I524712

(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 I524712 B**

(45)公告日： 中華民國 105 (2016) 年 03 月 01 日

(21)申請案號：099115640 (22)申請日： 中華民國 99 (2010) 年 05 月 17 日

(51)Int. Cl.： ***H04L29/06 (2006.01)***

(71)申請人：中華電信股份有限公司 (中華民國) (TW)
桃園市楊梅區電研路 99 號

(72)發明人：林崇頤 (TW) ；王亮盛 (TW) ；邱華洲 (TW) ；羅志賢 (TW)

(74)代理人：李保祿

(56)參考文獻：

TW 200828939A CN 1598862A

CN 101625727

審查人員：謝文元

申請專利範圍項數：17 項 圖式數：9 共 37 頁

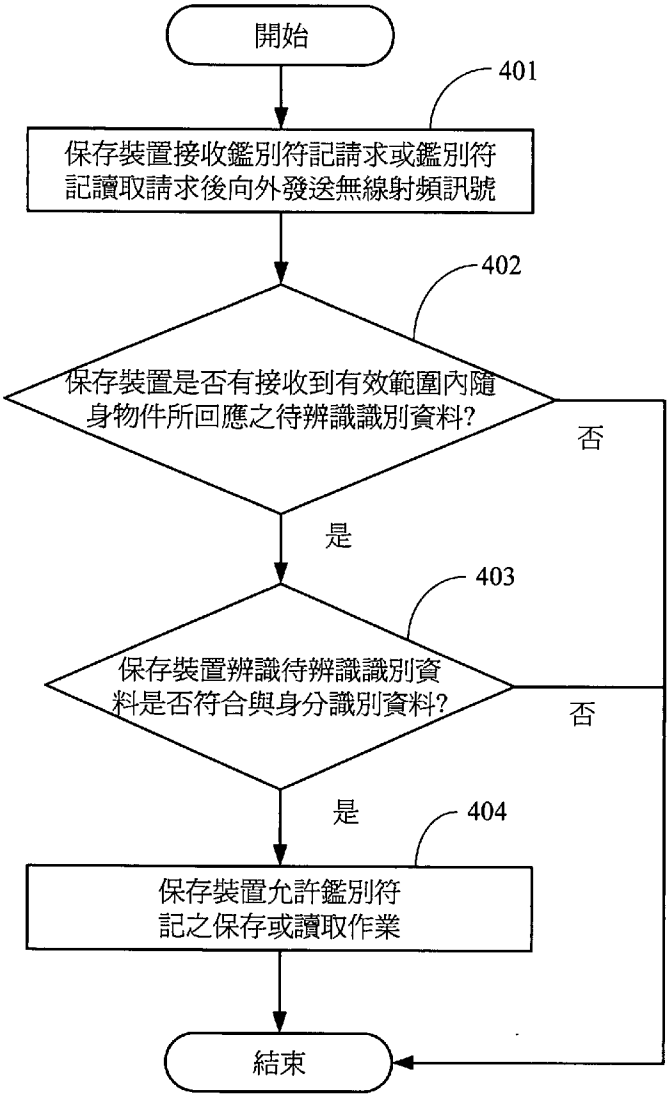
(54)名稱

防止鑑別符記被盜用之系統及其方法

(57)摘要

一種防止鑑別符記被盜用之系統及其方法，係利用設有一無線射頻讀取器以一身分識別資料之保存裝置以保存鑑別符記，另於安裝一射頻識別元件並設有一待辨識識別資料之隨身物件由使用者攜帶；其中，該保存裝置接收鑑別符記保存請求或鑑別符記讀取請求後，發出無線射頻訊號，於無線射頻訊號有效範圍內存在該隨身物件時，該保存裝置將接收該隨身物件所回應之待辨識別資料，並辨識待辨識識別資料是否符合與身分識別資料，若符合則該保存裝置才可允許鑑別符記之保存或讀取作業；本發明可於鑑別符記保護上立即辨識操作使用者且不需額外操作程序。

指定代表圖：


開始
401
保存裝置接收鑑別符記請求或鑑別符記讀取請求後向外發送無線射頻訊號
402
保存裝置是否有接收到有效範圍內隨身物件所回應之待辨識識別資料?
否
是
403
保存裝置辨識待辨識識別資料是否符合與身分識別資料?
否
是
404
保存裝置允許鑑別符記之保存或讀取作業
結束

圖四

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：99115640

※申請日：99.5.17　※IPC 分類：H04L 29/06 (2006.01)

一、發明名稱：（中文/英文）

防止鑑別符記被盜用之系統及其方法

二、中文發明摘要：

一種防止鑑別符記被盜用之系統及其方法，係利用設有一無線射頻讀取器以一身分識別資料之保存裝置以保存鑑別符記，另於安裝一射頻識別元件並設有一待辨識識別資料之隨身物件由使用者攜帶；其中，該保存裝置接收鑑別符記保存請求或鑑別符記讀取請求後，發出無線射頻訊號，於無線射頻訊號有效範圍內存在該隨身物件時，該保存裝置將接收該隨身物件所回應之待辨識別資料，並辨識待辨識識別資料是否符合與身分識別資料，若符合則該保存裝置才可允許鑑別符記之保存或讀取作業；本發明可於鑑別符記保護上立即辨識操作使用者且不需額外操作程序。

三、英文發明摘要：

四、指定代表圖：

(一)本案指定代表圖為：圖四

(二)本代表圖之元件符號簡單說明：

無

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】

本發明係關於一種安全資料處理系統，特別關於一種利用設有一無線射頻讀取器以一身分識別資料之保存裝置以保存鑑別符記，另於安裝一射頻識別元件並設有一待辨識識別資料之隨身物件由使用者攜帶，達成防止鑑別符記被盜用之系統及其方法。

【先前技術】

隨著越來越多網站攻擊事件的發生，導致許多重要機密資料(如客戶個資)外洩，目前網站採用多種安全機制來加以防護，如：身分鑑別與授權、資訊保密或實體網路安全等。其中，身分鑑別便是使用者在網站的資安機制層層把關下，面對的第一道關卡。各種方式如：帳號及密碼、智慧卡 PIN 碼、一次性動態密碼或生物特徵碼等，均需要使用者輸入身分鑑別資訊，待鑑別無誤後方可登入網站。但如果需記得多組網站帳號及密碼，並且需於每個網站一一鍵入鑑別資訊，此對使用者之操作上極為不便，而為提高身分鑑別流程之便利性，目前網站採用單一登入機制(Single Sign-On，SSO)，使得只需於一鑑別網站輸入一次鑑別資訊，即可一併登入其它複數個網站。

傳統單一登入機制由一鑑別網站進行集中身分鑑別，其係為使用者於用戶端連結鑑別網站並輸入身分鑑別資訊(如：帳號及密碼、智慧卡 PIN 碼或一次性動態密碼或生物特徵碼等)，在成功鑑別後將發行一鑑別符記至用戶端；而當使用者欲存取提供應用程式之網站時，該網站將會先檢查用戶端上是否持有該鑑別符記，若已經存在，則將於驗證鑑別符記及判斷使用者身分後允許使用者登入，若否，則會重新導向回鑑別網站要求重新進行身分鑑別；是故，單一登入機制中完

全信任鑑別符記作為鑑別依據，並擁有不必要求使用者再次進行鑑別作業即可直接存取網站之便利性，但倘若該鑑別符記遭受攻擊者盜用，則將造成攻擊者可直接跳過鑑別作業，並以原使用者身分存取網站進行後續攻擊。

而後，有業者試圖提出保護該鑑別符記以防止被盜用之方法，如已公開之中華民國專利證書公告號第 528957 號「以網路為基礎的跨網域單一登入鑑定之方法和系統」，該方法係利用一“引入鑑定記號”(即本發明敘述之“鑑別符記”)將一已經鑑定過的使用者從一網域透過單一登入機制引入到一新網域，並同時試圖於該引入鑑定記號上利用一密碼鍵編密保護及一有限的生命時限保護，藉此改善可能被盜用之問題；然而，上述該先前創作，其安全性與便利性仍是不足，安全性不足之原因在於鑑別符記仍然有機會遭到攻擊者盜用，而便利性不足之原因在於為保護鑑別符記卻需要增加使用者額外操作程序；首先，說明鑑別符記仍可能被盜用之原因。該先前創作係將鑑別符記存放於用戶端 cookie，而如眾所周知，該 cookie 可為一持續性檔案型態資料或是一暫時性記憶體型態資料，但是此兩種型態 cookie 資料都有可能被攻擊者藉由已知跨網站攻擊程式(Cross Site Scripting，簡稱 XSS)盜取，而其中檔案型態 cookie 資料更可能被攻擊者透過系統漏洞自遠端存取，因此，即使利用該先前創作所揭露之一密碼鍵編密，將鑑別符記以密文形式傳送以防止鑑別符記遭到攻擊者之竊取及竄改，但是由於該鑑別符記之密文仍係存放於用戶端 cookie，因此即可能透過上述 cookie 攻擊方式盜取到鑑別符記。又，即使於該先前創作再透過習用技術 https 於鑑別網站、應用程式網站、及用戶端進行編密傳送，雖可防止鑑別符記於傳送過程中被盜取，但是由於用戶端同樣係存放於易受攻擊之 cookie 中，因此攻擊者仍可能於用戶端上盜取到鑑

別符記，該鑑別符記之密文若被攻擊者於用戶端上或於應用程式網站傳送過程中盜取到後，於不需要進行任何修改下，直接往攻擊目標網站重新傳送，而因為該密碼鍵及該鑑別符記密文皆未遭到竄改，所以該網站可正常解密出該鑑別符記，進而允許攻擊者以盜用之身分登入網站，也因此無法解決鑑別符記可被盜用之問題。

此外，該先前創作以一有限的生命時限保護鑑別符記之方式，仍無法有效防止盜用之發生，該先前創作試圖於鑑別符記加上一生命時限，一旦超過該生命時限範圍，則鑑別符記將為無效力狀態，再無法繼續使用於單一登入作業。此方式可於鑑別符記即使遭受盜取複製，仍可利用一短時段限制攻擊時間，而降低被盜用之風險，然而，如生命時限之時間設定太短，則可能因為網路延遲問題使得正常單一登入作業無法繼續，如生命時限之時間設定太長，則增加了於時間內被攻擊盜用之機會，由此可知，該生命時限之時間設定，無法於不影響正常單一登入作業下有效解決防止鑑別符記被盜用之問題。

而另一鑑別符記可能被盜用之狀況起因於使用者的操作習慣，當使用者於單一登入狀態下臨時離開用戶端時，常會方便於不中斷原有工作，並不會每次都完全登出所有網站，因為一旦使用單一登出，則下次繼續工作時必須再至鑑別網站重新進行一次鑑別作業，若使用者離開用戶端時未完全登出所有網站，則存在用戶端之鑑別符記於生命時限範圍內仍為有效力之狀態，只要攻擊者得以於該時間限制內透過遠端或本機操作用戶端盜用鑑別符記，即可於不需要進行鑑別作業下利用原使用者身分存取應用程式網站。

現在說明該先前創作為保護鑑別符記而需要增加使用者額外操作程序之缺點，根據上述說明，因 cookie 可能被盜取、

生命時限內仍可能被重送、以及使用者離開用戶端時未完全登出之操作習慣等因素，鑑別符記仍存有被盜用之風險，為減少此部份資安漏洞，目前習用之技術為縮短該生命時限至可接收之時間範圍(如：30 分鐘)，然而，當使用者於網站之作業時間即將超過鑑別符記之生命時限範圍時，因鑑別符記之生命時限設定只會發生在鑑別網站進行成功之身分鑑別時，一旦開始進行應用程式網站之存取後便無法對生命時限進行設定，以確保該生命時限不會被非法變更，也就是說該生命時限到期時鑑別符記將為無效力之狀態並無法變更，所以使用者需再次於鑑別網站進行身分鑑別，或者透過鑑別網站之延長單一登入有效期間機制自行重新設定另一生命時限，由此可知，此方式同時增加使用者之不便。

又，另一習用技術為利用一密碼保護程式於一時間內閒置時鎖定用戶端，用戶端除原使用者輸入正確密碼外無法被其他人使用，進而使得攻擊者無法於用戶端鎖定後盜用鑑別符記，但是，此方式同樣也存在時間鎖定前仍可遭到有心人士盜用之安全問題，以及使用者於每次鎖定後都需再輸入密碼以解除保護之不便。

由此可見，上述習用方式中攻擊者仍得以利用鑑別符記生命時限到期前之時間差盜用鑑別符記存取應用程式網站，此外，為防止鑑別符記被盜用需使用者進行額外之操作程序。所以，存在安全性與便利性無法兩全的問題，實非一良善之設計，而亟待加以改良。

本案發明人鑑於上述習用方式所衍生的各項缺點，乃亟思加以改良創新，並經苦心孤詣潛心研究後，終於成功研發完成本件防止鑑別符記被盜用之系統及其方法。

【發明內容】

本發明之目的即在於提供一種防止鑑別符記被盜用之系

統及其方法，係於先前技藝鑑別符記保存與鑑別符記讀取之保護技術程序上增加辨識操作使用者步驟，可於攻擊者進行盜用之時立即辨識操作使用者是否原使用者，這使得鑑別符記無法被非法改寫與讀取，此外，只要使用者攜帶一隨身物件即可持續保持單一登入狀態，並於離開用戶端後，立即自動對鑑別符記進行保護以防止任何人使用任何方式盜用。藉此本發明可防止鑑別符記於儲存及傳送過程中被非法人士以竊取、竄改、重新傳送等方式盜用，並降低傳統鑑別符記保護機制所需之額外時間成本及人力成本，同時解決安全性與便利性不足問題。

可達成上述發明目的之一種防止鑑別符記被盜用之系統及其方法，係利用設有一無線射頻讀取器，其係利用無線射頻技術讀取使用者隨身物件及其射頻識別元件、一保存裝置，其係用以存放身分識別資料及保存鑑別符記、一射頻識別元件，以及一隨身物件，其係由使用者攜帶，並用以識別待辨識識別資料；本發明另提供一種防止鑑別符記被盜用之方法，首先該保存裝置於接收鑑別符記保存請求或鑑別符記讀取請求後，向外發送無線射頻訊號，若於該保存裝置所發送之無線射頻訊號有效範圍內存在該隨身物件時，則該保存裝置將可接收到該隨身物件所回應之該待辨識識別資料，而當該保存裝置接收到該待辨識識別資料時，則辨識待辨識識別資料是否符合與身分識別資料，若待辨識識別資料符合身分識別資料，則該保存裝置才可允許鑑別符記之保存或讀取作業。

因此本發明可提高鑑別符記安全性，係於於先前技藝鑑別符記保存與鑑別符記讀取之保護技術程序上增加辨識操作使用者步驟，可於攻擊者進行盜用之時立即辨識操作使用者是否原使用者，這使得鑑別符記無法被非法改寫與讀取，進而

防止鑑別符記於儲存及傳送過程中被非法人士以竊取、竄改、重新傳送等方式盜用。另外本發明可同時提高使用者便利性，係只要使用者攜帶一隨身物件即可持續保持單一登入狀態，並於離開用戶端後，立即自動對鑑別符記進行保護以防止任何人使用任何方式盜用，所以可於無需額外的操作程序下，降低為傳統鑑別符記保護機制所需之時間成本及人力成本。

【實施方式】

請參考圖一 A 所示為習用技術之架構圖，舉例說明於系統網路中單一登入機制中可能使用之防止鑑別符記被盜用之習知技術，存在一鑑別伺服器 240 為提供使用者輸入身分鑑別資訊，於鑑別成功後將發行一鑑別符記 218 至用戶端 260 保存，而該鑑別符記 218 通常保存於用戶端 260 之 cookie 內，因 cookie 已知為不安全之儲存區域，故加上編密保護以防止該鑑別符記 218 內容遭受竊取及竄改，至於使用者欲存取受保護資源之應用網路程式伺服器 250 時，則需讀取該用戶端 260 中之該鑑別符記 218 以作為鑑別依據與判斷使用者身分，而為降低重送攻擊之威脅，應用網路程式伺服器 250 需檢驗該鑑別符記 218 之生命時限是否為有效範圍後才允許存取。也就是說，該系統中完全信任鑑別伺服器 240 所發行於用戶端 260 之鑑別符記 218 作為鑑別依據，只要用戶端 260 存在有效之鑑別符記 218 即不必再次進行鑑別作業可直接存取受保護資源之應用網路程式伺服器 250。

請參考圖一 B 所示為習用技術之流程圖，表示鑑別伺服器、應用網路程式伺服器與用戶端間以時間發生先後順序之訊息傳遞與處理程序，當鑑別伺服器完成使用者身分鑑別並發行鑑別符記之過程中，防止鑑別符記被盜用之一習用技術程序：

步驟一：使用者於鑑別伺服器輸入身分鑑別資訊(101)；

步驟二：該鑑別伺服器鑑別身分鑑別資訊(102)；

步驟三：並於該鑑別伺服器0成功鑑別時，產生具一生命時限之鑑別符記(103)；

步驟四：該鑑別伺服器繼續使用已取得之應用網路程式伺服器公用密碼鍵編密鑑別符記，並產生鑑別符記密文(104)；

步驟五：該鑑別伺服器向該使用者操作之用戶端發行鑑別符記密文(105)；

步驟六：該用戶端保存該鑑別符記密文(106)；

步驟七：該用戶端回應保存鑑別符記成功訊息(107)；

步驟八：該鑑別伺服器將使用者導向存取受保護資源(108)。

請參考圖一C所示為習用技術之作業循序圖，舉例說明應用網路程式伺服器要求讀取鑑別符記並完成檢驗之過程中，防止鑑別符記被盜用之一習用技術程序：

步驟九：使用者要求存取受保護資源之應用網路程式伺服器(109)；

步驟十：應用網路程式伺服器要求讀取鑑別符記密文(110)；

步驟十一：用戶端讀取鑑別符記密文(111)；

步驟十二：用戶端於成功讀取回應鑑別符記密文後，將回應鑑別符記密文回應至應用網路程式伺服器(112)；

步驟十三：應用網路程式伺服器使用本身之私用密碼鍵解密鑑別符記密文(113)；

步驟十四：應用網路程式伺服器判斷鑑別符記是否於生命時限內(114)；

步驟十五：若鑑別符記於生命時限內之有效狀態，則允許使用者存取應用網路程式伺服器(115)。

請參閱圖二所示，為本發明一種防止鑑別符記被盜用之系統之架構圖，包括：

一隨身物件 230，其係安裝一射頻識別元件 231 並設有一待辨識識別資料 232；

一保存裝置 210，該保存裝置 210，係提供保放鑑別符記 218 之裝置，並設有一無線射頻讀取器 214 及一身分識別資料 217 可與隨身物件 230 的待辨識識別資料 232 做辨識用；

在本發明之一較佳實施例中，該保存裝置 210 在保存與讀取鑑別符記 218 時，係透過該無線射頻讀取器 214 向外發出一無線射頻訊號，而當該射頻識別元件 231 於有效範圍內感應到保存裝置 210 所發射之無線射頻訊號時，將該待辨識識別資料 232 回傳；

此外，該隨身物件 230 係可為項鍊、手鍊、戒指、鑰匙圈或識別證，使得使用者可於操控該用戶端 260 時隨身攜帶；而由於該隨身物件 230 中待辨識識別資料 232 與該保存裝置 210 中身分識別資料 217 為具唯一性之無線射頻識別碼，當待辨識識別資料 232 與該身分識別資料 217 不相符時，則該保存裝置 210 無法保存與讀取鑑別符記 218；

此外，為使得鑑別符記 218 於鑑別伺服器 240、用戶端 260、以及應用網路程式伺服器 250 之傳送過程、已經傳送至該用戶端 260 但尚未保存入保存裝置 210 前之保存過程、以及已經從該保存裝置 210 讀取出但尚未從用戶端 260 開始回傳之讀取過程無法被非法從中擷取，在該實施例中，請參閱圖二所示，於本發明進一步包括：

一發行模組 241、一讀取模組 251 以及一用戶端安控模組 261；其中，該發行模組 241 係安裝於鑑別伺服器 240，並提供鑑別符記 218 之加密與發行；其中，該讀取模組 251 係安裝於應用網路程式伺服器 250，並提供鑑別符記 218 之解密與

讀取；其中，該用戶端安控模組261係安裝於用戶端260，保存裝置210連接於用戶端260，使得該用戶端安控模組261可對保存裝置210做安控存取。

請參閱圖三所示，為本發明一種防止鑑別符記被盜用之系統之保存裝置示意圖，該保存裝置更包括：

一介面模組211、一加解密模組212、一辨識模組213、一處理器215，以及一記憶模組216；其中，該介面模組211係與該用戶端260連結之介面，並使得該發行模組241與該讀取模組251可透過該用戶端安控模組261存取保存裝置210中之鑑別符記218，此外該介面模組211係可為一PCI、PCI Express、PCMCIA或USB介面；其中該加解密模組212係提供加密計算與解密計算；其中該辨識模組213係提供辨識待辨識識別資料232與身分識別資料217是否相符之計算；其中該處理器215係為接收與執行各模組所傳遞程式訊號；其中該記憶模組216係為記憶與儲存身分識別資料217、鑑別符記218、公開金鑰219及私密金鑰220。

請參閱圖四所示，為本發明一種防止鑑別符記被盜用之方法之流程圖，其特徵為利用一種防止鑑別符記被盜用之系統的無線射頻讀取器及一身分識別資料之保存裝置以保存鑑別符記，另於安裝一射頻識別元件並設有一待辨識識別資料之隨身物件由使用者攜帶，並於實施時依下列步驟進行辨識操作使用者：

步驟一：該保存裝置於接收鑑別符記保存請求或鑑別符記讀取請求後，向外發送無線射頻訊號(401)；

步驟二：若於該保存裝置所發送之無線射頻訊號有效範圍內存在該隨身物件時，則該保存裝置將可接收到該隨身物件所回應之該待辨識識別資料(402)；

步驟三：而當該保存裝置接收到該待辨識識別資料時，則

辨識待辨識識別資料是否符合與身分識別資料(403)；

步驟四：若待辨識識別資料符合身分識別資料，則該保存裝置才可允許鑑別符記之保存或讀取作業(404)，並結束流程。

而為使得目前傳統單一登入機制可用更容易與更安全之形式實施本發明之方法，本發明進一步包括利用一種防止鑑別符記被盜用之系統，當於成功鑑別使用者身分並產生鑑別符記後由一發行模組啟動之鑑別符記安全發行方法，以及後續讀取鑑別符記作為成功鑑別依據時由一讀取模組啟動之鑑別符記安全讀取方法；其中，該鑑別符記安全發行方法與該鑑別符記安全讀取方法係經由一用戶端安控模組操控該保存裝置以無線射頻訊號讀取該隨身物件內該待辨識識別資料；亦即，鑑別符記安全發行方法(請參閱圖五所示)係為於該鑑別伺服器鑑別成功後發行鑑別符記之方法流程，而鑑別符記安全讀取方法(請參閱圖六所示)係為應用網路程式伺服器讀取鑑別符記以作為判斷允許使用者能否登入依據之方法流程；每次重新進行單一登入作業，均需至鑑別伺服器執行鑑別符記安全發行方法一次，且只要鑑別符記安全發行方法已執行完畢，後續連接至應用網路程式伺服器時僅需執行鑑別符記安全讀取方法。

請參閱圖五所示為本發明一種防止鑑別符記被盜用之方法之鑑別符記安全發行方法之流程圖，包括：

步驟一：鑑別伺服器將鑑別無誤後所產生之鑑別符記傳送至發行模組(501)；

步驟二：發行模組接收鑑別符記後，再向用戶端安控模組提出鑑別符記保存請求(502)；

步驟三：用戶端安控模組接收鑑別符記保存請求後，再向保存裝置提出鑑別符記保存請求(503)；

步驟四：保存裝置依步驟一至步驟三辨識操作使用者是否

合法(504)；

步驟五：若為合法操作使用者，則保存裝置保存鑑別符記(505)，並結束流程。

請參閱圖六所示為本發明一種防止鑑別符記被盜用之方法之鑑別符記安全讀取方法之流程圖，包括：

步驟一：應用網路程式伺服器向讀取模組提出鑑別符記讀取請求(601)；

步驟二：鑑別符記安全讀取模組接收鑑別符記讀取請求後，再向用戶端安控模組提出鑑別符記讀取請求(602)；

步驟三：用戶端安控模組接收鑑別符記讀取請求後，再向保存裝置提出鑑別符記讀取請求(603)；

步驟四：保存裝置依步驟一至步驟三辨識操作使用者是否合法(604)；

步驟五：若為合法操作使用者，則保存裝置讀取鑑別符記並回傳至用戶端安控模組(605)；

步驟六：再由用戶端安控模組回傳鑑別符記至讀取模組(606)；

步驟七：最後由讀取模組回傳鑑別符記至應用網路程式伺服器(607)，並結束流程。

又，為防止該鑑別符記於發行模組向該用戶端安控模組提出鑑別符記保存請求之傳送過程，以及已經傳送至該用戶端安控模組但尚未保存入保存裝置前之保存過程(步驟二)，被攻擊者於該用戶端從中擷取之機會，在該實施例中，鑑別符記將以密文資料形式於發行過程中傳送，請參閱圖七所示為本發明一種防止鑑別符記被盜用之方法之鑑別符記將以密文資料形式發行之方法流程圖，包括：

步驟一：發行模組接收鑑別符記後，先向用戶端安控模組提出公開金鑰讀取請求(701)；

步驟二：用戶端安控模組於接收公開金鑰讀取請求後，再向保存裝置提出公開金鑰讀取請求(702)；

步驟三：保存裝置接收公開金鑰讀取請求後，讀取公開金鑰並回傳至用戶端安控模組(703)；

步驟四：用戶端安控模組回傳公開金鑰至發行模組(704)；

步驟五：而發行模組接收公開金鑰後，使用公開金鑰對鑑別符記進行加密產生第一鑑別符記密文(705) ；

步驟六：發行模組以第一鑑別符記密文提出鑑別符記保存請求(706)，並結束流程。

為防止該鑑別符記於該用戶端安控模組回傳至讀取模組之傳送過程，及已經於該用戶端安控模組從該保存裝置讀取出但尚未開始回傳之讀取過程中被擷取與重新傳送(步驟六)，在該實施例中，鑑別符記將由讀取模組產生之亂數金鑰加密後，以密文資料形式於回傳過程中傳送，請參閱圖八所示為本發明一種防止鑑別符記被盜用之方法之以密文資料形式於回傳過程之流程圖，包括：

步驟一：用戶端安控模組接收到鑑別符記(第一鑑別符記密文)後，再向保存裝置提出公開金鑰讀取請求(801)；

步驟二：保存裝置接收公開金鑰讀取請求後，讀取公開金鑰並回傳至用戶端安控模組(802)；

步驟三：用戶端安控模組接收公開金鑰後，再向讀取模組傳送一夾帶公開金鑰之亂數金鑰產生請求(803)；

步驟四：而讀取模組接收亂數金鑰產生請求後，隨機產生一至少 64 位元亂數金鑰(804)；

步驟五：讀取模組利用公開金鑰對亂數金鑰加密產生亂數金鑰密文，並回傳至用戶端安控模組(805)；

步驟六：用戶端安控模組以第一鑑別符記密文及亂數金鑰密文向保存裝置提出第二鑑別符記密文產出請求(806)；

步驟七：保存裝置接收第二鑑別符記密文產出請求後，使用私密金鑰解密亂數金鑰密文並得出亂數金鑰明文(807)；

步驟八：保存裝置使用私密金鑰對為第一鑑別符記密文解密，並於得出鑑別符記明文後，再利用步驟七取得之亂數金鑰對鑑別符記加密產生第二鑑別符記密文(808)；

步驟九：保存裝置回應第二鑑別符記密文(809)；

步驟十：用戶端安控模組以第二鑑別符記密文回傳至讀取模組(810)；

步驟十一：讀取模組利用步驟四產生之亂數金鑰對第二鑑別符記密文解密並得出鑑別符記明文(811)，並結束流程。

現在請參照圖九 A 所示為本發明一種防止鑑別符記被盜用之方法被盜用之方法作業循序圖，包括：

步驟一：使用者於鑑別伺服器輸入身分鑑別資訊(901)；

步驟二：該鑑別伺服器鑑別身分鑑別資訊(902)；

步驟三：並於該鑑別伺服器成功鑑別時，產生鑑別符記，並傳送至發行模組，進行鑑別符記後續發行(903)；

步驟四：發行模組 接收鑑別符記後，利用向保存裝置讀取之公開金鑰進行鑑別符記加密並產生第一鑑別符記密文(904)；

步驟五：發行模組向用戶端安控模組發行第一鑑別符記密文(905)；

步驟六：用戶端安控模組向保存裝置要求保存第一鑑別符記密文(906)；

步驟七：保存裝置向隨身物件要求讀取待辨識識別資料(907)；

步驟八：當隨身物件存在保存裝置之無線射頻訊號有效範圍內時，回傳待辨識識別資料(908)；

步驟九：保存裝置辨識待辨識識別資料是否符合與身分識

別資料(909)；

步驟十：當保存裝置辨識待辨識識別資料符合與身分識別資料時，允許保存第一鑑別符記密文(910)；

步驟十一：保存裝置開始回應保存鑑別符記成功訊息(911)；

步驟十二：該鑑別伺服器將使用者導向存取受保護資源(912)；

現在請參照圖九 B 作業循序圖表示依照本發明一較佳具體實施例完全功能實施之應用網路程式伺服器讀取鑑別符記之資料處理程序，包括：

步驟十三：使用者要求存取受保護資源之應用網路程式伺服器(913)；

步驟十四：應用網路程式伺服器透過讀取模組要求讀取第一鑑別符記密文(914)；

步驟十五：讀取模組再透過用戶端安控模組要求讀取第一鑑別符記密文(915)；

步驟十六：用戶端安控模組向保存裝置要求讀取第一鑑別符記密文(916)；

步驟十七：保存裝置向隨身物件要求讀取待辨識識別資料(917)；

步驟十八：當隨身物件存在保存裝置之無線射頻訊號有效範圍內時，回傳待辨識識別資料(918)；

步驟十九：保存裝置辨識待辨識識別資料是否符合與身分識別資料(919)；

步驟二十：保存裝置辨識待辨識識別資料符合與身分識別資料時，允許讀取第一鑑別符記密文(920)；

步驟二十一：保存裝置回應第一鑑別符記密文至用戶端安控模組(921)；

步驟二十二：用戶端安控模組利用向保存裝置讀取之公開金鑰進行鑑別符記解密，再利用向讀取模組要求之亂數金鑰進行鑑別符記加密並產生第二鑑別符記密文(922)；

步驟二十三：用戶端安控模組回應第二鑑別符記密文至讀取模組(923)；

步驟二十四：讀取模組利用於步驟二十二產生之亂數金鑰進行鑑別符記解密，並還原得出鑑別符記(924)；

步驟二十五：讀取模組回應鑑別符記至應用網路程式伺服器(925)；

步驟二十六：允許使用者存取應用網路程式伺服器(926)，並結束流程。

【特點及功效】

本發明所提供之鑑別符記防止盜用方法及其系統，與其他習用技術相互比較時，更具備下列優點：

1.本發明可提高鑑別符記安全性，因單一登入機制中完全信任鑑別符記作為鑑別依據，不必要求使用者再次進行鑑別作業即允許存取網站，但於先前技藝中攻擊者仍得以利用鑑別符記生命時限到期前之時間差盜用鑑別符記存取受保護之應用程式網站。是故，本發明於先前技藝鑑別符記保存與鑑別符記讀取之保護技術程序上增加辨識操作使用者步驟，可於攻擊者進行盜用之時立即辨識操作使用者是否原使用者，這使得鑑別符記無法被非法改寫與讀取，進而防止鑑別符記於儲存及傳送過程中被非法人士以竊取、竄改、重新傳送等方式盜用。

2.本發明可同時保持使用者之便利性，因於防止鑑別符記被盜用之先前技藝中，使用者需要不斷延長單一登入之有效期間，並且於臨時離開用戶端時，每次都需要完全登出所有網站或者以一密碼保護程式鎖定用戶端。透過本發明所揭露

之技術，只要使用者攜帶一隨身物件即可持續保持單一登入狀態，並於離開用戶端後，立即自動對鑑別符記進行保護以防止任何人使用任何方式盜用，所以可於無需額外的操作程序下，降低為傳統鑑別符記保護機制所需之時間成本及人力成本。

上列詳細說明係針對本發明之一可行實施例之具體說明，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，本案不但在技術思想上確屬創新，並能較習用物品增進上述多項功效，應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A為習用技術之架構圖；

圖一B為習用技術之第一流程圖；

圖一C為習用技術之第二流程圖；

圖二為本發明一種防止鑑別符記被盜用之系統之架構圖；

圖三為本發明一種防止鑑別符記被盜用之系統之保存裝置示意圖；

圖四為本發明一種防止鑑別符記被盜用之方法之流程圖；

圖五為本發明一種防止鑑別符記被盜用之方法之鑑別符記安全發行方法之流程圖；

圖六為本發明一種防止鑑別符記被盜用之方法之鑑別符記安全讀取方法之流程圖；

圖七為本發明一種防止鑑別符記被盜用之方法之鑑別符記將以密文資料形式發行之方法流程圖；

圖八為本發明一種防止鑑別符記被盜用之方法之以密文資料形式於回傳過程之流程圖；

圖九 A 為本發明一種防止鑑別符記被盜用之方法被盜用之方法作業循序圖；以及

圖九 B 為本發明一種防止鑑別符記被盜用之方法之應用網路程式伺服器讀取鑑別符記之資料處理程序圖。

【主要元件符號說明】

210 保存裝置

211 介面模組

212 加解密模組

213 辨識模組

214 無線射頻讀取器

215 處理器

216 記憶模組

217 身分識別資料

218 鑑別符記

219 公開金鑰

220 私密金鑰

230 隨身物件

231 射頻識別元件

232 待辨識識別資料

240 鑑別伺服器

241 發行模組

250 應用網路程式伺服器

251 讀取模組

260 用戶端

261 用戶端安控模組

七、申請專利範圍：

1. 一種防止鑑別符記被盜用之系統，包括：

一用戶端；以及

一保存模組，與該用戶端通訊連接，該保存模組自該用戶端接收一鑑別符記保存請求或一鑑別符記讀取請求下，即於該保存模組即對外發送一無線射頻訊號，以觸發位於該保存模組之有效發送範圍內使用者所穿戴之一隨身物件回應一待辨識識別資料，該保存模組更判斷該待辨識識別資料是否符合一身分識別資料，以判斷是否具保存或讀取一鑑別符記之資格。

2. 如請求項1所述之系統，更包括：

一發行模組，係安裝於鑑別伺服器，並提供該鑑別符記之加密與發行；

一讀取模組，係安裝於應用網路程式伺服器，並提供該鑑別符記之解密與讀取；

一用戶端安控模組，係安裝於該用戶端，以提供該保存裝置連接該用戶端，使得該用戶端安控模組可對保存裝置做安控存取。

3. 如請求項1或2所述之系統，其中該保存裝置進一步包括：

一介面模組，係與該用戶端連結之介面，並使得該發行模組與該讀取模組可透過該用戶端安控模組存取保存裝置中之鑑別符記；

一加解密模組，係提供加密計算與解密計算；

一辨識模組，係提供辨識待辨識識別資料與身分識別資料是否符合之計算；

一處理器，係為接收與執行各模組所傳遞程式訊號；以及

一記憶模組，係為記憶與儲存身分識別資料、鑑別符記、

公開金鑰及私密金鑰。

4. 如請求項1所述之系統，其中該隨身物件更設有一射頻識別元件，該射頻識別元件係於有效發送範圍內感應到該保存裝置所發射之無線射頻訊號下，以回應該待辨識識別資料。

5. 如請求項1所述之系統，其中該隨身物件之該待辨識識別資料與該保存裝置之該身分識別資料為具唯一性之無線射頻識別碼，當該待辨識識別資料與該身分識別資料不相符時，則該保存裝置無法保存與讀取該鑑別符記。

6. 如請求項1所述之系統，其中該隨身物件係可為項鍊、手鍊、戒指、鑰匙圈或識別證。

7. 如請求項3所述之系統，其中該保存裝置的介面模組係為PCI、PCI Express、PCMCIA或USB。

8. 一種防止鑑別符記被盜用之方法，包含下列步驟：

a.一保存裝置自一用戶端接收一鑑別符記保存請求或鑑別符記讀取請求後，向外發送無線射頻訊號；

b.觸發位於該保存裝置有效發送範圍內使用者所穿戴之一隨物物件回應一待辨識識別資料；

c.該保存裝置接收到該待辨識識別資料時，則辨識待辨識識別資料是否符合一身分識別資料；以及

d.判斷該待辨識識別資料是否符合該身分識別資料，以決定該保存裝置是否具保存或讀取該鑑別符記之資格。

9. 如請求項8所述之方法，進一步包括下列步驟：

e.鑑別伺服器將鑑別無誤後所產生之該鑑別符記傳送至發行模組；

f.該發行模組接收該鑑別符記後，再向該用戶端之用戶端安控模組提出該鑑別符記保存請求；

g.該用戶端安控模組接收該鑑別符記保存請求後，再向保

存裝置提出該鑑別符記保存請求；

h.該保存裝置辨識操作使用者是否合法；以及

i.若為合法操作使用者，則該保存裝置保存該鑑別符記。

10.如請求項8所述之方法，進一步包括下列步驟：

j.應用網路程式伺服器向讀取模組提出該鑑別符記讀取請求；

k.該讀取模組接收該鑑別符記讀取請求後，再向該用戶端安控模組提出該鑑別符記讀取請求；

l.該用戶端安控模組接收該鑑別符記讀取請求後，再向該保存裝置提出該鑑別符記讀取請求；

m.該保存裝置辨識操作使用者是否合法；

n.若為合法操作使用者，則該保存裝置讀取該鑑別符記並回傳至該用戶端安控模組；

o.該用戶端安控模組回傳該鑑別符記至該讀取模組；以及

p.該讀取模組回傳該鑑別符記至該應用網路程式伺服器。

11.如請求項9所述之方法，其中步驟f進一步包括以下步驟：

a.該發行模組接收該鑑別符記後，先向該用戶端安控模組提出公開金鑰讀取請求；

b.該用戶端安控模組於接收該公開金鑰讀取請求後，再向該保存裝置提出該公開金鑰讀取請求；

c.該保存裝置接收該公開金鑰讀取請求後，讀取該公開金鑰並回傳至該用戶端安控模組；

d.該用戶端安控模組回傳公開金鑰至發行模組；

e.該發行模組接收該公開金鑰後，使用該公開金鑰對該鑑別符記進行加密產生第一鑑別符記密文；以及

f.該發行模組以第一鑑別符記密文提出該鑑別符記保存請求。

12.如請求項10所述之方法，其中步驟o進一步包括以下步

驟：

a.該用戶端安控模組接收到該鑑別符記後，再向該保存裝置提出該公開金鑰讀取請求；

b.該保存裝置接收該公開金鑰讀取請求後，讀取該公開金鑰並回傳至該用戶端安控模組；

c. 該用戶端安控模組接收該公開金鑰後，再向該讀取模組傳送一夾帶該公開金鑰之亂數金鑰產生請求；

d. 該讀取模組接收該亂數金鑰產生請求後，隨機產生一至少64位元亂數金鑰；

e. 該讀取模組利用該公開金鑰對該亂數金鑰加密產生亂數金鑰密文，並回傳至該用戶端安控模組；

f. 該用戶端安控模組以第一鑑別符記密文及該亂數金鑰密文傳送至該保存裝置提出第二鑑別符記密文產出請求；

g. 該保存裝置接收該第二鑑別符記密文產出請求後，使用私密金鑰解密亂數金鑰密文並得出亂數金鑰明文；

h. 該保存裝置使用該私密金鑰對為該第一鑑別符記密文解密，並於得出鑑別符記明文後，再利用步驟g取得之該亂數金鑰對該鑑別符記加密產生該第二鑑別符記密文；

i. 該保存裝置回應該第二鑑別符記密文；

j. 該用戶端安控模組以該第二鑑別符記密文回傳至該讀取模組；以及

k. 該讀取模組利用步驟 d 產生之該亂數金鑰對該第二鑑別符記密文解密並得出該鑑別符記明文。

13.如請求項8項所述之方法，其中該保存裝置進一步包括利用一介面模組與該用戶端連結之介面，並使得該發行模組與該讀取模組可透過該用戶端安控模組存取該保存裝置中之該鑑別符記。

14.如請求項8所述之方法，其中該保存裝置進一步包括利用

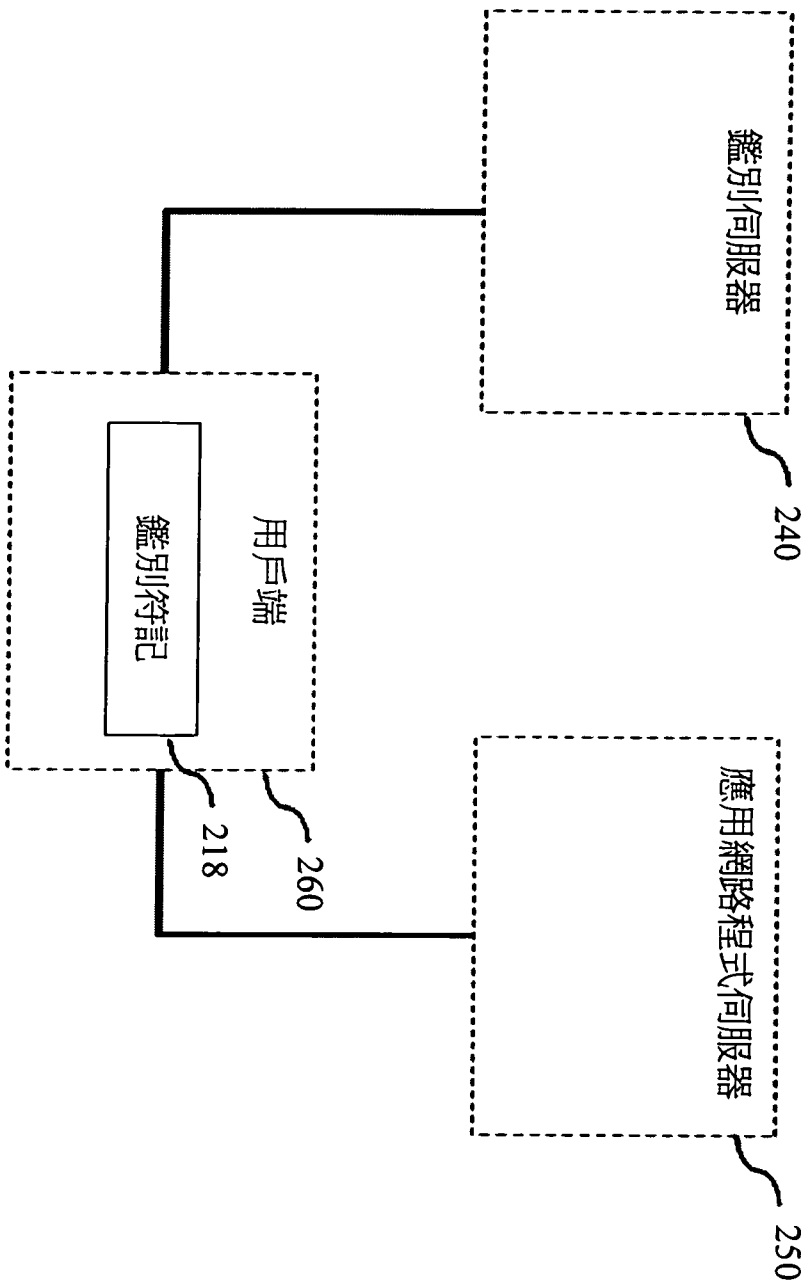
一加解密模組進行加密計算與解密計算。

15. 如請求項8所述之方法，其中該保存裝置進一步包括利用一辨識模組進行該辨識待辨識識別資料是否符合身分識別資料。

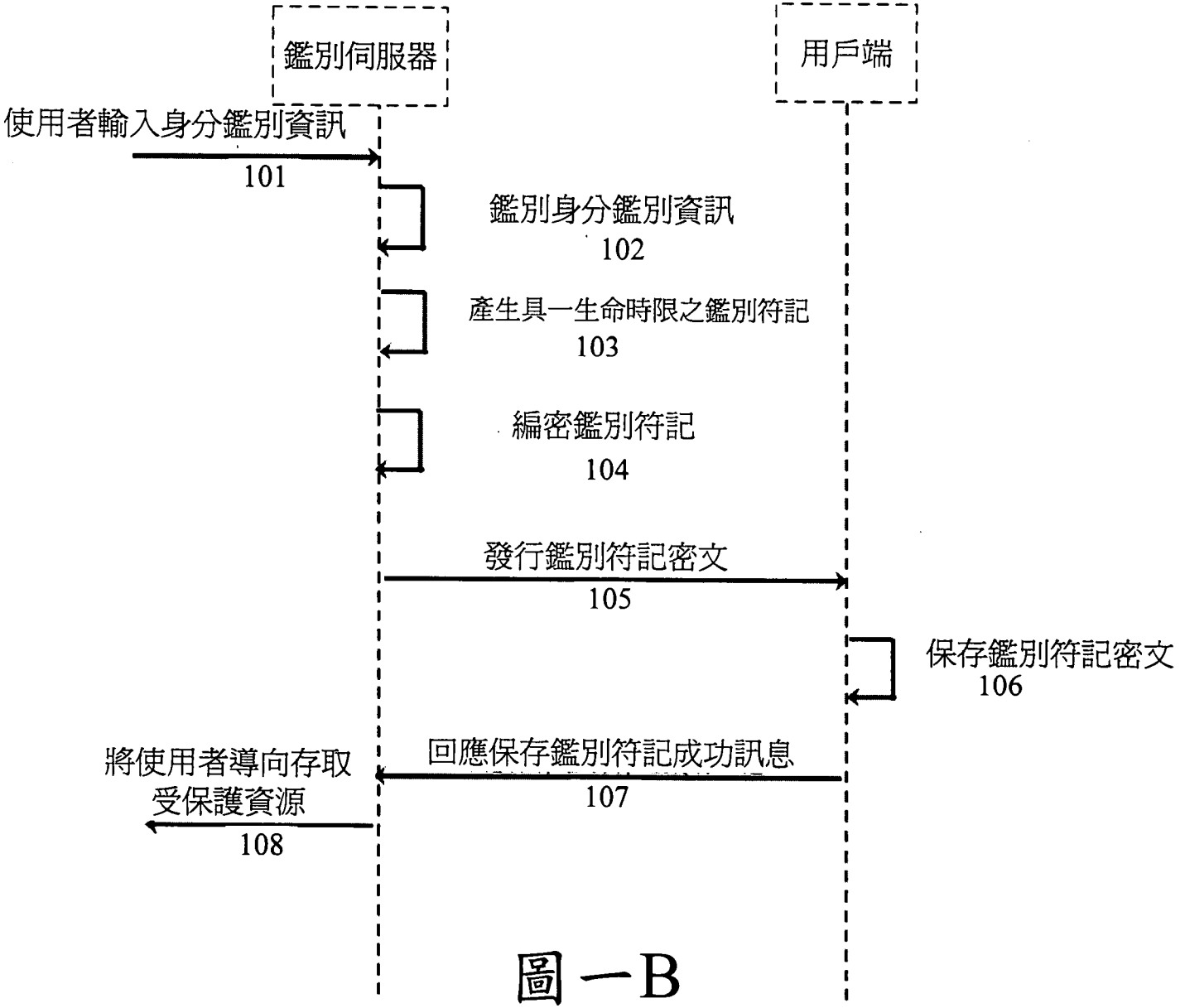
16. 如請求項8所述之方法，其中該保存裝置進一步包括利用一處理器接收與執行各模組所傳遞程式訊號。

17. 如請求項8所述之方法，其中該保存裝置進一步包括利用一記憶模組記憶身分識別資料、鑑別符記、公開金鑰及私密金鑰。

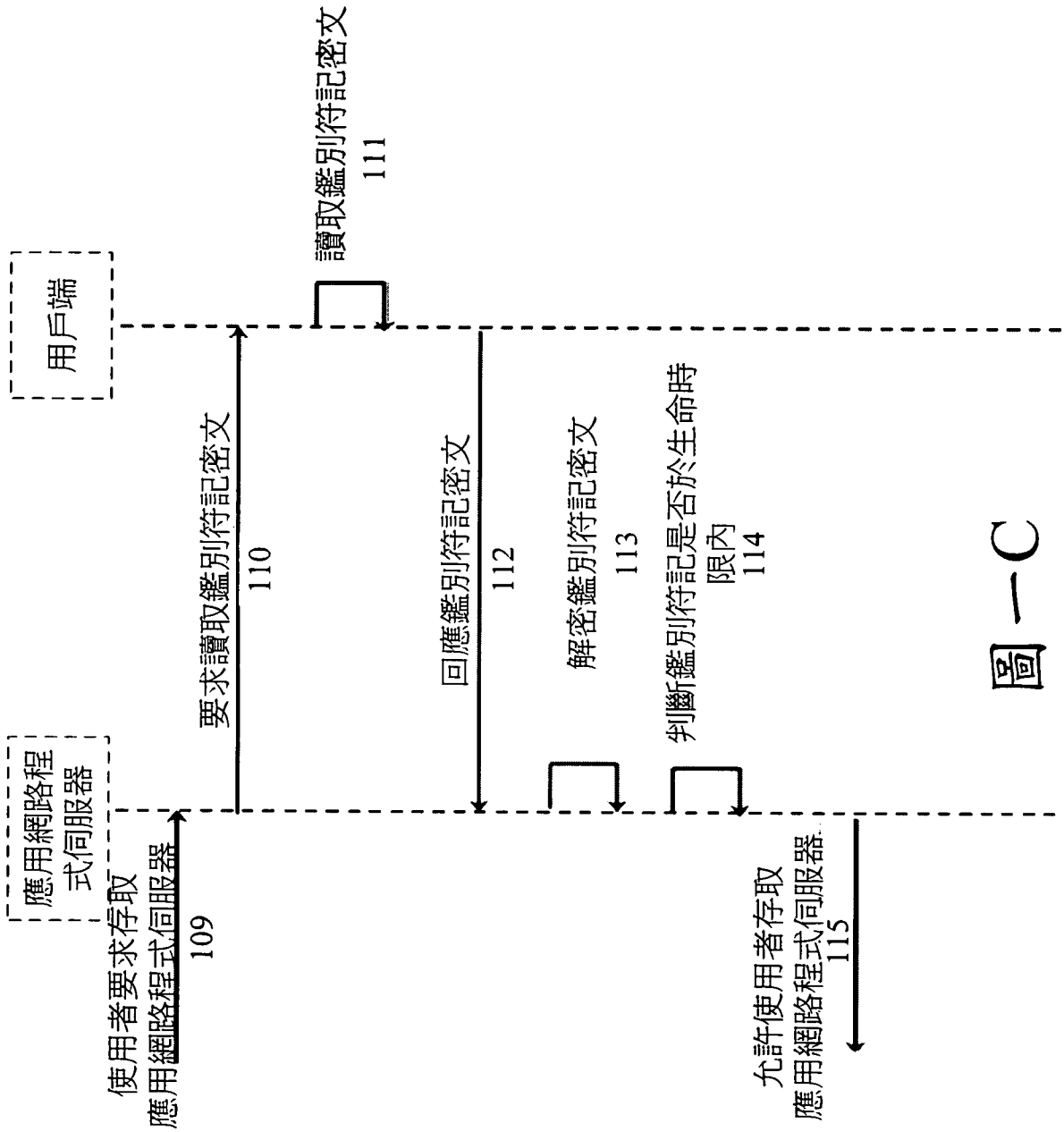
八、圖式：



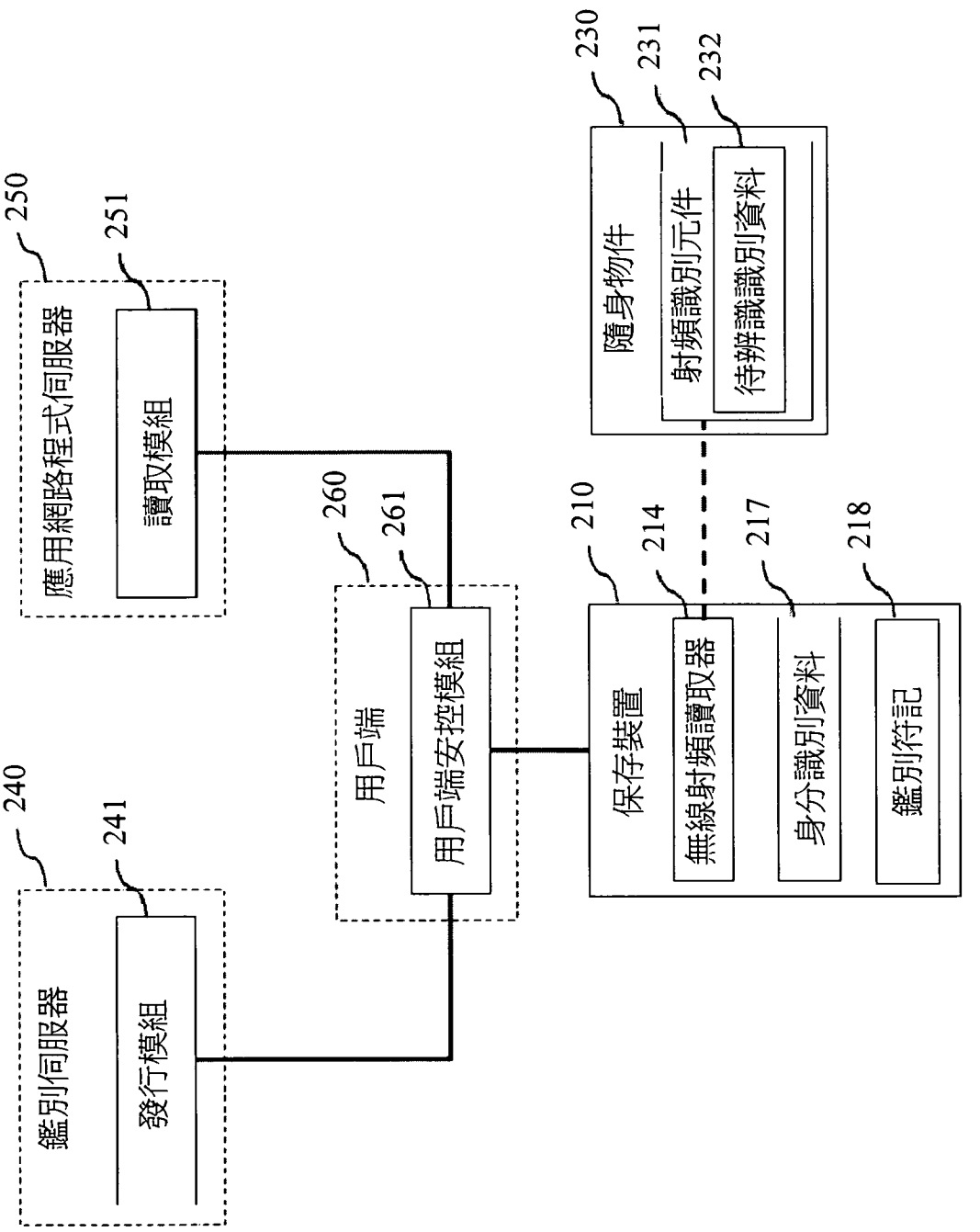
圖一A


鑑別伺服器
用戶端
使用者輸入身分鑑別資訊
101
鑑別身分鑑別資訊
102
產生具一生命時限之鑑別符記
103
編密鑑別符記
104
發行鑑別符記密文
105
保存鑑別符記密文
106
回應保存鑑別符記成功訊息
107
將使用者導向存取
受保護資源
108

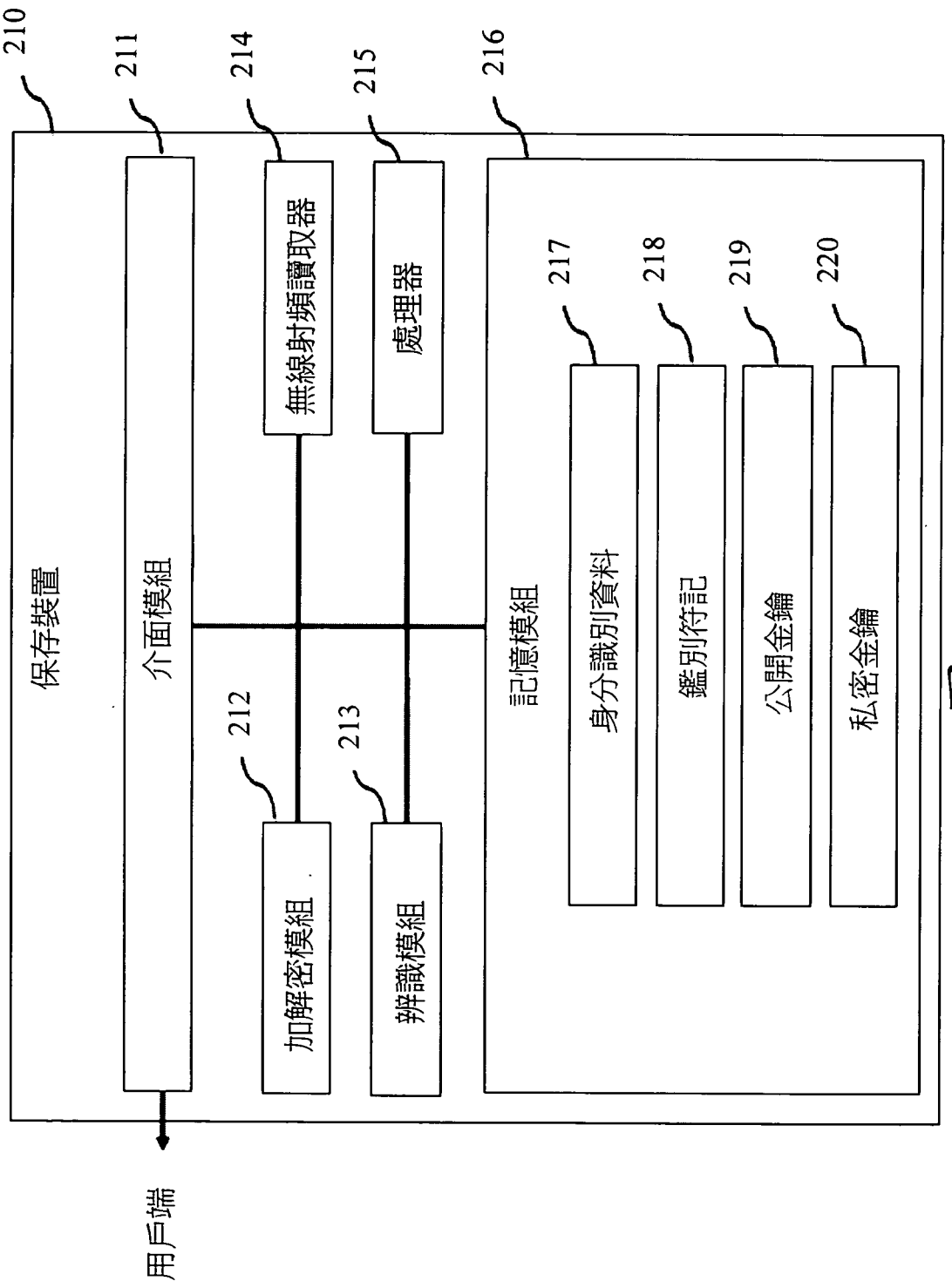
圖一B


用戶端
讀取鑑別符記密文
111
應用網路程式伺服器
要求讀取鑑別符記密文
110
回應鑑別符記密文
112
解密鑑別符記密文
113
判斷鑑別符記是否於生命時限內
114
使用者要求存取應用網路程式伺服器
109
允許使用者存取應用網路程式伺服器
115

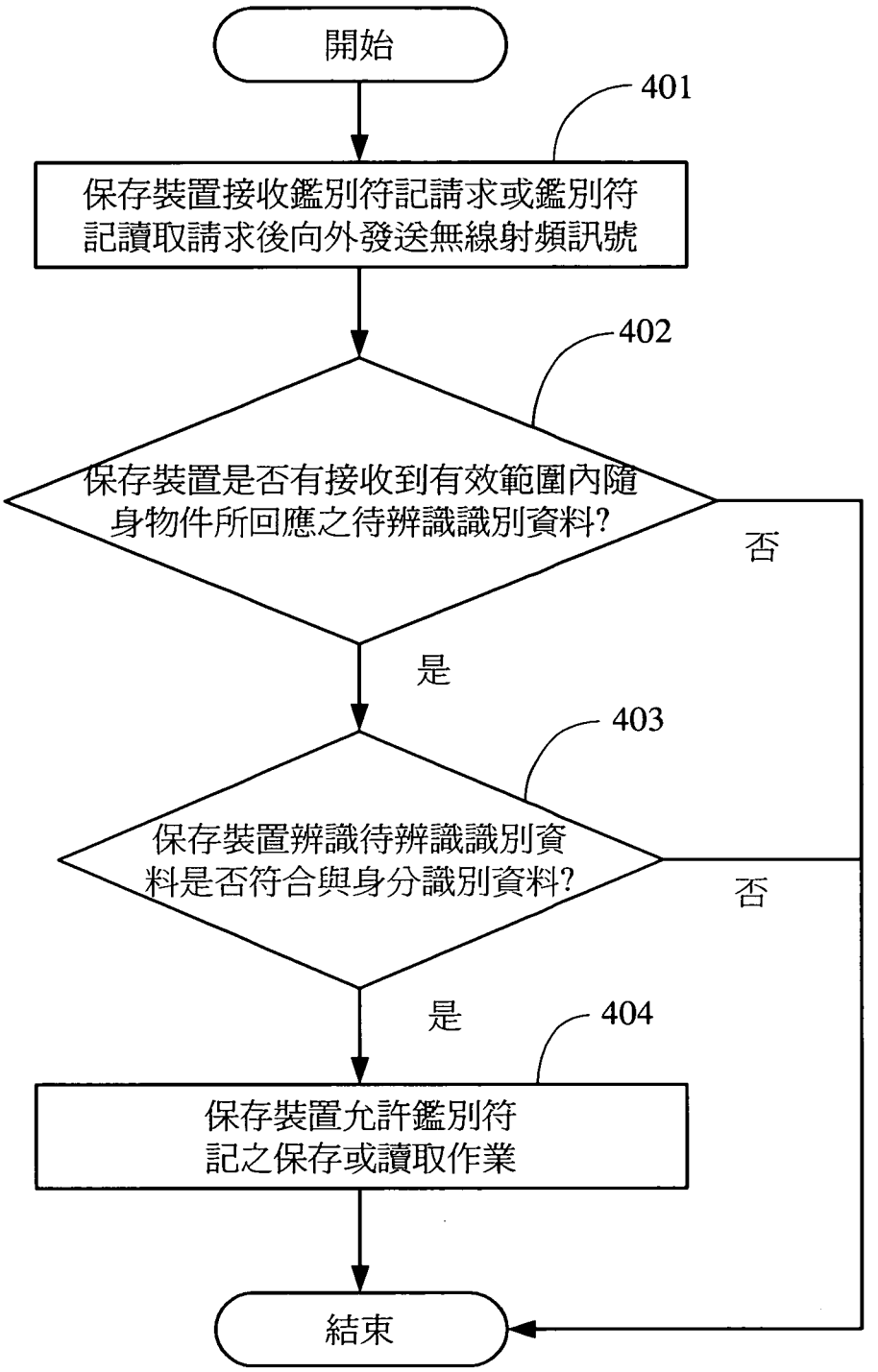
圖一C


鑑別伺服器
240
發行模組
241
應用網路程式伺服器
250
讀取模組
251
用戶端
260
用戶端安控模組
261
保存裝置
210
無線射頻讀取器
214
身分識別資料
217
鑑別符記
218
隨身物件
230
射頻識別元件
231
待辨識識別資料
232

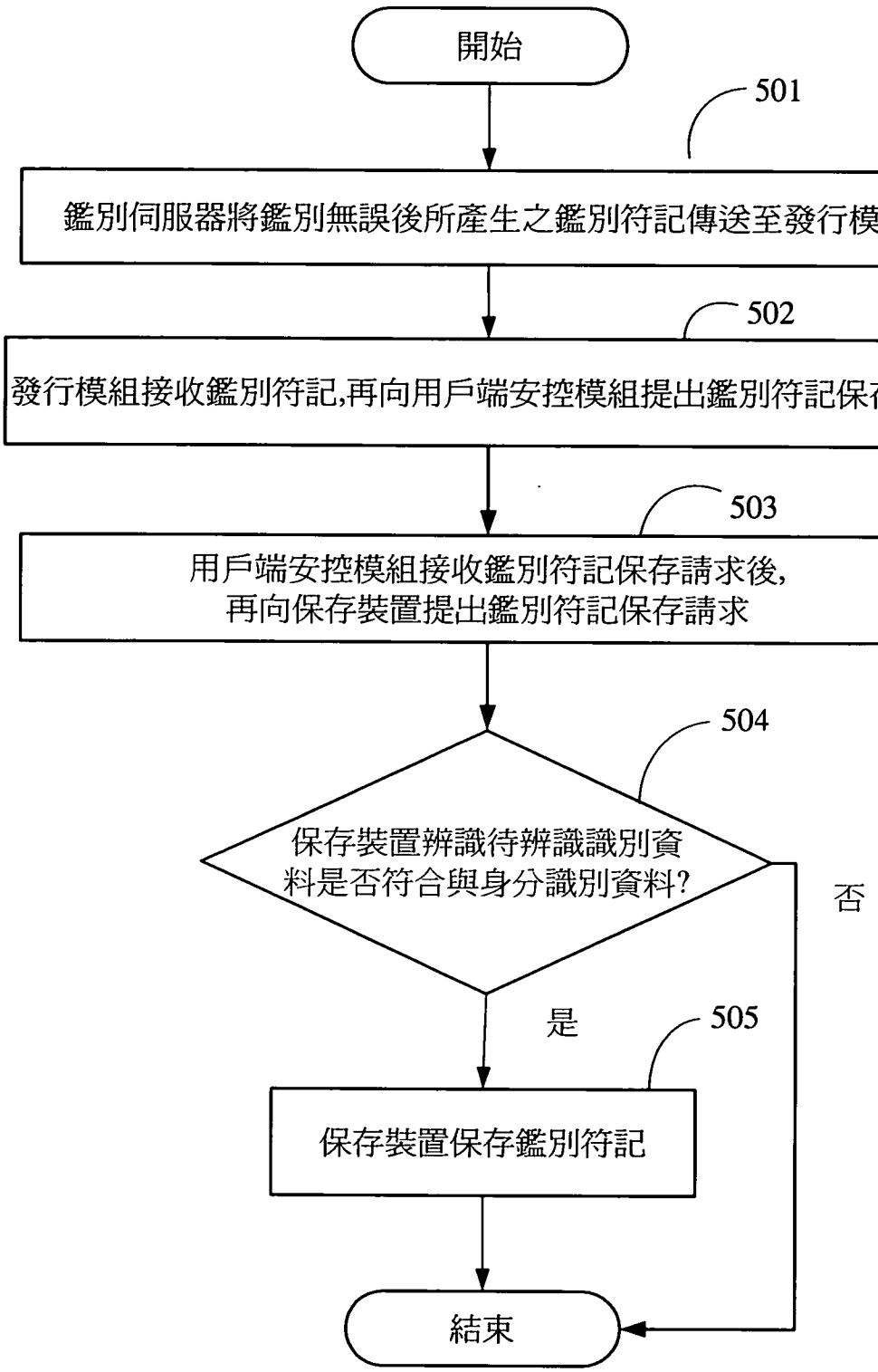
圖二


210
211
214
215
216
保存裝置
介面模組
無線射頻讀取器
處理器
記憶模組
212
213
217
218
219
220
加解密模組
辨識模組
身分識別資料
鑑別符記
公開金鑰
私密金鑰
用戶端

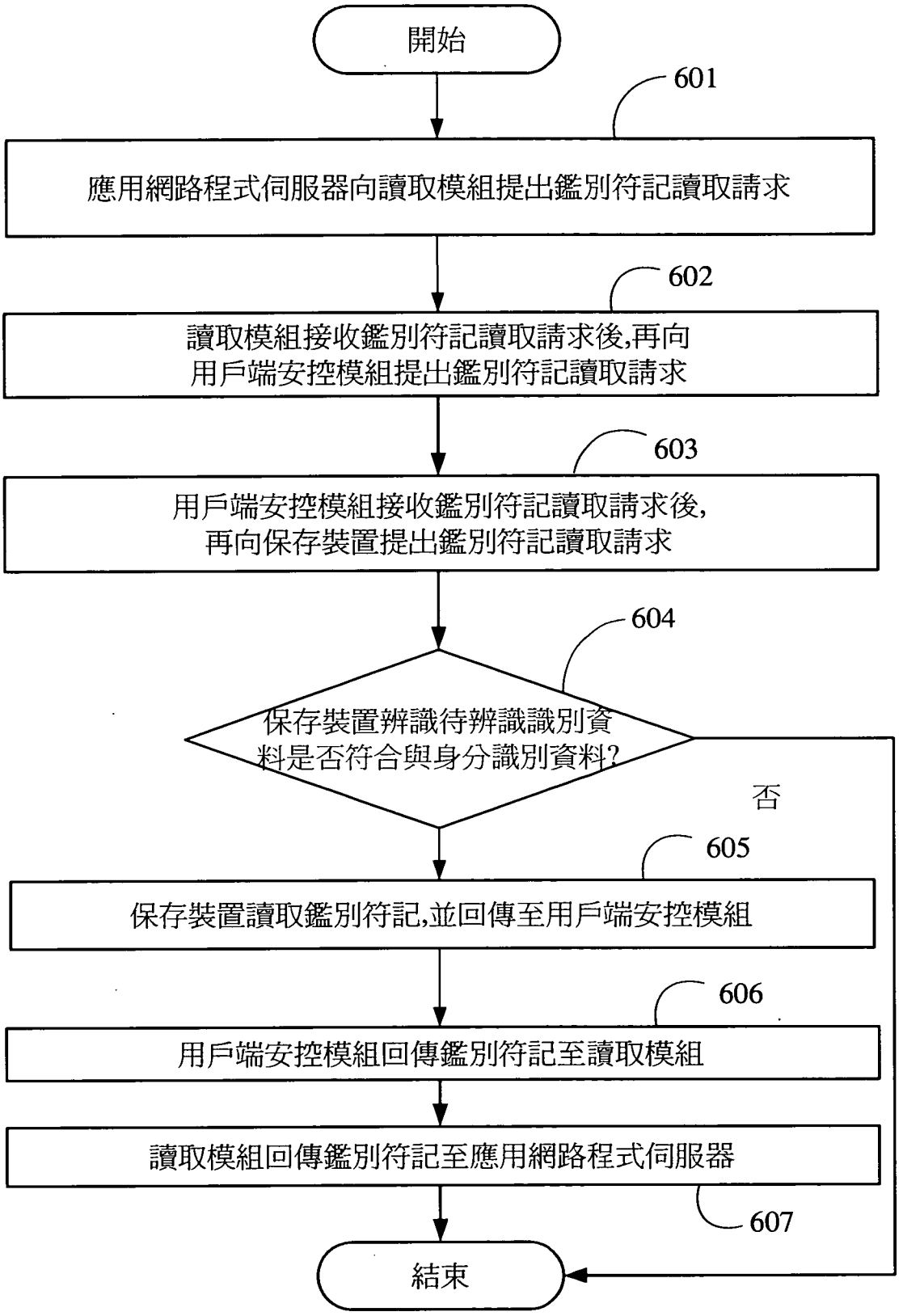
圖三


開始
401
保存裝置接收鑑別符記請求或鑑別符記讀取請求後向外發送無線射頻訊號
402
保存裝置是否有接收到有效範圍內隨身物件所回應之待辨識識別資料?
否
是
403
保存裝置辨識待辨識識別資料是否符合與身分識別資料?
否
是
404
保存裝置允許鑑別符記之保存或讀取作業
結束

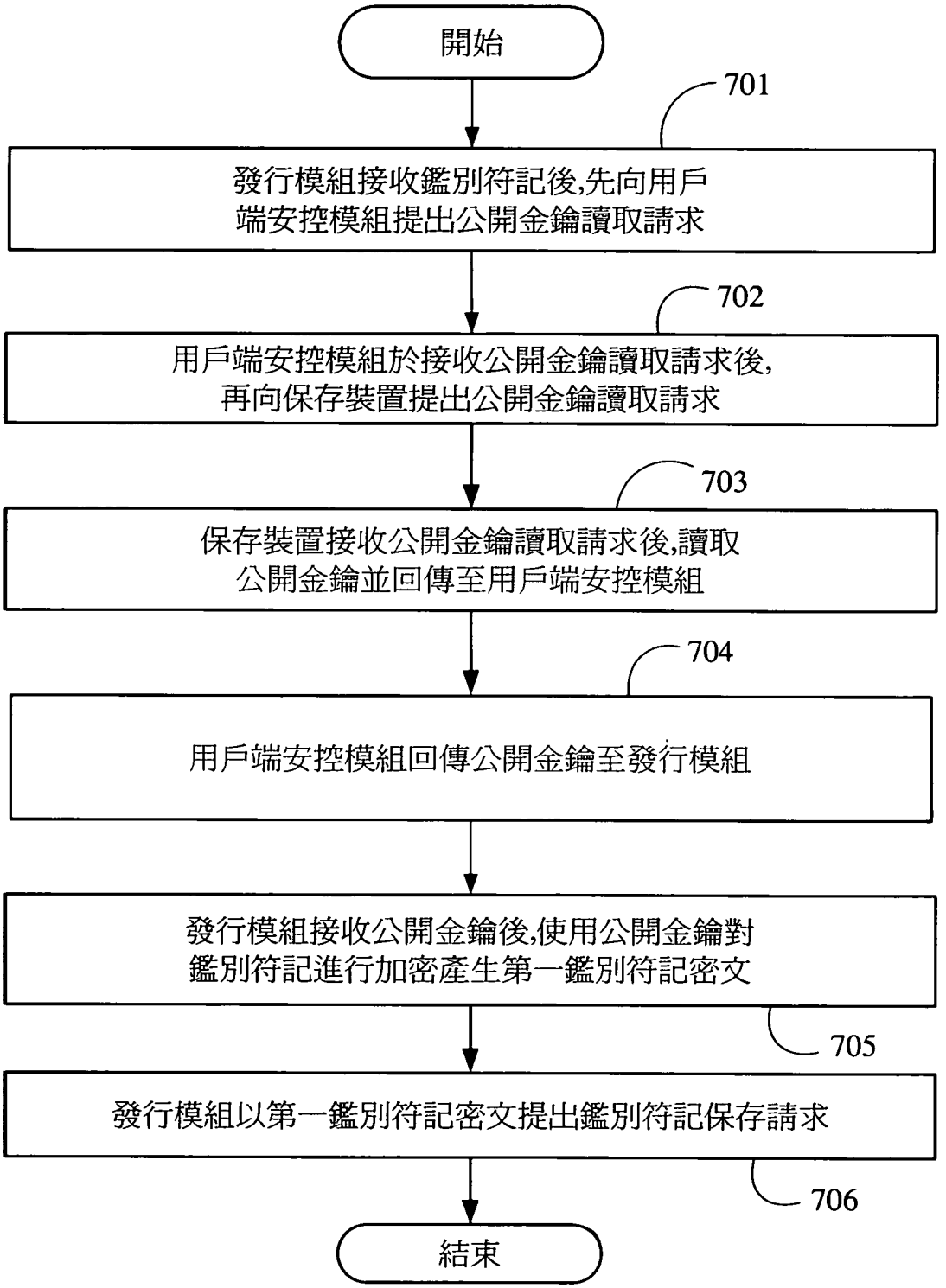
圖四


開始
501
鑑別伺服器將鑑別無誤後所產生之鑑別符記傳送至發行模組
502
發行模組接收鑑別符記,再向用戶端安控模組提出鑑別符記保存請求
503
用戶端安控模組接收鑑別符記保存請求後,
再向保存裝置提出鑑別符記保存請求
504
保存裝置辨識待辨識識別資料是否符合與身分識別資料?
否
是
505
保存裝置保存鑑別符記
結束

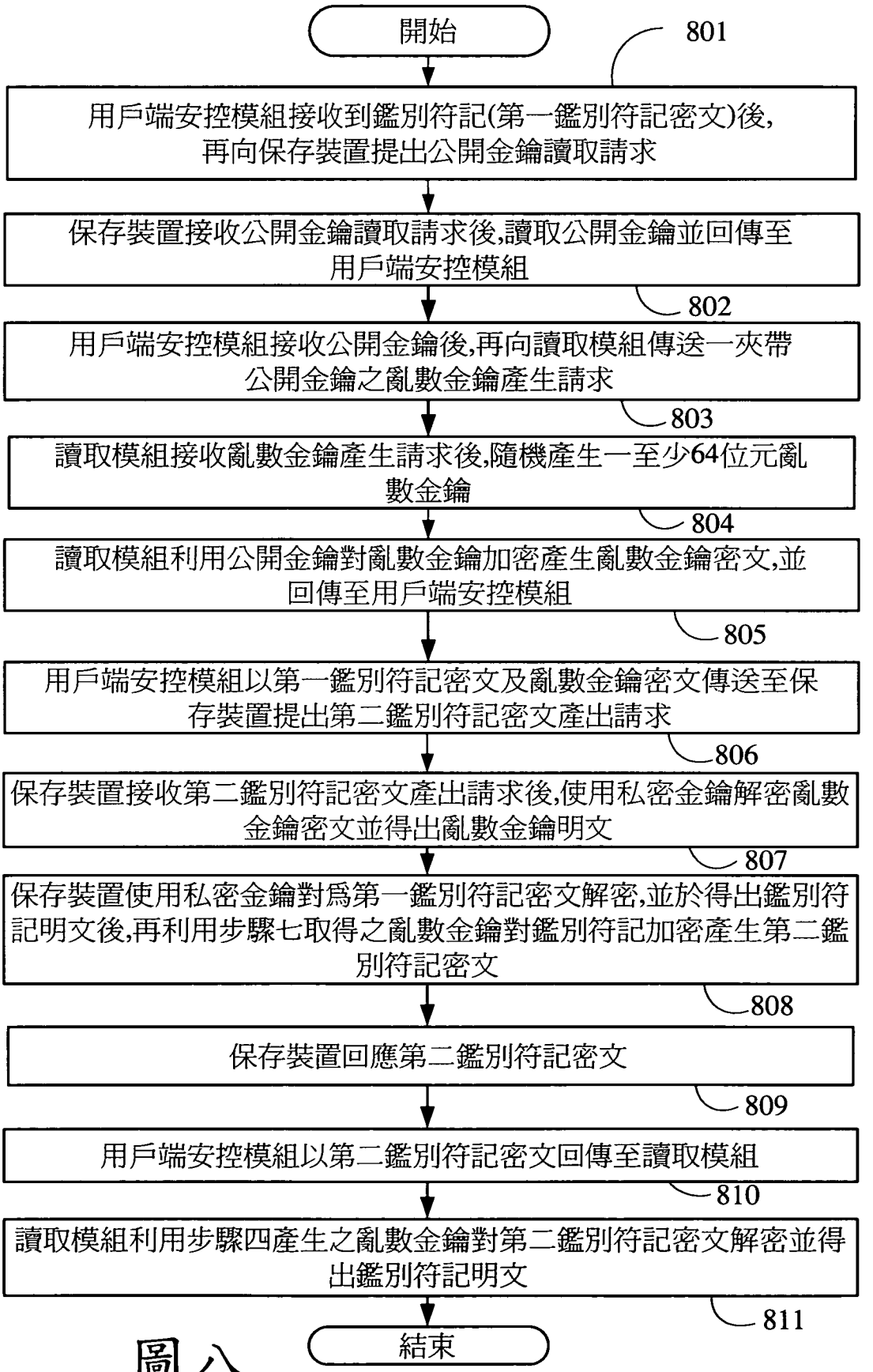
圖五


開始
601
應用網路程式伺服器向讀取模組提出鑑別符記讀取請求
602
讀取模組接收鑑別符記讀取請求後,再向
用戶端安控模組提出鑑別符記讀取請求
603
用戶端安控模組接收鑑別符記讀取請求後,
再向保存裝置提出鑑別符記讀取請求
604
保存裝置辨識待辨識識別資
料是否符合與身分識別資料?
否
605
保存裝置讀取鑑別符記,並回傳至用戶端安控模組
606
用戶端安控模組回傳鑑別符記至讀取模組
讀取模組回傳鑑別符記至應用網路程式伺服器
607
結束

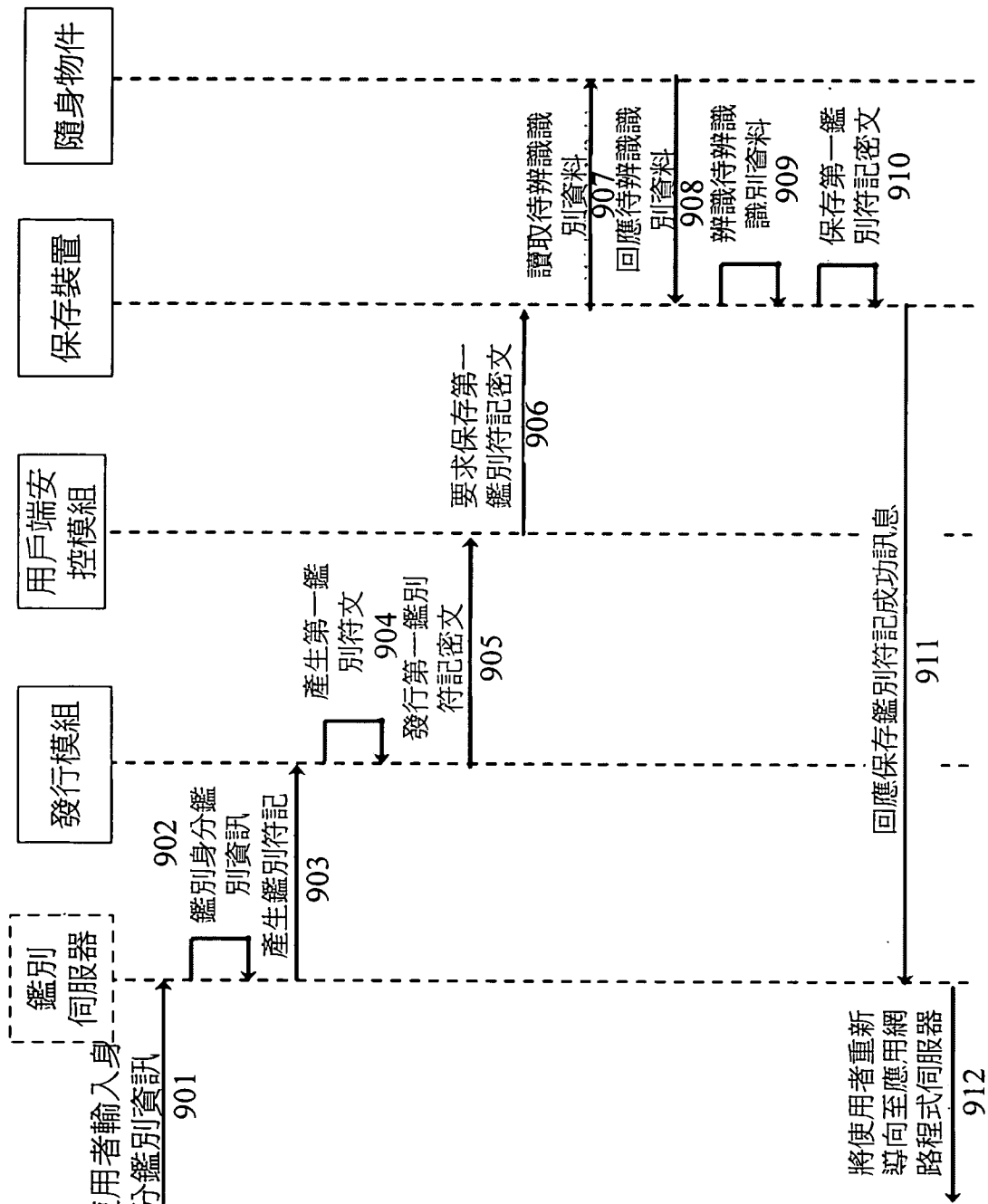
圖六


開始
701
發行模組接收鑑別符記後,先向用戶端安控模組提出公開金鑰讀取請求
702
用戶端安控模組於接收公開金鑰讀取請求後,再向保存裝置提出公開金鑰讀取請求
703
保存裝置接收公開金鑰讀取請求後,讀取公開金鑰並回傳至用戶端安控模組
704
用戶端安控模組回傳公開金鑰至發行模組
發行模組接收公開金鑰後,使用公開金鑰對鑑別符記進行加密產生第一鑑別符記密文
705
發行模組以第一鑑別符記密文提出鑑別符記保存請求
706
結束

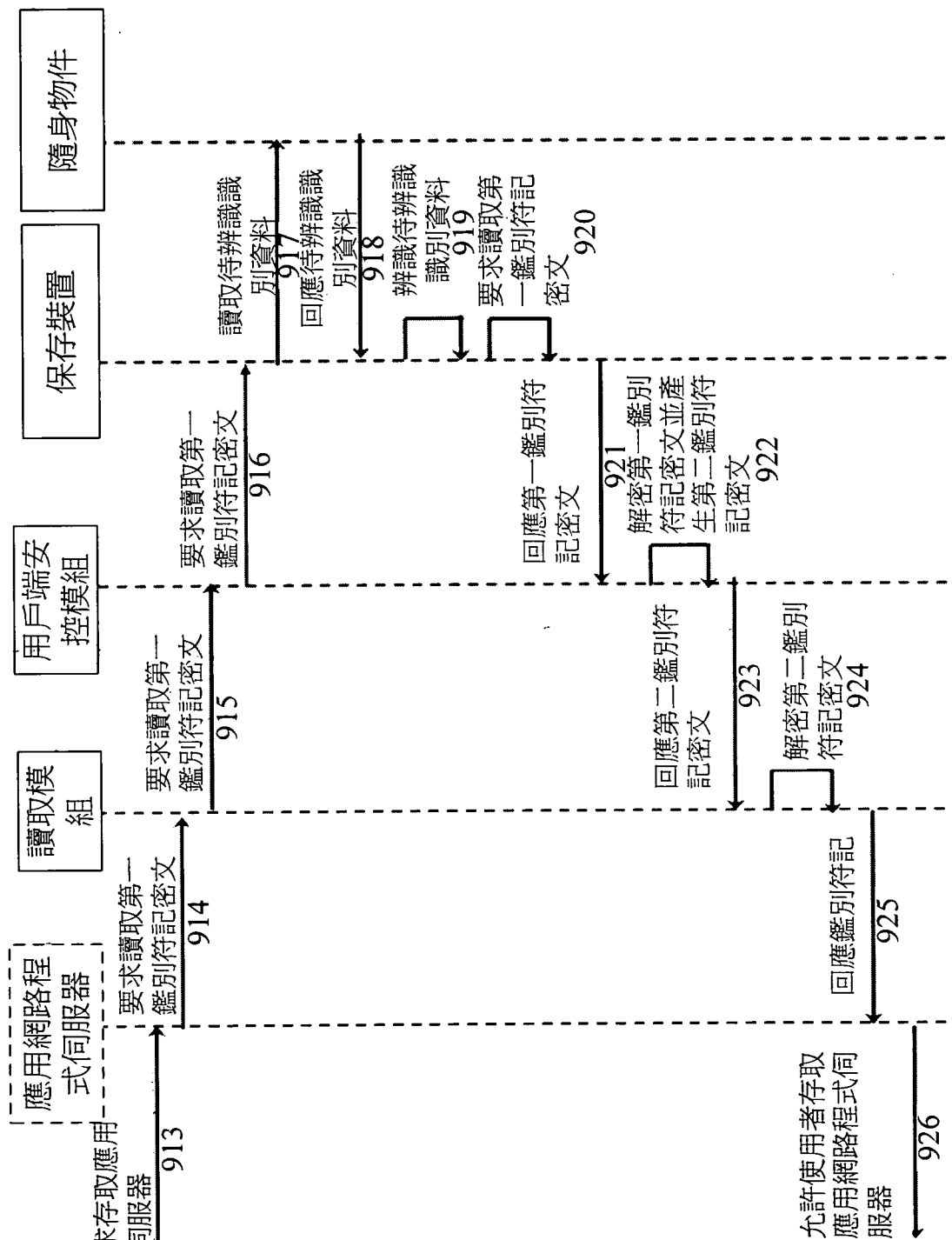
圖七


開始
801
用戶端安控模組接收到鑑別符記(第一鑑別符記密文)後,再向保存裝置提出公開金鑰讀取請求
保存裝置接收公開金鑰讀取請求後,讀取公開金鑰並回傳至用戶端安控模組
802
用戶端安控模組接收公開金鑰後,再向讀取模組傳送一夾帶公開金鑰之亂數金鑰產生請求
803
讀取模組接收亂數金鑰產生請求後,隨機產生一至少64位元亂數金鑰
804
讀取模組利用公開金鑰對亂數金鑰加密產生亂數金鑰密文,並回傳至用戶端安控模組
805
用戶端安控模組以第一鑑別符記密文及亂數金鑰密文傳送至保存裝置提出第二鑑別符記密文產出請求
806
保存裝置接收第二鑑別符記密文產出請求後,使用私密金鑰解密亂數金鑰密文並得出亂數金鑰明文
807
保存裝置使用私密金鑰對爲第一鑑別符記密文解密,並於得出鑑別符記明文後,再利用步驟七取得之亂數金鑰對鑑別符記加密產生第二鑑別符記密文
808
保存裝置回應第二鑑別符記密文
809
用戶端安控模組以第二鑑別符記密文回傳至讀取模組
810
讀取模組利用步驟四產生之亂數金鑰對第二鑑別符記密文解密並得出鑑別符記明文
811
結束

圖八


鑑別伺服器
發行模組
用戶端安控模組
保存裝置
隨身物件
使用者輸入身分鑑別資訊
901
902
鑑別身分鑑別資訊產生鑑別符記
903
產生第一鑑別符文
904
發行第一鑑別符記密文
905
要求保存第一鑑別符記密文
906
讀取待辨識識別資料
907
回應待辨識識別資料
908
辨識待辨識識別資料
909
保存第一鑑別符記密文
910
回應保存鑑別符記成功訊息
911
將使用者重新導向至應用網路程式伺服器
912

圖九A


使用者要求存取應用網路程式伺服器
913
應用網路程式伺服器
讀取模組
用戶端安控模組
保存裝置
隨身物件
要求讀取第一鑑別符記密文
914
要求讀取第一鑑別符記密文
915
要求讀取第一鑑別符記密文
916
讀取待辨識識別資料
917
回應待辨識識別資料
918
辨識待辨識識別資料
919
要求讀取第一鑑別符記密文
920
回應第一鑑別符記密文
921
解密第一鑑別符記密文並產生第二鑑別符記密文
922
回應第二鑑別符記密文
923
解密第二鑑別符記密文
924
回應鑑別符記
925
允許使用者存取應用網路程式伺服器
926

圖九B