I529641

(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 I529641 B**

(45)公告日： 中華民國 105 (2016) 年 04 月 11 日

(21)申請案號：103124465 (22)申請日： 中華民國 103 (2014) 年 07 月 17 日

(51)Int. Cl.： *G06Q20/40 (2012.01)* *G06F21/30 (2013.01)*
G06K19/06 (2006.01)

(71)申請人：捷碼數位科技股份有限公司 (中華民國) QUICK RETRIEVAL CORPORATION (TW)
臺北市信義區忠孝東路 5 段 472 號 9 樓

(72)發明人：黃介宏 HUANG, CHIEH HUNG (TW)

(74)代理人：林鼎鈞

(56)參考文獻：

TW	201421393A	CN	103415858A
US	8677116B1	US	8763097B2
US	2013/0048714A1	US	2013/0262163A1

審查人員：蔡茜堉

申請專利範圍項數：10 項 圖式數：6 共 37 頁

(54)名稱

驗證行動端動態顯示之資料之系統及其方法

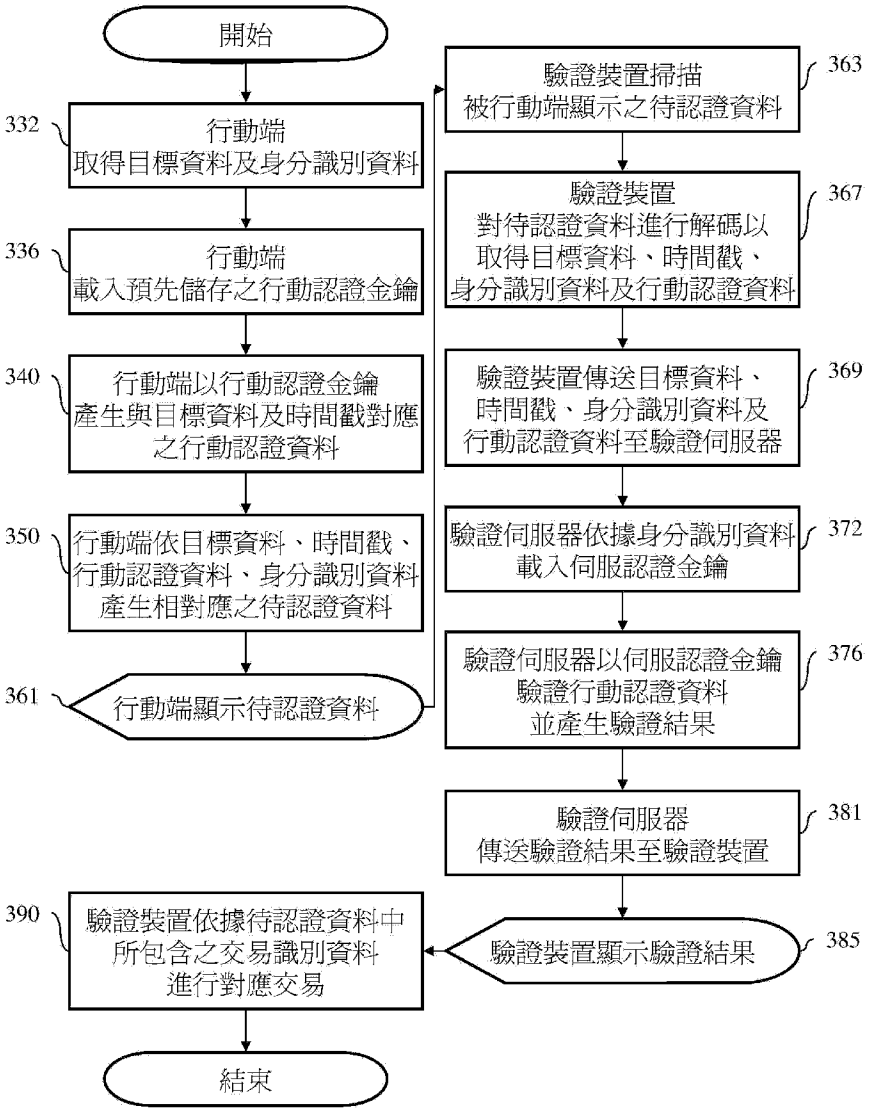
SYSTEM FOR VERIFYING DATA DISPLAYED DYNAMICALLY BY MOBILE AND METHOD THEREOF

(57)摘要

一種驗證行動端動態顯示之資料之系統及其方法，其透過行動端以行動認證金鑰產生與目標資料對應之行動認證資料後，依據目標資料、時間戳、行動認證資料、及身分識別資料產生相對應之待認證資料，驗證裝置掃描被行動端顯示之待認證資料後，對待認證資料進行解碼以取得目標資料、時間戳、身分識別資料及行動認證資料，驗證伺服器依據身分識別資料載入伺服認證金鑰後，以伺服認證金鑰驗證行動認證資料並產生驗證結果之技術手段，可以動態提供待認證資料以防止冒用，並達成快速簡易的進行認證的技術功效。

A system for verifying a data displayed dynamically by a mobile and a method thereof are provided. By generating an authenticate data in accordance with a target data, a timestamp, a mobile authenticate data, and an identification by a mobile after using a mobile authenticate key to generate the mobile authenticate data corresponding to the target data, obtaining the target data, the timestamp, the mobile authenticate data, and the identification from the authenticate data by a verification device after scanning the authenticate data displayed on the mobile, and using a server authenticate key to verify the mobile authenticate data and generating a verification result by a verification server after loading the server authenticate key according to the identification, the system and the method can provide dynamic authenticate data for preventing fraudulent, and achieve the effect of verifying authenticate data quickly and easily.

指定代表圖：



【第3C圖】

符號簡單說明：

步驟 332　行動端取得目標資料及身分識別資料 步驟 336　行動端載入預先儲存之行動認證金鑰 步驟 340　行動端以行動認證金鑰產生與目標資料及時間戳對應之行動認證資料 步驟 350　行動端依據目標資料、時間戳、行動認證資料、身分識別資料產生相對應之待認證資料 步驟 361　行動端顯示待認證資料 步驟 363　驗證裝置掃描被行動端顯示之待認證資料 步驟 367　驗證裝置對待認證資料進行解碼以取得目標資料、時間戳、身分識別資料及行動認證資料 步驟 369　驗證裝置傳送目標資料、時間戳、身分識別資料及行動認證資料至驗證伺服器 步驟 372　驗證伺服器依據身分識別資料載入伺服認證金鑰 步驟 376　驗證伺服器以伺服認證金鑰驗證行動認證資料並產生驗證結果 步驟 381　驗證伺服器傳送驗證結果至驗證裝置 步驟 385　驗證裝置顯示驗證結果 步驟 390　驗證裝置依據待認證資料

中所包含之交易識別
資料進行對應交易

I529641
專利案號：103124465

公告本

申請日：103. 7. 17
IPC分類：G06Q 30/02 (2012.01)
G06F 21/30
G06K 19/06 (2013.01)
(2006.01)

【發明摘要】

【中文發明名稱】 驗證行動端動態顯示之資料之系統及其方法

【英文發明名稱】 SYSTEM FOR VERIFYING DATA DISPLAYED DYNAMICALLY BY MOBILE AND METHOD THEREOF

【中文】

一種驗證行動端動態顯示之資料之系統及其方法，其透過行動端以行動認證金鑰產生與目標資料對應之行動認證資料後，依據目標資料、時間戳、行動認證資料、及身分識別資料產生相對應之待認證資料，驗證裝置掃描被行動端顯示之待認證資料後，對待認證資料進行解碼以取得目標資料、時間戳、身分識別資料及行動認證資料，驗證伺服器依據身分識別資料載入伺服認證金鑰後，以伺服認證金鑰驗證行動認證資料並產生驗證結果之技術手段，可以動態提供待認證資料以防止冒用，並達成快速簡易的進行認證的技術功效。

【英文】

A system for verifying a data displayed dynamically by a mobile and a method thereof are provided. By generating an authenticate data in accordance with a target data, a timestamp, a mobile authenticate data, and an identification by a mobile after using a mobile authenticate key to generate the mobile authenticate data corresponding to the target data, obtaining the target data, the timestamp, the mobile authenticate data, and the identification from the authenticate data by a verification device after scanning the authenticate data displayed on the mobile, and using a server authenticate key to verify the mobile authenticate data and generating a verification result by a verification server after loading the server authenticate key according to the identification, the

system and the method can provide dynamic authenticate data for preventing fraudulent, and achieve the effect of verifying authenticate data quickly and easily.

【指定代表圖】　第（ 3C ）圖。

【代表圖之符號簡單說明】

步驟 332　行動端取得目標資料及身分識別資料

步驟 336　行動端載入預先儲存之行動認證金鑰

步驟 340　行動端以行動認證金鑰產生與目標資料及時間戳對應之行動認證資料

步驟 350　行動端依據目標資料、時間戳、行動認證資料、身分識別資料產生相對應之待認證資料

步驟 361　行動端顯示待認證資料

步驟 363　驗證裝置掃描被行動端顯示之待認證資料

步驟 367　驗證裝置對待認證資料進行解碼以取得目標資料、時間戳、身分識別資料及行動認證資料

步驟 369　驗證裝置傳送目標資料、時間戳、身分識別資料及行動認證資料至驗證伺服器

步驟 372　驗證伺服器依據身分識別資料載入伺服認證金鑰

步驟 376　驗證伺服器以伺服認證金鑰驗證行動認證資料並產生驗證結果

步驟 381　驗證伺服器傳送驗證結果至驗證裝置

步驟 385　驗證裝置顯示驗證結果

步驟 390　驗證裝置依據待認證資料中所包含之交易識別資料進行對應交易

【發明說明書】

【中文發明名稱】 驗證行動端動態顯示之資料之系統及其方法

【英文發明名稱】 SYSTEM FOR VERIFYING DATA DISPLAYED DYNAMICALLY BY MOBILE AND METHOD THEREOF

【技術領域】

【0001】 一種資料驗證系統及其方法，特別係指一種驗證行動端動態顯示之資料之系統及其方法。

【先前技術】

【0002】 現今，條碼係普遍地被運用在資料之管理上。不論條碼的種類，至今的運用大多僅止於將其列印於書面等物品上，再以讀取裝置來加以讀取，進而取得條碼中所包含之資料。

【0003】 而隨著無線通訊科技之進步，現今個人化的行動裝置幾乎已是生活上不可或缺的使用物品。若是將電子條碼顯示於特定人士所持有之行動裝置的顯示器上，或是將該特定人士所取得之條碼傳送至條碼解讀裝置上，則可作爲各種判別或解讀的用途。舉例而言，特定人士可經由其所持有之行動電話或個人電子秘書裝置（PDA）等行動裝置來訂購其所需之商品，例如票卷等，而售票單位則可以使用電子條碼的方式將被訂購之入場票傳送至該位人士之行動裝置中，如此，對顯示於行動裝置上之電子條碼進行解讀後，解讀到的資料即可以作爲該位人士入場的憑證。

【0004】 然而，若是該位人士複製其所接收之電子條碼並傳送給其他人士，則於入場時，其他人士同樣可以經由其所持有之行動裝置顯示電子條碼，作爲入場憑證。由此可知，若電子條碼被複製，則可能會被冒用。

【0005】 綜上所述，可知先前技術中長期以來一直存在可以使用複製的電子條碼冒用身分的問題，因此有必要提出改進的技術手段，來解決此一問題。

【發明內容】

【0006】 有鑒於先前技術存在可以使用複製的電子條碼冒用身分的問題，本發明遂揭露一種驗證行動端動態顯示之資料之系統及其方法，其中：

【0007】 本發明所揭露之驗證行動端動態顯示之資料之系統，至少包含：驗證裝置以及驗證伺服器。驗證裝置用以掃描行動端所顯示之待認證資料及用以對待認證資料進行解碼以取得目標資料、時間戳、身分識別資料及行動認證資料，其中，待認證資料係行動端以行動認證金鑰產生，且與目標資料及時間戳對應；驗證伺服器，與該驗證裝置連接，用以依據身分識別資料載入伺服認證金鑰，並以伺服認證金鑰驗證行動認證資料以產生驗證結果，及用以傳送驗證結果至驗證裝置顯示。

【0008】 本發明所揭露之驗證行動端動態顯示之資料之方法，其步驟至少包括：行動端取得目標資料及身分識別資料；行動端載入預先儲存之行動認證金鑰；行動端以行動認證金鑰產生與目標資料及時間戳對應之行動認證資料；行動端至少依據目標資料、時間戳、行動認證資料、及身分識別資料產生相對應之待認證資料；行動端顯示待認證資料；驗證裝置掃描被行動端顯示之待認證資料；驗證裝置對待認證資料進行解碼以取得目標資料、時間戳、身分識別

資料及行動認證資料；驗證裝置傳送目標資料、時間戳、身分識別資料及行動認證資料至驗證伺服器；驗證伺服器依據身分識別資料載入伺服認證金鑰；驗證伺服器以伺服認證金鑰驗證行動認證資料並產生驗證結果；驗證伺服器傳送驗證結果至驗證裝置；驗證裝置顯示驗證結果。

【0009】 本發明所揭露之系統與方法如上，與先前技術之間的差異在於本發明透過行動端以行動認證金鑰產生與目標資料對應之行動認證資料後，依據目標資料、時間戳、行動認證資料、及身分識別資料產生相對應之待認證資料，驗證裝置掃描被行動端顯示之待認證資料後，對待認證資料進行解碼以取得目標資料、時間戳、身分識別資料及行動認證資料，驗證伺服器依據身分識別資料載入伺服認證金鑰後，以伺服認證金鑰驗證行動認證資料並產生驗證結果，藉以解決先前技術所存在的問題，並可以達成動態提供待認證資料，且能夠快速簡易的進行認證之技術功效。

【圖式簡單說明】

【0010】

第1圖爲本發明所提之驗證行動端動態顯示之資料之系統架構圖。

第2A圖爲本發明所提之行動端之元件示意圖。

第2B圖爲本發明所提之驗證伺服器之元件示意圖。

第3A圖爲本發明所提之使用者註冊之方法流程圖。

第3B圖爲本發明所提之另一種使用者註冊之方法流程圖。

第3C圖爲本發明所提之驗證行動端動態顯示之資料之方法流程圖。

【實施方式】

【0011】以下將配合圖式及實施例來詳細說明本發明之特徵與實施方式，內容足以使任何熟習相關技藝者能夠輕易地充分理解本發明解決技術問題所應用的技術手段並據以實施，藉此實現本發明可達成的功效。

【0012】本發明可以由行動端產生並顯示待認證資料，在驗證裝置掃描行動端所顯示的待認證資料後，將解析出的目標資料、時間戳、身分識別資料以及行動認證資料傳送到驗證伺服器進行驗證，藉以提供具有防僞、防複製、且具有時效性的驗證機制。

【0013】本發明所提之「目標資料」爲需要驗證的資料，可以是使用者的身分資料，也可以是電子票卷的票卷資料，還可以是電子交易的交易資料等，但本發明所提之「目標資料」並不以上述爲限，凡需要進行驗證的資料都可以做爲本發明所提之目標資料。

【0014】本發明所提之「時間戳」爲可以表示時間的資料。例如，「2014/7/8 17:39:13」等以特定格式記載的資料，或是特定時間至某一時間所經過的秒數等，本發明並沒有特別的限制。

【0015】本發明所提之「待認證資料」爲對資料進行特定運算所產生的資料，且可以解析待認證資料而取得原先進行運算的資料，例如，一維條碼或二維條碼、快速響應矩陣碼（Quick Response Code, QR-Code）、圖片等，但本發明所提之待認證資料並不以上述爲限。

【0016】本發明所提之「身分識別資料」可以是使用者預先建立的帳號、電子郵件地址、行動裝置的機碼、裝置識別碼、或發話號碼等可以對應至使用者的資料，但本發明所提之身分識別資料並不以上述爲限。另外，本發明所提

之「行動認證資料」爲經過特定編碼運算後所產生的資料，可以是文字、數字、符號的任意組合。

【0017】 以下先以「第1圖」本發明所提之驗證行動端動態顯示之資料之系統架構圖來說明本發明的系統運作。如「第1圖」所示，本發明之系統含有行動端100、驗證伺服器200、以及驗證裝置290。其中，行動端100可以透過網際網路400與驗證伺服器200連接；驗證裝置290與驗證伺服器200則可以直接連接，例如，透過串列（Serial）線與驗證伺服器200連接，驗證裝置290也可以透過如近端網路（local network）、或內部網路（intranet）等網路連接，本發明並沒有特別的限制。

【0018】 行動端100可以是行動裝置，也可以是執行於行動裝置上的應用程式，本發明並沒有特別的限制。其中，行動端100可以如「第2A圖」所示，包含讀取模組120、認證資料產生模組150、編碼模組160、顯示模組180，以及可附加的傳輸模組110、輸入模組130、加解密模組140。

【0019】 傳輸模組110可以與驗證伺服器200連接，藉以讓行動裝置的使用者可以至驗證伺服器200進行註冊程序。例如，接收驗證伺服器200所傳送的驗證資料與伺服認證金鑰、傳送身分識別資料與驗證資料至驗證伺服器200等，甚至，傳輸模組110還可以將驗證伺服器200所傳送的伺服認證金鑰做爲行動認證金鑰儲存至執行有本發明之行動裝置的儲存媒體中。

【0020】 一般而言，傳輸模組110會透過使用安全連接層（Secure Sockets Layer, SSL）或虛擬私人網路（Virtual Private Network, VPN）等技術所產生的安全通道與驗證伺服器200連線，但本發明並不以此爲限。

【0021】讀取模組120負責讀取目標資料、身分識別資料以及行動認證金鑰。在部份的實施例中，目標資料即爲身分識別資料，但本發明並不以此爲限。在部分的實施例中，輸入模組130也可以讀取行動端100之使用者的通訊資料。其中，通訊資料爲可以與使用者聯絡的資料，包含但不限於電子郵件地址、手機門號、即時通訊帳號等。

【0022】目標資料、身分識別資料、通訊資料以及行動認證金鑰通常預先被儲存於執行本發明之行動裝置的儲存媒體中。行動裝置之儲存媒體可以是內嵌於行動裝置的隨機存取記憶體（RAM）、唯讀記憶體（ROM）、可擦寫可程式化唯讀記憶體（RPROM）、快閃記憶體（Flash）等記憶體，也可以是與行動裝置連接的儲存裝置，本發明並沒有特別的限制，凡可以儲存資料者都可以做爲本發明所提之儲存媒體。

【0023】本發明所提之「行動認證金鑰」可以由特定數量的文字、數字、符號任意組合而成。在某些實施例中，行動認證金鑰可以是由驗證伺服器所產生的資料，而在某些實施例中，行動認證金鑰則可以是使用者所申請之電子憑證中的私鑰（Private key）。另外，在部分的實施例中，行動認證金鑰通常會在被加密後才會被儲存，但本發明並不以此爲限。

【0024】目標資料、身分識別資料、通訊資料以及行動認證金鑰並不一定會儲存在同一種儲存媒體中，例如，目標資料可以被儲存在隨機存取記憶體、身分識別資料可以被儲存在可擦寫可程式化唯讀記憶體、通訊資料與行動認證金鑰可以被儲存在快閃記憶體中等，如此，讀取模組120會分別至隨機存取記憶體、可擦寫可程式化唯讀記憶體、快閃記憶體中讀取目標資料、身分識別資料、通訊資料與行動認證金鑰。

【0025】實務上，讀取模組120並不一定只能從行動端100之儲存媒體中讀取目標資料、身分識別資料、通訊資料、以及行動認證金鑰等資料，也可以讀取傳輸模組110接受自外部伺服器或應用程式所提供之目標資料，甚至可以對一維條碼、二維條碼、或影像進行解析以取得資料，或是提供使用者介面使得使用者可以直接輸入資料，本發明並沒有特別的限制，凡可以讓讀取模組120取得資料的方式都可以在本發明中被使用。

【0026】輸入模組130可以提供輸入對行動認證金鑰進行加解密所使用的密碼。例如，在讀取模組120所讀出之行動認證金鑰被加密時，輸入模組130可以提供使用者介面，藉以讓使用者輸入解密的密碼。而在傳輸模組110接收到行動認證金鑰時，輸入模組130也可以提供使用者介面，藉以讓使用者輸入對行動認證金鑰加密的密碼。

【0027】加解密模組140可以依據輸入模組130提供輸入的密碼對讀取模組120所讀出之行動認證金鑰進行解密，並將解密後的行動認證金鑰提供給認證資料產生模組150。加解密模組140也可以依據輸入模組130提供輸入的密碼對傳輸模組110所接收到的行動認證金鑰進行加密，並將加密後的行動認證金鑰儲存至執行有本發明之行動裝置的儲存媒體中。

【0028】認證資料產生模組150負責以行動認證金鑰產生行動認證資料。當行動認證金鑰爲驗證伺服器所產生之資料時，認證資料產生模組150可以依據訊息認證碼（Message Authentication Code, MAC）、雜湊訊息認證碼（Hash Message Authentication Code, HMAC）、RFC 4226：HMAC式一次性密碼（HMAC-Based One-Time Password, HOPT）、或RFC 6238：時間式一次性密碼（Time-based One-Time Password, TOPT）等演算法，使用行動認證金鑰對目標

資料進行運算，並將運算後產生的押碼做爲行動認證資料；而當行動認證金鑰爲使用者所申請的私鑰時，認證資料產生模組150可以使用習知之簽章演算法對目標資料進行運算，並將運算後所產生的簽章作爲行動認證資料。

【0029】在部分的實施例中，認證資料產生模組150在使用行動認證金鑰進行運算產生行動認證資料時，被運算的資料並非只有目標資料，而是還包含用來表示當前時間的時間戳。也就是說，行動認證資料也可能是認證資料產生模組150使用行動認證金鑰對包含目標資料以及時間戳的資料進行運算所產生，如此，認證資料產生模組150每一次所產生的行動認證資料都會不同，也就是說，認證資料產生模組150可以動態的產生行動認證資料。

【0030】編碼模組160負責產生待認證資料。一般而言，編碼模組160至少會依據讀取模組120所讀出之目標資料與身分識別資料、認證資料產生模組150所產生之行動認證資料，以及認證資料產生模組150產生行動認證資料所使用之時間戳產生待認證資料。

【0031】顯示模組180負責顯示編碼模組160運算產生的待認證資料，使得編碼模組160產生的待認證資料被顯示在執行本發明之行動裝置的顯示螢幕上。

【0032】以下將進一步說明驗證伺服器200。驗證伺服器200負責進行資料的驗證。驗證伺服器200可以如「第2B圖」所示，包含儲存媒體201、傳輸模組210、識別載入模組220、認證資料驗證模組230，以及可附加的驗證資料產生模組250、驗證資料檢查模組260、金鑰產生模組270、憑證驗證模組280。

【0033】儲存媒體201負責儲存資料。儲存媒體201所儲存的資料中，有部份資料中的每一筆資料都包含身分識別資料以及相對應之伺服認證金鑰。本發明所提之「伺服認證金鑰」可以由特定數量的文字、數字、符號任意組合而成。

在某些實施例中，伺服認證金鑰可以是由金鑰產生模組270所產生的資料，而在某些實施例中，伺服認證金鑰則可以是使用者所申請之電子憑證中的公鑰（Public key）。另外，在部分的實施例中，伺服認證金鑰會在被加密後才會被儲存，但本發明並不以此爲限。

【0034】傳輸模組210與驗證裝置290連接，負責與驗證裝置290交換資料，藉以完成目標資料的驗證。

【0035】傳輸模組210也可以與行動端100連接，可以與行動端100交換資料，藉以完成行動端100之使用者的註冊程序。一般而言，傳輸模組210可以透過網際網路400與行動端100連接。

【0036】識別載入模組220負責在傳輸模組210接收到驗證裝置290所傳送的身分識別資料後，載入與傳輸模組210所接收之身分識別資料對應的伺服認證金鑰。例如，識別載入模組220可以至儲存媒體201中搜尋到傳輸模組210所接收之身分識別資料，並讀取相對應的伺服認證金鑰，藉以完成伺服認證金鑰的載入。

【0037】在部分的實施例中，若伺服認證金鑰是在被加密後才被儲存，則識別載入模組220可以先將伺服認證金鑰解密後才提供給認證資料驗證模組230。

【0038】認證資料驗證模組230負責以識別資料載入模組220所載入的伺服認證金鑰驗證行動認證資料，並在驗證後產生相對應的驗證結果。

【0039】一般而言，認證資料驗證模組230可以以伺服認證金鑰產生伺服認證資料，並接著比對所產生的伺服認證資料以及傳輸模組210所接收到的行動認證資料，藉以依據比對結果產生驗證結果。其中，認證資料驗證模組230需要

使用與行動端100之認證資料產生模組150產生行動認證金鑰所使用之演算法相同的演算法進行運算，也就是說，不論認證資料產生模組150是依據MAC、Hash-MAC、HOTP、或TOPT等演算法，或是依據簽章演算法，使用行動認證金鑰對目標資料進行運算而產生行動認證資料，認證資料驗證模組230也需要依據相同的演算法，使用伺服認證金鑰對目標資料進行運算而產生伺服認證資料。

【0040】 當認證資料驗證模組230所產生的伺服認證資料與傳輸模組210所接收到的行動認證資料不同時，表示行動認證資料通過驗證，認證資料驗證模組230可以產生表示行動認證資料通過驗證的驗證結果，而若伺服認證資料與行動認證資料不同，表示行動認證資料無法通過驗證，認證資料驗證模組230可以產生表示行動認證資料未通過驗證的驗證結果。

【0041】 在部分的實施例中，在認證資料驗證模組230判斷行動認證資料通過驗證後，認證資料驗證模組230通常不會直接產生驗證結果，而是會進一步判斷當前之時間與傳輸模組210所接收到之時間戳所表示的時間之時間差是否在預定的時間範圍內，若是，則認證資料驗證模組230才會產生表示行動認證資料通過驗證的驗證結果，而若當前之時間與時間戳所表示的時間之時間差沒有落在預定的時間範圍內，則認證資料驗證模組230依然會產生表示行動認證資料未通過驗證的驗證結果。但認證資料驗證模組230產生驗證結果之方式並不以上述爲限。其中，上述之預定的時間範圍例如10分鐘、半小時等，但本發明並不以此爲限。

【0042】 驗證資料產生模組250可以在傳輸模組210接收到行動端100所傳送的使用者資料後，產生驗證資料，並將傳輸模組210接收到的使用者資料以及所產生的驗證資料做爲一筆資料，儲存至儲存媒體201中。其中，傳輸模組210

所接收到之使用者資料包含身分識別資料、或身分識別資料與通訊資料，其中，若使用者資料僅包含身分識別資料，則表示足以依據身分識別資料與使用者通訊，例如爲電子郵件帳號或手機門號等；驗證資料產生模組250所產生驗證資料爲隨機產生的一次性資料，且具有時效性，但本發明並不以此爲限。

【0043】驗證資料產生模組250也可以透過傳輸模組210將所產生的驗證資料傳送至行動端100。一般而言，傳輸模組210可以依據使用者資料中的身分識別資料或通訊資料選擇使用簡訊、電子郵件、或即時訊息等方式傳送驗證資料，但本發明並不以此爲限。

【0044】驗證資料檢查模組260可以在傳輸模組210接收到行動端100所傳送的身分識別資料以及驗證資料後，依據傳輸模組210所接收到的身分識別資料至儲存媒體201讀取驗證資料，並比對被讀出的驗證資料以及被接收到的驗證資料，藉以判斷行動端100所傳送的驗證資料是否正確。當被讀出的驗證資料與被接收到的驗證資料相同，表示行動端100所傳送的驗證資料正確，而若被讀出的驗證資料與被接收到的驗證資料不同，表示行動端100所傳送的驗證資料不正確。

【0045】金鑰產生模組270可以在驗證資料檢查模組260判斷行動端100所傳送的驗證資料正確時，產生伺服認證金鑰。一般而言，金鑰產生模組270可以使用特定的演算法產生伺服認證金鑰，但本發明並不以此爲限，例如，金鑰產生模組270也可以隨機產生伺服認證金鑰。其中，上述金鑰產生模組270可以使用之演算法例如但不限於在RFC 5968、NIST SP 800-108、NIST SP 800-132等文件中所提之衍生金鑰（Key Derivation）演算法。

【0046】 金鑰產生模組270也可以將所產生的伺服認證金鑰以及傳輸模組210所接收到的使用者資料做爲一筆資料，儲存到儲存媒體201中。一般而言，金鑰產生模組270會先將伺服認證金鑰加密後才將加密後的伺服認證金鑰與身分識別資料儲存至儲存媒體201中，但本發明並不以此爲限。

【0047】 金鑰產生模組270也可以透過傳輸模組210將所產生的伺服認證金鑰傳送到行動端100，使得行動端100將接收到的伺服認證金鑰做爲行動認證金鑰。其中，傳輸模組210可以依據儲存媒體201中所儲存之身分識別資料或與身分識別資料一同被儲存之通訊資料，選擇使用簡訊、電子郵件、或即時訊息等方式傳送伺服認證金鑰，但本發明並不以此爲限，例如，傳輸模組210也可以使用行動端100所建立的SSL或VPN連線，直接傳送伺服認證金鑰給行動端100。

【0048】 憑證驗證模組280可以在傳輸模組210接收到行動端100所傳送的身分識別資料、識別資料以及使用者所申請的電子憑證後，且驗證資料檢查模組260判斷行動端100所傳送的驗證資料正確時，進一步判斷傳輸模組210所接收到的電子憑證是否正確。

【0049】 若憑證驗證模組280判斷傳輸模組210所接收到的電子憑證正確，則憑證驗證模組280可以將傳輸模組210所接收到之電子憑證中的公鑰做爲伺服認證金鑰，並將電子憑證中的公鑰以及傳輸模組210所接收到的身分識別資料做爲一筆資料，儲存到儲存媒體201中。與金鑰產生模組270相似的，憑證驗證模組280可以先將伺服認證金鑰加密後，才將加密後的伺服認證金鑰與身分識別資料儲存至儲存媒體201中，但本發明並不以此爲限。

【0050】 以下將繼續說明驗證裝置290。驗證裝置290負責掃描行動端100所顯示的待認證資料。驗證裝置290會隨著待認證資料的不同而使用不同的掃瞄

技術，例如，當待認證資料爲一維條碼時，驗證裝置290可以使用一維條碼掃瞄設備掃描待認證資料，而當待認證資料爲QR-code或圖像時，驗證裝置290則爲具有攝像鏡頭的裝置，藉以掃描待認證資料。

【0051】 驗證裝置290也負責對掃描所得之待認證資料進行解碼，並在解碼後取得目標資料、時間戳、身分識別資料、以及行動認證資料。

【0052】 驗證裝置290還負責將解碼待認證資料所取得的目標資料、時間戳、身分識別資料、行動認證資料等資料傳送到驗證伺服器200進行驗證，並顯示驗證伺服器200所傳回的驗證結果。

【0053】 在部份的實施例中，待認證資料在解碼後還可以取得交易識別資料，驗證裝置290可以在驗證伺服器200所產生之驗證結果表示行動認證資料通過驗證時，依據解碼待認證資料後所取得的交易識別資料，進行相對應的交易。

【0054】 接著以第一個實施例來解說本發明的運作系統與方法，並請參照「第3A圖」本發明所提之使用者註冊之方法流程圖以及「第3C圖」本發明所提之驗證行動端動態顯示之資料之方法流程圖。在本實施例中，假設有本發明外部之會員系統欲透過本發明驗證會員的身分。

【0055】 首先，該會員系統的會員（以下稱使用者）需要在其所使用的手機等行動裝置上安裝支援本發明的應用程式（行動端100），並完成註冊程序。

【0056】 在使用者安裝並執行支援本發明的應用程式後，行動端100的輸入模組130可以提供使用者輸入身分識別資料，或身分識別資料與通訊資料等使用者資料，並在使用者完成輸入後，透過行動端100的傳輸模組110將使用者所輸入的使用者資料透過SSL或VPN傳送給驗證伺服器200（步驟312）。在本實施

例中，假設身分識別資料爲使用者在該會員系統中的帳號，例如，電子郵件地址。

【0057】在驗證伺服器200的傳輸模組210接收到行動端100所傳送的使用者資料後，驗證伺服器200的驗證資料產生模組250可以產生一次性的驗證資料，並將所產生的驗證資料以及傳輸模組210所接收到的使用者資料做爲一筆資料暫存在驗證伺服器200的儲存媒體201中，以及透過傳輸模組210將所產生的驗證資料傳送給行動端100（步驟316）。在本實施例中，假設傳輸模組210是透過電子郵件將驗證資料傳送到使用者的電子郵件信箱（也就是使用者在該會員系統中的帳號）中。

【0058】在使用者至電子郵件信箱中閱讀驗證伺服器200所傳送之包含驗證資料的電子郵件後，使用者可以透過行動端100的輸入模組130輸入驗證資料，如此，行動端100的傳輸模組110可以透過SSL或VPN的連線，將輸入模組130提供使用者輸入的驗證資料以及使用者先前所輸入的身分識別資料傳送給驗證伺服器200（步驟318a）。

【0059】在驗證伺服器200的傳輸模組210接收到行動端100所傳送的驗證資料以及身分識別資料後，驗證伺服器200的驗證資料檢查模組260可以判斷傳輸模組210所接收到的驗證資料是否正確（步驟321）。在本實施例中，假設驗證資料檢查模組260會至驗證伺服器200的儲存媒體201中搜尋傳輸模組210所接收到的身分識別資料，並在搜尋到相同的身分識別資料時，讀取與被搜尋到之身分識別資料一同被儲存的驗證資料，接著，驗證資料檢查模組260會比對傳輸模組210所接收到的驗證資料以及被讀取出之驗證資料。若兩者相同，則表示傳

輸模組210所接收到的驗證資料正確；而若兩者不同，則表示傳輸模組210所接收到的驗證資料錯誤，驗證伺服器200將不再進行後續處理。

【0060】 當驗證伺服器200的驗證資料檢查模組260判斷驗證伺服器200之傳輸模組210所接收到的驗證資料正確時，驗證伺服器200的金鑰產生模組270可以產生伺服認證金鑰（步驟323）。在本實施例中，假設金鑰產生模組270會使用衍生金鑰演算法產生伺服認證金鑰。

【0061】 在驗證伺服器200的金鑰產生模組270產生伺服認證金鑰（步驟323）後，金鑰產生模組270可以將所產生的伺服認證金鑰以及驗證伺服器200之傳輸模組210所接收到的身分識別資料做爲一筆資料，儲存到驗證伺服器200的儲存媒體201中（步驟327），並透過傳輸模組210將所產生的伺服認證金鑰傳送至行動端100（步驟328）。在本實施例中，假設傳輸模組210會通過行動端100所建立的SSL和VPN連線，將伺服認證金鑰傳送給行動端100。

【0062】 行動端100的傳輸模組110在接收到驗證伺服器200所傳送的伺服認證金鑰後，可以將所接收到的伺服認證金鑰做爲行動認證金鑰，儲存至執行本發明之行動裝置（使用者所使用之手機）的儲存媒體中（步驟329），藉以完成註冊程序。在本實施例中，假設行動端100還包含加解密模組140，在行動認證金鑰被儲存至儲存媒體之前，加解密模組140更可以使用密碼加密行動認證金鑰，使得儲存媒體中儲存經過加密的行動認證金鑰。其中，加解密模組140用來加密行動認證金鑰的密碼是加解密模組140透過行動端100的輸入模組130要求使用者輸入。

【0063】 在使用者完成註冊程序後，當該會員系統要求使用者進行身分驗證時，使用者可以在手機上執行支援本發明的應用程式，如此，行動端100的讀

取模組120可以至執行本發明之行動裝置的儲存媒體中取得目標資料以及身分識別資料（步驟332），並載入先前在註冊程序中被儲存的行動認證金鑰（步驟336）。在本實施例中，讀取模組120所取得的目標資料可以是使用者的個人資料、或是與身分識別資料相同的會員帳號等；另外，由於行動認證金鑰經過加密，因此，加解密模組140可以透過輸入模組130要求使用者輸入與加密行動認證金鑰時相同的密碼，並使用使用者透過輸入模組130所輸入的密碼解密讀取模組120所讀出的行動認證金鑰。

【0064】在行動端100的讀取模組120取得目標資料以及身分識別資料（步驟332），並載入行動認證金鑰（步驟336）後，行動端100的認證資料產生模組150可以以行動認證金鑰產生與目標資料以及表示當前時間之時間戳對應的行動認證資料（步驟340）。在本實施例中，假設認證資料產生模組150會使用行動認證金鑰對目標資料與當前的時間（時間戳）所組成的資料進行RFC 4226或RFC 6238的演算以產生一次性的行動認證資料。

【0065】在行動端100的認證資料產生模組150以行動認證金鑰產生行動認證資料（步驟340）後，行動端100的編碼模組160可以產生待認證資料（步驟350）。在本實施例中，由於認證資料產生模組150是以行動認證金鑰對目標資料與時間戳所組成的資料進行演算而產生行動認證資料，因此，編碼模組160會對行動端100之讀取模組120所取得的目標資料、身分識別資料、認證資料產生模組150所產生的行動認證資料、以及認證資料產生模組150所使用的時間戳進行編碼，藉以產生相對應的QR-code（待認證資料）。

【0066】 在行動端100的編碼模組160產生待認證資料（步驟350）後，行動端100的顯示模組180可以顯示編碼模組160所產生的待認證資料（步驟361），使得待認證資料被顯示在執行本發明之行動裝置的顯示螢幕上。

【0067】 在行動端100的顯示模組180顯示待認證資料（步驟361）後，使用者可以將執行本發明之行動裝置的顯示螢幕接近驗證裝置290，使得驗證裝置290可以掃瞄被顯示在顯示螢幕上的待認證資料（步驟363）。在本實施例中，由於待認證資料爲QR-code，因此，驗證裝置290需要包含攝像鏡頭，藉以掃描執行本發明之行動裝置所顯示的QR-code。

【0068】 在驗證裝置290掃瞄待認證資料（步驟363）後，驗證裝置290可以對待認證資料進行解碼以取得行動端100的編碼模組160產生待認證資料所使用的目標資料、時間戳、身分識別資料、以及行動認證資料等資料（步驟367），並將解碼所取得的資料傳送到驗證伺服器200。

【0069】 在驗證伺服器200的傳輸模組210接收到驗證裝置290所傳送的資料後，驗證伺服器200的識別載入模組220可以依據傳輸模組210所接收到的身分識別資料載入伺服認證金鑰（步驟372）。在本實施例中，假設識別載入模組220會至驗證伺服器200的儲存媒體201中搜尋傳輸模組210所接收到的身分識別資料，並在搜尋到傳輸模組210所接收到的身分識別資料後，讀取在註冊程序中與被搜尋到之身分識別資料一同被儲存的伺服認證金鑰。

【0070】 在實務上，若註冊程序中，驗證伺服器200的金鑰產生模組270在儲存伺服認證金鑰（步驟327）時，先加密伺服認證金鑰才儲存加密後的伺服認證金鑰，則識別載入模組220需要在讀出經過加密的伺服認證金鑰後，將經過加密的伺服認證金鑰解密，藉以載入伺服認證金鑰。

【0071】在驗證伺服器200的識別載入模組220載入伺服認證金鑰（步驟372）後，驗證伺服器200的認證資料驗證模組230可以對驗證伺服器200之傳輸模組210所接收到的行動認證資料進行驗證，並在驗證後產生驗證結果（步驟376）。在本實施例中，假設認證資料驗證模組230會先使用識別載入模組220所載入的伺服認證金鑰，以與行動端100之認證資料產生模組150產生行動認證資料相同的演算法對傳輸模組210所接收到的目標資料與時間戳進行運算，藉以在運算後產生伺服認證資料。接著，認證資料驗證模組230會比對所產生的伺服認證資料以及傳輸模組210所接收到的行動認證資料。

【0072】若伺服認證資料與行動認證資料不同，則認證資料驗證模組230會產生表示行動認證資料未通過驗證的驗證結果；而當伺服認證資料與行動認證資料相同，驗證伺服器200的認證資料驗證模組230可以進一步判斷當前之時間與傳輸模組210所接收到之時間戳所表示之時間的時間差是否在預定時間範圍內，若是，則認證資料驗證模組230會產生表示行動認證資料通過驗證的驗證結果，而若當前之時間與時間戳所表示之時間的時間差沒有落在預定時間範圍內，則認證資料驗證模組230將產生表示行動認證資料未通過驗證的驗證結果。

【0073】在驗證伺服器200的認證資料驗證模組230產生驗證結果後，驗證伺服器200的傳輸模組210可以將認證資料驗證模組230所產生的驗證結果傳回驗證裝置290（步驟381）。驗證裝置290在接收到驗證伺服器200所傳送的驗證結果後，可以顯示所接收到的驗證結果。如此，透過本發明，使用者便可以完成身分驗證。

【0074】 以下繼續以第二個實施例來解說本發明的運作系統與方法，並請參照「第3B圖」本發明所提之另一種使用者註冊之方法流程圖以及「第3C圖」。在本實施例中，假設有本發明外部之票務系統欲使用本發明驗證票卷的正確性。

【0075】 首先，與第一實施例相同的，票卷的使用者需要在其所使用的手機（行動端100）上完成註冊程序。

【0076】 使用者可以先操作行動端100申請並下載電子憑證。在使用者完成電子憑證的下載後，行動端100的讀取模組120可以讀取行動端100所使用的電話門號（身分識別資料），行動端100的傳輸模組110可以透過SSL或VPN等安全通道，將身分識別資料傳送給驗證伺服器200（步驟312）。

【0077】 在驗證伺服器200的傳輸模組210接收到行動端100所傳送的身分識別資料後，驗證伺服器200的驗證資料產生模組250可以產生一次性的驗證資料，並將所產生的驗證資料以及傳輸模組210所接收到的身分識別資料做爲一筆資料暫存在驗證伺服器200的儲存媒體201中，以及透過傳輸模組210將所產生的驗證資料傳送給行動端100（步驟316）。在本實施例中，假設傳輸模組210是透過簡訊將驗證資料傳送到使用所接收到之身分識別資料（電話號碼）的行動端100。

【0078】 在行動端100接收到包含驗證資料的簡訊後，行動端100的讀取模組120可以讀取簡訊中的驗證資料，或是行動端100的輸入模組130可以提供使用者輸入記錄於簡訊中的驗證資料，如此，行動端100的傳輸模組110可以再次透過SSL或VPN的連線，將簡訊中的驗證資料、讀取模組120先前所讀取到的身分識別資料、以及儲存於行動端100之儲存媒體中的電子憑證傳送給驗證伺服器200（步驟318b）。

【0079】在驗證伺服器200的傳輸模組210接收到行動端100所傳送的驗證資料、身分識別資料以及電子憑證後，驗證伺服器200的驗證資料檢查模組260可以如第一實施例中的描述，判斷傳輸模組210所接收到的驗證資料是否正確（步驟321）。並在驗證資料檢查模組260判斷傳輸模組210所接收到的驗證資料正確時，驗證伺服器200的憑證驗證模組280可以進一步判斷傳輸模組210所接收到的電子憑證是否正確（步驟325）。

【0080】在驗證伺服器200的驗證資料檢查模組260判斷驗證伺服器200之傳輸模組210所接收到的驗證資料以及驗證伺服器200的憑證驗證模組判斷傳輸模組210所接收到的電子憑證都正確時，驗證伺服器200的憑證驗證模組280可以將傳輸模組210所接收到之身分識別資料以及電子憑證中的公鑰（伺服認證金鑰）做爲一筆資料，儲存至驗證伺服器200的儲存媒體201中（步驟327），如此，便完成註冊程序。

【0081】在註冊程序完成後，當票務系統欲驗證使用者所擁有的票卷時，使用者可以在手機（行動端100）上進行操作，藉以讓產生票卷之外部伺服器或外部應用程式可以將票卷資料提供給行動端100。在本實施例中，票卷資料是以明文被提供給行動端100。

【0082】如此，行動端100的讀取模組120可以至行動端100的儲存媒體中取得目標資料以及身分識別資料（步驟332），並載入電子憑證中的私鑰（行動認證金鑰）（步驟336）。在本實施例中，讀取模組120所取得的目標資料包含票卷資料以及交易識別資料。

【0083】在行動端100的讀取模組120取得目標資料以及身分識別資料（步驟332），並載入行動認證金鑰（步驟336）後，行動端100的認證資料產生模組

150可以以行動認證金鑰產生與目標資料對應的行動認證資料（步驟340）。在本實施例中，假設認證資料產生模組150會使用行動認證金鑰（私鑰）對目標資料與表示當前時間的時間戳進行簽章以產生行動認證資料。

【0084】在行動端100的認證資料產生模組150以行動認證金鑰產生與目標資料對應的行動認證資料（步驟340）後，行動端100的編碼模組160可以依據行動端100之讀取模組120所取得的目標資料、認證資料產生模組150所使用的時間戳、以及認證資料產生模組150所產生的行動認證資料產生待認證資料（步驟350）。在本實施例中，假設編碼模組160所產生的待認證資料爲QR-code。

【0085】在行動端100的編碼模組160產生待認證資料（步驟350）後，行動端100的顯示模組180可以顯示編碼模組160所產生的待認證資料（步驟361），使得待認證資料被顯示在執行本發明之行動裝置的顯示螢幕上。

【0086】在行動端100的顯示模組180顯示待認證資料（步驟361）後，使用者可以將執行本發明之行動裝置的顯示螢幕接近驗證裝置290，使得驗證裝置290可以掃瞄被顯示在顯示螢幕上的待認證資料（步驟363）。

【0087】之後，驗證裝置290可以對待認證資料進行解碼以取得行動端100的編碼模組160產生待認證資料所使用的目標資料、時間戳、身分識別資料、以及行動認證資料（步驟367），並將解碼所取得的目標資料、時間戳、身分識別資料、以及行動認證資料傳送到驗證伺服器200。

【0088】在驗證伺服器200的傳輸模組210接收到驗證裝置290所傳送的目標資料、時間戳、身分識別資料、以及行動認證資料後，驗證伺服器200的識別載入模組220可以依據傳輸模組210所接收到的身分識別資料載入伺服認證金鑰（步驟372）。在本實施例中，假設識別載入模組220會至驗證伺服器200的儲存

媒體201中搜尋傳輸模組210所接收到的身分識別資料，並在搜尋到傳輸模組210所接收到的身分識別資料後，讀取在註冊程序中與被搜尋到之身分識別資料一同被儲存的伺服認證金鑰，也就是使用者所申請的公鑰。

【0089】 在驗證伺服器200的識別載入模組220載入伺服認證金鑰（步驟372）後，驗證伺服器200的認證資料驗證模組230可以對驗證伺服器200之傳輸模組210所接收到的行動認證資料進行驗證，並在驗證後產生驗證結果（步驟376）。在本實施例中，假設認證資料驗證模組230會先使用識別載入模組220所載入的伺服認證金鑰（使用者所申請的公鑰）對傳輸模組210所接收到的目標資料與時間戳進行驗章。若驗章失敗，也就是目標資料與時間戳沒有通過驗章伺服認證資料與行動認證資料不同，則認證資料驗證模組230會產生表示行動認證資料未通過驗證的驗證結果；而當伺服認證資料與行動認證資料相同若驗章成功，驗證伺服器200的認證資料驗證模組230可以進一步判斷當前之時間與傳輸模組210所接收到之時間戳所表示之時間的時間差是否在預定時間範圍內，若是，則認證資料驗證模組230會產生表示行動認證資料通過驗證的驗證結果，而若當前之時間與時間戳所表示之時間的時間差沒有落在預定時間範圍內，則認證資料驗證模組230同樣可以產生表示未通過驗證的驗證結果。

【0090】 在驗證伺服器200的認證資料驗證模組230產生驗證結果後，驗證伺服器200的傳輸模組210可以將認證資料驗證模組230所產生的驗證結果傳回驗證裝置290（步驟381）。

【0091】 驗證裝置290在接收到驗證伺服器200所傳送的驗證結果後，可以顯示所接收到的驗證結果（步驟385），並可以依據待認證資料中所包含的交易

識別資料進行對應之交易（步驟390）。如此，透過本發明，便可以完成票卷的驗證。

【0092】綜上所述，可知本發明與先前技術之間的差異在於具有行動端以行動認證金鑰產生與目標資料對應之行動認證資料後，依據目標資料、時間戳、行動認證資料、及身分識別資料產生相對應之待認證資料，驗證裝置掃描被行動端顯示之待認證資料後，對待認證資料進行解碼以取得目標資料、時間戳、身分識別資料及行動認證資料，驗證伺服器依據身分識別資料載入伺服認證金鑰後，以伺服認證金鑰驗證行動認證資料並產生驗證結果之技術手段，藉由此一技術手段可以來解決先前技術所存在可以使用複製的電子條碼冒用身分的問題，進而達成動態提供待認證資料，且能夠快速簡易的進行認證之技術功效。

【0093】再者，本發明之驗證行動端動態顯示之資料之方法，可實現於硬體、軟體或硬體與軟體之組合中，亦可在電腦系統中以集中方式實現或以不同元件散佈於若干互連之電腦系統的分散方式實現。

【0094】雖然本發明所揭露之實施方式如上，惟所述之內容並非用以直接限定本發明之專利保護範圍。任何本發明所屬技術領域中具有通常知識者，在不脫離本發明所揭露之精神和範圍的前提下，對本發明之實施的形式上及細節上作些許之更動潤飾，均屬於本發明之專利保護範圍。本發明之專利保護範圍，仍須以所附之申請專利範圍所界定者爲準。

【符號說明】

【0095】

100　　行動端

110	傳輸模組
120	讀取模組
130	輸入模組
140	加解密模組
150	認證資料產生模組
160	編碼模組
180	顯示模組
200	驗證伺服器
201	儲存媒體
210	傳輸模組
220	識別載入模組
230	認證資料驗證模組
250	驗證資料產生模組
260	驗證資料檢查模組
270	金鑰產生模組
280	憑證驗證模組
290	驗證裝置
400	網際網路
步驟 301	行動端下載包含行動認證金鑰及伺服認證金鑰之電子憑證
步驟 312	行動端傳送身分識別資料至驗證伺服器
步驟 316	驗證伺服器傳送驗證資料至行動端
步驟 318a	行動端傳送驗證資料至驗證伺服器
步驟 318b	行動端傳送驗證資料及電子憑證至驗證伺服器
步驟 321	驗證伺服器判斷驗證資料是否正確
步驟 323	驗證伺服器產生伺服認證金鑰
步驟 325	驗證伺服器驗證電子憑證是否正確
步驟 327	驗證伺服器儲存身分識別資料及伺服認證金鑰
步驟 328	驗證伺服器傳送伺服認證金鑰至行動端
步驟 329	行動端以伺服認證金鑰做爲行動認證金鑰
步驟 332	行動端取得目標資料及身分識別資料

步驟 336　行動端載入預先儲存之行動認證金鑰

步驟 340　行動端以行動認證金鑰產生與目標資料及時間戳對應之行動認證資料

步驟 350　行動端依據目標資料、時間戳、行動認證資料、身分識別資料產生相對應之待認證資料

步驟 361　行動端顯示待認證資料

步驟 363　驗證裝置掃描被行動端顯示之待認證資料

步驟 367　驗證裝置對待認證資料進行解碼以取得目標資料、時間戳、身分識別資料及行動認證資料

步驟 369　驗證裝置傳送目標資料、時間戳、身分識別資料及行動認證資料至驗證伺服器

步驟 372　驗證伺服器依據身分識別資料載入伺服認證金鑰

步驟 376　驗證伺服器以伺服認證金鑰驗證行動認證資料並產生驗證結果

步驟 381　驗證伺服器傳送驗證結果至驗證裝置

步驟 385　驗證裝置顯示驗證結果

步驟 390　驗證裝置依據待認證資料中所包含之交易識別資料進行對應交易

【發明申請專利範圍】

【第1項】一種驗證行動端動態顯示之資料之方法，該方法至少包含下列步驟：

一行動端取得一目標資料及一身分識別資料；

該行動端載入預先儲存之一行動認證金鑰；

該行動端以該行動認證金鑰產生與該目標資料及一時間戳對應之一行動認證資料；

該行動端至少依據該目標資料、該時間戳、該行動認證資料、及一身分識別資料產生相對應之一待認證資料；

該行動端顯示該待認證資料；

一驗證裝置掃描被該行動端顯示之該待認證資料；

該驗證裝置對該待認證資料進行解碼以取得該目標資料、該時間戳、該身分識別資料及該行動認證資料；

該驗證裝置傳送該目標資料、該時間戳、該身分識別資料及該行動認證資料至一驗證伺服器；

該驗證伺服器依據該身分識別資料載入一伺服認證金鑰；

該驗證伺服器以該伺服認證金鑰驗證該行動認證資料並產生一驗證結果；

該驗證伺服器傳送該驗證結果至該驗證裝置；及

該驗證裝置顯示該驗證結果。

【第2項】如申請專利範圍第1項所述之驗證行動端動態顯示之資料之方法，其中該方法於該驗證伺服器傳送該驗證結果至該驗證裝置之步驟後，更包

含該驗證裝置依據該待認證資料中所包含之一交易識別資料進行對應交易之步驟。

【第3項】如申請專利範圍第1項所述之驗證行動端動態顯示之資料之方法，其中該方法於該行動端載入預先儲存之該行動認證金鑰之步驟前，更包含該行動端傳送該身分識別資料至該驗證伺服器，該驗證伺服器傳送一驗證資料至該行動端，該行動端傳送該驗證資料回該驗證伺服器，該驗證伺服器判斷該驗證資料正確後產生該伺服認證金鑰、儲存該身分識別資料及該伺服認證金鑰、並傳送該伺服認證金鑰至該行動端做爲該行動認證金鑰之步驟。

【第4項】如申請專利範圍第1項所述之驗證行動端動態顯示之資料之方法，其中該方法於該行動端載入預先儲存之該行動認證金鑰之步驟前，更包含該行動端下載包含該行動認證金鑰及該伺服認證金鑰之一電子憑證，該行動端傳送該身分識別資料至該驗證伺服器，該驗證伺服器傳送一驗證資料至該行動端，該行動端傳送該驗證資料及該電子憑證至該驗證伺服器，該驗證伺服器判斷該驗證資料正確並驗證該電子憑證正確後儲存該身分識別資料及該伺服認證金鑰之步驟。

【第5項】如申請專利範圍第1項所述之驗證行動端動態顯示之資料之方法，其中該行動端取得該目標資料之步驟爲讀取儲存於該行動端中之資料、接收外部伺服器或應用程式所提供之資料、解析一維條碼、二維條碼、或影像以取得資料、及/或提供輸入資料。

【第6項】如申請專利範圍第1項所述之驗證行動端動態顯示之資料之方法，其中該驗證伺服器驗證該行動認證資料之步驟爲該驗證伺服器以該伺服認

證金鑰產生與該目標資料對應之一伺服認證資料，並比對該行動認證資料與該伺服認證資料之步驟。

【第7項】一種驗證行動端動態顯示之資料之系統，該系統至少包含：

一驗證裝置，用以掃描一行動端所顯示之一待認證資料，及用以對該待認證資料進行解碼以取得一目標資料、一時間戳、一身分識別資料及一行動認證資料，其中，該待認證資料係該行動端以該行動認證金鑰產生，且與該目標資料及該時間戳對應；及

一驗證伺服器，與該驗證裝置連接，用以依據該身分識別資料載入一伺服認證金鑰，並以該伺服認證金鑰驗證該行動認證資料以產生一驗證結果，及用以傳送該驗證結果至該驗證裝置顯示。

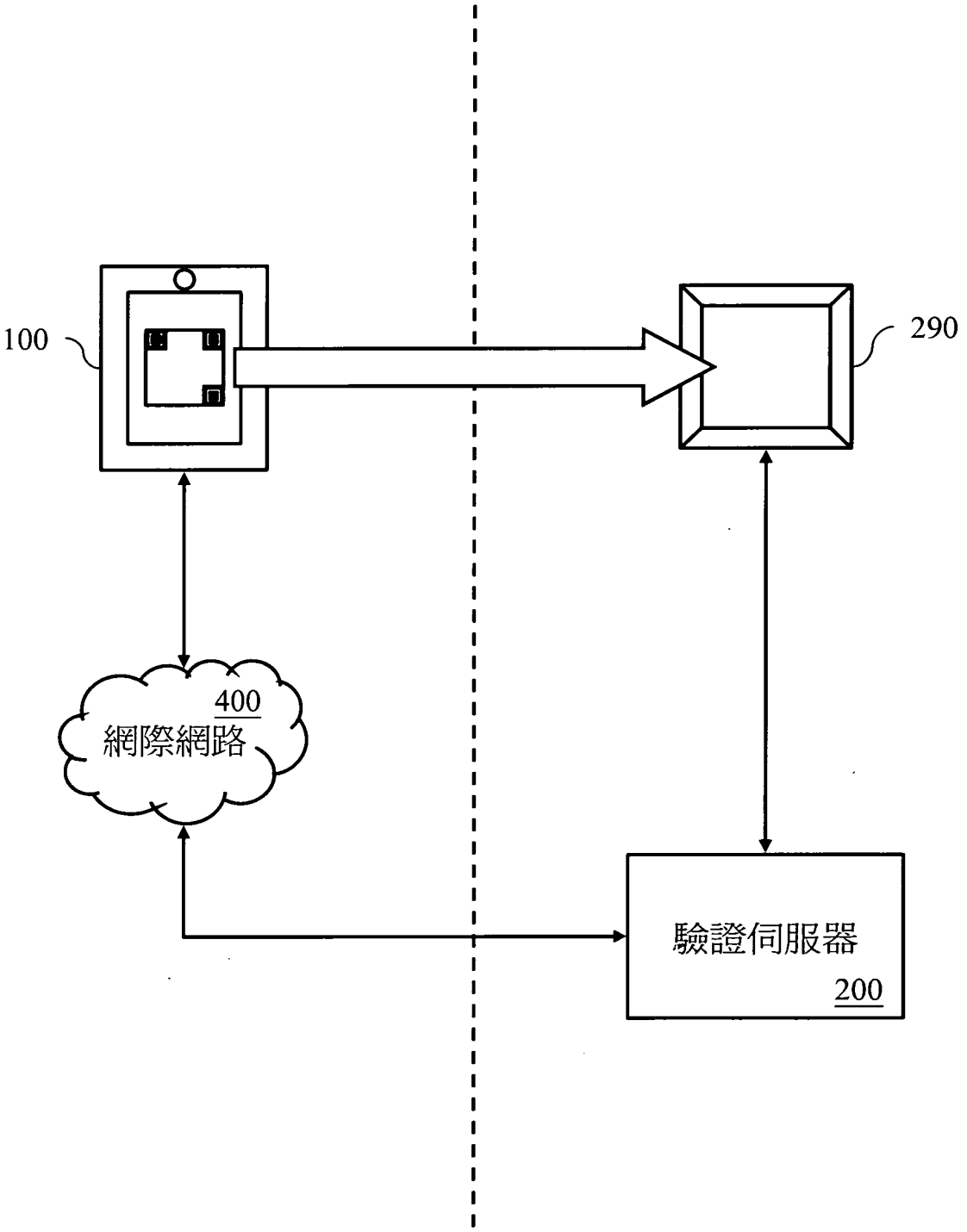
【第8項】如申請專利範圍第7項所述之驗證行動端動態顯示之資料之系統，其中該驗證裝置更用以依據該待認證資料中所包含之一交易識別資料進行對應交易。

【第9項】如申請專利範圍第7項所述之驗證行動端動態顯示之資料之系統，其中該驗證伺服器更用以於接收到該行動端所傳送之該身分識別資料時，並傳送一驗證資料至該行動端，及用以判斷該行動端所傳送之該驗證資料正確後，產生該伺服認證金鑰、儲存該身分識別資料及該伺服認證金鑰、並傳送該伺服認證金鑰至該行動端做爲該行動認證金鑰。

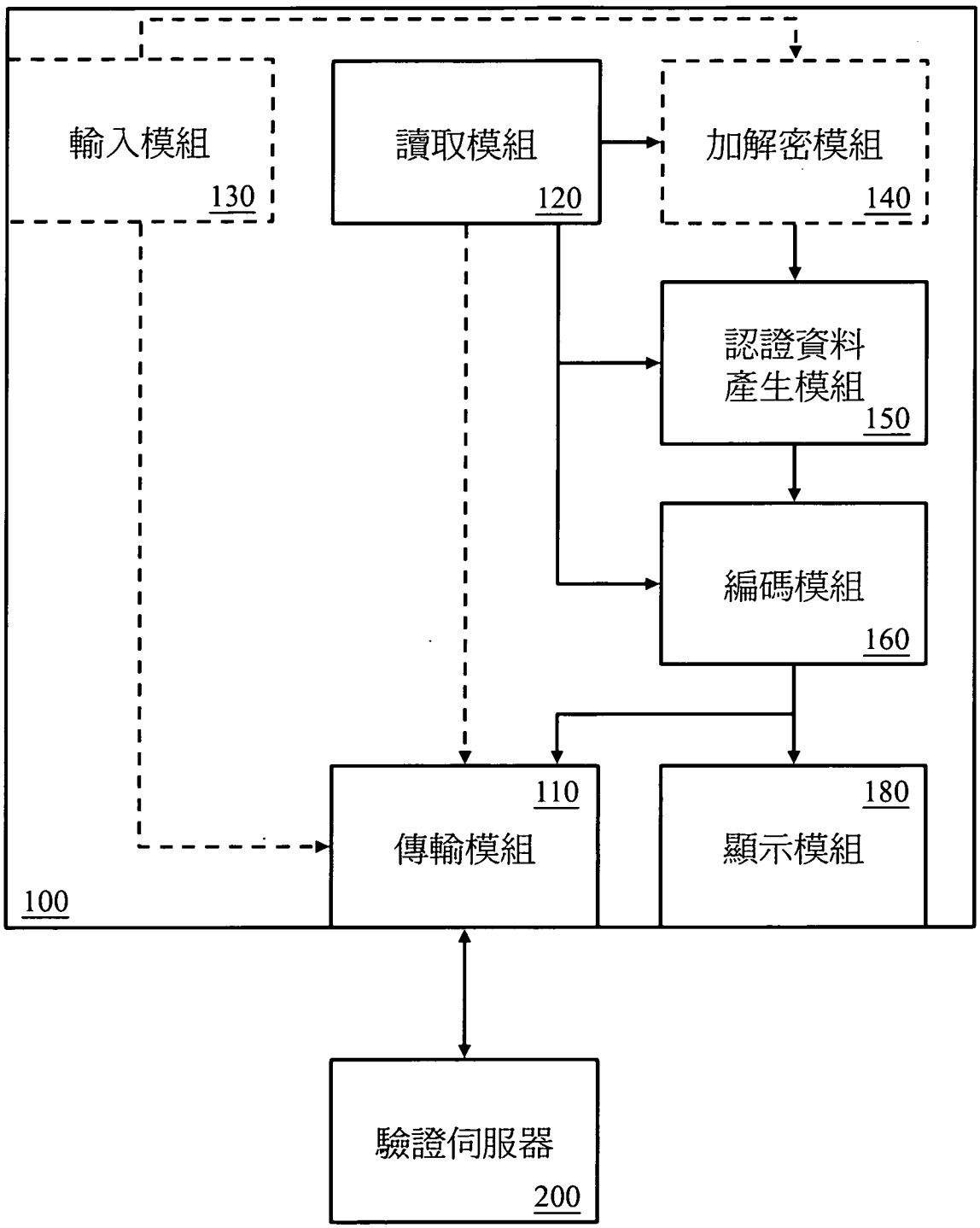
【第10項】如申請專利範圍第7項所述之驗證行動端動態顯示之資料之系統，其中該驗證伺服器更用以於接收到該行動端所傳送之該身分識別資料後，傳送一驗證資料至該行動端，及用以於判斷該行動端所傳送之該驗證資料正確

且該行動端所傳送之包含該行動認證金鑰及該伺服認證金鑰之一電子憑證正確後，儲存該身分識別資料及該伺服認證金鑰。

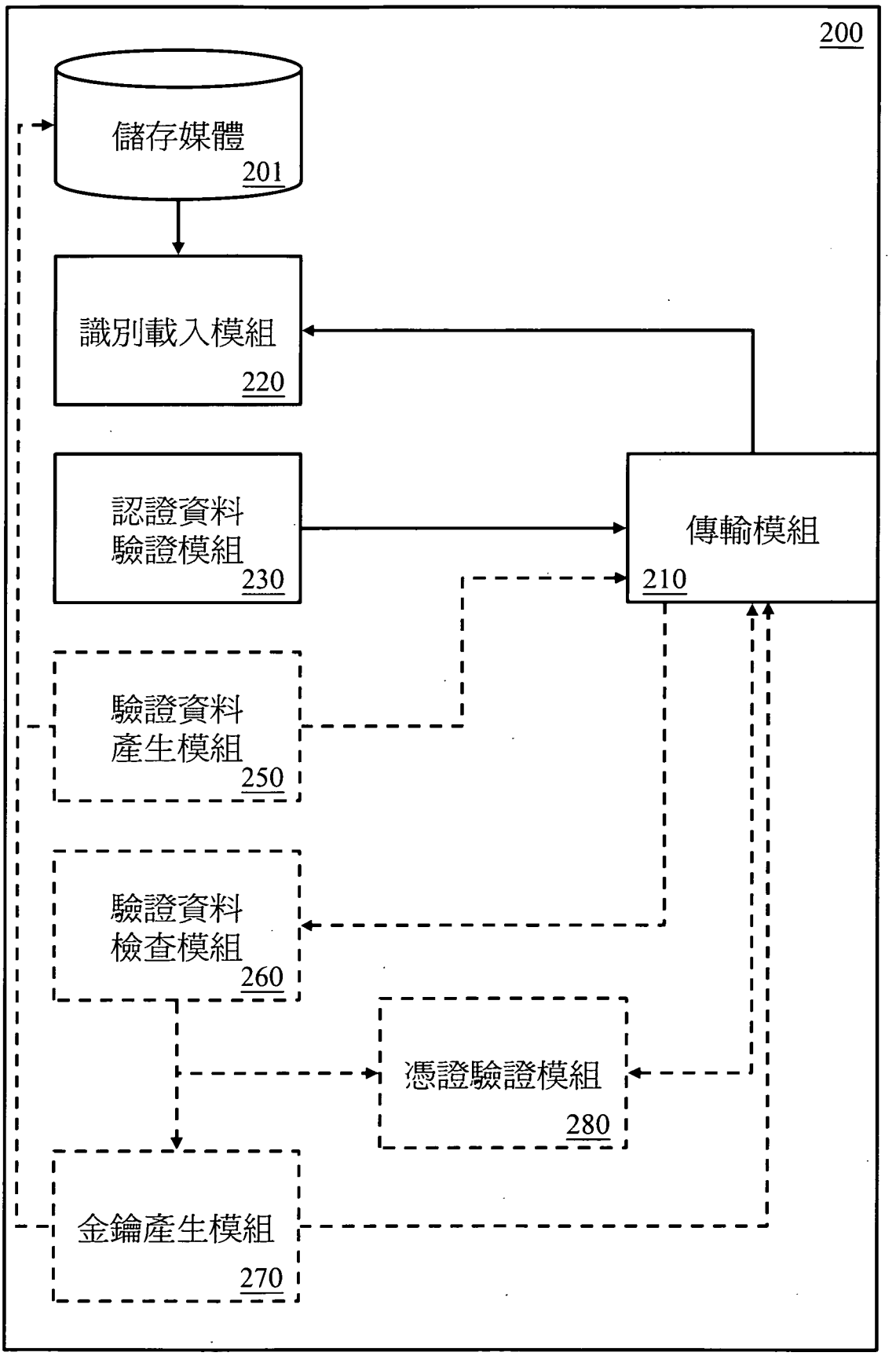
【發明圖式】



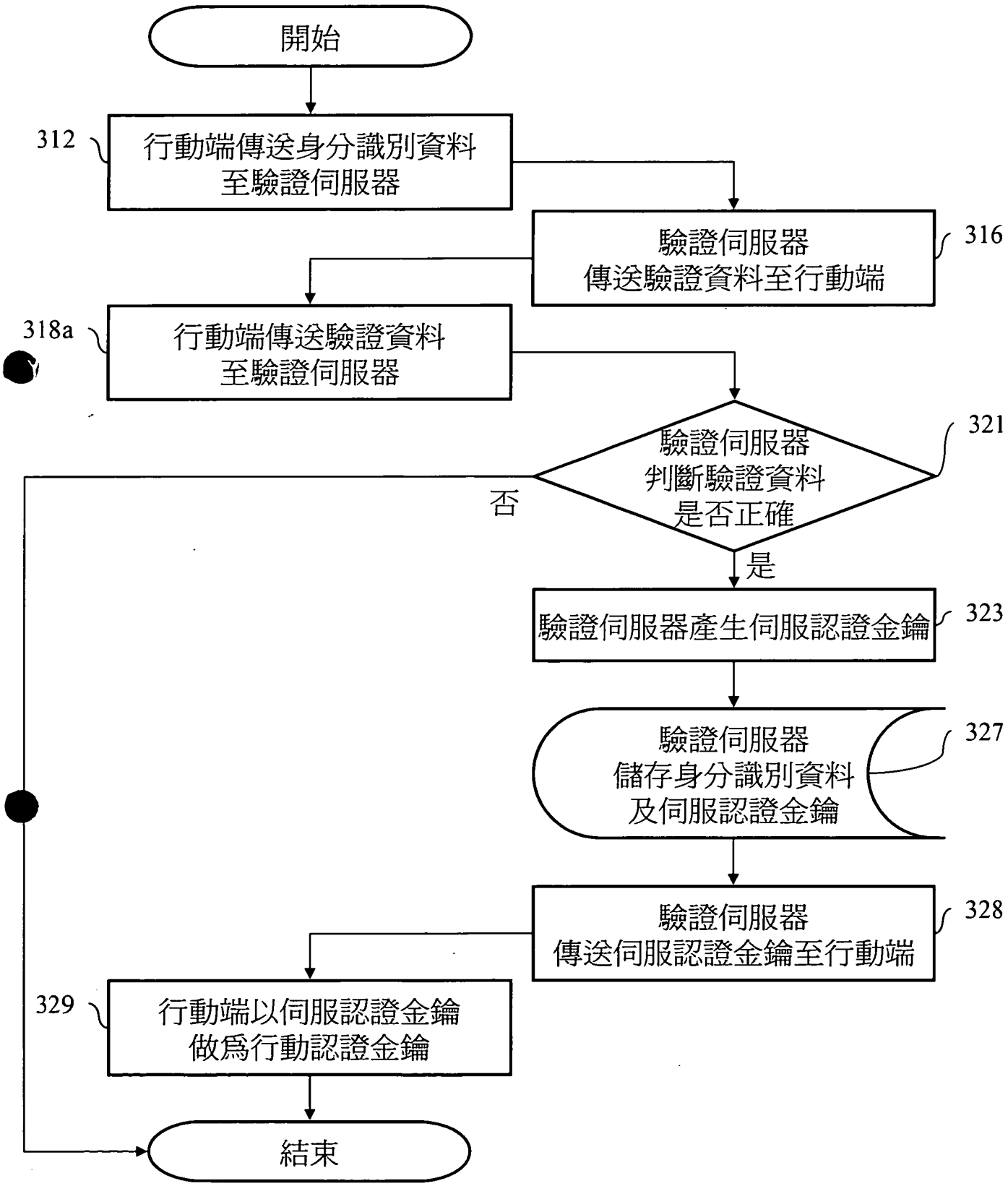
【第1圖】


輸入模組
130
讀取模組
120
加解密模組
140
認證資料
產生模組
150
編碼模組
160
110
傳輸模組
180
顯示模組
100
驗證伺服器
200

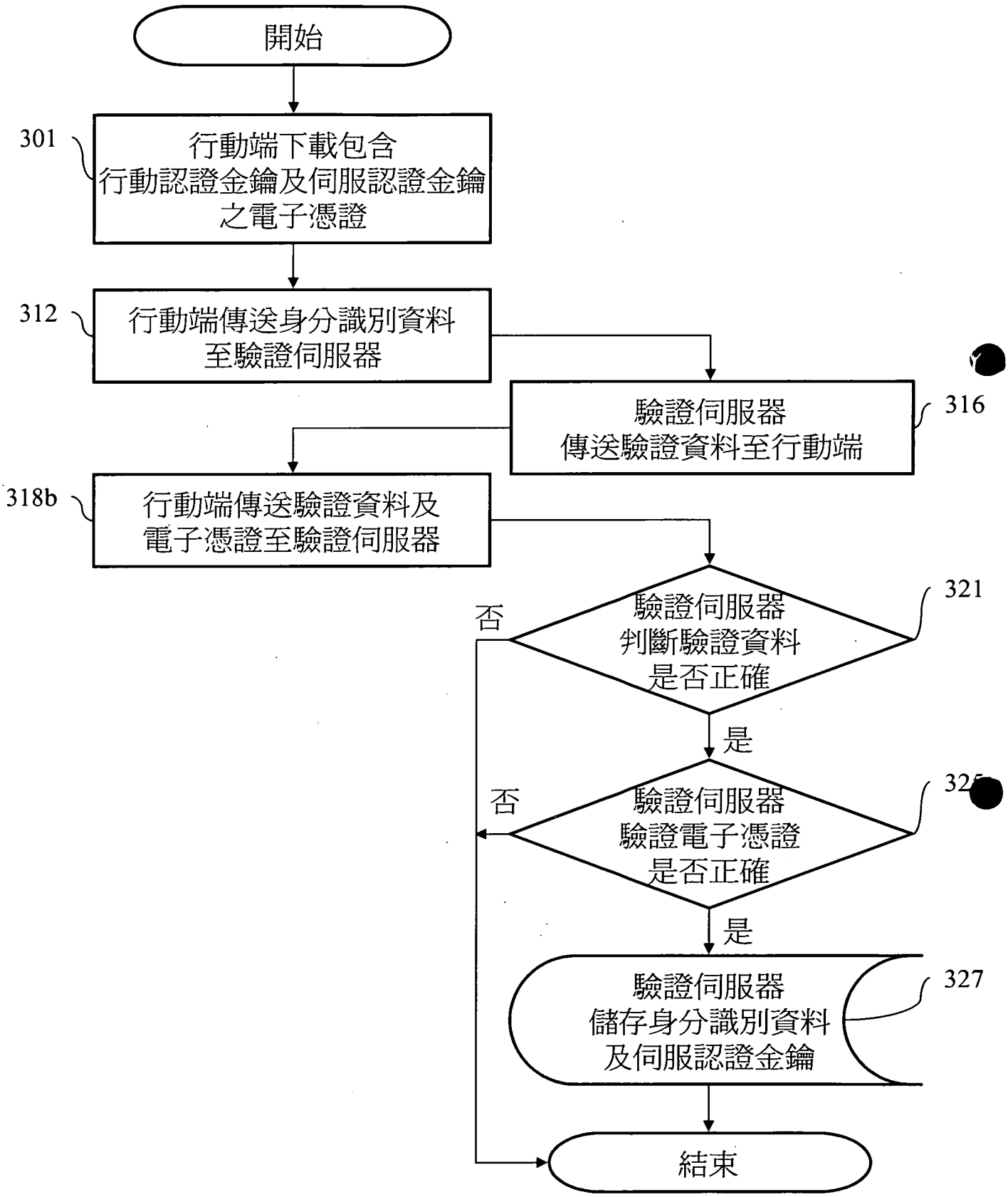
【第2A圖】


200
儲存媒體
201
識別載入模組
220
認證資料
驗證模組
230
傳輸模組
210
驗證資料
產生模組
250
驗證資料
檢查模組
260
憑證驗證模組
280
金鑰產生模組
270

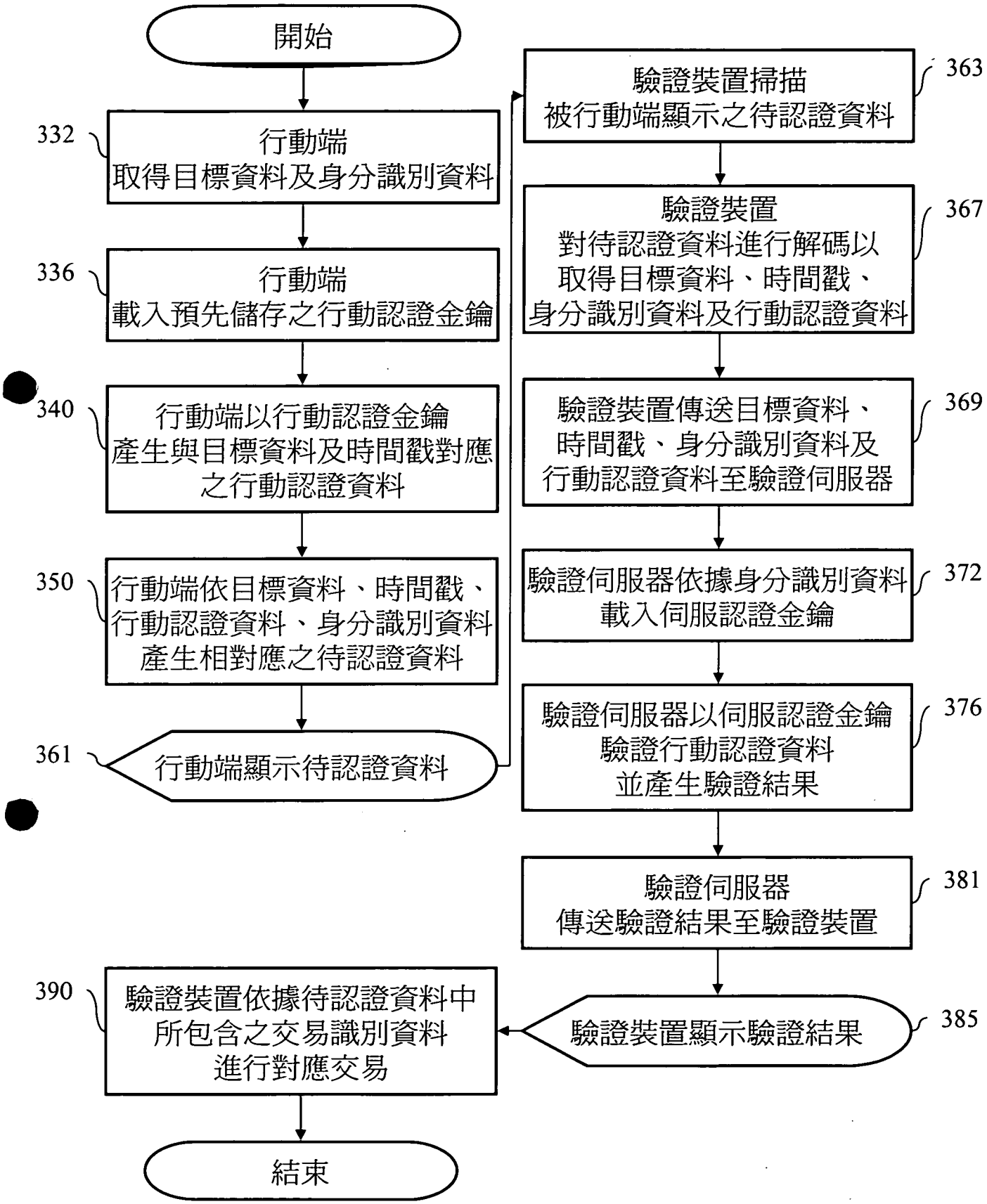
【第2B圖】


開始
312
行動端傳送身分識別資料
至驗證伺服器
驗證伺服器
傳送驗證資料至行動端
316
318a
行動端傳送驗證資料
至驗證伺服器
驗證伺服器
判斷驗證資料
是否正確
321
否
是
驗證伺服器產生伺服認證金鑰
323
驗證伺服器
儲存身分識別資料
及伺服認證金鑰
327
驗證伺服器
傳送伺服認證金鑰至行動端
328
329
行動端以伺服認證金鑰
做爲行動認證金鑰
結束

【第3A圖】


開始
301
行動端下載包含
行動認證金鑰及伺服認證金鑰
之電子憑證
312
行動端傳送身分識別資料
至驗證伺服器
驗證伺服器
傳送驗證資料至行動端
316
318b
行動端傳送驗證資料及
電子憑證至驗證伺服器
驗證伺服器
判斷驗證資料
是否正確
321
否
是
驗證伺服器
驗證電子憑證
是否正確
否
是
驗證伺服器
儲存身分識別資料
及伺服認證金鑰
327
結束

【第3B圖】


開始
332
行動端
取得目標資料及身分識別資料
336
行動端
載入預先儲存之行動認證金鑰
340
行動端以行動認證金鑰
產生與目標資料及時間戳對應
之行動認證資料
350
行動端依目標資料、時間戳、
行動認證資料、身分識別資料
產生相對應之待認證資料
361
行動端顯示待認證資料
363
驗證裝置掃描
被行動端顯示之待認證資料
367
驗證裝置
對待認證資料進行解碼以
取得目標資料、時間戳、
身分識別資料及行動認證資料
369
驗證裝置傳送目標資料、
時間戳、身分識別資料及
行動認證資料至驗證伺服器
372
驗證伺服器依據身分識別資料
載入伺服認證金鑰
376
驗證伺服器以伺服認證金鑰
驗證行動認證資料
並產生驗證結果
381
驗證伺服器
傳送驗證結果至驗證裝置
385
驗證裝置顯示驗證結果
390
驗證裝置依據待認證資料中
所包含之交易識別資料
進行對應交易
結束

【第3C圖】