202025051

(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 202025051 A

(43)公開日： 中華民國 109 (2020) 年 07 月 01 日

(21)申請案號：107146634　(22)申請日： 中華民國 107 (2018) 年 12 月 22 日

(51)Int. Cl.：　*G06Q40/00　(2012.01)*　*G06F21/31　(2013.01)*

(71)申請人：台新國際商業銀行股份有限公司 (中華民國) TAISHIN INTERNATIONAL BANK CO. LTD.　(TW)

臺北市中山區中山北路 2 段 44 號 1 樓

(72)發明人：王瑤璋 WANG, JOHNSON (TW)

(74)代理人：鄭志玲

申請實體審查：有　申請專利範圍項數：10 項　圖式數：2　　共 43 頁

(54)名稱

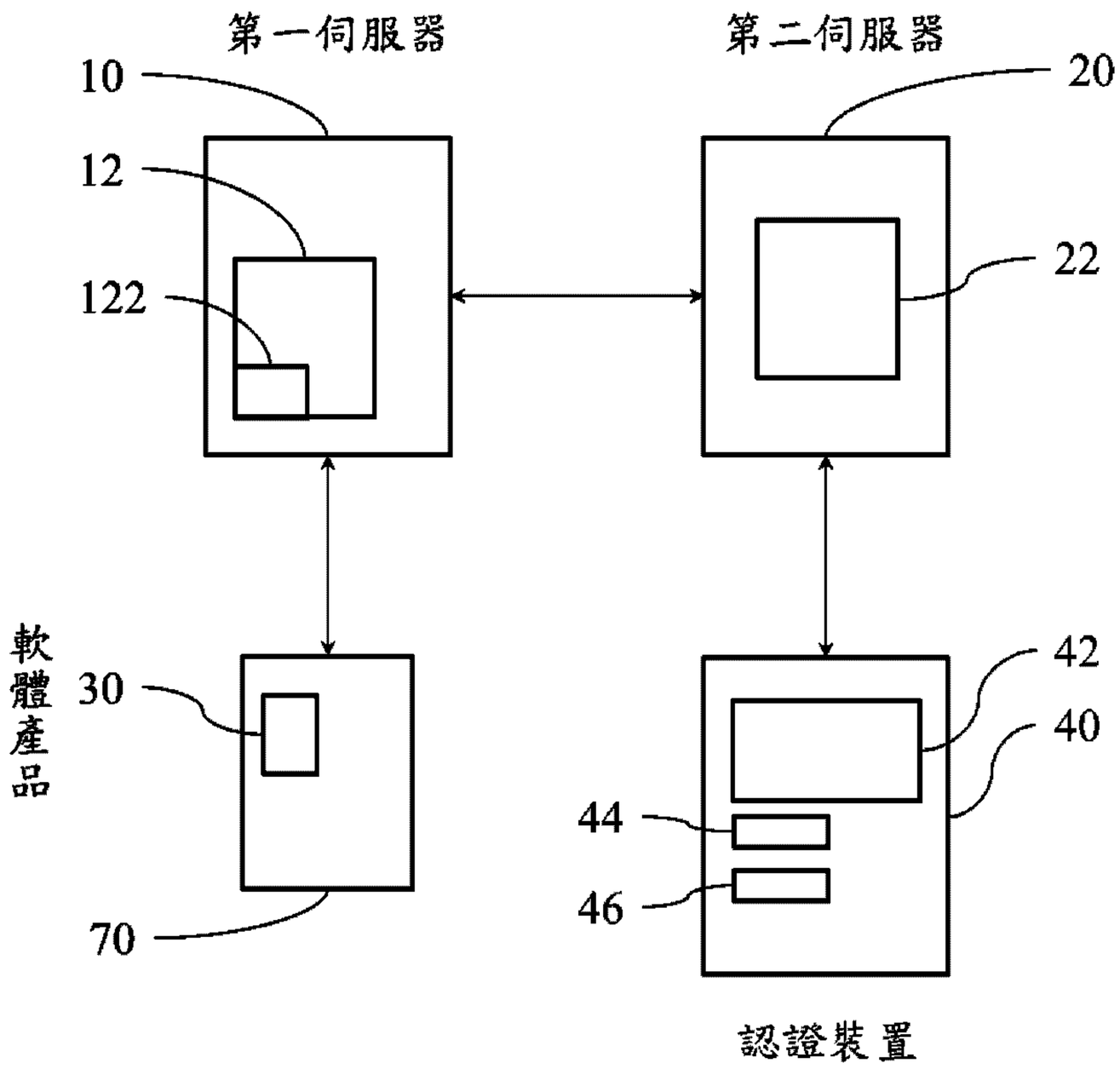
用於幫助持卡人首次設定金融卡密碼之系統及其方法

(57)摘要

本發明揭示一種用於幫助持卡人首次設定金融卡密碼之系統，及其方法。該系統包含一第一伺服器，設有一密碼設定模組，其包括一儲存子模組；一第二伺服器，與該第一伺服器電性連接，並設有一金融卡管理模組；一軟體產品（App），與該第一伺服器通訊連接，該 App 係安裝於該持卡人所持有的一行動裝置，且該 App 係經該密碼設定模組認證；以及一認證裝置，與該第二伺服器通訊連接，該認證裝置具有一顯示元件、一輸入元件及一金融卡讀寫元件。

Disclosed is a system for assisting a financial card holder in setting password for the first time, and a method thereof. Said system comprises a first sever configured with a password setting module including a storage submodule; a second sever electrically connected to the first sever and configured with a financial card management module; an App communicatively connected to the first sever and installed on a mobile device possessed by the financial card holder, the App being authenticated by the password setting module; and a authentication device communicatively connected to the second sever and having a display component, an input component and a financial card reading and writing component.

指定代表圖：



【圖1】

符號簡單說明：

1:用於幫助持卡人首次設定金融卡密碼之系統

10:第一伺服器

12:密碼設定模組

122:儲存子模組

20:第二伺服器

22:金融卡管理模組

30:軟體產品

40:認證裝置

42:顯示元件

44:輸入元件

46:金融卡讀寫元件

70:行動裝置

202025051

【發明摘要】

【中文發明名稱】 用於幫助持卡人首次設定金融卡密碼之系統及其方法

【英文發明名稱】 SYSTEM FOR ASSISTING A FINANCIAL CARD HOLDER IN SETTING PASSWORD FOR THE FIRST TIME AND METHOD THEREOF

【中文】

本發明揭示一種用於幫助持卡人首次設定金融卡密碼之系統，及其方法。該系統包含一第一伺服器，設有一密碼設定模組，其包括一儲存子模組；一第二伺服器，與該第一伺服器電性連接，並設有一金融卡管理模組；一軟體產品（App），與該第一伺服器通訊連接，該App係安裝於該持卡人所持有的一行動裝置，且該App係經該密碼設定模組認證；以及一認證裝置，與該第二伺服器通訊連接，該認證裝置具有一顯示元件、一輸入元件及一金融卡讀寫元件。

【英文】

Disclosed is a system for assisting a financial card holder in setting password for the first time, and a method thereof. Said system comprises a first sever configured with a password setting module including a storage submodule; a second sever electrically connected to the first sever and configured with a financial card management module; an App communicatively connected to the first sever and installed on a mobile device possessed by the financial card holder, the App being authenticated by the password setting module; and a authentication device communicatively connected to the second

sever and having a display component, an input component and a financial card reading and writing component.

【指定代表圖】　圖1

【代表圖之符號簡單說明】

1	用於幫助持卡人首次設定金融卡密碼之系統
10	第一伺服器
12	密碼設定模組
122	儲存子模組
20	第二伺服器
22	金融卡管理模組
30	軟體產品
40	認證裝置
42	顯示元件
44	輸入元件
46	金融卡讀寫元件
70	行動裝置

【特徵化學式】無

【發明說明書】

【中文發明名稱】 用於幫助持卡人首次設定金融卡密碼之系統及其方法

【英文發明名稱】 SYSTEM FOR ASSISTING A FINANCIAL CARD HOLDER IN SETTING PASSWORD FOR THE FIRST TIME AND METHOD THEREOF

【技術領域】

【0001】 本發明係關於一種用於幫助持卡人首次設定金融卡密碼之系統及其方法，特別係關於一種無需紙本金融卡密碼函的系統及方法。

【先前技術】

【0002】 現行金融卡密碼函係由金融卡系統相關功能產出密碼檔後，由特定安管人員於指定環境下，以人工操作指定機器設備與交易功能，完成金融卡密碼函列印作業；之後，經由專人打包、運送、郵遞到各指定分行；最後，由各分行指定專人清點收妥後入庫、儲藏、保管；於客戶到分行臨櫃辦理新金融卡申請時，再經指定專人於主管審核後，自保險庫取得該金融卡之密碼函，連同新申請之金融卡一起交付持卡人簽收。

【0003】 因此，對於金融業者而言，仍需要一種系統或方法，以取代現行通過人工操作列印密碼函的繁瑣程序，節省其間配套的相關人工作業、環境設施、列印機器、紙張、郵遞、保管儲存、資安控管及風險稽查等等作業成本負擔。此外，若能消除紙本金融卡密碼函之使用，亦能達到節能減碳的效果，有助於地球之環境保護。

【發明內容】

【0004】有鑑於此，本發明提供用於幫助持卡人首次設定金融卡密碼之系統及其方法，其無需紙本金融卡密碼函即可完成金融卡密碼之首次設定，並能兼顧密碼設定之安全性。

【0005】在一方面，本發明揭示一種用於幫助持卡人首次設定金融卡密碼之系統，包含：

一第一伺服器，設有一密碼設定模組，其包括一儲存子模組；

一第二伺服器，與該第一伺服器電性連接，並設有一金融卡管理模組；

一軟體產品（App），與該第一伺服器通訊連接，該App係安裝於該持卡人所持有的一行動裝置，且該App係經該密碼設定模組認證；以及

一認證裝置，與該第二伺服器通訊連接，該認證裝置具有一顯示元件、一輸入元件及一金融卡讀寫元件；

其中：

該密碼設定模組於一預先註冊程序中：接收一第一認證資料，其係由該行動裝置的識別資訊以及該持卡人的個人資訊所組成，並將該第一認證資料儲存於該儲存子模組；以及，接收一第二認證資料，其為一自選文摘，並將該第二認證資料儲存於該儲存子模組；

該認證裝置藉由該金融卡讀寫元件讀取該金融卡，並藉由該顯示元件提供一第一使用者介面，顯示首次設定金融卡密碼之選項，該選項經選擇後，該認證裝置向該金融卡管理模組發送首次設定金融卡密碼之請求；

該金融卡管理模組將該首次設定金融卡密碼之請求傳送予該密碼設定模組；

該密碼設定模組：根據一組合方法組合該第一認證資料，以產生一第一金鑰，其中，該組合方法係隨機挑選自複數個組合方法，並具有一第一編號；將該第一編號儲存於該儲存子模組；基於該第一金鑰對一原碼內容進行加密，產生一二維條碼，其中，該原碼內容包括該自選文摘；將該二維條碼傳送予該認證裝置；

該認證裝置藉由該顯示元件於該第一使用者介面顯示該二維條碼；

該App於啟動後自動觸發一事件，要求輸入個人資訊及金融卡之帳號，並將輸入之個人資訊及帳號傳送予該密碼設定模組；

該密碼設定模組於確認該App合法性後：根據儲存在儲存子模組中的第一編號，使用對應的組合方法組合該第一認證資料，以產生一第二金鑰；自複數個加密方法中隨機挑選一加密方法，該加密方法具有一第二編號；以及，向該App傳送該第一編號，及基於該第二金鑰加密後的確認資料，該確認資料包括一加密資訊，其中，該加密資訊包括該第二編號，及一開始取樣位置；

該App自該行動裝置取得該行動裝置的識別資訊以及該持卡人的個人資訊，並根據該第一編號所對應的組合方法，組合所述識別資訊及個人資訊，以產生一第三金鑰；

經由該行動裝置掃描讀取顯示於該認證裝置的該顯示元件上的該二維條碼後，該App使用該第三金鑰解譯該二維條碼得到該原碼內容，並根據該第二編號所對應的加密方法及該開始取樣位置，對該自選文摘進行加密，得到一加密值；以及，基於該第三金鑰對該加密值進行加密後傳送予該密碼設定模組；

該密碼設定模組於確認該加密值的正確性後，向該金融卡管理模組發送取得認證碼之請求，並取得一認證碼；以及，產生一認證碼圖像，並傳送予該App；

該App顯示該認證碼圖像，以供該持卡人藉由認證裝置首次設定該金融卡之密碼時使用；以及

該認證裝置藉由該顯示元件於該第一使用者介面顯示欄位，供該持卡人藉由該輸入元件輸入該認證碼以及該金融卡之新密碼，以完成首次密碼設定。

【0006】 在本發明之部分具體實施例中，該密碼設定模組提供一第二使用者介面，供該金融卡之發卡方作業人員輸入該第一認證資料及該第二認證資料。

【0007】 在本發明之部分具體實施例中，該App要求一啟動密碼。

【0008】 在本發明之部分具體實施例中，該認證裝置的該第一使用者介面要求輸入認證碼及新密碼，以及該個人資訊的至少一部分，並基於所輸入的資料向該金融卡管理模組發送設定新密碼之請求。在特定具體實施例中，該金融卡管理模組確認接收到的認證碼及個人資料無誤後，取得經亂碼化的新密碼，並傳送予該認證裝置，供其藉由該金融卡讀寫元件寫入該經亂碼化的新密碼至該金融卡。

【0009】 另一方面，本發明提供一種用於幫助持卡人首次設定金融卡密碼之方法，包含：

提供一第一伺服器，設有一密碼設定模組，其包括一儲存子模組；一第二伺服器，與該第一伺服器電性連接，並設有一金融卡管理模組；一軟體產品（App），與該第一伺服器通訊連接，該App係安裝於該持卡人所持有的一行動裝置，且該App係經該密碼設定模組認證；以及一認證裝置，與該第二伺服器通訊連接，該認證裝置具有一顯示元件、一輸入元件及一金融卡讀寫元件；

該密碼設定模組於一預先註冊程序中：接收一第一認證資料，其係由該行動裝置的識別資訊以及該持卡人的個人資訊所組成，並將該第一認證資料儲存於

該儲存子模組；以及，接收一第二認證資料，其為一自選文摘，並將該第二認證資料儲存於該儲存子模組；

該認證裝置藉由該金融卡讀寫元件讀取該金融卡，並藉由該顯示元件提供一第一使用者介面，顯示首次設定金融卡密碼之選項，該選項經選擇後，該認證裝置向該金融卡管理模組發送首次設定金融卡密碼之請求；

該金融卡管理模組將該首次設定金融卡密碼之請求傳送予該密碼設定模組；

該密碼設定模組：根據一組合方法組合該第一認證資料，以產生一第一金鑰，其中，該組合方法係隨機挑選自複數個組合方法，並具有一第一編號；將該第一編號儲存於該儲存子模組；基於該第一金鑰對一原碼內容進行加密，產生一二維條碼，其中，該原碼內容包括該自選文摘；將該二維條碼傳送予該認證裝置；

該認證裝置藉由該顯示元件於該第一使用者介面顯示該二維條碼；

該App於啟動後自動觸發一事件，要求輸入個人資訊及金融卡之帳號，並將輸入之個人資訊及帳號傳送予該密碼設定模組；

該密碼設定模組於確認該App合法性後：根據儲存在儲存子模組中的第一編號，使用對應的組合方法組合該第一認證資料，以產生一第二金鑰；自複數個加密方法中隨機挑選一加密方法，該加密方法具有一第二編號；以及，向該App傳送該第一編號，及基於該第二金鑰加密後的確認資料，該確認資料包括一加密資訊，其中，該加密資訊包括該第二編號，及一開始取樣位置；

該App自該行動裝置取得該行動裝置的識別資訊以及該持卡人的個人資訊，並根據該第一編號所對應的組合方法，組合所述識別資訊及個人資訊，以產生一第三金鑰；

經由該行動裝置掃描讀取顯示於該認證裝置的該顯示元件上的該二維條碼後，該App使用該第三金鑰解譯該二維條碼得到該原碼內容，並根據該第二編號所對應的加密方法及該開始取樣位置，對該自選文摘進行加密，得到一加密值；以及，基於該第三金鑰對該加密值進行加密後傳送予該密碼設定模組；該密碼設定模組於確認該加密值的正確性後，向該金融卡管理模組發送取得認證碼之請求，並取得一認證碼；以及，產生一認證碼圖像，並傳送予該App；該App顯示該認證碼圖像，以供該持卡人藉由認證裝置首次設定該金融卡之密碼時使用；以及

該認證裝置藉由該顯示元件於該第一使用者介面顯示欄位，供該持卡人藉由該輸入元件輸入該認證碼以及該金融卡之新密碼，以完成首次密碼設定。

【0010】在本發明之部分具體實施例中，該密碼設定模組提供一第二使用者介面，供該金融卡之發卡方作業人員輸入該第一認證資料及該第二認證資料。

【0011】在本發明之部分具體實施例中，該App要求一啟動密碼。

【0012】在本發明之部分具體實施例中，該認證裝置的該第一使用者介面要求輸入認證碼及新密碼，以及該個人資訊的至少一部分，並基於所輸入的資料向該金融卡管理模組發送設定新密碼之請求。在特定具體實施例中，該金融卡管理模組確認接收到的認證碼及個人資料無誤後，取得經亂碼化的新密碼，並傳送予該認證裝置，供其藉由該金融卡讀寫元件寫入該經亂碼化的新密碼至該金融卡。

【0013】本發明之其他目的及優點一部分記載於下述說明中，或可透過本發明的實施例而理解。應了解前文之發明內容及下文之實施方式僅為例示性及闡釋性之說明，而非如申請專利範圍般限定本發明。

【圖式簡單說明】

【0014】 **圖1**係繪示本發明之一具體實施例之系統之方塊圖。

【0015】 **圖2**係繪示本發明之一具體實施例之方法之流程圖。

【實施方式】

【0016】 需注意的是，除非另有指明，所有在此處使用的技術性和科學性術語具有如同本發明所屬技術領域中之通常技術者一般所瞭解的意義。再者，本說明書所使用的「一」乙詞，如未特別指明，係指至少一個（一個或一個以上）之數量，合先說明。

【0017】 在一方面，本發明提供一種用於幫助持卡人首次設定金融卡密碼之系統。所述系統包含：一第一伺服器、一第二伺服器、一軟體產品（App）以及一認證裝置。

【0018】 該第一伺服器設有一密碼設定模組，其包括一儲存子模組。

【0019】 該第二伺服器係與該第一伺服器電性連接，並設有一金融卡管理模組。

【0020】 根據本發明之較佳具體實施例，該第一及第二伺服器係設於該金融卡的發卡方。

【0021】 該軟體產品（App）係與該第一伺服器通訊連接，並安裝於該持卡人所持有的一行動裝置，且該App係經該密碼設定模組認證。根據本發明，該行動裝置包括但不限於一平板電腦或一智慧型手機，且較佳為一智慧型手機。該行動裝置較佳不包括一筆記型電腦。所述通訊連接較佳為藉由一網際網路通訊

連接。根據本發明，該軟體產品較佳係為一行動軟體產品（mobile application）。根據本發明，該行動裝置可包含一儲存單元，儲存有該軟體產品之程式碼，以及一處理單元，用於執行該軟體產品之程式碼。

【0022】 該認證裝置係與該第二伺服器通訊連接，且其具有一顯示元件、一輸入元件及一金融卡讀寫元件。在本發明之部分具體實施例中，該認證裝置為一自動櫃員機或一自動存提款機。根據本發明，該認證裝置較佳係藉由一專屬網路與該第二伺服器通訊連接。

【0023】 在一預先註冊程序中，該密碼設定模組接收一第一認證資料及一第二認證資料，並將該第一及第二認證資料儲存於該儲存子模組。該第一認證資料係由該行動裝置的識別資訊以及該持卡人的個人資訊所組成，該第二認證資料則為一自選文摘。在該預先註冊程序中，該密碼設定模組可提供一第二使用者介面，以供該金融卡之發卡的方作業人員輸入該第一認證資料及該第二認證資料。前述識別資訊包含IMEI、UDID、鑰匙圈（Keychain）、MAC位址或其組合。該自選文摘可由該持卡人自行提供、或由該作業人員自該儲存子模組的資料庫中挑選、或由該密碼設定模組隨機自該儲存子模組的資料庫中挑選。

【0024】 該認證裝置藉由 該金融卡讀寫元件讀取該金融卡，並藉由該顯示元件提供一第一使用者介面，顯示首次設定金融卡密碼之選項，該選項經選擇後，該認證裝置向該金融卡管理模組發送首次設定金融卡密碼之請求。

【0025】 該金融卡管理模組將該首次設定金融卡密碼之請求傳送予該密碼設定模組。接著，該密碼設定模組執行以下步驟：(1) 根據一組合方法組合該第一認證資料，以產生一第一金鑰，其中，該組合方法係隨機挑選自複數個組合方法，並具有一第一編號；(2) 將該第一編號儲存於該儲存子模組；(3) 基於該第一金鑰對一原碼內容進行加密，產生一二維條碼，其中，該原碼內容包括該自選

文摘；以及(4) 將該二維條碼傳送予該認證裝置。根據本發明，所述組合方法包括但不限於：對該第一認證資料的單一欄位、或多個欄位的完整資料進行組合、或對該第一認證資料的多個欄位之部份資料進行組合、或對該第一認證資料的同一欄位資料進行多次組合。

【0026】 然後，該認證裝置會藉由該顯示元件於該第一使用者介面顯示該二維條碼。根據本發明的較佳具體實施例，該二維條碼為一QR碼。

【0027】 該App於啟動後會自動觸發一事件，要求輸入個人資訊及金融卡之帳號，並將輸入之個人資訊及帳號傳送予該密碼設定模組。根據本發明的較佳具體實施例，該App要求一啟動密碼，驗證啟動密碼為正確後才會啟動該App。所述啟動密碼包括但不限於：圖形密碼、按鍵式密碼、指紋辨識或臉部辨識。

【0028】 該密碼設定模組於確認該App合法性後，執行以下步驟：(1) 根據儲存在儲存子模組中的第一編號，使用對應的組合方法組合該第一認證資料，以產生一第二金鑰；(2) 自複數個加密方法中隨機挑選一加密方法，該加密方法具有一第二編號；以及，(3) 向該App傳送該第一編號，及基於該第二金鑰加密後的確認資料，該確認資料包括一加密資訊，其中，該加密資訊包括該第二編號，及一開始取樣位置。所述開始取樣位置係用於指示加密方法從該自選文摘的哪個位置的文字開始取樣進行加密。

【0029】 接著，該App自該行動裝置取得該行動裝置的識別資訊以及該持卡人的個人資訊，並根據該第一編號所對應的組合方法，組合所述識別資訊及個人資訊，以產生一第三金鑰。該持卡人的個人資訊可由該持卡人自行登錄並儲存於該行動裝置。

【0030】 經由該行動裝置掃描讀取顯示於該認證裝置的該顯示元件上的該二維條碼後，該App使用該第三金鑰解譯該二維條碼得到該原碼內容，並根據該第二編號所對應的加密方法及該開始取樣位置，對該自選文摘進行加密，得到

一加密值；然後，該App基於該第三金鑰對該加密值進行加密後傳送予該密碼設定模組。

【0031】該密碼設定模組則於確認該加密值的正確性後，向該金融卡管理模組發送取得認證碼之請求，並取得一認證碼；以及，產生一認證碼圖像，並傳送予該App。所述認證碼較佳為6至8碼的隨機數字，但不以此為限。在本發明之一具體實施例中，採用視覺密碼學理論方法對該認證碼加密產出所述認證碼圖像，使其明碼值需要人工以眼睛目視方式才能正確讀取。

【0032】接著，該App會顯示該認證碼圖像，以供該持卡人藉由認證裝置首次設定該金融卡之密碼時使用。

【0033】最後，該認證裝置藉由該顯示元件於該第一使用者介面顯示欄位，供該持卡人藉由該輸入元件輸入該認證碼以及該金融卡之新密碼，以完成首次密碼設定。

【0034】在本發明之部分具體實施例中，該認證裝置的該第一使用者介面要求輸入認證碼及新密碼，以及該個人資訊的至少一部分，並基於所輸入的資料向該金融卡管理模組發送設定新密碼之請求。在特定具體實施例中，該金融卡管理模組確認接收到的認證碼及個人資料無誤後，取得經亂碼化的新密碼，並傳送予該認證裝置，供其藉由該金融卡讀寫元件寫入該經亂碼化的新密碼至該金融卡。

【0035】另一方面，本發明提供一種用於幫助持卡人首次設定金融卡密碼之方法，包含：

提供一第一伺服器，設有一密碼設定模組，其包括一儲存子模組；一第二伺服器，與該第一伺服器電性連接，並設有一金融卡管理模組；一軟體產品（App），與該第一伺服器通訊連接，該App係安裝於該持卡人所持有的一行動

裝置，且該App係經該密碼設定模組認證；以及一認證裝置，與該第二伺服器通訊連接，該認證裝置具有一顯示元件、一輸入元件及一金融卡讀寫元件；

該密碼設定模組於一預先註冊程序中：接收一第一認證資料，其係由該行動裝置的識別資訊以及該持卡人的個人資訊所組成，並將該第一認證資料儲存於該儲存子模組；以及，接收一第二認證資料，其為一自選文摘，並將該第二認證資料儲存於該儲存子模組；

該認證裝置藉由該金融卡讀寫元件讀取該金融卡，並藉由該顯示元件提供一第一使用者介面，顯示首次設定金融卡密碼之選項，該選項經選擇後，該認證裝置向該金融卡管理模組發送首次設定金融卡密碼之請求；

該金融卡管理模組將該首次設定金融卡密碼之請求傳送予該密碼設定模組；

該密碼設定模組：根據一組合方法組合該第一認證資料，以產生一第一金鑰，其中，該組合方法係隨機挑選自複數個組合方法，並具有一第一編號；將該第一編號儲存於該儲存子模組；基於該第一金鑰對一原碼內容進行加密，產生一二維條碼，其中，該原碼內容包括該自選文摘；將該二維條碼傳送予該認證裝置；

該認證裝置藉由該顯示元件於該第一使用者介面顯示該二維條碼；

該App於啟動後自動觸發一事件，要求輸入個人資訊及金融卡之帳號，並將輸入之個人資訊及帳號傳送予該密碼設定模組；

該密碼設定模組於確認該App合法性後：根據儲存在儲存子模組中的第一編號，使用對應的組合方法組合該第一認證資料，以產生一第二金鑰；自複數個加密方法中隨機挑選一加密方法，該加密方法具有一第二編號；以及，向該App

傳送該第一編號，及基於該第二金鑰加密後的確認資料，該確認資料包括一加密資訊，其中，該加密資訊包括該第二編號，及一開始取樣位置；該App自該行動裝置取得該行動裝置的識別資訊以及該持卡人的個人資訊，並根據該第一編號所對應的組合方法，組合所述識別資訊及個人資訊，以產生一第三金鑰；

經由該行動裝置掃描讀取顯示於該認證裝置的該顯示元件上的該二維條碼後，該App使用該第三金鑰解譯該二維條碼得到該原碼內容，並根據該第二編號所對應的加密方法及該開始取樣位置，對該自選文摘進行加密，得到一加密值；以及，基於該第三金鑰對該加密值進行加密後傳送予該密碼設定模組；該密碼設定模組於確認該加密值的正確性後，向該金融卡管理模組發送取得認證碼之請求，並取得一認證碼；以及，產生一認證碼圖像，並傳送予該App；該App顯示該認證碼圖像，以供該持卡人藉由認證裝置首次設定該金融卡之密碼時使用；以及

該認證裝置藉由該顯示元件於該第一使用者介面顯示欄位，供該持卡人藉由該輸入元件輸入該認證碼以及該金融卡之新密碼，以完成首次密碼設定。

【0036】在該預先註冊程序中，該密碼設定模組可提供一第二使用者介面，以供該金融卡之發卡的方作業人員輸入該第一認證資料及該第二認證資料。前述識別資訊包含IMEI、UDID、鑰匙圈（Keychain）、MAC位址或其組合。該自選文摘可由該持卡人自行提供、或由該作業人員自該儲存子模組的資料庫中挑選、或由該密碼設定模組隨機自該儲存子模組的資料庫中挑選。

【0037】在本發明之部分具體實施例中，該App要求一啟動密碼。所述啟動密碼包括但不限於：圖形密碼、按鍵式密碼、指紋辨識或臉部辨識。

【0038】在本發明之部分具體實施例中，該認證裝置的該第一使用者介面要求輸入認證碼及新密碼，以及該個人資訊的至少一部分，並基於所輸入的資料向該金融卡管理模組發送設定新密碼之請求。在特定具體實施例中，該金融卡管理模組確認接收到的認證碼及個人資料無誤後，取得經亂碼化的新密碼，並傳送予該認證裝置，供其藉由該金融卡讀寫元件寫入該經亂碼化的新密碼至該金融卡。

【0039】現配合**圖1**及**圖2**說明本發明之幫助持卡人首次設定金融卡密碼之系統及方法的特定較佳具體實施例。

【0040】首先請參見**圖1**，所示為本發明之一具體實施例之幫助持卡人首次設定金融卡密碼之系統。在本具體實施例中，幫助持卡人首次設定金融卡密碼之系統**1**包含一第一伺服器**10**、一第二伺服器**20**、一軟體產品（App）**30**以及一認證裝置**40**。該軟體產品**30**可為一行動軟體產品，例如，金融業者發行之App。

【0041】該第一伺服器**10**設有一密碼設定模組**12**，其包括一儲存子模組**122**。該第二伺服器**20**係與該第一伺服器**10**電性連接，並設有一金融卡管理模組**22**。該第一及第二伺服器**10**及**20**可設於該金融卡的發卡方。

【0042】該App **30**係與該第一伺服器**10**通訊連接，並安裝於該持卡人所持有的一行動裝置**70**，且該App **30**係經該密碼設定模組**12**認證。該行動裝置**70**可為一平板電腦或一智慧型手機，較佳為一智慧型手機。

【0043】該認證裝置**40**藉由一專屬網路與該第二伺服器**20**通訊連接，且其具有一顯示元件**42**、一輸入元件**44**及一金融卡讀寫元件**46**。在部分實例中，該認證裝置**40**為一自動櫃員機或一自動存提款機。

【0044】 在一預先註冊程序中，該密碼設定模組**12**接收一第一認證資料及一第二認證資料，並將該第一及第二認證資料儲存於該儲存子模組**122**。該第一認證資料係由該行動裝置**70**的識別資訊以及該持卡人的個人資訊所組成，該第二認證資料則為一自選文摘。該文摘之位元數較佳係介於512位元至1024位元之間。

【0045】 該認證裝置**40**藉由該金融卡讀寫元件**46**讀取該金融卡，並藉由該顯示元件**42**提供一第一使用者介面，顯示首次設定金融卡密碼之選項，該選項經選擇後，該認證裝置**40**向該金融卡管理模組**22**發送首次設定金融卡密碼之請求。該金融卡管理模組**22**將該首次設定金融卡密碼之請求傳送予該密碼設定模組**12**。接著，該密碼設定模組**12**執行以下步驟：(1) 根據一組合方法組合該第一認證資料，以產生一第一金鑰，其中，該組合方法係隨機挑選自複數個組合方法，並具有一第一編號；(2) 將該第一編號儲存於該儲存子模組**122**；(3) 基於該第一金鑰對一原碼內容進行加密，產生一二維條碼，其中，該原碼內容包括該自選文摘；以及(4) 將該二維條碼傳送予該認證裝置**40**。

【0046】 然後，該認證裝置**40**會藉由該顯示元件**42**於該第一使用者介面顯示該二維條碼，其較佳為一QR碼。

【0047】 另外，該App **30**於啟動後會自動觸發一事件，要求輸入個人資訊及金融卡之帳號，並將輸入之個人資訊及帳號傳送予該密碼設定模組**22**。該密碼設定模組**22**於確認該App **30**的合法性後，執行以下步驟：(1) 根據儲存在儲存子模組**122**中的第一編號，使用對應的組合方法組合該第一認證資料，以產生一第二金鑰；(2) 自複數個加密方法中隨機挑選一加密方法，該加密方法具有一第二編號；以及，(3) 向該App **30**傳送該第一編號，及基於該第二金鑰加密後的確認資料，該確認資料包括一加密資訊，其中，該加密資訊包括該第二編號，及一開

始取樣位置，其係用於指示加密方法從該自選文摘的哪個位置的文字開始取樣進行加密。

【0048】 接著，該App **30**自該行動裝置取得該行動裝置**70**的識別資訊以及該持卡人的個人資訊，並根據該第一編號所對應的組合方法，組合所述識別資訊及個人資訊，以產生一第三金鑰。此時，該持卡人可使用該行動裝置**70**掃描讀取顯示於該認證裝置**40**的該顯示元件**42**上的該二維條碼，之後，該App **30**藉由該第三金鑰解譯該二維條碼得到該原碼內容，並根據該第二編號所對應的加密方法及該開始取樣位置，對該自選文摘進行加密，得到一加密值。然後，該App **30**基於該第三金鑰對該加密值進行加密後傳送予該密碼設定模組**12**。

【0049】 該密碼設定模組**12**於確認該加密值的正確性後，向該金融卡管理模組**22**發送取得認證碼之請求，取得一認證碼，並產生一認證碼圖像傳送予該App **30**。接著，該App **30**顯示該認證碼圖像，以供該持卡人藉由認證裝置**40**首次設定該金融卡之密碼時使用。

【0050】 最後，該認證裝置**40**藉由該顯示元件**42**於該第一使用者介面顯示欄位，供該持卡人藉由該輸入元件**44**輸入該認證碼以及該金融卡之新密碼，以完成首次密碼設定。

【0051】 另一方面，本發明提供一種幫助持卡人首次設定金融卡密碼之方法。請參見**圖2**，其為本發明之幫助持卡人首次設定金融卡密碼之方法的一具體實施例之流程圖。如圖所示，該方法包含下列步驟：（**S110**）提供一第一伺服器，設有一密碼設定模組，其包括一儲存子模組； 一第二伺服器，與該第一伺服器電性連接，並設有一金融卡管理模組；一軟體產品（App），與該第一伺服器通訊連接，該App係安裝於該持卡人所持有的一行動裝置，且該App係經該密碼設定模組認證；以及一認證裝置，與該第二伺服器通訊連接，該認證裝置具有一顯

示元件、一輸入元件及一金融卡讀寫元件；（**S120**）該密碼設定模組於一預先註冊程序中：接收一第一認證資料，其係由該行動裝置的識別資訊以及該持卡人的個人資訊所組成，並將該第一認證資料儲存於該儲存子模組；以及，接收一第二認證資料，其為一自選文摘，並將該第二認證資料儲存於該儲存子模組；（**S210**）該認證裝置藉由該金融卡讀寫元件讀取該金融卡，並藉由該顯示元件提供一第一使用者介面，顯示首次設定金融卡密碼之選項，該選項經選擇後，該金融卡管理模組確認該金融卡之狀態，接著向該金融卡管理模組發送首次設定金融卡密碼之請求；（**S220**）該金融卡管理模組將該首次設定金融卡密碼之請求傳送予該密碼設定模組；（**S230**）該密碼設定模組：根據一組合方法組合該第一認證資料，以產生一第一金鑰，其中，該組合方法係隨機挑選自複數個組合方法，並具有一第一編號；將該第一編號儲存於該儲存子模組；基於該第一金鑰對一原碼內容進行加密，產生一二維條碼，其中，該原碼內容包括該自選文摘；將該二維條碼傳送予該認證裝置；（**S240**）該認證裝置藉由該顯示元件於該第一使用者介面顯示該二維條碼；（**S310**）該App於啟動後自動觸發一事件，要求輸入個人資訊及金融卡之帳號，並將輸入之個人資訊及帳號傳送予該密碼設定模組；（**S320**）該密碼設定模組於確認該App合法性後：根據儲存在儲存子模組中的第一編號，以對應的組合方法組合該第一認證資料，以產生一第二金鑰；自複數個加密方法中隨機挑選一加密方法，該加密方法具有一第二編號；以及，向該App傳送該第一編號，及基於該第二金鑰加密後的確認資料，該確認資料包括一加密資訊，其中，該加密資訊包括該第二編號，及一開始取樣位置；（**S330**）該App自該行動裝置取得該行動裝置的識別資訊以及該持卡人的個人資訊，並根據該第一編號所對應的組合方法，組合所述識別資訊及個人資訊，以產生一第三金鑰；（**S340**）經

由該行動裝置掃描讀取顯示於該認證裝置的該顯示元件上的該二維條碼後，該App使用該第三金鑰解譯該二維條碼得到該原碼內容，並根據該第二編號所對應的加密方法及該開始取樣位置，對該自選文摘進行加密，得到一加密值；以及，基於該第三金鑰對該加密值進行加密後傳送予該密碼設定模組；（**S410**）該密碼設定模組於確認該加密值的正確性後，向該金融卡管理模組發送取得認證碼之請求，並取得一認證碼；以及，產生一認證碼圖像，並傳送予該App；（**S510**）該App顯示該認證碼圖像，以供該持卡人藉由認證裝置首次設定該金融卡之密碼時使用；以及（**S610**）該認證裝置藉由該顯示元件於該第一使用者介面顯示欄位，供該持卡人藉由該輸入元件輸入該認證碼以及該金融卡之新密碼，以完成首次密碼設定。

【0052】 本發明之幫助持卡人首次設定金融卡密碼之方法可配合或不配合前述之幫助持卡人首次設定金融卡密碼之系統**1**完成。

【0053】 藉由以下實例更詳細地描述本發明的具體實施方式，但本發明並不受限於其中提供的特定配置、條件及方法。

【0054】 實例1：前置作業

【0055】 金融業者提供一管理伺服器（第一伺服器），其安裝有密碼設定模組，供行員為申請辦理新金融卡的使用者（金融卡持卡人，在實例中以「使用者」稱之），註冊登錄所約定的認證資料，該註冊資料儲存於密碼設定模組的資料庫內。其相關交易功能及註冊內容如下：

【0056】 1. 綁定使用者行動裝置設備認證資料（第一認證資料）：

a. 登錄IMEI/UDID/Keychain/MAC/身份證號/生日/手機電話號碼/等認證資料。

此處可由辦理新金融卡的使用者先到金融業者之分行櫃檯或預先在官方網站，自所屬手機查得IMEI/UDID/Keychain/MAC等資料後填入申請表單，行員配合申請單填寫內容將資料登錄系統。前述認證資料可與使用者的身份證號綁定。

b. 第一認證資料之使用：

(1) 於綁定第一認證資料時，密碼設定模組當下自動隨機亂數指定其組合方法之初始值，並將該組合方法儲存於資料庫（3個Bytes）。

(2) 該組合方法係用於將IMEI/UDID/Keychain/MAC/身份證號/生日/手機電話號碼/等欄位資料做隨機組合。

(3) 在資料庫儲存的「組合方法」（3個Bytes），實質是個數字，資料庫不儲存經組合後的資料原始內容。此處資料庫儲存的「組合方法」值，僅為一個初始值，密碼設定模組於每次受理請求須產出二維條碼（在本實例中為QR碼）之前，應重新自動隨機亂數產出「組合方法」值，以新的「組合方法」值更新資料庫該欄值。

(4) 經組合後的資料原始內容，後續以「Current_key」（此處為第一金鑰）稱之，其長度應至少128個Bytes。此「Current_key」即為後續欲對敏感性資料以進階加密標準（AES）加密時的金鑰。欲知Current_key需先知它的「組合方法」以及其相對應程式碼，當原註冊登錄綁定的第一認證資料外洩時，亦未直接暴露該使用者的Current_key內容。

【0057】 2. 綁定使用者識別資料（第二認證資料）：

行員為申辦新金融卡的使用者登錄自選文摘1則（512 Bytes≦ 文摘 ≦1024 Bytes）。第二認證資料亦可與使用者的身份證號綁定。該自選文摘可由使用者提供、或由行員、或由系統隨機自資料庫為使用者挑選。

a. 系統產出 QR 碼的內容：系統依據資料庫儲存該使用者的「組合方法」，以使用者原始綁定之行動裝置認證資料產出「Current_key」，再使用相

對應加解密程式碼以「Current_key」AES(網頁識別碼 + 自選文摘 + SHA-256(「Current_key」))加密產出 QR 碼亂碼化後之內容。欲知 QR 碼原碼內容，唯有使用正確的交易裝置掃描讀取 QR 碼、以正確的「組合方法」產出正確的「Current_key」，以相對應加解密程式碼才能解譯出 QR 碼的原碼內容。

(1) 解譯後 QR 碼原碼內容 =網頁識別碼 +自選文摘 + SHA-256(Current_key)。

(2) 解譯前 QR 碼內容 =以「Current_key」AES(網頁識別碼 +自選文摘 + SHA-256(Current_key))。

(3) QR 碼原碼內容需要經由「組合方法」之相對應加解密程式碼篩選處理產出「Current_key」內容之後，始能據之解譯出來。

b. 系統產出 QR 碼的時機：金融卡持卡人在自動存提款機操作特定交易，於上行電文經由金融卡管理模組對密碼設定模組發動交易當下密碼設定模組產出包含「QR 碼圖像」的下行電文回覆給金融卡管理模組；密碼設定模組另須將該上行電文內容等資訊儲存於資料庫：

(1) 上行電文內容包括：金融卡帳號、交易日期、交易時間、ATM 機號、ATM 交易序號等資料。

(2) 以身份證號、網頁識別碼等值作為金鑰，將該上行電文內容儲存於密碼設定模組的資料庫（儲存子模組）。網頁識別碼為密碼設定模組、「初始密碼應用程式」（軟體產品（App））、金融卡管理模組等多方系統針對同一請求交易的共同識別序號，網頁識別碼值由初始密碼函系統（密碼設定模組）產生。網頁識別碼值生命週期，於

金融卡系統（金融卡管理模組）向初始密碼函系統發動「QR 碼圖像」請求時產生、於初始密碼應用程式取得認證碼值圖像、持卡人操作自動存提款機（認證裝置）特定功能完成金融卡新密碼設定後結束。

(3) 將上行電文內容儲存於資料庫的目的： (i) 供後續交易裝置之初始密碼應用程式於讀取「QR 碼圖像」之後，對初始密碼函系統發動取得認證碼請求交易時，初始密碼函系統將之做為對交易勾稽核驗之用； (ii) 當資料庫無該金融卡帳號資料時，拒絕該交易需求，要求金融卡持卡人先持新申請金融卡操作自動存提款機，於自動存提款機介面顯示「QR 碼圖像」後，再操作執行 App；及 (iii) 當資料庫有該金融卡帳號資料，但已逾時（例如，10 分鐘以上），則可拒絕該 App 之交易請求。

【0058】 使用者於前述作業註冊資料完成後，即可操作交易裝置，從網路環境（Internet）下載/安裝「初始密碼應用程式」（軟體產品（App）），於完成安裝作業後，始告前置作業完成：

【0059】 1. App須強制提供圖形密碼、按鍵式密碼、指紋辨識、或臉部辨識等選項，供使用者設定App的啟動密碼。

【0060】 2. 使用者於每次執行該App時，App須要求使用者輸入使用者身份證號、生日、及金融卡帳號，並即時發送上行電文給密碼設定模組完成初步鑑別使用者身份。

a. 上行電文內容需包含身份證號、生日、金融卡帳號、及App的版號、日期等資訊。

b. 伺服器端的密碼設定模組鑑別使用者身份及其行動裝置設備無誤之後，須儲存該App的版號、日期、本次申請金融卡帳號等上行電文資訊，供未來在交易作業階段鑑別App合法性之用。

c. 該「金融卡帳號」須為新申請且尚未變更金融卡初始密碼之金融卡帳號。

【0061】 3. 初始密碼應用程式於取得初始密碼函系統下行電文回覆鑑別無誤之後，即直接顯示讀取QR碼的準備畫面於交易裝置（使用者之個人裝置）介面，等待使用者人工操作交易裝置，對準顯示在自動存提款機上的「QR碼圖像」，掃描讀取QR碼內容。

【0062】 實例2：交易作業

【0063】 1. 使用者以新申請實體金融卡插入自動存提款機（認證裝置）並操作特定交易，自動存提款機隨即發動上行電文，經由金融卡系統主機（第二伺服器）傳遞到初始密碼函系統主機（第一伺服器），初始密碼函系統（密碼設定模組）除了將該上行電文內容儲存於資料庫（儲存子模組）外，並產出、回覆「QR碼圖像」等下行電文資料，經金融卡系統（金融卡管理模組）將「QR碼圖像」等下行電文資料回覆給自動存提款機；自動存提款機將「QR碼」顯示於自動存提款機介面。

a. 較佳地，禁止使用者同時在多部自動存提款機操作多張新申請金融卡交易。

b. 初始密碼函系統以身份證號、網頁識別碼等值作為金鑰將上行電文內容儲存於資料庫。

(1) 該金融卡帳號須為新申請且尚未變更金融卡初始密碼之金融卡帳號。

(2) 網頁識別碼為初始密碼函系統、初始密碼應用程式（App）、金融卡系統等多方系統針對同一請求交易的共同識別序號，網頁識別碼值由初始密碼函系統產生。網頁識別碼值生命週期，於金融卡系統向初始密碼函系統發動「QR 碼圖像」請求時產生、於初始密碼應用程式（App）取得認證碼值圖像、及完成金融卡新密碼設定後結束。

c. 初始密碼函系統將上行電文內容儲存於資料庫之目的：

(1) 供後續使用者啟動交易裝置之初始密碼 APP，於登錄身份資料後，供初始密碼函系統確認使用者是否已先以新申請實體金融卡插入自動存提款機，完成操作特定交易，取得「QR 碼圖像」。

(2) 供後續交易裝置之初始密碼應用程式於掃描讀取「QR 碼圖像」之後、對初始密碼函系統發動取得認證碼請求交易時，初始密碼函系統將之做為對交易勾稽核驗之用。

(a) 當資料庫無該金融卡帳號資料時，拒絕 App 的交易需求，要求金融卡持卡人先持新申請金融卡操作自動存提款機，於自動存提款機介面顯示「QR 碼圖像」後，再操作執行 App。

(b) 當資料庫有該金融卡帳號資料、但已逾時（例如，10 分鐘以上），同前述說明拒絕 App 之交易需求。

d. 初始密碼函系統於當下須先自動隨機亂數產出「組合方法」值並更新資料庫該欄值，之後，以該「組合方法」值執行其相對應程式碼（將原登錄綁定行動裝置認證資料做組合），產出組合後的資料原始內容即為「Current_key」（第一金鑰）。前述「組合方法」值於交易當下隨機亂數產出，此隨機亂數值較佳係異於前三次記錄。

e. 初始密碼函系統於當下再以該「Current_key」、以及使用者所綁定的識別資料（自選文摘），產出 QR 碼內容、「QR 碼圖像」、以及下行電文等資料（含「QR 碼圖像」）。

(1) QR 碼原碼內容 = 網頁識別碼 +自選文摘 + SHA-256(Current_key)。

(2) QR 碼亂碼內容 = 「QR 碼圖像」內容 = 以「Current_key」AES(網頁識別碼 +自選文摘 + SHA-256(Current_key)) ，其中，SHA-256 為一雜湊函式。

(3) 欲解譯 QR 碼原碼內容，需先經「組合方法」之相對應程式碼產出「Current_key」內容，之後，始能以「Current_key」解譯出 QR 碼原碼內容。

f.「QR 碼圖像」等下行電文資料，經金融卡系統回覆給自動存提款機之後；自動存提款機即將「QR 碼圖像」顯示於自動存提款機介面，供後續使用者人工手持交易裝置（行動裝置）掃描讀取 QR 碼內容。

g. 金融卡系統應檢核上行電文內容，若不符合條件，應拒絕該交易請求：

(1) 確認該金融卡為有效卡、而且初始密碼尚未被變更完成。

(2) 確認該金融卡持卡人已經綁定行動裝置設備認證資料及使用者識別資料。

【0064】 2. 使用者在交易裝置介面登入「啟動密碼」後啟動如實例1之App，App要求使用者輸入身份鑑別資訊：

a. App於個人裝置介面顯示訊息，要求輸入使用者身份證號、生日、及金融卡帳號。

b. 上行電文關鍵內容包括：身份證號、生日、金融卡帳號、以及安裝該 App 之版號與日期等資訊。

c. 上行電文訊息經防火牆（Web AP F/W）解譯SSL加密內容後傳遞給密碼設定模組主機。

d. 密碼設定模組依據上行電文訊息審核該使用者所安裝App的合法性、以及確認使用者是否已先以新申請實體金融卡插入自動存提款機操作特定交易。

(1) 以身份證號、網頁識別碼等值作為金鑰查詢資料庫，當資料庫無該帳號資料時，拒絕 App 的交易需求，要求金融卡持卡人先持新申請金融卡操作自動存提款機，於自動存提款機介面顯示「QR Code 圖像」後，再操作執行 App。

(2) 當資料庫有該帳號資料、但已逾時（例如，10 分鐘以上)，同前述說明拒絕 App 之交易需求。

(3) 於鑑別使用者身份（身份證號、生日）不符合時，密碼設定模組須同步透過簡訊、電子郵件等通報持卡人。於累積錯誤次數超過 4 次時，系統應拒絕交易，並請使用者聯繫客服人員審核使用者身份之後重設累積錯誤次數。

e. 密碼設定模組審核上行電文訊息無誤後，產出下行電文回覆App：

(1) 系統依據資料庫儲存該使用者的「組合方法」，以使用者原始綁定之行動裝置認證資料產出「Current_key」（第二金鑰）。

(2) 下行電文關鍵內容 = 網頁識別碼 + 組合方法 + 以「Current_key」AES(加密方法 + SHA-256(「Current_key」（第二金鑰）)) + App 合法性鑑別結果，其中，SHA-256 為一雜湊函式。

(a)「加密方法」欄共計10個Bytes，前3個Bytes放置產出「Current_key」的「組合方法」、第4～6個Bytes放置當次加密方法項目、末4個Bytes放置當次加密時「自選文摘」的開始取樣位置。

(b) 上述「加密方法」值及「開始取樣位置」值均於交易當下隨機亂數產出，此隨機亂數值較佳係異於前三次記錄。

f. 將前述上行電文及下行電文內容儲存於密碼設定模組的資料庫，供後續交易鑑別勾稽使用者身份之用。

【0065】 3. App於收到密碼設定模組的下行電文後：

a. 當下行電文內容之「App合法性鑑別結果」值是成功時，依據下行電文之「組合方法」值（下行電文之「加密方法」欄的前3個Bytes值），自使用者的行動裝置取得該裝置資料（包含IMEI/UDID/ Keychain/MAC等資訊），以及該使用者的個人資訊（身份證號/生日等資訊，可由該使用者自行登錄並儲存於該行動裝置），以 產出「Current_key」（第三金鑰）（亦即，該App內建有複數個組合方法，可依據所接獲的編號來確定使用的組合方法），一來對下行電文之「加密方法」欄做解密，取得當次「加密方法」明碼值；二來鑑別下行電文之SHA-256 (「Current_key」)欄值的一致性（鑑別當下App所連結之密碼設定模組主機的合法性）。

b. App於交易裝置介面顯示可掃描讀取QR碼的環境，指示持卡人持交易裝置對自動存提款機的「QR碼圖像」掃描讀取其內容。

c. App掃描讀取「QR碼圖像」，並解譯其原始內容：

(1) 使用上述「Current_key」（第三金鑰）解譯「QR 碼圖像」之原始內容。

(a) QR碼原碼內容=網頁識別碼 + 自選文摘 + SHA-256

(「Current_key」)。

(b) QR 碼亂碼內容=「QR 碼圖像」內容 = 以「Current_key」

AES(網頁識別碼 +自選文摘 + SHA-256(Current_key))

(2) 解譯後再以交易裝置本機產出的 Current_key 驗證該 QR 碼內容之 SHA-256(「Current_key」)值的一致性（鑑別當下該「QR 碼圖像」的合法性）。

d. 再次產出上行電文，對初始密碼函系統發動請求取得使用者認證碼值：

(1) 上行電文關鍵內容 = 網頁識別碼 + Mobile 值 + Verify 值 + 前述各步驟上下行電文的部份資料。

(a) Mobile值 = SHA-256(從交易裝置本機產出的「Current_key」

(b) Verify值 = 以「Current_key」AES{(依加密方法對「解譯後的QR碼內容」內容做加密) + SHA-256(「解譯後的QR碼內容)} 。此處的「解譯後的QR碼內容」係指經解譯後的「自選文摘」原始內容。App依據前述下行電文取得的「加密方法」值，以所指定「自選文摘」的「開始取樣位置」值做開始取樣、以所指定的「加密方法」編號值執行對應的加密用程式碼，經加密後產出x值，其長度應至少128個Bytes。之後，再以「Current_key」（第三金鑰）AES加密保護該x值以及相關雜湊函數值。

(2) App 將本次上行電文經 SSL 加密後，傳送給初始密碼函系統主機。

【0066】 4. 密碼設定模組於收到App的上行電文（請求取得認證碼）後：

a. 依據該使用者本次交易資訊，檢核App的本次上行電文內容，鑑別該行動裝置設備內容（IMEI/UDID/Keychain/MAC）、該使用者的個人資訊（身份證號/生日）等資料的合法性、以及所安裝App的正確性，從而達到鑑別使用者身份的目的。

b. 於鑑別使用者身份不符合時，密碼設定模組須同步透過簡訊、電子郵件等通報持卡人。於累積錯誤次數超過4次時，系統應拒絕交易，並請使用者聯繫客服人員審核使用者身份之後重設累積錯誤次數。

c. 於鑑別使用者身份符合後，密碼設定模組產出上行電文內容，向金融卡系統主機（第二伺服器）發動請求取得當次認證碼值。

(1) 上行電文內容包括：網頁識別碼、金融卡帳號、交易日期、交易時間、ATM 機號、ATM 交易序號、認證碼值（此處為空白值）等資料。

(2) 金融卡系統（金融卡管理模組）核驗上行電文無誤後，隨機產出「認證碼值」並回覆給密碼設定模組。

(a)「認證碼」係為後續供持卡人以新申請實體金融卡插入自動存提款機（認證裝置）並操作特定交易、完成金融卡新密碼設定作業時，做為金融卡系統對持卡人身份鑑別之用。

(b) 金融卡管理模組每次動態隨機產出的「認證碼」，有效期10分鐘、認證碼值為6~8碼隨機數字。

(c) 金融卡管理模組儲存此交易需求內容，供後續持卡人以新申請實體金融卡插入自動存提款機並操作特定交易、完成金融卡新密碼設定作業時，做為金融卡系統對持卡人身份鑑別之用。

d. 密碼設定模組於收妥認證碼值後，先採「視覺密碼學理論方法」對金融卡初始密碼值明碼 產出「認證碼值圖像」，之後再產出下行電文（含加密後認證碼值圖像），經SSL加密後回覆給App。

(1) 採「視覺密碼學理論方法」加密產出「認證碼值圖像」：

(a) 步驟一：隨機取得底圖或底色

(b) 步驟二：在背景產製數條干擾線(線條顏色、粗細、長短、位置均隨機產生)

(c) 步驟三：產製數字(隨機數字顏色、字體、字形、向不同方向(PIXEL)移位產製多

次相同數字)

(d) 步驟四：在前景產製數條干擾線(線條顏色、粗細、長短、位置均隨機產生)

(e) 步驟五：產生JPEG圖檔

(f) 經此方法將密碼值明碼做妥適加密保護之後，該圖像之明碼值需要人工以眼睛目視方式才能正確讀取。

(2) 下行電文關鍵內容：網頁識別碼、認證碼值圖像、App 合法性鑑別結果等資料。

(3) 密碼設定模組更新資料庫之該使用者本次交易處理狀況與身份鑑別結果等資訊。

(4) 本次下行電文內容除了包含認證碼值圖像，另應包含通知持卡人儘速在限時內（例如，10 分鐘） 操作自動存提款機特定功能完成金融卡新密碼設定。

(5) 密碼設定模組須同步透過簡訊、電子郵件通知持卡人：認證碼值完成交付，請持卡人儘速在限時內操作自動存提款機特定功能完成金融卡新密碼設定等訊息。

【0067】 5. App於收到密碼設定模組的下行電文（含認證碼值圖像）後：

a. 顯示認證碼值圖像於個人裝置介面。

b. 顯示通知持卡人儘速在限時內操作自動存提款機特定功能完成金融卡新密碼設定等訊息於個人裝置介面。

c. App將本筆交易選擇重點資料儲存於個人裝置設備端的加密型檔案。該檔案採先進先出法，最多儲存十筆交易記錄軌跡。

【0068】 6. 使用者（持卡人）於取得認證碼後，須在限時內，以新申請實體金融卡插入自動存提款機（認證裝置）並操作特定交易，完成金融卡新密碼的設定作業。

a. 認證裝置的特定交易功能：

(1) 該特定交易功能係參照現行分行櫃檯「金融卡重設密碼」交易功能（非金融卡密碼變更交易），供持卡人以新申請實體金融卡插入自動存提款機、在自動存提款機介面輸入當次認證碼值、以及自行設定的金融卡新密碼值，完成金融卡新密碼的設定作業。

(2) 特定交易功能資料處理流程：

(a) 特定交易功能連線呼叫實體金融卡晶片內軟體，請其隨機產出一組亂數。

(b) 產出上行電文，向金融卡管理模組發動產出該金融卡新密碼值請求。上行電文關鍵資料：金融卡帳號、認證碼、金融卡新密碼、金融卡晶片軟體當次產出之亂數值等資料。

(c) 金融卡管理模組審核上行電文無誤後，連線呼叫實體亂碼化設備（Hardware DES）產出經亂碼化後的金融卡新密碼值。

(d) 金融卡管理模組產出下行電文（內含「經亂碼化後的金融卡新密碼值」）回覆給自動存提款機特定交易功能。

(e) 特定交易功能連線呼叫實體金融卡晶片內軟體，請其解鎖卡片、以及寫入「經亂碼化後的金融卡新密碼值」至晶片。

b. 金融卡管理模組每次動態隨機產出的「認證碼」，其具有特定有效時限，持卡人須在限時內)完成設定金融卡新密碼。

c. 當該金融卡已完成新密碼設定作業，自動存提款機應拒絕持卡人重覆執行特定交易功能。

【0069】 7. 當使用者（持卡人）忘記認證碼值時，使用者須重新執行交易作業（上述步驟1.～6.）的完整程序，以取得新的認證碼值。

【0070】 8. 當使用者（持卡人）未能在限時內從自動存提款機完成金融卡新密碼設定時，當次認證碼將逾時失效，使用者須重新執行交易作業（上述步驟1.～6.）的完整程序，以取得新的認證碼值。

【0071】 綜上所述，本發明在交易裝置（行動裝置設備）及認證裝置（自動存提款機）兩個實體裝置相互分離下，藉由持卡人以人工操作行動裝置，對準顯示在自動存提款機介面的「QR碼圖像」做掃描讀取，促使兩個實體裝置分工處理同一筆交易請求，限時限次的完成身份勾稽暨鑑別程序，讓持卡人可及時手

持金融卡在自動存提款機操作完成金融卡新密碼的設定作業。此等多因子交易安全模式，不僅符合主管機關對於交易安全設計應具使用「兩項（含）以上技術」的要求、更可確保該電子交易為人工操作完成，完全防範木馬程式自遠端操控交易的風險。

【0072】本發明係採二階段身份鑑別模式（包含對使用者個資資料、對所綁定的交易裝置認證資料及使用者識別資料、對交易是否為人工操作），有別於往常以「密碼」為唯一鑑別模式，對於使用者身份鑑別的交易安全門檻，可收到全面性的、實質性的強化效果。

【0073】本發明之交易框架的操作行為，需要使用者手持實體金融卡片插入自動存提款機取得「QR碼圖像」、需要使用者手持已綁定的實體行動裝置掃描讀取「QR碼圖像」。縱使交易裝置被植入遠端操控型（monitoring remote programs）木馬程式，駭客仍無法自遠端操控完成上述人工操作行為來取得認證碼值。

【0074】對於使用者而言，可排除紙本密碼函之相關保管、遺失、遭竊的負擔與風險。對於歹徒、駭客而言，需要同時取得使用者的實體金融卡、綁定的實體行動裝置、App的「啟動密碼」以及使用者個資之後，才有機會取得認證碼值 ，並需在限時內完成金融卡新密碼的設定作業。較諸往常只要取得紙本密碼函及實體金融卡後就可犯案，其防範門檻已明顯提昇。

【0075】對於金融機構而言，本發明除了確保資訊安全門檻提昇外，可為金融機構取代現行人工操作列印密碼函的繁瑣程序，節省其間配套的相關人工作業、環境設施、列印機器、紙張、郵遞、保管儲存、資安控管及風險稽查等等作業成本負擔，並能達到節能減碳的效果。

【符號說明】

【0076】

1	用於幫助持卡人首次設定金融卡密碼之系統
10	第一伺服器
12	密碼設定模組
122	儲存子模組
20	第二伺服器
22	金融卡管理模組
30	軟體產品
40	認證裝置
42	顯示元件
44	輸入元件
46	金融卡讀寫元件
70	行動裝置
S110~S610	步驟流程

【生物材料寄存】無

【發明申請專利範圍】

【第1項】一種用於幫助持卡人首次設定金融卡密碼之系統，包含：

一第一伺服器，設有一密碼設定模組，其包括一儲存子模組；

一第二伺服器，與該第一伺服器電性連接，並設有一金融卡管理模組；

一軟體產品（App），與該第一伺服器通訊連接，該App係安裝於該持卡人所持有的一行動裝置，且該App係經該密碼設定模組認證；以及

一認證裝置，與該第二伺服器通訊連接，該認證裝置具有一顯示元件、一輸入元件及一金融卡讀寫元件；

其中：

該密碼設定模組於一預先註冊程序中：接收一第一認證資料，其係由該行動裝置的識別資訊以及該持卡人的個人資訊所組成，並將該第一認證資料儲存於該儲存子模組；以及，接收一第二認證資料，其為一自選文摘，並將該第二認證資料儲存於該儲存子模組；

該認證裝置藉由該金融卡讀寫元件讀取該金融卡，並藉由該顯示元件提供一第一使用者介面，顯示首次設定金融卡密碼之選項，該選項經選擇後，該認證裝置向該金融卡管理模組發送首次設定金融卡密碼之請求；

該金融卡管理模組將該首次設定金融卡密碼之請求傳送予該密碼設定模組；

該密碼設定模組：根據一組合方法組合該第一認證資料，以產生一第一金鑰，其中，該組合方法係隨機挑選自複數個組合方法，並具有一第一編號；將該第一編號儲存於該儲存子模組；基於該第一金鑰對一原碼內容進行加密，產生

一二維條碼，其中，該原碼內容包括該自選文摘；將該二維條碼傳送予該認證裝置；

該認證裝置藉由該顯示元件於該第一使用者介面顯示該二維條碼；

該App於啟動後自動觸發一事件，要求輸入個人資訊及金融卡之帳號，並將輸入之個人資訊及帳號傳送予該密碼設定模組；

該密碼設定模組於確認該App合法性後：根據儲存在儲存子模組中的第一編號，使用對應的組合方法組合該第一認證資料，以產生一第二金鑰；自複數個加密方法中隨機挑選一加密方法，該加密方法具有一第二編號；以及，向該App傳送該第一編號，及基於該第二金鑰加密後的確認資料，該確認資料包括一加密資訊，其中，該加密資訊包括該第二編號，及一開始取樣位置；

該App自該行動裝置取得該行動裝置的識別資訊以及該持卡人的個人資訊，並根據該第一編號所對應的組合方法，組合所述識別資訊及個人資訊，以產生一第三金鑰；

經由該行動裝置掃描讀取顯示於該認證裝置的該顯示元件上的該二維條碼後，該App使用該第三金鑰解譯該二維條碼得到該原碼內容，並根據該第二編號所對應的加密方法及該開始取樣位置，對該自選文摘進行加密，得到一加密值；以及，基於該第三金鑰對該加密值進行加密後傳送予該密碼設定模組；

該密碼設定模組於確認該加密值的正確性後，向該金融卡管理模組發送取得認證碼之請求，並取得一認證碼；以及，產生一認證碼圖像，並傳送予該App；該App顯示該認證碼圖像，以供該持卡人藉由認證裝置首次設定該金融卡之密碼時使用；以及

該認證裝置藉由該顯示元件於該第一使用者介面顯示欄位，供該持卡人藉由該輸入元件輸入該認證碼以及該金融卡之新密碼，以完成首次密碼設定。

【第2項】 如請求項1之用於幫助持卡人首次設定金融卡密碼之系統，其中該密碼設定模組提供一第二使用者介面，供該金融卡之發卡方作業人員輸入該第一認證資料及該第二認證資料。

【第3項】 如請求項1之用於幫助持卡人首次設定金融卡密碼之系統，其中該App要求一啟動密碼。

【第4項】 如請求項1之用於幫助持卡人首次設定金融卡密碼之系統，其中該認證裝置的該第一使用者介面要求輸入認證碼及新密碼，以及該個人資訊的至少一部分，並基於所輸入的資料向該金融卡管理模組發送設定新密碼之請求。

【第5項】 如請求項4之用於幫助持卡人首次設定金融卡密碼之系統，其中該金融卡管理模組確認接收到的認證碼及個人資料無誤後，取得經亂碼化的新密碼，並傳送予該認證裝置，供其藉由該金融卡讀寫元件寫入該經亂碼化的新密碼至該金融卡。

【第6項】 一種用於幫助持卡人首次設定金融卡密碼之方法，包含：

提供一第一伺服器，設有一密碼設定模組，其包括一儲存子模組；一第二伺服器，與該第一伺服器電性連接，並設有一金融卡管理模組；一軟體產品（App），與該第一伺服器通訊連接，該App係安裝於該持卡人所持有的一行動裝置，且該App係經該密碼設定模組認證；以及一認證裝置，與該第二伺服器通訊連接，該認證裝置具有一顯示元件、一輸入元件及一金融卡讀寫元件；

該密碼設定模組於一預先註冊程序中：接收一第一認證資料，其係由該行動裝置的識別資訊以及該持卡人的個人資訊所組成，並將該第一認證資料儲存於該儲存子模組；以及，接收一第二認證資料，其為一自選文摘，並將該第二認證資料儲存於該儲存子模組；

該認證裝置藉由該金融卡讀寫元件讀取該金融卡，並藉由該顯示元件提供一第一使用者介面，顯示首次設定金融卡密碼之選項，該選項經選擇後，該認證裝置向該金融卡管理模組發送首次設定金融卡密碼之請求；

該金融卡管理模組將該首次設定金融卡密碼之請求傳送予該密碼設定模組；

該密碼設定模組：根據一組合方法組合該第一認證資料，以產生一第一金鑰，其中，該組合方法係隨機挑選自複數個組合方法，並具有一第一編號；將該第一編號儲存於該儲存子模組；基於該第一金鑰對一原碼內容進行加密，產生一二維條碼，其中，該原碼內容包括該自選文摘；將該二維條碼傳送予該認證裝置；

該認證裝置藉由該顯示元件於該第一使用者介面顯示該二維條碼；

該App於啟動後自動觸發一事件，要求輸入個人資訊及金融卡之帳號，並將輸入之個人資訊及帳號傳送予該密碼設定模組；

該密碼設定模組於確認該App合法性後：根據儲存在儲存子模組中的第一編號，使用對應的組合方法組合該第一認證資料，以產生一第二金鑰；自複數個加密方法中隨機挑選一加密方法，該加密方法具有一第二編號；以及，向該App傳送該第一編號，及基於該第二金鑰加密後的確認資料，該確認資料包括一加密資訊，其中，該加密資訊包括該第二編號，及一開始取樣位置；

該App自該行動裝置取得該行動裝置的識別資訊以及該持卡人的個人資訊，並根據該第一編號所對應的組合方法，組合所述識別資訊及個人資訊，以產生一第三金鑰；

經由該行動裝置掃描讀取顯示於該認證裝置的該顯示元件上的該二維條碼後，該App使用該第三金鑰解譯該二維條碼得到該原碼內容，並根據該第二編號所對應的加密方法及該開始取樣位置，對該自選文摘進行加密，得到一加密值；以及，基於該第三金鑰對該加密值進行加密後傳送予該密碼設定模組；該密碼設定模組於確認該加密值的正確性後，向該金融卡管理模組發送取得認證碼之請求，並取得一認證碼；以及，產生一認證碼圖像，並傳送予該App；該App顯示該認證碼圖像，以供該持卡人藉由認證裝置首次設定該金融卡之密碼時使用；以及

該認證裝置藉由該顯示元件於該第一使用者介面顯示欄位，供該持卡人藉由該輸入元件輸入該認證碼以及該金融卡之新密碼，以完成首次密碼設定。

【第7項】 如請求項6之幫助持卡人首次設定金融卡密碼之方法，其中該密碼設定模組提供一第二使用者介面，供該金融卡之發卡方作業人員輸入該第一認證資料及該第二認證資料。

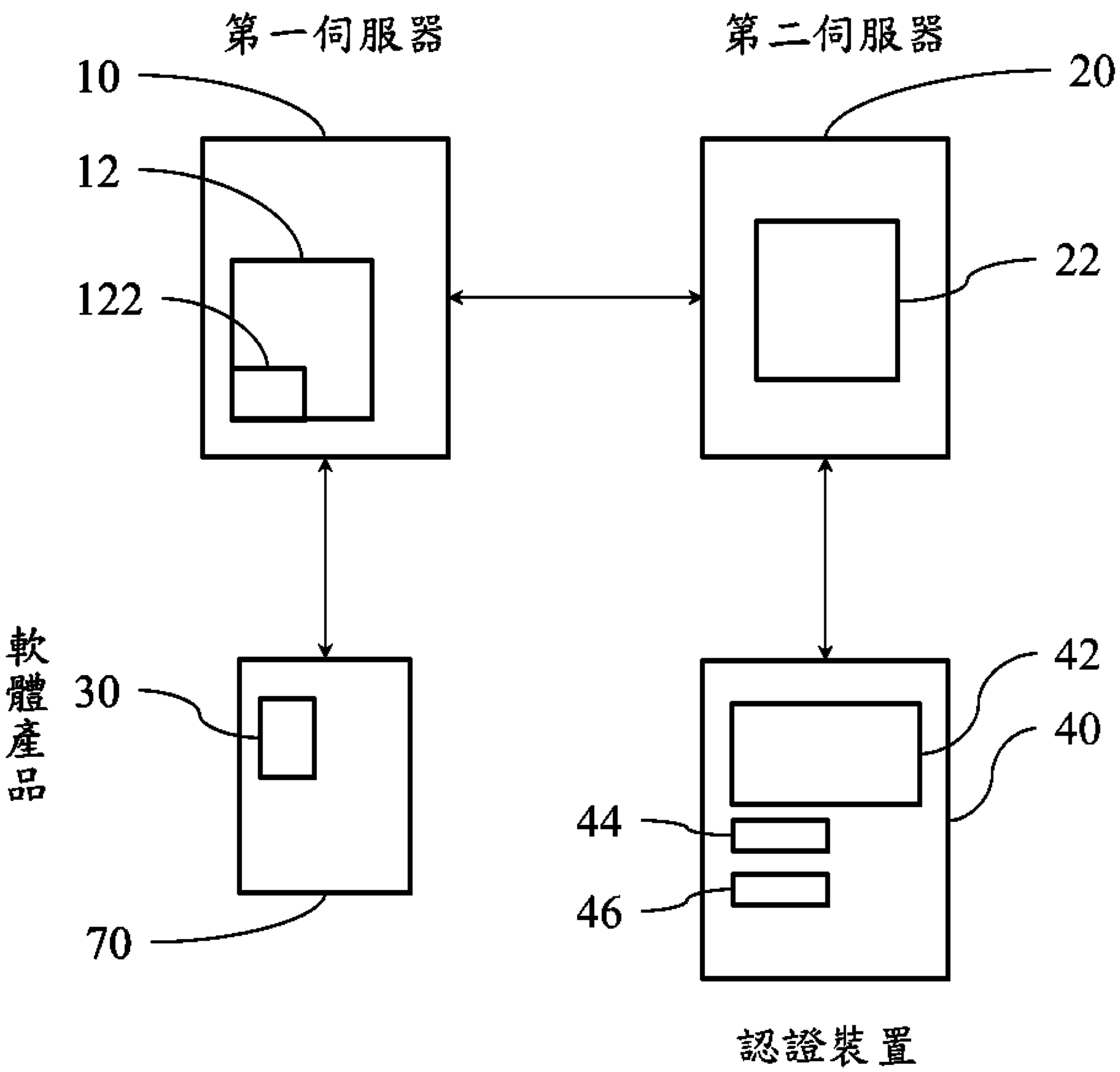
【第8項】 如請求項6之用於幫助持卡人首次設定金融卡密碼之方法，其中該App要求一啟動密碼。

【第9項】 如請求項6之用於幫助持卡人首次設定金融卡密碼之方法，其中該認證裝置的該第一使用者介面要求輸入認證碼及新密碼，以及該個人資訊的至少一部分，並基於所輸入的資料向該金融卡管理模組發送設定新密碼之請求。

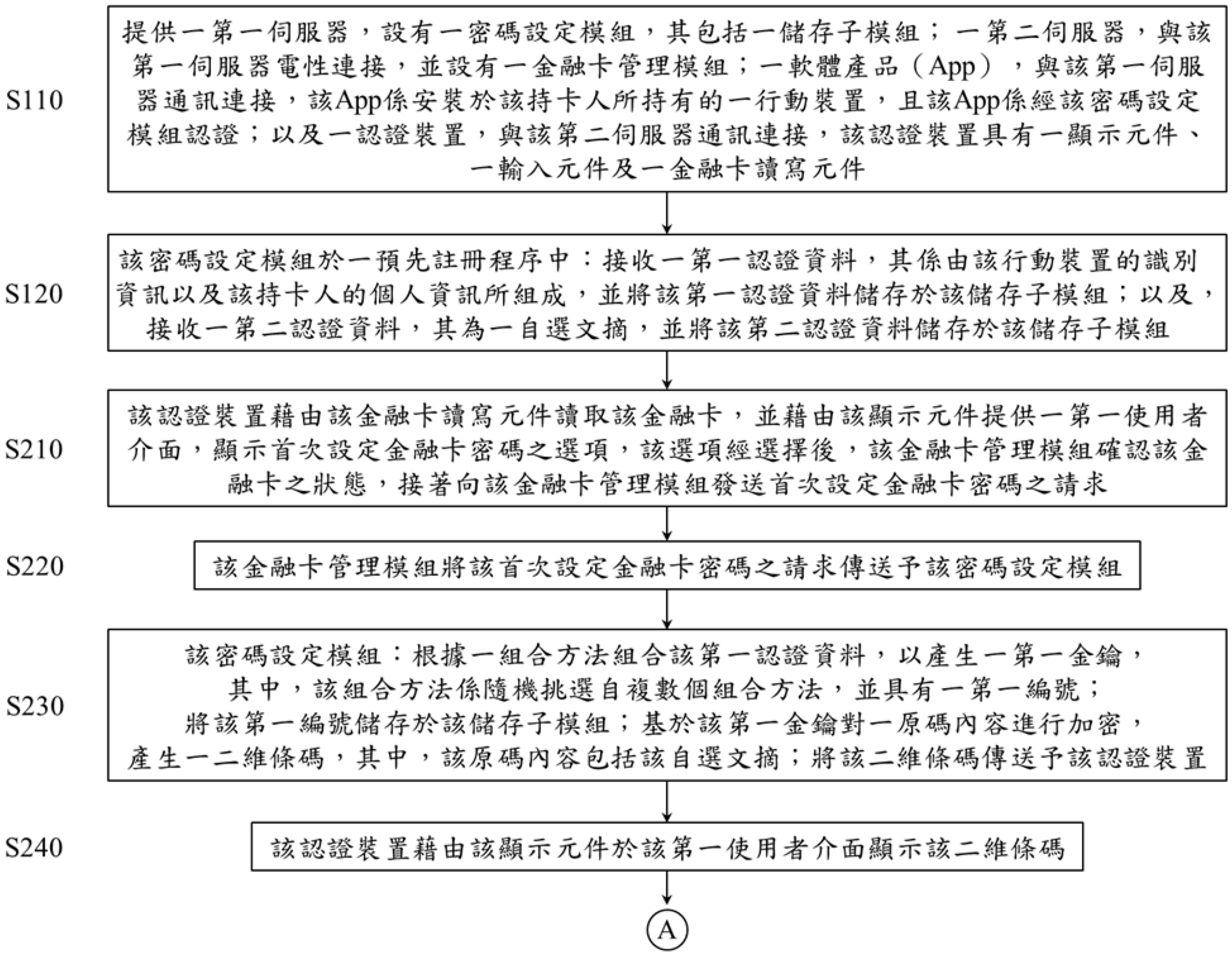
【第10項】如請求項9之用於幫助持卡人首次設定金融卡密碼之方法，其中該金融卡管理模組確認接收到的認證碼及個人資料無誤後，取得經亂碼化的新密碼，並傳送予該認證裝置，供其藉由該金融卡讀寫元件寫入該經亂碼化的新密碼至該金融卡。

【發明圖式】

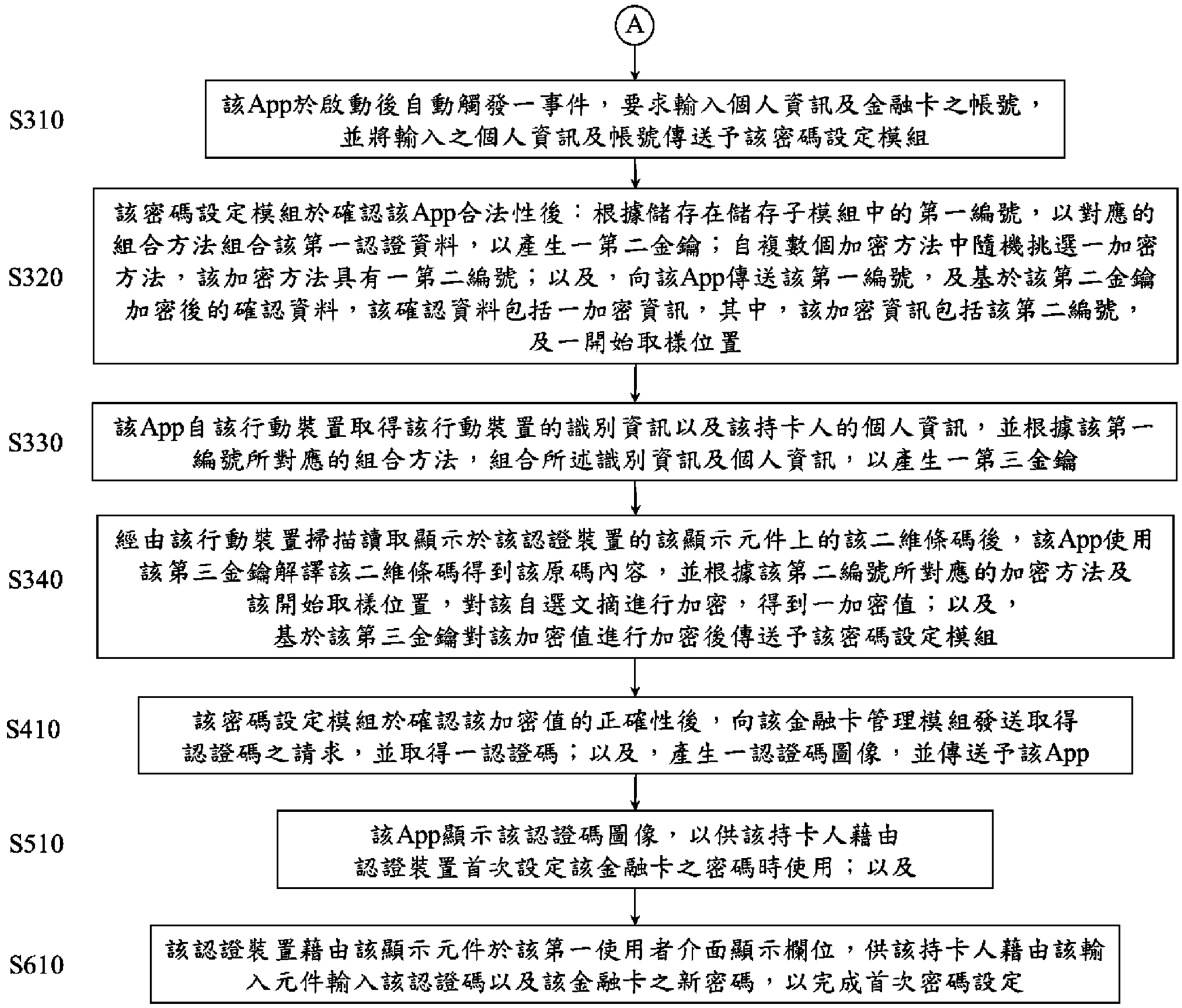
1



【圖1】


S110
提供一第一伺服器，設有一密碼設定模組，其包括一儲存子模組；一第二伺服器，與該第一伺服器電性連接，並設有一金融卡管理模組；一軟體產品（App），與該第一伺服器通訊連接，該App係安裝於該持卡人所持有的一行動裝置，且該App係經該密碼設定模組認證；以及一認證裝置，與該第二伺服器通訊連接，該認證裝置具有一顯示元件、一輸入元件及一金融卡讀寫元件
S120
該密碼設定模組於一預先註冊程序中：接收一第一認證資料，其係由該行動裝置的識別資訊以及該持卡人的個人資訊所組成，並將該第一認證資料儲存於該儲存子模組；以及，接收一第二認證資料，其為一自選文摘，並將該第二認證資料儲存於該儲存子模組
S210
該認證裝置藉由該金融卡讀寫元件讀取該金融卡，並藉由該顯示元件提供一第一使用者介面，顯示首次設定金融卡密碼之選項，該選項經選擇後，該金融卡管理模組確認該金融卡之狀態，接著向該金融卡管理模組發送首次設定金融卡密碼之請求
S220
該金融卡管理模組將該首次設定金融卡密碼之請求傳送予該密碼設定模組
S230
該密碼設定模組：根據一組合方法組合該第一認證資料，以產生一第一金鑰，
其中，該組合方法係隨機挑選自複數個組合方法，並具有一第一編號；
將該第一編號儲存於該儲存子模組；基於該第一金鑰對一原碼內容進行加密，
產生一二維條碼，其中，該原碼內容包括該自選文摘；將該二維條碼傳送予該認證裝置
S240
該認證裝置藉由該顯示元件於該第一使用者介面顯示該二維條碼
A

【圖2】


A
S310
該App於啟動後自動觸發一事件，要求輸入個人資訊及金融卡之帳號，並將輸入之個人資訊及帳號傳送予該密碼設定模組
S320
該密碼設定模組於確認該App合法性後：根據儲存在儲存子模組中的第一編號，以對應的組合方法組合該第一認證資料，以產生一第二金鑰；自複數個加密方法中隨機挑選一加密方法，該加密方法具有一第二編號；以及，向該App傳送該第一編號，及基於該第二金鑰加密後的確認資料，該確認資料包括一加密資訊，其中，該加密資訊包括該第二編號，及一開始取樣位置
S330
該App自該行動裝置取得該行動裝置的識別資訊以及該持卡人的個人資訊，並根據該第一編號所對應的組合方法，組合所述識別資訊及個人資訊，以產生一第三金鑰
S340
經由該行動裝置掃描讀取顯示於該認證裝置的該顯示元件上的該二維條碼後，該App使用該第三金鑰解譯該二維條碼得到該原碼內容，並根據該第二編號所對應的加密方法及該開始取樣位置，對該自選文摘進行加密，得到一加密值；以及，基於該第三金鑰對該加密值進行加密後傳送予該密碼設定模組
S410
該密碼設定模組於確認該加密值的正確性後，向該金融卡管理模組發送取得認證碼之請求，並取得一認證碼；以及，產生一認證碼圖像，並傳送予該App
S510
該App顯示該認證碼圖像，以供該持卡人藉由認證裝置首次設定該金融卡之密碼時使用；以及
S610
該認證裝置藉由該顯示元件於該第一使用者介面顯示欄位，供該持卡人藉由該輸入元件輸入該認證碼以及該金融卡之新密碼，以完成首次密碼設定

【圖2(續)】