行政院國家科學委員會專題研究計畫　成果報告

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(3/3)

計畫類別：整合型計畫
計畫編號：NSC92-2213-E-002-012-
執行期間：92 年 08 月 01 日至 93 年 07 月 31 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、江彬榮、蘇文鴻

報告類型：完整報告
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 93 年 12 月 23 日

摘要

隨著無線通訊技術蓬勃發展與無線裝置的普及，行動商務的浪潮成為繼電子商之後一股勢不可擋的新潮流。由於行動裝置具有高度的「anytime，anywhere，instanton」等特性，因此行動商務可以讓使用者真正隨時隨地存取資訊與服務，不僅能夠成為有線電子商務的延伸，更能開拓原本網際網路經濟無法觸及的市場。由於無線通訊與行動裝置具有許多先天上的限制，例如無線通訊可靠度較差且頻寬較低，而行動裝置的運算能力、儲存空間、螢幕大小都受到限制。因此我們不可能將原本網際網路上的服務直接搬到行動環境上。我們必須為行動環境開發專屬的內容服務，才能符合行動裝置的先天限制並且徹底發揮「無線」的優勢。本研究將探討及設計行動電子商務之安全代理人交易模式，並實作一套適用於行動商務的電子付款系統。用戶端的平台可以是 PDA、行動電話、智慧卡等可攜式無線裝置。使用者可以在實體商店申透過藍芽、紅外線、GSM 等無線通訊技術和商店端的 POS 終端溝通付款。當使用者瀏覽無線網際網路時，也能夠透過 GSM、無線區域網路等通訊管道和虛擬商店溝通。除了安全的考量外，我們的機制與系統也將使用者隱私權保護及風險評估與保障納入考慮。

第一章　緣起

隨著寬頻網路時代的來臨，網際網路已經帶給人們全新的生活體驗。多采多姿的聲光、方便快速的搜尋功能、更低廉的行銷成本，這些條件都將使網際網路上的商業行為持續地蓬勃發展。再加上近年來無線通訊的快速發展，行動商務 (Mobile eCommerce) 勢必成為一個重要的行銷通道。然而，方便而安全的付款技術是影響電子商務發展的重要因素之一，因此我們急需建構一套新一代的付款機制，以符合 E 世代民眾的需求。

本研究報告將建構一套既能透過網際網路付款，又能結合日常實體使用的電子貨幣系統。如此，民眾可以使用這套付款模式上網購物，也能坐公車、捷運、繳停車費、甚至可以到便利商店購物。這一套電子貨幣系統必須能保障使用者的隱私權、安全性、便利性，而且必須能滿足網際網路頻繁的小額付款。

隨著網路頻寬與電腦速度的突飛猛進，網路生活已經成為 E 世代人類不可或缺的部分。有許多交易行為必然地會在網際網路上發生，例如實體或軟體的買賣、資訊服務、資源使用…因此一套安全且便利的電子付款機制對於網際網路上的電子商務發展，具有舉足輕重的影響力。

在另一方面，民眾在現實的生活中，實體貨幣的使用有許多不便之處，因此塑膠貨幣的推展是世界各國都有的共識。民眾可以攜帶一張智慧卡（smartcard）打公用電話、從資訊服務站上網、搭公車、坐捷運、在商店購物、繳停車費，不但安全，而且攜帶方便。

如果網際網路上的付款機制和現實生活的塑膠貨幣可以整合成一套數位貨幣系統，結合兩者的優點，如此的系統將是下一代電子付款技術的目標。

對於講求速度快成本低的新一代電子付款系統而言，如何結合現有的基礎建設與機制來達成目標，是所有研究人員追求的目標。如果能利用電信業者既有的使用者群、用戶資料、帳單作業等基礎來發展一套完整的付款解決方案，必定可以降低系統建置的時程與成本，以及運作的金流成本。

當一個具有以上特性的付款機制能夠建構完成之後，相信可以帶動國內電子商務的蓬勃、上網人數的增加、民眾日常生活的便利，提早讓我國進入一個數位貨幣的時代。

第二章　現今流行的交易模式

2.1 現有實體商店的付款模式

我們先對目前實體商店常用的付款模式做一些討論：

(1) 現金

現金是目前全世界大部份的人都在使用的付款方式，不論我們身在何方，幾乎都可以用現金付款，現金的優點是普及、方便、快速。但現金的缺點也不少：例如現在偽鈔問題嚴重，增加社會大眾不少負擔。出門時須攜帶實體貨幣並不方便、且現金無法在 Internet 使用、遺失時被侵占性高…等等。

(2) 信用卡

信用卡是國人目前第二流行的付款模式，優點是出門時不用攜帶實體貨幣、且通用性高，在實體商店或虛擬商店皆可使用，可是衍生出的問題比現金嚴重的多，例如：交易時間過長、交易成本高(3%)、最嚴重的問題是安全上的問題良多，、容易被不肖人士盜用及側錄。

2.2 現有虛擬商店的付款模式

(1) 信用卡

在虛擬商店購物時最常使用的付款方式就是利用信用卡，但是如果有在網路購物的經驗，就會發現信用卡所要求的認証資料相當的少，不肖人士只要知道消費者的卡號及該

卡有效日期即可利用該卡購物，這對消費者十分沒有保障。

如果在十個網站使用信用卡購物、信用卡資料就會被這十個網站知道，也就是如果其中一個網站被侵入，消費者的資料也就全部落到有心人士的手上。今天一般消費者可能不只在一個網站購物，可能是幾十個，也可能是上百個，我們消費者如何保証每個網站都是可信任或不會被侵入呢？

(2) ATM 轉帳

比起信用卡而言，ATM 轉帳付款安全多了，虛擬商店不會知道消費者的任何訊息，但缺點是消費者必須特地出門尋找 ATM 提款機轉帳付款

(3) 貨到付款

貨到付款也是很多虛擬商店使用的付款模式，商店不用擔心收不到錢，但是消費者會擔心收到的貨品是否正確，因貨品必須付款簽收後才能領取，領取後才能檢查。

貨到付款的手續費過高，約新台幣 50 到 100 元，在很多小額付款的場合，這成本太高了

(4) Paypal 之類的付款系款

Paypal 是一種 Payment Service Provider，為什麼會有這種付款方式產生呢？這是為了增加信用卡安全性而衍生出的付款模式，消費者用使用卡購物時須信任每個網站，這風險太高了，所以 Paypal 就變成是中間人，我們付款給 Paypal，Paypal 再將款項付給該店家，這種作法的好處是

我們只須信任 Paypal，且店家無法知道我們的信用卡資料即可完成交易。

雖然 Paypal 乍聽起來似乎很完美，但還是有很大的安全性問題，利用 Paypal 在網路購物付款時，該店家網頁會彈出一個 Payal 的付款視窗，店家可以自己偽裝該付款的網頁，不小心檢查網址列的消費者就會被盜取 Paypal 的帳號密碼。

第三章　手機付款的類似模式

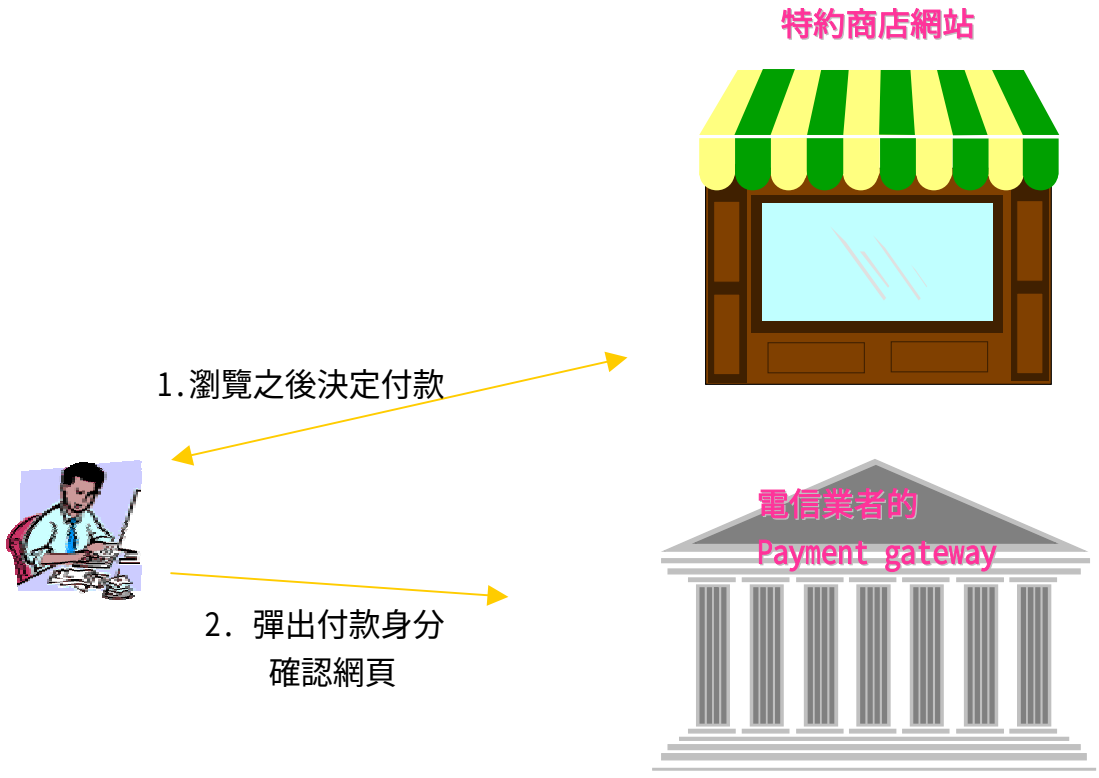
目前台灣與手機有關的付款模式有以下三種

遠傳 i-Style 小額付款

台灣大哥大小額付款

中華電信 839 小額付款

分別由三大電信業者提出，服務內容都大同小異，消費者若要使用這類服務須先用手機撥電話給電信業者，電信業者會給該消費者一組對應該門號的密碼，就可利用該組門號密碼在特約網頁上購物，帳單則是結合在手機帳單中。



虛擬商店付款時讓消費選擇各種付款方式

選擇使用遠傳 i-Style 付款時所彈跳出的付款視窗，沒有網址列，

消費者無法判別這個網頁是否真是遠傳電信的網頁

這類付款系統有以下這些缺點：

- 嚴重的安全風險

  若是遇到惡意的網站，偽造成付款認證網頁，進而偷取使用者的密碼 (中間人攻擊)。

- 侷限於特約商店

  目前有合作的特約商店僅二十幾家，要激起大眾的使用慾望沒有很大的說服力。

- 只有註冊時有利用手機確認身份，不算是用手機付款，只能說是將帳單結合到手機帳號上而已。

此外，中華電信、遠傳、和信等業者也相繼推出以 STK 為基礎的行動銀行服務，它們能夠提供行動線上金融轉帳等功能。但是線上轉帳並不適合頻繁的小額付款，因為金融轉帳的手續費高，而且在手機上要輸入對方帳號 (銀行代號 3 碼，帳號約 12~15 碼)、金額、PIN 碼，是非常緩慢、不便、且容易出錯的事情。

第四章　新一代電子付款機制的目標

我們針對國內電子商務與貨幣電子化發展的趨勢，歸納出下一代電子付款機制的目標與需求：

1. 方便性：現代人出門必帶的兩樣隨身物品是手機及錢包，如果我們能用手機取代實體貨幣及信用卡，那麼錢包的所要放的物品就會減少，甚而可以出門只帶個手機就好了。

2. 安全性：安全性是任何電子付款系統必要的先決條件。因此我們在設計電子付款系統時必須優先考慮安全性的問題。最好能解決信用卡容易被盜用側錄的問題、及現金遺失易被侵占的問題。

3. 通用性：一套電子付款機制必須具有通用性，不僅可以在 PC 上透過網際網路使用，也可以在實體商店、停車場、等等情境下使用。

4. 用戶端高效率：用戶端系統應該具有高度的可攜帶性，因此用戶端的作業平台大部分是 smart card、PDA、手機之類的行動裝置。這些裝置的運算能力遠不及一般桌上型 PC，因此我們在設計付款協定時，必須考慮到這些裝置所必須執行的計算量。

5. 適當的隱私保護：隱私是人類與生俱來的慾望，因此具有匿名性的電子付款系統才能符合消費者的期望。但是在另一方面，政府當局會希望她能夠掌控所有的金融流通，以打擊不法的活動。因此，當我們在設計電子付款系統時，應該找到這兩種需求的平衡點。

第五章　手機付款系統的實作

近年來，行動通訊的快速發展，幾乎人人都有手機。除了通訊用途之外，行動通訊業者為了擴展客源，無不絞盡腦汁，開發更多更方便的加值服務。在這種環境下，行動商務 (Mobile eCommerce) 就成為眾所矚目的焦點。

由於行動裝置具有高度的「anytime, anywhere, instant on」等特性，因此行動商務可以讓使用者真正隨時隨地存取資訊與服務，不僅能夠成為有線電子商務的延伸，更能開拓原本網際網路經濟無法觸及的市場。

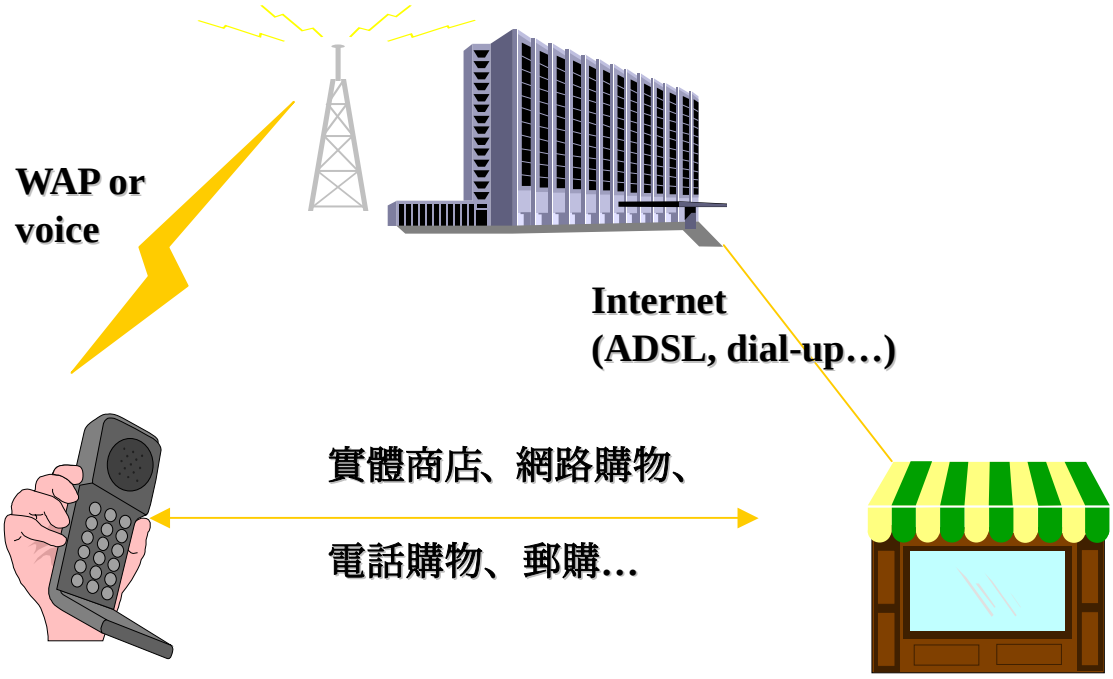
基於極高的手機普及率，行動商務勢必成為一個重要的行銷通道。有許多交易行為必然地會在行動通訊網路上發生，例如實體或軟體的買賣、資訊服務、資源使用…等等。然而，方便而安全的付款技術是影響行動商務發展的重要因素之一，因此我們急需建構一套新一代的付款機制，以符合 E 世代民眾的需求。

而我們的方案即是結合手機而產生的新付款機制。

5.1 設計理念

- 儘可能減少使用者操作手機按鍵的次數
- 儘可能保護使用者消費隱私
- 在方便與安全之間取得平衡點
- 不限定使用特定規格之手機

5.2 整體架構



此架構中，有三個主要的角色：使用者、商家、及電信業者。使用者在實體商店或是網路購物時與店家接觸，結帳時由店家及使用者以合作或個別的方式與電信業者溝通，商店以 ADSL 或是專線與電信業者溝通以產生交易紀錄 而使用者以 WAP 或是 Voice 的方式與電信業者交換交易資訊及確認付款。

5.3 Data Items

以下是我們實作時所要儲存及傳送的重要資訊：

- IDuser: 使用者代碼 (8-digit)

  IDuser 八位數是受限於手機能顯示條碼的位數（其中一碼是檢查碼），最多可有一千萬名用戶參與
- PhoneNo: 使用者手機門號 (10-digit)
- IDmerchant: 商店代碼 (8-digit)

- IDterminal: 端末機代碼 (optional)
- Amount: 交易金額
- Type: 交易類別
- Date-Time: 交易時間
- S/N: 交易序號

以上這些資料在我們的三大角色中，除了電信業者擁有所有的資訊，店家及消費者都只知道自己的代碼及部份交易資訊。

5.4 IDuser vs. PhoneNo

其實用 PhoneNo 就可以代表每一個使用者了，那為什麼要多設一個 IDuser 的代號呢？其實是為了使用者隱私而設計的，在我們的其中一個方案中是由電信業者直接撥電話給使用者，那就必須讓店家傳送使用者相關資訊至電信業者，可是若是告知店家我們的電話號碼，就可能被店家搜集門號日後發廣告短訊之類的困擾，所以我們只告知店家 IDuser（使用者代碼），店家只知道使用者代碼，但是不知道對應的手機門號（電信業者才知道），就可以達到儘量保護使用者隱私的目標。

5.5 依據資料流向設計的三大方案

- ***Scheme 1: 使用者 → 商店 → 電信業者***

  使用者告知商店使用者代碼，商店匯整交易資訊及商店資訊傳給電信業者，再由電信業者撥電話給該使用者確認付款

- ***Scheme 2: 使用者 → 電信業者 ← 商店***

1.商店傳送交易資訊及商店資訊至電信業者

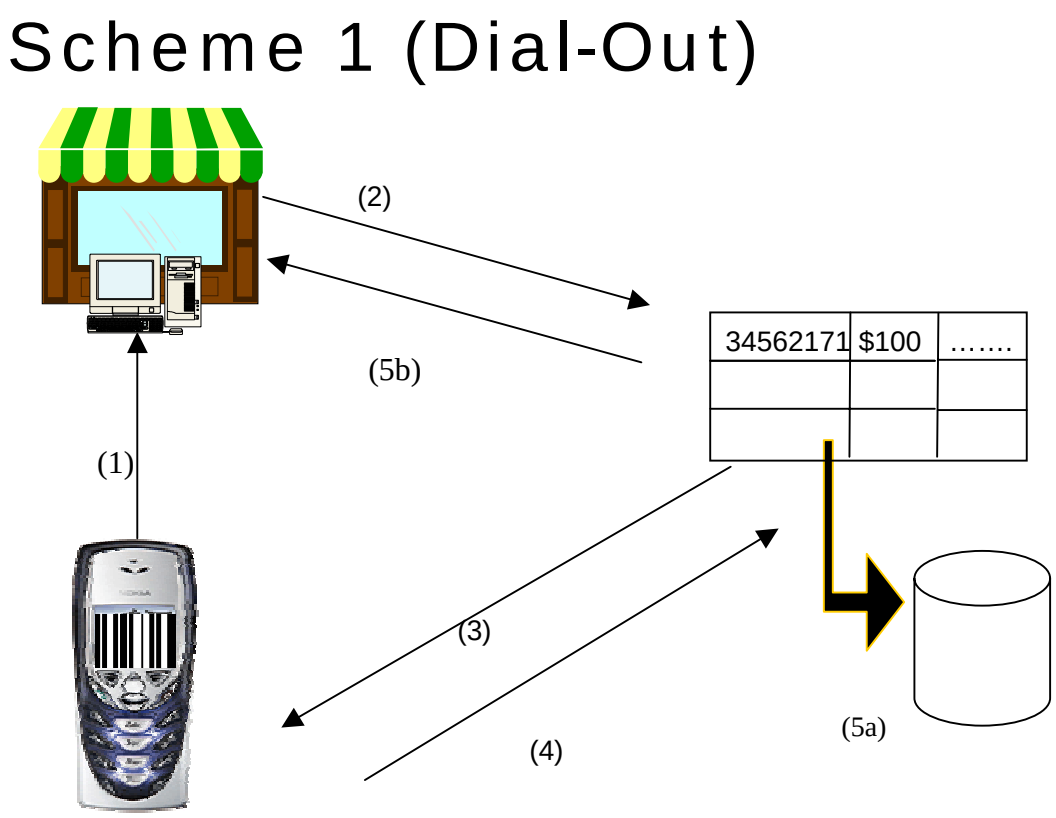
2.電信業者產生交易代碼並回傳給商店

3.商店告知使用者交易代碼

4.使用者用撥電話或用 WAP 連至電信業者確認付款

- ***Scheme 3: 商店 → 使用者 → 電信業者***

商店利用紅外線將商店資訊及交易資訊傳給使用者後再由使用者匯整傳給電信業者完成交易



詳細步驟：

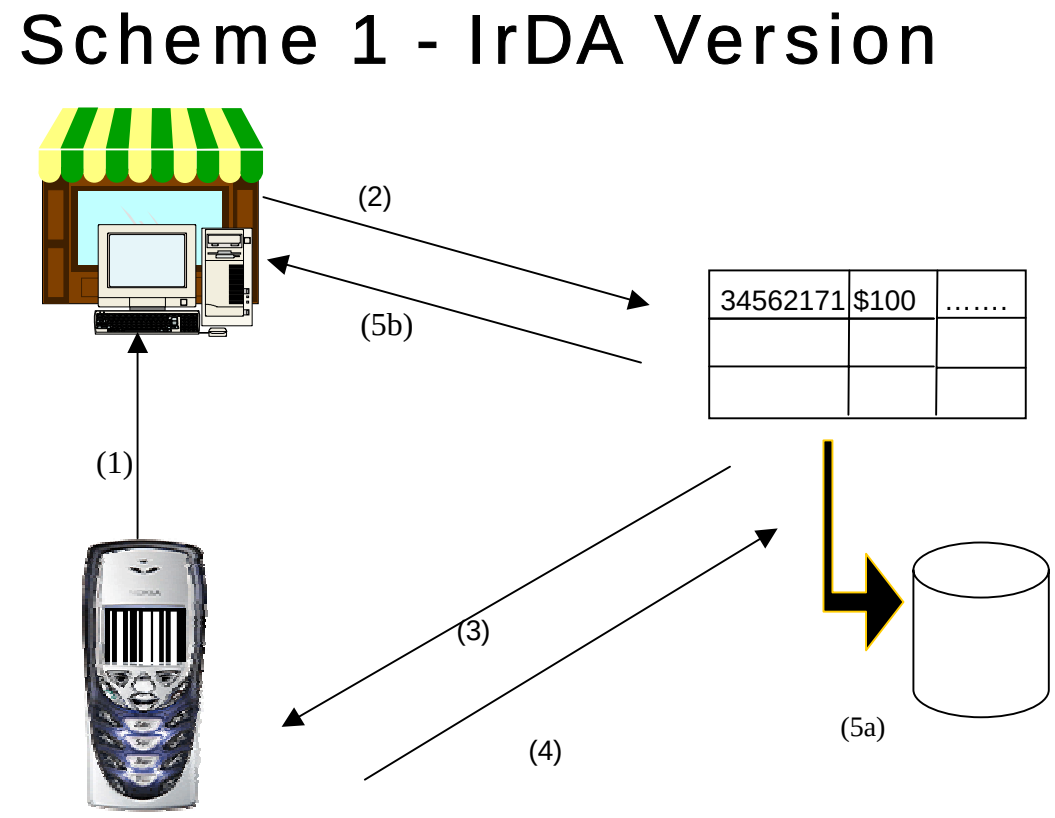
1.商店利用使用者手機上的條碼讀入 ID_{user} 或口頭告知 ID_{user}。

2.商店將使用者代號、商店代號、交易金額送到電信業者，電信業者產生交易紀錄。

3.電信業者撥電話至(Dial-Out)使用者告知該筆交易的商店名稱及交易金額。

4.使用者輸入密碼確認付款。

5.電信業者將結果存入資料庫(a)及送付款憑証至商店(b)。



詳細步驟：

1.商店利用使用者手機上的條碼讀入 ID_{user} 或口頭告知 ID_{user}。

2.商店將使用者代號、商店代號、交易金額送到電信業者，電信業者產生交易紀錄。

3.電信業者撥電話至(Dial-Out)使用者告知該筆交易的商店名稱及交易金額。

4.使用者輸入密碼確認付款。

5.電信業者將結果存入資料庫(a)及送付款憑証至商店(b)。

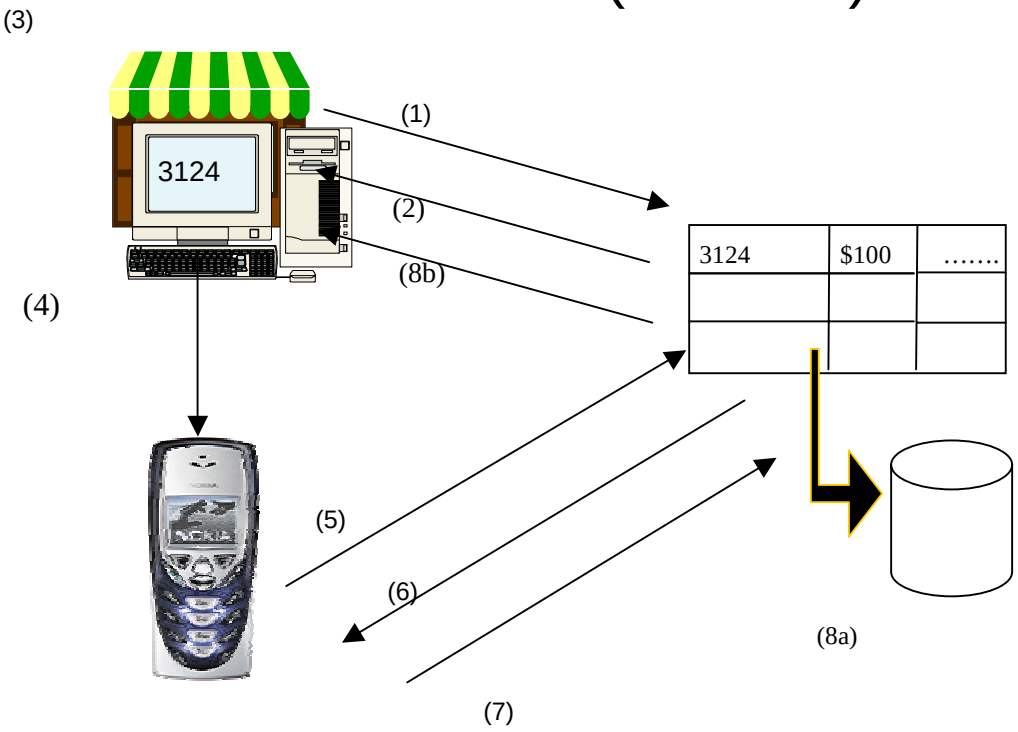
在 Scheme 1 中必須由使用者告知商店使用者代碼以使電信業者能主動打電話給使用者確認付款，告知使用者代碼有很多種方式，最快的方式是用條碼的方式讓商店掃描，或是以紅外線傳送，但不是每款手機的螢幕都能顯示條碼或是使用者不願在手機上貼條碼貼紙。那就必須用口頭告知的方式，雖較慢但也應為大眾所接受，因為就像告知統一編號一樣。

付款憑據是中華電信對以下資料項目的數位簽章：

IDuser, Date-Time, S/N, IDmerchant, IDterminal, Amount, Type

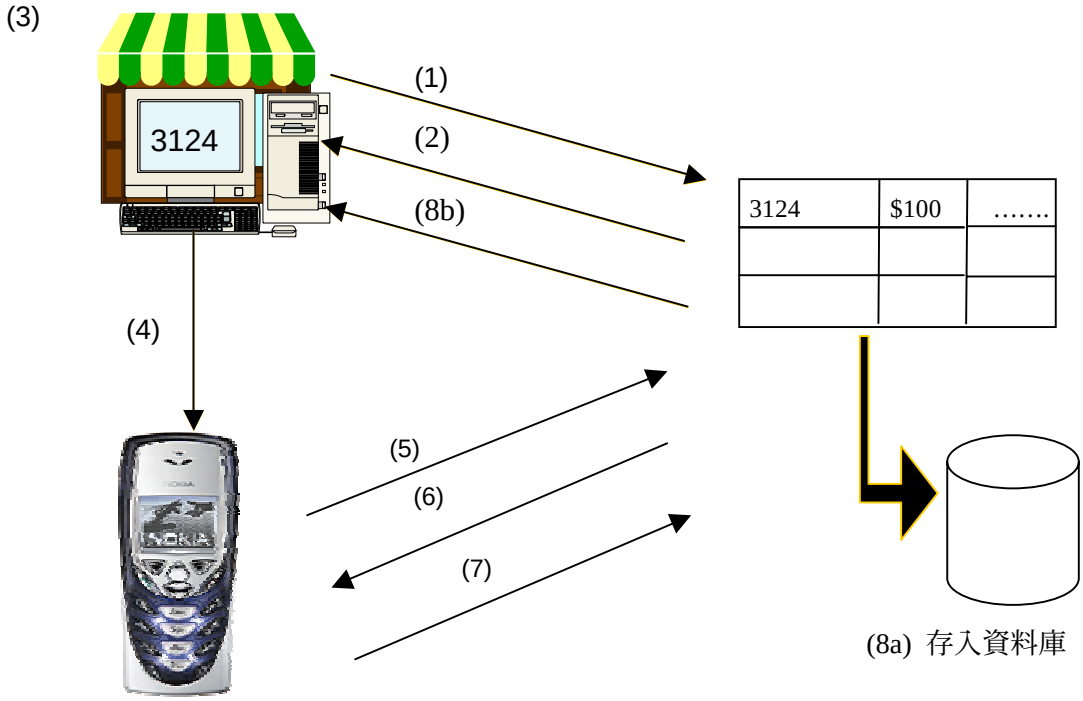
此付款憑據是為了保護商店能從電信業者拿到錢，商店在查詢交易狀態時若該使用者付款的話，電信業者須給商店付款憑據，以防止電信業者事後否認不付款。

Scheme 2 (Dial-In)



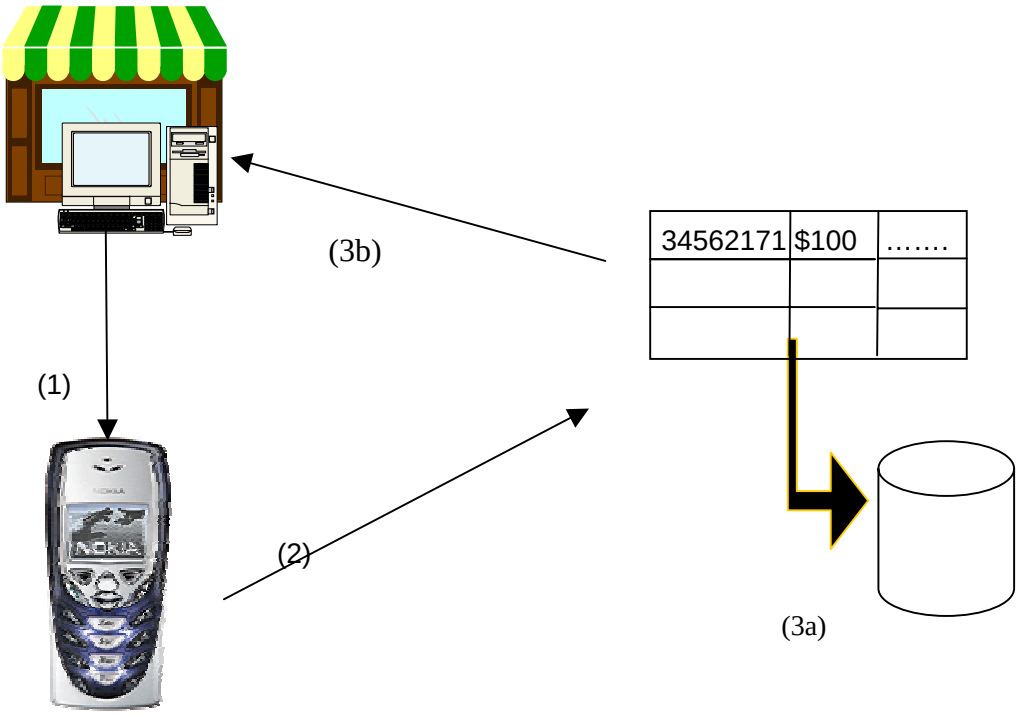
1. 商店端傳入商店代碼與交易金額到伺服器。
2. 伺服器傳回交易代碼。
3. 商店將交易代碼顯示在終端機的螢幕上。
4. 使用者在終端機上看到交易代碼，或店員告知交易代碼。
5. 使用者利用三碼的特殊門號和交易代碼進行撥號，如 888 3124。
6. 電話撥通後，語音告知交易內容，包括商店名稱及交易金額。
7. 使用者輸入密碼進行確認動作。
8. 伺服器確認完成後將交易資料存入資料庫(a)，並產生認證資訊給商店端(b)。

Scheme 2- WAP Version



1. 商店端傳入商店代碼與交易金額到伺服器。
2. 伺服器傳回交易代碼。
3. 商店將交易代碼顯示在終端機的螢幕上。
4. 使用者在終端機上看到交易代碼，或店員告知交易代碼。
5. WAP 連線到付款網頁，輸入交易代碼。
6. 電話撥通後，語音告知交易內容，包括商店名稱及交易金額
7. 使用者輸入密碼進行確認動作。
8. 伺服器確認完成後將交易資料存入資料庫(a)，並產生認證資訊給商店端(b)。

Scheme 3



1. 商店以紅外線傳輸商店名稱相關資料至手機。
2. 使用者利用手機傳使用者代號、商店代號、交易金額等資訊到伺服器。
3. 伺服器產生交易結果，存入資料庫中(a)，同時產生付款憑據給商店端來完成交易(b)。

5.6 執行細節說明

5.6.1 環境需求：

- 伺服器端

  硬體規格

  - PCI 數據卡（頂堅數據機，Intel 晶片）

  - 個人電腦

  軟體規格

  - Borland C++ Builder 6.0
  - Microsoft Access
  - Microsoft IIS
  - Microsoft Windows 2000 或以上（具有 TAPI 3.0）
  - ExceleTel TelTools 3.6
  - OpenSSL

- POS 端

  硬體規格

  - 個人電腦
  - 條碼掃描器

  軟體規格

  - Borland C++ Builder 6.0

- Mobile POS 端

  硬體規格

  - Pocket PC (Compaq ipaq 3630)
  - Wireless LAN Card (PCI NW-110)
  - GSM Dual Band PC Card (UbiNetics GC-201)

  軟體規格

  - Windows CE 3.0

- 網路商店端

  硬體規格

  - 個人電腦

軟體規格

- 有瀏覽器的任何作業系統

◆ 客戶付款機制

硬體規格

- IVR 部份：任何 GSM 手機 (OKWAP 166)
- WAP 部份：有支援 WAP 1.1 以上的任何手機 (OKWAP 166)

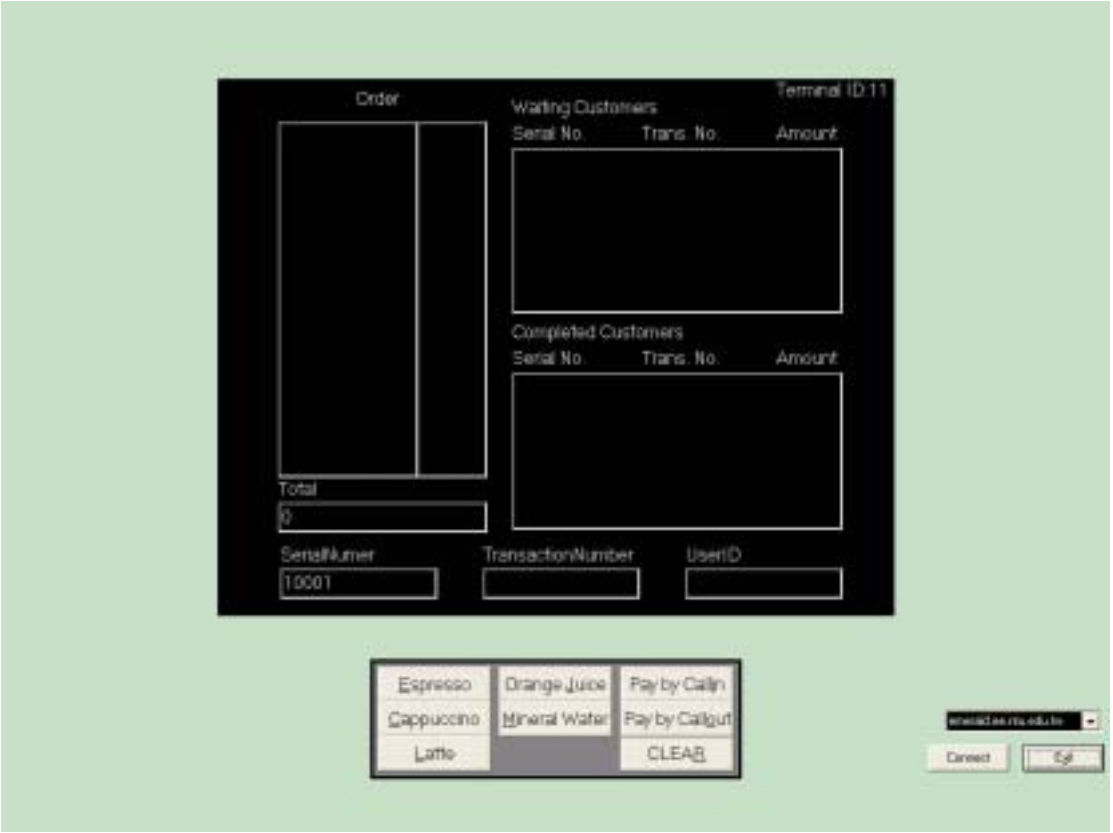
5.6.2 程式功能

1. 伺服器端：下圖為伺服器端的程式介面

其主要功能如下：

- ◆ 以 Access 作為資料庫，進行交易資料的存取，也可改用其他種資料庫作為資料庫的資料來源。
- ◆ 右上方兩個窗格中，上面的是等待進行的交易，會有交易代碼、客戶代碼及金額的顯示，下格則是已完成交易，會顯示交易的結果。
- ◆ 下方的三個窗格可監視各種交易的進行狀態，像電話的部份可看到電話目前是否有來電及接聽處理狀態。
- ◆ 交易狀態可以看到各種利用網際網路傳送進來的資訊，且所有利用網際網路的交易訊息均經過 SSL (Secure Socket Layer) 的加密傳輸。
- ◆ 語音狀態是目前撥放的語音的內容。

2. POS 端：下圖為 POS 端執行的畫面



- POS 端是模擬早期終端機的黑白螢幕，下方的按鈕則是模擬終端機上的按鍵。
- 商品的輸入不僅可利用按上面的鍵輸入，也可利用條碼的讀碼機來輸入（此部份尚待完成）。
- 完成購買後，可以選擇以 Dial-in 或是 Dial-out 的方式付款，並會出現在右上方的等待顧客窗格中
- 若顧客完成交易後，螢幕會自動閃爍，並將已完成交易的顧客資料移到下方的已完成的窗格中。

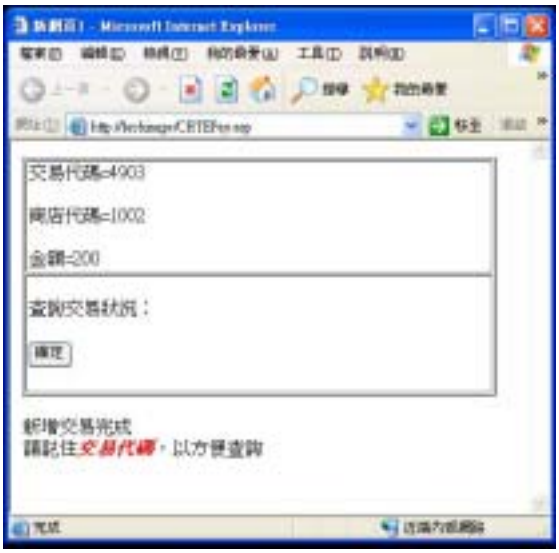
3. Mobile POS 端：

- ◆ 新增交易畫面：

  在這個畫面中可以進行新增交易，輸入店家代碼及金額，如左下圖所示：

- ◆ 交易代碼畫面：

  系統會顯示交易代碼，並可提供查詢交易進度狀況，如右下圖所示。



- ◆ 交易查詢畫面

交易完成與否會顯示在交易狀態列，若未完成可再進行查詢，若未完成，系統會定期自動更新目前交易狀態。

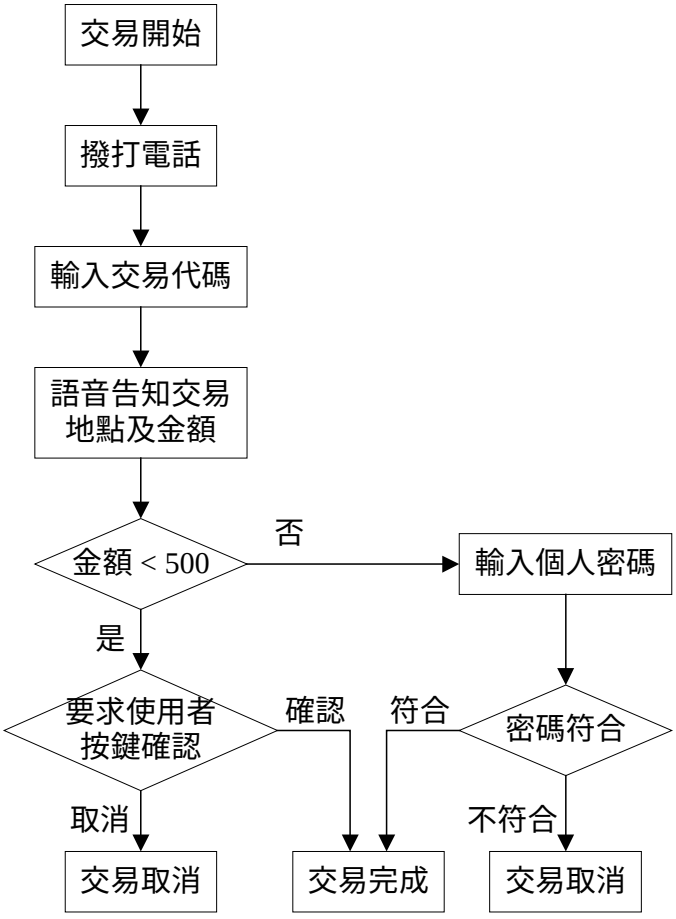
4. 網路商店端

目前僅做一個網路購物的雛型，主要為模擬使用者在網路上購物後提供另一個付款的管道，以方便使用者有更多的付款選擇。下圖為電子商城的購物畫面。

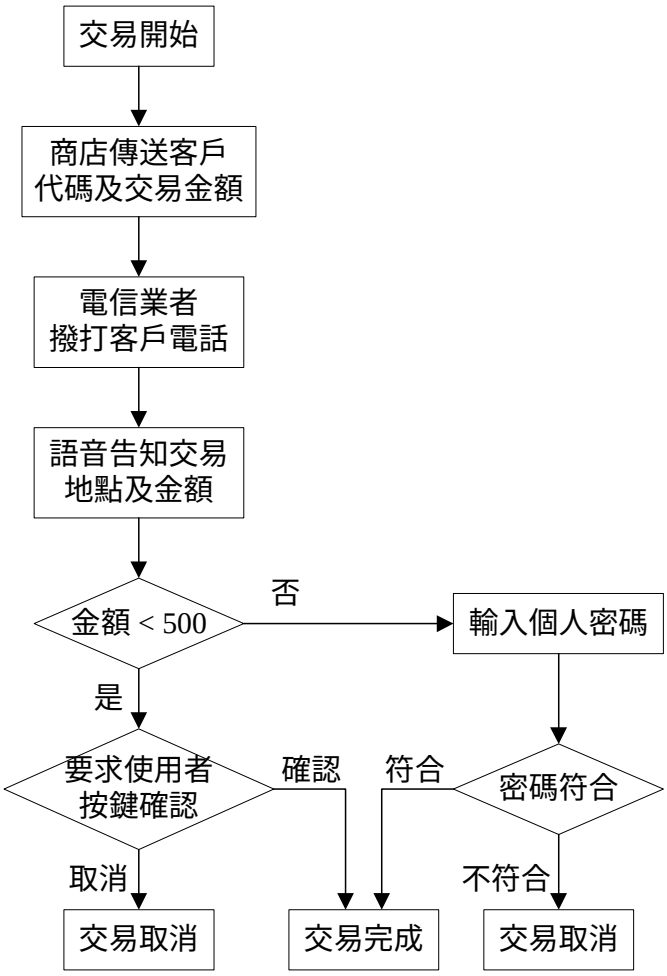
5.6.3 程式流程圖

1. 伺服器端交易流程圖

Dial-in 交易流程

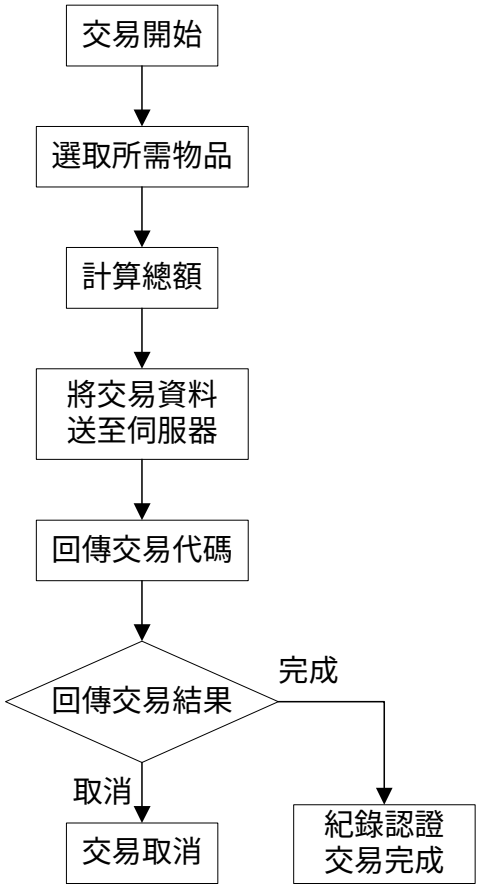


Dial-out 交易流程



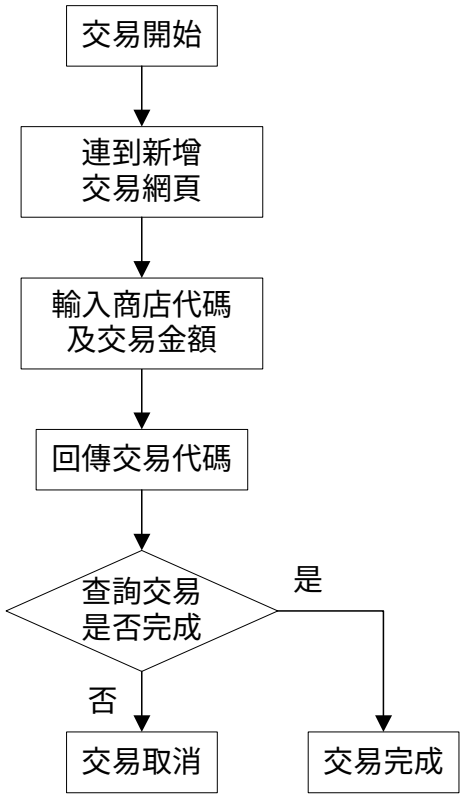
2. POS 端交易流程

POS 交易流程

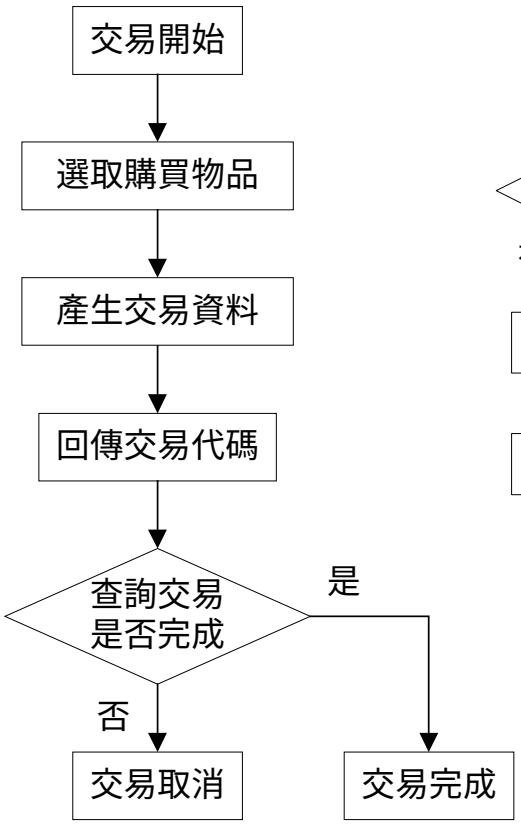


3. Mobile POS 端交易流程

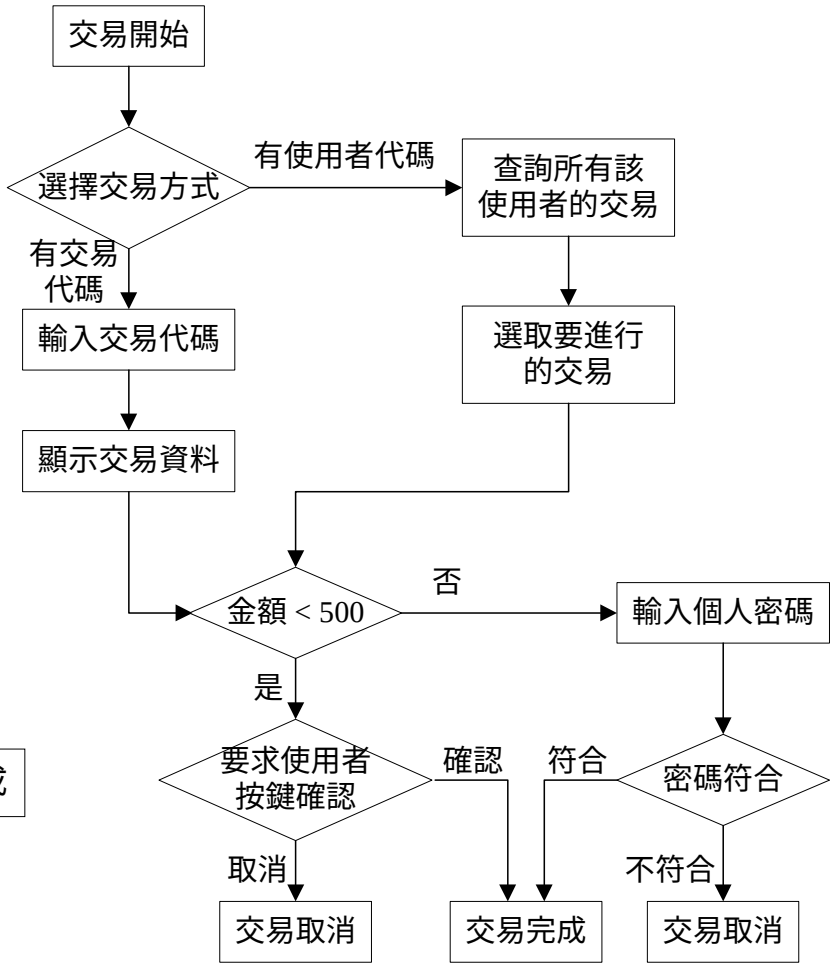
Mobile POS 交易流程



4. 網路商城交易流程



5. WAP 端交易流程



5.6.4 簡要程式碼相關資訊

下表為程式碼中主要定義的交易類型及其代碼和所需的參數, 供查詢對照程式用。

交易形式	代碼	參數 1	參數 2	參數 3
Dial-in 產生交易	11	商店代碼	金額	
Dial-in 回傳交易代碼	12	交易代碼		
Dial-in 交易完成	13	交易代碼	結果	
Dial-out 產生交易	21	商店代碼	金額	客戶代碼
Dial-out 回傳交易代碼	22	交易代碼		
Dial-out 交易完成	23	交易代碼	結果	
WAP 查詢交易代碼	41	客戶代碼		
WAP 查詢交易資料	42	交易代碼		
WAP 進行交易	43	交易代碼	密碼	
WEB 產生交易	51	商店代碼	金額	
WEB 回傳交易代碼	52	交易代碼		
WEB 查詢交易狀況	53	商店代碼	交易代碼	

第六章 手機付款在 Mobile POS 的應用

目前大部份的付款都是至定點結帳(Fixed POS)，但在一些場合並不適用，可以任意移動的結帳點(Mobile POS)會比較方便，以下是 Mobile POS 的應用例子：

- 餐廳服務生至客戶旁結帳

  比較高級的餐廳都是服務生至顧客餐桌旁結帳，此時以現金交易較方便及安全，若是以信用卡交易，服務生必須將卡帶回櫃台刷卡，若是顧客不隨行的話很不安全，因可能被盜刷或側錄，但顧客隨行至櫃台刷卡也就失去原本的方便性。而以手機付款的方式也可以同現金付款一樣，能在餐桌旁完成付款而不用擔心太多。

  餐廳消費簡略步驟如下：

  點菜

  1.服務生帶著 PDA 至顧客旁

  2.顧客點菜

  3.服務生用 PDA 將顧客所點菜單傳至餐廳 Server

  結帳

  1.PDA 送出交易資訊至電信業者

  2.電信業者回傳交易交碼

  3.服務生告知客戶交易代碼

  4.顧客以手機付款

  5.服務生以 PDA 確認付款

- Pizza Hut 外送結帳

  顧客打電話或以網路訂購 Pizza，送達後送貨員只收現金，因為

此時無法使用信用卡結帳。此時手機付款也可適用，送貨員可以手機或是 PDA 查詢顧客付款與否。

- 行動商販

有些商販都是與顧客約定時間地點當場交易，而沒有固定的店面，對他們來說只能收取現金，若是使用我們的手機付款方式，也可完成交易，步驟如下：

1.商販與顧客當場交易

2.商販以 Mobile POS 新增交易

3.電信業者回傳交易代碼

4.顧客以手機付款

5.商人以 Mobile POS 查詢付款與否

- KTV

現今 KTV 結帳方式是以現金及信用卡，但使用信用卡的話顧客必須隨行以防被盜刷或側錄，使用手機付款則能如同現金付款一樣在包廂內完成付款。

- 百貨專櫃

在百貨公司購物時，結帳時間都會花很長，因為結帳時店員都必須跑到統一的收銀台結帳，若能以手機付款達到 Mobile POS 的功能，相信會方便許多

完成 Moible POS 的解決方案：

- 手機 + WAP

以手機經由 WAP 新增交易、查詢交易、及付款就可完成所有現金可達到的 Mobile POS 功能。

- PDA + 無線網路 (或 GSM module)

  使用手機當 Mobile POS 有個缺點就是螢幕太小，對於產生交易或是查詢不太方便，若是能使用 PDA 當 Mobile POS 應會更方便，目前可使用 PDA + GSM module 的方式變成大螢幕手機當 Moible POS。無線網路日漸發達，日後在很多地方可直接以 PDA + 無線網路達到這個目標。

第七章 系統架構改良

在第三章所提出來的三種方案並沒有辦法完全達到我們所有的目標，第一個問題在於在第四章的三個方案只適用於小額付款，如果是太龐大的金額電信業者並不容易接受，因為電信業者畢竟不像銀行業，有豐富的處理呆帳能力，所以為了能達成高額付款的目標，在本章節提出與銀行配合的方案，第二個問題是行動電話如果離線(收不到訊號)時就沒辦法完成交易，我們參考一些關於電子錢幣(E-Cash)的研究，設計出另一套手機離線時使用的方案。

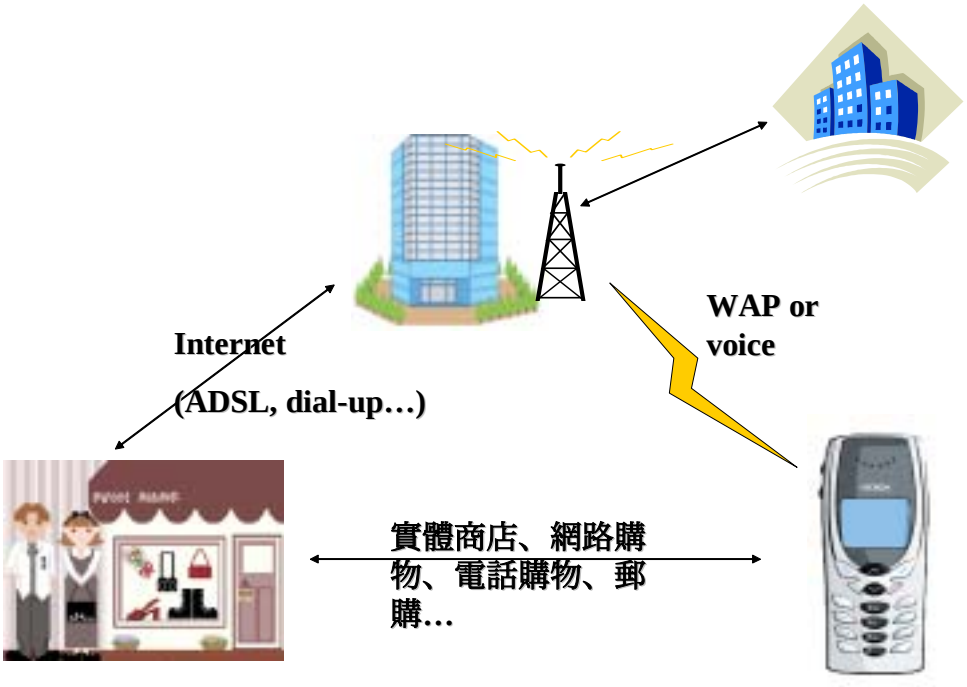


圖15.高額交易系統架構

7.1 高額交易

目前第三章所提出的方案仍只適用於比較小額的付款，因為若是開放大額付款，電信業者就必須要負擔隨之而來的呆帳風險，如果不能提高可使用的額度將會降低此付款機制的通用性及可行性，因銀行處理呆帳的能力比電信業者好多，所以提出一個與銀行合作的方案，將大額的收付款轉給銀行，而電信業者只負責收取中間的手續費，用手機付款的款項將列在銀行帳單而不是現今的手機通信帳單上。在高額交易方案中，使用者必須與電信業者簽約以授權電信業者能直接從該使用者銀行帳戶中扣款。圖 15 為我們高額交易系統的架構圖。

7.1.1 高額交易方案一

此方案即是第三章中的方案一與銀行配合的新版本(圖 16)

詳細步驟：

1. 商店利用使用者手機上的條碼讀入 ID_{user} 或口頭告知 ID_{user}。
2. 商店將使用者代號、商店代號、交易金額送到電信業者，電信業者產生交易紀錄。
3. 電信業者向銀行查詢該使用者的帳戶餘額是否足夠付款，不足的話取消此筆交易，充足則繼續。
4. 電信業者撥電話至(Dial-Out)使用者告知該筆交易的商店名稱、交易金額、交易序號並告知此筆交易將由銀行帳戶扣款，並要求使用者口述交易序號及輸入密碼。
5. 使用者口述交易序號及輸入密碼確認付款。
6. 電信業者語音辨識及聲紋比對無誤後向銀行索取轉帳憑據。
7. 銀行傳送轉帳憑據至電信業者
8. 電信業者將結果存入資料庫 8(a)及送付款憑証至商店 8(b)，及利用簡訊傳送收據給使用者 8(c)。

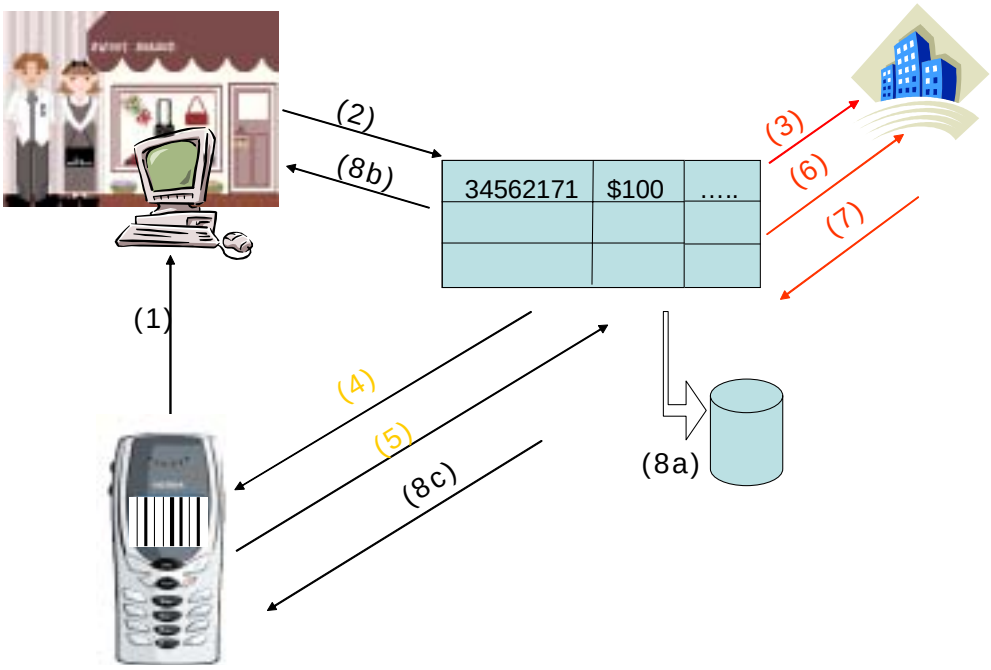


圖16.高額交易方案一

7.1.2 高額交易方案二

此方案即是第三章中的方案二與銀行配合的新版本(圖 17)

詳細步驟：

1. 商店端傳入商店代碼與交易金額到伺服器。
2. 伺服器傳回交易代碼。
3. 商店將交易代碼顯示在終端機的螢幕上。使用者在終端機上看到交易代碼，或店員告知交易代碼。
4. 使用者利用三碼的特殊門號和交易代碼進行撥號，如 888 3124 。

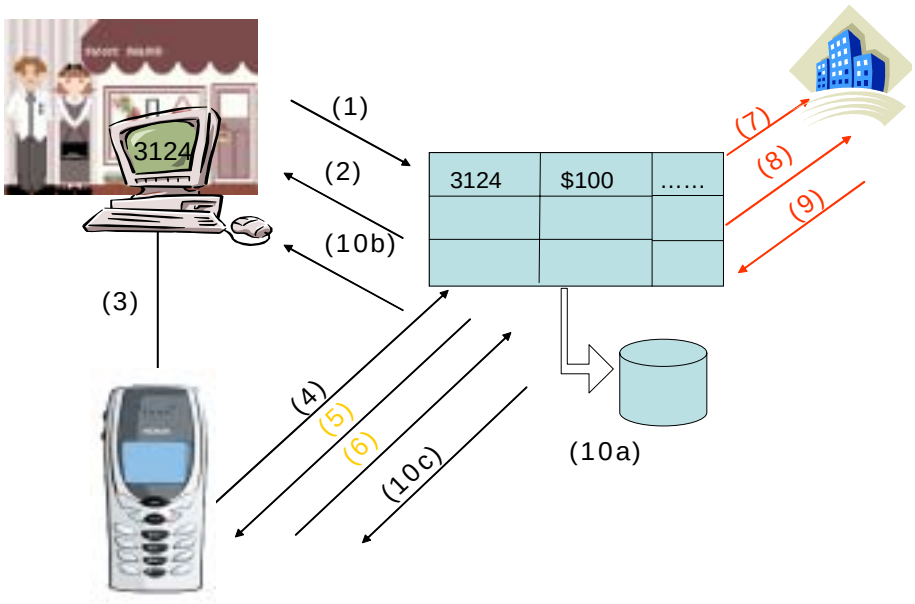


圖17.高額交易方案二

5. 電話撥通後，語音告知交易內容，包括商店名稱及交易金額、交易序號並告知此筆交易將由銀行帳戶扣款，並要求使用者口述交易序號及輸入密碼。

6. 使用者口述交易序號及輸入密碼確認付款。

7. 電信業者語音辨識及聲紋比對無誤後向銀行查詢該使用者的帳戶餘額是否足夠付款，不足的話取消此筆交易，充足則繼續。

8. 電信業者向銀行索取轉帳憑據。

9. 銀行傳送轉帳憑據至電信業者。

10. 電信業者將結果存入資料 (a)及送付款憑証至商店(b)，及利用簡訊傳送收據給使用者(c)。

7.1.3 不可否認性的加強

本來的方案使用PIN碼已俱有不可否認性的功能，但為了防止PIN碼有可能洩露的風險(例如店家裝設針孔攝影機偷錄或無意間被朋友得知)，我們希望在高額交易時能有更強的不可否認性，因此分別在方案一改良版的步驟四、五及方案二改良版的步驟六、七中加入了使用者必須口述交易序號的部份，而在電信業者端則要加入語音辨識及聲紋比對的功能。使用者在確認付款的過程中增加口述交易序號的步驟，雖然會拉長交易的時間，但卻可增加高額交易時所重視的不可否認性。使用者口述的聲音可讓電信業者利用聲紋比對的方式確認是否為該使用者，那麼為何要口述交易序號呢？假設只單靠聲紋比對，有可能出現的問題是不肖人士暗中錄下我們的聲音以實行重送攻擊。每次口述的交易序號均不同，那麼除非攻擊者錄到我們念所有數字的聲音，不然重送攻擊是不會成功的。況且在實體商店購物時要實行重送攻擊難度很高，因為付款的時候有店員在監督是不可能直接拿出播音機播發數字給手機聽的。

7.1.2 降低交易成本

在高額交易時因加入了銀行端，所以交易成本必然會上升，

那麼要如何有效地降低交易成本呢？假設電信業者可接受的信用額度為 5000 元，額度不足時就直接從銀行端轉帳扣款，這樣的作法在每次額度不足時都會被銀行收取手續費，那麼有兩種情況對消費者是非常吃虧的，第一種情況是常常高額交易的人會被銀行收取手續費，另一種情況則是小額交易也會被銀行收取手續費，例如在月底時結帳前我們的額度有可能是接近用光的狀態，那麼此時任何一筆消費不論高額小額都會從銀行端扣款而被多收取手續費，那麼要如何才能降低銀行收取手續費而增加的成本呢？

既然只要從銀行轉帳就會被多收錢，那麼就想辦法減少用到銀行的機會。一般國人手機帳單常用的付款方式為後付(Post-Pay)，也就是到結帳日再付清，而我們設計降低手續費的方式則為半預付式，平常沒有用完額度時仍是採用月底結帳日才付款，但若在結帳日前即用完額度而須從銀行扣款時，使用者則可以設定連帶目前所有的帳款從銀行一次付清，以解決小額付款也會被收取手續費的窘況，這方案就屬於預付 0 元的方案。對常常用到會用到高額交易的人也可採用預付較多金額的方式來增加強可用額度來減少自銀行轉帳的次數。也就是說，如果採用預付 2000 元的方案，在每次使用到銀行扣款時除了付清所有帳款外，還要多扣 2000 元作為預付款，此時的可用額度就為 7000 元。

舉個例子來說，某個消費者採用預付 2000 元的方案，而他目前的帳款為 3000 元，那麼現在他若要消費一筆 3000 元的金額，由於所剩額度只剩 2000 元，所以將會從銀行直接扣款，電信業者這次交易就會從銀行扣款 3000(消費)+3000(目前帳款)+2000(預付額)=8000 元，此時的可用額度為 7000 元，此額

度足夠進行兩次不須要經過銀行的 3000 元交易，所以平均起來，每次 3000 元的交易只須要支付三分之一的銀行手續費。若是預付的愈多，那麼分攤後手續費就愈少。預付的方式是可行的，因為預付的部份若做為將來的通訊費用則有優惠，那麼有些人就會為了減低手續費的部份及通訊費優惠而欣然加入預付的行列。

7.2 手機離線方案

手機收不到訊號時時第三章的所有方案都無法完成交易，為了要解決這個問題，我們參考了許多電子錢幣 (E-Cash) 的研究，以期能找到或是設計新的一套電子錢幣機制，讓我們在手機離線時仍然可以完成交易。

E-cash 兼具安全性與匿名性的特點，一直是眾多學者在考慮電子付款機制時的首選。但是 E-cash 底層所使用的數位簽章技術到目前仍有一些需要改進的地方。例如：

- 減少使用者端的計算量

  因為在我們設計的電子付款系統中，使用者端的計算平台是 smart card、PDA/PDA、手機之類的裝置，它們的計算能力遠不如桌上型 PC，更不能和銀行端的大型電腦相提並論。所以如果電子錢幣的提款（withdraw）協定能夠將使用者端的計算量降低，可以有效減少使用者在提款時必須等待的時間。

- 可分割性

  因為傳統的電子貨幣系統都是以一個數位簽章代表一個貨幣單位，假設我們的電子錢幣最小單位是一元，那麼當我們想要提領 1000 元，就必須取得 1000 組數位簽章。假設每一組簽章的長度是 200 Bytes，1000 元就需要約 200 KB 的記憶體來存放。以目前的 SIM card 來說，扣除應用程式佔用的空間之後，可供存放資料的記憶體空間約在 8K~16K 左右，因此根本無法滿足傳統電子貨幣系統的需求。可分割的電子貨幣正好可以滿足這樣的需求。

- 公正性

  盲目數位簽章(blind digital signature)可以提供良好的匿名性，因此可以保護消費者的隱私。但是，完美的匿名性卻可能遭到不法之徒利用，例如當作洗錢的管道或恐嚇勒贖的取贖管道。因此，具有公正性的電子錢幣是近年來各國學者研究努力的方向。一般而言，公正性的電子錢幣必須有公正第三者的存在，而公正第三者的負擔越輕越好。

根據以上的需求，我們設計了一套具有公正性、可分割性、使用者端高效率的電子錢幣系統。整個系統參與的角色共有使用者、電信業者、商店、公正第三者（TTP)。整個電子貨幣的運作共可分為四個步驟：(1)領取信任憑證、(2)領取電子錢幣、(3)付款交易與回存。除此之外，在系統開始運作之前，必須公佈必要的參數。而當有不法行為發生時，公正第三者必須參與追查的動作。以下我們將詳細說明各個步驟。

1. 公佈參數

電信業者選擇兩個安全大質數 p_1, p_2（$p_1 \equiv p_2 \equiv 3 \bmod 4$），然後公佈 n（$= p_1 p_2$）。

TTP 也選擇兩個安全質數 p_3, p_4（$p_3 \equiv p_4 \equiv 3 \bmod 4$），而且 $p_3 p_4 > n$。然後 TTP 公佈 $\hat{n}$（$= p_3 p_4$）與一個字串 ϖ。

2. 領取信任憑證

(a) 使用者與 TTP 互相完成身分確認之後，使用者向 TTP 提出領取信任憑證的要求。

(b) TTP 隨機選取一個二進位字串 σ 與一個整數 r，其中 r 同時屬於 Z_n^* 與 $Z_{\hat{n}}^*$。

接著 TTP 為這位使用者產生一個匿名的身分符記 $I = (\varpi \| ID_{user} \| \sigma)^2 \bmod \hat{n}$，因為這個內含身分資訊的符記是經過二次方處理，所以只有 TTP 可以解得出來。

再來，我們必須讓電信業者端沒有辦法看出這個符記的長相，才不會破壞盲目數位簽章的不可追蹤性，因此 TTP 將用下列的方法來產生最終的匿名身分憑證：

TTP 計算 $\tilde{I} = H(I) r^4 \bmod n$，並且將 r 加密：$\tilde{r} = E(I)$，其中 $E()$ 代表對稱式加密函數，所使用的金鑰只有 TTP 知道。

最後 TTP 對這些元素進行數位簽章構成匿名身分憑證：

$(Sig(\tilde{I},\tilde{r}),\tilde{I},\tilde{r})$。

TTP 將匿名身分憑證與r^{-1}傳送給使用者。

(c) 使用者收到匿名憑證的時候，會先檢查 TTP 是否正確，如果正確無誤，就存下來作為將來領錢時使用。

3. 領取電子錢幣

為了達到可分割的性質，我們加入了小額付款 (micro payment) 機制中所使用到的 hash chain。因為我們目前設計的系統是屬於線上查驗 (on-line checking) 的，所以我們可以不用考慮使用者或商店可能的舞弊行為。假設我們每一個簽章可以代表 100 元，使用者在選取被簽章訊息m時，會先做 100 次 hash 運算，然後用$h^{100}(m)$當作給電信業者簽章的標的。每當使用者要領取一個代表 100 元的電子錢幣時，必須遵守以下協定：

(a) 使用者在Z_n^*中隨機選取m,u,v，使得$\alpha = h^{100}(m)(u^2+v^2) \bmod n$屬於$Z_n^*$。

然後使用者將α與一組匿名憑證$(Sig(\tilde{I},\tilde{r}),\tilde{I},\tilde{r})$傳送給電信業者。

(b) 電信業者在驗證過使用者出示的匿名憑證後，在Z_n^*中隨機選取x使得$(\alpha(x^2+1))^3 \bmod n \in QR_n$。接著電信業者將$x$傳送給使用者。

(c) 使用者在 Z_n^* 中隨機選取 b，並且計算

$$\delta = b^4 \bmod n$$
$$\beta = \delta(u - vx) \bmod n$$

接著他將 β 傳送給電信業者。

(d) 電信業者先算出 $\lambda = \beta^{-1} \bmod n$。因為電信業者有能力在 mod n 之下計算方根，所以電信業者可以找到一個 t 使得 $t^8 \equiv_n \tilde{I}^2(\alpha(x^2+1))^3\lambda^6$，然後電信業者將 (λ, t) 傳送給使用者。

(e) 最後使用者作以下解除彌封（unblinding）的動作

$$s = b^3 r^{-1} t \bmod n$$
$$c = \delta\lambda(ux + v) \bmod n$$

就可以得到最後的電子錢幣 $(I, h^{100}(m), s, c)$。

4. 付款交易與回存

使用者可以持用步驟(2)中所領取的電子錢幣進行消費。由於每個電子錢幣代表 100 元，因此使用者可能拿同一個電子錢幣在不同地方消費。假設使用者已經使用這個電子錢幣消費 k 元，而他這次要付 j 元（k+j<=100），那麼付款動作如下：

(a) 使用者將 $(I, h^{100}(m), s, c)$ 與 $h^{100-j-k}(m)$ 傳送給商店。

(b) 商店將使用者傳送來的資料連同預期付款金額 j 傳送給電信業者。

(c) 電信業者檢查資料庫是否已經有 m 的紀錄。如果沒有，就代表使用者是第一次使用該錢幣。反之則表示該使用者以

前曾經使用過這一枚電子錢幣。如果資料庫裡記錄著該枚錢幣已經使用 i 元，而 i=k，則電信業者端會將 j 元轉入商店端的帳戶，並且更新資料庫。否則，電信業者端會通知商店端「存入失敗」。

在以上協定中，雖然消費者可以享有匿名性，但是他持用同一枚電子錢幣所作的所有消費行為是可以被連結起來的。這個特性是目前所有可分割電子貨幣系統具有的共通現象。如果要克服這個問題，我們可以在使用者端軟體作修正，使得同一枚硬幣不要用在不同商店。如果使用者累積太多零碎的電子錢幣時，可以透過匿名通訊管道向電信業者端要求更新錢幣。

另一個問題是商店端可能侵占消費者的電子錢幣。商店端可能接收消費者的電子錢幣之後，沒有向電信業者作回存的動作或者故意讓回存失敗，然後向消費者宣稱該枚錢幣是無效的。之後商店端就可以那這些電子錢幣向其他商店消費。然而，大部分線上(on-line)的電子錢幣系統都不去考慮這個問題，因為商店端如果舞弊，會立即就被發現並且產生糾紛，而商店端獲得的利益將遠低於其建置的成本與商譽的損失。所以，相對上商店端是比較可信的。如果一定要解決這個問題，可以在付款協定中加入一段 zero-knowledge proof，使得只有電子錢幣真正的持有人能夠完成付款的動作。

5. 匿名性的撤銷

當我們發現有不法之徒濫用電子貨幣的匿名性時，我們可以在 TTP 的協助下撤銷特定電子錢幣的匿名性。撤銷的形式有兩種，我們分別說明如下：

(a) 電子錢幣追蹤(coin tracing)：

當我們發現歹徒領取電子錢幣當作取款的管道時，我們必須重建出歹徒手上持有之電子錢幣的長相，才能夠防堵他們使用手上的電子錢幣。在我們的系統中，追蹤的方法如下：

電信業者將使用者領取電子錢幣時使用的匿名身分憑證 $(Sig(\tilde{I},\tilde{r}),\tilde{I},\tilde{r})$ 交給 TTP 處理。TTP 首先將 $\tilde{r}$ 解密得到 I，而這個 I 是電子錢幣的其中一項元素，因此 TTP 就可以將 I 加入黑名單中，通知所有商店不可以接受含有 I 的電子錢幣。

(b) 使用者追蹤(owner tracing)：

當我們在犯罪事件中發現歹徒使用到電子錢幣時，我們可以透過 TTP 的協助追查出該電子錢幣的持有人，因而查出歹徒的身分。追查的方法是相關執法單位將電子錢幣 $(I,h^{100}(m),s,c)$ 交給 TTP。其中 I 是持有人的匿名身分符記，

TTP 計算出 I 的方根之後，就可以找出持有人的真實身份。

以上我們所提出來的電子貨幣系統具有公正性、可分割性、與使用者端高效率的特色。我們分別討論如下：

- 公正性

  在上述第(4)點中我們討論過匿名性的撤銷方法。有了這樣的機制之後，可以有效的防止歹徒利用電子貨幣來進行犯罪行為。

- 可分割性

  在我們上述的協定中，我們是以 100 元為一個電子錢幣的面額，而每個電子錢幣是可以分割使用的。因此我們可以讓一張 SIM card 能夠攜帶的金額提高許多。在實務上我們可以有彈性的調整每一枚電子錢幣的面額，例如發行 10、50、100 等面額。

第八章 分析比較

本章為本交易系統的各項分析及與其他付款機制的比較

8.1 安全性

在第三章的假設中，我們假設 GSM 通訊協定不容易被侵入及破解，所以偽造 SIM 卡所要投資的成本也遠比偽造信用卡要高得多，況且在我們的架構中，偽造了 SIM 卡也只能完成五百元以下的超小額交易，超過五百元的交易必須得知 PIN 碼，而高額交易更是需要聲紋的比對，對於不肖人士而言要從中獲利並不是一件簡單的事。

在我們的架構中，消費者與電信業者間是以 GSM 通訊協定不容易被侵入的前提設計的，而在商店端與電信者間則是以專線或撥接方式通訊，可利用 SSL 通訊協定，可讓電信業者及商店能互相認証及防止被竊聽。

表 2.各種付款機制安全性比較

	遺失保護	偽造可能性	須信任商家與否
我們的方案	**PIN、聲紋**	**低**	**否**
信用卡	**簽名**	**高**	**是**
現金	**被侵佔**	**高**	**否**
智慧卡	**PIN**	**低**	**是**
Paybox	**PIN**	**低**	**否**
GiSMo	**無**	**低**	**否**

表 2 是我們的系統與其他付款機制的安全性比較，與現金、信用卡相比，我們的付款機制在手機遺失時的風險是很小的，不僅有 PIN 碼保護且高額交易時更須要聲紋的比對。而被偽造的可能性也低得多。網路購物時不用提供該商家太多資訊即可完成交易，不用像信用卡怕機密資料被該交易網站濫用或是擔心交易過的網站被駭客入侵而得到我們的資料。也不用怕像信用卡在實體商店購物時遇到假的刷卡機被複製信用卡資料。智慧卡由於無顯示裝置，所以在有可能遇到假的刷卡機時而被溢刷(刷卡機會顯示假的金額)。Paybox 及 GiSMo 是類似的系統，Paybox 在遺失時只有 PIN 碼保護，但 GiSMo 對手機遺失是完全無防禦能力的。我們設計的系統架構並無以上的這些安全性問題。

8.2 不可否認性

在不可否認性的部份，交易時電信業者都會傳送付款憑據給商家，因此商家不用擔心拿不到錢。在電信業者為可信任的前提下，使用者也無法利用否認有確認交易而拒絕付款給電信業者(皆可由通聯紀錄檢查得知)。

在高額交易時，銀行也會傳送付款憑據給電信業者，所以電信業者也不用擔心從銀行那邊拿不到錢，再加上聲紋及口述交易序號的機制，使用者更是無從否認起。

8.3 使用者隱私

現今的社會，個人主義意識高漲，使用者隱私也愈來愈被注重，而目前很多付款機制都會透露不少使用者資訊給商家，雖不一定都是重要資料(例如：姓名)，但使用者最喜歡的仍是提供愈少資訊愈好。

在我們的其中一個方案中是由電信業者直接撥電話給使用者，那就必須讓店家傳送使用者相關資訊至電信業者，可是若是告知店家我們的電話號碼，就可能被店家搜集門號日後發廣告短訊之類的困擾，所以我們只告知店家 IDuser（使用者代碼），店家只知道使用者代碼，但是不知道對應的手機門號（電信業者才知道），就可以達到適當保護使用者隱私的目標。

在手線離線的方案中，我們採用的電子錢幣機制也有匿名性的功能，所以就像使用現金一樣，對商家及電信業者而言是具有匿名性的，不會透露任何使用者資訊給商家。

表 3. 輸入按鍵數比.

	須輸入PIN碼	不須輸入PIN碼
方案一 Dial out	5	1
方案二 Dial in	12	8
方案三	4	0
信用卡	20	20

8.4 通用性

目前很多付款機制的通用性都不足，現金只適用於實體商店，Paypal 只能使用於虛擬商店，信用卡、Paybox 及 GiSMo 不適用於小額交易(因成本高)、智慧卡不適用於高額交易。而我們設計的交易系統不僅適用於實體店購物、在虛擬商店也同樣行得通，不僅如此，小額及高額的交易。

8.5 交易時間統計

我們交易時間的計算方式以收銀員告知金額到遞出發票之時距

現金交易所需時間主要花在顧客掏現金、收銀員驗鈔、及找錢

信用卡交易時所花的時間從顧客掏出信用卡、刷卡、等銀行反

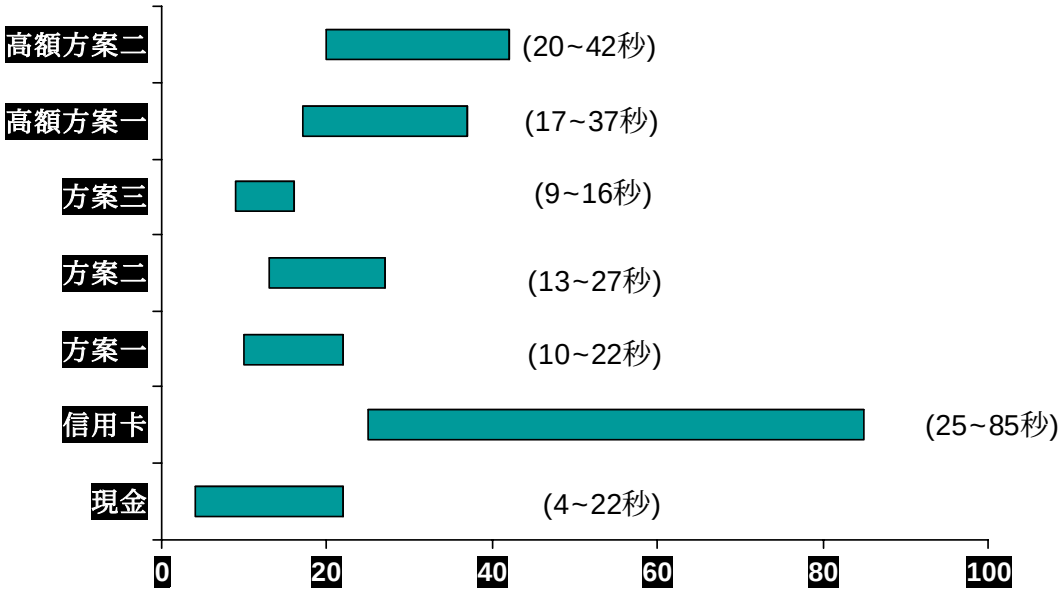


圖 18.交易時間比較

應、顧客簽名及最後的收銀員比對簽名，這中間花最多時間的在等待銀行反應的時間。大家如果有在屈臣士刷卡付款的話就會很有感觸，在一旁等候刷卡機的反應時，以現金付款的人早已結帳好幾人了。

由圖 18 可以看到，信用卡所花的時間非常的長，而我們提出的手機付款方式在小額交易時並不會比現金交易慢太多。Dial-out 的方案由電信業者直接撥給使用者，所以會比 Dial-in 的方案快上兩秒至五秒，因使用 Dial-in 方式使用者必須多花時間在撥號碼。而高額交易時會比小額交易多花約 7-15 秒的時間，因為多加入了口述交易序號及從銀行轉帳的部份。

表 4.付款機制綜合比較

	我們的系統	信用卡	現金	智慧卡
安全性	安全	遭冒用 風險高	偽鈔 易遭侵占	遺失損失大 商店溢刷
交易速度	快	非常慢	快	極快
使用者隱私	○	×	○	○
即時轉帳	○	×	△	△
高額交易	○	○	○	△
通用性	○	○	△	△
交易成本	低	高	最低	低

8.6 各種付款方式比較

綜合表 4 表 5 的比較後，我們可以看的出來，我們設計的系統，安全性則是各付款機制中最為完善的，即使在失竊冒用的情況下，受到的損失也不大，因此所需承擔的冒用風險相對較低。在其他方面例如交易成本、通用性、交易速度也都為翹中之楚。

再者，在使用者適應方面，因為交易的過程需要撥打或接聽電話，因此可能需要使用者熟悉手機的操作，但這對現代國人來

表 5.付款機制綜合比較二

	我們的系統	PayBox	GiSMo	PayPal
安全性	◎	○	△	△
交易速度	快	快	快	非常慢
使用者隱私	○	○	○	○
即時轉帳	○	○	○	△
高額交易	○	○	○	○
小額交易	○	×	×	×
通用性	○	△	△	△
交易成本	低	高	高	高

說已不成問題，因行動電話的普及率非常高，因此會操作並不是問題，因而在實際交易的情況中，若使用者能有效率的將交易分成幾個步驟進行，即可快速完成交易，比現金也不遑多讓。

在網路購物愈來愈盛行的現代，因為網路購物的風險更大，因此提供一個雙方都信任的交易媒介，並且能降低彼此的風險，讓我們能在安全的環境中方便、快速的完成交易。我們提供的交易系統能具備如此多的優點，相信在未來行動商務的推廣將是一大助力。

第九章 未來目標

網路購物實作

這次期中實作的版本只是個雛型，很多功能尚未完善，希望在期末時能完成一個功能較完善的版本

行動商販實作

在 Mobile POS 中的行動商販尚未實作，期末可能會採用『手機 + WAP』的方案完成行動商販的實作。

較大金額與銀行配合

目前所提出的方案仍只適用於比較小額的付款，因為若是開放大額付款，電信業者就必須要負擔隨之而來的呆帳風險，如果不能提高可使用的額度將會降低此付款機制的通用性及可行性，因銀行處理呆帳的能力比電信業者好多，所以將在期末提出一個與銀行合作的方案，將大額的收付款轉給銀行，而電信業者只負責收取中間的手續費，用手機付款的款項將列在銀行帳單而不是現今的手機通信帳單上。

安全性分析

期中報告的重點著重在實作的部份，但此架構的安全性分析將會在期末時提出。

可行性分析

期中報告中尚未對可行性的部份做出評估與分析，在期末會與其他的付款方式做比較詳細的評估及分析。

第九章 結論

在科技發達的現代，我們可預見使用者對交易的多樣化的需求會與日俱增，因此提供使用者更多樣且方便的付款方式便是取得先機的立基。

在本研究報告中，我們完成高安全度行動付款協定之設計規劃與雛型實作。我們的系統不僅可以使用在實體商店與網際網路虛擬商店，更能夠在行動商務上使用。

我們提出的方案，可以讓使用者在不需要更新手邊的現有的設備（比如手機）就可進行更方便的付款方式，使得使用者使用的意願增加，這也正是我們提出此方案的所著眼的目標。

而在使用者的參與部份，我們將強化系統的安全性，並儘量減少使用者對新交易流程的疑慮，並同時簡化流程，讓使用者能安心快速的進行交易。

經過我們的實作後，系統已能依我們所規畫的目標運作，並且再進一步擴大使用者的參與，讓更多的人來試用我們的系統，以進行下一階段的改進。

在未來的時間裡，我們期望能使系統的穩定性更好、使用者的便利性更佳、還有更多的使用者經驗回饋，以符合正式上線的需求。

參考文獻

[1] N. Borenstein, “Vulnerability of Software Based Credit Card Encryption,” At http://fv.com/ccdanger/index.html; see also San Jose Mercury News, 29 January 1996, “Program shows ease of stealing credit information” by Simpson L.Garfinkel.

[2] S. Brands, “Untraceable Off-Line Cash in Wallets with Observers,” Lecture Notes in Computer Science 773, Advances in Cryptology: Proc. Crypto '93, Springer, pp. 302 –318, 1994.

[3] R. Atkinson, “Security Architecture for the Internet Protocol,” RFC 1825, NavalResearch Laboratory, 1995.

[4] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G.Tsudik, and M. Waidner, “iKP – A Family of Secure Electronic Payment Protocols,” Extended Abstract, USENIX Workshop on Electronic Commerce. July11-12, 1995.

[5] Paypal. X.com, available at http://www.paypal.com.

[6] R. Braden, D. Clark, S. Crocker and C. Huitema, “Security in the Internet Architecture,” RFC 1636, 1994.

[7] Brokat. X-Pay, available at http://www.brokat.com.

[8] D. Chaum, A. Fiat, and N. Naor, “Untraceable electronic cash,” LNCS 403, Proceedings Crypto '88, pp. 319-327, 1988.

[9] C. I. Fan, and C. L. Lei, “User Efficient Blind Signatures,” IEE Electronics Letters, Vol. 34, No. 6, pp. 544-546, 1998.

[10] C. I. Fan, and C. L. Lei, “Low-Computation Blind Signature Schemes Based on Quadratic Residues,” IEE Electronics Letters, Vol. 32, No. 17, pp. 1569-1570, 1996.

[11] C. I. Fan, and C. L. Lei, “An Efficient Blind Signature Scheme Based on Quadratic Residues,” IEE Electronics Letters, Vol. 32, No. 9, pp. 814-816, 1996.

[12] C. I. Fan and C. L. Lei, “Efficient Fair Blind Signatures for

Electronic Cash," Proceedings of National Computer Symposium 1997, Vol. 2, pp. C-89-C-94, 1997.

[13]C. I. Fan, and C. L. Lei, "On the Analysis of Public-Key Cryptosystems," Proceedings of the 6th Conference on Information Security, pp. 228-235, 1996.

[14]C. I. Fan, C. L. Lei, C. Y. Chang, and P. L. Yu, "An Efficient Divisible Blind 215-Signature Scheme," Proceedings of the 8th Conference on Information Security, pp. 224, 1998.

[15]W. S. Juang, and C. L. Lei, "Fair Blind Threshold Signatures Based on Discrete Logarithm," Proceedings of National Computer Symposium 1997, Vol. 2, pp. C-95-C-100, 1997.

[16]W. S. Juang, and C. L. Lei, "Blind Threshold Signatures Based on Discrete Notes Logarithm," Proceedings of the 2nd Asian Computing Science Conference, Lecture in Computer Science 1179, Springer-Verlag, pp. 172-181, 1996.

[17]C. L. Lei, C. Y. Chang, and W. S. Juang, "A Java Security Model Based on and Information Flow Control," Proceedings of International Conference on Cryptology Information Security, pp. 176-183, Kaohsung, 1996.

[18]C. L. Lei, and C. I. Fan, "Low Computation Partially Blind Signatures for 101-C-Electronic Cash," Proceedings of National Computer Symposium 1997, Vol. 2, pp. C-106, 1997.

[19]C. L. Lei, and W. S. Juang, "Provably Secure Blind Threshold Signatures Based on Discrete Logarithm," Proceedings of 1999 National Computer Symposium, pp. C198-C205, 1999.

[20]C. L. Lei, W. S. Juang, and C. I. Fan, "Anonymous Channel and Conference Authentication in Wireless Communication," Proceedings of International on Networking and Multimedia, pp. 227-234, Kaohsung, 1996.

[21]B. Cox. "Maintaining Privacy in Electronic Transactions," Information Networking Institute Technical Report TR 1994—8,

Fall 1994.

[22]B. Cox, J. D. Tygar, and Marvin Sirbu, “NetBill Security and Transaction Protocol,” Proceedings of the First USENIX Workshop in Electronic Commerce, pp. 77~88, 1995.

[23]D. W. Davies and W. L. Price, “Security for Computer Networks, an Introduction to Data Security in Teleporcessing and Electronic Funds Transfer,” 2nd Edition. Wiley, 1989.

[24]S. Fischmeister, G. Hagleitner, W. Pree. “Hermes--A Lean M-commerce Software Platform Utilizing Electronic Signatures,” Proceedings of 35th Annual Hawaii International Conference on System Sciences (HICSS'02)-Volume 9 January 07-10, 2002

[25]H. Gobioff, S. Smith, J. D. Tygar and B. Yee, “Smartcards in Hostile Commerce, Environments,” Proceedings of the Second lJSENlX Workshop on Electronic November 1996.

[26]E. B. Hickman and T. Elgamal, “The SSL Protocol,” Internet Draft. June 1995.

[27]R. Housley, W. Ford, W. Polk and D. Solo, “Internet Public Key Infrastructure, X.509 Certificate and CRL Profile,” RFC [tbd], 1997.

[28]G. Jennifer, B. Steiner, C. Neuman and J. I. Schiller, “Kerberos: An Authentication Service for Open Network Systems,” USENIX Winter Conference, pp. 191-202, February 1988.

[29]P. Loshin, “Electronic Commerce – On-Line Ordering and Digital Money,” Charles River Media, Inc. 1995.

[30]D. C. Lynch and L. Lundquist, “Digital Money – The New Era of Internet Commerce,” John Wiley & Sons, Inc, p. 96, 1996.

[31]K. Maddox, M. Wagner, and C. Wilder, “Making Money on the Web,” Information Week, pp. 31-40, 1995.

[32]General Magic. Telescript Technology, “The Foundation for the Electronic.Marketplace,” Technical report, General Magic, 1996. http://www.Genmagic.Com/Telescript/Whitepapers/wpl/whitepaper

-1.html

[33]Mastercard International and Visa International, “Secure Electronic Transaction (SET) Specification,” June 1996, http://www.visa.com or http://www.mastercard.com.

[34]Mastercard International and Visa International, “Business Description.Draft for Public comment,” Secure Electronic Transaction (SET) Specification, Book1, February 23, 1996.

[35]P. Neumann, “Risks in Digital Commerce,” Communications of the ACM. January 1996.

[36]P. Panurach, “Money in Electronic Commerce: Digital Cash, Electronic Fund Transfer, and Ecash,” Communications of the ACM, pp. 45-50, 1996.

[37]Paybox. Die paybox-Gruppe strukturiert um, available at http://www.paybox.de.

[38]R. Rivest, A. Shamir, and I. Adleman, “A Method for Obtaining Digital No. 2, pp 42. Signatures and Public-Key Cryptosystems,” Communications of the ACM, Vol. 21, 120-126, 1978.

[39]M. Sirbu and J. D. Tygar. “NetBill: an Internet Commerce System Optimized for Network Delivered Services,” IEEE Personal Communications, pp. 34-39, August 1995.

[40]The WAP Forum, “Wireless Application Protocol Architecture Specification,” available at http://www1.wapforum.org /tech/documents/ WAP-210-WAPArch-20010712-a.pdf

[41]The WAP Forum, “Wireless Transport Layer Security Specification,” available at http://www1.wapforum.org /tech/terms.asp?doc= WAP-261-WTLS-20010406-a.pdf

[42]J. D. Tygar. “Atomicity in Electronic Commerce,” the 21st ACM Principles of Distributed Computation, 1996.

[43]SANS Institute, “The GSM Standard (An overview of its security),” available at http://www.sans.org/rr/papers/58/317.pdf

[44]B. Yee and J. D. Tygar, “Secure Coprocessors in Electronic

Commerce Applications," Proceedings of the First USENIX Workshop on Electronic Commerce, pp. 155-170, July 1995.

[45]D. Abrazhevich, "Classification and Characteristics of Electronic Payment Systems," EC-Web 2001, Lecture Notes in Computer Science 2115, pp. 81-90, 2001.

[46]H. Yamamoto, T. Kobayashi, M. Morita, and R. Yamada, "Public-Key-Based High-Speed Payment (Electronic Money) System Using Contact-Less Smart Cards," E-smart 2001, Lecture Notes in Computer Science 2140, pp. 242-254, 2001.

[47]GiSMo,"Millicom International Celluar Sa Announce Secure Internet Shopping with Your Mobile Phone", available at http://www.mobic.com/oldnews/9911/millicom_international_cellular_.htm