無線射頻識別票據可行性研究

張瑞益
信聯社南區資訊中心科長
國立成功大學工程科學系碩士在職專班
scu054@mail.scu.org.tw

摘要

國內的金融市場日趨自由化、國際化、證券化及電腦化，使銀行經營環境產生了極大的變化，金融環境亦日趨複雜，而金融相關資訊科技的日新月異，改變了競爭型態。在金融機構投入大量成本於資訊科技的同時，新的資訊科技是否能為其經營績效帶來預期的收益，是一個值得深思探討的議題。

為順應金融百貨化及資訊科技應用的潮流趨勢，結合電子通訊科技而發展的電子銀行服務，成為銀行業參與市場競爭的關鍵資源。故本研究在於探討金融機構之票據，使用無線射頻識別系統(Radio Frequency Identification, RFID)架構，結合票據上磁性墨水字元識別(Magnetic Ink Character Recognition, MICR)的鍵印，以加強票據的防偽功能、防污辨識力，並有效改善銀行櫃員峰日處理票據存款戶票據兌領效率，減少櫃員操作時的錯誤及負擔，可行性之評估研究。

關鍵詞：無線射頻識別、讀取器、電子標籤、發票人、付款行

ABSTRACT

The domestic financial market trend liberalization, the internationalization, the securitization and the computerization, caused the bank management environment to have the enormous change, the financial environment day by day has been also complex, but financial correlation information science and technology changing with each new day, changed the competition condition. While financial organ investment massive costs to information technology, information technology whether can bring the anticipated result for its management achievements, is subject which is worth discussing.

Complied with the financial general merchandise and the information advance in technology tendency, the bonding electron communication technology development electronic banking service, become the bank to participate in one of market competition essential resource bases. Therefore this study discusses a note which probes into the financial institution, use Radio Frequency Identification, RFID Structure, Magnetic Ink Character Recognition, MICR to accord with the check Key print, anti-counterfeit in order to strengthening note function, antipollution to last discernment, and the persons who improve the bank cupboard effectively deal with check account's cash efficiency on day in peak, mistake and burden when the persons who reduce the cupboard operate, the assessment research of feasibility.

Keyword：Radio Frequency Identification、Reader、Tag、Drawer、Paying Bank

1．緒論

1．1 研究背景與動機

金融業的興衰不但與民生息息相關，金融業的營運方向更時刻掌握了社會經濟的脈動。我國金融業近年來在政府金融改革政策的驅動下規模日益壯大，而其所提供的金融商品及服務也不斷地推陳出新，國內金融業的蓬勃發展與競爭由此可見一斑。

隨著資訊科技的日新月異，金融業資訊化

的發展更呈現出嶄新的風貌，銀行業者為了提供客戶更完整而方便的金融服務，以期由眾多競爭者中獲得青睞，無不藉著資訊科技這個競爭利器。為滿足顧客，銀行業者積極投入資金結合先進的電子、通訊科技，開發電子化作業服務，以利於金融商品及業務創新發展、並達到降低作業成本，提升經營效能、創造利潤等多重目的。

1. 2 研究目的

本研究的目的以銀行為研究對象，探討銀行以資訊科技為基礎，引進RFID的運用，結合票據上磁性墨水字元(MICR)的鍵印，以加強票據的防偽功能、防污辨識力，並有效改善銀行櫃員峰日處理票據存款戶票據兌領效率，減少櫃員操作時的錯誤及負擔。

1. 3 研究範圍

本研究的範圍在於探討銀行業建置RFID票據時，所運用之RFID技術和所採用之驗證安全機制，在實務上運用之可行性評估，以做為銀行業建置推行RFID票據時之決策參考。

1. 4 研究限制

本研究受限於無法取得具有讀寫功能之RFID TAG設備，將只針對RFID票據建置及使用模擬探討，希望能透過模擬情境分析，可以提供給經營決策主管作一參考。

2 .文獻的探討與回顧

2.1 理論基礎

2.1.1 RFID應用基本概念

RFID是一種無線射頻物件辨識技術，由電子標籤（Tag）、讀取器（Reader）與軟體系統設計整合（Middleware & System Integration）三者串聯而成的架構(圖1)[5]。其動作原理是由Reader發射特定頻率之無線電波給Tag，用以驅動Tag之電路將晶片內部之資料傳回，Reader便可以接收到資料。

一、電子標籤(Tag)：通常以電池的有無區分為被動式和主動式兩種類型。被動式Tag 是接收讀取器所傳送的能量，轉換成電子標籤內部電路操作電能，不需外加電池；可達到體積小、價格便宜、壽命長以及數位資料可攜性等優點，而天線在電子標籤和讀取器間傳遞射頻信號。

二、讀取器(Reader)：利用高頻電磁波傳遞能量與訊號，電子標籤的辨識速率每秒可達50 個以上。可以利用有線或無線通訊方式，與應用系統結合使用，一般設計為掌上型或固定式。

三、軟體系統設計整合(Middleware & System Integration)：具有傳遞(Passing)資訊、解譯資料、安全性、資料廣播、錯誤恢復、定位網路資源、提供除錯工具等特性並結合資料庫管理系統、電腦網路與防火牆等技術，提供全自動安全便利的即時監控系統功能。

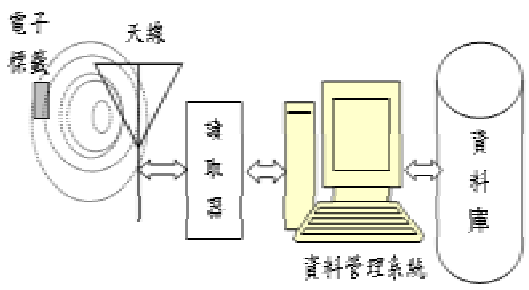

圖 1 無線射頻識別系統架構圖

2.1.2 RFID國際標準

國際上的RFID 標準包括三大陣營，為ISO系列、EPC 系列及日本的UID 系列。2006 年7月中旬，EPCglobal 於2004 年12 月建立的第二代電子標籤空中介面規範，經過ISO 審核後被批准為Ｃ類UHF 電子標籤標準，列入ISO/IEC18000-6修訂標準。由於生產規模增大和成本的降低，RFID 的發展正在邁入普及化發展階段。國際上幾大標準化組織正加緊制定RFID 的相關標準，而美國、歐洲和日本等發達國家正在佈局國際標準的主導權和產業主導權。

2.1.3 RFID與MICR功能比較

為使票據交換清算作業達到迅速正確，並減輕人力負荷目的，採自動化處理方法，使票據上加印的磁性墨水字輸入電子閱讀分類機，閱讀票面上磁字的銀行代號、金額、日期等等資訊，再予分類並核計，這是全世界各大票據交換所採用的一種技術，也就是」磁性墨水字體辨認」， 通稱磁碼， 英文全名為「Magnetic Ink Character Recognition」，簡稱MICR，在世界上有兩種常用字體系統，一種是CMC-7即歐洲通用的符號，而另一種是E-13B，是美國國家標準規格，也是我國所採用的字體，而RFID不同於MICR，如表1。

表1 RFID與MICR功能比較

功能	RFID	MICR
運算處理	可	無
讀取數量	可同時多個	一次一個
傳遞訊號	被動式或主動式	被動式
通信距離	遠，數公分至數公尺	近，50公分
讀取光線需求	不需光線即可讀取、更新	需要光線
資料容量	多(數萬bytes)	少(數十bytes)
讀寫能力	電子資料可以反覆讀寫（R/W）	號碼資料不可更新
讀取方便性	輕薄且隱藏於包裝內仍可讀取	需看得見且清楚
對環境變化的容忍度及耐污性	高	低
防偽機制	有	無

2.2 相關文獻

在鄭博仁、陳林福、陳品儀、謝德鑫撰「有價票證防偽架構」一文中指出[3]，系統只是防偽功能之一，還需採用多項特殊物理防偽技術，例如：特殊紙張、凸起觸感、水印、金屬油墨、變色油墨、安全線及光影變化箔膜等特殊設計，使一般民眾可用肉眼或簡單儀器加以辨識，但是偽造難度高，也使仿冒者難以得逞。奚正德、張克章「RFID相關應用與安全機制簡介」研究指出[4]，RFID在鈔票中之應用應注意，RFID鈔票要具備保護隱私的能力，應預防未授權的追蹤，進而改變RFID標籤內容，使用加密技術改變RFID資訊，以避免非法者追蹤，另重複加密時可使明文未變更下，顯示出不同的密文；提出安全的解決策略上有兩個重要問題必須注意：(i)重複加密行為要在被授權者的合法時間內實施。(ii)新的資訊是確認經過驗證的，才能取代舊資訊。

3.研究設計

3.1 研究方法

本研究經由相關文獻推論出RFID票據設計時應探討之五大構面，茲簡述整理如下：

3.1.1 RFID票據之便利性

由於RFID票據之規劃，係以加強票據的防偽功能、防污辨識力，並有效改善銀行櫃員峰日處理票據存款戶票據兌領效率，減少櫃員操作時的錯誤及負擔為目標，因此，使用操作上應更趨便利簡單，讓使用者易於接受。

3.1.2 RFID票據之成本效益

金融機構開發電子化作業服務，在於降低作業成本，提升經營效能、創造利潤等多重目的，使用RFID票據所獲得之效益應大於所產生之各項費用成本。

3.1.3 RFID票據之流通性

台灣票據交換所票據統計資料顯示台灣地區2005.11~2006.10一年交換票據數量達1億五千萬張，RFID票據之設計應注意台灣地區票據使用人之使用習慣，如何讓發票人只要增加少許設備和費用，即可享有票據的防偽功能及與後端應用系統整合運用的便利性，才有大量流通之可能。

3.1.4 RFID票據之保護隱私能力

由於RFID運用原理特性，無法保障票據持

有人在持有票據期間的隱私不被洩漏，設計採用怎樣的安全機制以預防非法追蹤、非法變更、讀取RFID票據資料，甚至破壞RFID票據使之失效。

3.1.5 RFID票據之防偽機制

探討設計RFID票據在製發階段、開立階段、提示兌付階段，各階段之防偽機制運用。

3.2 RFID票據建置分析

RFID票據的使用必須符合政府及相關單位有關票據存款業務及電子化作業服務之相關規定，例如「銀行法」、「票據法」、「電子簽章法」、「金融機構辦理電子銀行業務安全控管作業基準」、台灣票據交換所相關作業規定及金融機構內部作業手冊等相關規定。

考量一個簡單的票據防偽系統架構，讓所有資料存放於無線射頻識別標籤上並加入電子簽章，且只有合法的使用者才能讀取驗證。票據加上無線射頻識別標籤(TAG)後，還需將金融機構的原有MICR鍵印機加裝讀取TAG的功能，或在金融機構及發票人端(客戶端)單獨裝置TAG讀取器(Reader)，將可以快速又大量的輸入鑑別票據真偽。

4 .個案探討

假設國內某一金融機構計劃推行RFID票據，其相關建置背景資訊及構想，概述如下：

4.1背景資訊

4.1.1 專有名辭說明

各專有名辭說明如下：

一、 銀行櫃員：負責銀行櫃檯業務與操作之人員，通常分為一線式全能櫃員及二線式專屬櫃員。

二、 票據：票據法第 1 條：「本法所稱票據，為匯票、本票、及票據」。票據法第 4 條：「稱票據者，謂發票人簽發一定之金額，委託金融業者於見票時，無條件支付與受款人或執票人之票據」。

三、 票據存款：銀行法第 6 條：「本法稱票據存款，謂依約定憑存款人簽發票據，或利用自動化設備委託支付隨時提取不計利息之存款。」

四、 提示：執票人於票據發票日後一年內，出示票據請求付款人兌付之作為。

五、 票據管理資料庫：金融機構紀錄客戶領用票據票據種類、票據號碼、領用日期、回籠日期、票據狀況。

六、 票據存款應用系統：金融機構紀錄票據存款客戶基本資料、票據存款帳戶資料、支存票據管理資料、票據存款交易資料之應用系統。

七、 應付票據管理應用系統：發票人紀錄票據發票日、到期日、票據金額、執票人、票據狀況等資料之應用系統。

八、 金鑰管理應用系統：管理、產生、紀錄私鑰、公鑰之相關資訊。

4.1.2 MICR 票據樣張

MICR 票據樣張如圖 2。

圖 2 MICR 票據樣張

4.1.3 票據兌付流程

票據兌付流程如圖 3，情境說明如下：

一、正常流程說明 Normal/Main Flow)

1・票據存款客戶開戶後，填寫領用票據申請書向銀行櫃員申請領用票據，領

用張數可為單張、10 張、20 張、50 張、100 張。

1- 1・銀行櫃員依客戶票據回籠狀況及往來情形，登錄票據號碼及帳號後發出空白票據給客戶(A1)。

2・票據存款客戶(發票人)領回空白票據備用(A2)。

3・發票人依照支付需要，填具發票日(到期日)及金額於票據上後(尚可填上受款人、畫平行(交換)線、禁止背書轉讓等)，交受款人(執票人)持有(A3)。

4・執票人於票據到期時，持票存入往來銀行帳戶辦理託收或交換提示；亦可存入付款行帳戶內兌現或直接兌領現金。

5・提示行整理到期票據並鍵印票據金額後，向當地票據交換所提出票據辦理提示交換。

6・付款行至當地票據交換所辦理提示交換提回票據。

7・付款行核對到期票據印鑑、發票日、金額等要項後兌付或退票(A4)。

8・銀行櫃員可依需要查詢票據使用及回籠狀況。

二、替代流程說明(Alternative Flow)

A1・如果客戶的票據回籠狀況及往來情形未達標準，則酌減領用票據張數，回到步驟 2。

A2・如果客戶的空白票據遺失，應向開戶單位辦理掛失，結束該票據兌付流程。

A3・如果執票人的票據遺失，應向付款行辦理掛失止付，付款行應登錄事故事項並提存備付票款，結束該票據兌付流程。

A4・如果票據因故退票(印鑑不符、存款不足等)，退還票據給執票人，回到步驟 4。

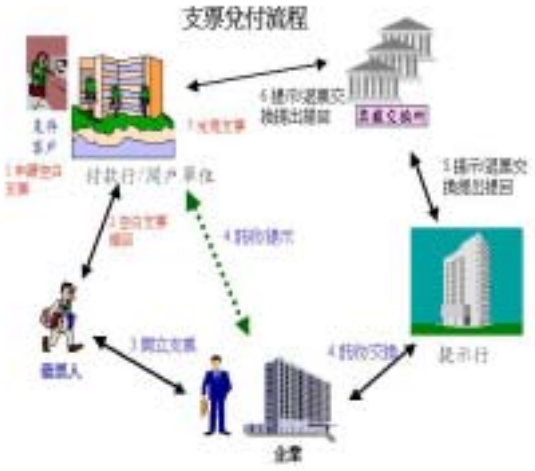

圖3 票據兌付流程

4.1.4 安全機制理論

一、加密及電子簽章之安全機制，擬使用PGP(Pretty Good Privacy)，PGP從1991年由原作者Philip Zimmermann 發表後，立刻非常引人注目，在近代密碼學相關產品中，PGP可說是最被廣泛採用的套裝軟體。因為一方面他採用被全世界密碼學專家公認安全而且可信賴的幾種基本密碼演算法，例如IDEA對稱式文件加密演算法、RSA 或 Diffie-Hellman 的非對稱式加密演算法處理公開金鑰及私鑰之加解密、以及利用 SHA1 單向雜湊函數應用在文件標註、電子簽章認證上。這些密碼演算法都是早已公開發表的，並且曾經被學者反覆推算驗證過的加解密演算法。

二、交易安全防護措施符合銀行公會訂定之「金融機構辦理電子銀行業務安全控管作業基準」規範：[1]

1. 訊息隱密性(Confidentiality)：係指訊息不會遭截取、窺竊而洩漏資料內容致損害其秘密性。
2. 訊息完整性(Integrity)：係指訊息內容不會遭篡改而造成資料不正確性，即訊息如遭篡改時，該筆訊息無效。

3. 訊息來源辨識(Authentication)：係指傳送方無法冒名傳送資料。
4. 訊息不可重複性(Non-duplication)：係指訊息內容不得重複。
5. 無法否認傳送訊息(Non-repudiation of sender)：係指傳送方無法否認其傳送訊息行為。
6. 無法否認接收訊息(Non-repudiation of receiver)：係指接收方無法否認其接收訊息行為。

三、TAG讀取器及無線射頻識別標籤使用一套簡單而適當的「交互鑑別（ mutual authentication)」通訊規約[8]，讓無線射頻辨識標籤辨識對方如果是台合法授權的TAG讀取器的話，就允許它讀取標籤內的資料，否則就拒絕回應。

4.2建構說明

針對票據內容、TAG讀取器(讀碼機)及無線射頻識別標籤等技術規劃RFID票據防偽構想描述如下：

1. 票據原磁性墨水字元識別(Magnetic Ink Character Recognition, MICR)作業相關鍵印流程不變。
2. 無線射頻識別標籤需薄如紙張，以便於嵌入票據內；或是可以印刷方式植入票據中。
3. 設計並建置金鑰(公私鑰)管理之驗證應用系統及無線射頻識別讀取器，供金融機構及發票人(客戶)使用；採「封閉型」管理架構，信任方式採直接信任、完全信任模式。
4. 產生一把付款行(原存行)專門在票據簽章用的私鑰(Private Key)。
5. 每一客戶產生一把專門在票據簽章用的私鑰(Private Key)。
6. 對每一張客戶領用之空白票據，根據它的「票據號碼、付款行、票據種類、帳號等資料」，使用雜湊函數處理後用付款行私鑰產生一個「數位簽章1」 (圖4)[7]。
7. 把每一張空白票據內「票據號碼、付款行、票據種類、帳號等資料」及「數位簽章1」，以階段金鑰1加密產生「密文1」；將階段金鑰1以客戶公鑰加密為「en(階段金鑰1)」(圖5)[7]；最後將「密文1、en(階段金鑰1)」、「客戶金鑰ID明文」、「付款行金鑰ID明文」、「數位簽章1」寫入無線射頻識別標籤的記憶體內。
8. 客戶開立票據時，將無線射頻識別標籤的記憶體內資料讀出，先依據「客戶金鑰ID」取出客戶私鑰將en(階段金鑰1)解密後，再以階段金鑰1將密文1解密(圖6)[7]；再依據付款行金鑰ID取出付款行公鑰，驗證空白票據原內容無誤。再將「票據號碼、付款行、票據種類、帳號、發票日、開立票面金額等資料」，使用雜湊函數處理後用客戶私鑰產生一個「數位簽章2」。
9. 將每一張開立票據內「票據號碼、付款行、票據種類、帳號、發票日、開立票面金額等資料」及「數位簽章2」，以階段金鑰2加密產生「密文2」；將階段金鑰2以付款行公鑰加密為「en(階段金鑰2)」；最後將「密文2、en(階段金鑰2)」、「客戶金鑰ID明文」、「付款行金鑰ID明文」、「數位簽章1」寫入無線射頻識別標籤的記憶體內。
10. 執票人向付款行提示時，付款行將無線射頻識別標籤的記憶體內資料讀出，先依據付款行金鑰ID取出付款行私鑰將en(階段金鑰2)解密後，再以階段金鑰2將密文2解密；再依據客戶金鑰ID取出客戶公鑰，驗證提示票據內容無誤。
11. 付款行以讀出TAG之票據票據號碼、付款行、票據種類、帳號、發票日、開立票面金額等資料內容，進行票據存款應用系統資料核對、更新相關處理(連動印鑑核對及兌現)。

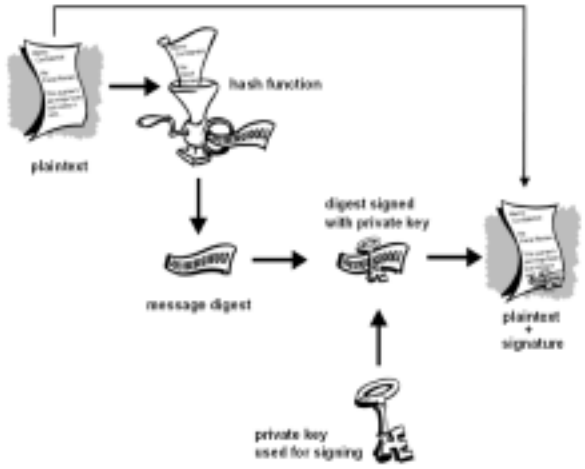

圖4 PGP 數位簽章程序

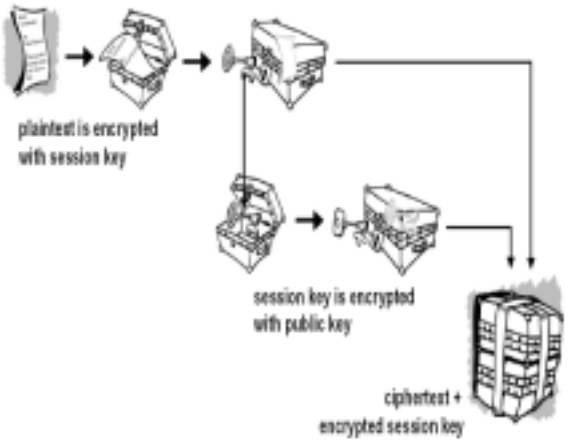

圖5 PGP 加密程序

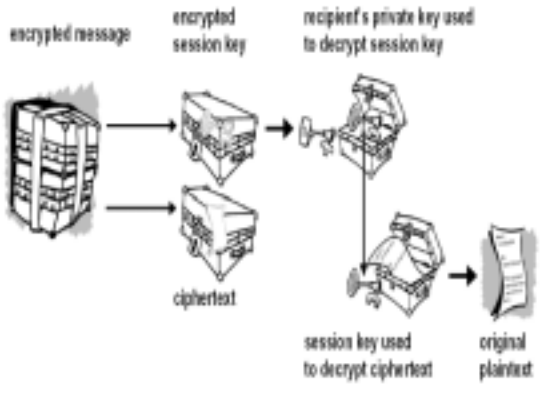

圖6 PGP 解密程序

5.結論與建議

發展電子化作業服務必須落實顧客導向，因為再好的產品也要客戶願意使用，才能發揮它的功效。所以規劃系統時，務必以客戶的需求為最終目標，且因為核心資源是組織取得利潤與優勢的來源，隨著資訊科技的更新資訊技術開發的能力，累積銀行內的技術創新與智慧分享傳遞的價值，配合行銷策略之擬訂，以更具效率的運作程序及更高的顧客滿意程度，進而創建企業形象，來達成其所欲追求的競爭優勢。

應用於票據之資訊科技必須符合實務上之使用狀況，要讓使用者易於操作且使用便利，才可能推廣使用。本研究得知，引進RFID的運用，在不考量所增加之額外成本多寡之下，結合票據上磁性墨水字元(MICR)的鍵印，對加強票據的防偽功能、防污辨識力，減少櫃員操作時的錯誤及負擔，確實有其可行性。

而未來針對成本效益之量化評估及與後端應用系統之整合應用都是值得繼續探討研究之課題。

參考文獻

[1] 銀行公會全國聯合會撰，金融機構辦理電子銀行業務安全控管作業基準，中華民國銀行商業同業公會全國聯合會公文，民國九十四年。

[2] 鄭博仁、陳林福、陳品儀、謝德鑫撰，有價票證防偽架構，無線射頻辨識技術與資訊安全應用，資訊安全技術通訊，第10卷，第2期，頁78-86，民國九十三年。

[3] 奚正德、張克章撰，RFID相關應用與安全機制簡介，資通安全專論 T95013，民國九十五年。

[4] 鄭博仁撰，RFID無線射頻識別在金融防偽之應用，財金資訊雙月刊，第044期，民國九十五年。

[5] 蕭榮興、許育嘉撰，無線射頻技術的應用與發展趨勢，電子商務導航，第六卷，第十三期，民國九十三年。

[6] 參閱Copyright c 1990-1999 Network Associates, Inc. and its Affiliated Companies. All Rights Reserved. ftp://ftp.pgpi.org/pub/pgp/6.5/docs/english/IntroToCrypto.pdf
[7] Juels, A. and R. Pappu, Squealing Euros: Privacy Protection in RFID-Enabled Banknotes, R. Wright, Ed., Financial Cryptography 2003, LNCS No. 2742, Springer-Verlag, pp.103-121, 2003.
[8] Gildas Avoine, Privacy issues in RFID banknote protection schemes, The Sixth International Conference on Smart Card Research and Advanced Applications -- CARDIS, pp.33-48, Toulouse, France, August 2004.
[9] Jeongkyu Yang, Jaemin Park, Hyunrok Lee, Kui Ren, and Kwangjo Kim, Mutual Authentication Protocol for Low-Cost RFID, Proc. of Workshop on RFID and Lightweight Crypto, pp.17-24, Jul. 14~15, 2005, Graz, Austria.
[10]Yang Xiao, Xuemin Shen, BO Sun, Lin Cai, Security and privacy in RFID and applications in telemedicine, IEEE Communications Magazine, Vol. 44, pp.64-72,Issue 4/April 2006.
[11]Chung-Fu Lu, Privacy-Protection in RFID-Enabled Banknotes, Taiwan Information Security Center, National Taiwan University of Science and Technology, Customary seminar Apr. 26, 2006.
[12]Melanie R. Rieback, Bruno Crispo, and Andrew S. Tanenbaum. The Evolution of RFID Security. IEEE Pervasive Computing, Vol. 5, No.1, pp. 62-69, January-March 2006.