(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201245956 A1
(43)公開日： 中華民國 101 (2012) 年 11 月 16 日

(21)申請案號：101105275 (22)申請日： 中華民國 101 (2012) 年 02 月 17 日
(51)Int. Cl.： *G06F12/00 (2006.01)* *H04L9/32 (2006.01)*
H04L9/14 (2006.01)
(30)優先權：2011/05/04 中華民國 100115596
(71)申請人：楊建綱 (中華民國) YANG, CHIEN KANG (TW)
臺北市大安區敦化南路 2 段 67 號 19 樓
(72)發明人：楊建綱 YANG, CHIEN KANG (TW)
(74)代理人：高玉駿；楊祺雄
申請實體審查：有 申請專利範圍項數：15 項 圖式數：8 共 32 頁

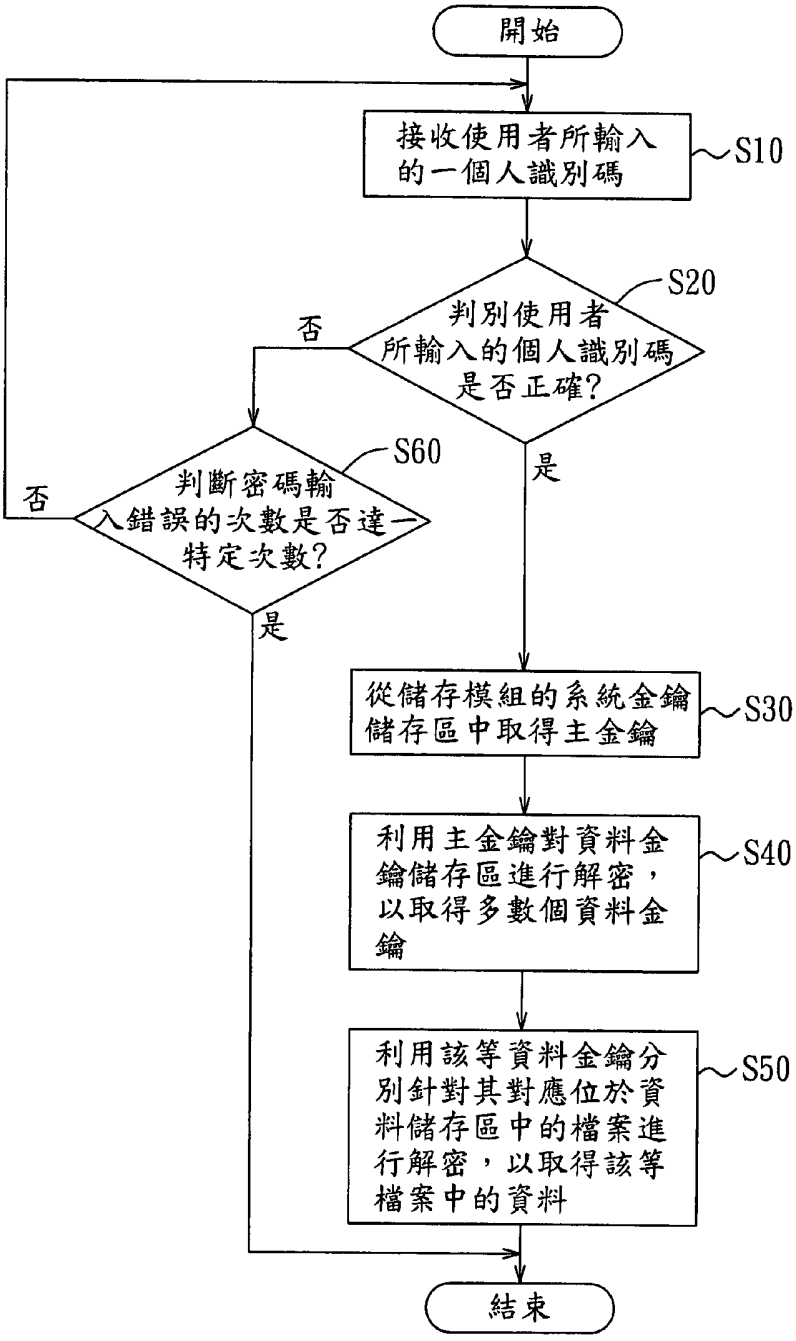
(54)名稱

記憶卡及其讀取、資料加密、金鑰產生及變更方法

(57)摘要

一種記憶卡的讀取方法，係於一控制單元中執行，用以讀取一記憶卡中的資料，該讀取方法首先會接收一個人識別碼，然後判別該個人識別碼是否正確，若是，則從記憶卡中取得一主金鑰，並利用該主金鑰對記憶卡的一資料金鑰儲存區進行解密，以取得多數個分別對應記憶卡的一資料儲存區中多數個檔案的資料金鑰，接著利用該等資料金鑰分別針對其對應的檔案進行解密，以讀取該等檔案中的資料，如此一來，透過主金鑰及資料金鑰的雙重保護，以及，且每個檔案分別利用唯一且不同的資料金鑰加密，使得每個檔案獨立控管，如此將可更加確保資料的安全性。

S10~S60：步驟


開始
接收使用者所輸入的一個人識別碼
S10
判別使用者所輸入的個人識別碼是否正確?
S20
否
是
判斷密碼輸入錯誤的次數是否達一特定次數?
S60
否
是
從儲存模組的系統金鑰儲存區中取得主金鑰
S30
利用主金鑰對資料金鑰儲存區進行解密，以取得多數個資料金鑰
S40
利用該等資料金鑰分別針對其對應位於資料儲存區中的檔案進行解密，以取得該等檔案中的資料
S50
結束

(19)中華民國智慧財產局
(12)發明說明書公開本 (11)公開編號：TW 201245956 A1
(43)公開日： 中華民國 101 (2012) 年 11 月 16 日

(21)申請案號：101105275 (22)申請日： 中華民國 101 (2012) 年 02 月 17 日
(51)Int. Cl.： *G06F12/00 (2006.01)* *H04L9/32 (2006.01)*
H04L9/14 (2006.01)
(30)優先權：2011/05/04 中華民國 100115596
(71)申請人：楊建綱 (中華民國) YANG, CHIEN KANG (TW)
臺北市大安區敦化南路 2 段 67 號 19 樓
(72)發明人：楊建綱 YANG, CHIEN KANG (TW)
(74)代理人：高玉駿；楊祺雄
申請實體審查：有 申請專利範圍項數：15 項 圖式數：8 共 32 頁

(54)名稱

記憶卡及其讀取、資料加密、金鑰產生及變更方法

(57)摘要

一種記憶卡的讀取方法，係於一控制單元中執行，用以讀取一記憶卡中的資料，該讀取方法首先會接收一個人識別碼，然後判別該個人識別碼是否正確，若是，則從記憶卡中取得一主金鑰，並利用該主金鑰對記憶卡的一資料金鑰儲存區進行解密，以取得多數個分別對應記憶卡的一資料儲存區中多數個檔案的資料金鑰，接著利用該等資料金鑰分別針對其對應的檔案進行解密，以讀取該等檔案中的資料，如此一來，透過主金鑰及資料金鑰的雙重保護，以及，且每個檔案分別利用唯一且不同的資料金鑰加密，使得每個檔案獨立控管，如此將可更加確保資料的安全性。

六、發明說明：

【發明所屬之技術領域】

本發明是有關於一種記憶卡的讀取方法，特別是指一種應用於行動裝置的記憶卡的讀取方法。

【先前技術】

記憶卡擁有體積小、容量大及攜帶方便等優點，近年來，已成為行動裝置(例如：手機)用以儲存個人重要資料的儲存媒體。然而，當記憶卡不小心遺失時，其中所儲存的資料也可能隨之被盜用。

智慧卡(Smart Card)是一種具有如微處理器、操作系統、記憶體等的積體電路晶片(Chip)，因此，智慧卡可提供計算、加密等功能，使得智慧卡除了擁有儲存資料的功能外，還具有對所儲存的資料加以保護的功能。但是，以往的智慧卡只對其所儲存的資料作單層的保護，即僅比對使用者所輸入的密碼是否正確，此對資料的保護並不嚴密，且在智慧卡中儲存著供比對的密碼，也增加了智慧卡若遺失導致密碼被盜的可能性，在變更密碼時，現有的智慧卡需要將其所儲存的資料先進行解密，再利用新密碼進行加密，如此也耗費了過多的作業時間。

【發明內容】

因此，本發明之目的，即在提供一種可以更加確保資料的安全性的記憶卡的讀取方法。

於是，本發明記憶卡的讀取方法，係於一控制單元中執行，用以讀取一記憶卡中的資料，該讀取方法包含以下

步驟：

(A)接收一個人識別碼(Personal Identification Number code，PIN code)；

(B)判別個人識別碼是否正確，若是，則執行步驟(C)；

(C)從記憶卡中取得一主金鑰；

(D)利用主金鑰對記憶卡的一資料金鑰儲存區進行解密，以取得多數個分別對應記憶卡的一資料儲存區中多數個檔案的資料金鑰；

(E)利用該等資料金鑰分別針對其對應的檔案進行解密，以讀取該等檔案中的資料。如此透過主金鑰及資料金鑰的雙重保護，以及每個檔案是分別利用唯一且不同的資料金鑰加密，使得每個檔案能獨立控管，並提供不同存取權限之組合的功能，如此將大幅提升資料的安全性。

其中，步驟(A)是由該控制單元的一使用者介面接收該個人識別碼。

進一步來說，針對於步驟(B)中，判別該個人識別碼是否正確，可包含以下子步驟：

(B-1)使用者介面將該個人識別碼傳送至控制單元的一應用程式介面；

(B-2)該應用程式介面將個人識別碼打散及攪亂後傳送至控制單元的一雜湊值產生程式；

(B-3)雜湊值產生程式將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生一第一雜湊值；及

(B-4)控制單元的一識別程式判別第一雜湊值是否與一

第二雜湊值相同，若是，則執行步驟(C)。如此一來，利用雜湊值比對的方式來判別個人識別碼的正確性，可降低個人識別碼被竊取的機率。

而第二雜湊值是由本發明之金鑰產生方法產生，該金鑰產生方法係於一控制單元中執行，用以產生一主金鑰以對一記憶卡中的資料加密，其中包含以下步驟：

(A)控制單元的一使用者介面接收一個人識別碼；

(B)使用者介面將個人識別碼傳送至控制單元的一應用程式介面；

(C)應用程式介面將個人識別碼打散及攪亂後傳送至控制單元的一雜湊值產生程式；

(D)雜湊值產生程式將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生一雜湊值；

(E)控制單元的一主金鑰產生程式產生與雜湊值具對應關係的主金鑰；及

(F)主金鑰產生程式將主金鑰儲存於一記憶卡的一系統金鑰儲存區。

本讀取方法可為一內儲於一電腦程式產品的讀取程式，當電腦載入該讀取程式並執行後，可完成上述的讀取方法。

此外，本發明之另一目的，還提供一種多重加密以提升資料安全性的記憶卡的資料加密方法。

該記憶卡的資料加密方法，係於一控制單元中執行，用以對一記憶卡中的資料加密，其步驟如下：

(A)開啟該記憶卡中多數個檔案，以供資料存入；

(B)分別對應根據該等檔案產生一對應該檔案的資料金鑰；

(C)利用該等資料金鑰對各自對應的檔案進行加密；

(D)將加密後的該等資料金鑰儲存於該記憶卡的一資料金鑰儲存區；

(E)根據該資料金鑰儲存區產生一主金鑰；

(F)利用該主金鑰對該資料金鑰儲存區進行加密；及

(G)將該主金鑰儲存於該記憶卡的一系統金鑰儲存區。

再者，本發明還提供一種可執行上述步驟的記憶卡，該記憶卡包含一儲存模組及一控制單元。

儲存模組包括一系統金鑰儲存區、一資料金鑰儲存區及一資料儲存區；控制單元耦接於儲存模組，該控制單元接收一個人識別碼，並判別個人識別碼是否正確，若判定為正確，則從系統金鑰儲存區中取得一主金鑰，且先利用主金鑰對資料金鑰儲存區進行解密，以取得多數個分別對應儲存於資料儲存區中多數個檔案的資料金鑰，再利用該等資料金鑰分別針對其對應的檔案進行解密，以讀取該等檔案中的資料。

其中，控制單元中可具有一使用者介面、一應用程式介面、一雜湊值產生程式及一識別程式，於使用者介面接收個人識別碼，應用程式介面將該個人識別碼打散及攪亂後傳送至雜湊值產生程式，雜湊值產生程式將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生一

第一雜湊值，識別程式判別第一雜湊值是否與一第二雜湊值相同，若是，則判定個人識別碼為正確。

此外，本發明之另一目的，還提供一種可以快速換密的記憶卡密碼的變更方法。

本變更方法，係於一控制單元中執行，該變更方法是首先接收一個人識別碼，並判別該個人識別碼是否正確，若判定為正確，則從記憶卡中取得一主金鑰，再接收另一新個人識別碼，並根據該新個人識別碼產生另一主金鑰，接著，先利用原先主金鑰對記憶卡的資料金鑰儲存區進行解密，再利用新主金鑰對資料金鑰儲存區進行加密，並於加密後，將新主金鑰儲存於記憶卡的系統金鑰儲存區中，如此換密作業將不需將資料重新解密再加密，因此本記憶卡將具備快速換密之能力。

本發明記憶卡的讀取方法具有以下功效：

1. 透過雜湊值的比對來判別個人識別碼的正確性，可避免有心人士惡意掃描記憶卡而盜取密碼。
2. 個人識別碼是以打散及攪亂的方式傳輸，使得個人識別碼不連續存放，如此可降低個人識別碼被竊取的機率，更加確保傳輸上的安全性。
3. 資料儲存區中的各個檔案分別利用一隨機產生且唯一的資料金鑰加密，使得每個檔案可獨立控管，以達不同存取權限之組合的功能。
4. 利用主金鑰及資料金鑰達到多重加密技術，可提升資料加密的強度，更加確保資料的安全性。

5. 變更密碼時，僅需透過原先主金鑰及新主金鑰分別對資料金鑰儲存區進行解密及加密，不需針對資料進行加/解密，以節省系統作業的時間。

【實施方式】

有關本發明之前述及其他技術內容、特點與功效，在以下配合參考圖式之一個較佳實施例的詳細說明中，將可清楚的呈現。

參閱圖 1 及圖 2，為本發明記憶卡的讀取方法之較佳實施例，本實施例之讀取方法是應用於一可內建或由外部安裝於行動裝置的一記憶卡 100 中，該記憶卡 100 是一智慧卡(Smart Card)，其中包含一儲存模組 1，及一耦接於儲存模組 1 的控制單元 2，在本實施例中，儲存模組 1 與控制單元 2 是整合於同一個晶片(Chip)中，且行動裝置是以手機為例，但不以此為限。

儲存模組 1 包括一一般資料儲存區(Normal Zone)10 及一隱密資料儲存區(Hidden Zone)20。一般資料儲存區 10 用以儲存一般使用者常用或欲備份的資料等；隱密資料儲存區 20 則主要是用以儲存重要性較高的資料，例如：使用者帳號或密碼等，且在隱密資料儲存區 20 中可再區分出一系統金鑰儲存區(System Key Store)21、一資料金鑰儲存區(Key Store)22 及一資料儲存區(Data Store)23，系統金鑰儲存區 21 用以儲存一主金鑰(Master Key)，及一與一個人識別碼(Personal Identification Number code，PIN code)有關的第二雜湊值；資料金鑰儲存區 22 用以儲存多數個資料金鑰

(Data Key)；資料儲存區 23 中具有多數個可分別供該等資料金鑰加密的檔案，而重要性較高的資料則是儲存於該些檔案中。

配合參閱圖 3，控制單元 2 內儲有一使用者介面 200、一應用程式介面(Application Programming Interface，API)201、一雜湊值產生程式 202、一識別程式 203 及一主金鑰產生程式 204。特別說明的是，隱密資料儲存區 20 僅能由控制單元 2 的應用程式介面 201 偵測到，行動裝置的作業系統僅能偵測到一般資料儲存區 10，以確保隱密資料儲存區 20 中資料的隱密性。

參閱圖 1、圖 2 及圖 3，以下將詳細說明控制單元 2 是如何讀取儲存模組 1 的隱密資料儲存區 20 中的資料，以及隱密資料儲存區 20 中資料的加/解密流程。

步驟 S10，控制單元 2 的使用者介面 200 接收一由使用者輸入的個人識別碼。

接著步驟 S20，控制單元 2 會判別使用者所輸入的個人識別碼是否正確，若輸入正確，則執行步驟 S30；若輸入錯誤，則執行步驟 S60，控制單元 2 會判斷密碼輸入錯誤的次數是否達一特定次數(例如：10 次)，若是，則結束流程，並且鎖定記憶卡 100，使得使用者將無法看到隱密資料儲存區 20 中的資料，也無法對其進行讀取、編輯等動作。若密碼輸入錯誤的次數未達特定次數，則重複執行步驟 S10。

為了防止有心人士刻意掃描記憶卡 100 以竊取隱密資料儲存區 20 中的資料，在步驟 S20 中，控制單元 2 會利用

個人識別碼產生雜湊值，並透過雜湊值的比對來判斷個人識別碼的正確性，其細部動作如下：

參閱圖 2、圖 3 及圖 4，使用者介面 200 先將該個人識別碼傳送至應用程式介面 201(步驟 S21)，應用程式介面 201 將該個人識別碼打散及攪亂後傳送至雜湊值產生程式 202(步驟 S22)，雜湊值產生程式 202 將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生一第一雜湊值(步驟 S23)，最後識別程式 203 可判別由個人識別碼所產生的第一雜湊值是否與儲存於系統金鑰儲存區 21 中的第二雜湊值相同(步驟 S24)，若第一雜湊值與第二雜湊值相同，則表示使用者所輸入的個人識別碼無誤，控制單元 2 將會執行步驟 S30。反之，則執行步驟 S60。

特別說明的是，本實施例之個人識別碼是由 8~24 個以上的字元所組成，且使用者介面 200 是將每一個字元分別傳送至應用程式介面 201，使得應用程式介面 201 會將每一次接收到的字元與之前接收到且已打散攪亂的字元重複打散並攪亂，也就是說，整個個人識別碼中的所有字元皆不連續存放，如此可增加個人識別碼傳輸上的安全。

步驟 S30，控制單元 2 從儲存模組 1 的系統金鑰儲存區 21 中取得主金鑰。

步驟 S40，控制單元 2 利用主金鑰對資料金鑰儲存區 22 進行解密，以取得多數個分別對應儲存於資料儲存區 23 中的多數個檔案的資料金鑰。

步驟 S50，控制單元 2 利用該等資料金鑰分別針對其對

應位於資料儲存區 23 中的檔案進行解密，以取得該等檔案中的資料，並供使用者對該些檔案執行讀/存取資料、變更名稱、格式化等檔案管理功能。

換言之，使用者透過行動裝置的使用者介面輸入個人識別碼後，控制單元 2 會以比對雜湊值的方式來判斷該個人識別碼的正確性，以增加記憶卡 100 的安全性，且個人識別碼是以打散及攪亂的方式傳輸，如此將可避免記憶卡 100 掃描的攻擊。再者，在確認個人識別碼輸入無誤後，控制單元 2 會先取得主金鑰，並對資料金鑰儲存區 22 進行第一次的解密，再利用解密出的資料金鑰分別對資料儲存區 23 中的各個檔案進行第二次的解密，以取得其中被保護的資料，如此多重加密技術可更提升資料的保密性，此外，每個位於資料儲存區 23 中的檔案各自獨立且皆有對應且唯一的資料金鑰保護，將可大幅降低隱密資料儲存區 20 中資料被竊取的機率。

相反地，參閱圖 5，當控制單元 2 將資料儲存區 23 中的各個檔案開啟，以供使用者將重要資料存入後(步驟 S71)，會分別根據各個檔案隨機(Random)產生一對應該檔案的資料金鑰(步驟 S72)，接著，控制單元 2 利用該等資料金鑰對各自對應的檔案進行第一次的加密(步驟 S73)，並於加密後將該等資料金鑰儲存於資料金鑰儲存區 22 中(步驟 S74)，控制單元 2 會再根據資料金鑰儲存區 22 隨機產生一主金鑰(步驟 S75)，並利用主金鑰對資料金鑰儲存區 22 進行第二次的加密(步驟 S76)，最後再將主金鑰儲存於系統金

鑰儲存區 21(步驟 S77)，如此可達到多重加密以提升資料的保密性之功效。

然而參閱圖 3 及圖 6，在本實施例中，當記憶卡 100 第一次設定密碼時，控制單元 2 會將使用者所輸入之個人識別碼轉換成第二雜湊值，並儲存於系統金鑰儲存區 21，其詳細步驟如下：

步驟 S81，使用者介面 200 接收一由使用者輸入的個人識別碼。

步驟 S82，使用者介面 200 將個人識別碼傳送至應用程式介面 201。

步驟 S83，應用程式介面 201 將個人識別碼打散及攪亂後傳送至雜湊值產生程式 202。

步驟 S84，雜湊值產生程式 202 將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生第二雜湊值。特別說明的是，使用者欲設定密碼時，使用者介面 200 會提供使用者設定密碼的畫面，雜湊值產生程式 202 會產生第二雜湊值並儲存於系統金鑰儲存區 21，而其後使用者輸入密碼(即個人識別碼)時，雜湊值產生程式 202 則是根據該個人識別碼產生第一雜湊值，並與儲存於系統金鑰儲存區 21 的第二雜湊值比較，以判斷該個人識別碼是否正確。

步驟 S85，主金鑰產生程式 204 產生與第二雜湊值具對應關係的主金鑰。在本實施例中，主金鑰產生程式 204 是根據第二雜湊值直接產生主金鑰，但也可以是主金鑰產生程式 204 先隨機產生主金鑰，再將該主金鑰對應於第二雜

湊值，故不以本實施例為限。

步驟 S86，主金鑰產生程式 204 將主金鑰儲存於一記憶卡 100 的系統金鑰儲存區 21。

參閱圖 7 及圖 8，當使用者欲變更密碼時，控制單元 2 係利用原先的主金鑰先對資料金鑰儲存區 22 進行解密，以更換其中的資料金鑰，接著再利用新的主金鑰對資料金鑰儲存區 22 進行加密，如此將不需要針對資料進行加/解密，以節省系統作業的時間。其細部動作如下：

步驟 S91，控制單元 2 的使用者介面 200 接收一由使用者輸入的個人識別碼。

步驟 S92，控制單元 2 判別該個人識別碼是否正確，若是，則執行步驟 S93；若否，則執行步驟 S99，控制單元 2 會判斷密碼輸入錯誤的次數是否達一特定次數，若是，則結束流程，並且鎖定記憶卡 100，使得使用者將無法看到隱密資料儲存區 20 中的資料，也無法對其進行讀取、編輯等動作。若密碼輸入錯誤的次數未達特定次數，則重複執行步驟 S91。

步驟 S93，控制單元 2 從記憶卡 100 的系統金鑰儲存區 21 中取得原先之主金鑰。

步驟 S94，控制單元 2 的使用者介面 200 接收另一新的個人識別碼，即使用者所輸入之新密碼。

步驟 S95，控制單元 2 根據該另一個人識別碼產生另一主金鑰，其方法可如之前所述，控制單元 2 的主金鑰產生程式 204 可以根據雜湊值直接產生主金鑰，或是隨機產生

主金鑰，並不限定何種方式。

步驟 S96，控制單元 2 利用步驟 S93 中所取得之主金鑰(即原先的主金鑰)對記憶卡 100 的資料金鑰儲存區 22 進行解密。於圖 8(a)中，資料金鑰儲存區 22 儲存多數資料金鑰 DK1~DKN，資料儲存區 23 則儲存多數位址對應該等資料金鑰 DK1~DKN 的資料 data1~dataN，該等資料金鑰 DK1~DKN 是用於分別針對該等資料 data1~dataN 進行加/解密。

步驟 S97，利用新的主金鑰對資料金鑰儲存區 22 進行加密。如圖 8(b)所示，資料金鑰儲存區 22 中的資料金鑰會因為新主金鑰的設定而變更為 DK'1~DK'N，但該等資料金鑰 DK'1~DK'N 的位址並無改變，故同樣能針對該等資料 data1~dataN 進行加/解密。如此一來，在本發明之主金鑰及資料金鑰雙重加密之設計下，換密作業將不需將資料重新解密再加密，因此本記憶卡 100 將具備快速換密之能力。

步驟 S98，將新的主金鑰儲存於該記憶卡的系統金鑰儲存區 21。

此外，本實施例之讀取方法可為一內儲於一電腦程式產品(例如：光碟)的讀取程式，當一電子裝置(例如：電腦)載入該讀取程式並執行後，可完成上述的讀取方法。且在另一實施例中，記憶卡 100 可為一安全數位(Secure Digital，SD)卡，其中可以只包括儲存模組 1，而控制單元 2 則可設於行動裝置中，如此同樣能藉由控制單元 2 執行上述步驟而對儲存模組 1 進行加/解密、讀/存取等動作。

綜上所述，本發明記憶卡 100 的讀取方法，藉由將使用者所輸入的個人識別碼轉換成雜湊值來比對，以降低個人識別碼被竊取的機率，且個人識別碼是以打散及攪亂的方式傳輸，也更加確保傳輸上的安全性。再者，資料儲存區 23 中的各個檔案分別利用一隨機產生且唯一的資料金鑰加密，如此將可達到每個檔案獨立控管且可有不同存取權限之組合的功能，更加確保資料的安全性，不僅如此，用於儲存各個資料金鑰的資料金鑰儲存區 22 還再利用一主金鑰進行第二次的加密，以達到多重加密技術，更加提升資料加密的強度，且在更換密碼時，也僅需要針對資料金鑰儲存區 22 進行加/解密，更節省了系統作業時間，故確實能達成本發明之目的。

惟以上所述者，僅為本發明之較佳實施例而已，當不能以此限定本發明實施之範圍，即大凡依本發明申請專利範圍及發明說明內容所作之簡單的等效變化與修飾，皆仍屬本發明專利涵蓋之範圍內。

【圖式簡單說明】

圖 1 是說明本發明記憶卡的讀取方法之較佳實施例的流程圖；

圖 2 是說明記憶卡中的電路方塊示意圖；

圖 3 是說明控制單元中所燒錄的程式；

圖 4 是說明本讀取方法中控制單元是如何判別個人識別碼的正確性的流程圖；

圖 5 是說明控制單元對資料進行加密的流程圖；

圖 6 是說明控制單元產生金鑰的流程圖；

圖 7 是說明控制單元變更記憶卡密碼的流程圖；

圖 8(a)是說明密碼未變更前，資料金鑰儲存區中的資料金鑰與資料儲存區中的資料的對應關係；及

圖 8(b)是說明密碼變更後，資料金鑰儲存區中的資料金鑰與資料儲存區中的資料的對應關係。

【主要元件符號說明】

S10~S60 步驟
S21~S24 步驟
S71~S77 步驟
S81~S86 步驟
S91~S99 步驟
100……記憶卡
1……儲存模組
10……一般資料儲存區
20……隱密資料儲存區
21……系統金鑰儲存區
22……資料金鑰儲存區
23……資料儲存區
2……控制單元
200……使用者介面
201……應用程式介面
202……雜湊值產生程式
203……識別程式
204……主金鑰產生程式

201245956

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：101105275

※申請日：101.2.17　※IPC分類：G06F12/00 (2006.01)
H04L 9/32 (2006.01)
H04L 9/14 (2006.01)

一、發明名稱：（中文/英文）

記憶卡及其讀取、資料加密、金鑰產生及變更方法

二、中文發明摘要：

一種記憶卡的讀取方法，係於一控制單元中執行，用以讀取一記憶卡中的資料，該讀取方法首先會接收一個人識別碼，然後判別該個人識別碼是否正確，若是，則從記憶卡中取得一主金鑰，並利用該主金鑰對記憶卡的一資料金鑰儲存區進行解密，以取得多數個分別對應記憶卡的一資料儲存區中多數個檔案的資料金鑰，接著利用該等資料金鑰分別針對其對應的檔案進行解密，以讀取該等檔案中的資料，如此一來，透過主金鑰及資料金鑰的雙重保護，以及，且每個檔案分別利用唯一且不同的資料金鑰加密，使得每個檔案獨立控管，如此將可更加確保資料的安全性。

三、英文發明摘要：

七、申請專利範圍：

1. 一種記憶卡的讀取方法，係於一控制單元中執行，用以讀取一記憶卡中的資料，該讀取方法包含以下步驟：

(A)接收一個人識別碼；

(B)判別該個人識別碼是否正確，若是，則執行步驟(C)；

(C)從該記憶卡中取得一主金鑰；

(D)利用該主金鑰對該記憶卡的一資料金鑰儲存區進行解密，以取得多數個分別對應該記憶卡的一資料儲存區中多數個檔案的資料金鑰；

(E)利用該等資料金鑰分別針對其對應的檔案進行解密，以讀取該等檔案中的資料。

2. 依據申請專利範圍第 1 項所述之記憶卡的讀取方法，其中，該步驟(A)是由該控制單元的一使用者介面接收該個人識別碼。

3. 依據申請專利範圍第 2 項所述之記憶卡的讀取方法，其中，該步驟(B)包含以下子步驟：

(B-1)該使用者介面將該個人識別碼傳送至該控制單元的一應用程式介面；

(B-2)該應用程式介面會將該個人識別碼打散及攪亂後傳送至該控制單元的一雜湊值產生程式；

(B-3)該雜湊值產生程式將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生一第一雜湊值；及

(B-4)該控制單元的一識別程式判別該第一雜湊值是否與一第二雜湊值相同，若是，則執行步驟(C)。

4. 依據申請專利範圍第 3 項所述之記憶卡的讀取方法，其中，該步驟(C)是從該記憶卡的一系統金鑰儲存區中取得該主金鑰。

5. 一種內儲用於讀取記憶卡的讀取程式之電腦程式產品，當電腦載入該讀取程式並執行後，可完成申請專利範圍第 1 至 4 項中任一項所述的讀取方法。

6. 一種記憶卡的資料加密方法，係於一控制單元中執行，用以對一記憶卡中的資料加密，該資料加密方法包含以下步驟：

(A)開啟該記憶卡中多數個檔案，以供資料存入；

(B)分別對應根據該等檔案產生一對應該檔案的資料金鑰；

(C)利用該等資料金鑰對各自對應的檔案進行加密；

(D)將加密後的該等資料金鑰儲存於該記憶卡的一資料金鑰儲存區；

(E)根據該資料金鑰儲存區產生一主金鑰；

(F)利用該主金鑰對該資料金鑰儲存區進行加密；及

(G)將該主金鑰儲存於該記憶卡的一系統金鑰儲存區。

7. 依據申請專利範圍第 6 項所述之記憶卡的資料加密方法，其中，該步驟(B)是分別對應根據該等檔案隨機產生該等資料金鑰。

8. 一種記憶卡，包含：

一儲存模組，包括一系統金鑰儲存區、一資料金鑰儲存區及一資料儲存區；及

一控制單元，耦接於該儲存模組，該控制單元接收一個人識別碼，並判別該個人識別碼是否正確，若判定為正確，則從該系統金鑰儲存區中取得一主金鑰，先利用該主金鑰對該資料金鑰儲存區進行解密，以取得多數個分別對應儲存於該資料儲存區中多數個檔案的資料金鑰，再利用該等資料金鑰分別針對其對應的檔案進行解密，以讀取該等檔案中的資料。

9. 依據申請專利範圍第 8 項所述之記憶卡，其中，該控制單元中具有一使用者介面、一應用程式介面、一雜湊值產生程式及一識別程式，於該使用者介面接收該個人識別碼，該應用程式介面將該個人識別碼打散及攪亂後傳送至該雜湊值產生程式，該雜湊值產生程式將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生一第一雜湊值，該識別程式判別該第一雜湊值是否與一第二雜湊值相同，若是，則判定該個人識別碼為正確。

10. 依據申請專利範圍第 9 項所述之記憶卡，其中，該第二雜湊值係儲存於該系統金鑰儲存區中。

11. 依據申請專利範圍第 10 項所述之記憶卡，其中，該儲存模組還包括一用以儲存一般資料的一般資料儲存區，及一用以儲存重要資料的隱密資料儲存區，該系統金鑰儲

存區、該資料金鑰儲存區及該資料儲存區則係位於該隱密資料儲存區中。

12.一種金鑰產生方法，係於一控制單元中執行，用以產生一主金鑰以對一記憶卡中的資料加密，該金鑰產生方法包含以下步驟：

(A)該控制單元的一使用者介面接收一個人識別碼；

(B)該使用者介面將該個人識別碼傳送至該控制單元的一應用程式介面；

(C)該應用程式介面將該個人識別碼打散及攪亂後傳送至該控制單元的一雜湊值產生程式；

(D)該雜湊值產生程式將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生一雜湊值；

(E)該控制單元的一主金鑰產生程式產生與該雜湊值具對應關係的主金鑰；及

(F)該主金鑰產生程式將該主金鑰儲存於該記憶卡的一系統金鑰儲存區。

13.依據申請專利範圍第 12 項所述之金鑰產生方法，其該步驟(E)中，該主金鑰產生程式是根據該雜湊值產生該主金鑰。

14.依據申請專利範圍第 12 項所述之金鑰產生方法，其該步驟(E)中，該主金鑰產生程式是先隨機產生該主金鑰，再將該主金鑰對應於該雜湊值。

15.一種記憶卡密碼的變更方法，係於一控制單元中執行，該變更方法包含以下步驟：

(A)接收一個人識別碼；

(B)判別該個人識別碼是否正確，若是，則執行步驟(C)；

(C)從該記憶卡中取得一主金鑰；

(D)接收另一個人識別碼；

(E)根據該另一個人識別碼產生另一主金鑰；

(F)利用該主金鑰對該記憶卡的一資料金鑰儲存區進行解密；

(G)利用該另一主金鑰對該資料金鑰儲存區進行加密；

(H)將該另一主金鑰儲存於該記憶卡的一系統金鑰儲存區。

八、圖式：

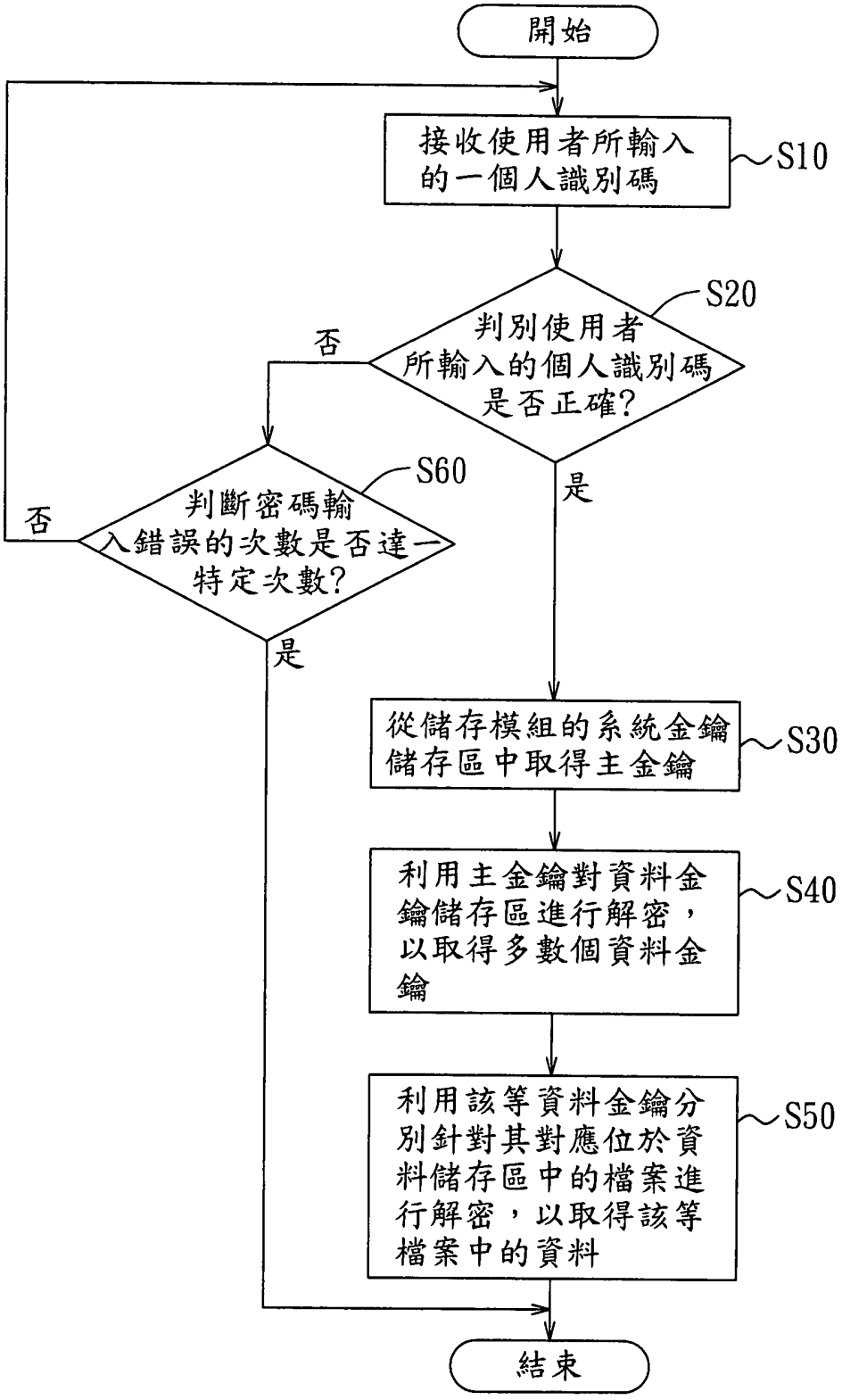

開始
接收使用者所輸入的一個人識別碼
S10
判別使用者所輸入的個人識別碼是否正確?
S20
否
是
判斷密碼輸入錯誤的次數是否達一特定次數?
S60
否
是
從儲存模組的系統金鑰儲存區中取得主金鑰
S30
利用主金鑰對資料金鑰儲存區進行解密，以取得多數個資料金鑰
S40
利用該等資料金鑰分別針對其對應位於資料儲存區中的檔案進行解密，以取得該等檔案中的資料
S50
結束

圖 1

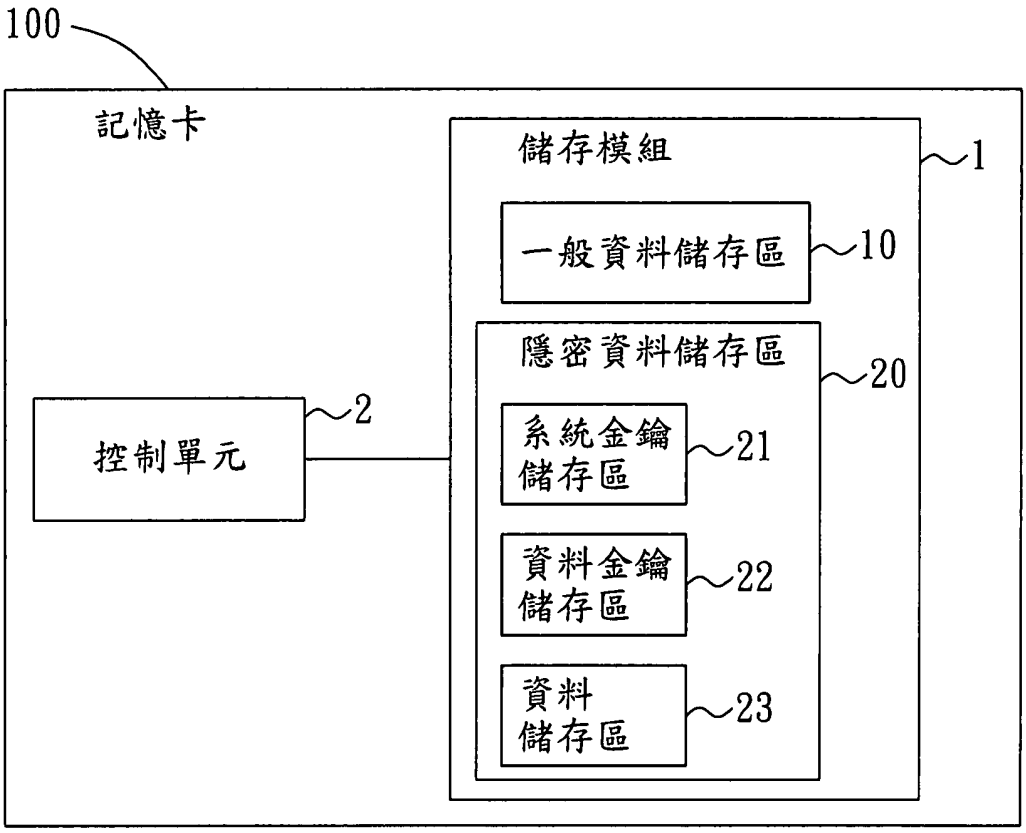

100
記憶卡
儲存模組
1
一般資料儲存區
10
隱密資料儲存區
20
系統金鑰儲存區
21
資料金鑰儲存區
22
資料儲存區
23
控制單元
2

圖 2

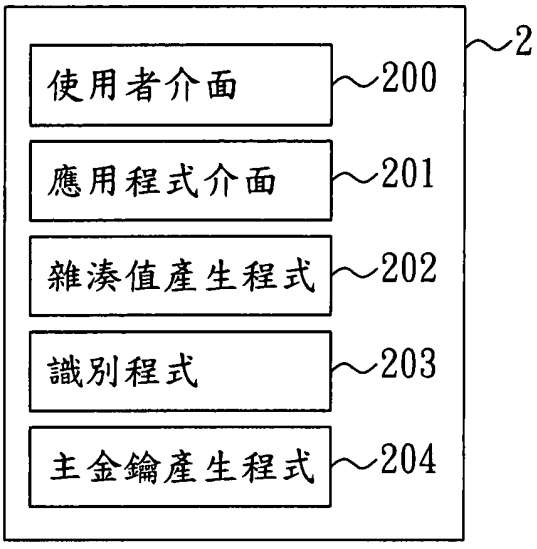

2
使用者介面
200
應用程式介面
201
雜湊值產生程式
202
識別程式
203
主金鑰產生程式
204

圖 3

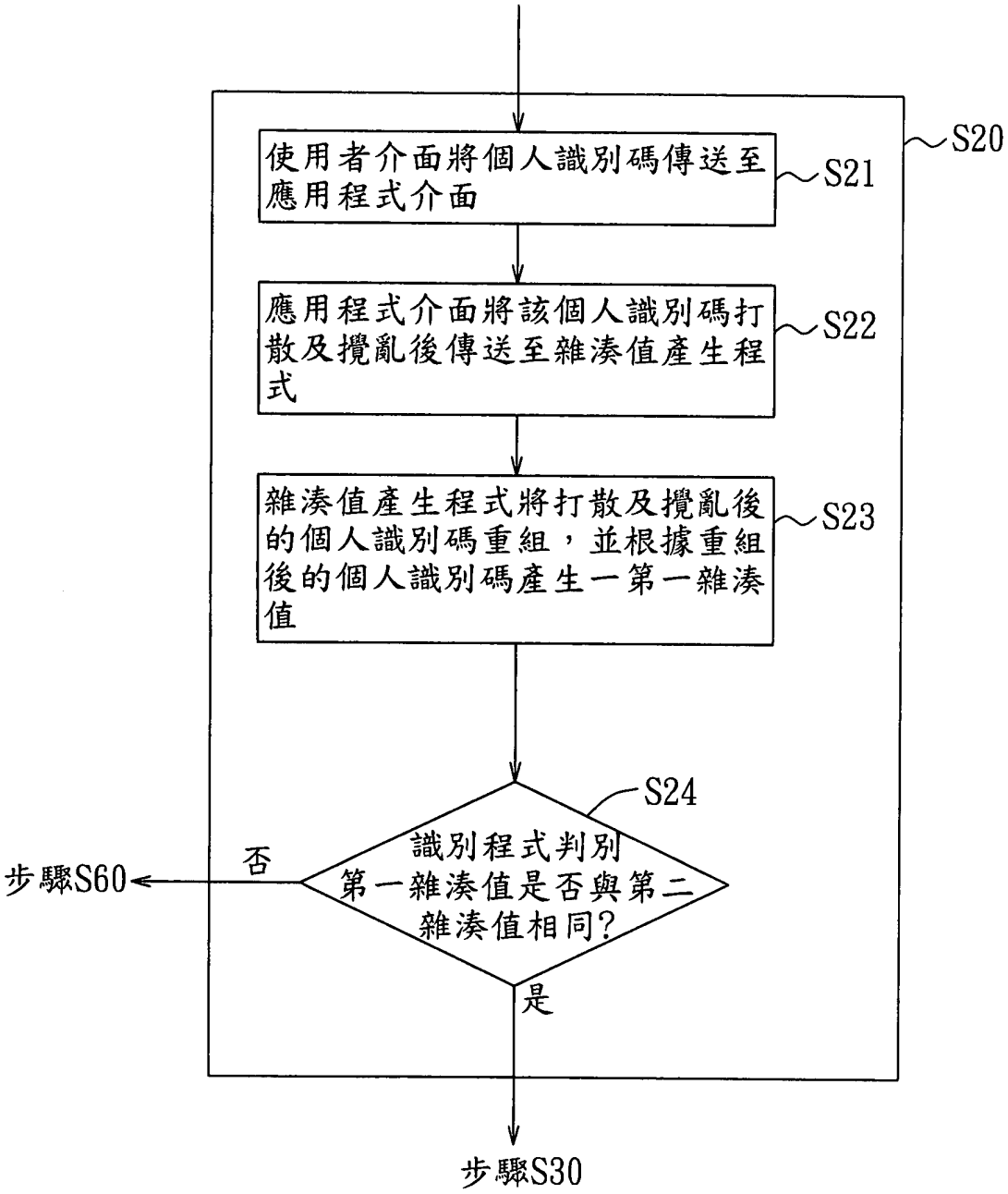

S20
使用者介面將個人識別碼傳送至應用程式介面
S21
應用程式介面將該個人識別碼打散及攪亂後傳送至雜湊值產生程式
S22
雜湊值產生程式將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生一第一雜湊值
S23
S24
識別程式判別第一雜湊值是否與第二雜湊值相同?
否
步驟S60
是
步驟S30

圖 4

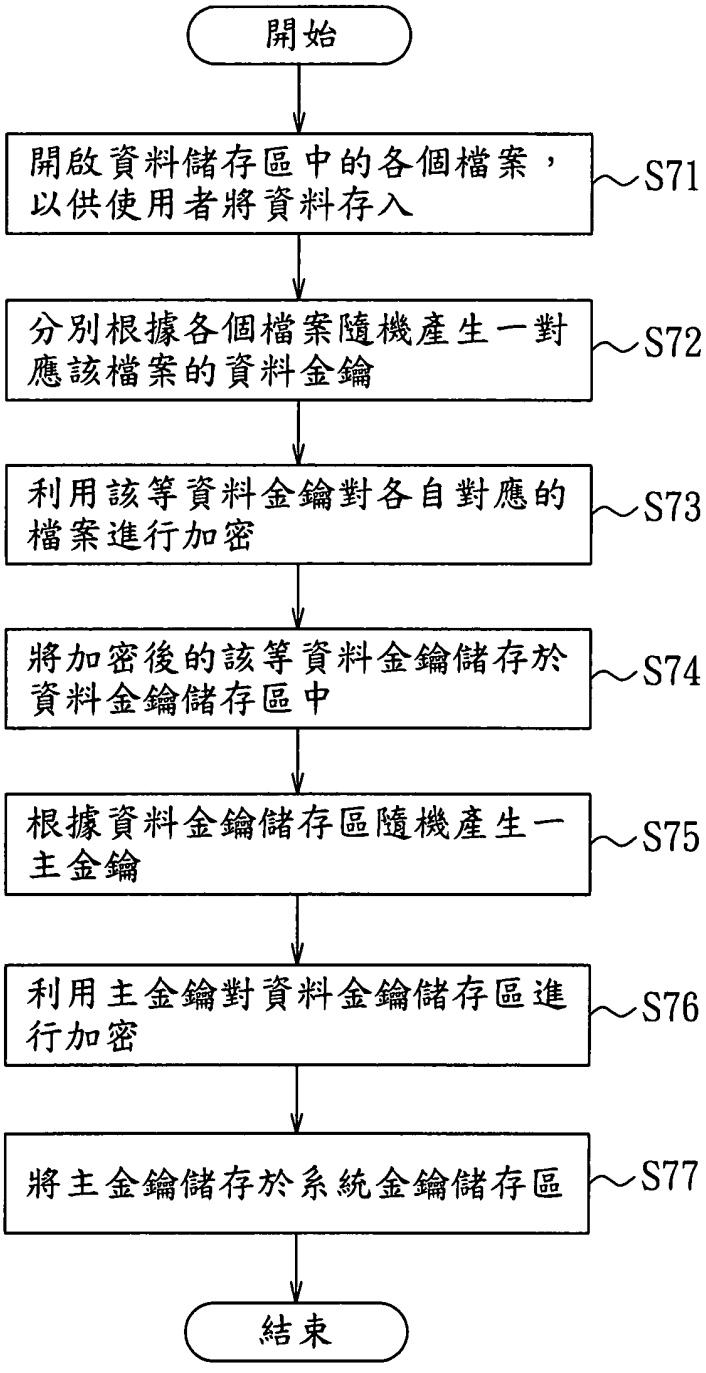

開始
開啟資料儲存區中的各個檔案，以供使用者將資料存入
S71
分別根據各個檔案隨機產生一對應該檔案的資料金鑰
S72
利用該等資料金鑰對各自對應的檔案進行加密
S73
將加密後的該等資料金鑰儲存於資料金鑰儲存區中
S74
根據資料金鑰儲存區隨機產生一主金鑰
S75
利用主金鑰對資料金鑰儲存區進行加密
S76
將主金鑰儲存於系統金鑰儲存區
S77
結束

圖 5

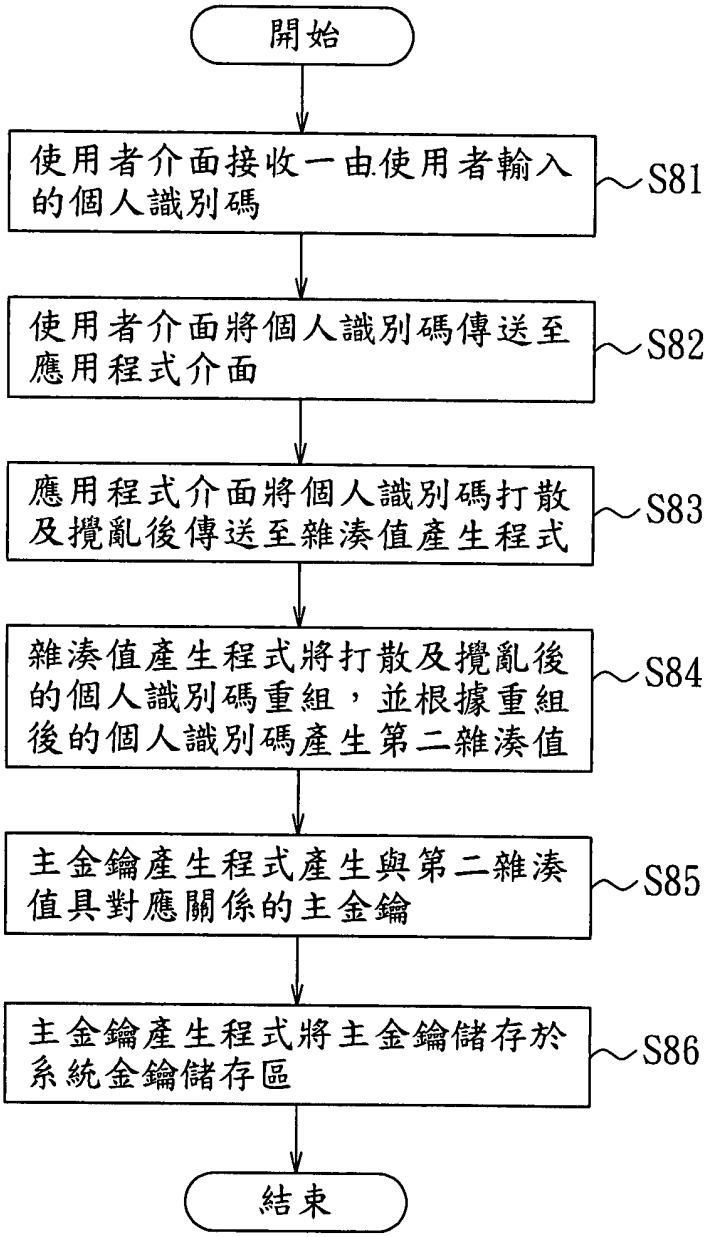

開始
使用者介面接收一由使用者輸入的個人識別碼
S81
使用者介面將個人識別碼傳送至應用程式介面
S82
應用程式介面將個人識別碼打散及攪亂後傳送至雜湊值產生程式
S83
雜湊值產生程式將打散及攪亂後的個人識別碼重組，並根據重組後的個人識別碼產生第二雜湊值
S84
主金鑰產生程式產生與第二雜湊值具對應關係的主金鑰
S85
主金鑰產生程式將主金鑰儲存於系統金鑰儲存區
S86
結束

圖 6

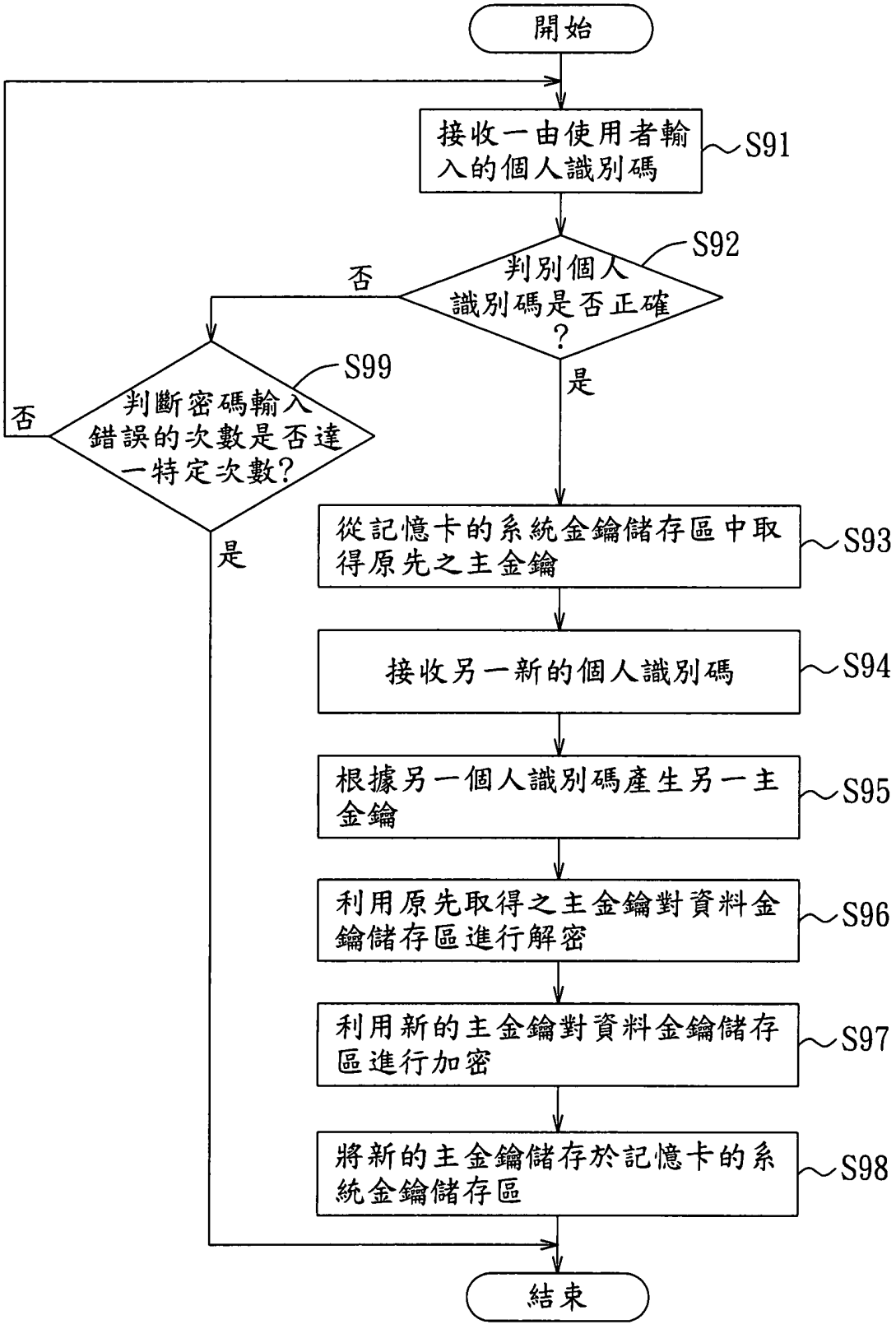

開始
接收一由使用者輸入的個人識別碼
S91
判別個人識別碼是否正確？
S92
否
是
判斷密碼輸入錯誤的次數是否達一特定次數?
S99
否
是
從記憶卡的系統金鑰儲存區中取得原先之主金鑰
S93
接收另一新的個人識別碼
S94
根據另一個人識別碼產生另一主金鑰
S95
利用原先取得之主金鑰對資料金鑰儲存區進行解密
S96
利用新的主金鑰對資料金鑰儲存區進行加密
S97
將新的主金鑰儲存於記憶卡的系統金鑰儲存區
S98
結束

圖 7

address	data
0000	data 1
0001	data 2
⋮	⋮
	data N

address	data key
0000	DK 1
0001	DK 2
⋮	⋮
	DK N

(a)

address	data
0000	data 1
0001	data 2
⋮	⋮
	data N

address	data key
0000	DK' 1
0001	DK' 2
⋮	⋮
	DK' N

(b)

圖 8

四、指定代表圖：

(一)本案指定代表圖為：圖（ 1 ）。

(二)本代表圖之元件符號簡單說明：

S10~S60 步驟

五、本案若有化學式時，請揭示最能顯示發明特徵的化學式：