



(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 I668589 B

(45)公告日：中華民國 108 (2019) 年 08 月 11 日

(21)申請案號：106102208

(22)申請日：中華民國 106 (2017) 年 01 月 20 日

(51)Int. Cl. : G06F21/32 (2013.01)

G06F21/31 (2013.01)

(30)優先權：2016/03/25 中國大陸

201610180030.4

(71)申請人：香港商阿里巴巴集團服務有限公司 (香港地區) ALIBABA GROUP SERVICES
LIMITED (HK)

香港

(72)發明人：孟飛 (CN)

(74)代理人：林志剛

(56)參考文獻：

CN 101340285A

CN 102523213A

US 2011142234A1

審查人員：陳昱潭

申請專利範圍項數：12 項 圖式數：4 共 26 頁

(54)名稱

身份註冊方法及裝置

(57)摘要

本發明公開了一種身份註冊方法及裝置，該方法由終端接收用戶的待驗證的生物特徵資訊，匹配與該待驗證的生物特徵資訊一致的標準生物特徵資訊，當根據該標準生物特徵資訊對應的標識，未查找該標識對應的私鑰時，根據該待驗證的生物特徵資訊，向伺服器註冊該用戶的身份，使伺服器保存該待驗證的生物特徵資訊對應的公鑰。通過上述方法，無論用戶註冊時使用的生物特徵資訊是哪個，只要待驗證的生物特徵資訊已經保存在終端本地，就可直接根據該待驗證的生物特徵資訊，註冊該用戶的身份，進而完成業務處理，給用戶使用業務帶來很大的便利，同時也有有效的提高了使用業務的成功率。

指定代表圖：

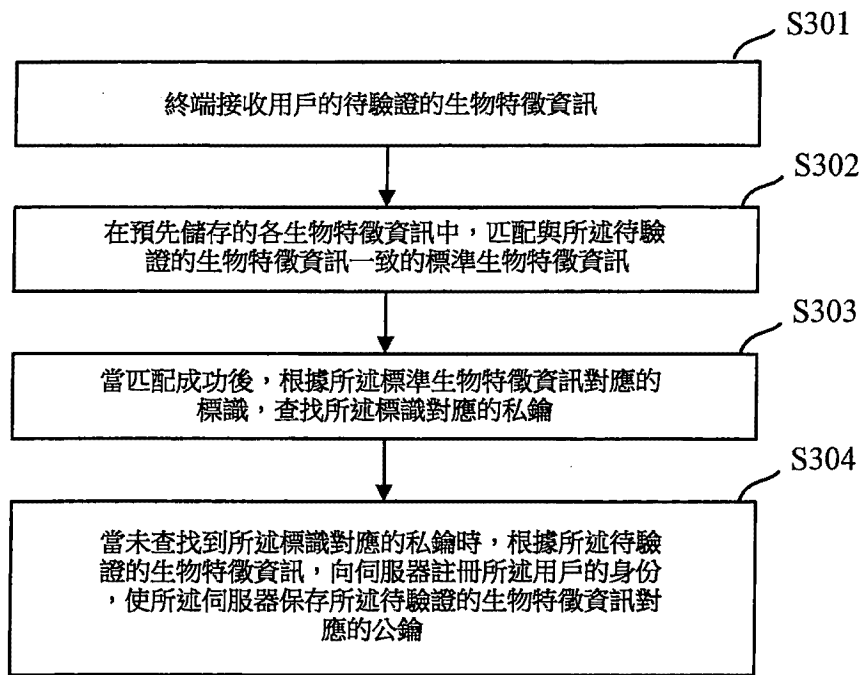


圖 3

發明專利說明書

(本說明書格式、順序，請勿任意更動)

【發明名稱】(中文/英文)

身份註冊方法及裝置

【技術領域】

本發明係關於計算機技術領域，尤其係關於一種身份註冊方法及裝置。

【先前技術】

隨著網路技術的不斷發展，人們通過網路使用業務已經成為生活中不可獲取的一部分，如，人們通過網路使用天氣查詢業務。

目前，為了提高用戶在使用業務過程中的資訊的安全性，因此，用戶在使用業務之前，需要針對該業務，預先註冊該用戶的身份，後續，該用戶在通過網路使用業務時，需要對該用戶的身份進行驗證，當驗證通過後，用戶才可以使用該業務，如，採用指紋資訊來表示用戶的身份，因此，需要預先註冊用戶指紋資訊。

由於在實際應用中指紋資訊識別在終端中已經應用的越來越普遍，如，利用用戶的指紋資訊來對鎖屏界面進行解鎖，因此，針對任一業務，該業務的伺服器通過用戶的指紋資訊來註冊該用戶的身份以及後續通過用戶的指紋資訊驗證用戶的身份的整個過程，均可利用終端去完成。

進一步的，隨著計算機技術的不斷完善，終端內部可以同時保存有用戶的多個指紋資訊，而針對任一業務，在通過用戶上傳的指紋資訊來註冊該用戶的身份時，首先需要通過終端來驗證該指紋資訊是否為已儲存在終端內的多個指紋資訊中的一個，如果是，則終端可根據該指紋資訊，向伺服器註冊該用戶的身份，如果否，則終端直接提示用戶身份註冊失敗。

在現有技術中，用戶的指紋資訊的註冊過程具體如圖 1 所示：

S101：終端接收到用戶的註冊操作；

S102：採集該用戶的指紋資訊；

S103：判斷該指紋資訊是否已經預先儲存在終端本地中，如果是則執行 S104，若是否則執行 S105；

S104：在終端本地查詢出預先儲存的該指紋資訊對應的標識，並產生該標識對應的私鑰和公鑰，將該私鑰與該指紋資訊對應的標識的對應關係儲存到終端本地中，將該公鑰與該指紋資訊對應的標識的對應關係發送給伺服器儲存。

S105：提示用戶註冊失敗。

後續，用戶使用業務的過程具體如圖 2 所示：

S201：終端接收用戶的指紋資訊；

S202：匹配與該指紋資訊一致的標準生物特徵資訊；

S203：根據該標準生物特徵資訊對應的標識，查找該標識對應的私鑰；

S204：當查找到該標識對應的私鑰時，則通過私鑰對業務資訊進行簽名，並將簽名後的業務資訊以及該指紋資訊對應的標識攜帶在業務處理請求中發送給伺服器，使伺服器確定接收到的該業務處理請求中攜帶的標識對應的公鑰，並根據該公鑰以及業務資訊進行業務處理，當未查找到該標識對應的私鑰時，則提示用戶業務處理失敗。

但是，在實際應用中，如果用戶遺忘了錄入的指紋是哪個手指的指紋，則會導致用戶需要進行多次指紋驗證，給用戶使用業務帶來很大的不便，同時也會降低使用業務的成功率，與此同時，如果用戶註冊時所用的手指在日常生活中出現受傷的情況，則會直接導致用戶無法通過驗證而無法使用業務。

【發明內容】

本發明實施例提供一種身份註冊方法及裝置，用以解決現有技術中用戶遺忘了錄入的指紋是哪個手指的指紋，給用戶使用業務帶來很大的不便以及用戶註冊時所用的手指在日常生活中出現受傷的情況，則無法通過驗證而無法使用業務的問題。

本發明實施例提供的一種身份註冊方法，所述方法包括：

終端接收用戶的待驗證的生物特徵資訊；

在預先儲存的各生物特徵資訊中，匹配與所述待驗證的生物特徵資訊一致的標準生物特徵資訊；

當匹配成功後，根據所述標準生物特徵資訊對應的標識，查找所述標識對應的私鑰；

當未查找到所述標識對應的私鑰時，根據所述待驗證的生物特徵資訊，向伺服器註冊所述用戶的身份，使所述伺服器保存所述待驗證的生物特徵資訊對應的公鑰。

本發明實施例提供的一種身份註冊裝置，所述裝置包括：

接收模組，用於接收用戶的待驗證的生物特徵資訊；

匹配模組，用於在預先儲存的各生物特徵資訊中，匹配與所述待驗證的生物特徵資訊一致的標準生物特徵資訊；

查找模組，用於當匹配成功後，根據所述標準生物特徵資訊對應的標識，查找所述標識對應的私鑰；

註冊模組，用於當未查找到所述標識對應的私鑰時，根據所述待驗證的生物特徵資訊，向伺服器註冊所述用戶的身份，使所述伺服器保存所述待驗證的生物特徵資訊對應的公鑰。

本發明實施例提供一種身份註冊方法及裝置，該方法由終端接收用戶的待驗證的生物特徵資訊，匹配與該待驗證的生物特徵資訊一致的標準生物特徵資訊，當匹配成功後，根據該標準生物特徵資訊對應的標識，查找該標識對應的私鑰，當未查找到該標識對應的私鑰時，根據該待驗證的生物特徵資訊，向伺服器註冊該用戶的身份，使伺服器保存該待驗證的生物特徵資訊對應的公鑰。通過上述方

法，無論用戶註冊時使用的生物特徵資訊是哪個，終端只要能夠匹配出與待驗證的生物特徵資訊一致的標準生物特徵資訊，即使根據該標準生物特徵資訊對應的標識，沒有在終端本地查找到該標識對應的私鑰，也可直接根據該待驗證的生物特徵資訊，註冊該用戶的身份，進而完成業務處理，給用戶使用業務帶來很大的便利，同時也有有效的提高了使用業務的成功率。

【圖式簡單說明】

此處所說明的附圖用來提供對本發明的進一步理解，構成本發明的一部分，本發明的示意性實施例及其說明用於解釋本發明，並不構成對本發明的不當限定。在附圖中：

圖 1 為本發明實施例提供的現有技術中用戶的指紋資訊的註冊過程示意圖；

圖 2 為本發明實施例提供的現有技術中用戶使用業務的過程示意圖；

圖 3 為本發明實施例提供的身份註冊過程示意圖；

圖 4 為本發明實施例提供的身份註冊裝置結構示意圖。

【實施方式】

為使本發明的目的、技術方案和優點更加清楚，下面將結合本發明具體實施例及相應的附圖對本發明技術方案

進行清楚、完整地描述。顯然，所描述的實施例僅是本發明一部分實施例，而不是全部的實施例。基於本發明中的實施例，本領域普通技術人員在沒有做出創造性勞動前提下所獲得的所有其他實施例，都屬本發明保護的範圍。

圖 3 為本發明實施例提供的身份註冊過程，具體包括以下步驟：

S301：終端接收用戶的待驗證的生物特徵資訊。

在實際應用中，為了提高用戶使用業務過程中的資訊的安全性，因此，用戶在使用業務的過程中，首先需要對當前用戶的身份進行驗證，以此確認當前用戶的身份是合法的。

因此，在本發明中，首先接收用戶的待驗證的生物特徵資訊，而由於在實際應用中生物特徵資訊識別在終端（如，手機）中已經應用的越來越普遍，因此，接收用戶的待驗證的生物特徵資訊可以是由終端完成的，終端在接收完成後並做出相應的響應，其中，所述生物特徵資訊指的是用戶的體征，可以是眼睛的虹膜，也可以是手指的指紋，主要用於唯一表徵用戶的身份。

另外，由於在實際應用中，在驗證當前用戶的身份時，驗證用戶的指紋資訊已經應用的越來越普遍，而且技術也比較成熟，因此，以下以生物特徵資訊為指紋資訊為例進行詳細說明。

例如，假設某論壇只給註冊過帳號的用戶提供查詢資料的業務，並且用戶在登錄帳號時可以使用指紋資訊進行

登錄，因此，當用戶需要在該論壇中查詢資料時，用戶點開位於手機（即，終端）上的該論壇對應的應用，並按壓指紋，後續，手機（即，終端）接收到用戶的待驗證的指紋資訊，並執行步驟 S302。

S302：在預先儲存的各生物特徵資訊中，匹配與所述待驗證的生物特徵資訊一致的標準生物特徵資訊。

由於在實際應用中指紋資訊（即，生物特徵資訊）識別在終端中已經應用的越來越普遍，如，利用用戶的指紋資訊來對鎖屏界面進行解鎖，因此，針對任一業務，該業務的伺服器通過用戶的指紋資訊來註冊該用戶的身份以及後續通過用戶的指紋資訊驗證用戶的身份的整個過程，均可利用終端中已儲存的指紋資訊去完成，也就是說，只要終端隨機存取記憶體儲存有指紋資訊，在本發明中均可利用該指紋資訊去完成整個業務處理。

在此需要說明的是，終端中已經儲存的指紋資訊可以是用戶使用終端的其他功能的時候錄入進去的，並不是用戶在使用業務之前針對該業務註冊身份所用的指紋資訊，如，用戶使用終端的通過指紋資訊對鎖屏界面進行解鎖的功能，終端可將該指紋資訊儲存到終端本地。

另外，為了在本發明中能夠區分出已儲存的指紋資訊，和用戶在使用業務時終端接收的指紋資訊，因此，可將已儲存的指紋資訊作為標準指紋資訊（即，標準生物特徵資訊），主要用於校驗用戶在使用業務的過程中，是否能夠通過身份驗證，並為該用戶提供業務處理。

因此，在本發明中，終端在接收到用戶的待驗證的指紋資訊（即，生物特徵資訊）後，直接在終端本地匹配與該待驗證的指紋資訊一致的標準指紋資訊（即，標準生物特徵資訊）。

延續上例，手機在接收到用戶的待驗證的指紋資訊後，在手機本地匹配與該待驗證的指紋資訊一致的標準指紋資訊，假設匹配到了與該待驗證的指紋資訊一致的標準指紋資訊。

S303：當匹配成功後，根據所述標準生物特徵資訊對應的標識，查找所述標識對應的私鑰。

在本發明中，為了區分出已經儲存到終端本地的每個指紋資訊（即，生物特徵資訊），因此，終端可在儲存指紋資訊時，給每個指紋資訊分配一個指紋資訊標識（即，生物特徵資訊標識）。

另外，為了後續業務對應的伺服器驗證用戶身份，也就是說，業務對應的伺服器需要知道到底是哪個用戶在使用業務，因此，在本發明中，需要根據註冊時所使用的指紋資訊對應的標識，產生該標識對應的一個私鑰和一個公鑰，該私鑰和公鑰均代表了用戶的身份，並將產生的私鑰儲存在終端本地，終端在向伺服器發送業務處理請求時，需要使用私鑰對業務處理請求進行簽名，將簽名後的業務處理請求發送給伺服器。

因此，在本發明中，終端在匹配到與該待驗證的指紋資訊一致的標準指紋資訊後，需要根據該標準指紋資訊對

應的標識，查找該標識對應的私鑰。

延續上例，手機在匹配到與該待驗證的指紋資訊一致的標準指紋資訊後，根據該標準指紋資訊對應的標識，查找該標識對應的私鑰。

S304：當未查找到所述標識對應的私鑰時，根據所述待驗證的生物特徵資訊，向伺服器註冊所述用戶的身份，使所述伺服器保存所述待驗證的生物特徵資訊對應的公鑰。

在本發明中，如果終端在步驟 S302 中匹配出了與待驗證的指紋資訊一致的標準指紋資訊，但是根據該標準指紋資訊對應的標識，卻沒有查找該標識對應的私鑰，說明該待驗證的指紋資訊確實是該用戶的，但不是註冊時所使用的指紋資訊，為了能夠繼續為該用戶提供所需的業務，可直接根據待驗證的指紋資訊（即，生物特徵資訊），向伺服器註冊該用戶的身份。

另外，本發明提供了一個註冊用戶的身份的具體過程，具體如下：

根據與該待驗證的生物特徵資訊匹配的標準生物特徵資訊對應的標識，產生該標識對應的私鑰和公鑰，將該標識與產生的私鑰的對應關係儲存在該終端本地，將該標識與產生的公鑰的對應關係發送給伺服器保存。

在此需要說明的是，標準生物特徵資訊有唯一對應的標準生物特徵資訊的標識，標準生物特徵資訊的標識有唯一對應的私鑰和公鑰，也就是說，標準生物特徵資訊、標

準生物資訊的標識與私鑰公鑰是一一對應的，而在本發明中，如果待驗證的生物特徵資訊已經存在在終端本地，則在步驟 S302 中就能夠唯一匹配到一個標準生物特徵資訊，也就是說，將該標識與產生的公鑰的對應關係發送給伺服器保存也可以說使該伺服器保存待驗證的生物特徵資訊對應的公鑰。

為了進一步的提高用戶使用業務的資訊的安全性，也就是說，雖然在終端本地中已經儲存了沒有查找到私鑰的指紋資訊（即，生物特徵資訊），但是也有可能是不是該用戶的指紋資訊，因此，在本發明中，在根據待驗證的生物特徵資訊，向伺服器註冊該用戶的身份之前，可提示用戶輸入使用業務的密碼，並接收用戶輸入的密碼，驗證密碼是否正確，如果驗證正確，則可根據待驗證的生物特徵資訊，向伺服器註冊該用戶的身份，如果驗證不正確，則不根據待驗證的生物特徵資訊，向伺服器註冊該用戶的身份，並提示用戶業務處理失敗。

另外，在此需要說明是，終端在未查找到所述標識對應的私鑰時，也可直接返回給用戶業務處理失敗，此時，用戶要想繼續使用業務，只能通過輸入使用業務的密碼才可以繼續使用業務，終端可接收用戶輸入的密碼，並驗證密碼是否正確，如果正確，再根據待驗證的生物特徵資訊，向伺服器註冊用戶的身份。

延續上例，假設手機在查找該標識對應的私鑰的過程中，並沒有查找到，因此，手機提示用戶使用查詢資料業

務的密碼，假設用戶輸入了密碼：xxxx，終端在接收到用戶輸入的密碼：xxxx 後，驗證密碼是正確的，則根據與該待驗證的指紋資訊匹配的標準指紋資訊對應的標識，產生該標識對應的私鑰和公鑰，將該標識與產生的私鑰的對應關係儲存在該手機本地，將該標識與產生的公鑰的對應關係發送給伺服器保存。

通過上述方法，無論用戶註冊時使用的生物特徵資訊是哪個，終端只要能夠匹配出與待驗證的生物特徵資訊一致的標準生物特徵資訊，即使根據該標準生物特徵資訊對應的標識，沒有在終端本地查找到該標識對應的私鑰，也可直接根據該待驗證的生物特徵資訊，註冊該用戶的身份，進而完成業務處理，給用戶使用業務帶來很大的便利，同時也有有效的提高了使用業務的成功率。

進一步的，在實際應用中，當向伺服器註冊完該用戶的身份之後，可根據待驗證的生物特徵資訊，向伺服器發送業務處理請求，使該伺服器根據該待驗證的生物特徵資訊對應的公鑰進行業務處理。

由於在步驟 S304 中已經根據待驗證的指紋資訊（即，生物特徵資訊）重新產生了該指紋資訊的標識對應私鑰和公鑰，並將公鑰發送給伺服器保存，因此，在根據該待驗證的指紋資訊，向該伺服器發送業務處理請求的過程中，本發明具體可以：根據產生的私鑰，對業務資訊進行簽名，並將攜帶有簽名後的業務資訊以及該標識的業務處理請求發送給伺服器，使該伺服器根據業務處理請求中

攜帶的標識，確定該標識對應的公鑰，並根據確定出的公鑰，對業務處理請求中攜帶的業務資訊進行驗簽，以此驗證該用戶的身份，伺服器再對業務資訊進行業務處理。

延續上例，手機根據產生的該標識的私鑰對登錄資訊進行簽名，並將攜帶有簽名後的登錄資訊以及該標識的登錄處理請求發送給伺服器，伺服器根據登錄處理請求中攜帶的標識，查找出該標識對應的公鑰，使用公鑰對登錄處理請求中攜帶的登錄資訊進行驗簽，並完成用戶的登錄。

在實際應用中，使用支付應用對購買的商品進行支付已經變得越來越普遍，在本發明中，以下以業務處理請求為支付請求為例詳細說明本發明。

例如，假設用戶 A 已經在支付應用中註冊了指紋資訊（即，身份資訊），後續，用戶 A 使用支付應用對購買的商品進行支付，用戶 A 點開位於手機（即，終端）上的該支付應用，並按壓指紋，手機在接收到用戶的待驗證的指紋資訊後，在手機本地匹配與該待驗證的指紋資訊一致的標準指紋資訊，假設匹配到了與該待驗證的指紋資訊一致的標準指紋資訊，根據該標準指紋資訊對應的標識，查找該標識對應的私鑰，假設手機在查找該標識對應的私鑰的過程中，並沒有查找到，直接提示用戶輸入支付密碼，手機接收用戶輸入的支付密碼：cccc，並驗證密碼是否正確，假設是正確的，則手機根據與該待驗證的指紋資訊匹配的標準指紋資訊對應的標識，產生該標識對應的私鑰和公鑰，將該標識與產生的私鑰的對應關係儲存在該手機本

地，將該標識與產生的公鑰的對應關係發送給伺服器保存。

後續在對該支付業務進行處理的過程中，手機根據產生的該標識對應的私鑰對支付資訊進行簽名，並將攜帶有簽名後的支付資訊以及該標識的支付處理請求發送給伺服器，伺服器根據支付處理請求中攜帶的標識，查找出該標識對應的公鑰，使用該公鑰對支付資訊進行驗簽，並成功完成支付。

以上為本發明實施例提供的身份註冊方法，基於同樣的思路，本發明還提供了相應的身份註冊裝置，如圖 4 所示。

圖 4 為本發明實施例提供的身份註冊裝置結構示意圖，包括：

接收模組 401，用於接收用戶的待驗證的生物特徵資訊；

匹配模組 402，用於在預先儲存的各生物特徵資訊中，匹配與所述待驗證的生物特徵資訊一致的標準生物特徵資訊；

查找模組 403，用於當匹配成功後，根據所述標準生物特徵資訊對應的標識，查找所述標識對應的私鑰；

註冊模組 404，用於當所述查找模組 403 未查找到所述標識對應的私鑰時，根據所述待驗證的生物特徵資訊，向伺服器註冊所述用戶的身份，使所述伺服器保存所述待驗證的生物特徵資訊對應的公鑰。

所述裝置還包括：

密碼驗證模組 405，用於所述註冊模組 404 根據所述待驗證的生物特徵資訊，向伺服器註冊所述用戶的身份之前，接收用戶輸入的密碼，驗證所述密碼正確。

所述註冊模組 404 具體用於，根據與所述待驗證的生物特徵資訊匹配的標準生物特徵資訊對應的標識，產生所述標識對應的私鑰和公鑰，將所述標識與產生的私鑰的對應關係儲存在所述終端本地，將所述標識與產生的公鑰的對應關係發送給伺服器保存。

所述裝置還包括：

處理模組 406，用於所述註冊模組 404 向伺服器註冊所述用戶的身份之後，根據所述待驗證的生物特徵資訊，向所述伺服器發送業務處理請求，使所述伺服器根據所述待驗證的生物特徵資訊對應的公鑰進行業務處理。

所述處理模組 406 具體用於，根據產生的私鑰，對業務資訊進行簽名，並將攜帶有簽名後的業務資訊以及所述標識的業務處理請求發送給伺服器，使所述伺服器確定接收到的所述業務處理請求中攜帶的標識對應的公鑰，並根據確定的公鑰和所述簽名後的業務資訊進行業務處理。

業務處理請求包括支付請求。

在一個典型的配置中，計算設備包括一個或多個處理器（CPU）、輸入/輸出介面、網路介面和隨機存取記憶體。

隨機存取記憶體可能包括計算機可讀媒體中的非永久

性記憶體，隨機存取記憶體 (RAM) 和/或非易失性隨機存取記憶體等形式，如唯讀記憶體 (ROM) 或閃存(flash RAM)。隨機存取記憶體是計算機可讀媒體的示例。

計算機可讀媒體包括永久性和非永久性、可移動和非可移動媒體可以由任何方法或技術來實現資訊儲存。資訊可以是計算機可讀指令、資料結構、程式的模組或其他資料。計算機的儲存媒體的例子包括，但不限於相變隨機存取記憶體 (PRAM)、靜態隨機存取記憶體 (SRAM)、動態隨機存取記憶體 (DRAM)、其他類型的隨機存取記憶體 (RAM)、唯讀記憶體 (ROM)、電可抹除可編程唯讀記憶體 (EEPROM)、快閃記憶體或其他隨機存取記憶體技術、光碟唯讀記憶體 (CD-ROM)、數位多功能光碟 (DVD) 或其他光學儲存、磁盒式磁帶，磁帶磁盤儲存或其他磁性儲存設備或任何其他非傳輸媒體，可用於儲存可以被計算設備存取的資訊。按照本文中的界定，計算機可讀媒體不包括暫存電腦可讀媒體 (transitory media)，如調變的資料信號和載波。

還需要說明的是，術語“包括”、“包含”或者其任何其他變體意在涵蓋非排他性的包含，從而使得包括一系列要素的過程、方法、商品或者設備不僅包括那些要素，而且還包括沒有明確列出的其他要素，或者是還包括為這種過程、方法、商品或者設備所固有的要素。在沒有更多限制的情況下，由語句“包括一個……”限定的要素，並不排除在包括所述要素的過程、方法、商品或者設備中還存在另

外的相同要素。

本領域技術人員應明白，本發明的實施例可提供為方法、系統或計算機程式產品。因此，本發明可採用完全硬體實施例、完全軟體實施例或結合軟體和硬體方面的實施例的形式。而且，本發明可採用在一個或多個其中包含有計算機可用程式代碼的計算機可用儲存媒體（包括但不限於磁盤記憶體、CD-ROM、光學記憶體等）上實施的計算機程式產品的形式。

以上所述僅為本發明的實施例而已，並不用於限制本發明。對於本領域技術人員來說，本發明可以有各種更改和變化。凡在本發明的精神和原理之內所作的任何修改、等同替換、改進等，均應包含在本發明的申請專利範圍之內。

【符號說明】

401：接收模組

402：匹配模組

403：查找模組

404：註冊模組

405：密碼驗證模組

406：處理模組

I668589

發明摘要

※申請案號：106102208

※申請日：106 年 01 月 20 日

※IPC 分類： **G06F 21/32** (2013.01)
G06F 21/31 (2013.01)

【發明名稱】(中文/英文)

身份註冊方法及裝置

【中文】

本發明公開了一種身份註冊方法及裝置，該方法由終端接收用戶的待驗證的生物特徵資訊，匹配與該待驗證的生物特徵資訊一致的標準生物特徵資訊，當根據該標準生物特徵資訊對應的標識，未查找該標識對應的私鑰時，根據該待驗證的生物特徵資訊，向伺服器註冊該用戶的身份，使伺服器保存該待驗證的生物特徵資訊對應的公鑰。通過上述方法，無論用戶註冊時使用的生物特徵資訊是哪個，只要待驗證的生物特徵資訊已經保存在終端本地，就可直接根據該待驗證的生物特徵資訊，註冊該用戶的身份，進而完成業務處理，給用戶使用業務帶來很大的便利，同時也有有效的提高了使用業務的成功率。

【英文】

【代表圖】

【本案指定代表圖】：第(3)圖。

【本代表圖之符號簡單說明】：無

【本案若有化學式時，請揭示最能顯示發明特徵的化學式】：無

圖式

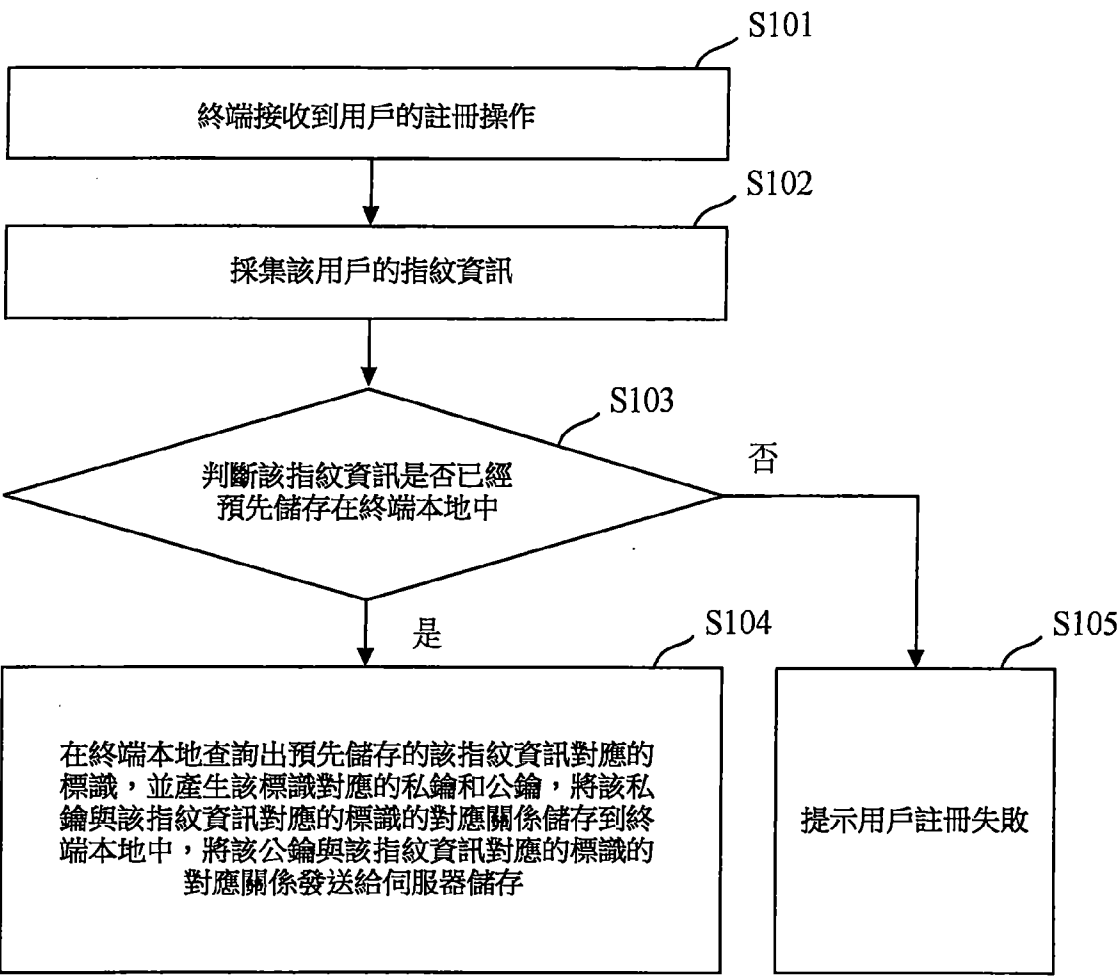


圖 1

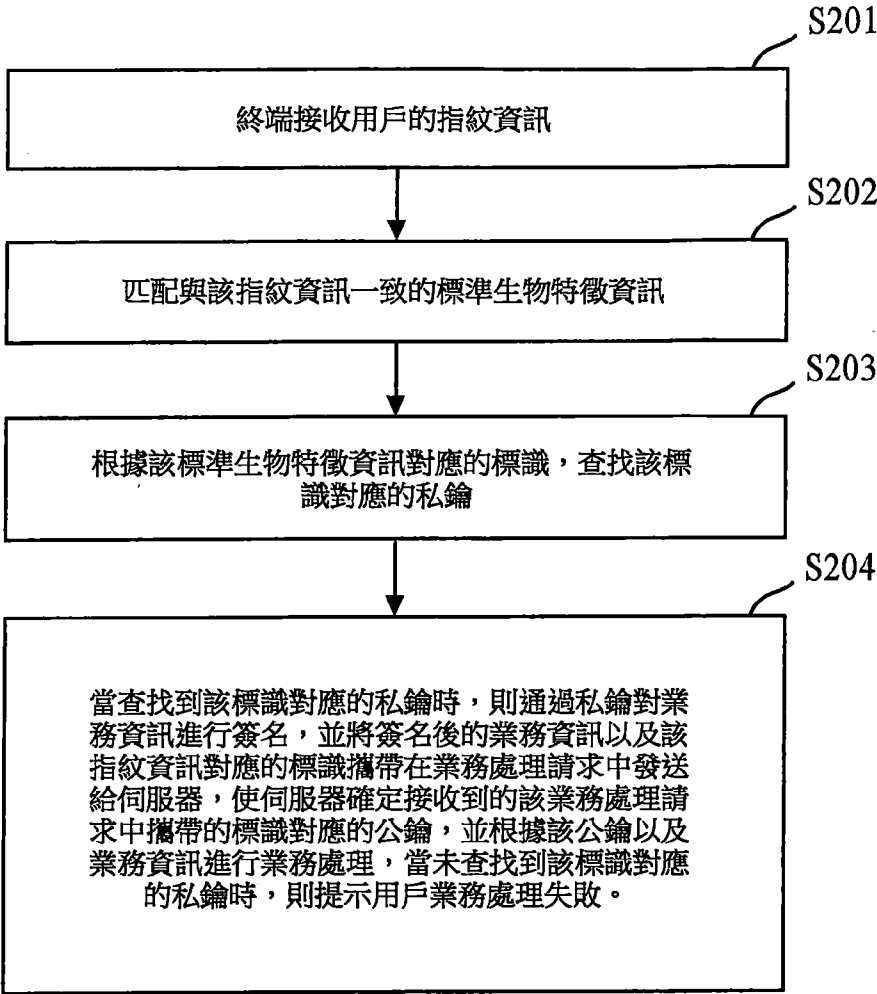


圖 2

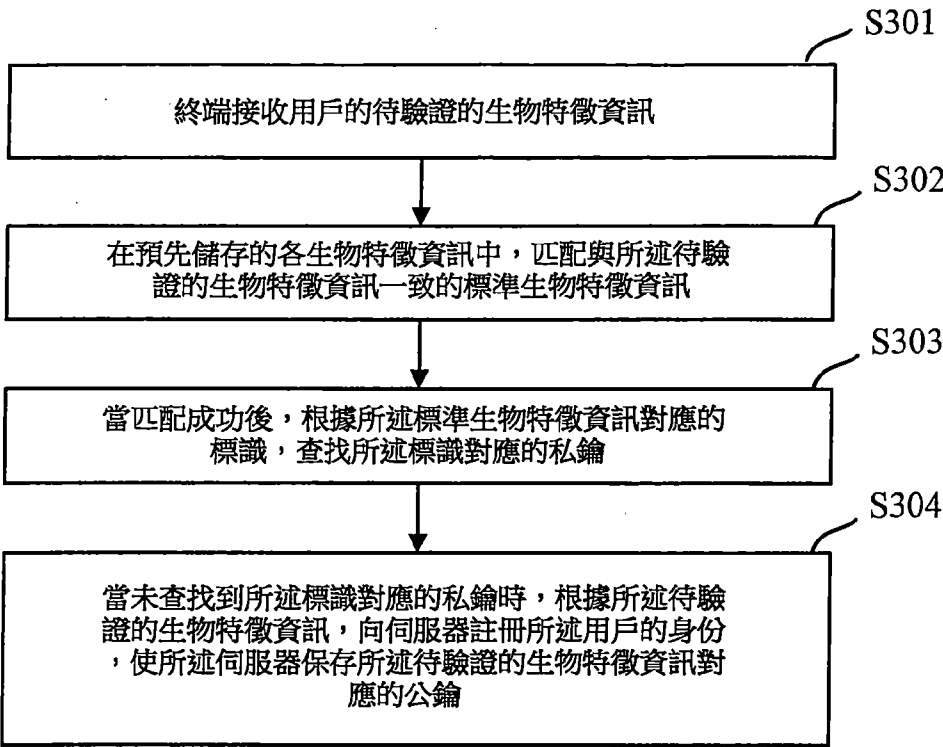


圖 3

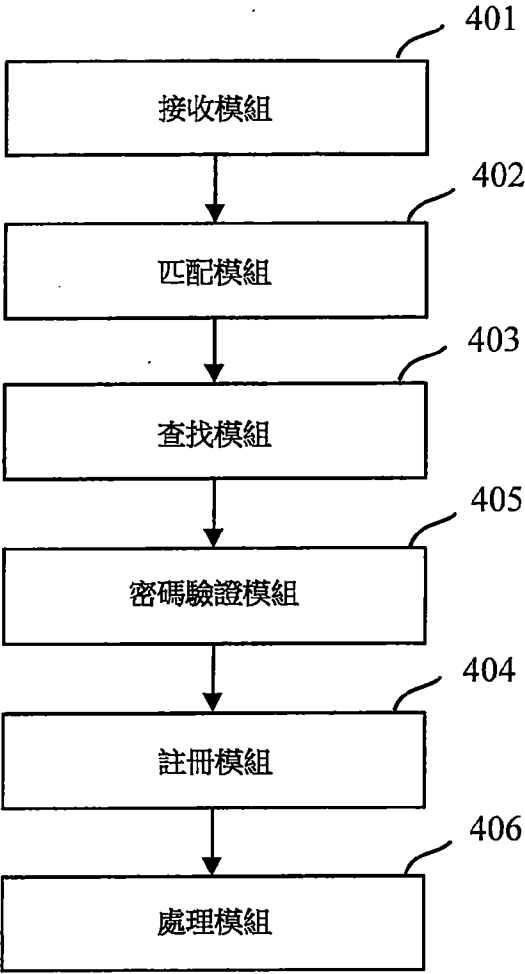


圖 4

申請專利範圍

1. 一種身份註冊方法，所述方法包括：

終端接收用戶的待驗證的生物特徵資訊；

在預先儲存的各生物特徵資訊中，匹配與所述待驗證的生物特徵資訊一致的標準生物特徵資訊，其中該待驗證的生物特徵資訊包括所述用戶並未註冊的生物特徵資訊；

當匹配成功後，根據所述標準生物特徵資訊對應的標識，查找所述標識對應的私鑰；

當未查找到所述標識對應的私鑰時，根據所述待驗證的生物特徵資訊，向伺服器驗證所述用戶的身份，使所述伺服器保存所述待驗證的生物特徵資訊對應的公鑰。

2. 如申請專利範圍第 1 項所述的方法，其中，在根據所述待驗證的生物特徵資訊，向伺服器註冊所述用戶的身份之前，所述方法還包括：

接收用戶輸入的密碼；

驗證所述密碼正確。

3. 如申請專利範圍第 1 項所述的方法，其中，根據所述待驗證的生物特徵資訊，向伺服器註冊所述用戶的身份，具體包括：

根據與所述待驗證的生物特徵資訊匹配的標準生物特徵資訊對應的標識，產生所述標識對應的私鑰和公鑰；

將所述標識與產生的私鑰的對應關係儲存在所述終端本地；

將所述標識與產生的公鑰的對應關係發送給伺服器保

第 106102208 號

民國 108 年 4 月 12 日修正

存。

4. 如申請專利範圍第 1 項所述的方法，其中，向伺服器註冊所述用戶的身份之後，所述方法還包括：

根據所述待驗證的生物特徵資訊，向所述伺服器發送業務處理請求，使所述伺服器根據所述待驗證的生物特徵資訊對應的公鑰進行業務處理。

5. 如申請專利範圍第 4 項所述的方法，其中，根據所述待驗證的生物特徵資訊，向所述伺服器發送業務處理請求，具體包括：

根據產生的私鑰，對業務資訊進行簽名，並將攜帶有簽名後的業務資訊以及所述標識的業務處理請求發送給伺服器，使所述伺服器確定接收到的所述業務處理請求中攜帶的標識對應的公鑰，並根據確定的公鑰和所述簽名後的業務資訊進行業務處理。

6. 如申請專利範圍第 4 或 5 項所述的方法，其中，業務處理請求包括支付請求。

7. 一種身份註冊的裝置，所述裝置包括：

接收模組，用於接收用戶的待驗證的生物特徵資訊；

匹配模組，用於在預先儲存的各生物特徵資訊中，匹配與所述待驗證的生物特徵資訊一致的標準生物特徵資訊，其中該待驗證的生物特徵資訊包括所述用戶並未註冊的生物特徵資訊；

查找模組，用於當匹配成功後，根據所述標準生物特徵資訊對應的標識，查找所述標識對應的私鑰；

第 106102208 號

民國 108 年 4 月 12 日修正

註冊模組，用於當所述查找模組未查找到所述標識對應的私鑰時，根據所述待驗證的生物特徵資訊，向伺服器驗證所述用戶的身份，使所述伺服器保存所述待驗證的生物特徵資訊對應的公鑰。

8. 如申請專利範圍第 7 項所述的裝置，其中，所述裝置還包括：

密碼驗證模組，用於所述註冊模組根據所述待驗證的生物特徵資訊，向伺服器註冊所述用戶的身份之前，接收用戶輸入的密碼，驗證所述密碼正確。

9. 如申請專利範圍第 7 項所述的裝置，其中，所述註冊模組具體用於，根據與所述待驗證的生物特徵資訊匹配的標準生物特徵資訊對應的標識，產生所述標識對應的私鑰和公鑰，將所述標識與產生的私鑰的對應關係儲存在所述終端本地，將所述標識與產生的公鑰的對應關係發送給伺服器保存。

10. 如申請專利範圍第 7 項所述的裝置，其中，所述裝置還包括：

處理模組，用於所述註冊模組向伺服器註冊所述用戶的身份之後，根據所述待驗證的生物特徵資訊，向所述伺服器發送業務處理請求，使所述伺服器根據所述待驗證的生物特徵資訊對應的公鑰進行業務處理。

11. 如申請專利範圍第 10 項所述的裝置，其中，所述處理模組具體用於，根據產生的私鑰，對業務資訊進行簽名，並將攜帶有簽名後的業務資訊以及所述標識的業務

第 106102208 號

民國 108 年 4 月 12 日修正

處理請求發送給伺服器，使所述伺服器確定接收到的所述業務處理請求中攜帶的標識對應的公鑰，並根據確定的公鑰和所述簽名後的業務資訊進行業務處理。

12. 如申請專利範圍第 10 或 11 項所述的裝置，其中，業務處理請求包括支付請求。