200929986

發明專利說明書

（本說明書格式、順序及粗體字，請勿任意更動，※記號部分請勿填寫）

※ 申請案號：96150715

※ 申請日期：96. 12. 28　　※IPC 分類：H04L 9/14 (2006.01)

G06K 19/07 (2006.01)

一、發明名稱：（中文/英文）

安全認證模組之認證系統及方法

二、申請人：（共 1 人）

姓名或名稱：（中文/英文）

關貿網路股份有限公司

代表人：（中文/英文） 林永堅

住居所或營業所地址：（中文/英文）

台北市南港區三重路19之13號6樓

國　籍：（中文/英文） 中華民國

三、發明人：（共1人）

姓　名：（中文/英文）

李建賢 / LEE, CHIEN HSIEN

國　籍：（中文/英文）中華民國

四、聲明事項：

☐ 主張專利法第二十二條第二項☐第一款或☐第二款規定之事實，其事實發生日期為：　年　月　日。

☐ 申請前已向下列國家（地區）申請專利：

【格式請依：受理國家（地區）、申請日、申請案號　順序註記】

☐ 有主張專利法第二十七條第一項國際優先權：

☐ 無主張專利法第二十七條第一項國際優先權：

☐ 主張專利法第二十九條第一項國內優先權：

【格式請依：申請日、申請案號　順序註記】

☐ 主張專利法第三十條生物材料：

☐ 須寄存生物材料者：

國內生物材料　【格式請依：寄存機構、日期、號碼　順序註記】

國外生物材料　【格式請依：寄存國家、機構、日期、號碼　順序註記】

☐ 不須寄存生物材料者：

所屬技術領域中具有通常知識者易於獲得時，不須寄存。

九、發明說明：

【發明所屬之技術領域】

本發明係有關於一種認證系統及方法，更詳而言之，係有關於一種應用安全認證模組之系統及方法。

【先前技術】

目前智慧 IC 卡已普遍應用於社會的各個領域，且有日益普及的趨勢，一個人身上同時具有多張 IC 卡已不足為奇。在 IC 卡的應用領域中，通常卡片本身係一般大眾較常看見的一部份，然而單靠卡片是無法完成整體系統的運作，後端電腦、應用軟體、讀卡機設備等都是不可缺少的要件，其中該讀卡機設備負責後端的軟硬體與 IC 卡間的資訊傳遞工作。而就功能設計而言，由於其應用環境的差異而有顯著的不同，基本上，有接觸式與非接觸式的區別。

相較於接觸式 IC 卡系統，非接觸式 IC 卡由於卡片與讀卡機的訊息傳遞不必直接接觸，所以在使用上較為便利，且可免除許多接觸式 IC 系統的接點磨損等缺點，因此，在社會上各階層的應用越來越多，其應用範圍包括會員卡、金融卡、信用卡、門禁卡、校園卡、儲值卡、記帳卡、掛號證、保險證、以及捷運及公車所用的悠遊卡等。非接觸式 IC 卡又以 RFID 之技術為主，RFID 是「Radio Frequency Identification」的縮寫，中文可以稱為「無線射頻識別系統」。 通常是由感應器(Reader)和 RFID 標籤(Tag)所組成的系統，其運作的原理是利用感應器發射無

線電波，觸動感應範圍內的RFID標籤，藉由電磁感應產生電流，供應RFID標籤上的晶片運作並發出電磁波回應感應器。

由於上述的非接觸式IC卡大部分只有辨識功能而少有安全認證設計，故僅是用於低安全性且簡單的識別。為解決非接觸式IC卡之低安全性問題，遂有針對其安全性問題而開發的非接觸式智慧IC卡的出現，目前非接觸式智慧IC卡讀卡機及智慧IC卡大都使用飛利浦的Mifare技術，該技術係遵照ISO 14443非接觸式智慧卡與讀卡機國際標準。其中所用的Mifare卡內晶片可讀／寫資料，更在每個磁區獨立加密，使其具備更好的安全性。

然而，目前的非接觸式RFID讀卡機仍有其安全上的顧慮，即，SAM卡若被竊取等於得到可以任意存取或修改非接觸IC卡的權限，因此控管機制較差，故有需要提供額外的控管機制以增加RFID讀卡機之安全性，也可同時降低金鑰在讀卡機外部被側錄的情況發生。

綜上所述，如何解決上述非接觸式RFID讀卡機之安全上的顧慮，以防止安全認證模組卡被盜取後被任意使用，遂成為目前亟待解決之問題。

【發明內容】

鑒於以上習知技術之缺點，本發明之主要目的在於提供一種安全認證模組之認證系統及方法，係應用於具有RFID電路之讀卡機與Mifare卡上，透過此認證機制，可防止SAM被拿到該對應讀卡機以外的地方使用。

本發明之另一目的在於提供一種安全認證模組之認證系統及方法，係應用於具有 RFID 電路之讀卡機與 Mifare 卡上，透過此認證機制，可在安全認證模組卡被盜取後防止取得複製金鑰(A/B key)。

本發明之又一目的在於提供一種安全認證模組之認證系統及方法，係應用於具有 RFID 電路之讀卡機與 Mifare 卡上，透過此認證機制，可增加非接觸式讀卡機之安全性。

為達上揭及其它目的，本發明提供一種安全認證模組之認證系統，係應用於具有 RFID 電路之讀卡機與 Mifare 卡，該讀卡機具有可分別插置安全認證模組卡與認證卡之安全認證模組卡插槽及認證卡插槽，該安全認證模組卡與該認證卡分別具有金鑰儲存區，且該安全認證模組卡之金鑰儲存區儲存有複製金鑰，該安全認證模組之認證系統包括：金鑰生成交換模組，係內建於該安全認證模組卡，用以令該安全認證模組卡產生包括公鑰與私鑰之 RSA 金鑰對，並將該金鑰對中的公鑰傳送至該讀卡機，該私鑰則係儲存於該安全認證模組卡中；金鑰傳送模組，係內建於該認證卡，用以令該讀卡機將其所接收的公鑰傳入該認證卡中；認證金鑰生成模組，係內建於該認證卡，用以在該認證卡上產生認證金鑰，並將該認證金鑰儲存於該認證卡之金鑰儲存區中；認證金鑰加密模組，係內建於該認證卡，用以將認證金鑰生成模組所產生之認證金鑰透過該金鑰傳送模組所傳入之公鑰予以加密，並透過該金鑰傳送模組

回傳該加密過之認證金鑰給該讀卡機；以及金鑰註冊功能模組，係內建於該安全認證模組卡，用以將該讀卡機所接收之加密過的認證金鑰傳入該安全認證模組卡內，再使用其私鑰將該加密過的認證金鑰解密，並判斷該認證金鑰解密是否成功，若是，則將該認證金鑰儲存至該安全認證模組卡之金鑰儲存區中；若否，則不予以儲存。

前述安全認證模組之認證系統的另一實施例中，該安全認證模組之認證系統復包括複製金鑰加密模組，係內建於該安全認證模組卡，用以當 Mifare 卡插入該讀卡機時，呼叫安全認證模組卡取得該複製金鑰，接著令該安全認證模組卡使用該認證金鑰將該複製金鑰加密，並傳給認證卡；以及複製金鑰解密模組，係內建於該認證卡，用以解密加密過後的複製金鑰，換言之，將該加密過的複製金鑰傳入該認證卡並令儲存於該認證卡中的認證金鑰將該加密過的複製金鑰解密，並將該解密過之複製金鑰傳送至該 Mifare 卡。

本發明之安全認證模組之認證方法，係應用於具有 RFID 電路之讀卡機與 Mifare 卡，該讀卡機具有可分別插置安全認證模組卡與認證卡之安全認證模組卡插槽及認證卡插槽，該安全認證模組卡與該認證卡分別具有金鑰儲存區，且該安全認證模組卡之金鑰儲存區儲存有複製金鑰，該安全認證模組之方法包括：透過該安全認證模組卡產生包括公鑰與私鑰之 RSA 金鑰對，並將該金鑰對其中的公鑰傳送至該讀卡機；透過該讀卡機將其所接收的公鑰

傳入該認證卡中，並在該認證卡上產生認證金鑰；將該認證金鑰儲存於該認證卡之金鑰儲存區中，同時將該認證金鑰透過該讀卡機所傳入之公鑰予以加密，再傳送該加密過之認證金鑰至該讀卡機；令該讀卡機所接收之加密過的認證金鑰傳入該安全認證模組卡內，並透過該私鑰將該加密過的認證金鑰解密；以及判斷認證金鑰解密是否成功，若是，則將該認證金鑰儲存至該安全認證模組卡之金鑰儲存區中；若否，則不予以儲存。

前述安全認證模組之認證方法的另一實施例復包括：將 Mifare 卡插入讀卡機中；呼叫安全認證模組卡取得該複製金鑰；令該安全認證模組卡使用認證金鑰加密該複製金鑰，並傳給認證卡；令該認證卡使用認證金鑰將該加密過的複製金鑰解密；以及將該解密過之複製金鑰傳送至該 Mifare 卡。

因此，本發明之安全認證模組之認證系統及方法係透過插置有安全認證模組卡及認證卡之 RFID 讀卡機來施行認證機制，首先由該 RFID 讀卡機呼叫安全認證模組卡交換金鑰產生功能，然後將讀卡機電路板上所產生 RSA 金鑰對傳送至安全認證模組卡並回傳其中的公鑰(public key)、將該公鑰傳入讀卡機之認證卡並於該認證卡之電路板上產生認證金鑰(Des3)、使用該公鑰加密此認證金鑰並回傳加密過之該認證金鑰、將該加密過之認證金鑰傳入該安全認證模組卡中並使用該安全認證模組卡中之 RSA 私鑰(private key)解密、若解密成功則將該認證金鑰儲存至

安全認證模組卡中，藉此，以後若需要透過該讀卡機取得該安全認證模組卡之複製金鑰時，就需要透過該讀卡機之該認證金鑰來認證，因此可防止盜取安全認證模組卡及防止側錄之情形發生，因而提高非接觸式 RFID 讀卡機之安全性。

【實施方式】

以下係藉由特定的具體實施例說明本發明之實施方式，熟悉此技藝之人士可由本說明書所揭示之內容輕易地瞭解本發明之其他優點與功效。本發明亦可藉由其他不同的具體實施例加以施行或應用，本說明書中的各項細節亦可基於不同觀點與應用，在不悖離本發明之精神下進行各種修飾與變更。

請參閱第 1(A)圖，用以顯示本發明之安全認證模組之認證系統 1 之一實施例的系統架構方塊示意圖。本發明之安全認證模組之認證系統係例如建構在具有 RFID 電路之 Mifare 讀卡機上，該讀卡機具有可分別插置安全認證模組卡與認證卡之安全認證模組卡插槽及認證卡插槽，該安全認證模組卡與該認證卡分別具有金鑰儲存區，且該安全認證模組卡之金鑰儲存區儲存有複製金鑰，藉由本發明之安全認證模組之認證系統 1 之建置可以增加 RFID 讀卡機之安全性。如圖所示，該安全認證模組之認證系統 1 包括安全認證模組卡 10 內的金鑰生成交換模組 12、與金鑰註冊功能模組 14、以及認證卡 20 內的金鑰傳送模組 22、認證金鑰生成模組 23、和認證金鑰加密模組 24。該

安全認證模組係如同讀卡機之識別機制，亦即讀卡機上傳、更新、開機確認時都需要使用到安全認證模組卡 10。

當欲進行本發明安全認證模組認證之初始設定時，需先同時準備兩張安控卡，一張為安全認證模組卡，另一張則為讀卡機認證卡。讀卡機認證卡是空白卡，發給讀卡機廠商並內建於讀卡機中；而安全認證模組卡提供 Mifare 複製金鑰，其預儲存於安全認證模組卡之儲存區內，用來提供存取 Mifare 卡認證使用，其中該 Mifare 卡可例如為符合 ISO 14443 標準之塑膠卡片，其可以是 PVC、ABS 或更高級的合成塑膠材質，內含有微處理或記憶體與控制邏輯所組成的晶片以及與該讀卡機通訊的介面。

使用者取得安全認證模組卡後安裝於讀卡機 1 的安全認證模組插槽(未顯示於圖中)中，然後啟動初始設定，於是該讀卡機 1 透過內建於該安全認證模組卡 10 之金鑰生成交換模組 12 而令該安全認證模組卡產生包括公鑰與私鑰之 RSA 金鑰對(RSA key pair)，並將該金鑰對其中的公鑰(Kpuk)傳送至該讀卡機 1，其中該 RSA 金鑰對係結合讀卡機上的序號產生，且該 RSA 金鑰對包括一把公鑰(public key)和一把私鑰(private key)，由於該私鑰(Kpvk)係於該安全認證模組卡中，故無法回傳。需補充說明者，較佳者，RSA 金鑰對係以 onboard 方式產生，則私鑰係 onboard 於該安全認證模組卡中。

金鑰傳送模組 22 係內建於該認證卡 20，用以令該讀卡機 1 將其所接收的公鑰(Kpuk)傳入該認證卡 20 中，亦

即，一旦該讀卡機 1 接收到公鑰(Kpuk)便會通知該金鑰傳送模組 22 立即擷取該公鑰(Kpuk)。

認證金鑰生成模組 23，係內建於該認證卡 20，用以在該認證卡 20 上產生認證金鑰(Triple-DES, Kdes3)，並將該認證金鑰(Kdes3)儲存於該認證卡之金鑰儲存區中，其中該認證金鑰係屬於一種三重資料加密標準(Triple Data Encryption Standard)演算法的基底類別，所有 Triple DES 實作(Implementation) 必須從它衍生。需補充說明者，較佳者，認證金鑰係以 onboard 方式產生。

認證金鑰加密模組 24，係內建於該認證卡 20，用以將認證金鑰生成模組 23 所產生之認證金鑰(Kdes3)透過該金鑰傳送模組 22 所傳入之公鑰(Kpuk)予以加密並透過該金鑰傳送模組 22 回傳該加密過之認證金鑰(E(Kpuk, Kdes3))給該讀卡機 1。

金鑰註冊功能模組 14，係內建於該安全認證模組卡 10，用以將該讀卡機 1 所接收之加密過的認證金鑰(E(Kpuk, Kdes3))傳入該安全認證模組卡 10 內，並使用其私鑰(Kpvk)將該加密過的認證金鑰解密(E(Kpuk, Kdes3))，若解密成功，則將該認證金鑰(Kdes3)儲存至該安全認證模組卡 10 之金鑰儲存區(圖中未顯示)中，此時即完成 SAM 認證之初始設定，若否，則不予以儲存。

上述內容中，需要附加說明的是該安全認證模組卡 10 中的金鑰對產生及認證金鑰註冊被設計成只能被寫入一次，而且是無法被讀取的(write only & once)，而認證

卡 20 之認證金鑰(Kdes3)產生被設計成只能被寫入無法讀取，但能覆寫多次(write only)。由此可知，安全認證模組設計成 write only & once 表示一經設定就無法更改，認證卡 20 允許覆寫是因為可能需要更換安全認證模組卡 10，一旦更換該安全認證模組卡 10 就須重新設定認證卡 20 中的認證金鑰(Kdes3)，由於兩者都無法被讀取金鑰，因此，可確保認證金鑰(Kdes3)不會被側錄外洩。

請參閱第 1(B)圖，其用以顯示本發明之安全認證模組之認證系統 1'之另一實施例的系統架構方塊示意圖。本實施例之安全認證模組之認證系統 1'，其中除複製金鑰加密模組 16 與複製金鑰解密模組 21 外，各系統構件間的運作關係與第 1(A)圖相同，故在此將不另贅述，惟本圖加入一 Mifare 卡 30 作為該安全認證模組認證初始設定完成後之示範操作實施例。透過本實施例可瞭解 Mifare 卡 30 如何取得安全認證模組卡 10 之複製金鑰及如何透過讀卡機 1 之認證金鑰(kdes3)來認證。

複製金鑰加密模組 16，係內建於該安全認證模組卡 10，用以當 Mifare 卡 30 插入該讀卡機 1'時，令該安全認證模組卡 10 使用該認證金鑰(kdes3)將該複製金鑰加密，並傳給認證卡 20。

複製金鑰解密模組 21，係內建於認證卡 20，用以解密加密過後的複製金鑰，換言之，將該加密過的複製金鑰傳入認證卡 20 並令儲存於該認證卡中的認證金鑰(kdes3)將該加密過的複製金鑰解密，並將該解密過之複製金鑰傳

送至該 Mifare 卡。

請參閱第 2 圖，係顯示本發明之安全認證模組之認證方法的基本運作流程示意圖，其係應用於具有 RFID 電路之讀卡機與 Mifare 卡，該讀卡機具有可分別插置於其安全認證模組卡插槽及認證卡插槽之安全認證模組卡與認證卡，透過本方法之設定，可初始該安全認證模組認證之設定，該流程包括以下步驟。

於步驟 S22 中，令該安全認證模組卡產生包括公鑰與私鑰之 RSA 金鑰對(RSA key pair)，並將該金鑰對其中的公鑰(Kpuk)傳送至該讀卡機，需補充說明者，較佳者，RSA 金鑰對係以 onboard 方式產生。接著進行步驟 S23。RSA 係由羅納德·李維斯特(Ron Rivest)、阿迪·薩莫爾(Adi Shamir)和倫納德·阿德曼(Leonard Adleman)於 1977 年共同提出的非對稱加密演算法。

於步驟 S23 中，令該讀卡機將其所接收的公鑰(Kpuk)傳入該認證卡中，並在該認證卡上產生認證金鑰(Kdes3)，需補充說明者，較佳者，認證金鑰係以 onboard 方式產生。接著進行步驟 S24。

於步驟 S24 中，將該認證金鑰(Kdes3)儲存於該認證卡之金鑰儲存區中，同時將該認證金鑰(Kdes3)透過該讀卡機所傳入之公鑰(Kpuk)予以加密，然後傳送該加密過之認證金鑰 E(Kpuk, Kdes3)至該讀卡機，接著進行步驟 S25。

於步驟 S25 中，令該讀卡機所接收之加密過的認證金鑰 E(Kpuk, Kdes3)傳入該安全認證模組卡內，並透過其私

鑰(Kpvk)將該加密過的認證金鑰 E(Kpuk, Kdes3)解密，若解密成功，接著進行步驟 S26，若否，則不儲存。

於步驟 S26 中，令該認證金鑰(Kdes3)儲存至該安全認證模組卡之金鑰儲存區中。

請參閱第 3 圖，係顯示本發明之使用 Mifare 卡取得複製金鑰之加解密方法的一實施例的運作流程示意圖，用以說明依據第 2 圖所完成 SAM 認證初始設定後之運作流程式示意圖。透過該流程可讓使用者瞭解認證卡與該讀卡機(安全認證模組卡)間的運作及如何加解密複製金鑰，該流程包括以下步驟。

於步驟 S30 中，將 Mifare 卡插入讀卡機中，接著進行步驟 S31。

於步驟 S31 中，呼叫安全認證模組卡取得複製金鑰，接著進行步驟 S32。

於步驟 S32 中，令該安全認證模組卡使用認證金鑰加密該複製金鑰，接著進行步驟 S34。

於步驟 S34 中，令該加密過的複製金鑰傳送至認證卡中，接著進行步驟 S36。

於步驟 S36 中，令該認證卡使用認證金鑰解密該加密過之複製金鑰，接著進行步驟 S38。

於步驟 S38 中，將該解密過之複製金鑰傳送至該 Mifare 卡。

綜上所述，本發明之安全認證模組之認證系統及方法係透過插置有安全認證模組卡及認證卡之 RFID 讀卡機來

施行認證機制，透過此認證機制，安全認證模組卡一經設定就無法更改、覆寫，且其所產生之認證金鑰亦無法被讀取，因此可防止安全認證模組卡被盜取及防止側錄之情形發生，因而提高非接觸式 RFID 讀卡機之安全性。

上述實施例僅為例示性說明本發明之原理及其功效，而非用於限制本發明。任何熟習此項技藝之人士均可在不違背本發明之精神及範疇下，對上述實施例進行修飾與變化。因此，本發明之權利保護範圍，應如後述之申請專利範圍所列。

【圖式簡單說明】

第 1(A)圖係用以顯示本發明之安全認證模組之認證系統 1 之一實施例的系統架構方塊示意圖；

第 1(B)圖係用以顯示本發明之安全認證模組之認證系統 1'之另一實施例的系統架構方塊示意圖。；

第 2 圖係顯示本發明之安全認證模組之認證方法的基本運作流程示意圖；以及

第 3 圖係顯示本發明之使用 Mifare 卡取得複製金鑰之加解密方法的一實施例的運作流程示意圖。

【主要元件符號說明】

1, 1'　讀卡機

2　讀卡機本身

10　安全認證模組卡

12　金鑰生成交換模組

14　金鑰註冊功能模組

16 複製金鑰加密模組

20 認證卡

21 複製金鑰解密模組

22 金鑰傳送模組

23 認證金鑰生成模組

24 認證金鑰加密模組

30 Mifare 卡

S22, S23, S24, S25, S23 步驟

S30, S31, S32, S34, S36, S38 步驟

五、中文發明摘要：

一種安全認證模組之認證系統及方法，主要係令安全認證模組卡產生包括公鑰與私鑰之RSA金鑰對，並將該公鑰傳送至讀卡機，再令讀卡機該公鑰傳入認證卡中，並在認證卡上產生認證金鑰，接著將認證金鑰儲存於認證卡之金鑰儲存區中，同時將認證金鑰透過讀卡機所傳入之公鑰予以加密，然後傳送加密過之認證金鑰至讀卡機，俾令讀卡機所接收之加密過的認證金鑰傳入安全認證模組卡內，並透其私鑰將加密過的認證金鑰解密，於解密成功後，再將認證金鑰儲存至安全認證模組卡之金鑰儲存區中。據此，可防止安全認證模組卡被盜取及防止側錄之情形發生，因而提高非接觸式RFID讀卡機之安全性。

六、英文發明摘要：

十、申請專利範圍：

1. 一種安全認證模組之認證系統，係應用於具有 RFID 電路之讀卡機與 Mifare 卡，該讀卡機具有可分別插置安全認證模組卡與認證卡之安全認證模組卡插槽及認證卡插槽，該安全認證模組卡與該認證卡分別具有金鑰儲存區，且該安全認證模組卡之金鑰儲存區儲存有複製金鑰，該安全認證模組之認證系統包括：

金鑰生成交換模組，係內建於該安全認證模組卡，用以令該安全認證模組卡產生包括公鑰與私鑰之 RSA 金鑰對，並將該金鑰對中的公鑰傳送至該讀卡機，該私鑰則係儲存於該安全認證模組卡中；

金鑰傳送模組，係內建於該認證卡，用以令該讀卡機將其所接收的公鑰傳入該認證卡中；

認證金鑰生成模組，係內建於該認證卡，用以在該認證卡上產生認證金鑰，並將該認證金鑰儲存於該認證卡之金鑰儲存區中；

認證金鑰加密模組，係內建於該認證卡，用以將認證金鑰生成模組所產生之認證金鑰透過該金鑰傳送模組所傳入之公鑰予以加密，並透過該金鑰傳送模組回傳該加密過之認證金鑰給該讀卡機；以及

金鑰註冊功能模組，係內建於該安全認證模組卡，用以將該讀卡機所接收之加密過的認證金鑰傳入該安全認證模組卡內，再使用其私鑰將該加密過的認證金鑰解密，並判斷該認證金鑰解密是否成功，若是，

則將該認證金鑰儲存至該安全認證模組卡之金鑰儲存區中；若否，則不予以儲存。

2. 如申請專利範圍第 1 項之安全認證模組之認證系統，其中，該金鑰註冊功能模組所解密的認證金鑰只能寫入該安全認證模組卡之金鑰儲存區一次，且無法被讀取。

3. 如申請專利範圍第 2 項之安全認證模組之認證系統，其中，該解密的認證金鑰於寫入該安全認證模組卡之金鑰儲存區後即無法變更。

4. 如申請專利範圍第 1 項之安全認證模組之認證系統，其中，該認證金鑰生成模組所產生之認證金鑰只能被寫入而無法讀取，且能覆寫多次至該認證卡之金鑰儲存區。

5. 如申請專利範圍第 1 項之安全認證模組之認證系統，其中，該安全認證模組卡僅對應單獨之認證金鑰。

6. 如申請專利範圍第 1 項之安全認證模組之認證系統，復包括一複製金鑰加密模組，係內建於該安全認證模組卡，用以當 Mifare 卡插入該讀卡機時，呼叫安全認證模組卡取得該複製金鑰，接著令該安全認證模組卡使用該認證金鑰將該複製金鑰加密，並將該加密過的複製金鑰傳送至該認證卡。

7. 如申請專利範圍第 6 項之安全認證模組之認證系統，復包括一複製金鑰解密模組，係內建於該認證卡，用以將該加密過的複製金鑰解密，並將該解密過之複製

金鑰傳送至該 Mifare 卡。

8. 如申請專利範圍第 1 項之安全認證模組之認證系統，其中，該安全認證模組卡係以 onboard 方式產生該 RSA 金鑰對。

9. 如申請專利範圍第 1 項之安全認證模組之認證系統，其中，該認證卡係以 onboard 方式產生認證金鑰。

10. 一種安全認證模組之認證方法，係應用於具有 RFID 電路之讀卡機與 Mifare 卡，該讀卡機具有可分別插置安全認證模組卡與認證卡之安全認證模組卡插槽及認證卡插槽，該安全認證模組卡與該認證卡分別具有金鑰儲存區，且該安全認證模組卡之金鑰儲存區儲存有複製金鑰，該安全認證模組之方法包括：

透過該安全認證模組卡產生包括公鑰與私鑰之 RSA 金鑰對，並將該金鑰對其中的公鑰傳送至該讀卡機；

透過該讀卡機將其所接收的公鑰傳入該認證卡中，並在該認證卡上產生認證金鑰；

將該認證金鑰儲存於該認證卡之金鑰儲存區中，同時將該認證金鑰透過該讀卡機所傳入之公鑰予以加密，再傳送該加密過之認證金鑰至該讀卡機；

令該讀卡機所接收之加密過的認證金鑰傳入該安全認證模組卡內，並透過該私鑰將該加密過的認證金鑰解密；以及

判斷認證金鑰解密是否成功，若是，則將該認證

金鑰儲存至該安全認證模組卡之金鑰儲存區中；若否，則不予以儲存。

11. 如申請專利範圍第 10 項之安全認證模組之認證方法，復包括使用該 Mifare 卡取得安全認證模組卡複製金鑰的方法，包括：

將 Mifare 卡插入讀卡機中；

呼叫安全認證模組卡取得該複製金鑰；

令該安全認證模組卡使用認證金鑰加密該複製金鑰；

令該加密過的複製金鑰傳送至認證卡中；

令該認證卡使用認證金鑰解密該加密過之複製金鑰；以及

將該解密過之複製金鑰傳送至該 Mifare 卡。

12. 如申請專利範圍第 10 項之安全認證模組之認證方法，其中，該解密的認證金鑰只能寫入該安全認證模組卡之金鑰儲存區一次，且無法被讀取。

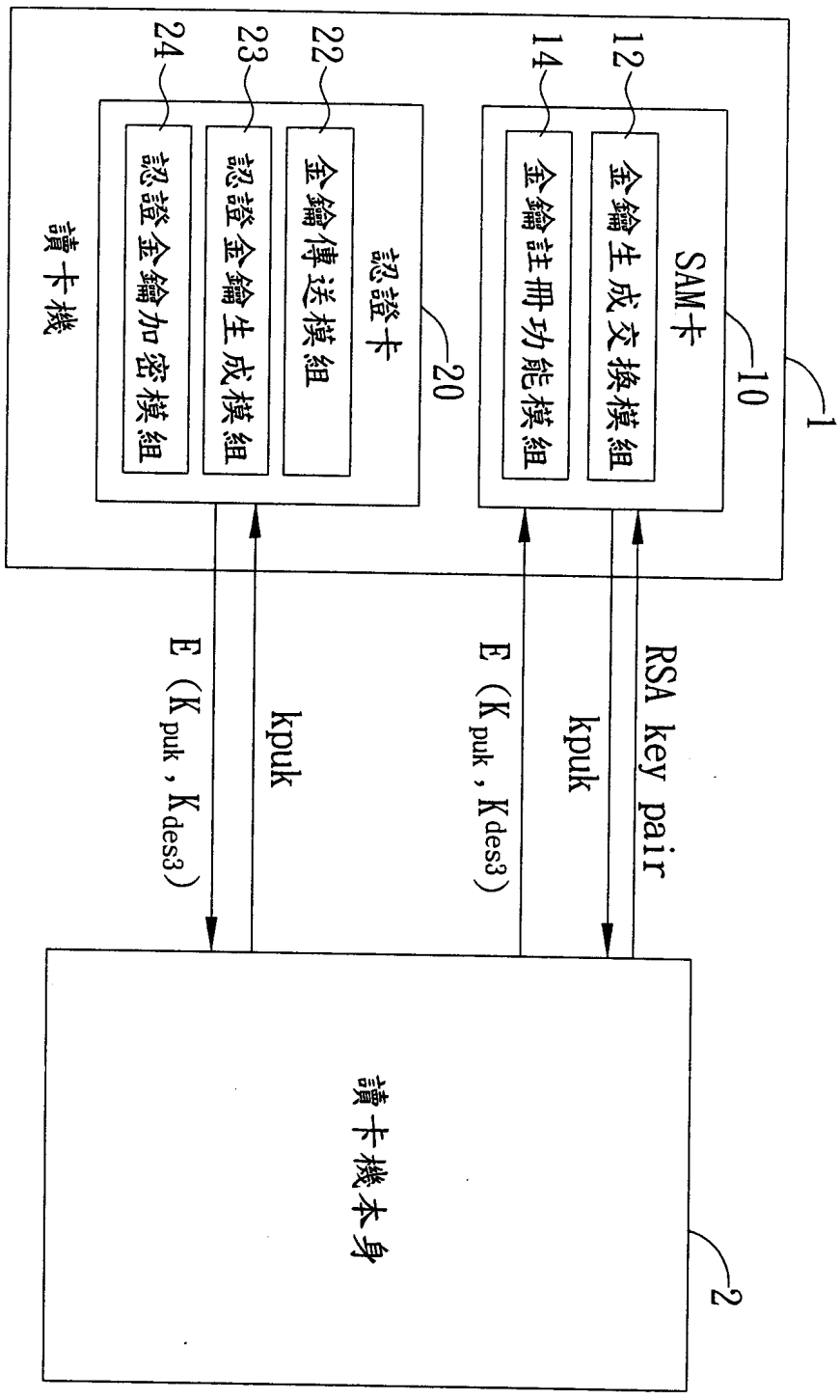
13. 如申請專利範圍第 11 項之認證方法，其中，該解密的認證金鑰寫入該安全認證模組卡之金鑰儲存區後即無法變更。

14. 如申請專利範圍第 10 項之安全認證模組之認證方法，其中，該認證金鑰只能被寫入而無法讀取，且能覆寫多次至該認證卡之金鑰儲存區。

15. 如申請專利範圍第 10 項之安全認證模組之認證方法，其中，該安全認證模組卡僅對應單獨之認證金鑰。

16. 如申請專利範圍第 10 項之安全認證模組之認證方法，其中，該安全認證模組卡係以 onboard 方式產生該 RSA 金鑰對。

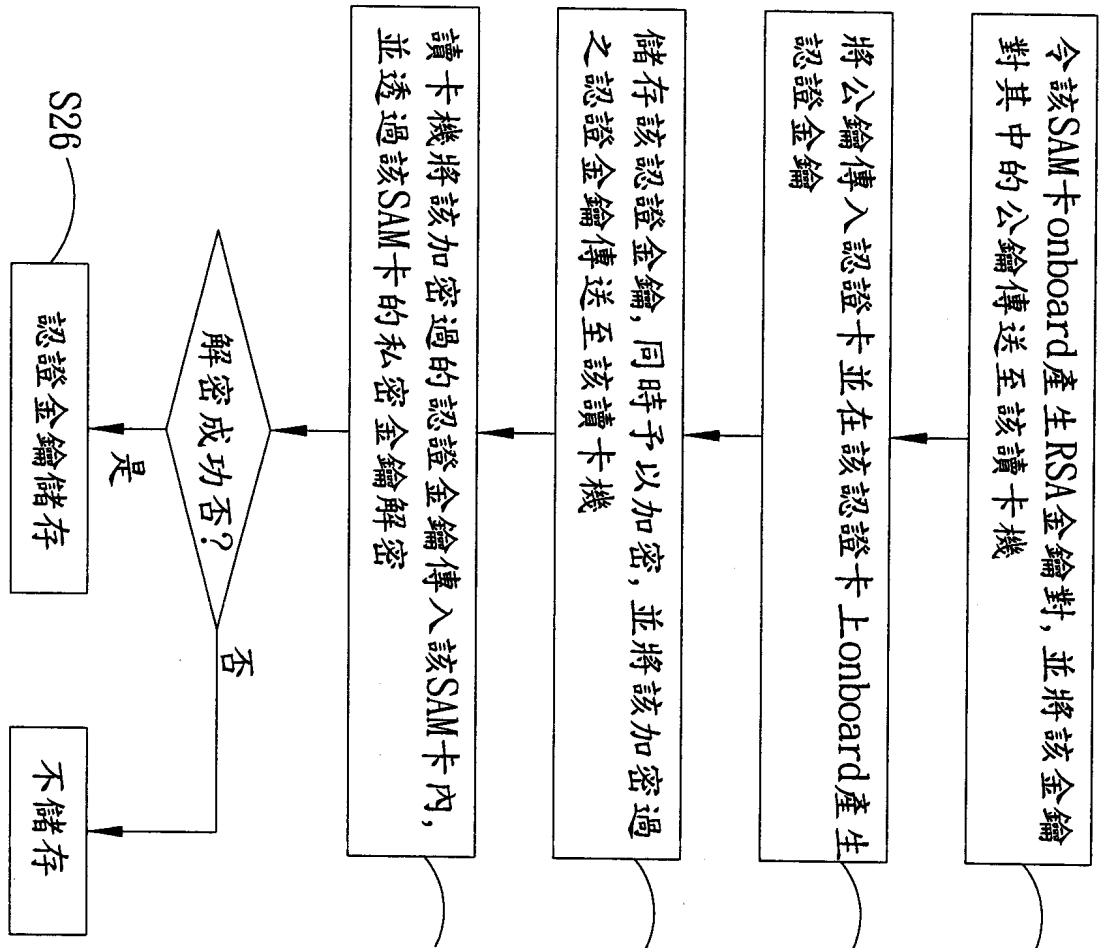
17. 如申請專利範圍第 10 項之安全認證模組之認證方法，其中，該認證卡係以 onboard 方式產生認證金鑰。


1
SAM卡
10
金鑰生成交換模組
12
金鑰註冊功能模組
14
認證卡
20
金鑰傳送模組
22
認證金鑰生成模組
23
認證金鑰加密模組
24
讀卡機
RSA key pair
kpuk
E（K puk , K des3）
kpuk
E（K puk , K des3）
讀卡機本身
2

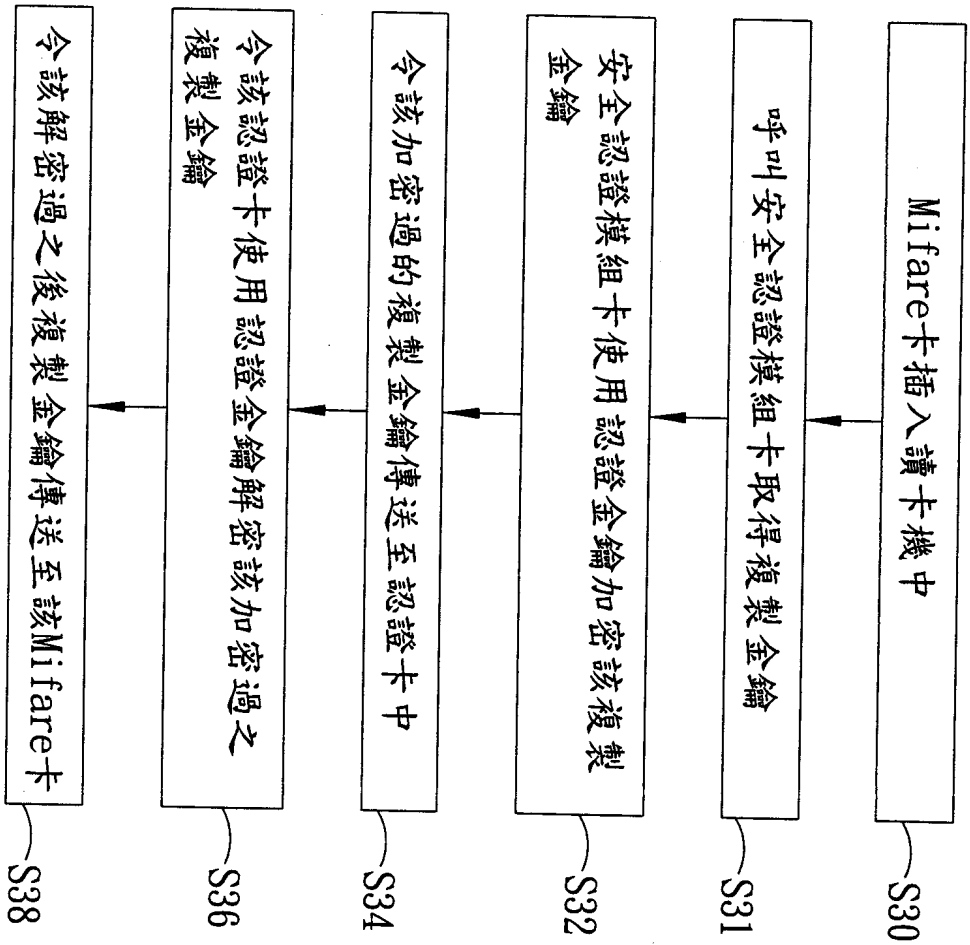
第 1(A) 圖

1'
安全認證模組卡
10
金鑰生成交換模組
12
金鑰註冊功能模組
14
複製金鑰加密模組
16
認證卡
20
複製金鑰解密模組
21
金鑰傳送模組
22
認證金鑰生成模組
23
認證金鑰加密模組
24
讀卡機
(K_A, K_B)
30
Mifare卡

第 1(B) 圖


令該SAM卡onboard產生RSA金鑰對，並將該金鑰對其中的公鑰傳送至該讀卡機
S22
將公鑰傳入認證卡並在該認證卡上onboard產生認證金鑰
S23
儲存該認證金鑰，同時予以加密，並將該加密過之認證金鑰傳送至該讀卡機
S24
讀卡機將該加密過的認證金鑰傳入該SAM卡內，並透過該SAM卡的私密金鑰解密
S25
解密成功否?
否
是
不儲存
認證金鑰儲存
S26

第 2 圖


Mifare卡插入讀卡機中
S30
呼叫安全認證模組卡取得複製金鑰
S31
安全認證模組卡使用認證金鑰加密該複製金鑰
S32
令該加密過的複製金鑰傳送至認證卡中
S34
令該認證卡使用認證金鑰解密該加密過之複製金鑰
S36
令該解密過之後複製金鑰傳送至該Mifare卡
S38

第 3 圖

七、指定代表圖：

(一)本案指定代表圖為：第（1A）圖。

(二)本代表圖之元件代表符號簡單說明：

1	讀卡機
2	讀卡機本身
10	安全認證模組卡
12	金鑰生成交換模組
14	金鑰註冊功能模組
20	認證卡
22	金鑰傳送模組
23	認證金鑰生成模組
24	認證金鑰加密模組

八、本案若有化學式時，請揭示最能顯示發明特徵的化學式：