I419536

(19)中華民國智慧財產局

(12)發明說明書公告本 **(11)證書號數：TW I419536 B**

(45)公告日： 中華民國 102 (2013) 年 12 月 11 日

(21)申請案號：098120541 (22)申請日： 中華民國 98 (2009) 年 06 月 19 日

(51)Int. Cl.： ***H04L9/32 (2006.01)***

(71)申請人：中華電信股份有限公司 (中華民國) CHUNGHWA TELECOM CO., LTD. (TW)
桃園縣楊梅市民族路 5 段 551 巷 12 號

(72)發明人：謝東明 (TW) ；詹景傑 (TW) ；蕭崇懃 (TW) ；林景榮 (TW)

(74)代理人：李保祿

(56)參考文獻：

TW I293530 TW 200513086A1

審查人員：陳雍宗

申請專利範圍項數：6 項 圖式數：3 共 0 頁

(54)名稱

整合憑證與ＩＣ卡管理的安全認證方法

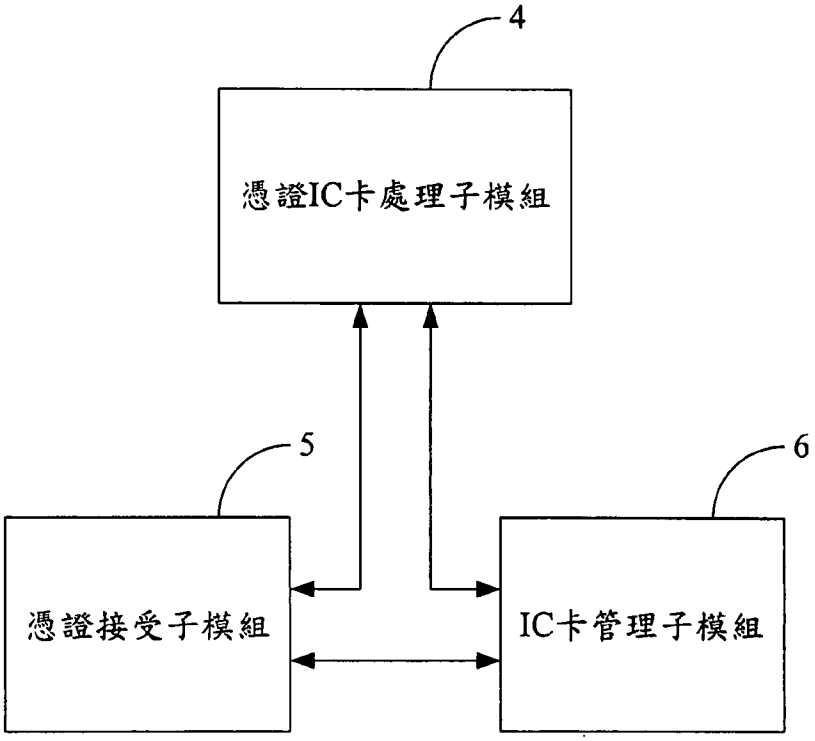
(57)摘要

一種整合憑證與 IC 卡管理的安全認證方法，係使用一安全認證碼將憑證與智慧 IC 卡管理，做安全與有效率地整合，可同時做為 IC 卡 PIN 碼管理服務、線上憑證接受服務、線上憑證停用與憑證復用服務等服務之驗證碼；包含安全認證碼的設定作業及實施安全認證碼設定作業之模組，使該完成設定之安全認證碼可於網路上提供整合 IC 卡之 PIN 碼的管理、線上憑證接受、線上憑證停用與復用等目的。

4・・・憑證 IC 卡處理子模組

5・・・憑證接受子模組

6・・・IC 卡管理子模組



圖二

I419536

公告本

發明專利說明書

（本說明書格式、順序，請勿任意更動，※記號部分請勿填寫）

※申請案號：098120541

※申請日：98 6 19 ※IPC 分類：H04L 9/32 (2006.01)

一、發明名稱：（中文/英文）

整合憑證與IC卡管理的安全認證方法

二、中文發明摘要：

一種整合憑證與IC卡管理的安全認證方法，係使用一安全認證碼將憑證與智慧IC卡管理，做安全與有效率地整合，可同時做為IC卡PIN碼管理服務、線上憑證接受服務、線上憑證停用與憑證復用服務等服務之驗證碼；包含安全認證碼的設定作業及實施安全認證碼設定作業之模組，使該完成設定之安全認證碼可於網路上提供整合IC卡之PIN碼的管理、線上憑證接受、線上憑證停用與復用等目的。

三、英文發明摘要：

四、指定代表圖：

（一）本案指定代表圖為：圖二

（二）本代表圖之元件符號簡單說明：

4　憑證IC卡處理子模組

5　憑證接受子模組

6　IC卡管理子模組

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

六、發明說明：

【發明所屬之技術領域】

本發明係一種整合憑證與IC卡管理的安全認證方法，特別係關於一種運用資訊通信安全之公開金鑰基礎建設(PKI)領域中的憑證管理與 IC 卡管理技術，以達成在網路上提供整合IC卡之PIN碼之管理、線上憑證接受、線上憑證停用與復用等目的。

【先前技術】

目前既有的幾種金融與電信消費的驗證模式，如下所述：

1. 列印密碼函之 PIN 碼傳送：有些網際網路服務提供者（Internet Service Provider，以下簡稱ISP）就是使用所謂的刮刮卡或是列印密碼函之方式，將用戶上網連線的身份驗證密碼放於刮刮卡或密碼函中，用戶在刮開刮刮卡或是拆開密碼函後即可得到連線之密碼；

此模式之缺點為：列印刮刮卡或是密碼函需要紙張及經費，同時於密碼函運送途中可能會造成遺失或是弄錯。

2. 儲值卡：儲值卡於交易之安全性考量方法，通常驗證身份之程序與買賣雙方通訊連絡之程序分開；有些採用網路驗證方式，例如臺灣郵政電子儲值卡，其驗證方式為輸入卡片流水號、刮開之號碼、密碼及個人身分證件號碼或公司之統一編號；

此模式之缺點為：程式複雜且列印密碼函或刮刮卡需要紙張及經費，同時於密碼函運送途中可能會造成遺失或是弄錯。

3. 行動電話之SIM卡：一般行動電話之SIM卡不需要開通，一旦連續三次驗證個人識別碼(Personal Identification Number，以下簡稱PIN)失敗，會造成鎖卡，則持卡者需透過客服，以電話告知身分證字號及出生年月日，便可以取得該SIM卡解鎖之PIN解鎖碼(PIN Unblock Key，以下簡稱PUK)；

此模式之缺點為：以電話告知客服簡單的身分認證就給出PUK碼，在安全的考量上較為不足。

4. 使用 PKI 技術的 IC 卡：一般使用公開金鑰基礎建設(Public Key Infrastructure，以下簡稱 PKI)相關技術之 IC 卡，其 PIN 碼之管理，也是使用前述第 1 項之密碼函之方式，傳送 IC 卡之初始設定 PIN 碼；此外，此種內含憑證之 IC 卡(以下簡稱憑證 IC 卡)遭到鎖卡，其解碼之方式係利用一個含有解鎖卡金鑰之應用安全模組(Secure Application Module，以下簡稱 SAM)之卡，來進行解卡，但是 SAM 之卡係由憑證註冊審驗人員(Registration Authority Operator，以下簡稱 RAO)所保管，其中持卡人也必須親自到註冊窗口(Registration Authority Counter，以下簡稱 RAC)才可以進行解鎖卡；

此模式之缺點為：使用 SAM 卡才可以進行解鎖卡者，雖然於認證的安全性上係足夠，但是用戶必須臨櫃到服務窗口而造成不方便，以及大部分 SAM 卡中都會遇到之 PUK 之管理問題，一旦所有之 IC 卡都用相同之 PUK，只要有任一個 SAM 卡被破解，則 PUK 就被得知；而如果 IC 卡以指號或是每個 IC 卡都用不同之 PUK，則發行與管理這些 SAM 卡便會是營運的一大負荷。

5. 信用卡或複合式金融卡：一般信用卡或金融卡之開卡流程，可利用電話語音開卡或是 ATM(Automatic Teller Machine)自動櫃員機開卡之方式開卡；電話語音開卡之程序一般為撥打專線電話，接著輸入信用卡卡號、信用卡西元有效期限、民國出生年月日，經驗證無誤後，便可完成開卡程序；若是採用 ATM 自動櫃員機開卡，其流程為插入複合式金融卡，輸入密碼單之指定密碼，再輸入個人設定之密碼，再經確認新密碼，變更成功後即啟用成功；如果信用卡或金融卡連續三次驗證 PIN 碼失敗，而造成鎖卡(PIN Block)，則持卡者就必須要回原發卡銀行才可以解碼(Unblock PIN)；

此模式之缺點為：必須回原發卡銀行，造成使用者不方便。

6. 回傳憑證 IC 卡之簽收聯之憑證接受作業：憑證接受(Certificate Acceptance)作業係依照國際規範在憑證簽發後，申請者必須完成之作業，否則簽發出來之憑證便屬無效憑證；憑證管理中心(Certification Authority，以下簡稱 CA)系統，便要求申請者在接到所簽發之憑證 IC 卡後，必須要簽署憑證 IC 卡簽收聯，並將這個簽收聯回寄給憑證管理中心，用以解決憑證

無效之問題；

此模式之缺點為：回傳憑證IC卡簽收聯的方式來進行憑證接受作業之係郵寄而非線上之方式，令使用者感到不方便；無法電子化之作業有收集、登打與保管憑證IC卡簽收聯不易之困擾；此機制之結果係申請者之配合意願低落，造成在申請後便成為尚未有效之「呆卡」，浪費系統之維運成本。

7. 電子現金：消費者先行向發行電子現金之機構購買，或是從個人存摺帳戶中提領一筆電子現金，該發行電子現金之機構之系統便會據此從消費者之指定帳戶中扣除同等金額，消費者在提領出電子現金之後，便可以將電子現金儲存到自己的電腦中，以供日後消費時使用；商店或銀行則是利用數位簽章之技術來驗證電子現金，因此，對於商店或銀行而言，只要判斷電子現金的合法性及有無偽造，或重複使用即可，不需驗證消費者的資料；

此模式之缺點為：無驗證消費者資料的功能，安全考量上較為不足。

由此可見，上述習用物品仍有諸多缺失，實非一良善之設計者，而亟待加以改良。

本案發明人鑑於上述習用整合憑證與 IC 卡管理的安全認證方法所衍生的各項缺點，乃亟思加以改良創新，並經過多年苦心孤詣潛心研究後，終於成功研發完成本件整合憑證與IC卡管理的安全認證方法。

【發明內容】

本發明之目的係在於提供一種整合憑證與 IC 卡管理的安全認證方法，係在發卡前，由持卡者自行選定用以管理 PIN 碼之密碼，達到方便之目的。

本發明之次一目的係在於提供一種整合憑證與 IC 卡管理的安全認證方法，係由持卡人可以在線上透過安全的認證與加解密機制，即可以進行IC 卡之鎖卡解碼，此密碼是持卡人自行設定，所以沒有傳送安全之問題，也可以做到每張IC卡之PUK都是不同的，達到安全之目的。

本發明之再一目的係在於提供一種整合憑證與 IC 卡管理的安全認證

5

方法，係不必列印密碼函或試刮刮卡，達到經濟之目的。

本發明之又一目的係在於提供一種整合憑證與 IC 卡管理的安全認證方法，係在不必發出解鎖卡所需的 SAM 卡，達成不需要管理 SAM 之安全性之目的。

達成上述發明目的之整合憑證與 IC 卡管理安全認證方法，包含一實施用戶代碼設定作業之模組，其中該模組主要係提供用戶代碼之設定作業，又，其中該用戶代碼之設定作業於憑證申請時由用戶自行設定，係包含：自行選定用戶代碼，以該用戶代碼及憑證 IC 卡進行線上憑證接受作業，及以該安全認證碼及憑證 IC 卡進行 IC 卡之 PIN 碼之個人化設定；實施用戶代碼設定作業之模組係包含一憑證 IC 卡處理子模組，該模組執行憑證接受作業；實施用戶代碼設定作業之模組係包含一憑證接受子模組，該模組執行憑證驗證作業；實施用戶代碼設定作業之模組係包含一 IC 卡管理子模組，該模組執行 IC 卡啟用作業；本發明係提供一個可將憑證與智慧 IC 卡管理兩者作安全與有效率地整合，並同時做為 IC 卡 PIN 碼管理服務、線上憑證接受服務、線上憑證停用與憑證復用服務等服務之驗證碼。

【實施方式】

請參閱圖一所示，係本發明所提供之一種整合憑證與 IC 卡管理的安全認證方法之運作架構圖，主要包含有：

一憑證管理中心 1，該憑證管理中心 1 係負責憑證之簽發管理；

一憑證用戶端 2，該憑證用戶端 2 係供該用戶自行設定用戶碼作為憑證管理與 IC 卡 PIN 碼管理，以達到在整合運作時所需之安全認證碼之目的；

一卡管中心 3，該卡管中心 3 主要係負責 IC 卡之初始化及 IC 卡相關存取權限之管理作業；

另外，該憑證管理中心 1、憑證用戶端 2 以及卡管中心 3，彼此係使用 HTTP/HTTPS 協定來傳輸網路訊息。

其中，前述所謂的可由使用者自行設定的用戶代碼，其內容是由使用者自己想出的一組文字、數字或符號，此內容並非藉由任何硬體裝置產生

或得知，也並非藉由任何通訊方法得知。

請參閱圖二所示，為實施本發明之 IC 卡之卡管中心之系統架構示意圖，係包含：

一憑證 IC 卡處理子模組 4，該憑證 IC 卡處理子模組 4 負責讀取 IC 卡資料與憑證資料，並將所讀取之憑證資料做解析後呈獻給用戶確認，用戶確認憑證內容無誤後，該憑證 IC 卡處理子模組 4 再接收用戶所輸入之用戶代碼，並將用戶代碼及 IC 卡資料、憑證資料上傳至憑證接受子模組 5 以及 IC 卡管理子模組 6；

一憑證接受子模組 5，該憑證接受子模組 5 負責將接收來自於憑證 IC 卡處理子模組 4 之用戶代碼、IC 卡資料與憑證資料做資料驗證及進行憑證接受作業；該憑證接受子模組 5 將驗證 IC 卡資料與用戶代碼是否與憑證申請時之資料相符，若不相符則取消憑證接受作業，並傳送通知憑證給 IC 卡處理子模組 6；若資料完全相符，則進行憑證接受作業，並完成用戶之憑證接受；另外，也必須接收 IC 卡管理子模組 6 藉由 IC 卡資料確認憑證是否已被接受之訊息，提供正確的用戶代碼資料，以輔助 IC 卡管理子模組 6 進行驗證作業；

一 IC 卡管理子模組 6，該 IC 卡管理子模組 6 負責將接收來自於憑證 IC 卡處理子模組 4 之用戶代碼與 IC 卡資料，做資料驗證，進行 PIN 碼修改作業；該 IC 卡管理子模組 6，也必須接收來自於憑證接受子模組 5 之憑證通知；另外，該 IC 卡管理子模組 6，將驗證 IC 卡資料與用戶代碼資料是否相符，若相符合便授權給憑證 IC 卡處理子模組 4 進行 PIN 碼之修改作業；

此外，其中該憑證 IC 卡處理子模組 4 接收用戶所輸入之用戶代碼，並將用戶代碼及 IC 卡資料、憑證資料上傳至憑證接受子模組 5，待憑證接受子模組 5 完成憑證接受作業後，再將用戶代碼及 IC 卡資料上傳至 IC 卡管理子模組 6，並由 IC 卡管理子模組 6 取得修改用戶 IC 卡資料之權限，對用戶之 IC 卡進行 PIN 碼修改，完成憑證接受及啟用 IC 卡程序。

請參閱圖三所示，為實施本發明之 IC 卡之卡管中心之系統架構之示意

圖，憑證申請者在憑證申請時，個人用戶代碼之設定作業流程，同步憑證接受子模組 5 將驗證 IC 卡資料與用戶代碼是否與憑證申請時之資料相符，若資料完全相符，則進行憑證接受作業，並完成用戶之憑證接受，其步驟包含：

1. 憑證申請者在憑證申請時，可選擇以臨櫃或公文方式申請，先選定自己之用戶代碼 301；
2. 憑證申請者於臨櫃申請憑證時，於憑證註冊窗口向 RAO 人員送交自設之用戶代碼，而由 RAO 代理申請者將用戶代碼輸入到憑證註冊窗口系統中，RAO 再將所得到之用戶代碼加以銷毀，在以公文方式申請憑證時，在線上以憑證註冊窗口系統所佈建之安全通道，而將用戶代碼傳送到憑證註冊窗口系統中 302；完成用戶代碼申請後，憑證申請者安全妥善的保管其所設定的用戶代碼；

當憑證申請者收到他所申請的憑證 IC 卡後，接下來就必須要進行憑證接受作業，在我國政府機關公開金鑰基礎建設(Government Public Key Infrastructure, 以下簡稱 GPKI)體系中，這是依據 GPKI 憑證政策(CP)的規範，當 CA 完成憑證簽發後，憑證申請者也必須完成憑證接受作業後，則該憑證才能算是有效的憑證；以內政部憑證管理中心(MOICA)自然人憑證為例，憑證申請者可視其需要使用以下兩種方式之一來進行憑證接受作業，第一種為臨櫃方式進行接受憑證，第二種為線上方式進行憑證接受，而以第二種方式，即線上方式，做憑證接受時，就會使用到之前用戶所選定的用戶代碼；此外，當用戶最初收到憑證 IC 卡時，IC 卡的 PIN 碼是被設定成為只有卡管中心才知道之一串亂數，以便於保護 IC 卡在未傳送給其持卡者前，不會被擅意不正當的使用，所以憑證申請者必須再進行該 IC 卡之 PIN 碼個人化設定；

進行線上憑證接受及該 IC 卡的 PIN 碼之個人化設定同步於憑證 IC 卡處理子模組 4 負責讀取 IC 卡資料與憑證資料，並將所讀取之憑證資料做解析後呈獻給用戶確認，用戶確認憑證內容無誤後，該憑證 IC 卡處理子模組 4 再接收用戶所輸入之用戶代碼，並將用戶代碼及 IC 卡資料、憑證資料上

傳至憑證接受子模組 5 之步驟包含：

3. 憑證申請者備妥憑證 IC 卡使用的軟硬體環境，並且將收到的憑證 IC 卡插入到讀卡機內，憑證申請者到訪線上憑證接受的網站，點選憑證接受作業項目，憑證申請者檢視憑證接受網頁所呈現的個人憑證的內容，如果確實無誤，則在網頁中輸入用戶代碼 303；
4. 憑證申請者輸入用戶代碼，並點選送交憑證接受的申請訊息；接著憑證註冊窗口系統便會自動聯結到 PIN 碼之個人化設定網頁，憑證申請者輸入其用戶代碼，等卡管中心驗證用戶代碼與該 IC 卡是配對的之後，即完成進行憑證接受 304；

進行 IC 卡之 PIN 碼之個人化修改，意即卡管中心如何驗證用戶代碼與該 IC 卡是否配對並修改 IC 卡 PIN 碼，其流程同步於憑證 IC 卡處理子模組 4 接收用戶所輸入之用戶代碼，並將用戶代碼及 IC 卡資料、憑證資料上傳至憑證接受子模組 5，待憑證接受子模組 5 完成憑證接受作業後，再將用戶代碼及 IC 卡資料上傳至 IC 卡管理子模組 6，並由 IC 卡管理子模組 6 取得修改用戶 IC 卡資料之權限，對用戶之 IC 卡進行 PIN 碼修改，意即將原本 IC 卡的初始 PIN 碼，這個只有卡片管理中心才知道之一串亂數，改成使用者要的 PIN 碼，完成憑證接受及啟用 IC 卡程序之步驟包含：

5. 完成進行憑證接受 304 後，便會允許憑證申請者以用戶代碼進行該 IC 卡之 PIN 碼修改 305；
6. 完成該 IC 卡之 PIN 碼之修改 306；

如果用戶的憑證 IC 卡遺失，或是短期內不想使用該憑證 IC 卡，由於用戶代碼是用戶與 CA 先前約定好的另一種安全管道的身分鑑別依據，所以用戶便可以應用此用戶代碼來進行憑證，同步於憑證 IC 卡處理子模組 4 負責讀取 IC 卡資料與憑證資料，並將所讀取之憑證資料做解析後呈獻給用戶確認，用戶確認憑證內容無誤後，該憑證 IC 卡處理子模組 4 再接收用戶所輸入之用戶代碼，並將用戶代碼及 IC 卡資料、憑證資料上傳至憑證接受子模組 5 之步驟包含：

7. 停用或復用 307；

8. 完成進行憑證之停用或復用 308；

用戶完成憑證接受及該 IC 卡之 PIN 碼之個人化設定後，如果由於 IC 卡之 PIN 碼忘記，或是 IC 卡被鎖卡，則執行前述同步於憑證 IC 卡處理子模組 4 接收用戶所輸入之用戶代碼，並將用戶代碼及 IC 卡資料、憑證資料上傳至憑證接受子模組 5，待憑證接受子模組 5 完成憑證接受作業後，再將用戶代碼及 IC 卡資料上傳至 IC 卡管理子模組 6，並由 IC 卡管理子模組 6 取得修改用戶 IC 卡資料之權限，對用戶之 IC 卡進行 PIN 碼修改，完成憑證接受及啟用 IC 卡程序就可以以用戶代碼進行解鎖之步驟包含：

9. 以用戶代碼進行解鎖 309；

10. 完成以用戶代碼進行解鎖 310。

本發明所提供之一種整合憑證與 IC 卡管理的安全認證碼，與其他習用技術相互比較時，更具備下列優點：

1.本發明係由持卡者自行設定用戶代碼，所以無安全傳送之問題。

2.本發明可做到每張 IC 卡之 PUK 都是不同的。

3.本發明可做到不必列印密碼函。

4.本發明不必再發出解鎖卡所需的 SAM 卡，更沒有管理 SAM 卡安全之工作。

上列詳細說明乃針對本發明之一可行實施例進行具體說明，惟該實施例並非用以限制本發明之專利範圍，凡未脫離本發明技藝精神所為之等效實施或變更，均應包含於本案之專利範圍中。

綜上所述，本案不僅於技術思想上確屬創新，並具備習用之傳統方法所不及之上述多項功效，已充分符合新穎性及進步性之法定發明專利要件，爰依法提出申請，懇請　貴局核准本件發明專利申請案，以勵發明，至感德便。

【圖式簡單說明】

圖一為本發明整合憑證與 IC 卡管理的安全認證方法之運作架構圖；

圖二為本發明整合憑證與 IC 卡管理的安全認證方法之 IC 卡的卡管中心之系統架構示意圖；

圖三為本發明整合憑證與 IC 卡管理的安全認證方法之時序流程圖。

【主要元件符號說明】

1　憑證管理中心

2　憑證用戶端

3　卡管中心

4　憑證 IC 卡處理子模組

5　憑證接受子模組

6　IC 卡管理子模組

102 年 8 月 22 日修正替換頁

七、申請專利範圍：

1. 一種整合憑證與IC卡管理的安全認證方法，係包括：

設定一安全認證碼，該安全認證碼係由使用者自行設定，非藉由任一硬體裝置產生或得知，非藉由任何通訊方法得知；以及

一該安全認證碼之憑證接受作業，係指使用者完成憑證IC卡申請作業時，簽發出的憑證IC卡的憑證仍屬無效憑證，必須將此憑證IC卡寄送給使用者，使用者收到IC卡後進行證明目前持卡者確實是使用者本人，證明通過後才能使此憑證IC卡的憑證成為有效憑證。

2. 如申請專利範圍第 1 項所述之憑證與 IC 卡管理的安全認證方法，其中的該安全認證碼除了憑證管理中心外，只有使用者本人知道內容，能夠代表使用者本人，作為憑證接受作業中使用者和憑證管理中心約定的安全管道的身份鑑別依據，以驗證該安全認證碼來整合及取代過去憑證接受作業中，使用者簽名並回寄簽收聯給憑證管理中心，以及，卡片管理中心寄發 PIN 碼信函給使用者等動作，解決其驗證身份和資料傳送安全問題。

3. 如申請專利範圍第 1 項所述之憑證與 IC 卡管理的安全認證方法，其中更包含：

先將該安全認證碼儲存到憑證資訊系統；

再使用該安全認證碼進行憑證接受作業。

4. 如申請專利範圍第 3 項所述之憑證與 IC 卡管理的安全認證方法，其中該安全認證碼儲存到憑證資訊系統更包含：

使用者在做憑證申請時，若選擇臨櫃申請，則使用者自己先想好該安全認證碼，在 RAO 憑證註冊窗口臨櫃申請憑證的同時，向 RAO 人員送交該安全認證碼，而由 RAO 人員將該安全認證碼輸入到憑證註冊窗口系統，RAO 人員再將所得到之安全認證碼加以銷毀；

或者，使用者在做憑證申請時，若選擇公文申請，則使用者自己先想好該安全認證碼，然後直接在線上以憑證註冊窗口系統所佈建之安全通道，將該安全認證碼傳送到憑證資訊系統中。

5. 如申請專利範圍第 3 項所述之憑證與 IC 卡管理的安全認證方法，其中該安全認證碼進行憑證接受作業更包含：

a.使用者在完成憑證申請作業後，將收到憑證管理中心寄發的憑證 IC 卡，此 IC 卡的初始 PIN 碼是被設定成為只有卡片管理中心才知道之一串亂數，以保護 IC 卡在未寄發給其使用者，並且使用者未完成憑證接受作業前，不會被擅意不正當的使用；

b.使用者將收到的憑證 IC 卡插入讀卡機，然後進入憑證接受作業網站，點擊憑證接受作業項目；

c.憑證 IC 卡處理子模組讀取使用者的 IC 卡資料與其中的憑證資料，並將所讀取的憑證資料做解析後做呈現；以及

d.使用者在憑證接受作業網頁檢視所呈現的個人憑證內容，如果確實無誤，則在網頁中輸入用戶代碼，並點選送交憑證接受的申請訊息；接著憑證註冊窗口系統自動聯結到 PIN 碼之個人化設定網頁，憑證申請者輸入其用戶代碼，由卡片管理中心驗證用戶代碼與該 IC 卡是否配對，若配對，即完成憑證接受作業。

6. 如申請專利範圍第 5 項所述之憑證與 IC 卡管理的安全認證方法，其中卡片管理中心驗證用戶代碼與該 IC 卡是否配對，步驟如下：憑證 IC 卡處理子模組將接收使用者輸入之安全認證碼，並將此安全認證碼及 IC 卡資料、憑證資料，上傳至一憑證接受子模組；

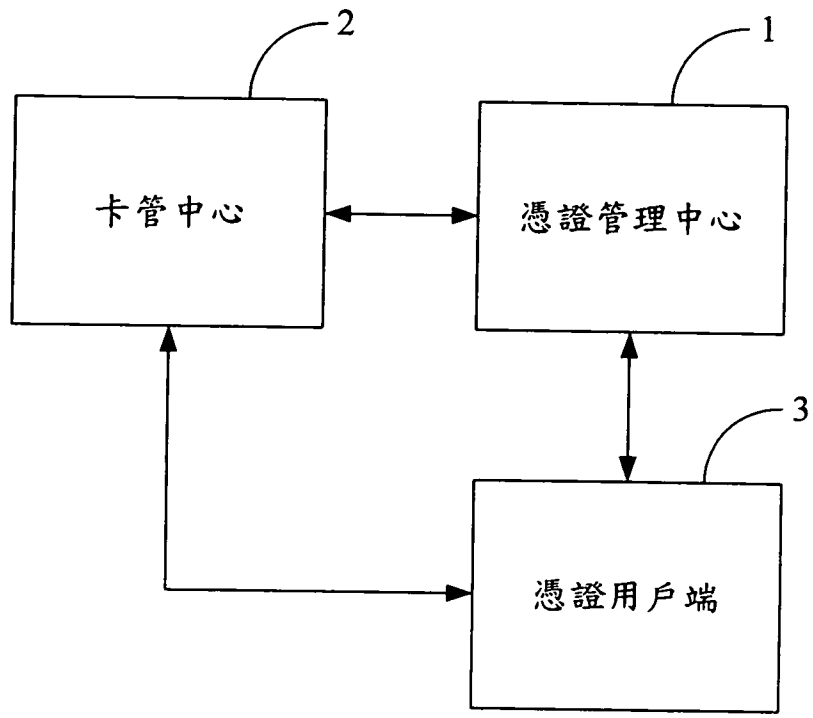
該憑證接受子模組驗證安全認證碼與 IC 卡資料是否與憑證申請時相符，若不相符則取消憑證接受作業，並傳送通知憑證給 IC 卡處理子模組；

若相符，則進行憑證接受作業，並完成用戶之憑證接受；以及

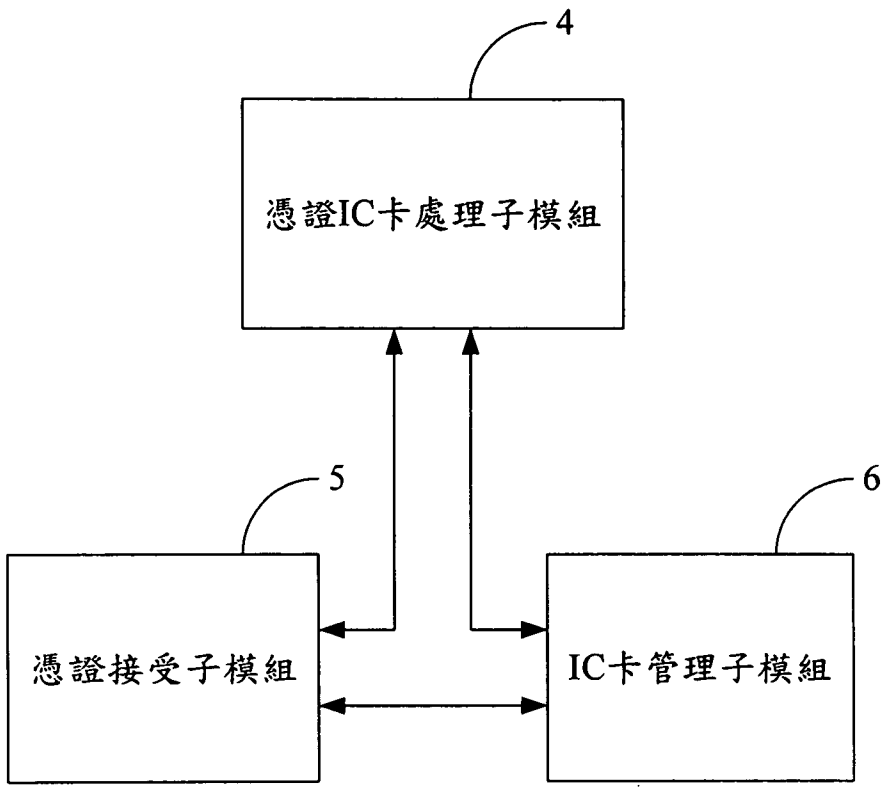
憑證接受子模組完成憑證接受作業之後，再將用戶代碼及 IC 卡

憑證接受子模組完成憑證接受作業之後，再將用戶代碼及 IC 卡資料上傳至 IC 卡管理子模組，並由 IC 卡管理子模組取得修改用戶 IC 卡資料之權限，對用戶之 IC 卡進行 PIN 碼修改，意即將原本 IC 卡的初始 PIN 碼，這個只有卡片管理中心才知道之一串亂數，改成使用者要的 PIN 碼，完成憑證接受及啟用 IC 卡程序。

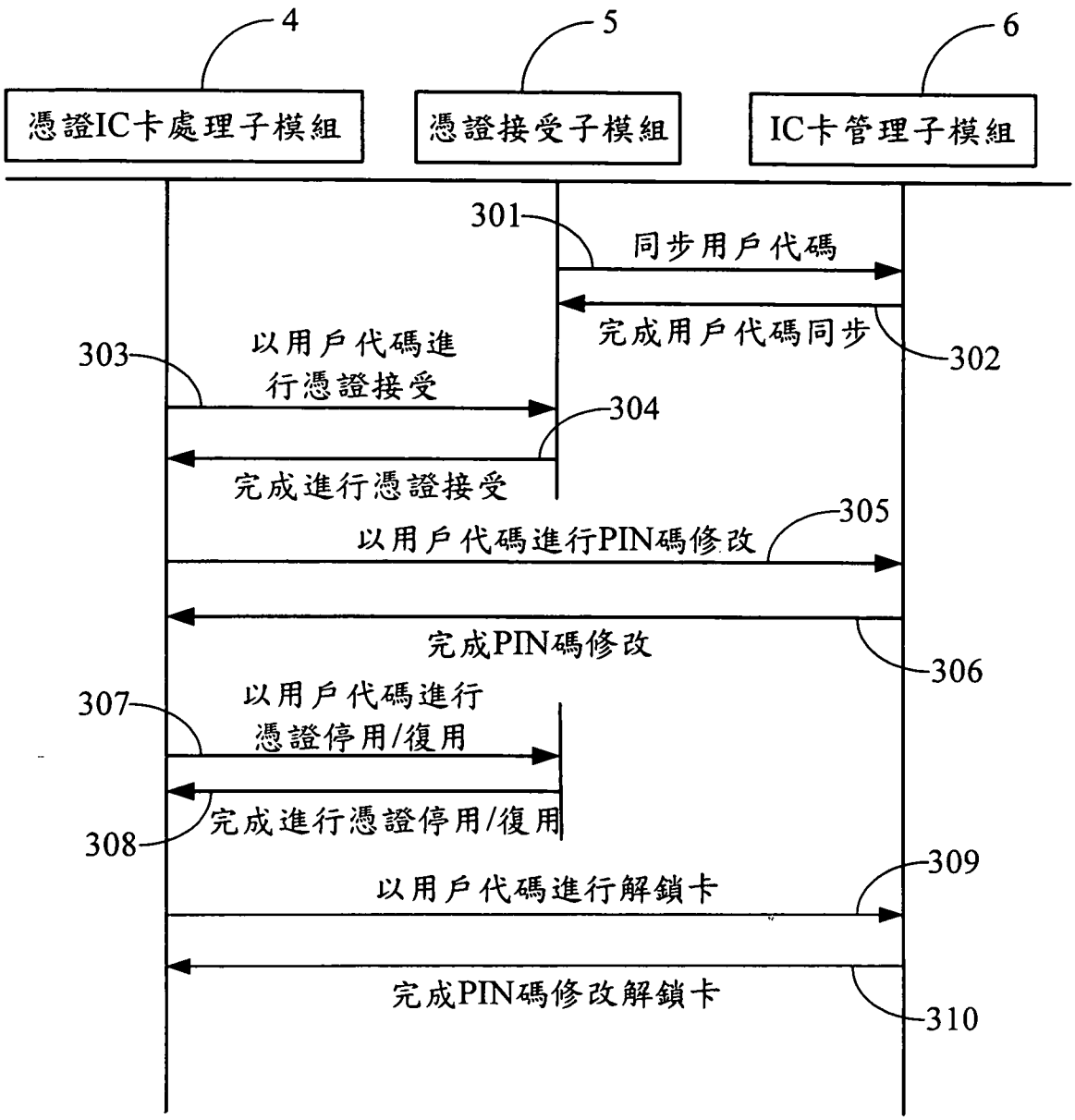
八、圖式：



圖一



圖二


4
5
6
憑證IC卡處理子模組
憑證接受子模組
IC卡管理子模組
301
同步用戶代碼
完成用戶代碼同步
302
303
以用戶代碼進行憑證接受
304
完成進行憑證接受
305
以用戶代碼進行PIN碼修改
完成PIN碼修改
306
307
以用戶代碼進行憑證停用/復用
308
完成進行憑證停用/復用
309
以用戶代碼進行解鎖卡
完成PIN碼修改解鎖卡
310

圖三