Mobile RFID 跨領域所有權轉移

楊明豪
中原大學資訊工程系
mhyang@cycu.edu.tw

蔡宗成
中原大學資訊工程系
cheng1012@gmail.com

***摘要*—無線射頻識別(Radio Frequency Identification, RFID)被廣泛應用在多個領域。而近年發展出 Mobile RFID，結合行動通訊設備與 RFID 讀取功能，提供不受限於使用地點的 RFID 應用服務，使人們透過行動讀取器進行電子交易。然而隨著 RFID 技術快速發展，也陸續出現許多須克服的瓶頸，其中一個重要的議題為所有權轉移(Ownership Transfer)。為能夠透過所有權轉移協定，安全的將嵌入電子標籤物品的物權轉移給他人，並應用在多伺服器的行動商務上，因此我們在本文中提出適用於 Mobile RFID 環境且支援跨越不同管轄領域伺服器的所有權轉移協定(Cross Authority Ownership Transfer)，並證明我們所提出的所有權轉移方法滿足向前安全和雙向認證，防止重送攻擊、中間人攻擊、資料不同步之阻絕服務攻擊等安全威脅，分析我們方法的效能與所需的儲存空間，並其它現有的所有權轉移方法進行比較，證明我們方法的可行性。**

***關鍵詞*—Mobile RFID、中間人攻擊、所有權轉移、跨領域、重送攻擊**

一、前言

近年無線射頻識別技術持續進步與成本不斷降低，使其應用快速成長，目前應用已跨越物流管理、生產製造、設備資產管理、門禁管制、票據付款、智慧家電、醫療用藥管理等多個領域。例如:美國最大的零售百貨業 Wal-Mart 在 2005 年開始導入 RFID，藉由 RFID 追蹤貨品在供應鏈上的資訊，提升補貨速度並有效降低庫存，使得收益增加[4] 。另外還有美國政府使用的 RFID 護照[14] ，以及其他組織[9] 和公司已投入 RFID 產業的標準訂定和產品生產[11] [15] [31] 。這些例子顯示，隨著 RFID 應用技術趨於成熟，越來越普遍的應用於人類的生活之中。

對於無法架設固定式讀取器的環境，近年來發展出具移動性的無線行動讀取器，行動無線射頻識別(Mobile RFID)[1] 。使用具 RFID 讀取功能的個人行動手持設備作為行動讀取器，如行動電話或 PDA，並整合無線通訊技術，提供使用者具機動性的無線射頻識別服務。不同於傳統的 RFID 系統將讀取器設置於固定地點，使用者可以攜帶讀取器到處移動，在讀取 RFID 電子標籤後，利用電信通訊網路或 IEEE802.11 等無線通訊技術，將資料透過網際網路傳回管理伺服器進行應用服務[1] [21] ，例如：行動讀取器讀取貼附於地標與景點的電子標籤，透過管理伺服器的辨識，可以獲得定位資訊，進而提供地理資訊服務。讀取貼附於公車的電子標籤取得公車路線圖[7] [19] 。在未來，Mobile RFID 將是極具潛力的 RFID 應用型態。

但隨著 RFID 的應用越來越廣泛，也陸續出現許多必須克服的瓶頸，RFID 安全議題為其中的重要議題之一，並且越來越被重視。RFID 之安全問題起因於 RFID 標籤之運算能力有限，以及 RFID 標籤透過無線電波傳送資訊，因此容易受到攻擊者之竊聽、追蹤、中間人攻擊、重送攻擊、阻斷式服務攻擊等各種危害[17] [19] [27] 。使用者可能因為這些危害造成隱私洩漏，財產損

This work was supported in part by National Science Council under the grants NSC-98-2221-E-003-041-.

失，嚴重可能因系統被有意人士利用造成極大威脅，因此有許多的 RFID 之研究正朝向具備安全性的 RFID 協定方法。

由於人們利用電子標籤進行各種物品的管理與物品的交易活動，因此衍生出一個在無線射頻識別應用重要的議題—所有權轉移(Ownership Transfer)。在一個電子標籤的生命週期中，我們可以藉由所有權轉移來達到交易物品的目的，並且將物品的管理權限交給新物品之擁有者。透過所有權轉移的機制，我們可以更容易對電子標籤進行權限的控管，只有擁有者才能對電子標籤進行存取的權限，防止非擁有者對電子標籤進行竄改，確保在商品轉手之後，貼有電子標籤的商品不因他人的存取，而造成隱私外漏，而可繼續使用電子標籤之功能進行管理。因此 Y. Seo 等人提出以 Re-encrypted 之方法進行所有權轉移[32] 。K. H. S. S. Koralalage 等人提出適用於 EPC Class-1 Gen-2 Base 之所有權轉移協定[16] 。D. Molnar 等人在研究[8] 中則提出 one-way key chain 來更新金鑰的 RFID 認證與所有權轉移協定。S. Fouladgar 等人提出 Hash Based 與 Encryption base 兩種方法之標籤管理委任協定與所有權轉移協定，使讀取器可在與伺服器離線時，進行標籤識別服務[25] [26] [27] 。楊等人提出運作於 Mobile RFID 環境下，提供具雙向認證之所有權轉移協定，且可指定所有權轉移之對象[1] 。Osaka 等人提出一次性暫時之電子標籤識別碼的所有權轉移方法[17] [10] [17]，但其方法並無法抵抗阻斷服務攻擊，且未達到向前性安全[10] 。

S. Fouladgar 等人提出所有權轉移協定[26] [27] ，使消費者能將電子標籤之所有權自零售商之管理伺服器轉移至消費者的 Smart Home system 伺服器。但其方法因後端伺服器直接傳送標籤金鑰給轉移目地之伺服器，因此並未完全達到向前性安全，且未提出在伺服器間進行雙向認證之方法，因此並不適用於 Mobile RFID 環境。

楊等人提出之所有權轉移方法可運作於 Mobile RFID 環境下，並符合安全性需求，但只能運用在單一後端管理(authority)資料庫伺服器，並不適用在多管理伺服器環境下進行跨伺服器之所有權轉移。為解決 Mobile RFID 環境下可能跨管理伺服器進行所有權轉移之情形，我們提出一個可以運作於 Mobile RFID 環境且支援跨伺服器之跨領域所有權轉移 (Cross Authority Ownership Transfer , CAOT)協定，並且符合 RFID 所有權轉移的安全需求。我們提出的方法可以使電子標籤擁有者透過行動讀取設備進行所有權轉移，並且可將後端管理的權限轉移至新擁有者所指定的管理伺服器，使得無線射頻識別系統不再侷限為只有單一管理伺服器，拓展為可以在多個管理伺服器之間進行所有權轉移，並使新擁有者的管理伺服器可以繼承來自原標籤之管理伺服器所提供的物品管理資訊，因此所有權轉移後的電子標籤可以立即與新的管理伺服器的服務做結合。標籤的新擁有者可以在進行跨領域所有權轉移時，將購買的商品之管理權限與所有權登錄到私人的管理伺服器、公司的管理伺服器或是專門提供管理服務的伺服器，這使得標籤擁有者可以對電子標籤進行更有彈性的管理與服務。另外，我們的方法也將同時確保在所有權轉移的過程可以抵擋重送攻擊、防止竊聽、防範訊息竄改、提供行蹤隱私保護、新舊擁有者之間雙向認證的安全需求。

本篇論文在第二章介紹本論文所提的跨領域所有權轉移協定環境假設，第三章詳細介紹我們所提出的協定，並說明協定的每一步驟的意義。接著在第四章分析協定的安全性並與目前我們已知其它 RFID 所有權轉移方法的安全性做比較。第五章對於我們提出方法的計算和儲存效能做分析並和相關研究做比較。最後第六章是本篇論文的結論。

二、跨領域所有權轉移環境假設

我們提出一個在 Mobile RFID 環境下進行所有權轉移的方法，RFID 跨領域所有權轉移(Cross Authority Ownership Transfer, CAOT)。該方法使得電子標籤擁有者可以在不同管理權責的伺服器之間進行所有權轉移，達到標籤所有權之擁有者變更、標籤金鑰更新以及標籤管理權限從原本的管理伺服器轉移至指定的管理伺服器。我們的方法會以 Mobile RFID 的網路服務為基礎架構，如 Namje Park 等人在[23] 所提及，以個人行動手持設備作為讀取器，透過該行動手持設備讀取電子標籤以及透過網際網路連結後端伺服器進行電子標籤管理的服務架構。

在 CAOT 方法中，我們假設的標籤管理服務環境有三點性質。第一點，我們假設行動讀取器在同一時間內只會連結至單一後端管理伺服器對行動電子標籤進行管理，且轉入、轉出的行動讀取器之管轄的後端伺服器可能為同一個或是分別屬於不同管轄(Authority)的後端伺服器。也就是說任一個由伺服器 DID^i 所管轄之讀取器 RID_p^i 和讀取器集合 R^i 必須滿足式(1)中的關係。

$$R^i = \{RID_1^i, RID_2^i, \ldots\ldots, RID_n^i\}，R^i 為 DID^i 所管轄，且滿足$$

$$\forall i, j\ R^i \cap R^j = \emptyset\ iff\ i \neq j，否則 R^i \cap R^j = R^i \qquad (1)$$

在式(1)中表示，若 R^i 和 R^j 內沒有任一相同讀取器則 R^i 和 R^j 必分屬在不同的伺服器，反之 R^i 和 R^j 則在同一管理伺服器內進行所有權轉移。

第二點，任一電子標籤必定只屬於特定之讀取器 RID_p^i 所擁有，也就是只有該讀取器有權限對其擁有之標籤集合 T_p^i 內任一電子標籤 TID_a^i 進行所有權轉移。標籤與讀取器關係如式(2)所示。

$$T_p^i = \{TID_1^i, TID_2^i, \ldots\ldots, TID_m^i\}，T_p^i 為 RID_p^i 所擁有，且滿足$$

$$\forall i, j\ T_p^i \cap T_q^j = \emptyset\ iff\ i \neq j，否則 T_p^i \cap T_q^j = T_p^i \qquad (2)$$

假設一屬於式(2)之標籤群 T_p^i 的電子標籤 TID_a^i 轉出到標籤群 T_q^j，且 T_p^i 和 T_q^j 內沒有任一相同電子標籤則 T_p^i 和 T_q^j 必分屬在不同的讀取器 RID_p^i 和 RID_q^j 的管轄，由式(1)讀取器和伺服器的關係可知其標籤屬於不同伺服器管轄，反之 TID_a^i 則在同一後端伺服器內進行所有權轉移。

第三點，標籤之所有權對應至擁有者之專屬行動設備並將此一資訊儲存於後端管理伺服器，且預設後端資料庫和電子標籤利用其它的安全通道共享一把金鑰 Kx。

我們所提出的 CAOT 所有權轉換協定之網路架構如圖 1 所示，包含 RFID 標籤、行動讀取器和管理伺服器三種類型的設備。由於上列三種設備的計算能力與移動能力不同，因此設備之間的網路連線依安全等級由高至低分為三種類型:

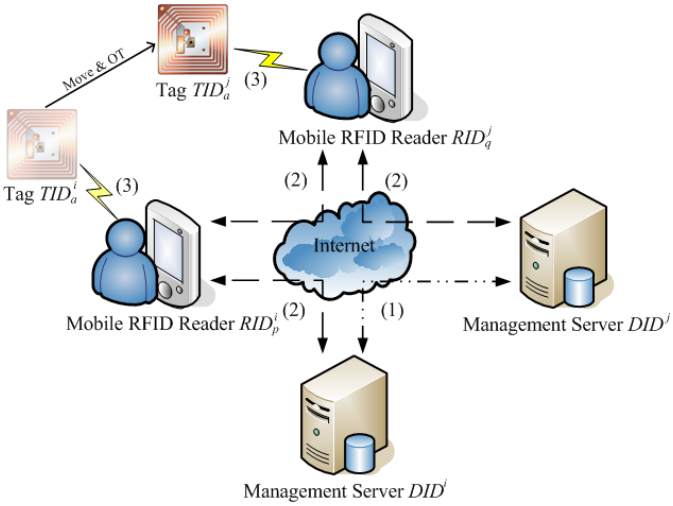

圖 1 所有權轉換網路環境架構圖

1. 管理伺服器 DID^i 與 DID^j 之間透過有線的網際網路連結，如圖 1 中的連線(1)所示。由於伺服器計算能力足以負擔現有最安全之加密方法，如 AES、RSA，且伺服器相較於行動設備，為固定地點的設備，因此網路不會因設備移動而造成無法存取的狀況，所以我們利用現有的加密方法來確保訊息傳輸的安全性，並假設伺服器之間的通訊是安全的。

2. 行動讀取器藉由現有個人行動通訊技術或 IEEE802.11 之無線網路技術連結至網際網路，對後端管理伺服器或其他的行動讀取器進行雙向通訊，如圖 1 中的連線(2)所示。由於行動讀取設備的計算能力不如伺服器的計算能力，且行動讀取器具有移動特性，而需要使用無線網路，因此通訊安全性相對低於第一種類型。但我們可以藉由無線網路現有之安全通訊技術來保護訊息傳輸的安全性。如 3G 在 3GPP 的 Security Architecture[3] ，或是 IEEE802.11i[12] 的 WPA2。當兩個行動讀取器之間進行連線時，我們假設標籤擁有者之行動讀取器透過 Mobile IPv6[6] 等方法連結至網際網路找到另一方行動讀取器，所以我們環境不需要考慮因讀取器移動而找不到無線設備的問題。

3. 電子標籤與行動讀取裝置之間透過無線傳輸的方式進行通訊，如圖 1 中的連線(3)所示。由於電子標籤以及行動讀取裝置具有可移動性質，且無線傳輸之訊號直接在開放空間中廣播傳送，因而在無線通訊的過程中，可能遭受來自惡意攻擊者的竊聽、重送攻擊、中間人攻擊等各種危害，造成電子標籤擁有者的個人資訊洩漏[30] 及隱私權的安全受到威脅。所以我們在電子標籤與行動讀取裝置間，透過以加密訊息的方式來進行通訊。由於加密訊息的方法會受限於電子標籤的運算能力，因而無法使用現行的加密演算法。因此必須使用實作於 RFID 標籤的加密演算法如 M. Feldhofer 等人提出以 AES-128 演算法的方法[20] 或是 S. Kumar 與 K. Sakiyama 等人提出利用橢圓曲線密碼學方法進行加密[18] [28] 。但這類加密方法計算負擔仍太大，所以我們的 CAOT 利用後端資料庫和電子標籤的共享的金鑰Kx_a^i以及採用其他輕量級的加密演算法來進行電子標籤訊息的加密，如：DESLite[5] 和 Grain[22] 。我們在本文中將著重探討 RFID 標籤與行動讀取器之間通訊協定的安全問題，並且在我們提出的 CAOT 方法中解決這些安全問題。

由於我們的所有權轉移協定跨越一個管理區域，而讀取器之後端管理伺服器無法確認非後端管理伺服器所管轄之另一讀取器的身份，因此伺服器必須透過現有機制(如 Object Name Server)註冊並可查詢其位置。另外需要利用現有之方法(如：PKI[13])對所有權轉移雙方之身份進行雙向認證，取得執行所有權轉換用之階段金鑰(Session key)，並透過此方法來達到設備之間的雙向認證。舉例來說，行動讀取器和管理伺服器必須在數位憑證中心(CA)註冊並取得憑證。每次進行通訊前驗證憑證的正確性與時效性，並使用憑證中的公鑰及私鑰進行加密通訊和數位簽章，交換四把彼此的階段金鑰 SK_1、SK_2、SK_3、SK_4。

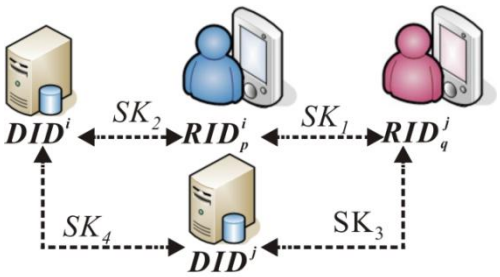

圖 2 資料庫與讀取器間的階段金鑰交換示意圖

如圖 2 所示，讀取器RID_p^i持有人想將其擁有的標籤物品之所有權轉移給已知讀取器RID_q^j之持有人時，RID_p^i與RID_q^j之間會透過現有機制交換階段金鑰 SK_1。同樣地，當RID_p^i與管轄RID_p^i的伺服器DID^i進行通訊時，會交換階段金鑰 SK_2，RID_q^j與管轄RID_q^j的伺服器DID^j所交換的階段金鑰為 SK_3。由於伺服器DID^i與伺服器DID^j之間會進行通訊，因此亦會交換階段金鑰 SK_4。當所有權轉換雙方之伺服器和讀取器擁有彼此溝通用的階段金鑰後，雙方就可以利用這四把金鑰進行所有權轉移方法溝通訊息的加密和認證。

三、跨領域所有權轉移方法

CAOT 協定分為兩個階段進行所有權轉移。第一階段協定，如圖 3、圖 4 所示，進行所有權轉移的前置作業，使得新擁有者之讀取器有能力和該電子標籤進行雙向認證，以及交換一個只有原有伺服器和電子標籤共享的階段性金鑰，並透過此階段性金鑰來確保所有權轉換完成前，未被授權之伺服器與讀取器在第二階段協定無法辨識該電子標籤，以保護電子標籤在所有權轉移前的安全。第二階段將電子標籤所有權轉移轉移至新擁有者，並確保舊擁有者無法再對該標籤進行讀取。在我們的協定中以 *E(,)*表示使用傳統對稱金鑰的加密方法，如 AES，對訊息進行加密。以 *LE(,)*表示用 DESLite[6]或 Grain[24] 等輕量對稱金鑰加密演算法。其中 *E(,)*和 *LE(,)*第一個參數表示加密演算法使用的金鑰，第二個參數表示需要加密的訊息，例如 $LE(Kx_a^i, TID_a^i||r_2)$，表示利用金鑰Kx_a^i將$TID_a^i||r_2$用輕量加密演算法變成密文，其中 "||"表示連結兩訊息的符號。

所有權轉換第一階段的部分主要分為三個部分，(1) 用來進行原物品持有者讀取器和物品電子標籤交換所有權轉移時雙向認證，並交換讀取器和電子標籤的階段性金鑰。(2)確認金鑰完成交換。(3)原標籤持有者之讀取器將金鑰移轉至新擁有者之讀取器，其三部分詳述如下。

第一部分包含第一階段協定的訊息 1 至 5，用以進行電子標籤與讀取器的雙向認證，並由伺服器產生標籤所有權轉移所需的階段性金鑰Ky_a^i、共享金鑰Kt_a^i與共享秘密S_a^i。當讀取器RID_p^i之持有者要將電子標籤TID_a^i轉移給讀取器RID_q^j之持有者，且已經獲得其和伺服器DID^i與讀取器RID_q^j溝通加密使用的兩把共享金鑰 SK_1 和 SK_2 時，RID_p^i會向欲轉出的電子標籤TID_a^i發出所有權轉移請求。標籤TID_a^i在收到請求訊息後，利用和資料庫DID^i共享的金鑰Kx_a^i和輕量加密演算法將隨機數 r_2 與TID_a^i加密後送給讀取器RID_p^i。在此 r_2 可以確保每次標籤傳出的訊息皆為不同，使攻擊者無法利用兩次訊息間的關係來追蹤標籤擁有者之位置。接著RID_p^i將標籤回傳的訊息 2 連同轉出對象的讀取器識別資訊RID_q^j與伺服器識別資訊DID^j傳送給RID_p^i的管理伺服器DID^i，如訊息 3 所示，以要求DID^i對標籤進行所有權轉移協定第一階段。DID^i在收到訊息 3 後，會先驗證RID_p^i是否為DID^i所管轄，若驗證成功，則利用金鑰Kx_a^i解密 $LE(Kx_a^i, r_2||TID_a^i)$，並比對識別碼TID_a^i來認證電子標籤。在完成標籤認證後，將隨機產生的金鑰Ky_a^i、Kt_a^i、共享秘密S_a^i、隨機數r_2、識別碼TID_a^i與指令 OT_1 加密為設定標籤之訊息，如圖 3 中的 M_3。而此訊息和金鑰Kt_a^i、共享秘密S_a^i會一同傳送給讀取器RID_p^i，如訊息 4 所示，並於伺服器上記錄轉移目標識別碼DID^j與RID_q^j。讀取器RID_p^i在收到訊息 4 後取出S_a^i和Kt_a^i後，將設定標籤之訊息傳送給標籤，如訊息 5 所示。在標籤收到訊息 5 後，利用標籤和資料庫共享的金鑰Ky_a^i解密，並比對識別碼TID_a^i，藉此方法驗證讀取器所傳送的訊息。

若讀取器成功通過認證，則電子標籤依據指令 OT_1 進行所有權轉移設定，更新第二階段原擁有者伺服器與標籤共享的金鑰Ky_a^i、Kt_a^i、標籤與新擁有者共享的秘密值S_a^i，並使表示標籤是否正在進行所有權轉移的旗標$flag_a^i$由尚未進行的 *None* 改變為正在進行所有權轉移的 *OT*。由於伺服器與讀取器尚未確認標籤是否完成階段性金鑰Ky_a^i的設定，為避免非同步而造成無法讀取，所以在完成設定後回傳$OT_{1success}$，以告之標籤設定成功。若驗證失敗，則回傳隨機數訊息，如訊息 6 所示。在RID_p^i收到訊息 6 後，則會轉送該訊息給DID^i，如訊息 7 所示，使伺服器可依此訊息來判斷標籤是否設定完成。若未成功更新標籤，則必須重新進行所有權轉移第一階段。在DID^i收

到訊息 7 後，若為$OT_{1success}$設定成功，則回傳$OT_{1success}$訊息給RID_p^i，如訊息 8，以告知標籤設定完成，反之則回傳失敗訊息給RID_p^i。一旦RID_p^i接收到失敗訊息，下次必須從重新進行所有權轉移第一階段程序。

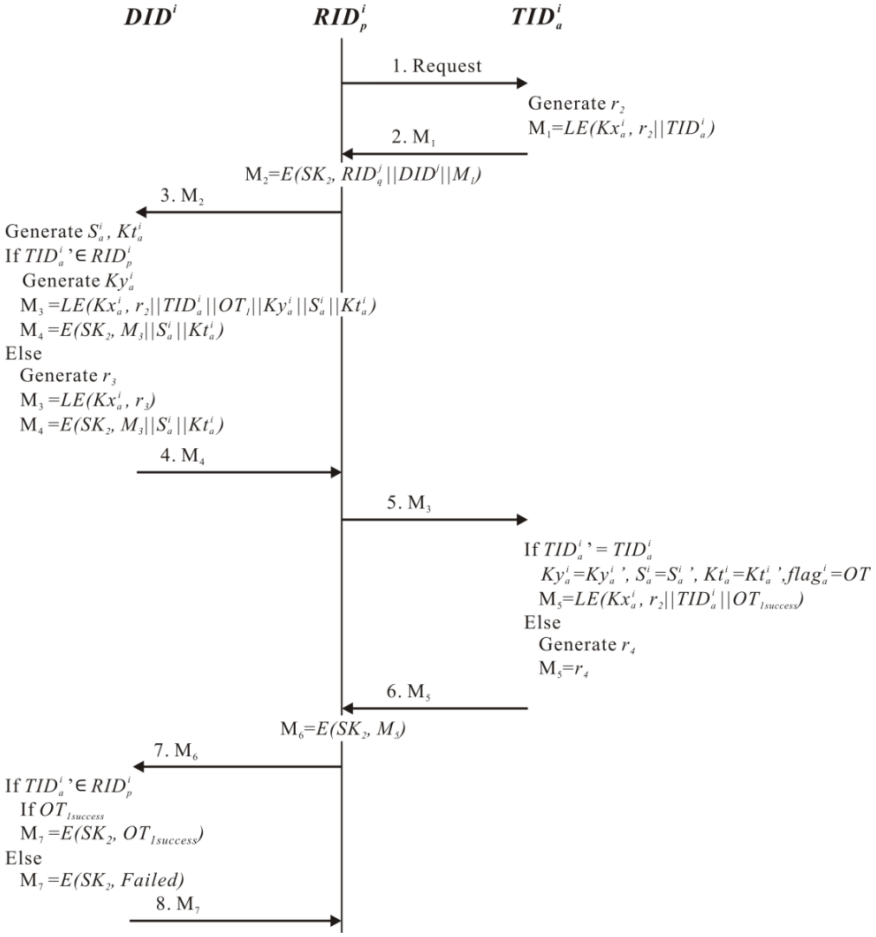

圖 3 所有權轉移第一階段，標籤與讀取器認證和標籤設定程序

在RID_p^i收到DID^i告知標籤完成設定的訊息後，一旦決定要進行所有權轉移，則會將識別碼DID^i、暫存的金鑰Kt_a^i與共享秘密S_a^i、r_1 加密傳送給指定之轉移目標讀取器RID_q^j，如圖 4 所示。

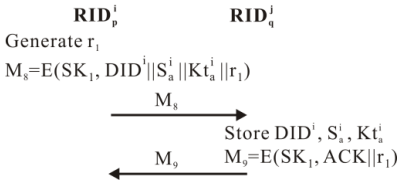

圖 4 所有權轉移第一階段，傳送認證金鑰

在RID_q^j收到RID_p^i的訊息後，會從訊息中擷取認證電子標籤的訊息S_a^i、Kt_a^i和所有權轉出管理伺服器資訊DID^i並將這些資料儲存於RID_q^j的關聯性資料表，如表格 1 所示。

表格 1 RID_q^j的關聯性資料表

共享秘密 s	共享金鑰 t	管理伺服器識別編號
S_a^i	Kt_a^i	DID^i
S_b^i	Kt_b^i	DID^i

在新讀取器RID_q^j取得能在下一階段認證電子標籤的資訊後，則完成所有權轉移協定第一階段。接下來轉入讀取器RID_q^j即可進行 CAOT 所有權轉移協定第二階段，如圖 5 所示，標籤的新擁有者將與所有權轉出管理伺服器DID^i進行驗證程序，以完成所有權轉移。

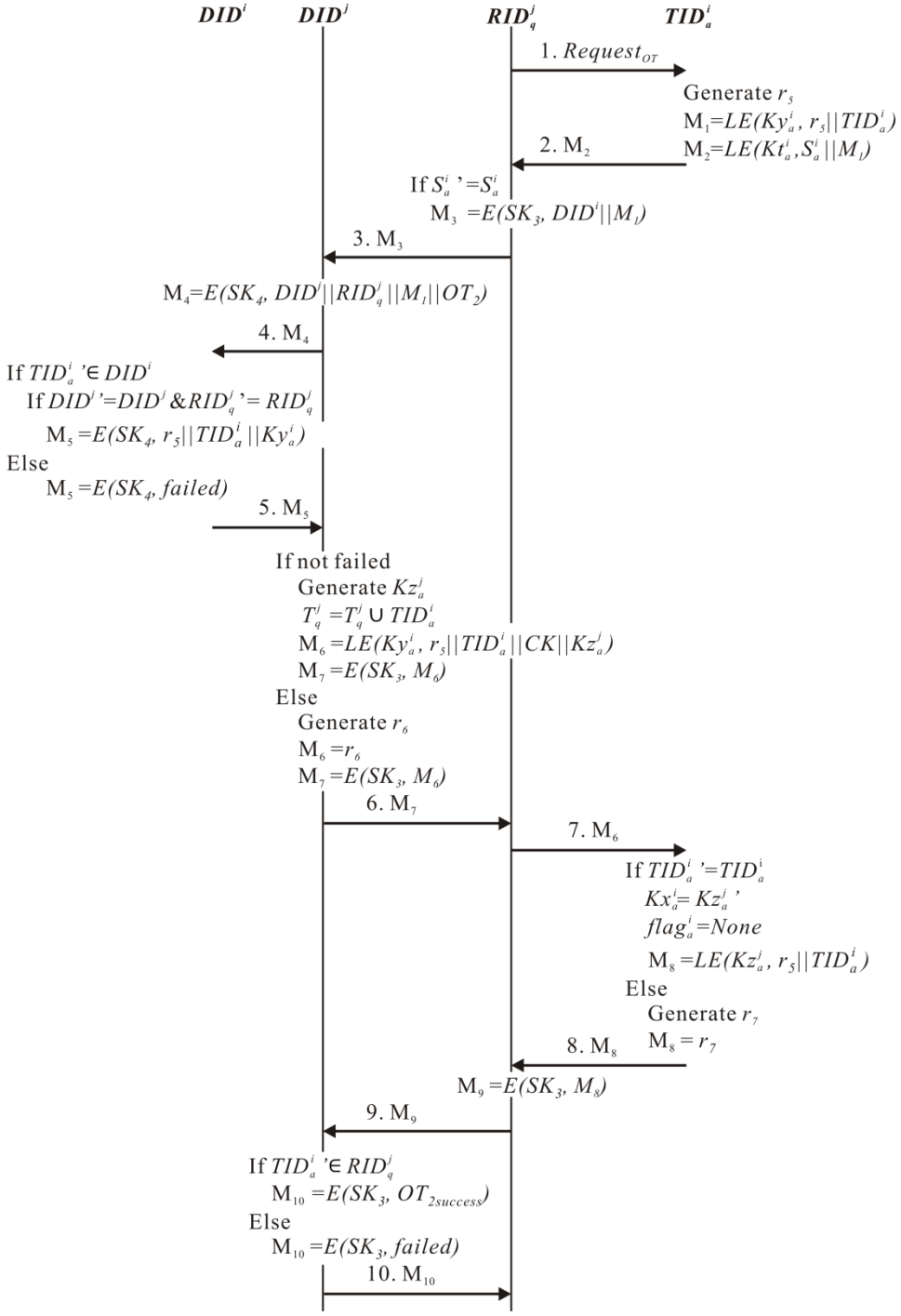

圖 5 所有權轉移第二階段，標籤金鑰更新與擁有者變更程序

所有權轉移第二階段主要分為四個部分，(1)讀取器與電子標籤進行認證程序 (2)新標籤管轄伺服器與原標籤管轄伺服器進行認證與所有權轉移 (3)伺服器進行標籤金鑰變更 (4)確認標籤

金鑰是否變更完成。

在第一部分包含訊息 1 至 3，新標籤擁有者使用行動讀取器RID_q^j發送所有權轉移請求$Request_{OT}$給標籤TID_a^i。標籤在收到請求後，將產生的隨機數 r_5、標籤識別碼TID_a^i以金鑰Ky_a^i加密，再將此加密訊息與共享祕密S_a^i以共享金鑰Kt_a^i進行第二次加密後傳送給RID_q^j，如圖 5 之訊息 2 所示。在RID_q^j收到訊息 2 後，嘗試找尋對應金鑰Kt_a^i解開密文並利用S_a^i認證電子標籤。認證通過後，將 $LE(Ky_a^i, TID_a^i)$與資料表(表格 1)中對應的伺服器識別碼DID^i傳送給欲轉入之讀取器RID_q^j的管理伺服器DID^j，如訊息 3 所示。

所有權轉入之管理伺服器收到要求所有權轉移請求和轉出伺服器之識別碼並經過現有之雙向認證方法確認雙方身分後，轉入伺服器DID^j會與轉出伺服器DID^i進行所有權轉移驗證，以取得所有權轉移的階段性金鑰Ky_a^i與標籤識別碼。首先，DID^j將自己本身的識別碼DID^j、讀取器識別碼RID_q^j以及標籤訊息傳送給 DID^i，如訊息 4 所示，以進行所有權轉移的驗證。DID^i收到訊息後，藉由解析標籤訊息 M_1 以確認自己為轉移標籤TID_a^i之管轄伺服器，並確認DID^j和RID_q^j的識別碼是否符合先前登錄所指定轉移的目標。若發生驗證失敗，則回傳錯誤訊息給DID^j；若驗證成功，則DID^i如訊息 5 所示回傳隨機數 r_5、所有權交換金鑰 $Ky_a{}^i$ 以及標籤識別碼TID_a^i給DID^j，並使轉入伺服器具有該標籤相關資訊查詢能力。

在所有權轉入伺服器通過認證得到標籤所有權轉換之必要資訊後，則可進行標籤金鑰Kt_a^i更換與指定擁有者來解除原有標籤擁有人對該標籤之所有權。在DID^j取得所有權轉移金鑰Ky_a^i後，將TID_a^i加入讀取器RID_q^j所管轄之電子標籤群T_q^j內。將隨機數 r_5、標籤識別碼TID_a^i、更換金鑰指令 CK 以及DID^j隨機產生的新標籤管理金鑰Kz_a^i以金鑰Ky_a^i加密為標籤更新金鑰訊息，傳送給RID_q^j，如訊息 6 所示，以進行標籤金鑰更換。同時 DID^j 的資料庫將對新標籤進行登錄，記錄其金鑰Kz_a^i、Ky_a^i、標籤資訊相關資訊與標籤識別碼TID_a^i，並指定標籤的所有權讀取器為RID_q^j。在RID_q^j收到訊息 6 後，將標籤金鑰更新訊息轉 M_6 送給標籤TID_a^i，以進行標籤金鑰更新，如訊息 7 所示。標籤TID_a^i在收到來訊息 7 後，會以金鑰Ky_a^i解密訊息，並驗證解密後的標籤識別碼TID_a^i是否符合。若驗證不符合則回傳隨機數訊息；若是驗證符合，則更新金鑰Kx_a^i為金鑰Kz_a^i，並且將標籤的狀態旗標$flag_a^i$由表示所有權轉換中的 OT 更改為所有權轉換完成的 $None$。最後以新的金鑰Kz_a^i加密隨機數r_5與標籤識別碼TID_a^i回傳給RID_q^j再轉送至後端伺服器，讓伺服器確認是否轉移成功，如訊息 8 所示。

最後，RID_q^j將收到的訊息 8 轉送至DID^j進行驗證，如訊息 9，使伺服器能確認是否正確完成標籤所有權轉移。而DID^j在收到訊息 9 後，嘗試以金鑰Kz_a^i將標籤訊息解密，並驗證識別碼TID_a^i是否符合，以確認標籤金鑰是否更新。若驗證資料不符，則回傳錯誤訊息告知RID_q^j驗證失敗；若是資料驗證正確，則在資料庫中記錄所有權交換成功、並且回傳$OT_{2success}$給RID_q^j，以告知所有權轉移完成。

四、安全性分析

在這此章節我們將針對我們提出的 CAOT 協定進行安全性分析。由於我們假設有線網路、個人行動通訊上網和 IEEE802.11 的無線上網方式因有對應的安全架構而可被信任，並且在有線網路和無線網路方面，都利用現有之機制，透過憑證驗證程序取得階段金鑰，進行加密通訊來確保通訊的安全性。因此在此節分析 CAOT 協定中行動讀取器與電子標籤之間通訊的安全性。

機密性：電子標籤送出的訊息利用和管轄標籤的

伺服器共享金鑰的Kx_a^i、Ky_a^i和標籤識別碼TID_a^i加密。攻擊者因無法解讀加密的訊息而無法取得這些資訊。

防止重送攻擊：由於 CAOT 協定在每一個完整階段的通訊過程中，電子標籤會產生一個隨機數共同加密，並且與伺服器共享這個隨機數，做為每次完整階段通訊的驗證值。所以當攻擊者在下一次通訊嘗試使用搜集的資訊進行重送攻擊時，會因無法符合電子標籤所產生的隨機數而失敗。

所有權轉移的雙向認證：由於所有權轉移的時候，行動讀取器和管理伺服器會利用彼此共享的金鑰確認身份，才能進行所有權轉移。因此在攻擊者沒有共享金鑰與標籤識別碼的狀況下，無法偽造標籤或讀取器以及後端資料庫的認證訊息，且我們已經證明攻擊者無法在我們協定中進行重送攻擊。所以在所有權轉移過程可以達到雙向認證的需求。

防止中間人攻擊：由於行動讀取器和電子標籤之通訊均加密，且攻擊者無法偽照標籤或讀取器以及後端資料庫的合法的訊息。且無法利用重送攻擊來躲過我們的雙向認證機制，因此攻擊者無法假裝成標籤或讀取器來進行中間人攻擊。

所有權轉移的向前性安全：由於所有權轉移的過程中，透過階段性金鑰Ky_a^i來更新原標籤管理金鑰Kx_a^i為新標籤管理金鑰Kz_a^i。又階段性金鑰Ky_a^i為一隨機產生之暫時性金鑰，新標籤擁有者並無法透過金鑰Ky_a^i推導出先前的金鑰Kx_a^i，因此 CAOT 協定達到所有權轉移的向前性安全。

抵禦資料不同步更新的阻斷服務攻擊：CAOT 協定因在管理伺服器在更新階段會記錄所有權交換金鑰與要更換的標籤管理金鑰，因此發生標籤管理金鑰不同步更新時，管理伺服器仍有所有權交換金鑰可以解讀標籤的加密訊息，所以 CAOT 協定並不會因阻斷服務攻擊而造成的電子標籤與管理伺服器產生不同步更新，而出現標籤管理金鑰失效的問題，因此我們的方法具抵禦資料不同步更新阻斷服務攻擊之能力。

位置隱私：由於協定中所有傳輸的訊息加密時會加入隨機數，使得每次同類型訊息的加密結果不會相同，因此攻擊者無法利用同一標籤兩次傳輸訊息的關係來分析使用者為何，也無法辨識是否為同一標籤所傳出之訊息，所以無法利用標籤傳輸的訊息來追蹤標籤持有人。

隱私保護：由於 CAOT 協定達到上文敘述的安全性需求以及具抵抗安全性威脅的能力，且標籤相關資料置於管理伺服器，藉由管理伺服器的權限控管，以及通訊過程的的雙向認證，在攻擊者沒有合法讀取器的狀況，難以取得電子標籤的相關資訊，因此可以保護標籤持有人的個人隱私。

為分析我們方法的安全性相對於其它所有權轉移方法的強度，我們對[26] 和[17] 的傳統 RFID 所有權轉移方法以及楊所提出運作於 Mobile RFID 環境的所有權轉移方法[1] ，以及我們所提出的 CAOT 方法進行安全性與功能性之比較分析。

表格 2 RFID 所有權轉移方法安全性比較表

Method / Function	Osaka's et al. Method[17]	S. Fouladgar et al.'s Method[27]	楊 et al.'s Method[1]	Our Method
Reply Attack	V	V	V	V
MITM Attack	N/A	V	V	V
DoS Attack	N/A	V	V	V
Forward Security	N/A	N/A	V	V
Mutual Authentication	N/A	V	V	V
Mobile RFID	N/A	N/A	V	V
Cross Authority	N/A	N/A	N/A	V

由表格 2 我們可以得知，我們提出的 CAOT 所有權轉移方法相較於 Osaka 等人的方法提供更多的安全性支援；我們的方法將 S.Fouladgar 等人提出在兩伺服器之間進行所有權轉移概念拓展至多伺服器環境，並且解決其向前性安全問題；相較於楊等人提出的方法，我們的方法可支援 Mobile RFID 環境下進行跨伺服器所有權轉移。

五、效能分析比較

在此章節,我們將針對 CAOT 方法的計算量與儲存空間做分析。

在表格 3 的 CAOT 計算量評估表中，我們各別評估兩階段協定中標籤、讀取器與伺服器所需的計算量。我們以 T_E 表示進行一次加解密通訊所需的時間，T_{LE} 表示進行一次輕量級加解密所需的時間，T_{RNG} 表示產生一個隨機數所需的時間。

表格 3 CAOT 計算量評估表

第一階段	TID_a^i	$3T_{LE}+T_{RNG}$
	RID_p^i	$6T_E+T_{RNG}$
	DID^i	$4T_E+3T_{LE}+3T_{RNG}$
	RID_q^j	$2T_E$
第二階段	TID_a^i	$4T_{LE}+T_{RNG}$
	RID_q^j	$4T_E$
	DID^j	$6T_E+T_{LE}+T_{RNG}$
	DID^i	$2T_E+T_{LE}$
總計		$23T_E+9T_{LE}+6T_{RNG}$

在表格 3 中可見,我們的方法因兩階段協定具有可分割性，在進行完第一階段協定後，可以隔一段時間再進行第二階段協定來完成所有權轉移，所以標籤上的運算量仍是電子標籤所能負擔的範圍。因此我們所提出的方法是可行的。

Koralalage 等人提出的方法[16] 中，對 EPC 規格之標籤進行擴展，假設使用 Martin Hell 等人提出的 Grain1 stream 加密演算法保護標籤送出的訊息。我們將參考其方法來評估我們方法在標籤上所需使用的記憶體空間，在表格 4 中，以括號內之值來表示。

表格 4 電子標籤儲存空間評估

TID	Tag ID (96bits)
Kx	Authentication key (80bits)
Ky	Authentication key (80bits)
Kt	Authentication key (80bits)
S	shared secret (48bits)
flag	Status flag (1 bit)
r	Nonce generated by tag (40bits)

由表格 4 電子標籤儲存空間評估可得知，我們方法電子標籤所需的記憶體空間只要 425bits，在 EPC 規格最大記憶體 512bits 的範圍內[9] 。所以我們提出的 CAOT 方法之記憶體需求，對 EPC 等級的電子標籤可負擔之範圍，因此在低成本的電子標籤上，我們的方法是可行的。

表格 5 相關研究計算量比較表

方法名稱	設備	所有權轉移協定計算量
S. Fouladgar et al.'s Method[27]	標籤	$T_{LE}+T_{RNG}$
	讀取器	T_{RNG}
	後端伺服器	$2T_{LE}+2T_{RNG}$
楊 et al.'s Method[1]	標籤	$11T_H+1T_{RNG}$
	讀取器	$2T_H+T_{RNG}$
	後端伺服器	$8T_H+T_{RNG}$
Our Method	標籤	$7T_{LE}+2T_{RNG}$
	讀取器	*None*
	後端伺服器	$5T_{LE}+4T_{RNG}$

在表格 5 相關研究計算量比較表，將 S. Fouladgar 等人提出之方法[26] 以及楊等人提出之方法[1] 與我們的 CAOT 方法進行計算量之比較。由於 S. Fouladgar 直接假設其方法在後端伺服器與讀取器之間透過安全的通道進行，並未說明透過何種機制，因此為站在公平的角度進行比較，我們不對建立安全通道所需的計算量進行分析，Osaka 等人方法因無法達到安全上的需求，因此我們不列入計算。

我們的方法在讀取器上所需的計算量優於另兩者之方法。在後端伺服器上所需的計算量相較於楊等人以及 S. Fouladgar 所提出的方法來得少。另外，在標籤上的計算量仍略優於楊等人的方法，但因為我們所提出的所有權轉移具有跨越管理伺服器的能力，所以標籤需要和兩個伺服器進行認證和所有權轉換，所以較 S. Fouladgar 提出的方法所需的計算量來得多。不過，依照我們在表 3 和表 4 分析在 RFID 標籤上利用 DESLit[5] 或 Grain[22] 實做加密電路以及我們的所有權交換協定所需的邏輯閘數可在 3000 個邏輯閘內達

成，因此我們提出的 CAOT 方法仍是可在 RFID 上被實行。

六、結論

在未來 RFID 的應用會更加的廣泛，並且隨著 Mobile RFID 的發展，帶動行動電子商務的發展，進而提供更多個人化的應用服務與商業服務。因此在 Mobile RFID 環境下進行交易活動，將成為未來趨勢，而所有權轉移的功能也將不可或缺。當生活周遭的許多物品都嵌入有 RFID 標籤，且提供相關服務的 RFID 管理伺服器的選擇越來越多樣化，將會延伸出在多伺服器進行所有權轉移的議題。因此我們提出一個跨所有權管理區域的所有權轉移協定，來解決利用隸屬於不同後端管理伺服器之行動讀取器以 RFID 標籤進行所有權轉換的問題，並且證明我們提出的方法可以抵禦竊聽、重送攻擊、中間人攻擊、阻斷服務攻擊等常發生於 RFID 通訊的攻擊，並且於利用 RFID 網路進行所有權轉移時滿足向前安全性與雙向認證的安全性需求，且在效能分析可於 RFID 標準提供之邏輯閘數目內完成，標籤儲存空間分析也滿足 EPC 標準所提供的容量範圍內，因此可使得使用者在安全的狀況下於 RFID 網路內進行跨領域所有權轉移。

七、參考文獻

[1] 楊明豪、羅嘉寧、李昱霖，“Mobile RFID 雙向認證及所有權轉移，” Taiwan Academic network conference 2008 , pp. 133-138.

[2] 3GPP, “Mobile-services Switching Centre-Base Station System (MSC-BSS) interface; layer 3 specification (Release 8),” 3GPP TS 48.008, March 2009.

[3] 3GPP;TSG SA, “3G Security; Security Architecture (Release 8),” 3GPP TS 33.102, March 2009.

[4] A. Juels, “RFID security and privacy: a research survey,” IEEE Journal on Selected Areas in Communications, 2006.

[5] A. Poschmann, G. Leander, K. Schramm, C. Paar, “New Light-Weight Crypto Algorithms for RFID,” Circuits and Systems, 2007, PP. 1843-1846.

[6] D. Johnson, C. Perkins, “Mobility Support in IPv6,” RFC 3775, June 2004.

[7] D. M. Konidala, K. Kim, “Mobile RFID Security Issues,” Symposium on Cryptography and Information Security SCIS, Hiroshima, Japan, IEICE, January 2006.

[8] D. Molnar, A. Soppera, and D. Wagner, “A scalable, delegatable pseudonym protocol enabling ownership transfer of RFID tags,” Proc. Sel. Areas Cryptography, B. Preneel and S. Tavares, Ed. New York: Springer-Verlag, 2005, Lecture Notes in Computer Science.

[9] EPCglobal Inc, Retrieved July. 1, 2009, from the World Wide Web: http://www.epcglobalinc.org/home

[10] Eun-Jun Yoon, Kee-Young Yoo, “Two Security Problems of RFID Security Method with Ownership Transfer,” Network and Parallel Computing, 2008. NPC 2008. pp. 68-73.

[11] HITACHI RFID Solutions - The Mu Chip Products Retrieved July. 1, 2009, from the World Wide Web: http://www.hitachi-eu.com/mu/Products/Mu%20Chip.htm

[12] Institute of Electrical and Electronics Engineers, Inc., “Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Medium Access Control (MAC) Security Enhancements,” Std.802.11i-2004, July, 2004.

[13] Internet X.509 Public Key Infrastructure Certificate Management Protocols, Retrieved July. 1, 2009, from the World Wide Web: http://www.ietf.org/rfc/rfc2510.txt

[14] P. Jappinen, H. Hamalainen, “Enhanced RFID Security Method with Ownership Transfer,” Computational Intelligence and Security, 2008. Volume 2, pp. 382-385.

[15] K. Finkenzeller. RFID-Handbook. Carl Hanser Verlag M¨unchen, 2nd edition, April 2003.

[16] K. H. S. S. Koralalage, M. R. Selim, J. Miura, Y. Goto, and J. Cheng, "POP Method: An Approach to Enhance the Security and Privacy of RFID Systems Used in Product Lifecycle with an Anonymous Ownership Transferring Mechanism," In Proc. SAC, ACM Press, 2007, pp. 270-275.

[17] K. Osaka, T. Takagi, K. Yamazaki, and O. Takahashi, "An Efficient and Secure RFID Security Method with Ownership Transfer," in International Conference on Computational Intelligence and Security, pp. 1090-1095, Nov. 2006.

[18] K. Sakiyama, L. Batina, N. Mentens, B. Preneel, and I. Verbauwhede, "Small-footprint ALU for public-key processors for pervasive security," presented at the Workshop RFID Sec., Graz, Austria, 2006.

[19] H. Lee and J. Kim, (2006), "Privacy Threats and Issues in Mobile RFID," Proceedings of the First International Conference on Availability, Reliability and Security (ARES'06), IEEE Computer Society, pp. 1-5.

[20] M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong authentication for RFID systems using the AES algorithm," in Proc. Workshop Cryptographic Hardware Embedded Syst.(CHES 2004), Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, vol. 3156, pp. 357-370.

[21] M.-H. Yang, J.-N. Luo, **"**Authentication Protocol in Mobile RFID Network," The Fourth International Conference on Systems (ICONS'09), 2009 pp. 108-113.

[22] Martin Hell, Thomas Johansson, WilliMeier, "Grain - a stream cipher for constrained environments," International Journal of Wireless and Mobile Computing, Volume 2, Issue 1 (May 2007), Pages 86-93

[23] Namje Park, Youjin Song, Dongho Won, "Policy and Role based Mobile RFID User Privacy Data Management System," Network Operations and Management Symposium, PP. 1003-1006, 2008.

[24] NFC Forum, Retrieved July. 1, 2009, from the World Wide Web: http://www.nfc-forum.org/home

[25] S. Fouladgar and H. Afifi(2007) , "A Simple Delegation Scheme for RFID Systems (SiDeS) ," IEEE International Conference on RFID,2007 ,pp.1-6.

[26] S. Fouladgar and H. Afifi., "A simple privacy protecting scheme enabling delegation and ownership transfer for RFID tags," Journal of Communications, 2(6):6-13, November 2007.

[27] S. Fouladgar and H. Afifi., "An efficient delegation and transfer of ownership protocol for RFID tags," In First International EURASIP Workshop on RFID Technology, Vienna, Austria, September 2007.

[28] S. Kumar and C. Paar, "Are standards compliant elliptic curve cryptosystems feasible on RFID?," presented at the Workshop RFID Sec., Graz, Austria, 2006.

[29] Sony Felica Web Site, Retrieved July. 1, 2009, from the World Wide Web: http://www.sony.net/Products/felica/index.html

[30] Vaudenay, S., "On Privacy Models for RFID," ASIACRYPT 2007. LNCS, vol. 4833, pp. 68-87. Springer, Heidelberg (2007).

[31] R. Want, "An introduction to RFID technology," Pervasive Computing, IEEE Volume 5, Issue 1, Jan.-March 2006 Page(s):25 - 33 Digital Object Identifier 10.1109/MPRV.2006.2

[32] Y. Seo, T. Asano, H. Lee, and K. Kim, "A Lightweight Protocol Enabling Ownership Transfer and Granular Data Access of RFID Tags," the 2007 Symposium on Cryptography and Information Security Sasebo, Japan, Jan. 2007, pp. 23-26.