相容於 NFC 之匿名行動付款協定

羅嘉寧[1]　楊明豪[2]　黃思穎[2]　蔡卓倫[1]
[1]銘傳大學電腦與通訊工程學系
[2]中原大學通訊工程碩士學位學程
deer@mail.mcu.edu.tw, mhyang@cycu.edu.tw, kobebryand76@gmail.com, luen19881015@gmail.com

摘要

從電子付款服務已廣泛的被人們所使用。演進到行動付款服務，手機構物、轉帳、NFC 付款等。NFC 付款服務，則可能曝露許多敏感的個人資訊，危害使用者之權益。個人隱私問題實為行動付款服務之一大課題。

本論文提出一個以 NFC 為基礎之匿名行動付款協定，以匿名行動付款方式結合 NFC 手機，具有以下特點：(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。

本論文之 NFC 為基礎之匿名行動付款協定，利用 TEE 和 MTM 解決 NFC 行動裝置之軟硬體執行的安全性問題，NFC 手機中的安全元件(Secure element, SE)結合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。

關鍵詞：NFC、MTM、TEE、EMV、匿名付款系統

1. 前言

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)[1][2]亦隨之盛行。行動電子商務[3]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[3][4][5][6][7][8]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[5]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[9]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帳單，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[7] 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[10]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。

廖等人[11]跨網域之匿名行動付款機制，提出有關行動付款機制，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[12]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[13]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。

2. 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，我們的方法用 TEE、MTM、EMV、PKI 等方式作延伸，整個機制包含(1)系統初始化 2. 遠端軟體驗證 3. 申請銀行虛擬帳戶階段 4. 服務帳號註冊 5. 虛擬信用卡簽發。

系統角色介紹如下：

- 軟體供應商 SP：提供軟體下載。
- 銀行 B:銀行提供使用者帳戶與驗證軟體合法性，銀行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. 遠端軟體驗證：交易軟體下載安裝於 NFC 手機時，須先通過 MTM 架構之軟體驗證程序，並將驗證碼存放於銀行端。每次手機啟動軟體時，皆會進行遠端軟體驗證以確保使用者是使用未經竄改之軟體與合法的 NFC 手機。
3. 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。
4. 服務帳號註冊：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，配發一服務帳號給使用者。
5. 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。

2.1 名詞定義表

表 1 名詞定義表

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
$CERT^{X}_{IDX}$	x 角色發行的憑證：如 CA 發給銀行的憑證$CERT^{CA}_{B}$，銀行發給使用者的匿名識別碼的憑證 $CERT^{B}_{AIDi}$
$K_{x,y}$	角色通訊者 x 與角色通訊者 y 角色之間的通訊金鑰
$SIGN(SK_x,M)$	用 x 私密金鑰將訊息 M 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	給 X 的訊息
TSMINFO	給 TSM 的訊息
TSMBINFO	TSM 給 B 的訊息
AuthDATA	驗證訊息
Status	驗證訊息狀態，成功/失敗
TIDi_CerditINFO	憑 EMV 發行信用卡的訊息
TIDiList	TSM 用來記錄匿名帳號信用授權表
Quote	舉證訊息

2.2 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 $CERT^{B}_{U}$ 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$CERT^{CA}_{B}$，軟體供應商 SP：軟體驗證碼、提供軟體。

以下是各角色系統初始化所擁有的資訊：

軟體供應商 SP：軟體驗證碼 $SIGN(SK_B, Quote)$、提供軟體。

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、$CERT^{CA}_{B}$ 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) ID 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、$CERT^{CA}_{U}$ 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、$CERT^{CA}_{SE}$ 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、$CERT^{CA}_{TSM}$ 經過 CA 簽署公開金鑰 PK_{TSM} 的憑證。

2.3 遠端軟體驗證

在使用手機進行行動付款前，NFC 手機必須具備行動可信模組的 MTM 架構。當 NFC 手機從軟體供應商(如 Google Play Market 或 Apple AppStore)下載特定軟體並執行安裝。本階段包含兩部分: 軟體下載驗證及軟體啟動驗證，分述如下:

2.3.1 軟體下載驗證

NFC 手機要執行軟體安裝時，MTM 平台之 Application Measurement 須先確認軟體是否經過簽名，並由 Attestation Service 詢問 Trusted Platform 確認其軟體驗證碼(fingerprint) 是否正確，驗證軟體為可信不可信。

若軟體可信賴，則於安裝後計算該軟體之 PCR 值，除存放於安全元件 SE 中，亦將 PCR 簽名後傳送至銀行，存放於銀行伺服器中。詳細步驟如下:

1. Application Measurement 下載軟體時會，收到軟體識別碼，產生隨機數 Nonce 給 Attestation Service。
2. Attestation Service 產生 Quote Request 去詢問 Trusted Platform
3. MTM 算出 Quote，Quote 為 MTM 簽名過的 PCRs 驗證通行碼、Nonce、軟體識別碼。
4. Attestation Service 向 Measurement Agent 請求平台驗證訊息。
5. Measurement Agent 會將平台驗證訊息傳給在 Measurement List 存放，報告 MTM，並回傳給 Application Measurement 透過 Attestation Service。
6. Application Measurement 平台驗證訊息、Quote 和軟體識別碼傳給銀行。
7. 銀行驗證手機平台和軟體識別碼，並通知 Application Measurement 安裝。

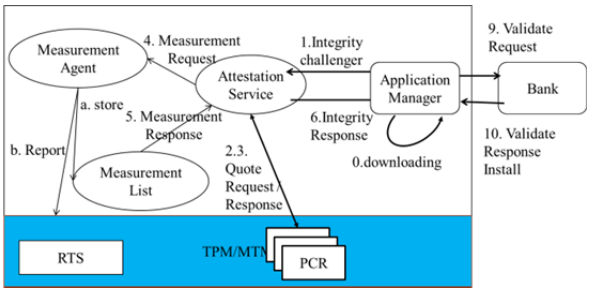

圖 1 軟體下載驗證流程圖

2.3.2 軟體啟動驗證

每次手機執行軟體時，Attestation Service 亦會計算軟體驗證碼，除與存放於安全元件中之 PCR 比對外，亦會加以簽名後傳送至銀行端請求驗證，若銀行確認該驗證碼與之前存放於伺服器中之驗證碼相同，則會允許使用者執行該軟體。詳細步驟如下：

1. 軟體啟動驗證，產生隨機數 Nonce。
2. Attestaion Service 產生 Quote Request 去尋問 Trusted Platform。
3. MTM 算出 Quote，Quote 為 MTM 簽名過的 PCRs 驗證通行碼與 Nonce。
4. Attestaion Service 向 Measurement Agent 請求平台驗證訊息。
5. Measurement Agent 會將平台驗證訊息傳給在 Measurement List 存放，報告 MTM，並 Measurement List 回傳給 Attestaion Service。
6. 軟體驗證訊息 Measurement List 訊息、Quote 和 Nonce 簽名回傳銀行驗證。

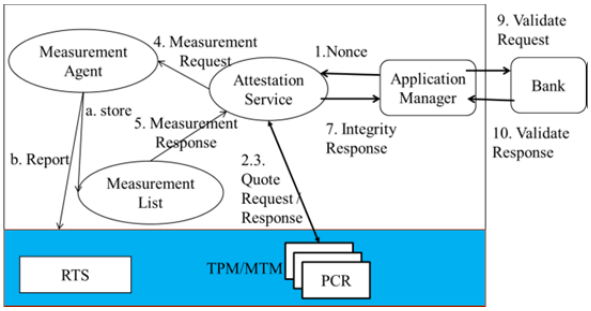

圖 2 軟體啟動驗證流程圖

2.4 申請銀行虛擬帳戶階段

為了保護使用者的隱私，使用者於確認軟體之正確性後，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 Request，將 ID_U 產生虛擬帳號 AIDi 與通訊金鑰 $K_{AIDi,B}$。
2. 銀行回應 ID_U 給與 AIDi 並建立通訊金鑰 $K_{AIDi,B}$。
3. 使用者得到 AIDi 時向 SE 提出產生一新公開金鑰對的請求。
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 $K_{AIDi,B}$ 加密傳回給銀行進行驗證。
6. 銀行解開訊息，得到 AIDi 的公開金鑰，將產生虛擬帳號 AIDi 銀行 B 所發行的 AIDi 憑證、AIDi 的到期時間 AIDi_ExpTime 、AIDi 帳戶的信用額度 AIDi_Limit 及與 AIDi 與通訊金鑰 $K_{AIDi,B}$，回傳給 IDU 訊息為到期時間、信用額度及加密過要給 SE 的 AIDi 通訊金鑰 $K_{AIDi,B}$。

7. IDU 將加密傳送到 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。

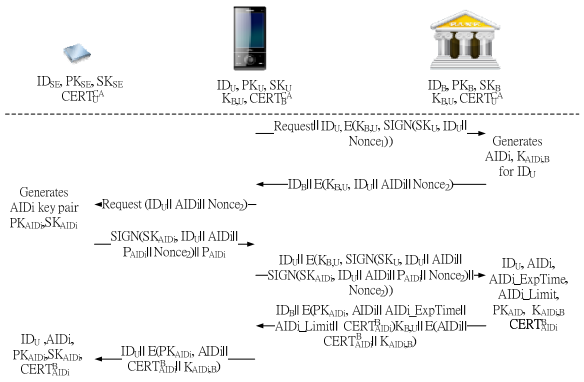

圖 3 銀行帳戶授權協定

2.5 申請 TSM 服務帳號註冊階段

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 SKAIDi 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. 使用者發出請求註冊
   - ID_U 建立帳號 TIDi，產生金鑰對(PK_{TIDi}, SK_{TIDi})，使用金鑰簽章並用 PKTSM 加密訊息 E(PK_{TSM}, SIGN(SK_{TIDi}, TIDi|| PK_{TIDi}|| TimeStamp))，請求建立 TIDi 訊息 E(PK_{TID}, SID|| TIDi || $K_{TIDi,TSM}$)並傳送 TSM。
   - ID_{TSM} 收到 TIDi 請求訊息解開，建立通訊金鑰 $K_{TSM,TIDi}$ 並且回傳給使用者並要求帳號提供信用證明，才可開通服務。
2. 使用者相關證明

ID_U 收到 ID_{TSM} 立建 TIDi，需提供信用證明才可啟用服務，建立給 ID_{TSM} 的訊息與給銀行訊息，銀行訊息需由 AIDi 與銀行之間的通訊金鑰 $K_{AIDi,B}$ 做出加密訊息並用 AIDi 的私鑰簽章；給可信服務管理訊息由 TIDi 與可信服務管理之間的通訊金鑰 $K_{TSM,TIDi}$ 做出加密訊息，並用 TIDi 的私鑰簽章。

- ID_U 請求 SID 會議身份識別碼、AIDi、和 AIDi 的銀行和隨機數 Nonce1 送給 IDSE。
- ID_SE 做出銀行給 AIDi 的相關訊息 BINFO、$Nonce_1$ 交給 IDU。BINFO=SIGN(SAIDi, E($K_{AIDi,B}$, SID || AIDi || ID_{TSM} || IDB || AIDi_ExpTime || AIDi_Limit || $Nonce_2$))。
- IDU 做出 IDTSM 給 TIDi 的相關訊息 TSMINFO。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 ID_{TSM}。
- TSM 收到 TIDi 提出的身份證明訊息。

3. 可信服務管理向銀行驗證

收到 TIDi 提出的身份證明訊息向銀行驗證。

- 將得到的訊息解密，得到 TSMINFO 解開取得 AIDi、IDB、SID、與 AIDi_ExpTime 到期間|| AIDi_Limit 信用額度。
- 將要銀行確認的 AIDi 身份和到期間時間、信用額度做出驗證訊息 TMSBINFO，TSMBINFO=SIGN(SK_{TSM}, E(PK_B, SID || AIDi || $Nonce_2$ || AIDi_ExpTime || AIDi_Limit || $K_{TSM,B}$))。
- 將 AIDi、BINFO 和 TMSBINFO 驗證的加密訊息傳送到 ID_B
- 解開訊息，比對 BINFO 和 TMSBINFO，內容是否一制，並將 AIDi 的信用資訊傳送給可信服務管理。

4. 可信服務管理接受 TIDi 是合法的使用都並取得服務，傳送給使用者，TIDi 的到期時間、信用額度。

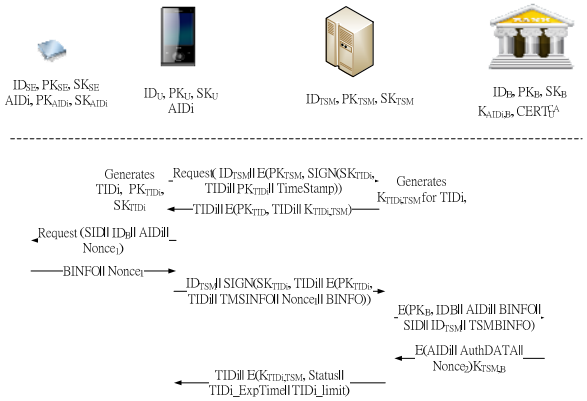

圖 4 TSM 申請帳戶協定

2.6 虛擬信用卡簽發

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。

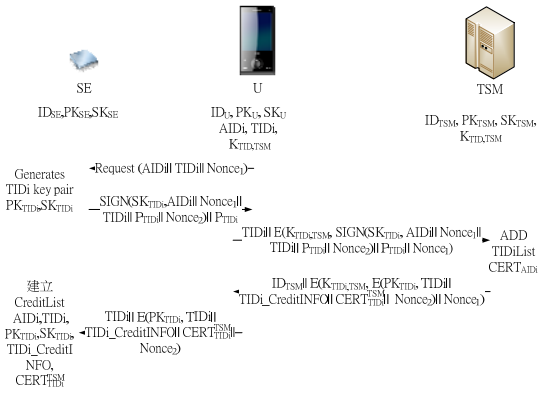

圖 5 虛擬信用卡協定

表 2 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	

3. 結論

本論文以基於 TEE、MTM、及 EMV 的規範結合 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。

參考文獻

[1] C.I. Fan and V.M. Huang, “Provably secure integrated on/off-line electronic cash for flexible and efficient payment,” in IEEE Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, vol. 40, pp. 567-579, 2010.

[2] Y. Chen, J.S. Chou, H.M. Sun, and M.H. Cho, “A novel electronic cash system with trustee-based anonymity revocation from pairing,” Electronic Commerce Research and Applications, 2011, vol. 10, pp. 673-682.

[3] M. Carr, "Mobile Payment systems and services: An introduction, “ in Mobile Payment Forum, 2007, pp. 1-12.

[4] W. Chen, G. Hancke, K. Mayes, Y. Lien, and J.H. Chiu, “NFC mobile transactions and authentication based on GSM network,” in Second International Workshop on Near Field Communication (NFC), 2010, pp. 83-89.

[5] 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,” in IEEE International Conference on Progress in Informatics and Computing (PIC), 2010, pp. 441-448.

[6] Z. Kabir, “User Centric Design of an NFC Mobile Wallet Framework,” KTH, 2011.

[7] R. Martínez-Peláez, F. Rico-Novella, and C. Satizábal, “Mobile payment Protocol for micropayments: withdrawal and payment anonymous,” in New Technologies, Mobility and Security, NTMS'08., 2008, pp. 1-5.

[8] M. Hassinen, K. Hyppönen, and E. Trichina, “Utilizing national public-key infrastructure in mobile payment systems,” Electronic Commerce Research and Applications, 2008, vol. 7, pp. 214-231.

[9] M. Toorani, A. Beheshti, “SSMS-A secure SMS messaging protocol for the m-payment systems,” Computers and Communications , 2008.

[10] S. Kungpisdan, B. Srinivasan, and P. D. Le, “A secure account-based mobile payment protocol,” in International Conference on Information Technology: Coding and Computing (ITCC), 2004, pp. 35-39.

[11] 廖鴻圖, “跨網域之匿名行動付款機制,” 電子商務學報, vol. 9, pp. 779-799, 2007.

[12] I. Molloy, J. Li, and N. Li, “Dynamic virtual credit card numbers,” in Financial Cryptography and Data Security, ed: Springer, 2007, pp. 208-223.

[13] 廖鴻圖, 廖偉鵬, 郭明煌, and 陳志瑋, “整合型電子票證機制之研究,” 2008.