東海大學資訊管理研究所

碩士學位論文

適用於 LTE 上 NFC 行動支付認證協定之研究

A Study of NFC Mobile Payment Authentication Protocol on LTE

指導教授：余心淳 博士

研究生：李嘉慈 撰

中華民國 104 年 7 月

致謝

不知不覺兩年的時間就過了，在這求學之路中我經歷了許多讓我覺得困難的事，但回想起這兩年實在是覺得充實且值得。

首先要感謝指導教授余心淳老師，本論文的研究工作是在余心淳老師的悉心指導下完成，從論文的選題、研究計畫的制訂，各個方面都離不開余心淳老師熱情耐心的幫助和指導，這兩年的學習，不僅使我的研究視野上了一個新臺階，更重要的是，在各方面我的能力均得到了提升，至此論文順利完成之際，我要向我尊敬的指導教授余心淳老師表達深深的敬意和無以言表的感謝。

在本論文審查期間，承蒙林正偉教授與李俊達教授在百忙之際出席筆者的論文口試，給予本論文寶貴的意見與建議，使得本論文可以更趨完整與充實，甚為感謝。

感謝本系的助教黃正炎博士，他對我來說亦師亦友，在論文的研究上給了我許多建議與鼓勵，而每次到系辦找他聊聊天總能讓我心情好起來。感謝我從大學以來一路相伴的摯友徐照芸與張怡凡，與他們在一起的日子總是開心且放鬆，並且在論文遇到瓶頸時感謝他們願意聽我抒發壓力，並且伴我一同努力。感謝朋友張智傑在我做研究期間對我十分照顧，謝謝他總是在我忙得不可開交的時候體貼我，並且總是我讓我有動力繼續努力下去。接著我要感謝並祝福所有研究室的同學們，一同在研究室奮鬥的日子令我難以忘懷，他們讓研究室就像個溫暖的大家庭。

最後要感謝我親愛的父母與家人，感謝他們在我求學期間一直以來對我的支持，讓我能心無旁騖的完成學業。

李嘉慈 謹誌

一百零四年七月

摘要

隨著全世界行動支付的標準愈來愈成熟，加上支援 NFC 功能的智慧型手機日益普及，帶動了相關市場與應用平臺的開發，讓行動支付服務邁出商用的步伐並開拓無限商機。無論行動支付發展如何多樣化，交易安全仍為行動支付模式成敗最重要關鍵，因此本論文提出一個適用在 LTE 行動通訊網路上，可支援電信業者代收付款模式下提供行動支付交易服務的安全認證機制。有別於以往的研究成果，本論文所提出的方案可解決消費者在 LTE 網路上，藉由 NFC 行動設備和行動應用軟體 App 與商家的電信業者代收付款的兩種銷售終端平臺，分別使用在傳統實體店家銷售點終端(POS)設備平臺與新興的行動收單終端(mPOS)設備平臺上進行安全的行動支付交易。兩者皆為使用 LTE 網路內部的認證與密鑰協商協議(AKA)進行認證，並融入橢圓曲線密碼系統使系統具安全性，另外我們改善了在 GSM 與 3G 行動通訊網路上相關認證機制的參數處理、系統效能與安全性等問題，減少交易過程中失敗的機率，讓使用 NFC 行動設備的顧客能透過無論是現今多數商家所使用傳統的 POS 或者新興的 mPOS 終端設備，均可進行快速安全的行動支付交易，給消費者享有更高的保障與更好的消費體驗。

關鍵字： 長期演進技術、行動支付、進場通訊、認證與密鑰協商協議、銷售點終端、行動銷售點終端、橢圓曲線密碼系統

Abstract

As mobile payment technology matures, and NFC-enabled smart phones becoming more popular, both of which drive the development of relevant market and application platforms, mobile payment service is becoming more acceptable in commercial use, while bringing in unlimited business opportunities. No matter how diversified mobile payment development is, transaction security is still the most important key to success for the mobile payment model. Hence, this thesis proposes a secure authentication mechanism that, is compatible with the LTE mobile telecommunication network, and provides mobile payment transaction service while supporting the direct carrier/operator billing model and mobile payment service. Unlike previous research, the scheme proposed in this study can resolve the issues derived from using NFC mobile devices, mobile Apps, and the two different payment collection platforms used by telecommunication operators on the merchant side: point of sale (POS) device platform used by conventional stores, and the emerging mobile point of sale (mPOS) device platform, and provide consumers with a secure environment for making mobile payment transactions on LTE networks. Both platforms are authenticated by the internal authentication system of the LTE network and Authentication and Key Agreement (AKA). Elliptic Curve Cryptography (ECC) is also integrated to make the transaction system even more secure. In addition, further improvements made on issues concerning parameter processing, system functions, and security of the relevant authentication mechanism on GSM and 3G mobile communications networks, is reducing the probability of failure in the transaction process. These improvements enable customers using NFC mobile devices to have a fast-and-secure mobile payment transaction, whether they are using the conventional POS adopted by a majority of merchants, or using the emerging mPOS, giving consumers better protection and experience.

Keywords : LTE, Mobile Payment, NFC, Authentication and Key Agreement, Point of Sale, Mobile Point of Sale, Elliptic Curve Cryptography

目次

致謝 II

摘要 III

英文摘要 IV

目次 V

圖次 VII

表次 VIII

第一章　緒論 1

　第一節　研究背景 1

　第二節　研究動機與目的 3

　第三節　研究範圍 5

第二章　文獻探討 6

　第一節　NFC 近場通訊技術 6

　第二節　行動支付 8

　第三節　POS 與 mPOS 12

　第四節　LTE 14

　第五節　橢圓曲線密碼系統 20

第三章　NFC-LTE 行動裝置在 POS 上的安全認證機制 25

　第一節　系統架構與前置設定 25

　第二節　在 LTE 架構中的行動支付與認證流程 26

　第三節　安全情境分析 31

　第四節　系統架構優缺點 33

　第五節　結論 34

第四章　NFC-LTE 行動裝置在 mPOS 上的安全認證機制 35

　第一節　系統架構與前置設定 35

　第二節　在 LTE 架構中的行動支付與認證流程 36

　第三節　安全情境分析 41

第四節　系統架構優缺點 43
第五節　總結 44
第五章　結論 46
第一節　研究回顧 46
第二節　研究貢獻 47
第三節　未來研究方向與展望 48
參考文獻 49
附錄一　字彙表 52

圖次

圖 2-1　資料交換方式……6
圖 2-2　NFC 行動裝置……11
圖 2-3　POS 系統架構……12
圖 2-4　mPOS 使用耳機孔連接讀卡機及其系統架構……14
圖 2-5　LTE 網路架構圖……16
圖 2-6　LTE 行動裝置認證流程……17
圖 2-7　LTE 密鑰層級……18
圖 2-8　換手密鑰產生與管理……19
圖 2-9　橢圓曲線E：$y^2 = x^3 - 2x + 3$……20
圖 2-10　橢圓曲線E：$y^2 = x^3 - 5x + 1$……20
圖 2-11　橢圓曲線的加法(a)……22
圖 2-12　橢圓曲線的加法(b)……22
圖 2-13　橢圓曲線的加法(c)……22
圖 2-14　橢圓曲線的加法(d)……22
圖 2-15　橢圓曲線加解密……23
圖 3-1　LTE 系統上整合 POS 的系統架構……26
圖 3-2　NFC-LTE 在使用 POS 環境下的 DCB 行動支付流程圖……27
圖 4-1　LTE 系統上整合 mPOS 的系統架構……36
圖 4-2　NFC-LTE 在使用 mPOS 環境下的 DCB 行動支付流程圖……37

表次

表 2-1　POS 與 mPOS 的相關特性比較表……14

表 2-2　RSA 與橢圓曲線密碼系統在相同安全度下金鑰長度之比較……..24

第一章　緒論

第一節　研究背景

由於近年來行動商務(Mobile Commerce)的快速發展與普及化，人們逐漸習慣使用行動商務所提供的各種服務，悠遊卡、信用卡與手機小額付款等應用廣泛的為社會大眾所接受。行動商務使消費者不需攜帶大量現金，均可隨時隨地皆可完成商務與金融交易，並且在無紙化的前提下將每一筆交易都保存了完整的電子交易紀錄，提供消費者日後在網路上查詢，相較於過去使用紙本發票容易遺失或毀損，行動商務給予消費者更高的保障。

為了強化行動商務的優勢與特性，許多產業商機相應而生，行動商務搭配各種創新技術已蔚為風潮，如無線高頻辨識近場通訊(Near Field Communication, NFC)與 QR Code 付款等在近年開始流行，其中又以搭配 NFC 技術的各項創新應用最為受各方關注，因其在行動支付相關的處理流程中有較佳的效率與發展前景。NFC 是且 Nokia、Philips(現改為恩智浦半導體)與 Sony 等三家公司共同研製開發，是基於無線射頻辨識技術(Radio Frequency Identification, RFID)上所發展出來的非接觸式近距離無線通訊技術，並由這三家公司於 2004 年成立了 NFC 論壇(NFC Forum)[1]的組織，提供了 NFC 技術架構、協定規範以及應用趨勢討論的空間，並推動其各項標準與應用服務，進一步促成了 NFC 的推廣和發展。由於 NFC 使用便利且具較高的保密性與安全性[2]，除了一般如門禁卡、會員卡、員工證或學生證等辨識功能的應用之外，也發展出許多在商業活動與金融交易整合的服務應用，例如在信用卡方面，Visa 與 MasterCard 分別推出的 payWave 與 PayPass 行動感應技術；在電子錢包方面，使用 NFC 功能的智慧型手機來提供手機電子錢包之悠遊電信卡與手機信用卡服務，如蘋果的 Apple Pay、Hami 智慧錢包與悠遊卡付款等。

且 NFC 的許多優點例如使用上便利、傳輸速度快、安全性高並且可與卡片讀取機硬體相容，使得具有 NFC 功能的智慧型手機與配件越來越普遍，不僅轉換現

有行動裝置使用者動態體驗，更催生出許多嶄新的互動方式，儼然已成為創新科技應用的一大趨勢。

NFC 的安全性與便利性，也加速推動行動商務在滿足流通零售連鎖業對整合銷售、金流、庫存與顧客資訊與管理的需求。其中已普遍可見在零售業、餐飲業、旅館與大眾運輸等行業將NFC與銷售點終端 (Point of Sale, POS) 資訊系統做連結，在生活中已經是相當普遍的一件事，只要走入便利商店，即可使用 NFC 悠遊卡進行線上付款交易，提供顧客及店家方便快速的即時交易模式。POS 系統亦能彙整資料進而與後端的企業資源規劃(Enterprise Resource Planning, ERP)與支援決策系統(Decision Support System, DSS)結合，以提供經營者做為決策的參考。

但一般 POS 畢竟是實體機台，仍舊受其不可移動性的影響，因此行動收單銷售終端 (mobile Point of Sale, mPOS)資訊系統因應而生，mPOS 藉由輕巧的讀卡機與智慧型手機、平板電腦等行動設備結合來完成非現金型式的收單、刷卡與結帳等作業；不僅攜帶輕便，不受實體環境的限制，更可提供無線傳輸特性的行動交易服務，以及無紙化的電子收據處理，其商業服務應用領域的多樣性又比傳統的 POS 系統更上一層樓，並且對於店家來說可降低建置成本，以及藉由提升顧客體驗來提高交易成功的機會，對於小型流動性店家有很大的吸引力。

隨著智慧型手機與行動智慧軟體App的崛起與廣泛使用，與行動商務結合行動支付(Mobile Payment)概念的實現，悄悄改變使用者之消費行為與支付習慣。行動支付係指以個人手持行動通訊設備進行轉帳、繳付帳單、線上購物等商業金流交易活動。行動支付是行動商務的技術核心，行動支付市場的興起，不僅在行動商務平臺上成功的整合商業活動、商品流與金流，提供給使用者完整的便利消費交易體驗；更將傳統電子商務中透過桌上型電腦的網路交易活動轉變成行動商務中透過個人手持行動設備在行動通訊網路上來完成商業交易行為，創造了廣大的商機。而近年來幾乎所有關於行動支付的創新，都是在想盡辦法要將「以卡片為基礎」的支付行為複製到「行動設備」上，再加上手機製造商、電信業者、銀行業

者等產業鏈的合作日益密切，無論在選擇使用POS或mPOS的環境下，如何將配有NFC功能的智慧型手機或平板電腦整合於行動支付相關的應用上，已成為現階段最熱門的產業發展與研究議題[3]。

第二節　研究動機與目的

本論文的主要研究目的是探討配備了NFC功能的智慧型手機在長期演進技術(Long Term Evolution, LTE)行動通訊網路中，如何結合電信業者代收付款(Direct Carrier/Operator Billing, DCB)的行動支付服務模式，並解決其在系統傳輸與交易上相關的安全協定議題。

LTE 行動通訊系統又稱 3.9G，是現階段由 3G 行動通訊網路升級到 4G 之前的一個過渡系統版本，相較於以往 2G 或 3G 行動通訊具有更高的頻寬供應與安全性。且 LTE 手機有更大的比例內建了 NFC 功能，各大手機製造商如 Nokia、Sony、LG、Samsung、HTC 等等在 2004 年起開始紛紛推出 NFC 手機，而在 2010 年後各大廠牌所推出之新型高階智慧型手機款式已幾乎具備 NFC 功能，並且一直未加入 NFC 功能的 Apple 在 2014 年也推出支援 NFC 功能的 iPhone 6 手機，在 NFC 漸漸普及的現在，可以說新推出的每一支 LTE 手機幾乎都具備有 NFC 功能，並且除了手機之外，具有 NFC 功能的 LTE 行動裝置產品如智慧手錶及平板也逐漸被推出。

本研究主題中的電信業者代收付款 DCB 為行動支付的應用模式之一，是由行動網路業者(Mobile Network Operator, MNO) 所提供的行動支付服務且大部份應用在小額支付系統(Micropayment Scheme)上。此種付款方式為消費者(亦為 MNO 的用戶)購買商品後，由電信業者先行付款而後以電信帳單的繳費模式來讓其完成付款交易，適合兒童、老人或其他等較不習慣或較不適合使用信用卡的用戶。電信業者代收付款市場的成長，在於行動通訊網路、智慧型手機、App、NFC、POS 與 mPOS 等相關技術的成熟、穩定與安全，並且手機用戶的數量遠遠超過信用卡的持有者，尤其對於信用卡尚未普及的國家有更高的吸引力，而對於信用卡已普及的

國家而言，將增加一種付款方式，讓不習慣使用信用卡或未擁有信用卡帳戶的用戶如老人及兒童也可以方便的進行交易，為電信業者在行動商務上創造出豐碩的商業契機。

由於行動支付的方便快速且生活化，部分學者已提出一些在 GSM 與 3G 系統上行動支付相關的安全認證機制[4][5][6]，但現今常用的行動支付仍然擁有許多尚未解決的安全性問題，尤其是與先進的行動網路，如 LTE、LTE-A 或 WiMAX 等，在整合與安全機制設計上的議題；另外在小額付款的部分則有許多盜用資料或者詐騙安全性與其架構問題[7][8][9]，至今尚無完整的解決方案。本論文中我們將針對在 LTE 網路上分別使用固定式 POS 與可移動式 mPOS 銷售點終端設備這二種在系統架構與資料流運作相異的環境下，進行行動支付在安全交易認證的研究討論。

在透過傳統固定式 POS 與 NFC-LTE 個人行動手持裝置進行行動支付方面，由於 POS 在目前實體店面的使用上擁有相當高的市占率，因此在 LTE 網路上透過 NFC 裝置與 POS 上進行行動交易將會是個趨勢，而規劃一套完整的安全交易機制仍是必須的，至今少有在 2G/3G 行動網路上使用 NFC 技術與實體店面 POS 進行安全認證交易的相關研究成果[10][11][12][13]，但尚未有針對 LTE 系統上的 NFC 手機在 DCB 行動支付上安全性相關議題的研究論文發表。因此本論文決定針對此議題做探討，我們改善了 Chen[10]等人在 3G 上所提出的 DCB 安全交易認證機制，並利用現行 LTE 行動通訊的安全架構擬定了一個更加完善的 NFC 行動支付的安全交易機制。

而利用可移動式的行動收單銷售終端 mPOS 與 NFC-LTE 個人行動裝置進行行動支付方面，相較於傳統的 POS，mPOS 具有更高的靈活性與市場價值，並且對於店家來說更可大幅的降低成本，因此使用 mPOS 在未來想必將會是個趨勢，如今一般市面上的 mPOS 為透過智慧型手機或平板以藍芽或耳機孔連接刷卡機而成，並再透過 Wi-Fi 連結商家固網以達到 mPOS 的移動性，而現今 NFC 技術已純熟，

且 LTE 網路相較於以往 2G/3G 行動通訊網路更加的穩定、快速且安全，並且已於近年來漸漸普及,因此我們提出的安全交易認證機制將 mPOS 與 NFC-LTE 做結合，讓顧客能夠更安全且快速的在任何移動的場景中進行交易，無論是火車、巴士或高速鐵路等等交通工具上，或是應用在夜市、流動市場等中小型商業活動的商圈環境中。

第三節　研究範圍

在本論文提出的安全認證機制研究方法中，我們假設的線上付款交易機制皆利用行動裝置與 POS 或 mPOS 之間的 NFC 晶片進行資料傳輸活動,並利用橢圓曲線密碼學進行機密資料的加密以進行交易，並且透過 LTE 行動電信業者端以 DCB 電信業者代收付款行動支付方式完成交易，在 POS 及 mPOS 兩種平台上的交易機制中，我們皆借用了現行 LTE 在系統與使用者手機端原本的安全架構，期望能使得無論在 POS 或者 mPOS 上的行動支付服務能夠更具有安全性。

本論文共分為五個章節，第一章為緒論，描述了本論文的研究背景，並且提出進行研究的動機、目的與欲解決的問題。第二章為文獻探討，探討本論文研究主題上所需配合的相關技術、標準及理論基礎。第三章一開始先介紹其他學者在行動網路上 NFC 行動支付的相關研究成果，再進一步探討行動電信業者與商家在 LTE 網路上實現 DCB 電信業者代收付款所需的安全認證議題，並設計可供消費者手持 NFC 個人行動裝置透過在商家端的傳統 POS 進行在 LTE 行動網路上與 DCB 認證的安全交易機制，並探討其安全性分析及優缺點。第四章則是探討與電信業者合作進行電信業者代收付款，並透過具有移動能力的 mPOS 結合 NFC 技術與行動裝置在 LTE 行動網路上與 DCB 認證的安全交易機制,並進行其安全性分析與優缺點的比較。第五章為結論，將進行文獻回顧及將本研究所提出的兩個交易機制做比較，探討所提出之機制對本論文研究主題上的貢獻，以及在未來可適用的電子商務應用範圍，並對未來安全機制上的改善空間與研究方向提出具體意見。

第二章　文獻探討

本章將針對此研究的核心技術進行回顧與討論，包括 NFC 進場通訊技術、行動支付一般常見的模式、銷售點終端(POS)與移動式銷售點終端(mPOS)的介紹、LTE 安全架構以及橢圓曲線加密法,探討本論文研究主題上所需配合的相關技術、標準及理論基礎。

第一節　NFC 近場通訊技術

NFC 為 Near Field Communication 近場無線通訊縮寫，是一種以 RFID 為基礎的近距離通訊技術，其原理是使用晶片結合感應讀卡器與感應式卡片，利用點對點功能，在 20 公分距離內以 13.56MHz 頻率範圍運作，NFC 定義於 ISO/IEC 18092[14]與 ISO/IEC 21481 中,並且可相容於 ISO/IEC 14443[15]、ISO/IEC 15693[16]與 FeliCa[17]，是一個兼具 Type A、Type B 與 FeliCa 通訊與感知規格的短距無線通訊協定，透過 NFC 使用者只需要一個碰觸的動作就可以傳送或接收資料，機器間配對時間極短，使用方式簡便快速且應用層面廣，並且擁有低耗電量與較低的建置成本的優點， NFC 的資訊交換方式如下圖 2-1，為利用兩個導電線圈的磁場耦合形成電磁場域來進行資料交換。

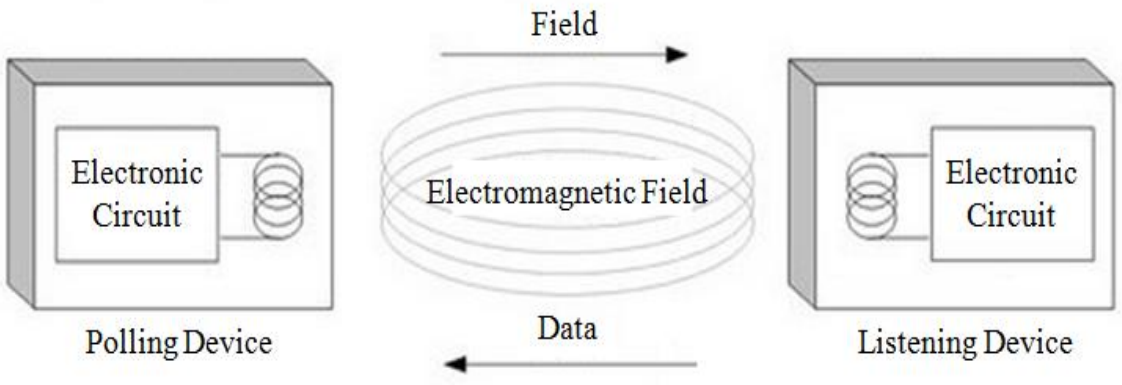


圖 2-1 資料交換方式

NFC 主要有三種使用模式[1]:

1. 卡片模擬（Card Emulation Mode）: 在此功能狀態下，NFC 晶片相當於一張 RFID 技術的 IC 卡，可作為信用卡與悠遊卡等用途。
2. 點對點模式（P2P Mode）: 用於資料傳輸與交換，機器間配對時間極短，可完成下載圖片、音樂及交換名片等功能。
3. 讀/寫模式（Reader/Writer Mode）: 在此模式中擁有 NFC 晶片的機器可將自身當作非接觸式讀卡機，可從電子標籤上讀取資訊。

而其中卡片模擬模式又可分為硬體上的卡片模擬(Virtual Card Mode)與軟體上的卡片模擬(Host Card Mode)，前者的 NFC 行動裝置安裝具有獨立記憶體與控制器之安全原件，再以安全介面存取安全原件中的應用程式與機密資料，後者則是讓應用程式以 CPU 作為虛擬卡片處理器，裝置即使無安全原件也可進行卡片模擬，以 2014 年 Google 所發表的 HCE 技術為主[18]。

以下為 NFC 技術與行動裝置做結合的基本應用實務：

1. 接觸通過(Touch and Go): 透過將儲存票證或門控密碼的行動設備靠近讀取器以完成辨識，多用於門禁管制、停車場管理、車票或門票等。
2. 接觸支付(Touch and Confirm): 使用者須將行動設備靠近同樣擁有 NFC 功能的 POS 機，直接付款或輸入密碼以完成交易，多用於移動支付。
3. 接觸連接(Touch and Connect): 將兩個擁有 NFC 功能的行動裝置互相靠近，以進行點對點的資料傳輸，常用於交換影像、圖片或同步，店家也可利用 NFC 行動裝置取代 POS 以提升交易效率。
4. 接觸瀏覽(Touch and Explore): 使用者可將行動裝置靠近擁有 NFC 功能的公用電話或海報以瀏覽訊息，或者藉由與另一設備接觸以瞭解該設備所能提供的功能與服務。
5. 接觸下載(Load and Touch): 一般為透過網路下載交易票券或折扣優惠，而後與店家透過該 NFC 訊息進行交易，或使用者可透過發送特定格式的短訊至他

人行動裝置，以利用其進行門禁控管。

第二節　行動支付

行動支付(Mobile Payment)的定義為消費者使用智慧型行動電話與行動智慧軟體 App 來進行線上金融交易付款機制，常見的應用諸如購買音樂、來電答鈴、遊戲或支付車票費用等等，而現今新興的行動支付與 POS 或 mPOS 機台結合，更包括各種實體商品的購物,如便利商店 NFC 付款、百貨公司或各種攤販的刷卡等等，行動支付約可分成幾下幾種以移動設備為付款工具的付費型態：

壹、簡訊付款(SMS based Transactional Payment)

為透過簡訊來進行付款的一種交易模式，曾經為最普遍被運用的一種行動服務，消費者可利用簡訊購買如新聞、氣像、財經等等資訊服務或購買遊戲內的商品，而付費方式則是與電信帳單合併付費，但由於 SMS 付款無法支援行動裝置進行上網付費購買音樂、影音等等商品，交易的簡訊費用須由消費者自行負擔，且交易完成時消費者所能保留的購買資訊有限，很難記住曾經購買的地點及方式以像朋友推薦購買等等因素，簡訊付款目前已漸漸式微。

貳、電信業者代收付款(Direct Carrier Billing)

又稱 Direct Operator Billing，此種交易方式由使用者的行動帳單進行付款，當交易成功後商家將直接由使用者所設定之行動帳戶中扣款，其好處在於，使用者不需要擁有信用卡或事先登記註冊，因為在擁有電話號碼的同時，個人資料已經被行動網路業者擁有，進行電信業者代收付款時不需再額外填寫，能帶給顧客更高的信賴度,且對於不習慣擁有信用卡的族群如老人及兒童來說使用上較無負擔，並且對於信用卡普及率較低的國家，將擁有更高的市場潛力。

如今包括 Google 以及 Microsoft 已經加入了這一塊市場,分別與電信業者合作,讓消費者可以使用電信業者代收付款購買購物商城內的各種應用服務與 APP 等等，

此種交易方法通常用來購買較小金額的商品，付款金額可以非常彈性，並且相較於使用信用卡交易，電信業者代收付款不需要輸入冗長的表格，可以迅速的完成交易。

歐洲著名市調公司 Juniper Research 公司表示[35]，在 2019 年透過電信業者代收付款的交易金額將達到 140 億美元，在他們的研究中發現在電信業者代收付款在 APP 購買上有明顯的增加，在某些狀況下超過信用卡支付的 30 倍，並且促成更高的交易平均金額、數量以及 APP 內的購買；而另一家同樣為歐洲著名的的市調公司 Analysys Mason 則預測，電信業者代收付款將在 2022 年為全球的電信業者帶來 120 億美元的收益[36]，並且在 2014 年的發表中提出對於行動支付的潛力分級[37]，利用手機普及率與銀行帳戶普及率將各國家分為四個使用行動支付的潛力等級，發現對於大多數的國家，行動支付應該將擁有高的吸引力(High Appeal)，因為其手機普及率均遠遠高於銀行帳普及率，舉例來說非洲肯尼亞的信用卡普及率僅有總人口的 3%，但其擁有智慧型手機的用戶卻有 43%，吸引了行動支付商 Fortumo 在 2015 年初進駐肯尼亞，讓肯尼亞人能透過電信業者代收付款在行動裝置上購物。

在台灣電信業者代收付款交易已盛行於五大電信業者包含中華電信、台灣大哥大、遠傳、亞太與台灣之星，在 2010 前普遍多應用於在手機內購買遊戲點數、購買手機 APP、購買手機來電答鈴或在網路購物中付款，顧客僅需輸入帳號密碼及身分證字號即可進行交易，並於月底繳交電信帳單時付款，而在 2010 年後則紛紛與 Google Play 進行合作，使得顧客可以直接使用電信業者代收付款在 Google Play 的商城內進行 APP 的購買。

在國外，電信業者代收付款也同樣盛行，如 Bango 於 2012 年與 Google Play 整合，與澳大利亞的電信公司 Telstra 合作，提供顧客電信業者代收付款的服務；Boku 為在美國、日本、德國、英國等著名的垂直停車場業者，在各國允許顧客使用電信業者代收付款的服務支付停車費用；2012 年努爾奇無線營運公司 Trukcell

與電信業者代收付款營運商 Onebip 合作，讓顧客透過電信業者代收付款的方式購買國家足球隊的國際賽事門票；2014 年行動支付商 Fortumo 宣布和新加坡電信 SingTel 的「直接付款協議」，此協議讓顧客能在 APP 中直接進行點及付款，支援的系統包含桌面應用程式、網路服務、HTML5、Android、 Windows Phone 和 Windows 8。

參、行動網頁付款 (Mobile Web Payment)

由於近年來行動裝置如智慧手機與平板的上網功能已和電腦無太大的差別，因此讓消費者可透過行動裝置瀏覽網頁購買商品就像在電腦上購買一樣自在，此種付款方式主要為透過行動裝置上網，在網頁中或者額外安裝的應用程式中進行付款，此種付款方式可搭配電信業者代收付款或信用卡付款，讓無論是習慣於電信業者代收付款或者信用卡付款消費者都可以在熟悉的網頁或付款環境進行交易，並且可輕鬆的將經常購買的網頁或應用程式推薦給他人，為近年來盛行的行動支付模式之一。

肆、無接觸式 NFC 付款(Contactless NFC)

NFC 付款為近年來十分受矚目的一種交易模式，此種付款方式為利用 NFC 感應式付款在實體商店消費的商業應用， 2011 年 Google 推出了以 NFC 行動裝置為基礎的行動支付電子錢包服務－“Google Wallet”，並與 Visa、MasterCard、Citibank 和 Sprint 等共同合作來擴大 NFC 行動裝置行動支付的版圖，且同年度美國 AT&T、T-Mobile 與 Verizon Wireless 共同成立 ISIS 聯盟一起推動 NFC 行動支付。

目前以 Visa 推出的 payWave 以及 MasterCard 的 PayPass 行動感應技術最為盛行，而此技術又分為 Trusted Service Manager (TSM)與 Host Card Emulation (HCE)兩個流派，在台灣由於 TSM 引入的時間較早，較多數業者採行此方案。

蘋果的 Apple Pay 也是屬於此種類型，但是 Apple Pay 更進一步導入了 Visa

Token 的服務，後者則是由 Google 於 2013 年底推出，在台灣也引起了多方面的關注。

NFC 付款為透過 NFC 行動裝置進行行動支付，此技術配合相關的軟體與硬體，將非接觸式 IC 卡、點對點(Peer to Peer)資料傳輸及 RFID 讀卡機功能整合在一支行動裝置中，其架構如下圖 2-2[19]，主要由 SIM 卡、記憶卡、應用程式、NFC 控制器(NFC Controller)所與天線所構成，透過電信業者將 NFC 相關的應用程式傳到 NFC 行動裝置持有者的裝置，並將現金卡與信用卡資料存於行動裝置中，即可將行動裝置當成電子錢包或信用卡，在有非接觸式電子交易讀卡機的消費場所中當成一張多功能用途的智慧卡使用，因其使用方便快速且具有高的安全性，並且 NFC 行動裝置在近年來漸漸普及，因此前景十分看好，有極大的可能成為一種新的主流消費模式。

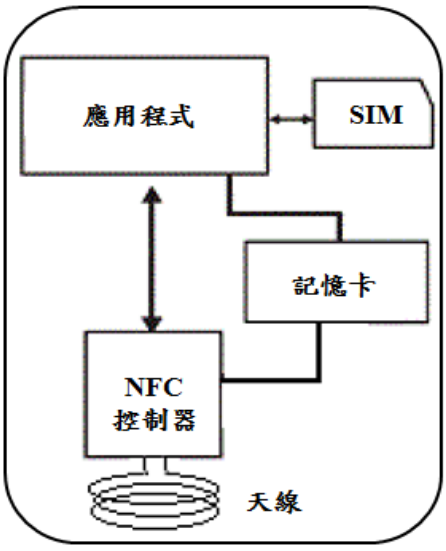


圖 2-2　NFC 行動裝置

第三節　POS 與 mPOS

壹、POS 系統

最早的 Point of Sale (POS)銷售點終端資訊系統發明於 1960 年代，當時的 POS 主要功能為利用條碼，讓店員能快速結帳並減少錯誤，接著 POS 開始與電腦結合，提供商家利用統計資料做各種分析，幫助商家能更有效率的瞭解顧客的消費傾向，如今 POS 系統不僅是擁有收銀機的功能，而是隨著時代的需求增加而衍生出更多功能，例如：旅館訂房資訊、圖書館資料查詢系統、餐飲業的點餐系統等等，一般的 POS 系統架構如圖 2-3 中所示。

如今 POS 系統的處理功能幾乎與一台電腦相當，並且可安裝 Windows 作業系統軟體與 POS 應用程式來運作，但 POS 系統不需做影像及文字處理，所以不需要強大的繪圖卡或高速的處理器，不過由於應用的環境可能在餐飲業等區域，所以需要有防水、防震等要功能，不同的商家為了因應不同的管理的方式也採用不同的 POS 裝置，如 PDA 或是其他特殊規格的掌上型裝置。

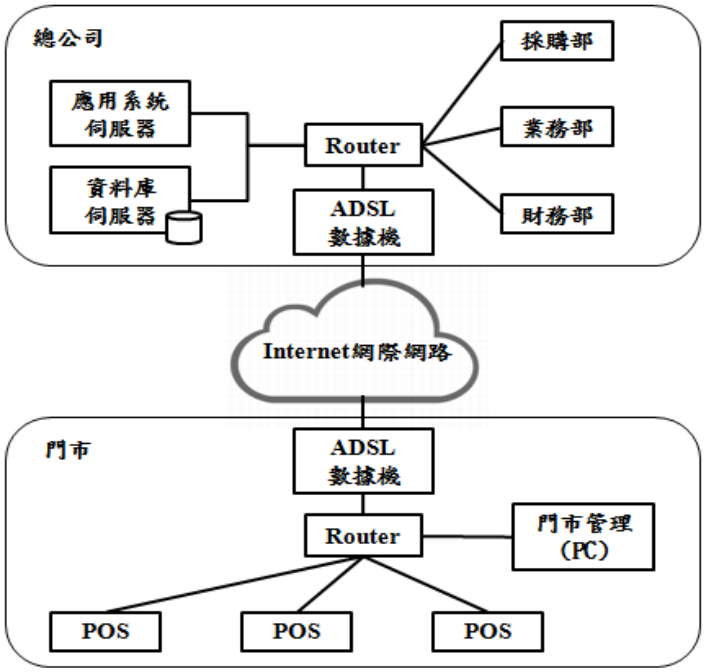


圖 2-3　POS 系統架構

當顧客結賬時，商家掃描商品條碼以提供收銀機商品資訊，透過此資訊收銀機可以計算交易金額，並且交給 POS 主機統計商品的銷售狀況，有些商家會要求顧客輸入個人資料，或結合信用卡、會員卡等等來管理顧客資訊，從而瞭解顧客的消費行為，而有些商家會將 POS 與網路連線以傳送交易資訊給後端企業總部，並且與電子訂貨系統、電子資料交換及電腦會計系統、電子訂貨系統等結合，提供業者各種商品的銷售及庫存狀況，並且分析不同顧客群的購買行為，從而讓業者更有效率的瞭解顧客的消費傾向、排除滯銷的商品，提供業者未來商品開發的參考，給業者帶來莫大的效益。

貳、mPOS 系統

Mobile POS (mPOS)約在 2000 年後興起，為可移動式的行動收單銷售終端資訊系統，它結合了行動載具、雲端技術及電子發票功能，相較於傳統 POS 有更加方便、快捷、節省空間與成本的優勢(表 2-1)。mPOS 相當適合於流動性高的營業場所如行動咖啡廳、流動攤商等，以及非固定可移動性的交易環境，如汽車、巴士、火車或高速鐵路等大眾運輸載具上，商家可用智慧手機或平板電腦利用耳機孔或藍芽連接外接刷卡機並安裝支付軟體，接著再運用無線網路資料傳輸，將行動裝置當作一台 mPOS 使用，如圖 2-4 中所示。

如今刷卡消費許多人的消費習慣之一，而相對的 POS 系統的應用也已非常普遍，隨著移動支付的普及，mPOS 也越來越普遍的被應用，已有許多廠商投入此塊市場的經營。中華電信提出了使用 mPOS 掃描顧客 QR code 以進行交易的行動支付方案，恩智浦在今年也提出將與台灣大車隊合作，利用 mPOS 移動性高的優勢，讓顧客在未來搭乘計程車時也可用悠遊卡或信用卡付款，國內大型系統整合公司淩群電腦也與中國信託的合作，在信用卡行動支付領域中推出「mPOS 行動收單系統」，就是期望在未來能達到無論在何時何地都能使用 mPOS 進行交易。

表 2-1　POS 與 mPOS 的相關特性比較表

特性比較項目	POS	mPOS
普及度	高	發展中
社會大眾接受程度	高	較低
移動性	低	高
可接受支付款方式	較多	較少
支援 NFC 付款	可	可
隨時隨地付款	較多限制	可
購置成本	較高	低

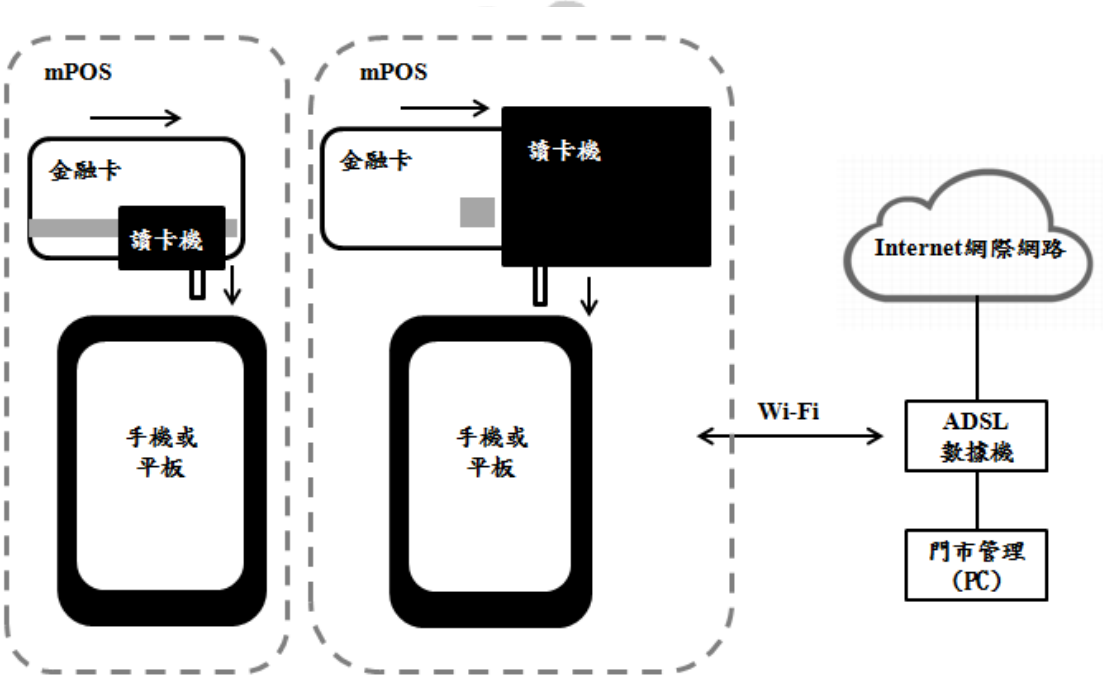


圖 2-4　mPOS 使用耳機孔連接讀卡機及其系統架構

第四節　LTE

為了應對不斷增加的行動數據及多媒體應用的需求，第三代合作夥伴計畫（3rd Generation Partnership Project, 3GPP）制訂了長期演進技術(Long Term Evolution, LTE)技術為下一代寬頻移動無線網路，LTE 的系統設計包含了較少的網路元素，

因而提高了系統的容量和覆蓋範圍，並提供高的數據傳輸速率與低存取遲緩，靈活的寬帶操作與現及和其他無線通信系統無縫的連結[34]。

壹、LTE 系統架構

LTE 的系統架構是由無線網路部份(Evolved-Universal Terrestrial Radio Access Network, E-UTRAN)與核心網路部份(Evolved Packet Core, EPC)所組成，E-UTRAN 包含了基地台(Evolved Node B, eNB)與家庭基站(Home eNode B, HeNB)來與使用者設備(User Equipment, UE)做溝通，而 EPC 是由 all-IP 與 Packet-switched 的骨幹網路所構成[20],，其內部包含了移動性管理組件(Mobility Management Entity, MME)、服務閘道(Serving Gateway, SGW)、數據封包網路閘道器(Packet Data Network Gateway, PGW)與歸屬用戶伺服器(Home Subscriber Server, HSS)，當行動裝置聯結到 EP 時，MME 將會代表 EPC 與行動裝置進行多重認證，系統架構圖請見圖 2-5，以下針對 EPC 和 E-UTRAN 各設備做詳細的介紹[21]：

- Home Subscriber Server (HSS)：其內資料庫包含用戶設定檔，以便執行用戶身分驗證與授權，負責用戶資料管理、執行身分認證(Authentication)及金鑰協商等安全性功能。
- Mobility Management Entity(MME)：負責管理控制訊號，其中包含了承載(bearer)建立與維護之管理工作，以及管理UE與其LTE建立連線時的維護、行動管理以及安全性相關參數。
- Serving Gateway (S-GW)：負責路由(Routes)和傳送(Forwards)用戶所有的IP封包資料，也就是說用戶所有的IP封包均會透過此設備傳送。而對於閒置模式(Idle Mode)的用戶，S-GW 會終止其下行資料路徑；除非當該用戶的下行資料到達S-GW 後，才會重新觸發呼叫(Paging)的動作。
- Packet Data Network Gateway (PGW)：透過SGi介面提供與外部資料網路的連接。其功能包含UE的 IP 位址分配，針對各個用戶之封包進行過濾及監聽。
- User Equipment (UE)：為能運作LTE 上控制面(Control plane)及使用者面(User plane)兩種協議棧(Protocol Stack)的行動通訊的使用者，可能為搭載LTE上網技術的行動裝置、平板或其他行動裝置。

- Evolved NodeB (eNB)：為LTE 接入網路(Access Network) 連接UE 之設備，主要負責無線資源管理，並且管理使用者資料壓縮與加密、UE連接時LTE網路時MME之選擇、傳送廣播資訊以及根據UE所提供的訊號測量資訊回報(Measurement Report)，對手上的資源進行排程(Scheduling)，以利接下來進行Handover的種種步驟。
- Home eNB (HeNB) ：為一個低功率的接入點，支援eNB的大部分功能，被用來提高室內網路的覆蓋量和容量，透過室內的寬頻網路連接無線存取網路(Radio Access Network)網路與核心網路(Core Network)。

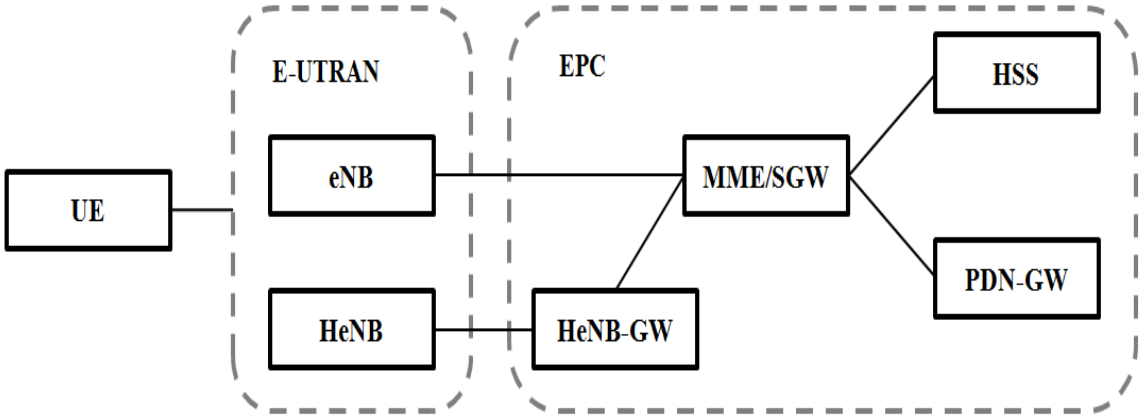


圖 2-5　LTE 網路架構圖

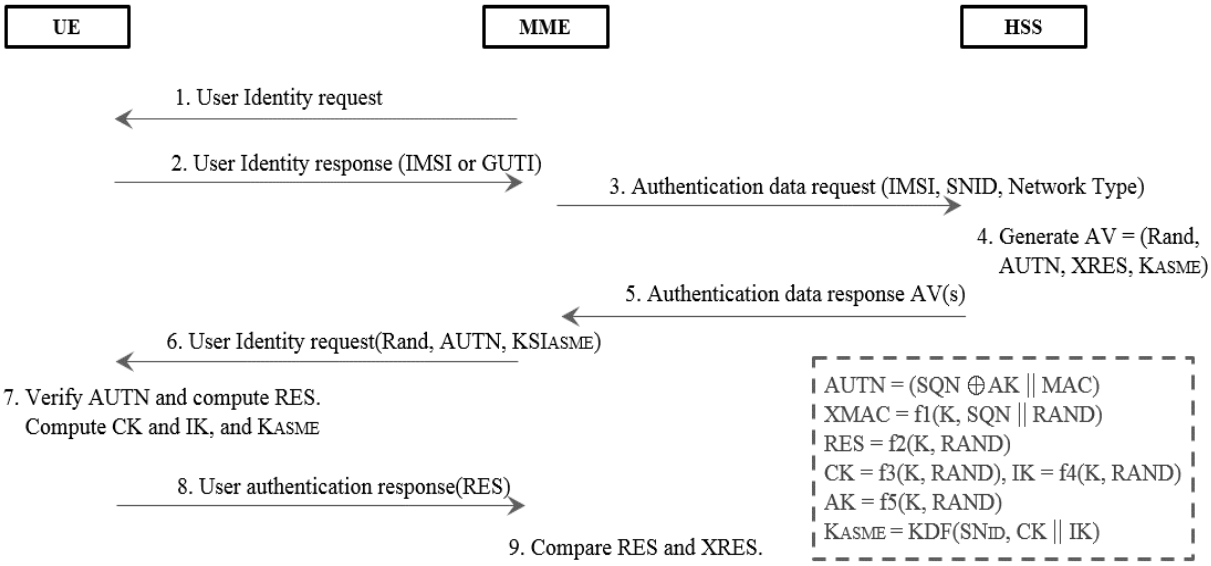
貳、LTE 網路系統安全

在 LTE 安全架構中最重要的安全特性是 UE 與 EPC 之間的相互認證，LTE 系統採用認證與密鑰協商協議(Authentication and Key Agreement, AKA)生成加密密鑰(CK)與完整性密鑰(IK)來實現 UE 與 EPC 間的互相認證[22]，當 UE 欲透過 E-UTRAN 連接到 EPC 時，MME 將代表 EPC 執行 AKA 協議如下圖 2-6。

開始 AKA 流程時，首先 MME 向 UE 傳送身分認證要求，而後 UE 將自身全球唯一臨時標識(Globally Unique Temporary Identity, GUTI)傳送給 MME，如果沒有則傳送國際移動用戶識別碼(International Mobile Subscriber Identity, IMSI)，MME 收到 GUTI 後，藉此找到 UE 的 IMSI，並向後端 HSS 索取認證所需的相關資料鑑

別向量(Authentication vectors, AV)(s)，其中包含了隨機亂數(Random Number, RAND)、預期的回應值(Expected Response, XRES)、認證代碼(Authentication Token, AUTN)及密鑰 K_{ASME}，當 MME 收到 AV(s)後，MME 將傳送其中一組 AV 中的 RAND、AUTN、KSI_{ASME} 給 UE 讓 UE 開始進行認證程式。

UE 收到上述參數後，首先會對 AUTN 內的訊息認證碼(Message Authentication Code, MAC)進行驗證，其中沿用自 3G 系統的 f1~f5 演算法同樣於[22]被 3GPP 定義於 LTE 系統，f1 和 f2 為認證函數，而 f3、f4、f5 和 KDF 為密鑰生成函數，序列號碼(Sequence Number, SQN)為一計數器，被用來運算出預期的訊息認證碼(Expected Message Authentication Code, XMAC)驗證所接收到的 MAC 是否來自合法的電信業者，若是則而後利用 RAND 密鑰 K 產生回應值(Response, RES)回傳給 MME 完成認證程式，如果認證成功，此後 UE 將可以透過此認證所產生的密鑰和



後端系統進行加密保護的資料傳輸。

圖 2-6　LTE 行動裝置認證流程

同時新的密鑰階層也將被引入以保護訊令與使用者的資料傳輸如下圖 2-7[22]，K 是儲存在全球用戶識別卡(Universal Subscriber Identity Module, USIM)和其電信

業者認證中心(Authentication Centre, AuC)中的固定私有金鑰，是所有金鑰生成演算法的基礎。K_{ASME} 是一個中間金鑰，在 AKA 過程中由 CK 和 IK 兩把鑰匙生成，K_{eNB} 也是一個中間密鑰，由 UE 和 MME 根據 K_{ASME} 生成，是 eNB 為了無線資源控制(Radio Resource Control, RRC)與使用者面(User Plane, UP)訊息傳輸所生成的金鑰，而最後為了能允許 MME 與 UE 之間非存取層(Non-access Stratum, NAS)訊息、eNB 與 UE 之間存取層(Access Stratum, AS)訊息和使用者面資料進行完整性保護和機密性保護，接著產生以下 5 個金鑰如下圖 2-4-3：

K_{NASenc}：UE 和 MME 根據 K_{ASME} 生成，用於特定的加密演算法來保護 NAS 訊息。

K_{NASint}：UE 和 MME 根據 K_{ASME} 生成，用於特定完整性演算法來保護 NAS 訊息。

K_{Upenc}：UE 和 eNB 由 K_{eNB} 和下一跳密鑰計數器(Next Hop Chaining Counters, NCC)運算所得，用於保護 UE 和 eNB 間使用者面的保密性加密。

K_{RRCint}：UE 和 eNB 由 K_{eNB} 和 NCC 運算所得，用於保護 UE 和 eNB 間無線資源控制訊息的完整性加密。

K_{RRCenc}：UE 和 eNB 由 K_{eNB} 和 NCC 運算所得，用於保護 UE 和 eNB 間無線資源控制訊息的保密性加密。

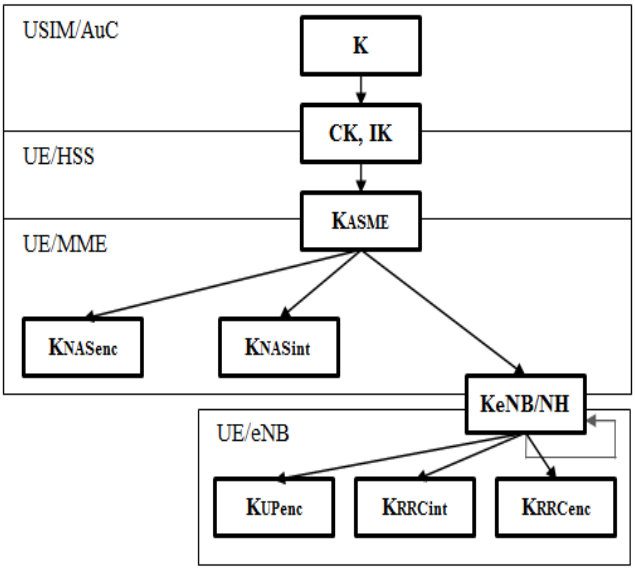


圖 2-7　LTE 密鑰層級

3GPP 對於 LTE 提出了不同於以往 GSM 及 3G 的換手(Handover)流程[22]，在內部 E-UTRAN 內的換手流程中，LTE 網路採用一種新的密鑰管理機制，包含了垂直與水準的密鑰推導，如圖 2-8[22]，為了達到 UE 與 eNB 的安全溝通，MME 與 UE 必須要從 K_{ASME} 計算出初始的下一跳密鑰(Next Hop key, NH)，NCC 則是 KeNB 及 NH 的計數器，每次進行換手程式後，所產生的新的一屆密鑰名為 KeNB*，將會被 UE 和目標的 eNB 由前一次的 KeNB 或 NH 產生。

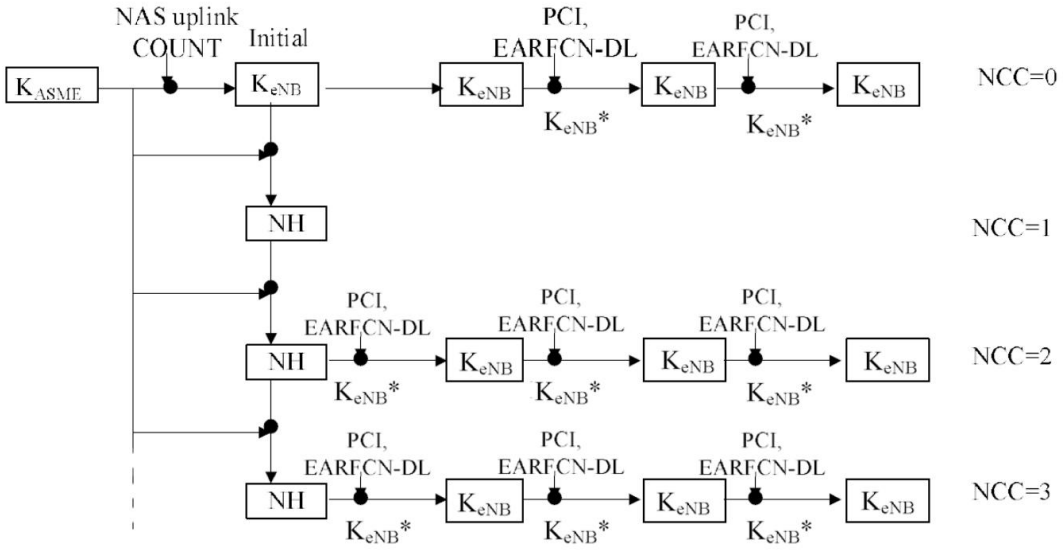


圖 2-8　換手密鑰產生與管理

參、LTE 網路的威脅

Jin 等人的論文[23]中提到，由於 3GPP LTE 網路架構為扁平化的基於 IP(IP-based)的架構，因此容易被攻擊者獲取的小成本基站 HeNB，攻擊者可創造一個屬於自己的 HeNB，以此模擬真正的 HeNB 吸引一般合法的行動裝置連接，雖然 3GPP 委員會已經針對此部分進行相關的安全要求(Security Requirements)但仍有許多漏洞在 LTE 網路移動性管理程式和換手機制中發現[23]。

Cao[26]等人表示 LTE 換手機制中缺乏向後的安全性，基於換手密鑰產生互相鏈結，當前的 eNB 可推導出往後多個目標的新密鑰，將造成移動設備與 eNB 間的資訊交換安全遭到威脅。另外，攻擊者可使用惡意的 HeNB 中斷行動裝置的 NCC 值更新，造成行動裝置進行換手時，目標的 eNB 與 MME 失去 NCC 的同步，造成行動裝置僅能進行水準的密鑰推導，降低接下來密鑰能提供的安全性。

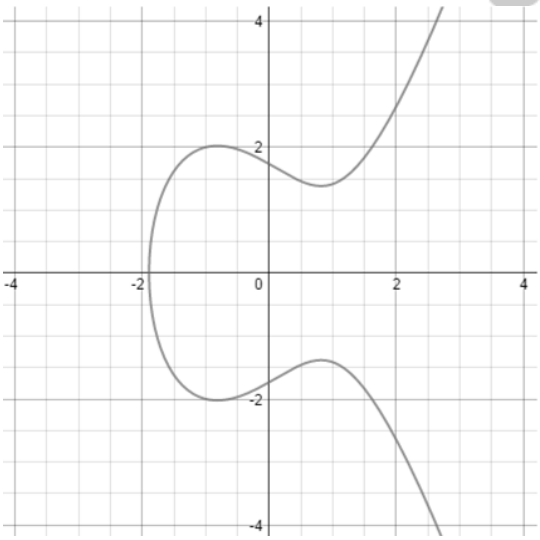
第五節　橢圓曲線密碼系統

橢圓曲線密碼系統(Elliptic Curve Cryptography, ECC)由 Miller 與 Koblitz 於 1980 年中期提出，他們將橢圓曲線帶進密碼學當中，設計了一套密碼系統。橢圓曲線密碼系統相較於其他密碼系統，僅需使用較小的密鑰便能提供較高的安全性，因為此特性，使得橢圓曲線加密系統廣泛的被應用在密碼學中。本論文接著要來介紹橢圓曲線加法[27][28]與其的加解密[29]的部分。

壹、橢圓曲線函數

橢圓曲線函數的圖形方程式如下，若將此方程式畫成圖形可如圖 2-9 與圖 2-10 中所示：

$$E: y^2 = x^3 + ax + b$$



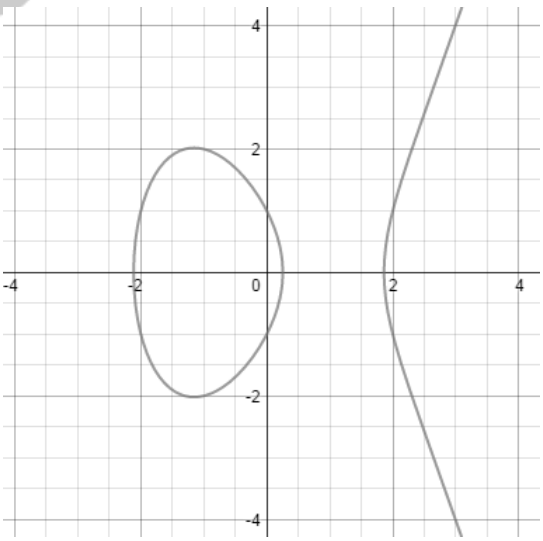


圖 2-9　橢圓曲線E：$y^2 = x^3 - 2x + 3$　　圖 2-10　橢圓曲線E：$y^2 = x^3 - 5x + 1$

方程式中的 a 與 b 可為任何數，但為了確保橢圓曲線沒有重根，橢圓曲線方程式中的 a 與 b 必須要符合$4a^3 + 27b^2 \neq 0$的規則，而所產生的橢圓曲線圖形將會對稱於$y = 0$。

貳、橢圓曲線上的加法

如果假設支橢圓曲線無重根,在橢圓曲線上選定不同 x 座標的兩個點 P 與 Q，令$P = (x_1, y_1)$、$Q = (x_2, y_2)$、$P + Q = (x_3, y_3)$以數學式運算：

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

其中 m 的計算方法為：

$$\text{if } P \neq Q,\ m = \frac{y_1 - y_2}{x_2 - x_1}$$

$$\text{if } P = Q,\ m = \frac{3x^2 + a}{2y_1}$$

若進行兩點相加的運算，將會發現在橢圓曲線上符合任共線之三點相加必等於∞，且$\infty = -\infty$，也就是說 $P + Q + R = \infty$。

橢圓曲線函數的加法運算分為以下幾種：

- 將 P 與 Q 兩點帶入橢圓曲線中運算後得出之值，恰好會等於 P 與 Q 兩點相連之 R 點對稱於 x 軸的點 -R，也可以說是 $P + Q = -R$，如下圖 2-11 橢圓曲線的加法(a)。
- 若 P 與 Q 兩點為同一點(P = Q)帶入橢圓曲線中運算後得出之值，恰好會等於 P 與 Q 兩點相連之 R 點對稱於 x 軸的點 -R，也可以說是 $P + Q = -R$，如下圖 2-12 橢圓曲線的加法(b)。

- 若 P 與 Q 對稱於 x 軸，也就是 Q = -P，則會發現 P+Q 之值等於 ∞ ，也可以說是$P+Q=P+(-P)=\infty$ ，如下圖 2-13 橢圓曲線的加法(c)。
- 若將 P 點與 ∞ 相加，經過運算後會發現得到的點仍然是 P，也可以說是$P+\infty=-R=P$ ，如下圖 2-14 橢圓曲線的加法(d)。

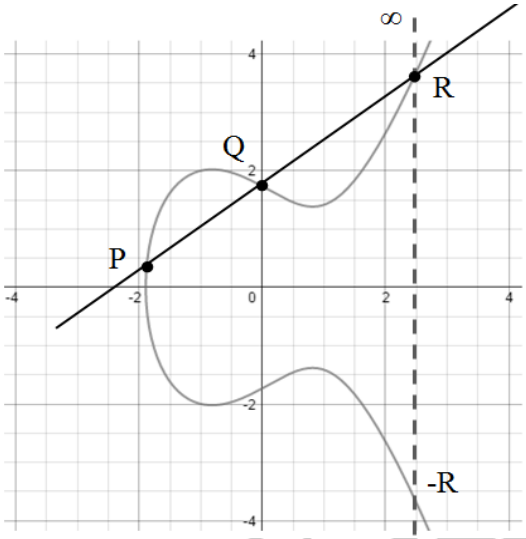


圖 2-11　橢圓曲線的加法(a)

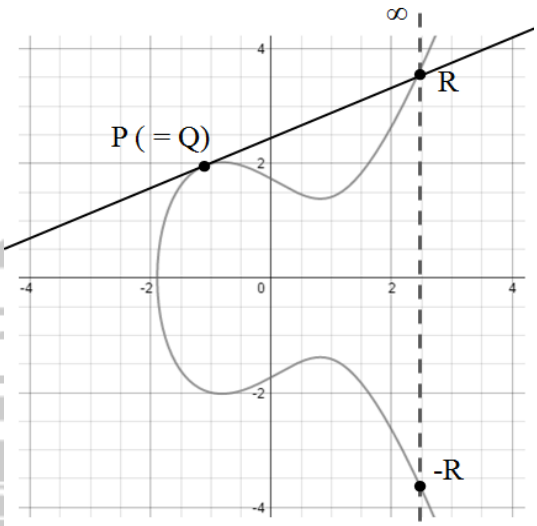


圖 2-12　橢圓曲線的加法(b)

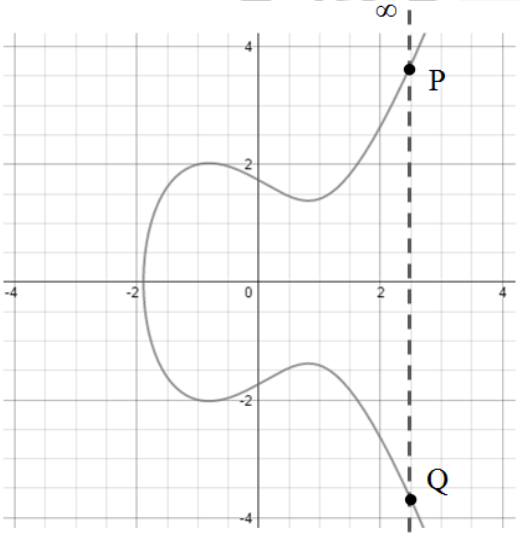


圖 2-13　橢圓曲線的加法(c)

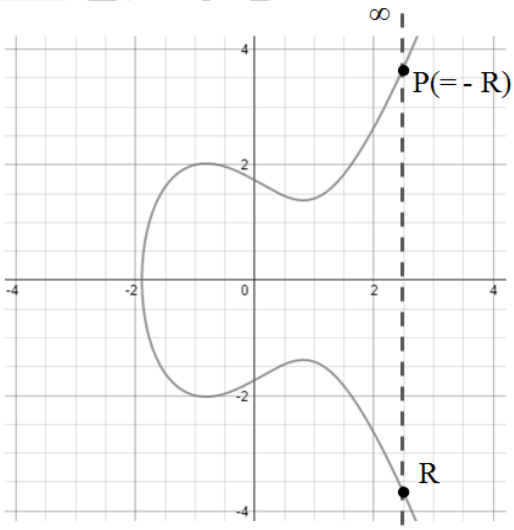


圖 2-14　橢圓曲線的加法(d)

而橢圓曲線上的乘法為加法的延伸，也就是說$2P=P+P$，$3P=P+P+P$，以此類推 nP 則為 n 個 P 相加。

參、利用橢圓曲線金鑰交換系統進行訊息加解密

若將橢圓曲線使用一個大質數進行 mod 運算，也就是E：$y^2 \equiv x^3 + ax + b \pmod p$，則可將橢圓曲線的值限制在一個固定的範圍中，此方法將橢圓曲線的加法變成更困難的離散對數題目，也就是說，若給定一點 P，要求得 R = nP 是很容易的，但若給定 P 與 R 要求得 n 將會非常困難，此為利用橢圓曲線加密的基礎。

今假設 Ally、Blue 兩方欲建立密鑰以進行資料交換，如下圖 2-15 所示:

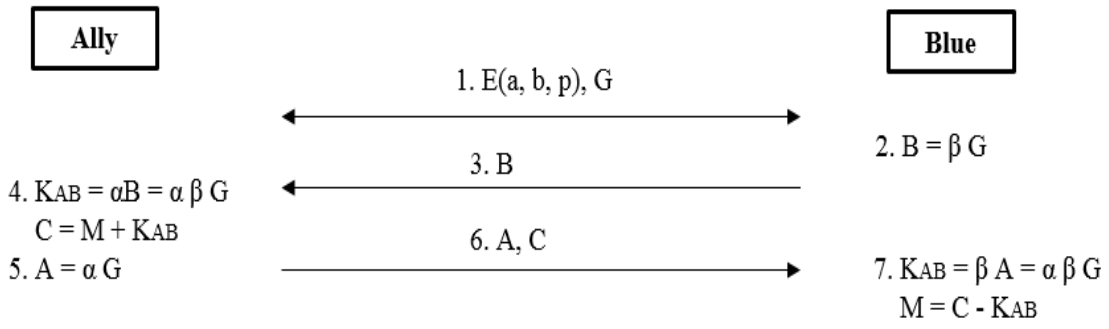


圖 2-15　橢圓曲線加解密

步驟 1： 首先雙方必須公開完整的橢圓曲線所必備的參數 E(a, b, p)及橢圓曲線上一點 G(x, y)。

步驟 2-3： 欲使 Ally 可傳送加密訊息給 Blue，Blue 必須取一亂數 β 當作私鑰對點 G 做乘法，並將乘法所得的點 B 作為公鑰傳送給 Ally。

步驟 4： 收到 Blue 傳送過來的點 P 後，將亂數產生的私鑰 α 乘上點 B 即可得到點 KAB，也就是 Ally 與 Blue 共有的私密金鑰。若要加密訊息則將訊息製作成橢圓曲線上的點 M 加上 KAB 即可得到加密的訊息 C。

步驟 5-7： 為了能讓 B 得以解開加密的訊息 C，Ally 必須要將點 G 乘上私鑰 α 運

算出點 A，並將點 A 和加密訊息 C 一起傳送給 Blue，Blue 收到訊息後即可使用點 A 乘上自身私鑰 β 得到與 Ally 共有的私密金鑰 K_{AB}，如此一來只要將 C 減去 K_{AB} 即可還原訊息 M，完成訊息的交換。

相較於其他密碼學系統如常見的 RSA，橢圓曲線密碼系統可用較小的密鑰提供提供較高的安全性，如下表 2-2，而橢圓曲線密碼系統的另一個優勢是可以定義群之間的雙線性映射，目前雙線性映射在密碼學中已大量的應用，例如基於身份的加密，而其缺點則是加密和解密操作的實現較其他機制花費的時間長。

表 2-2　RSA 與橢圓曲線密碼系統在相同安全度下金鑰長度之比較 [34]

RSA 與橢圓曲線密碼系統在相同安全度下的金鑰長度比較					
RSA	512	1024	2024	3072	7680
ECC	112	163	224	256	384
Key	1:5	1:6	1:9	1:12	1:20

第三章 NFC-LTE 行動裝置在 POS 上的安全認證機制

在此章節中，我們將提出使用傳統實體店面 POS 進行行動支付的系統架構，由於現在使用傳統 POS 的數量依舊占交易市場很大的比例，因此我們認為應該要將舊有的 POS 系統與新興的 NFC 行動支付服務以及 LTE 行動網路做整合，提供安全且方便的交易環境給顧客。

目前已有許多學者提出相關論文，Chen 等人首先提出如何在 GSM、3G 系統上實現 DCB 行動支付的概念架構[10][30]，並將 AKA 認證方法加入行動支付裡，提升實體店面上透過POS來解決DCB行動支付交易與資料傳輸上的安全性問題，論文[12]提出使用創新的NFC 閘道(Gateway)讓POS 透過用戶端移動設備連接線有無線網路，論文[13]提出了將顧客信用卡資料儲存在網路雲端資訊系統上以達到安全交易的目的，而論文[31]中實做了在 3G 網路的行動支付。

但目前為止，仍無學者針對 LTE 行動通訊網路在這方面的議題上進行研究討論，因此本論文在此提出了基於 LTE 行動通訊系統結合 NFC 在傳統 POS 上進行行動支付的安全方案，以提供顧客更安全的交易環境，詳細系統架構如下。

第一節　系統架構與前置設定

在LTE行動網路上整合POS與掌上型NFC個人行動裝置的系統架構圖如圖3-1中所示，同時在此系統需要有幾項前置設定:

1. 所有的實體協議必須屬於相同的行動通訊網路業者(MNO)，也就是說用戶行動裝置(User Equipment, UE)及 POS 皆必須先向相同的行動網路業者進行註冊，並且屬於行動網路業者後端系統的一部分。
2. 用戶行動裝置與 POS 皆須擁有 NFC 功能，並且透過一般規範電子錢包及行動裝置間互相交換資料的規範 ISO/ICE18092 進行溝通，其中 POS 為店家內的固定式結帳機台，可讀取條碼或 RFID 標籤以計算購買金額並顯示購買資訊，欲

進行交易時，顧客需到櫃檯結帳。

3. 用戶行動裝置必須開機且經過 LTE 行動網路認證，且用戶行動裝置必須和 HSS 擁有相同的密鑰 K 與密鑰生成演算法，以用來認證並產生加解密相關密鑰。
4. POS 與支付閘道之連結、行動網路業者後端系統間所有成員之連結均屬秘密頻道(Secure Channel)。
5. 支付閘道(Payment Gateway, PG)被定義在論文[6]中，在行動網路業者後端系統架構中類似一個 sub-MME，其工作為尋找與用戶行動裝置相對應的 MME，處理所有行動支付過程中來自 POS 的資料傳輸及認證，減輕 MME 的工作量。
6. LTE 電信系統端的帳務中心(Billing Centre, BC)為行動網路業者後端系統中，負責進行所有電話、簡訊及行動支付等相關帳務結算與紀錄的工作。

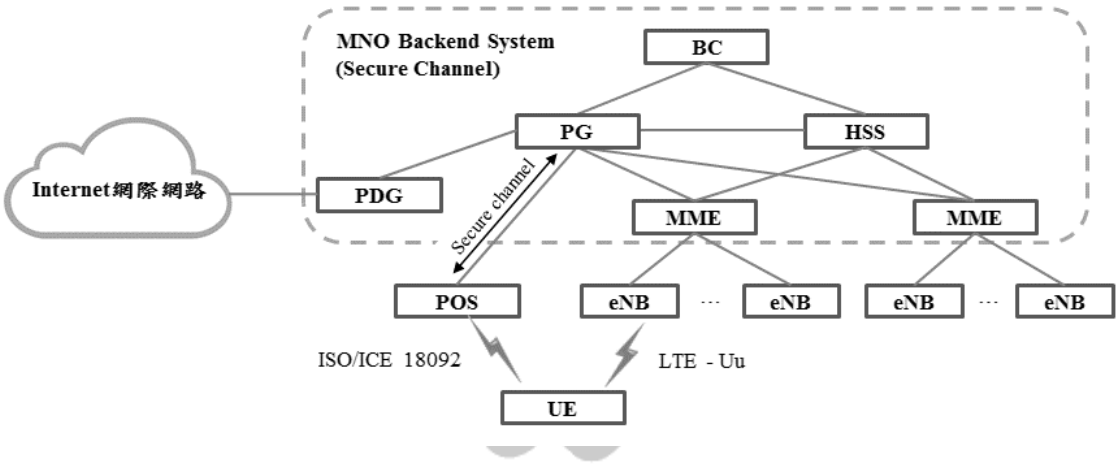


圖 3-1　LTE 系統上整合 POS 的系統架構

第二節　在 LTE 架構中的行動支付與認證流程

本論文將系統架構分為三個階段，如圖 3-2，前 5 個步驟為商品確認準備交易，價格確認在此部分進行，顧客可視覺上的確認商品價格是否有誤，並且決定是否繼續進行交易。接著步驟第 6 至 20 為相互認證階段，用戶行動裝置在這時與商家 POS 進行相互驗證。最後步驟 21 至 34 為交易執行，金錢的交易在此部分進行。

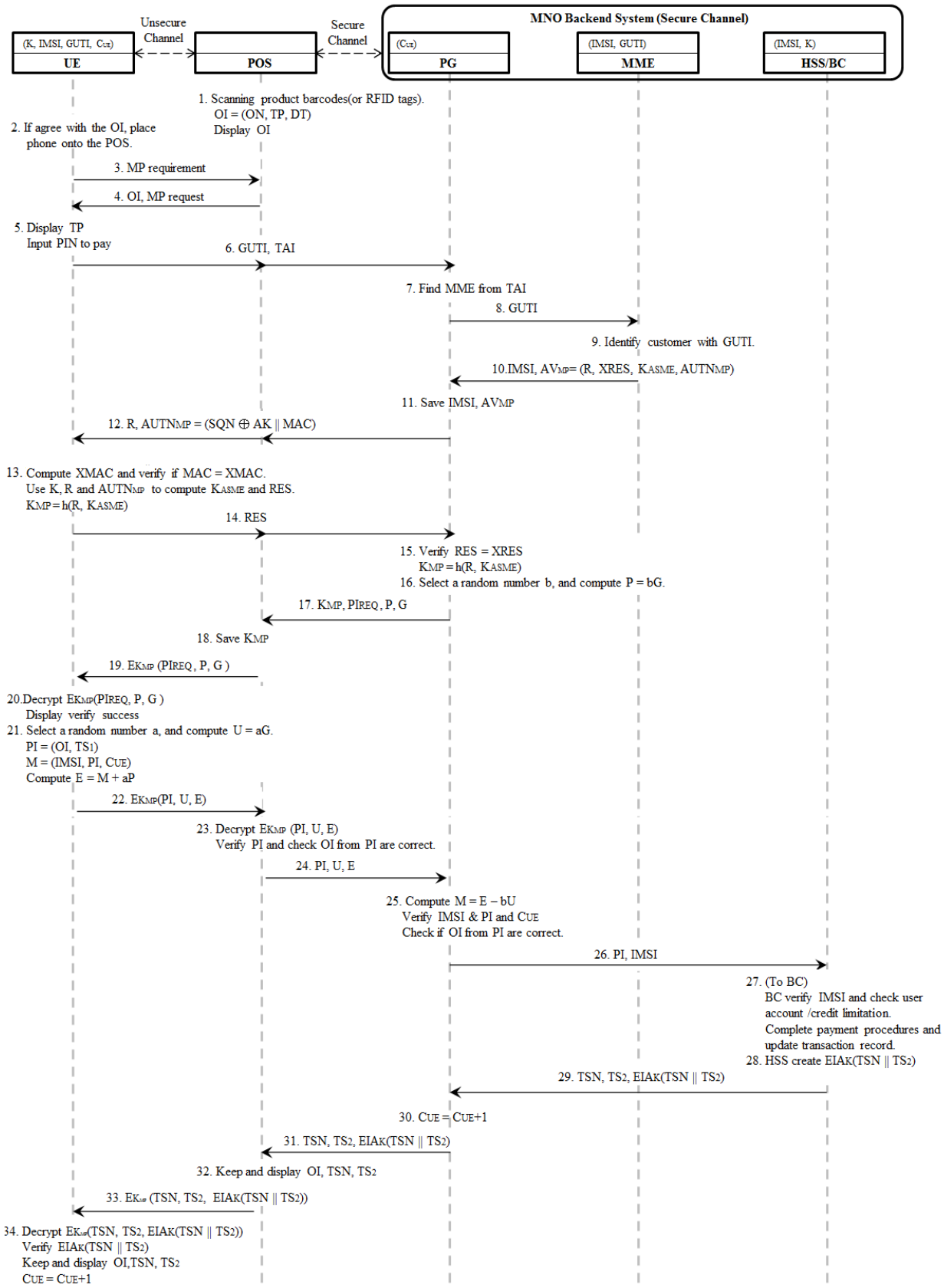


圖 3-2　NFC-LTE 在使用 POS 環境下的 DCB 行動支付流程圖

壹、商品確認準備交易

在此階段為顧客與商家開始交易時的準備動作，顧客選購完所有商品後拿到櫃台進行結帳，待此階段完全結束後才算是交易的開始，在此之前商家 POS 與顧客 UE 尚未有任何的資料往來。

步驟 1-2 : 首先,商家 POS 掃描顧客所選擇的商品上的條碼(Barcode)或者 RFID 標籤(Tag)並且計算購買價格，接著由購買編號(ON)、總金額(TP)與日期時間(DT)組成購買資訊(OI)顯示在螢幕上讓顧客查看,在此商品資訊將被店家保存當作紀錄與交易證明，當往後發生爭議時可供查閱。

步驟 3-5 : 顧客確認過 POS 上購買資訊內的總金額與日期時間後，須選擇用戶行動裝置中的行動支付服務，並將用戶行動裝置放置於 POS 上以開始 NFC 連結，接著用戶行動裝置會對 POS 發起行動支付需求傳送購買資訊給用戶行動裝置，在此時用戶行動裝置將顯示購買資訊的內容，若顧客同意此筆交易，則在用戶行動裝置輸入行動裝置密碼(PIN)開始交易，此動作不僅是確認此用戶行動裝置確實為此顧客所有，同時也代表顧客是出於自我意識地同意了這筆交易。

貳、相互認證階段

在此階段中,用戶行動裝置將開始與後端系統進行認證與密鑰協商協議(AKA)，電信業者後端系統將透過用戶行動裝置所發送來的 GUTI 來判斷用戶行動裝置的身分，並且傳送相對應的 MAC 讓用戶行動裝置對行動網路業者做身分認證，而用戶行動裝置將運用接收到的參數經過認證與運算後，回傳相對的回應值(RES)給後端系統以完成認證，如此一來金錢的交易便可開始進行。

步驟 6-9 : GUTI 為 LTE 在 MME 中暫時性代表用戶行動裝置的參數。在 POS 和用戶行動裝置建立秘密頻道前，GUTI 為非常適合代表用戶行動裝置讓 MME 識別顧

客身份的參數(IMSI 必須要保持私密)，MME 可以藉由 GUTI 找到顧客相對應的 IMSI。而經由 POS 傳送給支付閘道的追蹤區域辨識(Tracking Area Identity, TAI)中包含了 MME 的位置，支付閘道可藉此找到 UE 所屬的 MME 並向其索取接下來認證所需要的參數。

步驟 10-12： 在 MME 成功辨識顧客後，MME 將用戶行動裝置認證所需要的參數 AV_{MP} 傳送給支付閘道(在此使用 AV_{MP} 與用戶行動裝置初始認證用的 AV 做區隔)與用戶行動裝置的 IMSI 一併傳送給支付閘道，如此一來，支付閘道就可以在接下來的步驟透過IMSI來辨識用戶行動裝置是否被更改，而不會受GUTI更改的限制。支付閘道收到 AV_{MP} 後，將其中的 R 與 $AUTN_{MP}$ 傳送給用戶行動裝置(在此使用 $AUTN_{MP}$ 與 AV 中的 AUTN 做區隔)，以進行接下來 LTE 的認證。

步驟 13-15： 接著，用戶行動裝置由 $AUTN_{MP}$ 中的 MAC 驗證支付閘道是否屬於相同的行動網路業者，如果是則用戶行動裝置將使用所得的參數 R 和自身密鑰 K 產生 RES 回傳給支付閘道，支付閘道收到 RES 後則使用之前從 MME 接收到的 XRES 驗證 RES 以確認用戶行動裝置的合法性，而其中用戶行動裝置與支付閘道分別進行赫序函數 $h(R, K_{ASME})$生成 128 位元的密鑰 K_{MP}，做為之後用戶行動裝置與 POS 之間的密鑰。

步驟 16-20： 支付閘道也接著開始進行使用橢圓曲線加解密的準備動作，首先，支付閘道會選取一個橢圓取線上的 G 點當作基準點，再亂數選取一個數字 b 當作支付閘道橢圓曲線加密系統的的私鑰，將 b 乘上 G 點產生公鑰 P 點，完成準備動作。

接著，支付閘道將 K_{MP}、PI_{REQ}、P 與 G 傳送給 POS，而 POS 接收到後將 PI_{REQ}、P 與 G 使用 K_{MP} 加密傳送給用戶行動裝置。用戶行動裝置收到 PI_{REQ} 可得知認證成功並螢幕顯示，反之則顯示認證失敗。

參、交易執行

在此階段行動支付流程將邁入現金扣款的交易執行，用戶行動裝置與 POS 將分別傳送購買資訊以提供行動網路業者後端系統做交易資料比對，而交易結束後，行動網路業者後端系統也將傳送交易成功訊息給用戶行動裝置與商家 POS 以供保存與查證。

步驟 21-23 : 若要和支付閘道進行橢圓曲線加密的資料交換，用戶行動裝置也必須產生一個亂數 a 當作橢圓曲線加密法的私鑰，並將 a 乘上橢圓曲線上的點 G 生成另一點 U 作為公鑰傳送給支付閘道。

交易資訊(PI)由用戶行動裝置生成，包含了購買資訊、計數器(CUE)與時戳一(TS_1)，其中計數器與時戳一是用來防止重複攻擊(Replay Attack)，時戳一是交易資訊產生的時間，用來證明此交易是在期望的時間內進行。

用戶行動裝置將欲傳送的的訊息使用橢圓曲線運算加密成點 E 後，將交易資訊、公鑰 U 與點 E 一同由 KMP 再次加密後傳送給 POS。在此我們使用經橢圓曲線加密 IMSI、時戳一等機密資料，能有效的防止攻擊者竊聽，保護顧客資料的安全。

步驟 24-25 : POS 接收到來自用戶行動裝置的訊息後，首先使用從支付閘道接收到的 KMP 解密此訊息，接著比對來自用戶行動裝置的購買資訊與自身擁有的購買資訊是否相符合，若無誤則將訊息轉交給支付閘道。支付閘道接收到來自 POS 的訊息後，將加密的訊息點 E 經由橢圓曲線的運算得到訊息 M，接著使用顧客的 IMSI 與計數器認證用戶行動裝置身分，並接著比對分別來自用戶行動裝置與 POS 的購買資訊是否相符合。

步驟 26-29 : 支付閘道確認來自用戶行動裝置與與 POS 的資訊正確後，則將交易資訊及 IMSI 傳送給帳務中心，供帳務中心檢查使用者帳單/賒帳是否可完成此筆交易，如果顧客帳單合法交易將會進行，交易進行完畢後並產生交易結果的代號(TSN)與代表交易發生時間的時戳二(TS_2)，並交由 HSS 使用 K 及 LTE 內建的加密演算法 EIA 來製作交易結果憑證 EIAK(TSN||TS_2)，以保護資料的完整性以防攻擊者竄

改此資訊，接著再將交易結果傳送給支付閘道。

步驟 30-33： 若交易成功，則支付閘道內的計數器內容將增加一，並將交易結果代號、時戳二及交易結果簽章經由 POS 使用 K_{MP} 加密後傳送給用戶行動裝置，以防攻擊者竊取資料，同時 POS 將交易代號、時戳及購買資料顯示並保存。

步驟 34： 當用戶行動裝置收到加密的交易訊息後，用戶行動裝置將運算 TSN 與 TS_2 與所接收到的憑證是否相同，如果相同則將交易代號、時戳及購買資料顯示並保存，並將用戶行動裝置內計數器的內容增加一以完成交易。

第三節　安全情境分析

若要讓此系統可以安全的進行交易，則必須設想究竟有可能會遭遇到什麼樣的安全性問題，尤其是在交易進行的過程中將有金錢及顧客敏感資料的交換，無論是商家、顧客、或者竊取資料的中間人(Man-in-the-Middle)都有可能尋找此系統的漏洞進行攻擊，以從中獲取非法的利益，因此特別需要注重其安全性，在此本論文提出關於此此論文系統的安全性分析，並提出及改善論文[10]可能面臨的問題。本論文針對(1)資料完整性。(2)資料機密性。(3)交易匿名性。(4)交易參與者的身分認證。(5)不可否認性。以上幾點來進行分析。

壹、資料完整性：

在本論文系統中，所有金額時間及交易結果都經過了完整性加密的保護，在步驟 24 及 26 中，商家 POS 與支付閘道皆可重複確認商品資料是否被顧客或商家任何一方修改。我們在步驟 21 中使用橢圓曲線加密訊息傳送給支付閘道驗證訊息的正確性，此方法可讓用戶行動裝置的機密資料 IMSI 及計數器被安全及完整的傳送，以供支付閘道及行動網路業者後端系統做認證，在步驟 28 中由 HSS 使用 LTE 行動通訊系統內更具安全性的 EIA 方程式搭配僅為用戶行動裝置與行動網路業者共有的密鑰K產生憑證，保證了僅有用戶行動裝置及行動網路業者能產生此簽章，

達到更高的安全性。

貳、資料機密性：

當資料在用戶行動裝置與 mPOS 間交換資料為使用 NFC 技術，此技術優點在前面有描述過，僅允許在 10 公分以內進行交易，大幅降低中間人攻擊(Man-in-the-Middle)擷取交易資料、冒充顧用戶行動裝置進行交易。但若商家與中間人勾結，重要資料將有可能被不法攻擊者擷取，因此本系統之機密資料在步驟 19、22 與 33 中使用了 K_{MP} 加密做為保護以防洩漏，步驟 21 中重要資訊如 IMSI、計數器則使用橢圓曲線演算法的加密保護以防商家非法獲取顧客私人資料。

參、交易匿名性：

在交易過程中，商家無法透過 POS 得知特定顧客的消費習慣，因顧客僅在步驟 6 對 POS 透露暫時代表自我身分的 GUTI。而行動網路後端系統無法得知顧客的詳細交易內容，僅能在步驟 25 得知其購物金額、物品、時間及地點。

肆、交易參與者的身份認證：

在交易開始時，步驟 5 中用戶行動裝置用 PIN 的輸入對顧客進行認證，以確保該用戶行動裝置確實是屬於該顧客，接著才進行用戶行動裝置與後端系統之間的認證，透過在步驟 6 傳遞給後端的 GUTI 及 TAI，後端系統可得知用戶行動裝置的身分，以產生相對應的認證參數回傳給用戶行動裝置，收到認證參數後，用戶行動裝置可在步驟 13 中驗證後端系統的 MAC 與 SQN，以此得知 POS 與行動網路業者後端系統是否簽約於和自己相同的行動網路業者並具合法性，避免交易連結到非法的後端系統，而後用戶行動裝置在步驟 14 將運算出的 RES 回傳給支付閘道，讓行動網路業者後端系統得以確認用戶行動裝置身分，除此之外，後續交易如步驟 13 與 15 的 K_{MP} 為僅有用戶行動裝置與支付閘道能產生之密鑰，而用戶行動裝置再步驟 21 中將 IMSI 與計數器經橢圓曲線加密以供行動網路業者後端系統再次

認證，最後在步驟 28-29 中 HSS 將交易結果利用密鑰 K 做簽章提供用戶行動裝置做再次確認，經過如此多重的驗證，防止中間人攻擊，避免資料被竊取及竄改。

伍、不可否認性：

也就是說若交易完成，則交易參與者無法否認此筆交易，步驟 5 中必須是由顧客輸入 PIN 到用戶行動裝置裡，由此可知該筆交易是經過顧客有意識的同意而開始的，步驟 25 由 PG 確認經過加密的時戳，防止重複攻擊(Reply Attack)，避免攻擊者擷取並重複傳送資料導致重複扣款。交易結束後，商家及顧客在步驟 32 與 34 中保留包含交易商品內容、時間、地點、金額的單據，以供未來有糾紛時查詢。

第四節　系統架構優缺點

壹、優點：

1. 本論文利用現存的 LTE 行動網路安全認證機制及其後端硬體設備，減少建置時間與成本，此系統之行動支付可以更容易的被行動網路業者、商家及消費者接受，較能快速的被普及。
2. 無論對於商家或是顧客，本系統都極易操作，顧客僅需透過用戶行動裝置與商家 POS 的接觸及可完成交易，並且交易資料會存在用戶行動裝置裡，供顧客透過用戶行動裝置確認購買的商品是否有誤。而商家也可保留交易號碼與商品內容，可做為往後查詢或規劃產品策略所用。
3. 此架構使用加密的計數器及時戳以防範重複攻擊，並且擁有多重認證機制可防範中間人攻擊。
4. 顧客可在交易結束後第一時間確認購買結果，商家與顧可彼此皆可儲存交易結果以便往後有爭議時做為依據。
5. 掌管後端系統的行動網路業者將不會得知顧客的購物清單，僅能知道其購物金額、時間及地點，並且由於在資料傳輸時經橢圓曲線等加密保護，POS 將

無法得知用戶行動裝置之 IMSI 以及和行動網路業者共有的密鑰 K。

6. 本論文使用了橢圓曲線加密法加密傳送 IMSI 給支付閘道讓其對用戶行動裝置進行身分核對，由於橢圓曲線加解密法容許較大的資料加密傳輸，相較於論文[10]更加安全，並且決了其加密訊息長度須小於 128bits 的限制。
7. 我們使用 IMSI 做為再次認證用戶行動裝置參數,用戶行動裝置將不會因 GUTI 的定時更換，而造成支付閘道無法辨認顧客身分，減少交易失敗的機會。

貳、缺點：

1. 我們未解決用戶行動裝置無法在行動支付中進行換手的問題，因此本論文中的系統只能架構在非移動式的實體店面中。
2. 在行動支付的過程中，商家 POS 必須具備可上網的功能，才能與後端系統做資料交換。
3. 認證階段透過用戶行動裝置內部的認證與密鑰協商協議進行用戶行動裝置認證，此過程將改變用戶行動裝置內部與基地台及 MME 溝通的參數，因此在行動支付的過程中無法接聽電話。

第五節　結論

在此章節中我們提出了在實體店面 POS 進行基於電信業者代收付款的行動支付模式，克服了 Chen[10]等人所提出的架構中加密的字元數限制，並且加入橢圓曲線加密演算法，使得交易資料能更安全的被保護，能防止中間人攻擊與重複攻擊，且兼具資料完整性、資料機密性、交易匿名性與不可否認性，顧客能更放心的使用本機制進行交易，而對行動網路業者而言，此種機制不需要增設太多硬體設備，能節省建置成本，並且能幫助行動網路業者更進一步拓展電信業者代收付款擴大市場。

第四章NFC-LTE 行動裝置在 mPOS 上的安全認證機制

在此章節提出使用 mPOS 在 LTE 網路上進行 DCB 行動支付的系統架構與安全認證機制，相較於傳統實體店面所使用的固定式 POS 資訊系統，mPOS 的特色即為重量與體積輕薄且可攜性高，擁有相當高的移動能力，可以支援在各種移動商務環境中的行動支付服務與應用，比如說在巴士、火車、渡輪、遊艇等移動的交通運輸工具中，並且能克服在進行換手的狀況下的行動支付作業，包含基於 X2 的換手(X2-based Handover)、基於 S1 的 MME 內換手(S1-based Intra-MME Handover)、與基於 S1 的 MME-to-MME 間換手(S1-based Inter-MME Handover)與換手到關閉用戶群組或混和的家庭基站(Handover to a CSG/Hybrid HeNB)[40][41]。

由於 mPOS 成本低廉十分輕巧且攜帶方便，可讓諸如夜市或小型流動攤販得以隨處進行販賣，而精品賣家得以隨顧客移動以提供顧客更好的服務體驗，但在目前仍無任何研究討論在 LTE 網路上的 NFC 行動支付，而透過 mPOS 進行行動支付相較於傳統 POS 又有更多連結為非安全性的傳輸通道，因此我們認為應該要針對此部分做討論，以提供安全的 mPOS 行動支付系統，詳細系統架構如下。

第一節　系統架構與前置設定

在 LTE 行動網路上整合 mPOS 與掌上型 NFC 個人行動設備的系統架構圖可如圖 4-1 中所示，同時在此系統需要有幾項前置設定:

1. 所有的實體協議必須屬於相同的行動網路業者(MNO)，也就是說用戶行動裝置(UE)及 mPOS 資訊設備皆必須先向相同的行動網路業者進行註冊，其中支付閘道(PG)屬於行動網路業者後端系統的一部分。
2. 用戶行動裝置與 mPOS 皆須擁有 NFC 功能，並且透過一般規範電子錢包及行動裝置間互相交換資料的規範 ISO/ICE18092 進行溝通，其中 mPOS 為具備一定性的結帳機台，透過與 LTE 網路連線的在智慧型手機或平板安裝軟體以

擁有結帳功能，可讀取條碼或 RFID 標籤以計算購買金額並顯示購買資訊。

3. 用戶行動裝置必須開機且經過 LTE 行動網路認證，用戶行動裝置必須和 HSS 擁有相同的密鑰 K 與密鑰生成演算法，用來認證並產生加解密相關密鑰。

4. 行動網路業者後端系統中所有成員間連結均屬秘密頻道，而用戶行動裝置與 mPOS 之間、mPOS 與 eNB 之間均屬於非安全性的傳輸通道。

5. 支付閘道(PG)在行動網路業者後端系統架構中，作為認證用戶行動裝置與 mPOS 的主要角色，其同樣被定義在論文[6]中。

6. LTE 電信系統端的帳務中心(BC)為行動網路業者後端系統中，負責進行所有電話、簡訊及行動支付等相關帳務結算與紀錄的工作。

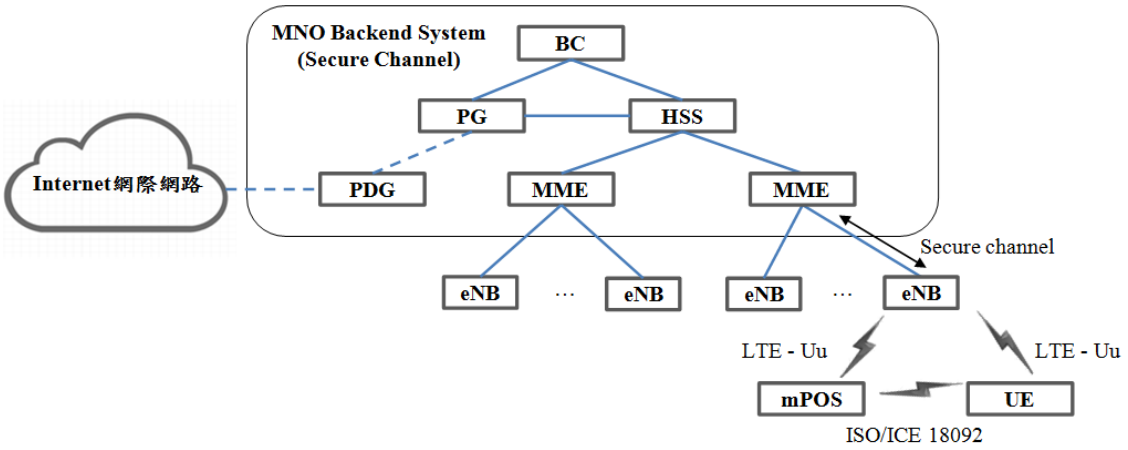


圖 4-1　LTE 系統上整合 mPOS 的系統架構

第二節　在 LTE 架構中的行動支付與認證流程

本論文將系統架構分為三個階段，如圖 4-2 中所示，前 5 個步驟為商品確認準備交易，價格確認在此部分進行，顧客可視覺上的確認商品價格是否有誤，並且決定是否繼續進行交易。接著第 6 至 18 步驟為相互認證階段，用戶行動裝置在這時與商家 mPOS 進行相互驗證。最後步驟 19 至 36 為交易執行，金錢的交易在此部分進行。

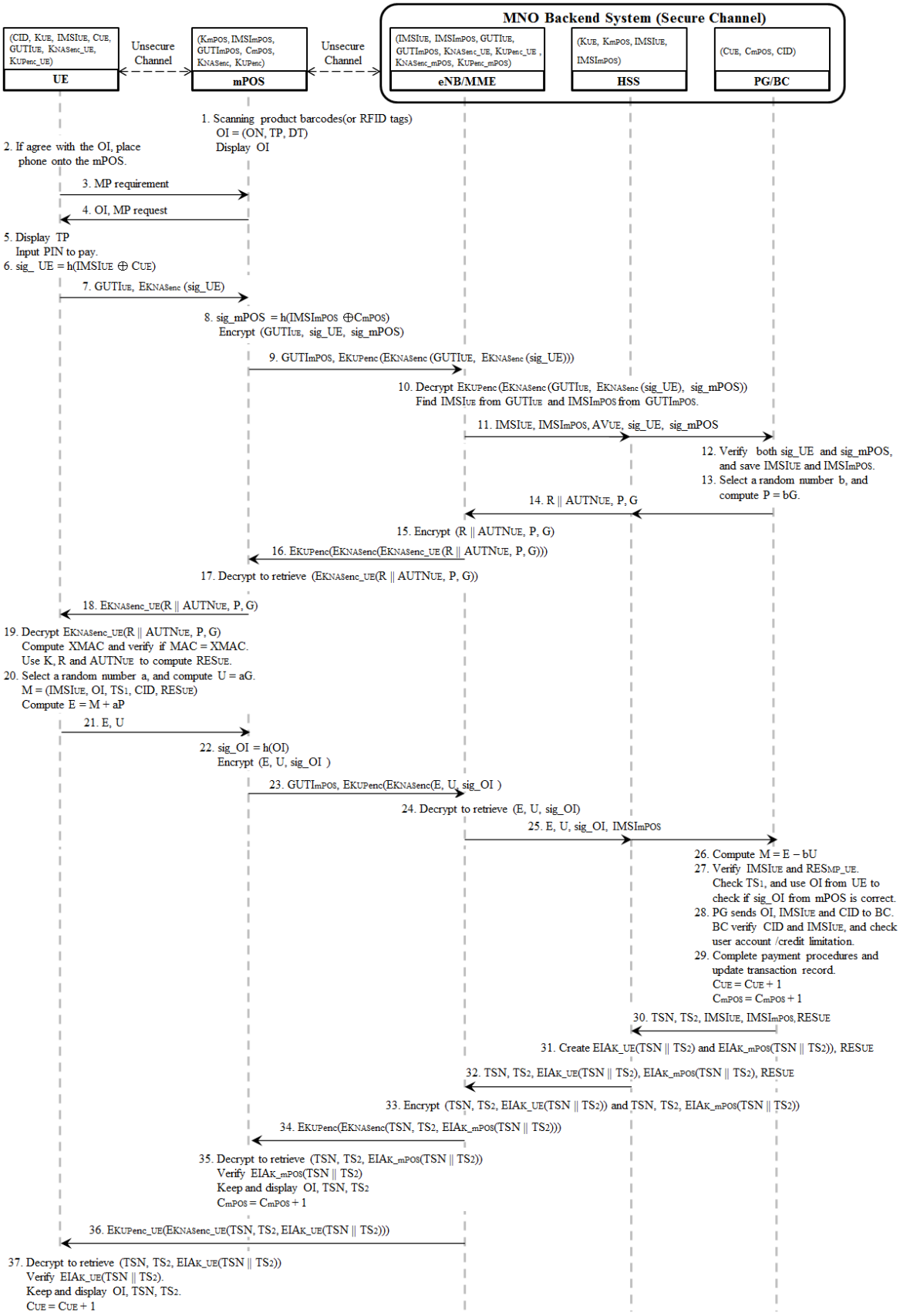


圖 4-2　NFC-LTE 在使用 mPOS 環境下的 DCB 行動支付流程圖

壹、商品確認準備交易

在此階段為顧客與商家開始交易時的準備動作，商家可隨顧客移動，使用 mPOS 將顧客選購的所有商品結帳，待此階段完全結束後才算是交易的開始，在此之前商家 mPOS 與顧客用戶行動裝置尚未有任何的資料往來。

步驟 1-2： 首先，商家使用 mPOS 掃描顧客所選擇的商品上的條碼(Barcode)或者 RFID 標籤(Tag)並且計算購買價格，接著由購買編號(ON)、總金額(TP)與日期時間(DT)組成購買資訊(OI)顯示在螢幕上讓顧客查看，在此商品資訊將被店家保存當作紀錄與交易證明，當往後發生爭議時可供查閱。

步驟 3-5： 顧顧客確認過 mPOS 上購買資訊內的總金額與日期時間後，須選擇用戶行動裝置中的行動支付服務，並將用戶行動裝置放置於 POS 上以開始 NFC 連結，接著用戶行動裝置會對 mPOS 發起行動支付需求傳送購買資訊給用戶行動裝置，在此時用戶行動裝置將會顯示購買資訊的內容，若顧客同意此筆交易，則在用戶行動裝置輸入行動裝置密碼(PIN)，此動作不僅是確認此用戶行動裝置確實為此顧客所有，同時也代表顧客是出於自我意識地同意了這筆交易。

貳、相互認證階段

在此階段中，用戶行動裝置將開始與後端系統進行相互認證，後端系統中的 MME 將會透過分別從用戶行動裝置與 mPOS 接收到的 GUTI 來判斷用戶行動裝置的身分，並且用戶行動裝置與 mPOS 的 IMSI、兩者經過赫序(Hash)所產生的簽章以及用作為後續認證用戶行動裝置的參數傳送給支付閘道，讓支付閘道可以辨識用戶行動裝置與 mPOS 的身分並且由簽章對兩者做認證。

步驟 6-9： 首先用戶行動裝置將 $IMSI_{UE}$ 與計數器(Counter UE, C_{UE})進行 Exclusive or (XOR)再經過赫序運算後製作成簽章 sig_UE，並將在 LTE 網路中暫時性代表自

身的參數 $GUTI_{UE}$ 與經過 NAS 層密鑰加密的 sig_UE 傳送給 mPOS，而 mPOS 也將利用與用戶行動裝置相同辦法產生自身的 sig_mPOS，接著將從用戶行動裝置接收到的訊息與自身簽章 sig_mPOS 一同使用 AS 層的 RRC 密鑰與 NAS 層密鑰進行加密，並附上 $GUTI_{mPOS}$ 一同傳送給 MME。

步驟 10-11 : eNB 與 MME 收到訊息後即使用相對的密鑰對訊息進行解密，接著由 MME 透過 $GUTI_{UE}$ 與 $GUTI_{mPOS}$ 分別尋找兩者相對應的 IMSI，並將兩者之 IMSI、簽章與讓支付閘道對用戶行動裝置作接下來認證的參數 AV 傳送給支付閘道，透過 IMSI 支付閘道可以辨識用戶行動裝置與 mPOS 身分是否被更改，而不會受換手時 GUTI 更改的限制。在步驟 10 中，若 MME 在步驟 10 中無法辨識用戶行動裝置之 $GUTI_{UE}$，則交易將失敗重新開始，表示用戶行動裝置可能在步驟 7 至 9 之間曾進行過換手流程，但由此段時間極短因此失敗機率將為極小，因此較不可能造成交易失敗。

步驟 12 : 支付閘道首先由接收到的用戶行動裝置與 mPOS 的 IMSI 與自身保存的用戶行動裝置與 mPOS 的 C 產生與兩者相同的簽章來分別驗證 sig_UE 與 sig_POS，若驗證成功則儲存兩者之 IMSI，並開始準備運用橢圓曲線密碼學的加密。

步驟 13-18 : 首先，支付閘道選取一個橢圓取線上的 G 點當作基準點，接著亂數選取一個數字 b 當作支付閘道在橢圓曲線加密法的私鑰，將 b 乘上 G 點產生公鑰 P 點，完成準備動作。接著支付閘道將要對用戶行動裝置進行驗證的參數 $R||AUTN_{UE}$、P 與 G 經由 MME 與 eNB 分別進行加密後經過 mPOS 解密交給用戶行動裝置。

步驟 19 : 接著，用戶行動裝置首先運算出 XMAC(Expect MAC)以對 MAC 做驗證，確認支付閘道是否屬於相同的行動網路業者，如果是則接著使用 K、R 與 $AUTN_{UE}$ 產生 RES_{UE} 與其加解密新密鑰。

參、交易執行

在此行動支付流程將邁入現金扣款的交易執行階段，用戶行動裝置與 mPOS 將分別傳送加密的購買資訊及經過過赫序的購買資訊以提供行動網路業者後端系統做交易資料比對，而交易結束後，行動網路業者後端系統也將傳送交易成功訊息給用戶行動裝置與商家 POS 以供保存與查證。

步驟 20-21 : 若要和支付閘道進行橢圓曲線加解密的資料交換，用戶行動裝置也必須產生一個亂數 a 當作橢圓曲線加密法的私鑰，並將 a 乘上橢圓曲線上的點 G 生成另一點 U 作為公鑰傳送給支付閘道。

接著顧客需對用戶行動裝置輸入身分證字號(Customer's Identify Number, CID)，而後用戶行動裝置將 $IMSI_{UE}$、購買資訊、時戳一(TS_1)、UID 與 RES_{UE} 製作成橢圓曲線上的點 E，接著將 E 與公鑰 U 一同傳送給 mPOS，其中計數器與時戳一是用來防止 replay attack，時戳一是交易資訊產生的時間，用來證明此交易是在期望的時間內進行。

步驟 22-25 : mPOS 將購買資訊使用赫序製作成簽章 sig_OI，接著將 E、U 與 sig_OI 加密後與 $GUTI_{mPOS}$ 一同傳送給 eNB 與 MME 做解密，而後將 E、U、sig_OI 與 IMSImPOS 傳送給支付閘道。

步驟 26-27 : 支付閘道將橢圓曲線加密的訊息 E 解密後得到訊息 M，並使用 $IMSI_{UE}$ 與 RES_{UE} 驗證用戶行動裝置身分，接著檢察時戳一是否正確，而後使用訊息 M 中的購買資訊與 sig_OI 相互驗證是否相符。

步驟 28-32 : 若來自用戶行動裝置與 mPOS 的資料皆正確，則支付閘道將購買資訊、$IMSI_{UE}$、顧客身分證字號與 $IMSI_{UE}$，傳送給帳務中心，供帳務中心驗證顧客身分證字號與 $IMSI_{UE}$ 並檢查使用者帳單/賒帳是否可完成此筆交易，如果顧客帳單合法交易將會進行。

交易進行完畢後並產生交易結果代號(TSN)與代表交易發生時間的時戳二(TS_2)，並交由 HSS 使用 K 及 LTE 內建的加密演算法 EIA 來製作交易結果憑證 $EIAK_{UE}(TSN||TS_2)$ 及 $EIAK_{mPOS}(TSN||TS_2)$，以保護資料的完整性以防攻擊者竄改此資訊，接著再將交易結果代號、時戳、交易結果憑證及 RES_{UE} 傳送給 MME。

步驟 33-37： 當 MME 收到 RES_{UE} 後則可開始與用戶行動裝置進行加密的資料傳輸，MME 與 eNB 分別將 $EIAK_{UE}(TSN||TS_2)$ 及 $EIAK_{mPOS}(TSN||TS_2)$使用用戶行動裝置及 mPOS 的密鑰進行加密，並於步驟 34 及 36 分別傳送至用戶行動裝置及 mPOS，而在步驟 35 及 37 中，用戶行動裝置及 mPOS 分別將訊息解密，並且對交易憑證作驗證，若驗證成功則分別將交易代號、時戳及購買資料顯示並保存，並將自身的計數器的內容將增加一完成交易。

第三節　安全情境分析

若要讓此系統可以安全的進行交易，則必須設想究竟有可能會遭遇到什麼樣的安全性問題，尤其是在交易進行的過程中將有金錢及顧客敏感資料的交換，無論是商家、顧客、或者竊取資料的中間人都有可能尋找此系統的漏洞進行攻擊，以從中獲取非法的利益，因此特別需要注重其安全性，在此本論文提出關於此此論文系統的安全性分析，並提出及改善論文[10]可能面臨的問題。本論文針對(1)資料完整性。(2)資料機密性。(3)交易匿名性。(4)交易參與者的身分認證。(5)不可否認性。以上幾點來進行分析。

壹、資料完整性：

在本論文系統中，所有金額時間及交易結果都經過了完整性加密的保護，在步驟 27 中，支付閘道可確認商品資料是否被顧客、商家或攻擊者修改。我們在步驟 20 中使用橢圓曲線加密訊息傳送給支付閘道驗證訊息的正確性，此方法可讓用戶行動裝置的機密資料 IMSI 及身分證字號被安全及完整的傳送，以供支付閘道及

帳務中心做認證，並且在步驟 31 我們使用 LTE 行動通訊系統的完整性保護運算 EIA 方程式搭配 K_{UE} 及 K_{mPOS} 分別為用戶行動裝置與 HSS 共有及 mPOS 與 HSS 共有的安全密鑰，攻擊者無法產生此憑證，達到更高的安全性。

貳、資料機密性：

當資料在用戶行動裝置與 POS 間交換資料為使用 NFC 技術，此技術優點在前面有描述過，僅允許在 10 公分以內進行交易，大幅降低中間人攻擊(Man-in-the-Middle)擷取交易資料，以冒充顧用戶行動裝置進行交易。但若商家與中間人勾結，資料將有可能被不法攻擊者擷取，因此本系統之機密資料在步驟 20 及 22 中分別使用了使用了橢圓曲線加密法及赫序，再加上 NAS 層及 AS 層加密保護。

參、交易匿名性：

在交易過程中，商家無法透過 mPOS 得知特定顧客的消費習慣，因顧客僅在步驟 7 對 POS 透露暫時代表自我身分的 GUTI。而支付閘道及其他行動網路後端系統無法得知顧客的詳細交易內容，僅能在步驟 26 中知道其購物金額、時間。

肆、交易參與者的身份認證：

在交易開始時，首先是用戶行動裝置用 PIN 的輸入對顧客進行認證，以確保該用戶行動裝置確實是屬於該顧客，接著才進行用戶行動裝置與後端系統之間的認證，透過在步驟 7 與 9 傳遞給後端的 $GUTI_{UE}$、sig_UE、$GUTI_{mPOS}$ 及 sig_mPOS，後端系統可得知用戶行動裝置及 mPOS 的身分並確認其合法性，因而產生相對應的認證參數回傳給用戶行動裝置，收到認證參數後，用戶行動裝置可在步驟 19 中驗證後端系統的 MAC 與 SQN，以此得知行動網路業者後端系統是否簽約於和自己相同的行動網路業者並具合法性，避免交易連結到非法的後端系統。

而後用戶行動裝置在步驟 21 將運算出的 RES 及自身擁有的 IMSI、計數器與

CID 將經橢圓曲線加密後回傳給行動網路業者後端系統，讓其得以確認用戶行動裝置身分，最後在步驟 31 中 HSS 將交易結果利用密鑰 K 做簽章提供用戶行動裝置及 mPOS 做再次確認，經過如此多重的驗證，防止中間人攻擊，避免資料被竊取及竄改。

伍、不可否認性：

也就是說若交易完成，則交易參與者無法否認此筆交易，步驟 5 中必須是由顧客輸入 PIN 到用戶行動裝置裡，由此可知該筆交易是經過顧客有意識的同意而開始的，步驟 25 由 PG 確認經過加密的時戳，避免攻擊者擷取並重複傳送資料導致重複扣款，防止重複攻擊(Reply Attack)。交易結束後，商家及顧客在步驟 32 與 34 中保留包含交易商品內容、時間、地點、金額的單據，以供未來有糾紛時提供查詢。

第四節　系統架構優缺點

壹、優點：

1. 本論文利用現存的 LTE 行動網路安全認證機制及其後端硬體設備，減少建置時間與成本，此系統之行動支付可以更容易的被行動網路業者、商家及消費者接受，較能快速的被普及。
2. 無論對於商家或是顧客，本系統都極易操作，顧客僅需透過用戶行動裝置與商家 mPOS 的接觸及可完成交易，並且交易資料會存在用戶行動裝置裡，供顧客透過用戶行動裝置確認購買的商品是否有誤。而商家也可保留交易號碼與商品內容，可做為往後查詢或規劃產品策略所用。
3. 此架構使用加密的計數器及時戳以防範重複攻擊(Reply Attack)，並且擁有多重認證機制可防範中間人攻擊。
4. 顧客可在交易結束後第一時間確認購買結果，商家與顧可彼此皆可儲存交易

結果以便往後有爭議時做為依據。

5. 掌管後端系統的行動網路業者將不會得知顧客的購物清單，僅能知道其購物金額、時間及地點，並且由於在資料傳輸時經橢圓曲線等加密保護，mPOS 將無法得知用戶行動裝置之 IMSI 以及密鑰 K 等機密資料。
6. 本論文使用了橢圓曲線加密法加密傳送 IMSI、CUE 與 CID 等機密資料給行動網路業者後端系統讓其對用戶行動裝置進行身分核對，由於橢圓曲線加解密法容許較大的資料加密傳輸，相較於論文[10]更加安全，並解決了其加密資料必須小於 128 位元長度的限制。
7. 我們使用 IMSI 做為再次認證用戶行動裝置身分的參數，用戶行動裝置將不會因為 GUTI 經過換手時更改或定時性的更換，而造成支付閘道無法辨認顧客身分，減少交易失敗的機會。
8. 此系統可以在支援移動的狀態中使用 LTE 行動網路進行安全的行動支付，提升商家的機動性。

貳、缺點：

1. 在行動支付的過程中，商家 mPOS 必須具備可使用 LTE 網路上網的功能，才能與後端系統連結與資料交換。
2. 認證階段透過用戶行動裝置內部的認證與密鑰協商協議進行用戶行動裝置認證，此過程將改變用戶行動裝置內部與基地台及 MME 溝通的參數，因此在行動支付的過程中無法接聽電話。

第五節　總結

在此章節中我們提出了在商家 mPOS 進行基於電信業者代收付款的行動支付模式，克服了 Chen[10]等人所提出的架構中加密的字元數限制及傳統 POS 移動性不高的缺點，並且由於透過電信系統進行資料交換，相較於傳統 POS 直接連接安全的 ADSL 實體線路網路有更多的安全風險，因此我們在此架構中更加地加強了

加密與簽章等安全驗證，並加入橢圓曲線加密演算法，使得交易資料能更安全的被保護，能防止中間人攻擊與重複攻擊，且兼具資料完整性、資料機密性、交易匿名性與不可否認性，顧客能更放心的使用本機制進行交易。

而對行動網路業者而言，此種機制不需要增設太多硬體設備，能節省建置成本，並且能幫助行動網路業者擴大市場，而對於小型攤販或流動攤販而言 mPOS 所需要花費的成本更小，能將擁有 LTE 網路功能的 NFC 行動裝置化為 mPOS，提供了更多讓商家與顧客面對面的機會，將能給顧客更好的服務體驗。

第五章　結論

如今行動支付技術發展成熟，行動裝置如智慧型手機、智慧手錶、平板等也越來越普及，並且習慣於使用行動支付的人口也越來越多，市面上各種行動支付方式如雨後春筍般越來越因應而生，而其中由於支援 NFC 功能的行動裝置日益普及，且透過行動裝置進行 NFC 付款的過程中，其交易距離短、配對快速、且可將資料進行加密的傳輸的特性，擁有較高的安全性，因此較容易被社會大眾所接受，各廠商如 Visa、MasterCard、Google、Apple 等均對 NFC 行動支付抱有相當大的期待，並於近年來紛紛開始投資此塊市場，造就了非接觸式 NFC 付款在近年來逐漸熱門起來，

第一節　研究回顧

而近年來 LTE 行動通訊網路也越趨普及，如前面章節所述，LTE 網路系統引入了許多新的安全架構與機制以達到較高的安全性，相較於 2G/3G 網路，LTE 網路系統更為穩定快速且安全，因此本論文提出了一個適用在 LTE 行動通訊網路上，可支援電信業者代收付款模式下提供行動支付交易服務的安全認證機制，藉由 NFC 行動設備和行動應用軟體 App 與商家的電信業者代收付款的行動支付機制，對於信用卡尚未普及的國家將有很高的吸引力，而對於信用卡已普及的國家而言，將增加一種付款方式，且能讓不習慣使用信用卡或未擁有信用卡帳戶的用戶如老人及兒童也可以方便的進行交易，

POS 為其中一種如今隨處可見的商家設備平臺，自 1960 年後被使用至今，經歷了許多世代的改進，成為我們現今在超商、量販店、圖書館、飯店等大大小小的店家隨處可見的設備平臺，目前已有許多學者針對此部分提出在 2G/3G 網路中透過 NFC 與傳統 POS 進行行動支付機制的研究[10][11][12][13][30]。而新興的行動收單終端(mPOS)，擁有較高的移動性且成本較低，對於小型攤販或流動型賣家有較高的吸引力，而如今尚未有學者針對此快問題做討論，因此本論文分別對於

使用傳統 POS 設備平臺與 mPOS 設備平臺上進行安全的行動支付交易進行討論。

我們使用 LTE 網路內部的認證與密鑰協商協議(AKA)使得 UE 與後端系統可以進行相互認證，讓 UE 及行動網路後端系統可以互相確認彼此身分，後續金錢交易進行時的二次身分認證，則是透過橢圓曲線密碼系統對機密資料 IMSI 與 C_{UE} 進行加密，由於 IMSI 並不會受 GUTI 定時更新的限制，將增加交易的成功機率，並且橢圓曲線密碼系統相較於 Chen[10]等人論文中使 f4()方程式進行完整性加密，有更高的安全性且其加密之訊息長度將不會被限制在 128 位元內，而最後由 HSS 使用密鑰 K 進行完整性加密交易結果以防傳送給 UE 的訊息被更改。

而在 NFC-LTE 行動裝置在 mPOS 上的安全認證機制中，我們同樣使用了 LTE 網路內部的認證與密鑰協商協議(AKA)使得 UE 與後端系統可以進行相互認證，讓 UE 及行動網路後端系統可以互相確認彼此身分，但由於 mPOS 與後端系統連結之網路為非秘密頻道，因此我們在這個部分增強了其安全性的認證，分別對 UE 和 mPOS 使用 IMSI 與 C 赫序產生簽章供行動網路後端系統認證兩者身分，並且利用 UE 與 mPOS 兩者的 NAS 層及 AS 層密鑰與 eNB 及 MME 進行加密訊息的交換，再透過橢圓曲線密碼系統加密 IMSI、C_{UE} 與 CID，提供 UE 安全的管道與後端系統間進行交易時的二次身分認證，而最後由 HSS 分別使用 UE 與 mPOS 的密鑰 K 進行完整性加密交易結果，以防分別傳給兩者之交易結果訊息被更改。

第二節　研究貢獻

在本論文中提出的兩個架構提供了分別在於傳統 POS 與新興的 mPOS 安全的付款機制並擁有以下貢獻：

1. 兩者皆進行了多重的認證與加密保護，尤其以在 mPOS 設備平臺上更進一步的使用 NAS 層及 AS 層的密鑰進行加密，可防禦重複攻擊與中間人攻擊，提供無論商家及顧客安全的交易環境。
2. 皆重複的利用了現存的 LTE 行動網路安全認證機制與其後端硬體設備，不需

在建置新設備上花費太多的成本，較能被行動通訊網路業者、商家與消費者接受進而快速的被普及。

3. 在系統使用上兩者都極易操作，顧客與商家皆可在交易結束後第一時間確認購買結果，並儲存作為交易的依據，並且商家可由儲存的資料進行分析已規劃產品策略，而行動通訊網路業者可得知顧客購買的金額、時間及地點，經過整理與規劃以在未來提供顧客更好的服務。

在此論文中對於 POS 的行動支付機制可應用於一般商店中，提供更加安全的行動裝置 NFC 支付方式，並且行動通訊網路業者可利用此架構推廣電信業者代收付款，增加一般大眾對於電信業者代收付款的熟悉度，電信業者可以與商家合作或者在電信業者所開立的商店中應用，由方便快速且不用太多註冊的交易模式吸引顧客使用此系統並成為常客。而在於 mPOS 設備平臺方面，則可應用在移動中的交易場合如巴士、輪船或流動攤販或任何可能會面臨 LTE 換手機制的場合，也可利用此系統可移動性高的特點，針對客戶進行隨身的商品講解，若顧客欲購買商品時，則可隨時隨地結帳，提供顧客更進一步的服務體驗。

第三節　未來研究方向與展望

我們認為應該可以在未來將全球最多人使用的 3G 網路與 LTE 網路的行動支付機制做上下世代的整合，雖然兩者後端網路系統差異甚大，但其後端系統的 VLR 與 MME 之間，擁有共同追蹤行動裝置以接通電話的功能，因此我們認為 LTE 網路上的行動支付將有機會與 3G 網路透過互相傳喚的的系統運作方式，互相交換資訊以進行行動支付，促成未來透過電信業者代收付款的行動支付系統能更加的被應用。並且我們期望能在未來對 2G~5G 等不同世代的網路架構作進行上下世代整合，並提出跨領域跨平臺的 NFC 行動支付架構，使顧客無論使用何種電信網路均使用此方案進行行動支付的交易，讓透過電信業者代收付款的 NFC 行動支付可以更加普及的被應用。

參考文獻

[1] NFC Forum, “What Is NFC? What It Does?”, NFC Forum, published at http://nfc-forum.org/what-is-nfc/what-it-does/, Mar, 2015

[2] E. Haselsteiner and K. Breitfuß, “Security in Near Field Communication (NFC), Strengths and Weaknesses”, Workshop on RFID Security, 2006.

[3] Smart Card Alliance, “The Mobile Payments and NFC Landscape: a U.S. Perspective”, Smart Card Alliance, published at http://www.smartcardalliance.org, 2011.

[4] Q. Zhang, “Mobile Payment in Mobile E-Commerce”, 7th World Congress on Intelligent Control and Automation, WCICA , pp. 6650-6654, 2008.

[5] G. Lao, and H. Liu, “Study of Mobile Payment Business Model Based on Third-party Mobile Payment Service Provider”, IEEE International Conference on Management and Service Science, pp.1-4, 2011.

[6] F. Cheng, G. Zhang and C. Meinel, “SIMPA: A SIP-based Mobile Payment Architecture”, 7th IEEE/ACIS International Conference on Computer and Information Science, pp. 287-292, 2008.

[7] H. Min, “The Study on the Security Services in Mobile Payment Systems”, 3rd International Conference on Convergence and Hybrid Information Technology, pp. 267-278, 2008.

[8] J.T. Isaac, S. Zeadally, “An Anonymous Secure Payment Protocol in A Payment Gateway Centric Model”, Procedia Computer Science, Vol. 10, pp. 758-765, 2012.

[9] Y.C. Tsai, “A Secure Billing-based Mobile Payment Protocol”, Master’s Thesis, National Central University Department of Information Management, 2005.

[10] W.D. Chen, G.P. Hancke, K.E. Mayes, Y. Lien, and J.H. Chiu, “Using 3G network components to enable NFC mobile transactions and authentication”, IEEE International Conference on Progress in Informatics and Computing, Vol. 1, pp. 441-448, 2010.

[11] P. Pourghomi, M.Q. Saeed, and G. Ghinea, “A Proposed NFC Payment Application”, International Journal of Advanced Computer Science and Applications, Vol. 4, No. 8, pp. 173-181, 2013.

[12] T. Ali and M. Abdul Awal, “Secure Mobile Communication in M-payment System Using NFC Technology”, Proceedings of the International Conference on Informatics, Electronics & Vision, pp. 133-136, 2012.

[13] P. Pourghomi, M.Q. Saeed, and G. Ghinea, “A Secure Cloud-based NFC Mobile Payment Protocol”, International Journal of Advanced Computer Science and Applications, Vol. 5, No. 10, pp. 24-31, 2014

[14] ISOIIEC 18092 (ECMA-340), “Information Technology - Telecommunications and Information Exchange Between Systems - Near Field Communication - Interface and Protocol (NFCIP-l)”.

[15] ISO/IEC 14443, “Identification Cards - Contactless Integrated Circuit Cards - Proximity Cards”.

[16] ISO/IEC 15693, “Identification Cards - Contactless Integrated Circuit Cards - Proximity Cards”.

[17] FeliCa, published at http://www.sony.net/Products/felica/.

[18] Android Developers, “Host-based Card Emulation”, published at http://developer.android.com/guide/topics/connectivity/nfc/hce.html/, 2014

[19] EMVCo Contactless Mobile Payment, “Contactless Mobile Payment Architecture Overview Version 1.0”, June 2010.

[20] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS) (Release 11)”, 3GPP TS 23.228 V11.6.0 , Sept. 2012.

[21] GPP TS 36.300, “Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN) (Release 10)”, V10.3.0, March 2011.

[22] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Service and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture (Release 12)”, 3GPP TS 33.401 V12.5.0, Sept. 2012.

[23] J. Cao, M. Ma, H. Li and Y. Zhang, “A Survey on Security Aspects for LTE and LTE-A Networks”, in IEEE Communications Surveys & Tutorials, Vol. 16, Issue 1, pp. 283-302, 2013.

[24] M. Al-Humaigani, D. Dunn, and D. Brown, ”Security Transition Roadmap to 4G and Future Generations Wireless Networks,” Proc. 41st Southeastern Symposium on System Theory (SSST 2009), pp.94-97, 2009.

[25] M. Aiash, G. Mapp, A. Lasebae, and R. Phan, ”Providing Security in 4G Systems: Unveiling the Challenges,” Proc. Sixth Advanced International Conference on Telecommunications (AICT), pp.439-444, 2010.

[26] T.S. Chen, T.P. Liu., and Y. F. Chung., “A Proxy-Protected Proxy Signature Scheme Based on Elliptic Curve Cryptosystem’, Proceedings of IEEE TNECON’02, pp.184-187, 1997.

[27] N. Koblitz, “Elliptic curve cryptosystems”, Mathematics of Computation, Vol. 48, No. 177, pp. 203-209, 1987.

[28] J.J. Botes and W.T. Penzhorn, “Public-key Cryptosystems Based on Elliptic Curves”, Proceedings of IEEE South African Symposium on Communications and

Signal Processing, 1993.
[29] J. Menezes, “Elliptic Curve Public Key Cryptosystems”, Kluwer Academic, 1993
[30] W.D. Chen, G.P. Hancke, K.E. Mayes, Y. Lien, and J.H. Chiu, “NFC Mobile Transactions and Authentication Based on GSM Network”, NFC, 2nd International Workshop on Near Field Communication, pp.83-89, 2010
[31] W.D. Chen, “Secure e-Payment Portal Solutions Using Mobile Technologies and Citizen Identity Scheme”, Ph.D. Dissertation, Department of Mathematics at University of London, 2013
[32] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN); Overall description, (Release 11)”, 3GPP TS 36.300 V11.3.0, Sept. 2012.
[33] 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Home Node B (HNB) and Home eNode B (HeNB) (Release 11)”, 3GPP TS 22.220 V11.6.0, Sept. 2012.
[34] D. Astely, E. Dahlman, A. Furuskar, Y. Jading, M. Lindstrom, and S. Parkvall, “LTE: The Evolution of Mobile Broadband”, IEEE Communications Magazine, Vol.47, No.4, pp.44-51, 2009
[35] S. Smith “Digital Content Opportunity to Deliver $14bn Revenues for Operators by 2019”, Press releases of Juniper Research, published at http://www.juniperresearch.com/press/press-releases/digital-content-opportunity-deliver-14bn-revenue?utm_source=gorkanapr&utm_medium=email&utm_campaign=contentbusinessmodels15pr1, 2015.
[36] J. Abraham, J.V.D. Lande “Direct Carrier Billing : Giving CSPS a Share of the Mobile Payments Market”, Strategy report of Analysys Mason, published at http://www.analysysmason.com/Research/Content/Reports/direct-carrier-billing-Mar2013-RMA03/#01%20March%202013, 2013.
[37] N. Afonso, “Direct Carrier Billing has the Greatest Potential for Success in Emerging Markets”, Article of Analysys Mason, published at http://www.analysysmason.com/About-Us/News/Insight/DCB-emerging-markets-Jun2014/#03%20June%202014, 2014

附錄一　字彙表

2G	2nd Generation Mobile Communication	第二代移動通訊
3G	3rd Generation Mobile Communication	第三代移動通訊
3GPP	3rd Generation Partnership Project	第三代合作夥伴計畫，為國際標準化機構，其標準化包括了無線電、核心網路及服務架構。
AKA	Authentication and Key Agreement	認證與密鑰協商協議，行動裝置接入網路時的認證程序。
AS	Access Stratum	存取層，指 UE 與 eNB 之間的連線。
AuC	Authentication Centre	認證中心
AUTN	Authentication Token	認證代碼，包含了 SQN⊕AK 與 MAC，在 AKA 時傳送給用戶行動裝置以供相互認證。
AV	Authentication vectors	資料鑑別向量，為 AKA 認證用參數，包含了 RAND、XRES、AUTN 及 KASME。
BC	Billing Centre	帳務中心，為電信業者統計彙整所有顧客帳單之處。
DCB	Direct Operator Billing	電信業者代收付款，由電信業者代為收款並將交易帳單與電信帳單合併付款。
ECC	Elliptic curve cryptography	橢圓曲線密碼系統
eNB	Evolved Node B	基地台，為 LTE 接入網路連接 UE 之設備，主要負責無線資源管理。
EPC	Evolved Packet Core	演進的核心網路，包含了 MME、SGW、PGW 與 HSS 等。
E-UTRAN	Evolved-Universal Terrestrial Radio Access Network	演進的 UMTS 陸面無線接入網路，包含了 UE 與 eNB。
GSM	Global System for Mobile Communication	全球移動通信系統
GUTI	Globally Unique Temporary Identity	全球唯一臨時標識，由 MME 分配，為代表 UE 的臨時性編號。

HeNB	Home eNode B	家庭基站，小型的基地台，可為公司或住家擁有。
HSS	Home Subscriber Server	歸屬用戶伺服器，其內資料庫包含用戶設定檔，以便執行用戶身分驗證與授權。
IMSI	International Mobile Subscriber Identity	國際移動用戶識別碼，為 UE 唯一不變的識別碼。
LTE	Long Term Evolution	長期演進技術
MAC	Message Authentication Code	訊息認證碼，用做為讓 UE 辨識 MME 的身分的參數。
MME	Mobility Management Entity	移動性管理組件，負責管理控制訊號及管理 UE 與其 LTE 建立連線時的維護、行動管理以及安全性相關參數。
MNO	Mobile Network Operator	行動網路業者
mPOS	Mobile Point of Sale	行動收單銷售終端
NAS	Non-access Stratum	非存取層，指 MME 與 UE 間的安全連線。
NCC	Next Hop Chaining Counters	下一跳密鑰計數器，為換手時密鑰產生的計數器。
NFC	Near Field Communication	近場通訊
NH	Next Hop key	下一跳密鑰，在換手過程中用作為推導新的 KeNB 的密鑰。
PG	Payment Gateway	支付閘道，負責處理行動支付過程中來自資料傳輸及認證。
PGW	Packet Data Network Gateway	數據封包網路閘道器，功能包含 UE 的 IP 位址分配，針對各個用戶之封包進行過濾及監聽。
POS	Point of Sale	銷售點終端
RAND	Random Number	隨機亂數，為 AKA 中產生新密鑰的參數。
RES	Response	回應值，為 AKA 中使 MME 確認 UE 身份之參數。

RFID	Radio Frequency Identification	無線射頻辨識技術
RRC	Radio Resource Control	無線資源控制，UE 獲取空中資源的過程中與 eNB 的溝通。
SGW	Serving Gateway	服務閘道，負責路由和傳送用戶所有的 IP 封包資料，
SQN	Sequence Number	序列號碼，為 AKA 中 UE 認證 MME 之參數之一。
TAI	Tracking Area Identity	追蹤區域辨識，表示 UE 在 LTE 網路中位置之參數。
TS	Time Stamp	時戳，用作於防止重複攻擊。
TSN	Transaction Number	交易結果代號，在交易結束後用來代表交易結果的唯一編碼。
UE	User Equipment	用戶行動裝置
UMTS	Universal Mobile Telecommunications System	通用移動通訊系統，是當前最廣泛採用的一種 3G 行動電話技術。
UP	User Plane	使用者面，負責用戶訊務的處理，例如封包切割、重組和轉送等功能。
USIM	Universal Subscriber Identity Module	全球用戶識別卡
XMAC	Expected Message Authentication Code	預期的訊息認證碼，AKA 中用來與 MAC 做對照的認證參數。
XRES	Expected Response	預期的回應值，AKA 中用來與 RES 做對照的認證參數。