給用戶方才離去的漫遊電信業者。藉此，註冊電信業者可以即時管理用戶的消費情況，適度調整授權信用額度，以有效杜絕壞帳問題。為確保交易可順利進行，用戶可利用繳款來保持消費額度。另外，註冊電信業者可依據用戶漫遊區域的幣值，計算出該區大額或小額之價格界定值。在完成區域更新程序後，行動設備內即儲有該價格界定值；當用戶填寫條件採購單時，行動設備依據購買目標價，自動顯示大額或小額交易所對應之策略，以減少用戶需輸入的資訊量，並避免策略選取錯誤之發生。
2. 行動運算：隨著電信技術的進步與行動設備計算能力的提升，行動網路已能提供較高的資訊傳輸率，而搭配微型處理器之智慧型行動設備則允許用戶處理相較複雜的運算。而且，運算效率大幅超越 RSA 非對稱式密碼系統的橢圓曲線加解密與簽章技術，已經廣泛應用於資源相較為低的行動網路。這些發展，直接

提昇用戶端交易處理的效率。本文所提的商務協定除了可以保持上述因技術發展所帶來的效益，還可以因允許用戶無須全程線上參與而舒緩因複雜運算所帶來的負擔。

3. 用戶匿名：於網路上進行交易的消費者，對於其個人隱私問題日益重視，故所提出的協定可提供用戶匿名交易的特色。當用戶移動至新的電信網路區域內，行動設備隨機產生用戶代名，經由用戶註冊電信業者授權後，用戶便可於對應之漫遊電信網路內使用此代名來進行交易。透過用戶每次進入陌生行動網路或再次跨入曾經漫遊網路內皆會擁有不同身份代名的機制，可避免因商家或漫遊電信業者蒐集用戶之消費資料，而導致用戶遭受大量廣告信件騷擾。本文提出之協定可以提供用戶更高階的個人隱私保護。

陸、結論

本文提出之行動消費者主導商業模式，利用張貼條件採購單的方式，節省消費者所需之搜尋時間與通訊成本，而且賦予消費者擁有商品定價與規格制訂的權利，依據其心目中理想之採購條件購買個人化的商品或客製化之服務，不再單由商家主導制式規格或售價。協定針對消費者對於候選商家挑選條件的不同，提供跨區交易與採購策略之服務，精確篩選出個別消費者理想的交易對象，以提升消費者交易滿意度。協定中允許行動用戶無須全程連線參與交易之進行，用戶僅需於張貼採購單與付款時才需連線處理，此兩項程序亦可離線運算完成後再將結果連線傳送。而且，應用具效率的安全機制，可有效避免行動設備因計算資源不足所引起的處理時間過長，以降低交易失敗率的增加。本協定提供用戶一個具有低成本、便捷且安全等特性的全球化行動交易平台，期望藉以行動用戶最為關切之交易便捷性與安全性等議題的解決做為試金石，以提升行動商務之成交機會。

本文未來研究方向以建立智慧型條件採購單系統為主軸，利用具學習與分析能力的資訊技術，以挖掘個別行動用戶之消費策略以及操作習慣，進而模擬用戶參與交易之行為，彈性地提供具個人化的輸入介面，並有效減少採購單上所需之購買條件的輸入量與操作選項，透過模擬與學習機制，即時修訂用戶誤植的採購條件，有效降低因採購單內容錯誤所導致的交易失敗率。期望透過此智慧型系統，克服因行動設備受限於簡易輸出入介面所帶給行動用戶之不便，以利建置更具個人化與效率性的行動交易系統。

參考文獻

1. Asokan, N., Janson, P.A., Steiner, M. and Waidner, M., “The State of the Art in Electronic Payment Systems,” *IEEE Computer* (30:9) 1997, pp: 28-35

2. Barnes, S.J., "The Mobile Commerce Value Chain: Analysis and Future Developments," *International Journal of Information Management* (22:2) 2002, pp: 91-108
3. Bird, R., Gopal, I., Herzberg, A., Janson, P., Kutten, S., Molva, R. and Yung, M., "The KryptoKnight Family of Light-Weight Protocols for Authentication and Key Distribution," *IEEE/ACM Transactions on Networking* (3:1) 1995, pp: 31-41
4. Boman, K., Horn, G., Howard, P., and Niemi, V., "UMTS Security," *Electronics & Communication Engineering Journal* (14:5) 2002, pp: 191-204
5. Chen, H.B. and Hsueh, S.C., "Light-weight Authentication and Billing in Mobile Communications," *Proceedings of the 37th IEEE International Carnahan Conference on Security Technology*, Taipei, Taiwan, 2003, pp: 245-252
6. Dai, Y. and Zhang, L., "A Security Payment Scheme of Mobile E-Commerce," *Proceedings of the International Conference on Communication Technology* (2) 2003, pp: 949-952
7. Datamonitor Research Ltd., Mobile Payment Systems, http://uk.sun.com/wireless/resources/pdf/ datamonitor.pdf, 2000
8. Diffie, W. and Hellman, M., "New Directions in Cryptography," *IEEE Transactions on Information Theory* (22:6) 1976, pp: 644-654
9. Durlacher Research Ltd., Mobile Commerce Report, http://www.durlacher.com/download/mcomreport.pdf, 2000
10. ElGamal, T., "A Public-Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms," *IEEE Transactions on Information Theory* (IT-31:4) 1985, pp: 469-472
11. Foo, E. and C. Boyd, "A Payment Scheme using Vouchers," *Proceedings of the Financial Cryptology Conference*, LNCS 1465, Springer-Verlag, 1998, pp: 103-121
12. Foo, E. and C. Boyd, "Passive Entities: A Strategy for Electronic Payment Design," *Proceedings of the 5th Australasian Conference on Information Security and Privacy*, LNCS 1841, Springer-Verlag, 1998, pp: 134-148
13. Ginzboorg, P., "Seven Comments on Charging and Billing," *Communications of the ACM* (43:11) 2000, pp: 89-92
14. Grecas, C.F., Maniatis, S.I. and Venieris, I.S., "Introduction of the Asymmetric Cryptography in GSM, GPRS, UMTS, and Its Public Key Infrastructure Integration," *Mobile Networks and Applications* (8:2) 2003, pp: 145-150
15. Herzberg, A., "Payments and Banking with Mobile Personal Devices," *Communications of the ACM* (46:5) 2003, pp: 53-58
16. Horn, G. and Preneel, B., "Authentication and Payment in Future Mobile Systems," *Journal of Computer Security* (8) 2000, pp: 183-207
17. Jin, L., Ren, S., Feng, L. and Hua, G.Z., "Research on WAP Client Supports SET Payment Protocol," *IEEE Wireless Communications* (9:1) 2002, pp: 90-95
18. Kalakota, R. and Robinson, M., *M-Business: the Race to Mobility*, McGraw-Hill, 2001
19. Kelsey, J. and Schneier, B., "Conditional Purchase Orders," *Proceedings of the 4th ACM*

Conference on Computer and Communications Security, Switzer-land, 1997, pp: 117-124

20. Kim, M.A., Lee, H.K., Kim, S.W., Lee, W.H. and Kang, E.K., "Implementation of Anonymity-Based E-Payment System for M-Commerce," *Proceedings of the IEEE 2002 International Conference on Communications, Circuits and Systems and West Sino Expositions* (1) 2002, pp: 363-366
21. Lin, C.H. and Dow, C.R., "Efficient Checkpoint-based Failure Recovery Techniques in Mobile Computing Systems," *Journal of Information Science and Engineering* (17) 2001, pp: 549-573
22. Lin, T.H. and Shin, K.G., "Damage Assessment for Optimal Rollback Recovery," *IEEE Transactions on Computers* (47:5) 1998, pp: 603-613
23. Naruse, K., "Findings of the Mobile-Users Survey," *ECOM Journal* (4) 2002, pp: 52-57
24. NTT DoCoMo, Subscriber growth, http://www.nttdocomo.com/companyinfo/subscriber.html#06, accessed 22 Feb. 2004
25. Pagliusi, P.S., "A Contemporary Foreword on GSM Security," *Proceedings of International Conference on Infrastructure Security*, LNCS 2437, Springer Verlag, 2000, pp: 129-144
26. Park, T., Woo, N. and Yeom, H.Y., "An Efficient Optimistic Message Logging Scheme for Recoverable Mobile Computing Systems," *IEEE Transactions on Mobile Computing* (1:4) 2002, pp: 265-277
27. Park, T., Woo, N. and Yeom, H.Y., "An Efficient Recovery Scheme for Fault-Tolerant Mobile Computing Systems," *Future Generation Computer Systems* (19:1) 2003, pp: 37-53
28. Samfat, D., Molva, R. and Tsudik, G., "Authentication of Mobile Users," *IEEE Network, Special Issue on Mobile Communications Technologies* (8:2) 1994, pp: 26-34
29. Schneier, B., *Applied Cryptography*, 2nd Edition, John Wiley and Sons, New York, 1996
30. Senn, J.A., "The Emergence of M-Commerce," *IEEE Computer* (33:12) 2000, pp: 148-150
31. Shelfer, K.M. and Procaccino, J.D., "Smart Card Evolution," *Communications of the ACM* (45:7) 2002, pp: 83-88
32. Sirbu, M.A., "Credits and Debits on the Internet," *IEEE Spectrum* (34:2) 1997, pp: 23-29
33. Stach, J.F., Park, E.K. and Makki, K., "Performance of An Enhanced GSM Protocol Supporting Non-Repudiation of Service," *Computer Communications* (22:7) 1999, pp: 675-680
34. Tsalgatidou, A. and Pitoura, E., "Business Models and Transactions in Mobile Electronic Commerce: Requirements and Properties," *Computer Networks* (37) 2001, pp: 221-236
35. Varshney, U.R., Vetter, J. and Kalakota, R., "Mobile Commerce: A New Frontier," *IEEE Computer* (33:10) 2000, pp: 32-38
36. Varshney, U., "Mobile Payments," *IEEE Computer* (35:12) 2002, pp: 120-121
37. Zheng, X. and Chen, D., "Study of Mobile Payments System," *Proceedings of the IEEE International Conference on E-Commerce*, 2003, pp: 24-27