基植於 NFC 系統之匿名行動付款協定

An NFC-Based Anonymous Mobile Payment Protocol

羅嘉寧
銘傳大學電腦與通訊工程學系
桃園縣 333 龜山鄉德明路 5 號
deer@mail.mcu.edu.tw

楊明豪
中原大學資訊工程學系
桃園縣 320 中壢市中北路 200 號
mhyang@cycu.edu.tw

摘要

本論文提出一個以 NFC 為基礎之匿名行動付款協定，以 NFC 手機中的安全元件及手機之可信賴之執行環境，發展出一個具備認證(Authentication)、授權(Authorization)及稽核(Audit)的匿名行動付款系統。使用者必須先向其往來銀行註冊並配發一虛擬帳戶存於 NFC 手機之安全元件中，再利用該虛擬帳戶向公信的第三者(TSM)申請具有特定信用額度之虛擬信用卡。當虛擬信用卡之有效期限將至，TSM 會重新配發另一虛擬信用卡給使用者。而當帳戶之餘額低於銀行之授信額度時，TSM 將要求使用者重新進行授信。

本系統具有以下特點：(1)便利性：本協定與 EMV 標準相容，使用者僅需擁有 NFC 手機即可取代信用卡、現金。(2)不可連結性：使用者消費時，商家只會拿到一具短時效之虛擬信用卡資訊，無法從多次交易紀錄分析並連結至使用者身份。TSM 雖擁有使用者之消費資訊，然而其僅擁有使用者提供之銀行匿名帳戶，無法得知真實使用者之銀行帳戶資訊。而銀行端亦僅能得知使用者利用 TSM 付款，並無法得知使用者之消費紀錄。(3)匿名性：除銀行知曉使用者之真實身分外，使用者對 TSM 及商店皆匿名。(4)不可否認性：所有之帳戶註冊訊息、虛擬信用卡之製作及交易訊息皆須進行數位簽名，達成不可否認性。

關鍵詞：NFC、MTM、TEE、EMV、匿名付款系統

Abstract

We propose a new anonymous payment protocol for current NFC-based mobile payment services. Our scheme combines NFC phones' built-in secure element (SE) with the trusted execution environment (TEE) and mobile trust module (MTM) to create a reliable execution environment. It is designed to achieve authentication, authorization and audition for anonymous mobile payment services. Firstly users have to apply for a virtual account from an issuing bank and to store it in the SE. Then they use the account to apply for a virtual credit card from a trust service manager (TSM). The card has only limited credits and has to comply

with EMV standards. If the card is going to expire, TSM will issue a new one to the user. When the account balance is lower than the credits, TSM will require the user to re-apply for new authorization.

The main contributions of our protocol include: (1) Convenience. Our protocol complies with EMV standards and it allows users to take their NFC-enabled cellphones as credit cards or e-cash for transactions. It is convenient and fast. (2) Unlinkability. During a transaction, merchants can only receive the information of a temporary virtual credit card. They cannot analyze transaction records to find any links between users' identity and the records. Although the TSM keeps consumers' transaction records, it can only find users' anonymized bank accounts. It is unable to know users' real accounts. And the banks can only know their users pay through a TSM, but they cannot access their transaction records. (3) Anonymity. Users' real identity is only known to their banks. It is kept anonymous to merchants and the TSM. (4) Undeniability. Digital signatures are required for every account registration, virtual credit card application, and transaction, so as to achieve undeniability.

Keywords: NFC, MTM, TEE, EMV, Anonymous Payment

一、緒論

隨著無線網路和行動通訊的快速發展，及智慧型手機、平板電腦之大量普及，行動電子商務 (Mobile Commerce, M-commerce)[7][9]亦隨之盛行。行動電子商務[4]使用者可利用隨身攜帶之智慧型手機或平板電腦於開放的網路環境下進行各種商貿活動，如網路購物、網路拍賣、影音租賃、線上電子付款等。

對於一般使用者而言，行動電子商務之導入將會提高個人生活的方便化、自由化、與個人化；對於企業而言，導入行動電子商務將增加顧客資訊的正確性與效率性，並藉著準確的顧客分析進而得以提高顧客的忠誠滿意度。

然而在行動電子商務中，付款機制一直是一個重要議題。雖然現今之智慧型手機已可提供強大運算能力和存儲能力，然而付款機制大部分仍沿用傳統付款方式：如使用貨到付款、自動提款機（ATM）轉帳、信用卡、小額電子貨幣儲值等。近年來許多學者提出行動付款[4][5][6][10][11][13]機制，希望使用者能透過簡單的操作並能夠進行個性化的應用程序，以滿足使用者的快速付款需求，以取代信用卡或現金等傳統付款機制，增加消費者於付款上之便利性。此外行動付款服務同時也增加了商家和消費者互動的管道：商家可以藉由行動付款，推出更加豐富、個人化的廣告和折扣方案；行動付款也將進一步刺激行動商務，創造更多的應用和商業模式。

在各種行動付款之機制中，Chen 等人[6]提出以 3G-UMTS 為基礎之付款機制，方法側重於傳統的店內付款環境，與實體和隨後的值得信賴的交易正在通過 3G 和 USIM 安全服務之間的相互驗證。用簡單的方法來實施，同時提供合理的安全保護，以及便於用戶使用的移動支付系統。行動付款應用程序正在開發的在線和店內購買，近場通信（NFC）技術允許在現有的非接觸式應用的基礎設施，如銷售點終端（POS）用手機付款為一體的移動設備。結合現有的 3G 加密演算法，除了 USIM 卡的標識和認證功能的，與 NFC 技術來實現一個行動付款系統。系統可以用當前的 3G 基礎設施，並提供更好的

可擴展性和無處不在的行動付款服務。使用交易正在通過 3G 和 USIM 安全服務之間的相互驗證，因此消費交易隱私全曝露在電信業者，電信業者可從多次交易紀錄分析並連結至使用者身份。

Toorani 等人[15]提出一個安全的簡訊行動付款協議，以簡訊付款則是另一種經由手機購物的方式。以小額交易，沒有能力設置專屬的金流服務平台，就可以透過簡訊付款來交易。消費者只要鍵入手機號碼，商家將會利用交換簡訊的方式，讓消費者確認交易金額。這筆金額最後會出現在消費者的手機賬單，消費者不需要動用現金或信用卡。交換簡訊缺點重覆傳送交易訊息、偽造的交易簡訊。

另外 NFC（近場通訊）是時下最受矚目的行動付款技術，如電子錢包，為用戶提供行動付款服務，還得保證隱私安全性。

Martínez-Peláez 等人[13]提出小額行動付款協議：提款和付款匿名，利用匿名電子現金基礎上使用小額行動付款的實用的協議，為客戶提供匿名性和不可連結性。移動在協議中使用的現金，可以是不同的價值及面額。經由銀行簽署它與特定的私鑰。該銀行存儲電子現金的值和對應的公鑰之間的關係。該協議避免重複消費和偽造攻擊。客戶可以使用匿名證書進行身份驗證使用 WTLS 協議不透露個人信息。銀行擁有使用者之消費資訊，得知客戶消費資訊的隱私。

Kungpisdan 等人[12]基於安全帳戶的行動付款協議，提出一個安全帳戶為基礎的付款協議，這是適用於無線網絡。擬議的協議採用對稱密鑰的操作要求較低的計算在所有參與方比現有的支付協議。擬議的協議也滿足基於公共密鑰的付款協議，如 SET 和 IKP 交易安全性能。

廖[1]提出跨網域之匿名行動付款機制，在行動通訊中讓使用者與不同商家進行消費，消費方式用可分割的電子現金，提供使用者匿名性需求，在手機網域進行消費付款，也讓電信業者保有電子現金發行權，提升現實環境的可行性，採用離線驗證和支後追蹤達成付款驗證。電信業者知道使用者的付款記錄，存放手機電子現金安全保護。商家從多次交易紀錄分析並連結至使用者身份。

Molloy 等人[14]提出虛擬信用卡機制，提出一個動態的虛擬信用卡號碼，減少所造成的損失由偷來的信用卡號碼。用戶可以使用現有的信用卡帳戶生成多個虛擬信用卡號碼，是一個單一的交易中使用或特定商戶。

廖等人[2]提出整合型電子票證機制之研究，整合電子票卷與電子錢幣之應用，提出具有電子票卷與電子錢幣功能之票證機制，結合行動設備與資訊安全技術的應用，讓原有行動設備晶片卡，擁有儲存電子票卷的資訊，節省實體票卷交付過程，消費者隱私權的完整保障。

目前行動付款在安全隱私與信任、及行動付款機制牽涉了手機硬體、軟體、金融業、電信業、零售商家、消費者各個層面上的整合，使系統能與其他系統的交互應用是為討論話題，一位使用者必須能夠信任的行動付款應用程序的供應商，信用卡或卡片信息不被濫用。當這些交易成為記錄客戶的隱私是否應該為優先，客戶的信用記錄和消費模式的不應該公開給公眾的監督。

NFC 的通訊晶片，已經有詳細的規格制定；相反地，安全元件和軟體方面，則提供相當大的發揮空間。尤其是安全元件 SE 決定了 NFC 手機的功用和效能，因此我們硬體

基於安全硬體平台的安全性使用可信任執行環境 TEE 確保安全元件 SE 環境安全。MTM 要求行動通訊裝置的安全性，檢查行動裝置測量系統完整性。兼容 EMV 支付款系統。

由於 NFC 付款也牽涉到資訊安全、資料處理架構、硬體基於安全硬體平台的安全性等各方面的技術。

本論文提出以 NFC 為基礎之匿名行動付款協定。在我們的協定中，使用者必須先向其往來銀行註冊帳戶，銀行會配發虛擬帳戶給使用者並存在使用者 NFC 手機之安全元件中。使用者利用該虛擬帳戶向公信的第三者 (TSM) 申請具有特定信用額度之虛擬信用卡。TSM 會向使用者之往來銀行確認虛擬帳戶之正確性及有效性，接著簽發一張具有短時效及少於使用者之信用額度之虛擬信用卡並存在使用者之安全元件中。該配發之虛擬信用卡須滿足 EMV 協定之所有要求。隨後，使用者可以使用 NFC 之 Card-Emulation Mode 進行交易。TSM 將維護使用者之虛擬信用卡帳戶之餘額及有效期限。當虛擬信用卡之有效期限將至時，TSM 會重新配發另一虛擬信用卡給使用者。而當帳戶之餘額低於銀行之授信額度時，TSM 將要求使用者提供另一銀行之虛擬帳戶以重新進行授信。

本論文預期達到以下特性：(1)便利性：使用者僅需擁有 NFC 手機取代信用卡、現金，減輕消費者出門的負擔，加快結帳速度。(2)不可連結性：商家只會拿到一具短時效之虛擬信用卡資訊，無法從多次交易紀錄分析並連結至使用者身份。TSM 雖擁有使用者之消費資訊，然而其僅擁有使用者提供之銀行匿名帳戶，無法得知真實使用者之銀行帳戶資訊。而銀行端亦僅能得知使用者利用 TSM 付款，並無法得知使用者之消費紀錄。(3)匿名性：除銀行知曉使用者之真實身分外，使用者對 TSM 及商店皆匿名。(4)不可否認性：所有之帳戶註冊訊息、虛擬信用卡之製作及交易訊息皆須進行數位簽名，達成不可否認性。

二、相關文獻

本章描述 NFC 手機匿名行動付款匿名機制一些需求，介紹包含 NFC 近場通訊之基礎架構，及 EMV 協定之基礎。

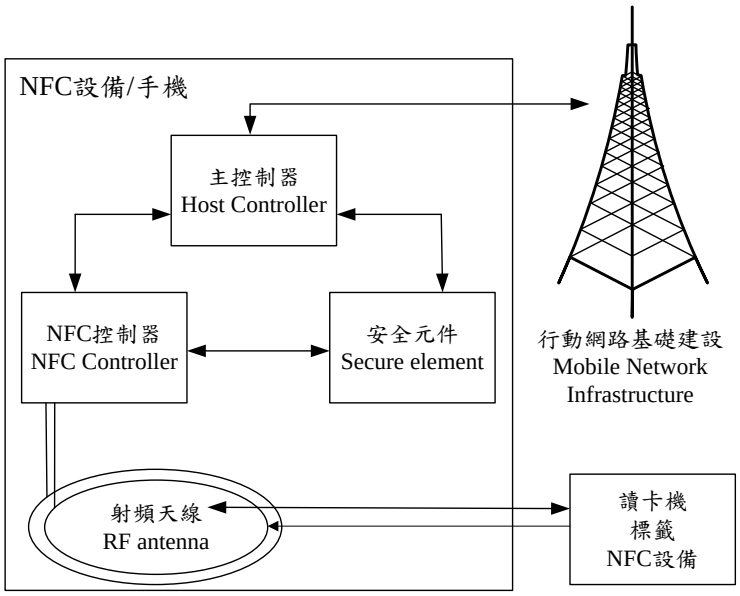
1. NFC 近場通訊

NFC 手機是目前常見結合 NFC 技術的電子產品，將原有的手機架構加上智慧卡安全晶片和 NFC 晶片，使得手機擁有更多應用功能。NFC 手機中的硬體元件如圖一所示：

- 安全元件(Secure Element, SE)：主要用來儲存重要資訊，例如：使用者帳戶資料、錢包餘額、PIN 碼、金鑰等。它也可以運算程序、儲存數據，且只允許可信任軟體存取資料，所以惡意軟體並不能存取到安全元件裡的數據資料。為了保護所儲存的數據資料的安全，安全元件與手機的作業系統和硬體是各自獨立的，，藉由儲存於安全元件中的私密金鑰將傳送資料加密，確保與外界溝通是以加密形式傳輸，保證資料的安全。
- 主控制器(Host Controller)：負責行動裝置與 NFC 控制器之通訊傳輸，主控制器亦可至安全元件存取資料。
- NFC 控制器(NFC Controller)：NFC 控制器為主控制器(Host Controller)、安全元件之

橋樑，並透過射頻天線收發訊號透過 NFC 控制器傳輸所需數據、資料等。

- 射頻天線(RF antenna)：負責發送和接收射頻訊號。



圖一: NFC 手機架構

NFC 硬體安全上的架構，安全元件 SE 是三種不同的組合，NFC 手機設備被嵌入到一個專門的晶片 ，由 NFC 控制器組合成單一晶片 。

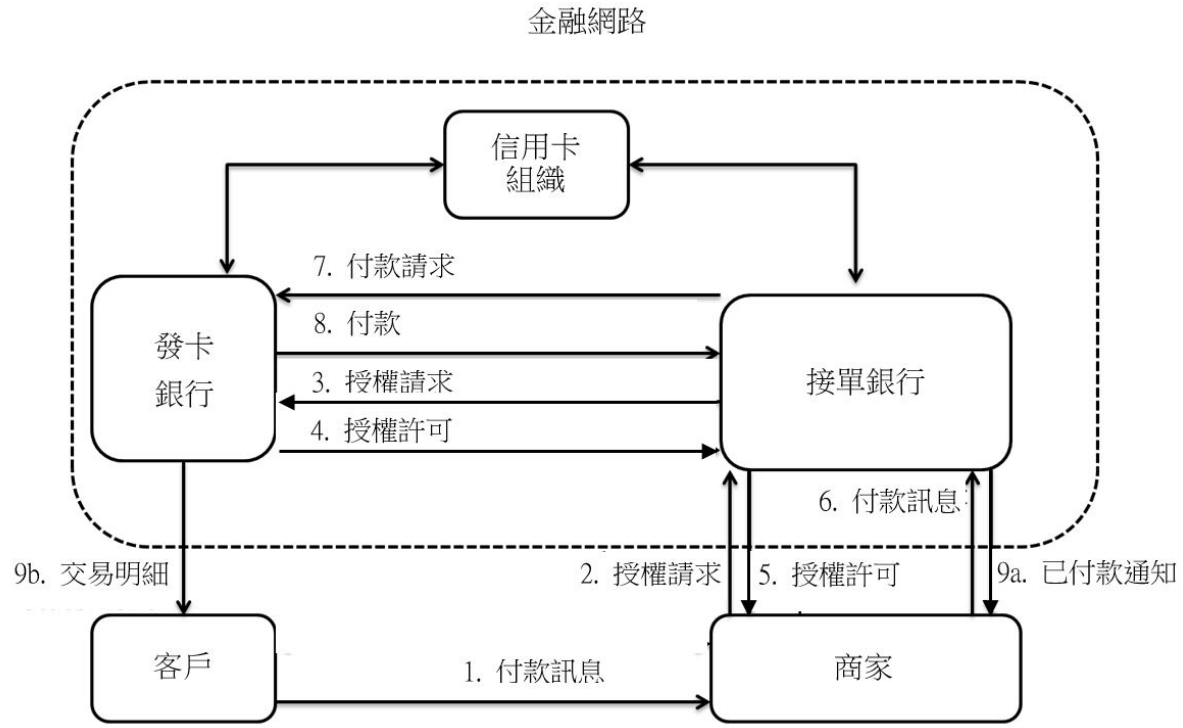
2. Europay-Visa-Mastercard (EMV)

EMV [3][8]來自於（Europay）、萬事達卡（MasterCard）與威士卡（VISA）三大國際組織英文名稱的字首所組成在 1993 年開始共同制定用於付款的 IC 卡通用規範。EMV 是國際金融業界對於智慧卡與可使用晶片卡的 POS 終端機，以及銀行機構所廣泛設置的自動櫃員機等所制定的專業交易與認證的標準規範，主要任務係發展制定與主管維護 EMV 支付晶片卡的規格、標準與認證，監督並確保該標準於全球的安全互通性與其付款環境的可用性，是針對晶片信用卡與現金卡的支付款系統（Payment System）相關軟硬體所設置的標準。此三大組織於 1999 年 2 月共同成立之 EMVCo 組織，負責維護 EMV 規範、EMV 測試流程和案例。此國際標準規範中對於晶片卡的介面標準則有相當比例係根據 ISO 7816。

EMV 支付款系統處理模型為四個角色如圖二所示。客戶擁有 EMV 標準的晶片卡，由發卡銀行所發行；商家 POS 終端機與收單銀行註冊。銀行間透過金融網路交換授權及付款訊息。

- 步驟 1：客戶可以使用該晶片卡在商家進行交易。
- 步驟 2-5：商家根據客戶提供之晶片卡資料，透過收單銀行向客戶的發卡銀行請求授權。發卡銀行會回覆該授權請求是否被接受。
- 步驟 6-9：商家經由收單銀行要求進行清算交易。發卡銀行將款項傳送到收單銀行之商家賬戶中，並向使用者收取款項。

我們依照 EMV 標準的晶片卡規範，將用 NFC 產生晶片卡，交易流程兼容 EMV 支付款系統。



圖二: EMV 協議流程圖

三、以 NFC 為基礎之匿名行動付款協定

本章我們提出我們的方法-以 NFC 為基礎之匿名行動付款協定，適用 NFC 手機進行匿名行動付款協議機制，整個機制包含 (1) 系統初始化；(2) 申請銀行虛擬帳戶階段；(3) 申請 TSM 信用卡帳戶階段；(4) 虛擬信用卡簽發階段。

系統角色介紹如下：

- 銀行 B：銀行提供使用者帳戶，與可信服務管理進行請款與付款之行為。
- 使用者 U：持有 NFC 手機使用者簡稱使用者，使用者個人身份、資訊，與銀行申請帳戶，主要利用 NFC 手機模擬信用卡，並使用利用 NFC 手機進行匿名的行動付款。
- 安全元件 SE：NFC 手機中的安全元件，通常與使用者綁在一起，SE 提供安全的存放空間及運算並產生金鑰。
- 可信服務管理 TSM：提供匿名信用卡服務並管理，為公信的第三方，與使用者進行認證並簽發信用卡匿名授權；與銀行取得驗證匿名授權及請款；與商家進行認證提供交易服務。
- 商家 M：商家。

我們提出之以 NFC 為基礎之匿名行動付款協定架構具備以下五個部分：

1. 系統初始化：協定初始化設定，主要是產生此交易付款系統於運作中所需之參數和資訊。
2. 申請銀行虛擬帳戶階段：使用者向銀行申請一虛擬帳戶，並取得授權。
3. 申請信用卡帳戶階段：使用者向 TSM 提出交易帳號註冊需求，並提供銀行所簽發之虛擬帳戶資訊以供驗證。TSM 向銀行驗證使用者之授信額度後，配發

一信用卡帳戶給使用者。

4. 虛擬信用卡簽發：使用者請求 TSM 配發一短時效之虛擬信用卡，並將其存放在 SE 之中。

1. 符號表

表一列出本文所使用到的符號/代號及其解釋：

表一: 符號表

IDx	*x* 身份識別碼如：ID_{SE} 為使用者(安全元件)身份識別碼，ID_U 使用者的身份識別碼，ID_B 銀行業者的身份識別碼。
AIDi	銀行給使用者的匿名識別碼
TIDi	使用者給 TSM 的匿名識別碼
PKx	每個角色 *x* 的公開金鑰
SKx	每個角色 *x* 的私密金鑰
SID	會議身份識別碼
$CERT_{IDY}^{X}$	*x* 角色發行的憑證：如 CA 發給銀行的憑證$CERT_B^{CA}$，銀行發給使用者的匿名識別碼的憑證$CERT_{AIDi}^{B}$
$K_{x,y}$	角色通訊者 *x* 與角色通訊者 *y* 角色之間的通訊金鑰
SIGN(*SKx*,*M*)	用 *x* 私密金鑰簽章
$Nonce_Z$	隨機數
‖	訊息連接符號
E(*key*,*M*)	用 key 加密訊息 *M* 的加密函式
D(*key*,*M*)	用 key 解密訊息 *M* 的解密函式
X_ExpTime	*X* 的憑證到期時間
X_Limit	*X* 的信用額度
BINFO	由安全元件產生給銀行之付款訊息
TSMINFO	使用者產生給 TSM 之交易訊息
TSMBINFO	TSM 產生給銀行之交易驗證訊息
AuthDATA	驗證訊息
Status	驗證訊息狀態，成功/失敗
TIDi_CerditINFO	憑 EMV 發行之虛擬信用卡的相關資訊
TIDiList	TSM 用來記錄匿名帳號信用授權表

2. 系統初始化

在初始化設定時，安全元件、使用者、銀行和可信服務管理 TSM，都各自擁有唯一的識別碼：ID_{SE}、ID_U、ID_B、ID_{TSM}。每一個角色的識別碼皆有一組非對稱式金鑰對(PK_{ID}, SK_{ID})，且公開金鑰皆經過 CA 所簽署，並存放於 PKI 架構中。

在系統開始時，使用者需要先向其往來銀行開立信用卡帳號，並持 NFC 手機至銀行註冊。銀行會透過安全通道將 NFC 手機平台檢查碼用 SK_{SE} 簽名過的 PCR 驗證通行碼

和 Measurement List 訊息與安全元件所產生之公開金鑰 PK_U 存放於放置於銀行伺服器中，銀行並會為此公開金鑰 PK_U 簽發一憑證$CERT_U^B$並建立彼此之間的通訊金鑰 $K_{B,U}$。使用者有 NFC 手機在 TEE 的環境下與 SE 通訊，SE 提供安全的存放空間及運算並產生金鑰。可信服務管理 TSM 則擁有銀行經過 CA 所簽署的憑證$CERT_B^{CA}$。

以下是各角色系統初始化所擁有的資訊：

銀行 B：ID_B 為銀行的 ID 識別碼、(PK_B, SK_B)銀行的非對稱式金鑰對、$K_{B,U}$ 銀行與使用者建立的通訊金鑰、$CERT_B^{CA}$皆經過 CA 簽署公開金鑰 PK_B 的憑證。

使用者 U：ID_U 為使用者的 ID 識別碼、(PK_U, SK_U)使用者的非對稱式金鑰對、$K_{B,U}$ 銀行與使用者建立的通訊金鑰、$CERT_U^{CA}$皆經過 CA 簽署公開金鑰 PK_U 的憑證。

安全元件 SE：ID_{SE} 為 SE 的 ID 識別碼、(PK_{SE}, SK_{SE})SE 的非對稱式金鑰對、$CERT_{SE}^{CA}$皆經過 CA 簽署公開金鑰 PK_{SE} 的憑證。

可信服務管理 TSM：ID_{TSM} 為 TSM 的 ID 識別碼、(PK_{TSM}, SK_{TSM})TSM 的非對稱式金鑰對、$CERT_{TSM}^{CA}$經過 CA 簽署公開金鑰 PK_{TSM} 的憑證。

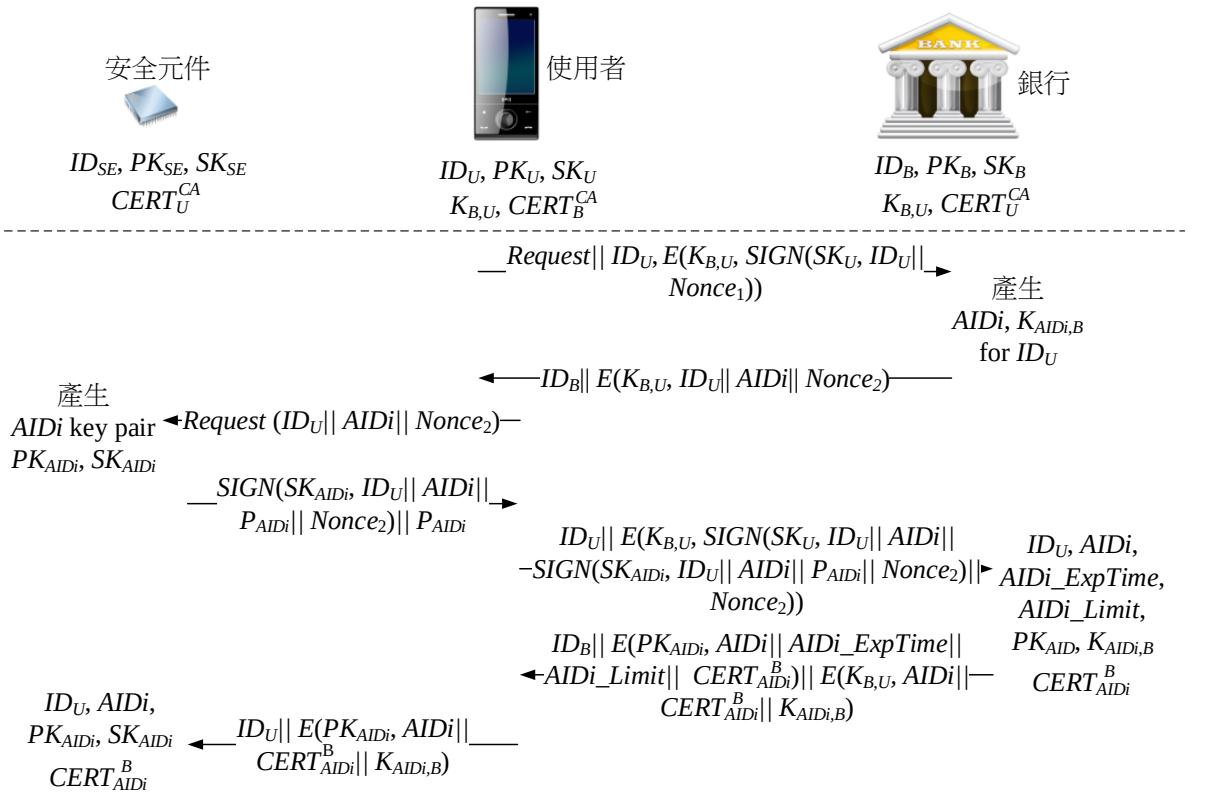
3. 申請銀行虛擬帳戶階段

如圖三所示，使用者向銀行請求建立一虛擬帳戶識別碼 *AIDi*，此時使用者 NFC 手機之安全元件將產生一組新的公開金鑰對(PK_{AIDi}, SK_{AIDi})後，利用其中之祕密金鑰(SK_{AIDi})將相對應之公開金鑰(PK_{AIDi})執行自我簽署 (self-signed)後，傳送至銀行確認。當銀行確認使用者之身分後，將簽發一相對應 *AIDi* 的公開金鑰之數位憑證給予使用者，以供後續交易使用。其步驟如下所示：

(1) 使用者身份 ID_U 向銀行發出請求請求。
(2) 銀行產生虛擬帳號 *AIDi* 與通訊金鑰 $K_{AIDi,B}$，並將 *AIDi* 傳給使用者。
(3) 使用者得到 *AIDi* 時向安全元件要求產生一新公開金鑰對。
(4) SE 建立的 *AIDi* 金鑰對 (PK_{AIDi}, SK_{AIDi})，並以 SK_{AIDi} 進行自我簽章後送回給使用者。
(5) 使用者將 *AIDi* 金鑰簽章訊息與申請的虛擬帳號 *AIDi* 使用通訊金鑰 $K_{B,U}$ 加密傳回給銀行。
(6) 銀行解開訊息得到 *AIDi* 的公開金鑰後，將產生 *AIDi* 的憑證，並將憑證、*AIDi* 的到期時間 *AIDi_ExpTime*、*AIDi* 帳戶的信用額度 *AIDi_Limit*，回傳給使用者。同時，銀行利用 *AIDi* 之公開金鑰，將通訊金鑰 $K_{AIDi,B}$ 加密傳送至安全元件。
(7) ID_U 將加密隻通訊金鑰 $K_{AIDi,B}$ 傳送到 SE
(8) SE 用產生的 *AIDi* 的私密金鑰解開，得到 *AIDi* 產生的通訊金鑰 $K_{AIDi,B}$ 及銀行發行的 *AIDi* 憑證，完成申請。

4. 申請信用卡帳戶階段

如圖四所示，當使用者向銀行註冊後，亦須向可信服務管理 TSM 註冊，以取得實際交易所使用之虛擬信用卡。在此階段中，使用者將於 TSM 建立一預儲, 之信用卡帳戶，並可自訂一最高交易額度。該預儲帳戶將使用銀行之虛擬帳戶進行電子付款。為了確保付款之安全性，使用者將付款訊息 *BINFO* 包含虛擬帳戶名稱 *AIDi*、虛擬帳戶到期



圖三: 銀行帳戶授權協定

圖四:申請信用卡帳戶協定

時間 *AIDi_ExpTime*、虛擬帳戶信用額度 *AIDi_Limit*、以與銀行共享之金鑰 $K_{AIDi,B}$ 加密後並以 SK_{AIDi} 簽名後，透過 TSM 傳送至銀行。使用者亦會將付款訊息以與 TSM 共享之金鑰 $K_{TIDi,TSM}$ 加密後並以 SK_{TIDi} 簽名後，一併傳送給 TSM。TSM 僅知交易銀行，但無法解開使用者傳送給銀行之付款訊息。

隨後 TSM 將解開之付款訊息 *TSMINFO*，經重新以與銀行公開金鑰 PK_B 加密及 SK_{TSM} 私鑰簽名後，連同使用者傳送給銀行之加密付款訊息 *TMSBINFO* 傳送至交易銀行。交易銀行將使用者傳送之付款訊息解開後，比對 TSM 所傳送之付款訊息是否一致。若銀行比對結果兩者一致則將虛擬帳戶之信用資訊傳送至 TSM，詳細步驟如下:

(1) 使用者建立帳號 *TIDi*，產生金鑰對(PK_{TIDi}, SK_{TIDi})，使用金鑰簽章並用 PK_{TSM} 加密訊息 $E(PK_{TSM}, SIGN(SK_{TIDi}, TIDi \| PK_{TIDi} \| TimeStamp))$並傳送至 TSM。

(2) TSM 收到請求訊息後，建立通訊金鑰 $K_{TIDi,TSM}$ 並且回傳給使用者。使用者產生一付款識別碼 *SID* 並將 *AIDi*、銀行 ID_B 和隨機數 $Nonce_1$ 送給安全元件。

(3) 安全元件產生付款訊息 $BINFO=SIGN(S_{AIDi}, E(K_{AIDi,B}, SID \| AIDi \| ID_{TSM} \| ID_B \| AIDi\_ExpTime \| AIDi\_Limit \| Nonce_2))$，並將 *BINFO*、 $Nonce_1$ 交給使用者。

(4) 使用者產生交易訊息 $TSMINFO=SIGN(SK_{TIDi}, E(K_{TIDi,TSM}, SID \| AIDi \| ID_{TSM} \| ID_B \| Nonce_2 \| AIDi\_ExpTime \| AIDi\_Limit))$。將訊息 *BINFO*、*TSMINFO*、$Nonce_1$ 加密並使用 SK_{TIDi} 簽名傳送給 TSM

(5) TSM 將得到的訊息解密後產生驗證訊息 $TSMBINFO=SIGN(SK_{TSM}, E(PK_B, SID \| AIDi \| Nonce_2 \| AIDi\_ExpTime \| AIDi\_Limit \| K_{TSM,B}))$。並將 *AIDi*、*BINFO* 和 *TMSBINFO* 驗證的加密訊息傳送到銀行確認。

(6) 銀行比對 *BINFO* 和 *TMSBINFO*，內容是否一致，並將 *AIDi* 的信用資訊傳送給 TSM。

(7) 可信服務管理 TSM 傳送給使用者，*TIDi* 的到期時間、信用額度。

5. 虛擬信用卡簽發

如圖五所示，使用者隨後即可向可信服務管理申請虛擬信用卡，可信服務管理將簽發一具有效期限較短、信用額度較低且符合 EMV 規範之信用卡資訊，傳送給使用者後存放於安全元件中。當該虛擬信用卡過期時，則使用者須重新進行此階段之步驟以取得另一張虛擬信用卡。詳細步驟如下：

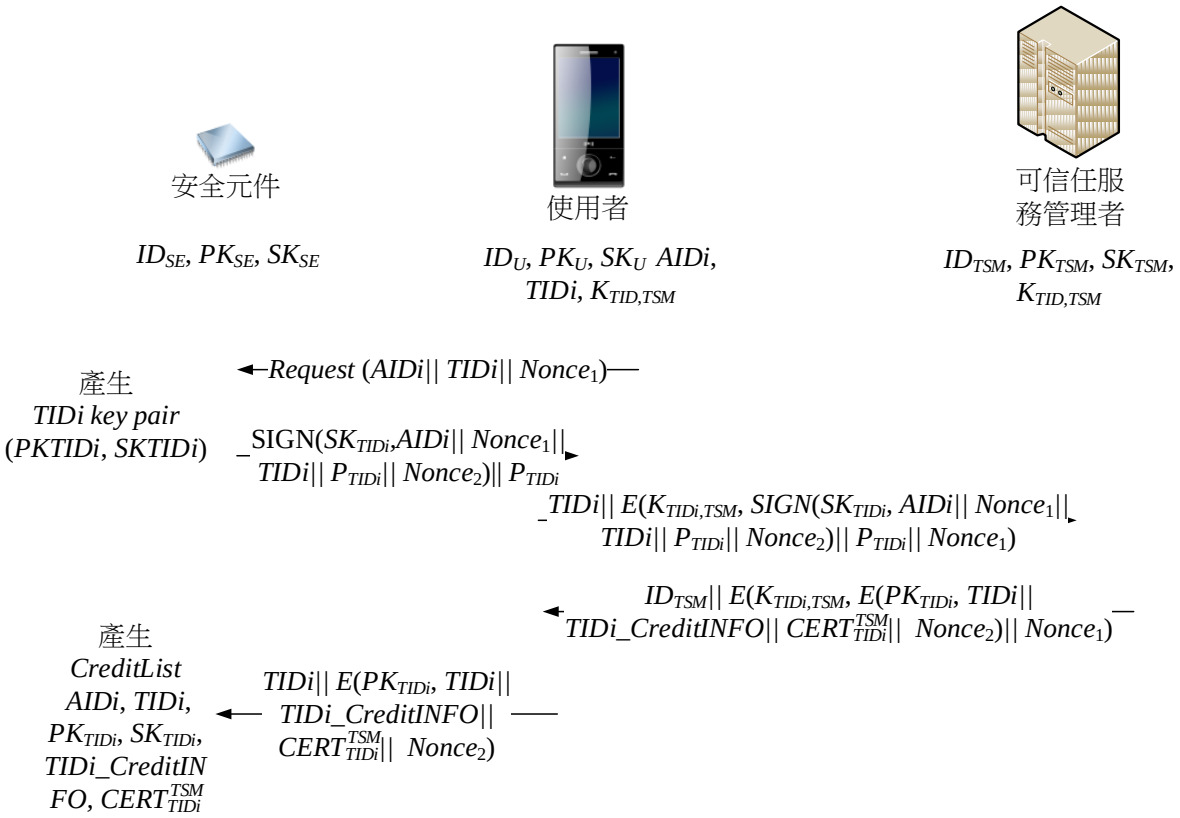
(1) 使用者與 ID_{SE} 請求 *TIDi* 的金鑰對(PK_{TIDi}, SK_{TIDi})，用來向可信服務管理簽發信用卡卡片金鑰。

(2) 使用者傳送請求給 ID_{SE}，產生 *TIDi* 的金鑰對(PK_{TIDi}, SK_{TIDi})

(3) 使用者傳送申請訊息，使用者申請服務帳 *TID* 與 ID_{SE} 產生金鑰簽章送給 ID_{TSM}，簽發憑證。

(4) TSM 簽發虛擬信用卡訊息資料，由 SE 保護。收到訊息，產生$CERT_{TIDi}^{TSM}$和虛擬信用卡資訊 *TIDi_CreditINFO* 存放在安全元件內。

(5) 後序交易流程遵照 EMV 交易流程用 NFC 手機的卡片模擬方式，產生虛擬信用卡進行交易。



圖五: 虛擬信用卡協定

四、安全性分析

本章我們提出以 NFC 為基礎之匿名行動付款協定安全性分析，就以匿名性、完整性、不可否認性、機密性、防止重送攻擊、防止中間人攻擊作為探討分析。

匿名性

申請銀行虛擬帳戶階段：使用者只向銀行進行身份認證並取得虛擬帳戶授權 *AIDi*，因此只有銀行知道使用者的真實身份，後續的交易皆使用虛擬帳戶達成匿名使用者的真實身份。

申請 TSM 服務帳號註冊階段：使用者向 TSM 申請匿名帳號 *TIDi*，此帳號為使用者自行取名建立帳號，並且使用者將於 TSM 建立帳號的預儲帳戶。該預儲帳戶將使用銀行之虛擬帳戶進行電子付款。因此 TSM 只會收到銀行虛擬帳戶的授權和銀行驗證虛擬帳戶簽發的授權期限 *AIDi_ExpTime*、信用額度 *AIDi_Limit*。如表二所示，由於預儲帳戶裡只有虛擬帳戶識別碼與授權期限、信用額度，因此 TSM 得知使用者申請的帳號有可使用的銀行授權，但無法得知使用者的真實身份。另外使用者使用匿名帳號向 TSM 交易，銀行無法得知使用者在 TSM 那的匿名帳號，因此使用者在 TSM 那進行的交易銀行無法得知使用者的交易資訊。

表二: TSM 用來記錄匿名帳號信用授權表

TIDi	*AIDi*	PK_{TIDi}	$CERT_{TIDi}^{TSM}$	*TIDi_CreditINFO*	*AIDi_ExpTime*	*AIDi_Limit*

虛擬信用卡階段：使用者向 TSM 申請虛擬信用卡，可信服務管理將簽發具有效期且符合 EMV 規範之信用卡資訊，傳送給使用者後存放於安全元件中，使用者交易時使用此信用卡交易，由於信用卡資訊無使用者身份，因此交易中收單銀行無法得知使用者交易訊息，商家也無法得知使用者真實身份。

在以 NFC 為基礎之匿名行動付款協定中，使用者除了向銀行申請虛擬帳戶授權外，在交易註冊過程中沒有曝露其真實身份。

完整性

完整性的部份，我們將分成包含三個部份為申請銀行虛擬帳戶階段、申請信用卡帳戶階段及虛擬信用卡簽發階段:

申請銀行虛擬帳戶階段：使用者到銀行業者申請虛擬帳戶，銀行將確認使用者手持的 NFC 手機的安全元件，並將使用者與銀行申請虛擬帳戶建立通訊金鑰 $K_{B,U}$，此通訊金鑰只有使用者與銀行得知，其他人是無法得知與使用。

帳戶授權建立使用者與銀行申請虛擬帳戶，利用使用者私鑰簽章與銀行的通訊金鑰保證訊息，使用者的私鑰與銀行的通訊金鑰存放在安全元件，他人無法取得。虛擬帳戶授權金鑰由安全元件產生，每次產生虛擬帳戶授權金鑰不同並且唯一，惡意使用者無法竄改，送出虛擬帳戶授權公鑰時，訊息利用使用者私鑰簽章與銀行的通訊金鑰加密保證訊息的完整性，因此傳輸的訊息無法造假及竄改。

申請信用卡帳戶階段：使用者與 TSM 建立帳戶，使用者將欲申請的帳號資訊，用自我簽署方式申請帳號，申請帳號訊息利用 TSM 公鑰加密，因此只有 TSM 才得知訊息內容，惡意攔截訊息竄改，則帳號也無法成功申請，另外此帳號與 TSM 可成功建立則將帳號需與銀行的虛擬帳戶做連結，TSM 確認使用者的合法性不被假冒及竄改。因 TSM 無法得知使用者真實身份，則藉由銀行確定，因此使用者申請時會使用安全元件建立給銀行之訊息，此付款訊息 *BINFO* 以與銀行共享之金鑰 $K_{AIDi,B}$ 加密後並以 SK_{AIDi} 私鑰簽章保證此訊息無法竄改及造假。另外使用者也建立給 TSM 之付款訊息用 TSM 共享之金鑰 $K_{TIDi,TSM}$ 加密後並以 SK_{TIDi} 私鑰簽章保證此訊息無法竄改及造假，一併傳送到 TSM，TSM 需解開付款訊息 *TSMINFO*，得知使用者資訊並將確認，故建立 *TMSBINFO* 資訊，為重新以與銀行公開金鑰 PK_B 加密及 SK_{TSM} 私鑰簽章，連同 SE 傳送給銀行之加密付款訊息 *BINFO* 傳送至交易銀行。傳送之間的付款訊息都經過加密及簽章，確定傳送間的訊息都無法造假及竄改。

虛擬信用卡階段：此階段主要為使用者與 TSM 申請虛擬信用卡訊息確認，及卡片資訊的完整性。首先使用者與 TSM 申請虛擬信用卡訊息，都利用使用者的 SK_{TIDi} 私鑰簽章保證訊息不可造假，再利用帳戶與 TSM 通訊金鑰加密使得惡意使用者無法得知訊息及竄改。再者虛擬信用卡金鑰由 SE 產生惡意使用者無法竄改及取得金鑰，且產生卡片資訊需由 TSM 簽發憑證認可並存放 SE，卡片資訊每個一段時間及限額需回 TSM 更新從新確認。

不可否認性

由於協定中為匿名，所有之帳戶註冊訊息、虛擬信用卡之製作及交易訊息皆須進行數位簽名，因此為了能防止使用者否認曾經發出訊息，則 TSM 與銀行必須握有使用者傳送過該訊息的證據達成不可否認性。

申請銀行虛擬帳戶階段：手機之安全元件給虛擬帳戶識別碼 *AIDi* 產生一組新的公開金鑰對(PK_{AIDi}, SK_{AIDi})，使用自我簽署方式，與銀行確認簽發相對應 *AIDi* 的公開金鑰之數位憑證給予使用者，因此後續交易使用以 SK_{AIDi} 簽名確認為虛擬帳戶簽章，確認使用者使用此虛擬帳戶交易且無法抵賴。

申請信用卡帳戶階段：TSM 建立一預儲帳戶，產生金鑰對(PK_{TIDi}, SK_{TIDi})，使用自我簽署方式，與 TSM 確認簽發相對應 *TIDi* 的公開金鑰之數位憑證給予使用者。使用者申請時使用銀行之虛擬帳戶進行電子付款需提供 *AIDi* 相關證明，因此付款訊息 *BINFO* 都使用 SK_{AIDi} 簽名後，透過 TSM 傳送至銀行。另外使用者給 TSM 付款訊息 *TSMINFO*，都使用 SK_{TIDi} 簽名後，證明為使用者用 *TIDi* 申請。TSM 解開之付款訊息 *TSMINFO* 使用 SK_{TSM} 私鑰簽名後，連同使用者傳送給銀行之加密付款訊息 *TMSBINFO* 傳送至交易銀行。建立帳號都由使用者的虛擬帳戶簽名，並且也使用建立帳戶的私鑰簽名，無法否認沒建立帳號，且使用者帳號申請需配合虛擬帳戶。

虛擬信用卡階段：使用者向可信服務管理申請虛擬信用卡時，使用者須將 *TID* 與 ID_{SE} 以私鑰簽章後送至 TSM 簽發憑證。之後進行交易時，皆須使用卡片中的私鑰簽章，達成交易不可否認性。若是使用虛擬信用卡交易時，產生爭議，皆可使用交易資訊得知使用者是否使用過此張信用卡，並且透過 TSM 及銀行得知交易過程由使用者的信用卡簽章過，不可抵賴。

機密性

就 NFC 通訊晶片有詳細的規格制定，安全元件用來儲存重要資訊，安全元件與手機的作業系統和硬體是各自獨立的，並且支援加密協定來加強授權控制，藉由儲存於安全元件中的私密金鑰將傳送資料加密，確保與外界溝通是以加密形式傳輸，保證資料的機密性。因此在手機部分金鑰管理存放並交由安全元件來管理，只有安全元件才可以產生金鑰，並且解開加密訊息，安全元件所產生的金鑰唯獨一無二，因此用安全元件金鑰加密可保證訊息傳輸的安全。

申請銀行虛擬帳戶階段：使用者的安全元件與銀行之間訊息傳輸都經過非對稱式金鑰對加密，由於金鑰為安全元件存取且訊息加解密也交由安全元件執行，故可以保證申請時訊息的機密性。申請銀行虛擬帳戶後續傳送出去的訊息也利用共享的通訊金鑰進行加密，共享之通訊金鑰只有使用者與銀行得知，攻擊者因無法解讀加密的資訊而無法取得傳輸的資訊，另外申請授權重要資訊存放在安全元件中，需有訪問與控制的權限才可以讀取。

申請信用卡帳戶階段：使用者與 TSM 之間訊息傳輸都經過示對稱式金鑰對加密，並與安全元件建立帳號對稱式通訊金鑰，由於金鑰為安全元件存取且訊息加解密也交由安全元件執行，故可以保證申請時訊息的機密性。申請 TSM 服務帳號後續傳送出去的訊息也利用共享的通訊金鑰進行加密，共享之通訊金鑰只有使用者的安全元件與 TSM 得知，攻擊者因無法解讀加密的資訊而無法取得傳輸的資訊，另外申請 TSM 帳號註冊授權重要資訊存放在安全元件中，需有訪問與控制的權限才可以讀取。

虛擬信用卡階段：虛擬信用卡階段訊息利用之前的通訊金鑰加密傳輸訊息，使用者的 SE 與 TSM 之間訊息傳輸都經過非對稱式金鑰對，且公開金鑰皆經過 TSM 與銀行所簽署產生相關的憑證。使用通訊金鑰 $K_{TIDi,TSM}$ 加密傳輸訊息，及安全元件產生非對稱式

金鑰對的 PK_{TIDi} 金鑰傳送給 TSM。TSM 信用卡訊息，使用通訊金鑰加密傳輸訊息並金鑰加密信用卡資訊給安全元件存取解密，攻擊者因無法解讀加密資訊而無法取得傳輸及卡片的資訊內容。

防止重送攻擊

協定中每一階段通訊過程中利用隨機數與傳輸訊息共同加密，使得每一次傳送的訊息會隨著隨機數的不同而改變。因此攻擊者藉由重送之前的訊息是無法認證成功的。

申請銀行虛擬帳戶階段：在申請虛擬帳戶授權時，當惡意的使用者不斷送出與銀行要求訊息，訊息經過通訊金鑰加密，惡意的使用者也無法重送得知相關訊息，也無法從重送取得重要帳戶訊息。另外訊息內加入隨機數，防止非同步重送攻擊。若是重送銀行授權訊息，也因銀行與安全元件通訊訊息經過加密，無法得知內容，重送也無法得知相關訊息及相關資料。

申請信用卡帳戶階段：在申請請 TSM 服務帳號註冊時，如同申請銀行虛擬帳戶，訊息經過通訊金鑰加密，惡意的使用者也無法重送得知相關訊息，若是不斷重送給 TSM 與銀行資訊，訊息內加入隨機數，將會得知訊息遭受重送攻擊，並且訊息內有加入簽章可得知那個帳戶是有問題，並可停權處理，使得該帳戶無法使用。

虛擬信用卡階段：信用卡取得訊息皆有加密，並且信用卡資訊由 TSM 發行並且只有短暫的期限及金額限定，在申請虛擬信用卡時訊息被重送，也無法多得其他信用卡，另外信用卡資訊取得為直接存放安全元件內，一般是無法取得權限使用。

五、結論

本論文植基於 NFC 手機並加入 TSM 公信的第三方，實現安全且便利的匿名行動付款系統。銀行及 TSM 兩個匿名機制方式保有信用卡特色且改善不可匿名、可連結性問題。本方法保護使用者個人隱私與增加消費便利性與安全性。就使用者隱私而言，使用者匿名向 TSM 進行註冊，利用銀行帳戶身份驗證，而 TSM 只知道像銀行帳戶請款，而銀行無法得知使用者進行交易訊息，商家像 TSM 請款也無法得知使用者的銀行資訊，進而無法假冒使用者身份及分析使用者的交易習慣，然而當有消費紛爭或信用問題時，TSM 可像銀行申請追蹤帳戶使用者的真實身份。就交易方面而言，使用者只需使用 NFC 手機取得 TSM 授權虛擬信用卡即可完成整個付款流程。

[謝啟]

本研究由國科會計畫 NSC101-2221-E-033-016-MY2 補助支持，特此致謝。

參考文獻

[1] 廖鴻圖，“跨網域之匿名行動付款機制”，*電子商務學報*，第九期，2007：頁 779-799。

[2] 廖鴻圖、廖偉鵬、郭明煌、陳志瑋，*整合型電子票證機制之研究*，碩士論文，世新大學資訊管理學研究所，2008。

[3] Balfe, S. and Paterson, K.G. "e-EMV: Emulating EMV for Internet Payments with Trusted Computing Technologies," *Proceedings of the 3rd ACM workshop on Scalable Trusted Computing*, Alexandria, Virginia, USA, 2008.

[4] Carr, M. "Mobile Payment Systems and Services: An Introduction," *Mobile Payment Forum*, 2007: pp. 1-12.

[5] Chen, W., Hancke, G., Mayes, K., Lien, Y. and Chiu, J.H. "NFC Mobile Transactions and Authentication Based on GSM Network," *Second International Workshop on Near Field Communication (NFC)*, 2010: pp. 83-89.

[6] Chen, W.D., Hancke, G., Mayes, K., Lien, Y. and Chiu, J.H. "Using 3G Network Components to Enable NFC Mobile Transactions and Authentication," *IEEE International Conference on Progress in Informatics and Computing (PIC)*, 2010: pp. 441-448.

[7] Chen, Y., Chou, J.S., Sun, H.M. and Cho, M.H. "A Novel Electronic Cash System with Trustee-Based Anonymity Revocation from Pairing," *Electronic Commerce Research and Applications*, (10), 2011: pp. 673-682.

[8] EMVCo "Integrated Circuit Card Specifications for Payment Systems: Book 2—Security and Key Management," ed: Version 4.3, November 2011.

[9] Fan, C.I. and Huang, V.M. "Provably Secure Integrated On/Off-Line Electronic Cash for Flexible and Efficient Payment," *IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews*, (40), 2010: pp. 567-579.

[10] Hassinen, M., Hyppönen, K. and Trichina, E. "Utilizing National Public-Key Infrastructure in Mobile Payment Systems," *Electronic Commerce Research and Applications*, (7), 2008: pp. 214-231.

[11] Kabir, Z. *User Centric Design of an NFC Mobile Wallet Framework*, Master Thesis, The Royal Institute of Technology (KTH), Stockholm, Sweden, 2011.

[12] Kungpisdan, S., Srinivasan, B. and Le, P.D. "A Secure Account-Based Mobile Payment Protocol," *Int. Conf. on Information Technology: Coding and Computing*, 2004: pp. 35-39.

[13] Martínez-Peláez, R., Rico-Novella, F. and Satizábal, C. "Mobile Payment Protocol for Micropayments: Withdrawal and Payment Anonymous," *New Technologies, Mobility and Security*, NTMS'08, 2008: pp. 1-5.

[14] Molloy, I., Li, J. and Li, N. "Dynamic Virtual Credit Card Numbers," *Financial Cryptography and Data Security*, ed: Springer, 2007: pp. 208-223.

[15] Toorani, M. and Beheshti, A. "SSMS-A Secure SMS Messaging Protocol for the m-Payment Systems," *Computers and Communications*, 2008.