結合 AES 網路安全機制的非接觸式 IC 卡網路門禁管理系統的設計與具體實現

楊中皇、曾郁凱、梁秀麗、章恩齊、謝良奇
國立高雄第一科技大學 資訊管理系
chyang@computer.org
http://www.nkfust.edu.tw/~chyang/

摘要

隨著網路技術的快速發展及應用，IC 卡的應用日趨廣泛，而校園 IC 卡也已在國內數所大專院校使用。現行校園 IC 卡多半使用接觸式 IC 卡，由於讀卡機也相對採接觸式而門禁使用頻繁，使得故障率也相對偏高，造成困擾。有鑑於此，我們研發 IC 卡的門禁資訊管理系統，改善現有一般的門鎖或接觸式 IC 卡而改用非接觸式 IC 卡做為進出空間的安全機制，使得同一張 IC 卡可控管不同的出入門禁同時減少讀卡機的故障率。本研究的重點在於所提供的安全機制與網際網路，經由讀取並記錄門禁及 IC 卡使用資訊，使進出空間的人員及時間能做透過網際網路進行即時的控管，達到門禁使用的安全性與管理的便利性。我們也在內含 6808 八位元中央處理器的摩托羅拉公司 MC68HC908AB32 微控制器上進行對稱式密碼學演算法 AES 演算法的具體實現，並開發低成本的資訊安全硬體雛型設備，提供發卡系統與門禁控制系統之間安全網路通信。

關鍵字：網路安全、IC 卡、門禁系統、對稱式密碼學演算法、AES

壹、前言

隨著網際網路與全球資訊網的快速成長，網路安全問題也逐漸浮現出來，而現有粗糙的網路防護措施，並不足以防止各式各樣的入侵、竄改和擅用。若以軟體裝置作為門禁系統之控管工具，則僅能以通行碼(password)方式作為身份的辨認，但是如此一來，通行碼有可能會被使用者忘記，或被有心人士給偷窺或盜取等等。

而改以資訊安全硬體裝置做資訊安全的控管不但安全性較高且使用方便，再加上使用密碼學技術將可對網路提供較佳的安全防禦。

IC 卡[1-4]是植入晶片的塑膠卡，大小是如同平常的信用卡，非常容易攜帶。IC 卡與傳統磁條卡或信用卡比較起來具有難以偽造與記憶空間較高的優點，然而價位也較磁條卡高。隨著網路技術的快速發展及應用，IC 卡的應用日趨廣泛。例如：目前應用最多且被金融界視為塑膠貨幣的金融 IC 卡、由中國信託商業銀行與文化大學合作結合金融卡與學生證功能之學生證智慧卡、中華電信推出之通話 IC 卡、十大書坊推出的租書 IC 卡、中央健保局的健保 IC 卡、中國信託商業銀行與中國石油公司和台北捷運局等將合作推出之卡票合一儲值金融卡、運用在停車場管理及收費的 IC 卡、以及政府大力推行之國民卡・・・等等。由以上實例可知 IC 卡的應用日趨重要亦是未來發展的趨勢。IC 卡所提供的多用途及資訊安全功能，使得 IC 卡不僅可安全無慮地用做身份識別用，也可同時提供電子郵件、電子商務、門禁管制、圖書借還書、成績輸入與查詢等多項功能。

一般而言，在需要對該空間的進出人員做有效的監管及稽查時，通常我們會利用具有一定資訊安全程度的門禁系統，來過濾場所進出人員的身份及時間，並留存其進出記錄，以便日後可以做為查詢之用。

在門禁系統的需求之下，許多需過濾人員進出的公共場合大部份使用以個人密碼(Personal Identification Number, PIN)或接觸式 IC 卡為控管基礎的門禁系統，但此兩者都各有其缺點；個人密碼可能由於使用者自身遺忘其所有的密碼而造成困擾，也容易在使用者輸入時遭旁人窺視而外洩。至於接觸式 IC 卡門禁系統雖然在安全性方面有優良的表現，但系統上的接觸式讀卡設備因有外部電子接觸點的緣故，日久容易故障，且很輕易的就會遭到有心人士的破壞。

綜合以上的觀點來看，我們需要一個兼具內部安全及外部安全的非接觸式 IC 卡門禁系統來補足上述所提的兩類系統的缺點。

發展 IC 卡這其實是未來社會的一種趨勢，尤其在政府鼓吹“健保 IC 卡”、“捷運 IC 卡”的風氣之下，這種想法漸漸行成。相較之下，現有一般常用之磁條卡(如信用卡、提款卡)有兩種缺點：

1、安全性

磁卡上沒有保密的技術，故任何人只要拿到磁卡和讀磁卡的機器，此磁卡上的資料便被人一覽無疑了。我們常可看到信用卡側錄偽卡的媒體報導，而如果這是張國民卡的話，那全國人民所需要負擔的風險是非常大的。

2、容量

IC 卡記憶容量大，資料可重複多次寫入或更新，具有發展為多目的、多功能卡的潛力。相對於 IC 卡，目前市場上較普遍之而磁條卡的記憶容量僅約為 110 個位元組，無法包含應有的資訊，並沒有辦法達到廣大的用途，所以較難使用。

上述的磁條卡兩項缺點改為 IC 卡時都已經改善了，無論是安全性與容量都可以達到使用者所需。而且非接觸式 IC 卡在使用上更是方便；我們可以將卡片放置於皮包之內，要進入門禁之時，只需將皮包在非接觸式讀卡機前面帶，則非接觸式讀卡機便可以接收到訊息，不必拿出拿入如此一來可以降低了失卡的風險。

非接觸式 IC 卡之門禁系統如果設計得宜，可以取代了我們生活中一人一串鑰匙的不便利。一但遭遇遺失卡片的情況，也可以立刻更新與遺失卡相關非接觸式讀卡機的資料，使該遺失卡片立刻於門禁系統失效，也不用重新換把門鎖，因為這一切都是由門禁系統所控制，萬無一失。未來只要讀卡機的價格持續下降，相信此種門禁系統將更為普及。

本研究採用 Client-Server 主從系統架構並以 Borland 公司 C++ Builder 4.0 [5]作為主要軟體開發工具。前端經由讀卡機將 IC 卡的資訊傳至後端處理，後端則結合微軟公司(Microsoft) SQL Server 7.0 建構資料庫。IC 卡的製作（發卡）則使用讀寫機將資料寫入並使用 SQL Server 建置發卡管理的資料庫。本研究的重點在於所提供的安全機制與網際網路監控，經由讀取並記錄門禁及 IC 卡使用資訊，使進出空間的人員及時間能做透過網際網路即時的控管，以此達到門禁使用的安全性與管理的便利性。

2000 年 10 月美國政府機構 NIST 正式宣布[6]選用 Rijndael 對稱式(symmetric)密碼學演算法作為 AES (Advanced Encryption Standard)[7]，且已於今年二月公布 AES 草案[8]，逐步取代行之已久之 DES。本研究同時將 AES 具體實現於摩托羅拉公司內含八位元 6808 中央處理位元之 MC68HC908AB32 [9]單晶片微處理器(microcontroller)進行具體實現。此單晶片內含 E^2PROM 可動態儲存金鑰而不需開模，我們正以 MC68HC908AB32 開發低製造成本的資訊安全硬體雛型設備。此雛型設備不但可提供發卡系統與門禁控制系統之間安全通信亦可用於以對稱式演算法為基礎的其他安全網路通信應用。

貳、MIFARE 非接觸式 IC 卡與讀卡機

IC 卡與磁條卡或信用卡比較起來具有難以偽造與記憶空間較高的優點，然而價位也較磁條卡高。IC 卡一般可分為接觸式與非接觸式兩種，前者歷史悠久且功能強大，後者則目前功能較簡單且多為單一用途(例如高速公路電子收費系統用非接觸式記憶型 IC 卡)。本系統所使用的非接觸式 IC 卡為 Philips 公司的 MIFARE 非接觸式 IC 卡[11]，與交通部高速公路電子收費試用計劃所用相同。

MIFARE 非接觸式 IC 卡如圖 1 所示，使用感應線圈傳遞資料。晶片內共有 1K 位元組的記憶體 EEPROM，記憶體分成 16 個相互獨立的區段(sector)，每一個區段由 4 個區塊(block)組成，每一個區塊的大小是 16 位元組，為此非接觸式 IC 卡讀寫的基本單位。

圖 1：Philips 公司 Mifare 非接觸式 IC 卡

MIFARE IC 卡不需外加電池，在 13.56 MHz 頻率下以無線半雙工加密傳送資料，而與讀卡機之間操作距離可達 6 公分。

系統使用 IC 卡片來儲存使用者的個人資料，每項資料都有固定存放的區段及區塊，如表一所示。

表一：門禁 IC 卡系統卡片內部資料

資料項目名稱	儲存區段	儲存區塊
卡號	0	1
密碼(PIN)	0	2
姓名	1	0
身份證號	1	1
學號	1	2
系所	2	0
級別	2	1
性別	2	2
住址	3	0
Email	3	1
電話	3	2

使用者使用非接觸式 IC 卡進出門禁系統時，門禁系統為驗證 IC 卡有效性與正確性，必須與非接觸式讀卡機連接。當讀卡機讀到 IC 卡片上之資料時，再做進一步的確認是否為有效的使用者，判斷是否開門。

我們採用韓國 KDE 公司的非接觸式 IC 卡讀卡機(KCV-7100) [10] 來作為門禁系統的讀卡機元件。圖 2 顯示此讀卡機的外觀。

圖 2：KDE 非接觸式 IC 卡讀卡機

KCV-7100 讀卡機內含電池，斷電時不會遺失門禁資料，可儲存二千筆以上出入資料。此一讀寫機與門禁控制電腦之間是透過 RS-232C 串列通訊界面來完成。此一非接觸式 IC 卡讀卡機已有完整的應用程式界面，可作為應用系統發展時的踏腳石，使得在讀卡機的程式處理上簡易許多。使用該非接觸式 IC 卡讀卡機之應用程式界面發展應用系統時，有一定通訊協定。

參、IC 卡門禁管理系統

我們 IC 卡門禁管理系統是採用 Client-Server 主從式系統架構(如圖 3)。

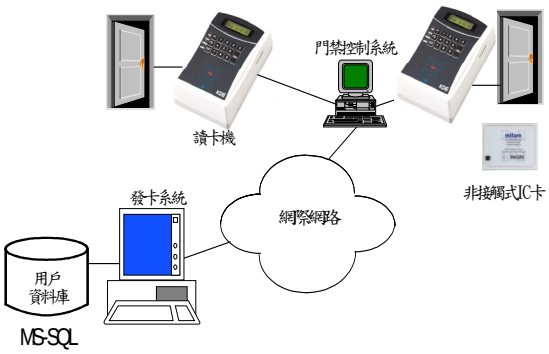

圖 3：IC 卡門禁系統作業架構

使用時前端門禁控制系統可經由讀卡機將 IC 卡的資訊傳至後端處理，後端則結合微軟公司 SQL 7.0 建構資料庫。IC 卡的製作（發卡）則透過非接觸式 IC 卡讀寫機將使用權限資料寫入並使用 SQL 伺服器建置發卡管理的資料庫，同時透過網際網路將使用者門禁權限資料傳至前端門禁控制系統；門禁系統自動決定哪些讀卡機資料須更新。當進出門之人員名單有所異動之時，前端電腦通知後伺服器將資料庫資料更新。同時於固定的時間，前端電腦會從讀卡機中讀出人員進出資料，並透過網際網路將資料寫入後端資料庫。

主從式架構的作業模式乃是多元化、異質性的軟硬體系統，可以依使用需求加以作適當的調整與變化，它容易隨著組織的或大而擴增新系統；使用者透過方便簡單的介面即可得到所要的資訊，進而提昇工作效率，再經由網路的使用而達到資源共享的目的。

IC 卡門禁管理系統的主要功能如圖 4 所示，基本上可分為發卡系統、門禁控制系統、與間觸發程式三部分。發卡系統主要功能為將使用者資料寫入卡片內，並管理後端資料庫；門禁控制系統則控管門禁讀卡機；間觸發程式處理系統定時的協調工作。功能簡述如下：

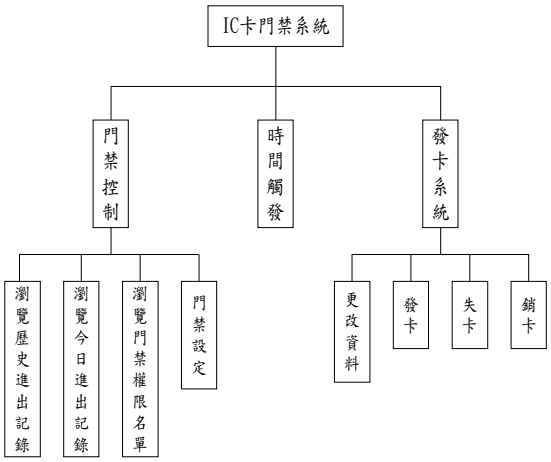

圖 4：系統功能架構

1、發卡系統

非接觸式 IC 卡門禁，將管理門禁安全的基礎建立非接觸式 IC 卡上。只要是門禁系統的使用者，在成為系統的合法使用者時，都會經由這個發卡系統製發而得到一張非接觸式 IC 卡片。發卡系統最主要的功能是製發門禁卡片，同時將使用者最初進出任何一道門禁的權限寫入卡片內並放入門進資料庫。除了發卡外，具有與卡片相關的所有功能，例如修改卡片所記錄的資料，使用者不再使用系統時，所必要執行的銷卡片功能。當然，也有失卡的選擇項目來處理使用者不小心遺失卡片的情況，另外，它還有一些附加的功能，如設定使用者群組、要求門禁控制系統更新可進出入的使用者名單及抓取進出入資料等等。

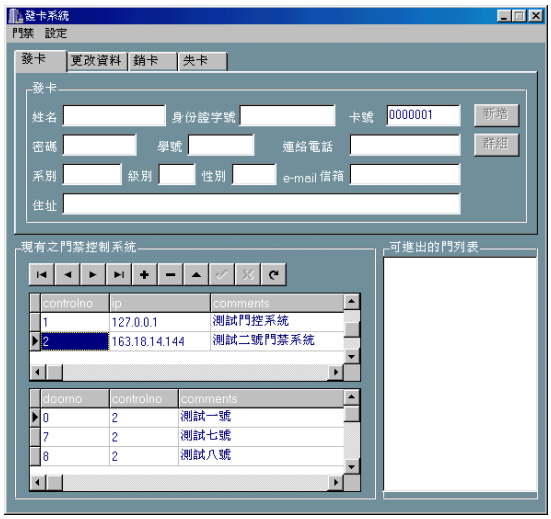

圖 5：發卡系統主畫面

發卡系統主畫面如圖 5，功能有：發卡、修改卡片資料、銷卡、失卡處理、系統現有門禁控制系統列表及可進出門禁列表。

- 發卡

  輸入使用者資料，設定群組，確認後寫入卡片完成發卡動作。卡號是由系統自動配置給使用者，不需使用者自行鍵入，其餘的資料項，姓名、身份證號、密碼，這三項資料屬於必須存在的項目，系統管理員必須輸入，才能夠完成發卡。

- 修改卡片資料

  先讀取使用者卡片資料並顯示，系統管理員修改並確認後，寫入卡片更新使用者資料及權限設定。

- 銷卡

  讀取卡片，顯示使用者資料經系統管理員確認無誤後，消除卡片上資料及系統內權限設定。

- 失卡

  輸入使用者身份證號，從資料庫中搜尋使用者身份，確認無誤後，消除使用者資料及該使用者之權限資料。

- 系統資料

  顯示系統的基本資料，包括說明、位址、時間觸發程式位址及寫卡機連接阜。

- 現有門禁控制系統

  列出系統中現有門禁控制系統資料，並可新增、修改及刪除資料。在選定門控系統後，將顯示出與該門控系統連接的門禁單位資料，此時可將該門禁列入進出權限列表中。

- 可進出之門禁列表

  該使用者具有的權限列表，表示使用者可以進出列表中的門禁單位。

- 設定群組

  為方便管理我們也提供使用者群組的工具，系統管理員可以經由設定群組，快速的選取門禁權限。相對的，門控系統也可以利用群組，簡便的選取多位使用者，而不需麻煩又費時的一位一位選擇。

2、門禁控制系統

門禁控制系統直接與數部讀卡機連接，具備控制讀卡機的能力，是負責門禁權限控管的第一線任務。門禁控制系統主畫面

如圖 6，功能包括讀卡機處理、權限名單設定、記錄進出入資料等。

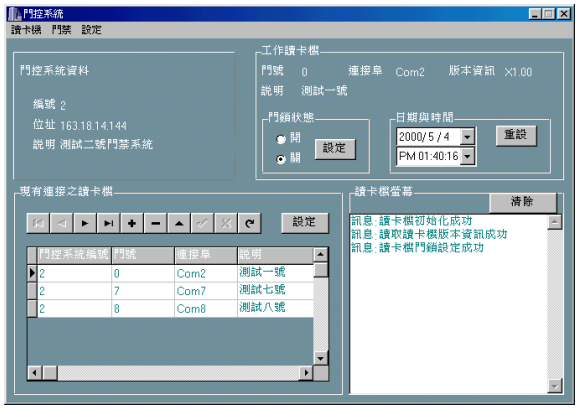

圖 6：門控系統主畫面

在程式顯示區域內，可分為幾個部份：門控系統資料、目前連接之讀卡機、工作讀卡機、讀卡機螢幕。各部份皆有特有功能與顯示資訊，說明如下：

- 門控系統資料

  用來顯示此門禁控制系統的基本資料，程式運作之初，向資料庫讀取。

- 目前連接之讀卡機

  可新增、修改、刪除本門控系統連接的讀卡機資料。選定工作讀卡機後，旁邊的設定按鈕，可以設定該讀卡機的門禁權限名單。

  門禁控制系統實體連接著讀卡機，一個運作中的門禁控制系統可能連接著多台讀卡機，在執行任何讀卡機控制命令前，必須先要選取命令的作用讀卡機，稱為工作讀卡機。

- 工作讀卡機

  顯示工作讀卡機的基本資料，如讀卡機門號、使用的連接阜、讀卡機的版本資訊、讀卡機的描述說明。還可以在此設定讀卡機的門鎖狀態及設定讀卡機內部時間。

  每一部讀卡機都有自己的門禁權限名單，記錄儲存在讀卡機內部的非揮發性記憶體中，而我們可以設定這些名單，達到門禁控管的目的。在選定工作讀卡機後，就可以利用系統提供的各項功能，對讀卡機進行操作，包括了門禁權限設定。

- 讀卡機螢幕

  主要是作為將系統命令發送的情況及讀卡機執行該命令的結果顯示區，系統與發卡系統及時間觸發程序間的訊息傳輸狀態也會出現在這裡。

3、時間觸發程式

間觸發程式本身不負責讀卡機或發卡的相關事項，而主要處理系統定時的協調工作。整個門禁系統開始運作後，因為不希望維護人員每天定時執行某些必要動作，所以我們設計此程式來定時自動處理某些事項：定時通知門控系統更新門禁權限名單、抓取進出入記錄、寄送郵件給使用者告知當天進出狀態這些功能。

肆、AES-128於MC68HC908AB32具體實現

摩托羅拉公司 MC68HC908AB32[9] 微控制器提供八位元的 6808 微處理機，32K 位元組(byte)快閃記憶體(Flash ROM)，512 位元組可讀寫唯讀記憶體(E^2PROM)，以及 1K 位元組隨機存取記憶體(RAM)。快閃記憶體區域可用來儲存作業系統程式和儲存 AES 密碼運算法或其他固定的應用程式，且可隨時線上更改；可程式唯讀記憶體區域是用來儲存個人化的資料(如私密金匙、PIN 等)；隨機存取記憶體區域則是供暫時性運算變數資料儲存用。MC68HC908AB32 中央處理器僅是八位元，RAM 僅有 1K 位元組，程式大小亦有限制；這使得晶片程式的開發必須以組合語言為主，以便有效地利用有限的資源。所以我們以組合語言撰寫 AES 程式，而我們只探討 128 位元(16 位元組)長度之 AES-128 具體實現，因為這最有可能取代 Triple-DES，且安全性足夠用於我們的門禁網路系統。

首先我們從分析 AES-128 之金鑰安排(key schedule)與加解密過程著手。金鑰安排會將輸入之 16 位元組加解密金鑰予以擴張處理成 176 位元組之回合金鑰(round key)。

AES 每回合的轉換沒有 Feistel 結構。反而，回合是數個可逆的轉換所組成，稱作層(layers)。我們實現的 AES-129 的加密過程約如圖 7 所示。金鑰先經計算找出 11 組 128 位元的回合鑰(round key)。明文則經 AddRoundKey（須用到回合金鑰）、ByteSubstitution、RotateRow、及

MixColumn 等層的轉換。

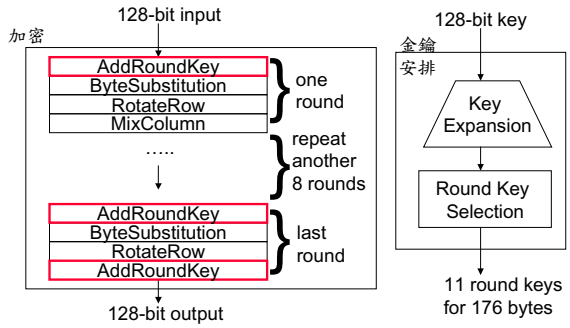

圖 7：AES-128 加密

初步 AES-128 實現結果如表二所示，其中我們假設 MC68HC908AB32 晶片內部時鐘(clock)為允許之 8 MHz。我們的 AES-128 程式與表格所佔用的記憶體差不多共為 2.5K 位元組，而加密速度可達 141 Kbits/s。

表二：AES-128 於 MC68HC908AB32 執行效率

金鑰安排(key schedule)時間	加密時間（每個區塊）	加密處理速度
0.22 ms 1759 cycles	0.9 ms 7258 cycles	141 Kbits/s

由於門禁控管資料將透過網際網路於發卡系統及門禁控管系統之間傳送，有可能受到惡意攻擊。所以我們以 MC68HC908AB32 開發低製造成本的資訊安全硬體雛型設備（初期僅採 RS-232 介面）。此雛型設備不但可配備於發卡系統及門禁控制系統，提供雙方之間安全通信（如圖 8），亦可用於以對稱式演算法為基礎的其他安全網路通信應用。

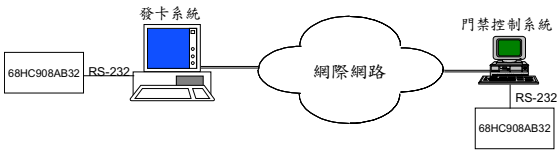

圖 8：AES 提供發卡系統與門禁控管系統之間的保密與認證安全

伍、結論

非接觸式 IC 卡片門禁管理系統能提供使用者進出入管制、權限及時間之控制等功能，並能定時更新門禁資料與寄發電子郵件給予當日有進出門控系統之人員的功能。以非接觸式讀卡機可減少故障率，對需要控管之門禁場所可依各使用者所擁有之 IC 卡片上記錄之門禁權限資料，即時決定是否使該人員通行。

本研究同時於摩托羅拉公司 MC68HC908AB32 微控制器上具體實現 AES-128，並開發低成本的資訊安全硬體雛型設備，提供發卡系統與門禁控制系統之間安全通信，以避免門禁資料於網際網路傳送時受到惡意攻擊。

致謝

本研究承蒙保而杰有限公司及國科會計畫(NSC 90-2213-E-327-008)的經費補助，特此致謝。

參考文獻

1. 楊中皇，校園IC卡的資訊安全系統設計，第十屆國際資訊管理學術研討會論文集，1999年6月，pp. 614-618。
2. W. Rankl and W. Effing, R. Wolfgang， Smart Card Handbook，2nd edition, John Wiley & Sons, 2000.
3. M. Hendry， Smart Card Security and Applications，Artech House, Inc., 1997.
4. ISO 7816 Part 1 to 6: Identification Cards - Integrated Circuit(s) Cards with Contacts, 1987 to 1996.
5. Borland C++Builder, http://www.borland.com/bcppbuilder/productinfo/.
6. NIST, "Commerce Department Announces Winner of Global Information Security Competition," October 2, 2000, http://www.nist.gov/public_affairs/releases/g00-176.htm 或 http://www.nist.gov/ aes/.
7. J. Demen and V. Rijmen, "The Rijndael Block Cipher," Document version 2, March 1999, http://www.esat.kuleuven.ac.be/~rijmen/rijndael.
8. NIST, Draft FIPS for the Advanced

Encryption Standard (AES), http://csrc.nist.gov/publications/drafts/dfips-AES.pdf, February 28, 2001.

9. *MC68HC908AB32 HCMOS Microcontroller Unit*, Rev. 1, Motorola Ltd., August 2000. 參見 http://www.mcu.motsps.com/ 或 http://e-www.motorola.com/brdata/PDFDB/docs/MC68HC908AB32.pdf.
10. Philips Products: Mifare, http://www-eu3.semiconductors.com/identification/products/mifare/
11. KDE Access Control Contactless RF Card Terminal, http://www.kde.co.kr/english1/product/kcv7000.html.