201719475

(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 201719475 A

(43)公開日： 中華民國 106 (2017) 年 06 月 01 日

(21)申請案號：105118603 (22)申請日： 中華民國 105 (2016) 年 06 月 14 日

(51)Int. Cl.： *G06F21/30 (2013.01)* *H04W12/06 (2009.01)*

(30)優先權：2015/11/24 中國大陸 201510825231.0

(71)申請人：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：汪小豐 (CN) ；萬煒欽 (CN) ；於洋 (CN)

(74)代理人：林志剛

申請實體審查：無 申請專利範圍項數：17 項 圖式數：9 共 47 頁

(54)名稱

身分驗證方法、系統、業務伺服器和驗證伺服器

(57)摘要

本發明提出一種身分驗證方法、業務伺服器、驗證伺服器和身分驗證系統，其中，該方法，包括：當透過網路接收到用戶端發送的資料交互請求時，獲取用戶端對應的第一用戶識別碼；將第一用戶識別碼發送至驗證伺服器；從驗證伺服器獲取與第一用戶識別碼對應的中間號碼；將中間號碼發送至用戶端，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫請求；接收驗證伺服器根據呼叫請求回饋的身分驗證的驗證結果；根據驗證結果處理資料交互請求。本發明的身分驗證方法，將電話通信網路的封閉性與網路的開放性特點相結合，有效提高了身分驗證的可靠性和安全性。

指定代表圖：

TW 201719475 A

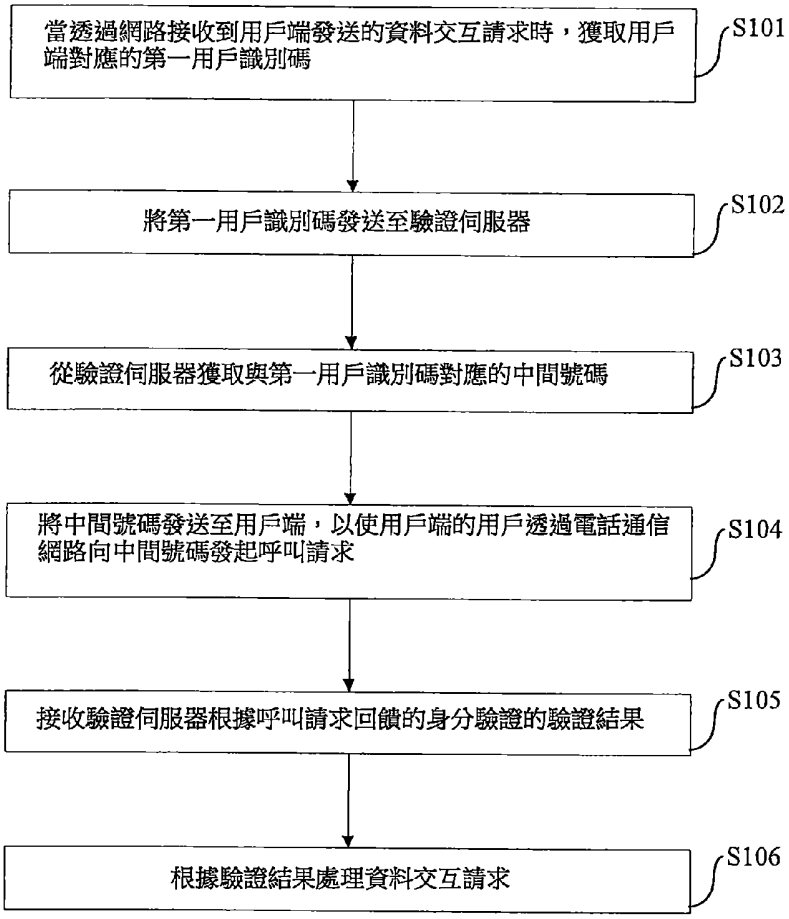

圖 1

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)

身分驗證方法、系統、業務伺服器和驗證伺服器

【技術領域】

本發明涉及網際網路技術領域，特別涉及一種身分驗證方法、系統、業務伺服器和驗證伺服器。

【先前技術】

隨著網際網路技術的不斷發展，越來越多的用戶可透過網際網路進行交互活動或者獲取服務。很多情況下，在用戶進行網際網路或者行動網際網路活動中的某些場景中，例如註冊、登錄等場景中，需要驗證用戶身分，以確認業務操作是由用戶本人發起的合法操作。目前，可透過語音或簡訊將驗證碼發送至用戶終端，用戶根據提示在相應的位置輸入該驗證碼後，該驗證碼可透過網際網路或行動網際網路傳送至後臺伺服器，然後由後臺伺服器驗證用戶填寫的驗證碼與之前發送給用戶的驗證碼是否一致，如果一致則通過驗證。但是，這種方式中驗證碼在傳輸過程或者在達到手機後，容易被第三方或者木馬截獲，安全性較低，且由於簡訊的到達率不能保證、語音播放驗證碼容易記錯，因此身分驗證的成功率難以達到理想值，影響用戶體驗。

【發明內容】

本發明旨在至少在一定程度上解決上述技術問題。

為此，本發明的第一個目的在於提出一種身分驗證方法，能夠有效提高身分驗證的可靠性和安全性。

本發明的第二個目的在於提出另一種身分驗證方法。

本發明的第三個目的在於提出一種業務伺服器。

本發明的第四個目的在於提出另一種驗證伺服器。

本發明的第五個目的在於提出另一種身分驗證系統。

為達上述目的，根據本發明第一方面實施例提出了一種身分驗證方法，包括以下步驟：當透過網路接收到用戶端發送的資料交互請求時，獲取所述用戶端對應的第一用戶識別碼；將所述第一用戶識別碼發送至驗證伺服器；從所述驗證伺服器獲取與所述第一用戶識別碼對應的中間號碼；將所述中間號碼發送至所述用戶端，以使所述用戶端的用戶透過電話通信網路向所述中間號碼發起呼叫請求；接收驗證伺服器根據所述呼叫請求回饋的所述身分驗證的驗證結果；根據所述驗證結果處理所述資料交互請求。

本發明實施例的身分驗證方法，在接收到用戶端的資料交互請求時，可獲取用戶端對應的第一用戶識別碼，並從驗證伺服器獲取與第一用戶識別碼相應的中間號碼發送之用戶端進行顯示，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫，並由驗證伺服器根據呼叫請求得到驗證結果。該實施例將電話通信網路的封閉性與網路的開

放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全性。

本發明第二方面實施例提供了另一種身分驗證方法，包括以下步驟：接收業務伺服器發送的第一用戶識別碼；為所述第一用戶識別碼分配對應的中間號碼；將所述中間號碼返回至所述業務伺服器，以透過所述業務伺服器將所述中間號碼提供給用戶的用戶端；從電話通信網路獲取向所述中間號碼發起所述呼叫的第二用戶識別碼；驗證所述第一用戶識別碼與所述第二用戶識別碼是否一致，並將驗證結果返回至所述業務伺服器。

本發明實施例的身分驗證方法，可為業務伺服器發送的第一用戶識別碼分配相應的中間號碼，並透過業務伺服器提供給用戶的用戶端，當中間號碼接收到呼叫時，從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼，並透過驗證所述第一用戶識別碼與所述第二用戶識別碼是否一致得到驗證結果。該實施例將電話通信網路的封閉性與網路的開放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全

性。

本發明第三方面實施例提供了一種業務伺服器，包括：第一獲取模組，用於當透過網路接收到用戶端發送的資料交互請求時，獲取所述用戶端對應的第一用戶識別碼；第一發送模組，用於將所述第一用戶識別碼發送至驗證伺服器；第二獲取模組，用於從所述驗證伺服器獲取與所述第一用戶識別碼對應的中間號碼；第二發送模組，用於將所述中間號碼發送至所述用戶端，以使所述用戶端的用戶透過電話通信網路向所述中間號碼發起呼叫請求；第一接收模組，用於接收驗證伺服器根據所述呼叫請求回饋的所述身分驗證的驗證結果；處理模組，用於根據所述驗證結果處理所述資料交互請求。

本發明實施例的業務伺服器，在接收到用戶端的資料交互請求時，可獲取用戶端對應的第一用戶識別碼，並從驗證伺服器獲取與第一用戶識別碼相應的中間號碼發送之用戶端進行顯示，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫，並由驗證伺服器根據呼叫請求得到驗證結果。該實施例將電話通信網路的封閉性與網路的開放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全性。

本發明第四方面實施例提供了一種驗證伺服器，包

括：接收模組，用於接收業務伺服器發送的第一用戶識別碼；分配模組，用於為所述第一用戶識別碼分配對應的中間號碼；返回模組，用於將所述中間號碼返回至所述業務伺服器，以透過所述業務伺服器將所述中間號碼提供給用戶的用戶端；獲取模組，用於從電話通信網路獲取向所述中間號碼發起所述呼叫的第二用戶識別碼；驗證模組，用於驗證所述第一用戶識別碼與所述第二用戶識別碼是否一致，並將驗證結果返回至所述業務伺服器。

本發明實施例的業務伺服器，可為業務伺服器發送的第一用戶識別碼分配相應的中間號碼，並透過業務伺服器提供給用戶的用戶端，當中間號碼接收到呼叫時，從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼，並透過驗證所述第一用戶識別碼與所述第二用戶識別碼是否一致得到驗證結果。該實施例將電話通信網路的封閉性與網路的開放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全性。

本發明第五方面實施例提供了一種身分驗證系統，包括：用戶端、本發明第三申請實施例的業務伺服器以及本發明第四方面實施例的驗證伺服器。

本發明實施例的身分驗證系統，業務伺服器在接收到用戶端的資料交互請求時，可獲取用戶端對應的第一用戶

識別碼，並從驗證伺服器獲取與第一用戶識別碼相應的中間號碼發送之用戶端進行顯示，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫，驗證伺服器可從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼，並透過驗證所述第一用戶識別碼與所述第二用戶識別碼是否一致得到驗證結果。該實施例將電話通信網路的封閉性與網路的開放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全性。

本發明的附加方面和優點將在下面的描述中部分給出，部分將從下面的描述中變得明顯，或透過本發明的實踐瞭解到。

【圖式簡單說明】

本發明的上述和/或附加的方面和優點從結合下面圖式對實施例的描述中將變得明顯和容易理解，其中：

圖 1 為根據本發明一個實施例的身分驗證方法的流程圖；

圖 2 為根據本發明又一個實施例的身分驗證方法的流程圖；

圖 3 為根據本發明另一個實施例的身分驗證方法的流程圖；

圖 4 為根據本發明一個實施例的驗證伺服器的同步位置更新的示意圖；

圖 5 為根據本發明一個實施例的業務伺服器的結構示意圖；

圖 6 為根據本發明另一個實施例的業務伺服器的結構示意圖；

圖 7 為根據本發明又一個實施例的業務伺服器的結構示意圖；

圖 8 為根據本發明一個實施例的驗證伺服器的結構示意圖；

圖 9 為根據本發明一個實施例的身分驗證系統的結構示意圖。

【實施方式】

下面詳細描述本發明的實施例，所述實施例的示例在圖式中示出，其中自始至終相同或類似的標號表示相同或類似的元件或具有相同或類似功能的元件。下面透過參考圖式描述的實施例是示例性的，僅用於解釋本發明，而不能理解為對本發明的限制。

由於網路（如網際網路，行動網際網路等）是一個開放的網路，接入門檻非常低，其安全性相對而言不是很高，因此，在身分驗證過程時透過網路傳輸驗證碼時，存在安全隱憂。因此，為了解決上述問題，本發明實施例提出了一種身分驗證方法、業務伺服器、驗證伺服器以及身

分驗證系統。

下面參考圖式描述根據本發明實施例的身分驗證方法、業務伺服器、驗證伺服器以及身分驗證系統。

圖 1 為根據本發明一個實施例的身分驗證方法的流程圖。

如圖 1 所示，根據本發明實施例的身分驗證方法，包括：

S101，當透過網路接收到用戶端發送的資料交互請求時，獲取用戶端對應的第一用戶識別碼。

其中，網路可為網際網路或行動網際網路，例如，基於 IP（Internet Protocol，網路之間互連的協定）協定的 IP 網路。

資料交互請求可以是註冊請求、登錄請求、用戶資訊變更請求、支付請求、轉帳請求、查詢請求等。其中，資料交互請求可以 HTTP（Hyper Text Transfer Protocol，超文本傳輸協定）請求的方式發送。

用戶端對應的第一用戶識別碼為用戶端用戶在電話通信網路中的身分標識資訊，用於在電話通信網路中唯一標識用戶端用戶。舉例來說，第一用戶識別碼可以是手機號碼、MSIN（Mobile Subscriber Identification Number，移動用戶識別號碼），IMSI（國際移動用戶識別碼）等。

其中，電話通信網路是由信號網和話務網組成的一個封閉的網路。

具體地，用戶端可根據用戶的操作向業務伺服器發送

相應的資料交互請求。業務伺服器在接收到用戶端發送的資料交互請求之後，可獲取該用戶端的用戶的第一用戶識別碼。

舉例來說，當用戶透過用戶端發起支付請求時，用戶端可向業務伺服器發送支付請求，然後由業務伺服器發起後續驗證過程。

在本發明的一個實施例中，業務伺服器可向用戶端發送用戶識別碼輸入請求，以使用戶端的用戶輸入第一用戶識別碼。具體地，業務伺服器在接收到資料交互請求之後，可向用戶端發送用戶識別碼輸入請求，用戶端在接收到用戶識別碼輸入請求後可提供用戶識別碼輸入介面，並提示用戶進行輸入，並將用戶輸入的用戶識別碼返回至業務伺服器。

在本發明的另一個實施例中，業務伺服器從用戶資料庫中提取用戶端的用戶的第一用戶識別碼。其中，業務伺服器可預先根據用戶的帳號資訊儲存與用戶帳號資訊相對應的用戶識別碼，從而在接收到資料交互請求之後，可根據接收到的資料交互請求對應的帳號資訊在用戶資料中查找該相應的用戶識別碼。舉例來說，用戶在註冊時，或者在註冊之後提交了手機號碼，則業務伺服器可保存該用戶的帳號與手機號碼的對應關係。當接收到來自該用戶的帳號的資料交互請求時，即可根據帳號提取對應的手機號碼。

S102，將第一用戶識別碼發送至驗證伺服器。

其中，驗證伺服器為對用戶進行身分驗證處理的伺服器，業務伺服器是用於為用戶端提供相應業務的伺服器。業務伺服器可透過網路與驗證伺服器進行通信。

S103，從驗證伺服器獲取與第一用戶識別碼對應的中間號碼。

在本發明的一個實施例中，當驗證伺服器接收到業務伺服器發送的第一用戶識別碼時，可為第一用戶識別碼分配對應的中間號碼，並返回給驗證伺服器。其中，中間號碼可為手機號碼、特服號、固定電話號碼或者網路電話號碼等。

在本發明的實施例中，中間號碼可為固定號碼或者臨時號碼。具體地，驗證伺服器可將預設的號碼作為第一用戶識別碼對應的中間號碼，即將一個預先設定的一個固定號碼作為中間號碼。另外，驗證伺服器也可從預設的號碼池中隨機選擇一個臨時號碼，並將臨時號碼作為第一用戶識別碼對應的中間號碼。其中，預設的號碼池可為業務伺服器從通信運營商處預先申請的。

S104，將中間號碼發送至用戶端，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫請求。

業務伺服器從驗證伺服器獲取與第一用戶識別碼對應的中間號碼之後，可將該中間號碼發送至用戶端。用戶端可顯示該中間號碼，從而，用戶端的用戶可透過電話通信網路向該中間號碼發起呼叫請求。

應當理解，本發明實施例中用戶所使用的發起呼叫的

設備可以是用戶端所在的設備，也可以是用戶的其他呼叫設備。舉例來說，如果用戶端所在的設備為手機，則用戶端可在手機中渲染中間號碼對應的呼叫介面，從而用戶可透過觸發撥號按鍵直接向中間號碼發起呼叫。如果用戶端所在的設備為電腦，則用戶可使用手機向用戶端顯示的中間號碼發起呼叫。

S105，接收驗證伺服器根據呼叫請求回饋的身分驗證的驗證結果。

在本發明的實施例中，驗證伺服器可從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼，並驗證第一用戶識別碼與第二用戶識別碼是否一致，然後將驗證結果返回至業務伺服器。

S106，根據驗證結果處理資料交互請求。

如果驗證伺服器返回的驗證結果為第一用戶識別碼與第二用戶識別碼一致，則判斷用戶端的用戶透過驗證（本次呼叫由用戶本人發起），可回應該資料交互請求；如果驗證伺服器返回的驗證結果為第一用戶識別碼與第二用戶識別碼不一致，則判斷用戶端的用戶未透過驗證（本次呼叫並非由用戶本人發起），可拒絕回應該資料交互請求，並提示用戶端的用戶驗證失敗。

本發明實施例的身分驗證方法，在接收到用戶端的資料交互請求時，可獲取用戶端對應的第一用戶識別碼，並從驗證伺服器獲取與第一用戶識別碼相應的中間號碼發送之用戶端進行顯示，以使用戶端的用戶透過電話通信網路

向中間號碼發起呼叫，並由驗證伺服器根據呼叫請求得到驗證結果。該實施例將電話通信網路的封閉性與網路的開放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全性。

此外，透過電話呼叫進行驗證，通話與驗證可即時同步完成，提高了驗證效率，提升了用戶的驗證體驗。

圖 2 為根據本發明又一個實施例的身分驗證方法的流程圖。

如圖 2 所示，根據本發明實施例的身分驗證方法，包括：

S201，當透過網路接收到用戶端發送的資料交互請求時，確定資料交互請求對應的風險等級。

在本發明的實施例中，業務伺服器可根據資料交互請求的請求類型確定相應的風險等級。不同請求類型對應的風險等級可為系統預設值，也可由用戶根據需要預先設定。舉例來說，如果資料交互請求為大額支付請求，則風險等級可為高級；如果資料交互請求為查詢請求，則風險等級可為低級；如果資料交互請求為用戶資訊修改請求，則風險等級可為中級。

S202，如果資料交互請求對應的風險等級高於預設等級，則獲取用戶端對應的第一用戶識別碼。

其中，預設等級可為預設設置，或者由用戶設置。舉例來說，預設等級可為中級。

由此，當資料交互請求對應的風險等級高於預設等級時，業務伺服器才獲取用戶端對應的第一用戶識別碼，並發起後續的驗證流程。

S203，將第一用戶識別碼發送至驗證伺服器。

S204，從驗證伺服器獲取與第一用戶識別碼對應的中間號碼。

S205，將中間號碼發送至用戶端，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫請求。

S206，接收驗證伺服器根據呼叫請求回饋的身分驗證的驗證結果。

S207，根據驗證結果處理資料交互請求。

S203-S207 與圖 1 所示實施例中 S102-S106 相同，因此可參照圖 1 所示實施例。

在本發明的一個實施例中，在對用戶端的用戶的身分進行驗證時，除了考慮驗證伺服器返回的驗證結果之外，還可考慮呼叫過程中用戶的交互操作進行驗證。

因此，本發明的實施例還可包括：接收驗證伺服器發送的呼叫過程中的交互記錄；根據交互記錄對用戶端的用戶進行身分驗證。也就是說，驗證伺服器可記錄呼叫過程中用戶的交互記錄，並返回至業務伺服器，業務伺服器可判斷交互記錄是否符合預設交互要求。如果交互記錄符合預設交互要求、且驗證伺服器返回的驗證結果為第一用戶

識別碼與第二用戶識別碼一致，則判斷用戶的身分驗證通過，否則，二者中有任一條件不滿足，則判斷用戶的身分驗證未通過。

其中，可根據不同的安全驗證等級設定用戶在呼叫過程中的交互場景。舉例說明如下：

場景一

低等級驗證：向中間號碼發起的呼叫被接聽後，驗證伺服器播放預設提示音，播放完畢之後，通話結束。在此過程中，用戶端的用戶不需要進行操作。通話完成，即表示交互記錄符合預設交互要求。

場景二

中等級驗證：向中間號碼發起的呼叫被接聽後，驗證伺服器播放提示用戶按相應的按鍵的語音，並記錄用戶的按鍵操作。如果用戶的按鍵操作與提示語音一致，則表示交互記錄符合預設交互要求。

場景三

高等級驗證：向中間號碼發起的呼叫被接聽後，驗證伺服器提示用戶輸入相應字串的語音，並記錄用戶輸入的字串。如果用戶輸入的字串與提示語音中的字串一致，則表示交互記錄符合預設交互要求。

其中，安全驗證等級可根據身分驗證請求對應的用戶的身分、用戶端的安全環境等設定。例如，如果用戶為正常狀態，用戶端使用環境安全，則選擇低等級驗證；如果用戶為異常狀態（如異地登錄），則選擇中等級驗證；如

果用戶被舉報，或者用戶端使用環境不安全（如被病毒或木馬惡意攻擊的環境）則選擇高等級驗證。

應當理解，判斷交互記錄是否符合預設交互要求也可由驗證伺服器執行，然後由驗證伺服器根據判斷結果以及對第一用戶識別碼與第二用戶識別碼的驗證結果判斷用戶的身分驗證是否通過，並將判斷結果返回至業務伺服器。

本發明實施例的身分驗證方法，在接收到客戶的資料交互請求時，可根據資料交互請求對應的風險等級判斷是否發起驗證過程，從而能夠過濾掉不需身分驗證的情況，能夠有效提高資料交互請求的相應速度。

為了實現上述實施例，本發明還提出另一種身分驗證方法。

圖 3 為根據本發明另一個實施例的身分驗證方法的流程圖。

如圖 3 所示，根據本發明實施例的身分驗證方法，包括：

S301，接收業務伺服器發送的第一用戶識別碼。

其中，驗證伺服器可透過網路接收業務伺服器發送的第一用戶識別碼。第一用戶識別碼為用戶端用戶在電話通信網路中的身分標識資訊，用於在電話通信網路中唯一標識用戶端用戶。舉例來說，第一用戶識別碼可以是手機號碼、MSIN（Mobile Subscriber Identification Number，移動用戶識別號碼），IMSI（國際移動用戶識別碼）等。

其中，驗證伺服器為對用戶進行身分驗證處理的伺服

器，業務伺服器是用於為用戶端提供相應業務的伺服器。業務伺服器可透過網路與驗證伺服器進行通信。

其中，網路可為網際網路或行動網際網路，例如，基於 IP（Internet Protocol，網路之間互連的協定）協定的 IP 網路。電話通信網路是由信號網和話務網組成的一個封閉的網路。

具體地，用戶端可根據用戶的操作向業務伺服器發送相應的資料交互請求。業務伺服器在接收到用戶端發送的資料交互請求之後，可獲取該用戶端的用戶的第一用戶識別碼。舉例來說，當用戶透過用戶端發起支付請求時，用戶端可向業務伺服器發送支付請求，然後由業務伺服器發起後續驗證過程。

其中，資料交互請求可以是註冊請求、登錄請求、用戶資訊變更請求、支付請求、轉帳請求、查詢請求等。其中，資料交互請求可以 HTTP（Hyper Text Transfer Protocol，超文本傳輸協定）請求的方式發送。

在本發明的實施例中，業務伺服器可向用戶端發送用戶識別碼輸入請求，以使用戶端的用戶輸入第一用戶識別碼。或者，業務伺服器從用戶資料庫中提取用戶端的用戶的第一用戶識別碼。

S302，為第一用戶識別碼分配對應的中間號碼。

其中，中間號碼可為手機號碼、特服號、固定電話號碼或者網路電話號碼等。

在本發明的實施例中，中間號碼可為固定號碼或者臨

時號碼。

在本發明的一個實施例中，驗證伺服器可將預設的號碼作為第一用戶識別碼對應的中間號碼，即將一個預先設定的一個固定號碼作為中間號碼。

如果以固定號碼作為中間號碼，則需要將電話通信網路中該固定號碼的路由指向驗證伺服器，以使對該固定號碼的呼叫能夠到達驗證伺服器。

在本發明的另一個實施例中，驗證伺服器也可從預設的號碼池中隨機選擇一個臨時號碼，並將臨時號碼作為第一用戶識別碼對應的中間號碼。其中，預設的號碼池可為業務伺服器從通信運營商處預先申請的。

如果以臨時號碼作為中間號碼，則驗證伺服器在選擇臨時號碼後，需要進行同步位置更新。即如圖 4 所示，通知電話通信網路中的 HLR（Home Location Register，本地暫存器）被選擇的臨時號碼的路由指向驗證伺服器。從而，對該臨時號碼的呼叫能夠到達驗證伺服器。使其中，驗證伺服器透過 HSTP/LSTP（High/Low Signal Transfer Point，傳統通信網中的信號傳輸點）與 HLR 發送進行通信。

S303，將中間號碼返回至業務伺服器，以透過業務伺服器將中間號碼提供給用戶的用戶端。

業務伺服器從驗證伺服器獲取與第一用戶識別碼對應的中間號碼之後，可將該中間號碼發送至用戶的用戶端。用戶端將該中間號碼顯示給用戶，從而，用戶端的用戶可

透過電話通信網路向該中間號碼發起呼叫請求。

S304，從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼。

由於中間號碼的路由指向驗證伺服器，因此，當中間號碼被呼叫時，驗證伺服器可接收到呼叫請求，並可從電話通信網路中獲取向中間號碼發起呼叫的號碼，即第二用戶識別碼。

S305，驗證第一用戶識別碼與第二用戶識別碼是否一致，並將驗證結果返回至業務伺服器。

如果驗證伺服器的驗證結果為第一用戶識別碼與第二用戶識別碼一致，則可判斷用戶端的用戶通過驗證（本次呼叫由用戶本人發起），業務伺服器可回應該資料交互請求；如果驗證伺服器的驗證結果為第一用戶識別碼與第二用戶識別碼不一致，則可判斷用戶端的用戶未通過驗證（本次呼叫並非由用戶本人發起），業務伺服器可拒絕回應該資料交互請求，並提示用戶端的用戶驗證失敗。

在本發明的一個實施例中，驗證伺服器還可記錄呼叫過程中用戶的交互記錄，並判斷該交互記錄是否符合預設交互要求。如果交互記錄符合預設交互要求、且驗證伺服器返回的驗證結果為第一用戶識別碼與第二用戶識別碼一致，則判斷用戶的身分驗證通過，否則，二者中有任一條件不滿足，則判斷用戶的身分驗證未通過。然後將驗證結果發送至業務伺服器。

當然，驗證伺服器也可將呼叫過程中用戶的交互記錄

發送之業務伺服器，然後由業務伺服器根據用戶識別碼的比對結果和交互記錄的判斷結果判斷用戶的身分驗證是否通過。

本發明實施例的身分驗證方法，可為業務伺服器發送的第一用戶識別碼分配相應的中間號碼，並透過業務伺服器提供給用戶的用戶端，當中間號碼接收到呼叫時，從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼，並透過驗證第一用戶識別碼與第二用戶識別碼是否一致得到驗證結果。該實施例將電話通信網路的封閉性與網路的開放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全性。

應當理解，在本發明的實施例中，業務伺服器與驗證伺服器可為同一伺服器，也可為不同的伺服器。

為了實現上述實施例，本發明還提出一種業務伺服器。

圖 5 為根據本發明一個實施例的業務伺服器的結構示意圖。

如圖 5 所示，根據本發明實施例的業務伺服器 100，包括：第一獲取模組 110、第一發送模組 120、第二獲取模組 130、第二發送模組 140、第一接收模組 150 和處理模組 160。

具體地，第一獲取模組 110 用於當透過網路接收到用戶端發送的資料交互請求時，獲取用戶端對應的第一用戶識別碼。

其中，用戶端可根據用戶的操作向業務伺服器發送相應的資料交互請求。第一獲取模組 110 在接收到用戶端發送的資料交互請求之後，可獲取該用戶端的用戶的第一用戶識別碼。

舉例來說，當用戶透過用戶端發起支付請求時，用戶端可向業務伺服器發送支付請求，然後由業務伺服器發起後續驗證過程。

在本發明的一個實施例中，第一獲取模組 110 可用於向用戶端發送用戶識別碼輸入請求，以使用戶端的用戶輸入第一用戶識別碼。具體地，第一獲取模組 110 在接收到資料交互請求之後，可向用戶端發送用戶識別碼輸入請求，用戶端在接收到用戶識別碼輸入請求後可提供用戶識別碼輸入介面，並提示用戶進行輸入，並將用戶輸入的用戶識別碼返回至業務伺服器。

在本發明的另一個實施例中，第一獲取模組 110 可用於從用戶資料庫中提取用戶端的用戶的第一用戶識別碼。其中，業務伺服器可預先根據用戶的帳號資訊儲存與用戶帳號資訊相對應的用戶識別碼，從而在接收到資料交互請求之後，第一獲取模組 110 可根據接收到的資料交互請求對應的帳號資訊在用戶資料中查找該相應的用戶識別碼。舉例來說，用戶在註冊時，或者在註冊之後提交了手機號

碼，則業務伺服器可保存該用戶的帳號與手機號碼的對應關係。當接收到來自該用戶的帳號的資料交互請求時，即可根據帳號提取對應的手機號碼。

第一發送模組 120 用於將第一用戶識別碼發送至驗證伺服器。

第二獲取模組 130 用於從驗證伺服器獲取與第一用戶識別碼對應的中間號碼。

在本發明的一個實施例中，當驗證伺服器接收到業務伺服器發送的第一用戶識別碼時，可為第一用戶識別碼分配對應的中間號碼，並返回給驗證伺服器。其中，中間號碼可為手機號碼、特服號、固定電話號碼或者網路電話號碼等。

在本發明的實施例中，中間號碼可為固定號碼或者臨時號碼。具體地，驗證伺服器可將預設的號碼作為第一用戶識別碼對應的中間號碼，即將一個預先設定的一個固定號碼作為中間號碼。另外，驗證伺服器也可從預設的號碼池中隨機選擇一個臨時號碼，並將臨時號碼作為第一用戶識別碼對應的中間號碼。其中，預設的號碼池可為業務伺服器從通信運營商處預先申請的。

第二發送模組 140 用於將中間號碼發送至用戶端，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫請求。

第二獲取模組 130 從驗證伺服器獲取與第一用戶識別碼對應的中間號碼之後，第二發送模組 140 可將該中間號

碼發送至用戶端。用戶端可顯示該中間號碼，從而，用戶端的用戶可透過電話通信網路向該中間號碼發起呼叫請求。

應當理解，本發明實施例中用戶所使用的發起呼叫的設備可以是用戶端所在的設備，也可以是用戶的其他呼叫設備。舉例來說，如果用戶端所在的設備為手機，則用戶端可在手機中渲染中間號碼對應的呼叫介面，從而用戶可透過觸發撥號按鍵直接向中間號碼發起呼叫。如果用戶端所在的設備為電腦，則用戶可使用手機向用戶端顯示的中間號碼發起呼叫。

第一接收模組 150 用於接收驗證伺服器根據呼叫請求回饋的身分驗證的驗證結果。

在本發明的實施例中，驗證伺服器可從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼，並驗證第一用戶識別碼與第二用戶識別碼是否一致，然後將驗證結果返回至業務伺服器。

處理模組 160 用於根據驗證結果處理資料交互請求。

如果驗證伺服器返回的驗證結果為第一用戶識別碼與第二用戶識別碼一致，則判斷用戶端的用戶通過驗證（本次呼叫由用戶本人發起），處理模組 160 可回應該資料交互請求；如果驗證伺服器返回的驗證結果為第一用戶識別碼與第二用戶識別碼不一致，則判斷用戶端的用戶未通過驗證（本次呼叫並非由用戶本人發起），處理模組 160 可拒絕回應該資料交互請求，並提示用戶端的用戶驗證失

敗。

本發明實施例的業務伺服器，在接收到用戶端的資料交互請求時，可獲取用戶端對應的第一用戶識別碼，並從驗證伺服器獲取與第一用戶識別碼相應的中間號碼發送之用戶端進行顯示，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫，並由驗證伺服器根據呼叫請求得到驗證結果。該實施例將電話通信網路的封閉性與網路的開放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全性。

圖 6 為根據本發明另一個實施例的業務伺服器的結構示意圖。

如圖 6 所示，本發明實施例的業務伺服器 100，包括：第一獲取模組 110、第一發送模組 120、第二獲取模組 130、第二發送模組 140、第一接收模組 150、處理模組 160 和確定模組 170。

具體地，第一獲取模組 110、第一發送模組 120、第二獲取模組 130、第二發送模組 140、第一接收模組 150 和處理模組 160，可參照圖 5 所示實施例。

確定模組 170 用於當透過網路接收到用戶端發送的資料交互請求時，確定資料交互請求對應的風險等級。

在本發明的實施例中，確定模組 170 可根據資料交互

請求的請求類型確定相應的風險等級。不同請求類型對應的風險等級可為系統預設值，也可由用戶根據需要預先設定。舉例來說，如果資料交互請求為大額支付請求，則風險等級可為高級；如果資料交互請求為查詢請求，則風險等級可為低級；如果資料交互請求為用戶資訊修改請求，則風險等級可為中級。

其中，第一獲取模組 110 用於在資料交互請求對應的風險等級高於預設等級時，獲取用戶端的用戶的第一用戶識別碼。

其中，預設等級可為預設設置，或者由用戶設置。舉例來說，預設等級可為中級。

由此，當資料交互請求對應的風險等級高於預設等級時，第一獲取模組 110 才獲取用戶端對應的第一用戶識別碼，並發起後續的驗證流程。

本發明實施例的業務伺服器，在接收到客戶的資料交互請求時，可根據資料交互請求對應的風險等級判斷是否發起驗證過程，從而能夠過濾掉不需身分驗證的情況，能夠有效提高資料交互請求的相應速度。

圖 7 為根據本發明又一個實施例的業務伺服器的結構示意圖。

如圖 7 所示，本發明實施例的業務伺服器 100，包括：第一獲取模組 110、第一發送模組 120、第二獲取模組 130、第二發送模組 140、第一接收模組 150、處理模組 160、確定模組 170、第二接收模組 180 和驗證模組

190。

具體地，第一獲取模組 110、第一發送模組 120、第二獲取模組 130、第二發送模組 140、第一接收模組 150、處理模組 160 和確定模組 170 可參照圖 6 所示實施例。

第二接收模組 180 用於接收驗證伺服器發送的呼叫過程中的交互記錄。

其中，驗證伺服器可記錄呼叫過程中用戶的交互記錄，並返回至業務伺服器。

驗證模組 190 用於根據交互記錄對用戶端的用戶進行身分驗證。

具體地，驗證模組 190 可判斷交互記錄是否符合預設交互要求。如果交互記錄符合預設交互要求、且驗證伺服器返回的驗證結果為第一用戶識別碼與第二用戶識別碼一致，則判斷用戶的身分驗證通過，否則，二者中有任一條件不滿足，則判斷用戶的身分驗證未通過。

其中，可根據不同的安全驗證等級設定用戶在呼叫過程中的交互場景。舉例說明如下：

場景一

低等級驗證：向中間號碼發起的呼叫被接聽後，驗證伺服器播放預設提示音，播放完畢之後，通話結束。在此過程中，用戶端的用戶不需要進行操作。通話完成，即表示交互記錄符合預設交互要求。

場景二

中等級驗證：向中間號碼發起的呼叫被接聽後，驗證伺服器播放提示用戶按相應的按鍵的語音，並記錄用戶的按鍵操作。如果用戶的按鍵操作與提示語音一致，則表示交互記錄符合預設交互要求。

場景三

高等級驗證：向中間號碼發起的呼叫被接聽後，驗證伺服器提示用戶輸入相應字串的語音，並記錄用戶輸入的字串。如果用戶輸入的字串與提示語音中的字串一致，則表示交互記錄符合預設交互要求。

其中，安全驗證等級可根據身分驗證請求對應的用戶的身分、用戶端的安全環境等設定。例如，如果用戶為正常狀態，用戶端使用環境安全，則選擇低等級驗證；如果用戶為異常狀態（如異地登錄），則選擇中等級驗證；如果用戶被舉報，或者用戶端使用環境不安全（如被病毒或木馬惡意攻擊的環境）則選擇高等級驗證。

為了實現上述實施例，本發明還提出一種驗證伺服器。

圖 8 為根據本發明一個實施例的驗證伺服器的結構示意圖。

如圖 8，根據本發明實施例的驗證伺服器 200，包括：接收模組 210、分配模組 220、返回模組 230、獲取模組 240 和驗證模組 250。

具體地，接收模組 210 用於接收業務伺服器發送的第一用戶識別碼。

接收模組 210 可透過網路接收業務伺服器發送的第一用戶識別碼。

其中，用戶端可根據用戶的操作向業務伺服器發送相應的資料交互請求。業務伺服器在接收到用戶端發送的資料交互請求之後，可獲取該用戶端的用戶的第一用戶識別碼。舉例來說，當用戶透過用戶端發起支付請求時，用戶端可向業務伺服器發送支付請求，然後由業務伺服器發起後續驗證過程。

分配模組 220 用於為第一用戶識別碼分配對應的中間號碼。

其中，中間號碼可為手機號碼、特服號、固定電話號碼或者網路電話號碼等。

在本發明的實施例中，中間號碼可為固定號碼或者臨時號碼。

在本發明的一個實施例中，分配模組 220 可用於將預設的號碼作為第一用戶識別碼對應的中間號碼，即將一個預先設定的一個固定號碼作為中間號碼。

如果以固定號碼作為中間號碼，則需要將電話通信網路中該固定號碼的路由指向驗證伺服器，以使對該固定號碼的呼叫能夠到達驗證伺服器。

在本發明的另一個實施例中，分配模組 220 也可用於從預設的號碼池中隨機選擇一個臨時號碼，並將臨時號碼作為第一用戶識別碼對應的中間號碼。其中，預設的號碼池可為業務伺服器從通信運營商處預先申請的。

如果以臨時號碼作為中間號碼，則驗證伺服器在選擇臨時號碼後，需要進行同步位置更新。即如圖 4 所示，通知電話通信網路中的 HLR（Home Location Register，本地暫存器）被選擇的臨時號碼的路由指向驗證伺服器。從而，對該臨時號碼的呼叫能夠到達驗證伺服器。使其中，驗證伺服器透過 HSTP/LSTP（High/Low Signal Transfer Point，傳統通信網中的信號傳輸點）與 HLR 發送進行通信。

返回模組 230 用於將中間號碼返回至業務伺服器，以透過業務伺服器將中間號碼提供給用戶的用戶端。

業務伺服器從驗證伺服器獲取與第一用戶識別碼對應的中間號碼之後，可將該中間號碼發送至用戶的用戶端。用戶端將該中間號碼顯示給用戶，從而，用戶端的用戶可透過電話通信網路向該中間號碼發起呼叫請求。

獲取模組 240 用於從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼。

由於中間號碼的路由指向驗證伺服器，因此，當中間號碼被呼叫時，驗證伺服器可接收到呼叫請求，獲取模組 240 可從電話通信網路中獲取向中間號碼發起呼叫的號碼，即第二用戶識別碼。

驗證模組 250 用於驗證第一用戶識別碼與第二用戶識別碼是否一致，並將驗證結果返回至業務伺服器。

如驗證模組 250 的驗證結果為第一用戶識別碼與第二用戶識別碼一致，則可判斷用戶端的用戶通過驗證（本次

呼叫由用戶本人發起），業務伺服器可回應該資料交互請求；如果驗證模組 250 的驗證結果為第一用戶識別碼與第二用戶識別碼不一致，則可判斷用戶端的用戶未通過驗證（本次呼叫並非由用戶本人發起），業務伺服器可拒絕回應該資料交互請求，並提示用戶端的用戶驗證失敗。

在本發明的一個實施例中，驗證模組 250 還可記錄呼叫過程中用戶的交互記錄，並判斷該交互記錄是否符合預設交互要求。如果交互記錄符合預設交互要求、且驗證模組 250 返回的驗證結果為第一用戶識別碼與第二用戶識別碼一致，則判斷用戶的身分驗證通過，否則，二者中有任一條件不滿足，則判斷用戶的身分驗證未通過。然後將驗證結果發送至業務伺服器。

本發明實施例的驗證伺服器，可為業務伺服器發送的第一用戶識別碼分配相應的中間號碼，並透過業務伺服器提供給用戶的用戶端，當中間號碼接收到呼叫時，從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼，並透過驗證第一用戶識別碼與第二用戶識別碼是否一致得到驗證結果。該實施例將電話通信網路的封閉性與網路的開放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全性。

為了實現上述實施例，本發明還提出一種身分驗證系

統。

圖 9 為根據本發明一個實施例的身分驗證系統的結構示意圖。

如圖 9 所示，根據本發明實施例的身分驗證系統，包括：業務伺服器 100、驗證伺服器 200 和用戶端 300。

其中，業務伺服器 100 可為本發明任一實施例的業務伺服器。

驗證伺服器 200 可為本發明任一實施例的驗證伺服器。

用戶端 300 可為 WEB 頁面端、APP 端或 WAP 頁面端等。

本發明實施例的身分驗證系統，業務伺服器在接收到用戶端的資料交互請求時，可獲取用戶端對應的第一用戶識別碼，並從驗證伺服器獲取與第一用戶識別碼相應的中間號碼發送之用戶端進行顯示，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫，驗證伺服器可從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼，並透過驗證第一用戶識別碼與第二用戶識別碼是否一致得到驗證結果。該實施例將電話通信網路的封閉性與網路的開放性特點相結合，而基於電話通信網路封閉性，電話通信網路相對於網路來說接入門檻較高，不易被外界接入，因此將高安全性的電話通信網路應用到傳統的網路中的身分驗證，且將身分驗證過程從非同步流程變成一個同步的流程，有效提高了身分驗證的可靠性和安全性。

流程圖中或在此以其他方式描述的任何過程或方法描述可以被理解為，表示包括一個或更多個用於實現特定邏輯功能或過程的步驟的可執行指令的代碼的模組、片段或部分，並且本發明的較佳實施方式的範圍包括另外的實現，其中可以不按所示出或討論的順序，包括根據所涉及的功能按基本同時的方式或按相反的順序，來執行功能，這應被本發明的實施例所屬技術領域的技術人員所理解。

在流程圖中表示或在此以其他方式描述的邏輯和/或步驟，例如，可以被認為是用於實現邏輯功能的可執行指令的定序列表，可以具體實現在任何電腦可讀介質中，以供指令執行系統、裝置或設備（如基於電腦的系統、包括處理器的系統或其他可以從指令執行系統、裝置或設備取指令並執行指令的系統）使用，或結合這些指令執行系統、裝置或設備而使用。就本說明書而言，"電腦可讀介質"可以是任何可以包含、儲存、通信、傳播或傳輸程式以供指令執行系統、裝置或設備或結合這些指令執行系統、裝置或設備而使用的裝置。電腦可讀介質的更具體的示例（非窮盡性列表）包括以下：具有一個或多個佈線的電連接部（電子裝置），可攜式電腦盤盒（磁裝置），隨機存取記憶體（RAM），唯讀記憶體（ROM），可擦除可程式化唯讀記憶體（EPROM或快閃記憶體），光纖裝置，以及可攜式光碟唯讀記憶體（CDROM）。另外，電腦可讀介質甚至可以是可在其上列印所述程式的紙或其他合適的介質，因為可以例如透過對紙或其他介質進行光學

掃描，接著進行編輯、解譯或必要時以其他合適方式進行處理來以電子方式獲得所述程式，然後將其儲存在電腦記憶體中。

應當理解，本發明的各部分可以用硬體、軟體、韌體或它們的組合來實現。在上述實施方式中，多個步驟或方法可以用儲存在記憶體中且由合適的指令執行系統執行的軟體或韌體來實現。例如，如果用硬體來實現，和在另一實施方式中一樣，可用本領域所知的下列技術中的任一項或他們的組合來實現：具有用於對資料信號實現邏輯功能的邏輯閘電路的離散邏輯電路，具有合適的組合邏輯閘電路的專用積體電路，可程式邏輯閘陣列（PGA），場可程式邏輯閘陣列（FPGA）等。

本技術領域的具有通常知識者可以理解實現上述實施例方法攜帶的全部或部分步驟是可以透過程式來指令相關的硬體完成，所述的程式可以儲存於一種電腦可讀儲存介質中，該程式在執行時，包括方法實施例的步驟之一或其組合。

此外，在本發明各個實施例中的各功能單元可以集成在一個處理模組中，也可以是各個單元單獨物理存在，也可以兩個或兩個以上單元集成在一個模組中。上述集成的模組既可以採用硬體的形式實現，也可以採用軟體功能模組的形式實現。所述集成的模組如果以軟體功能模組的形式實現並作為獨立的產品銷售或使用時，也可以儲存在一個電腦可讀取儲存介質中。

上述提到的儲存介質可以是唯讀記憶體，磁片或光碟等。

在本說明書的描述中，參考術語“一個實施例”、“一些實施例”、“示例”、“具體示例”、或“一些示例”等的描述意指結合該實施例或示例描述的具體特徵、結構、材料或者特點包含於本發明的至少一個實施例或示例中。在本說明書中，對上述術語的示意性表述不一定指的是相同的實施例或示例。而且，描述的具體特徵、結構、材料或者特點可以在任何的一個或多個實施例或示例中以合適的方式結合。

儘管已經示出和描述了本發明的實施例，本領域的具有通常知識者可以理解：在不脫離本發明的原理和宗旨的情況下可以對這些實施例進行多種變化、修改、替換和變型，本發明的範圍由申請專利範圍及其等同限定。

【符號說明】

S101~S106：步驟

S201~S207：步驟

S301~S305：步驟

100：業務伺服器

110：第一獲取模組

120：第一發送模組

130：第二獲取模組

140：第二發送模組

150：第一接收模組

160：處理模組

170：確定模組

180：第二接收模組

190：驗證模組

200：驗證伺服器

210：接收模組

220：分配模組

230：返回模組

240：獲取模組

250：驗證模組

300：用戶端

201719475

發明摘要

G06F 21/30 (2013.01)
H04W 12/06 (2009.01)

※申請案號：105118603

※申請日：105 年 06 月 14 日　　※IPC 分類：

【發明名稱】(中文/英文)

身分驗證方法、系統、業務伺服器和驗證伺服器

【中文】

本發明提出一種身分驗證方法、業務伺服器、驗證伺服器和身分驗證系統，其中，該方法，包括：當透過網路接收到用戶端發送的資料交互請求時，獲取用戶端對應的第一用戶識別碼；將第一用戶識別碼發送至驗證伺服器；從驗證伺服器獲取與第一用戶識別碼對應的中間號碼；將中間號碼發送至用戶端，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫請求；接收驗證伺服器根據呼叫請求回饋的身分驗證的驗證結果；根據驗證結果處理資料交互請求。本發明的身分驗證方法，將電話通信網路的封閉性與網路的開放性特點相結合，有效提高了身分驗證的可靠性和安全性。

【英文】

【代表圖】

【本案指定代表圖】：第(1)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

申請專利範圍

1. 一種身分驗證方法，其特徵在於，包括以下步驟：

當透過網路接收到用戶端發送的資料交互請求時，獲取該用戶端對應的第一用戶識別碼；

將該第一用戶識別碼發送至驗證伺服器；

從該驗證伺服器獲取與該第一用戶識別碼對應的中間號碼；

將該中間號碼發送至該用戶端，以使該用戶端的用戶透過電話通信網路向該中間號碼發起呼叫請求；

接收該驗證伺服器根據該呼叫請求回饋的該身分驗證的驗證結果；

根據該驗證結果處理該資料交互請求。

2. 如申請專利範圍第 1 項所述的身分驗證方法，還包括：

當透過網路接收到用戶端發送的資料交互請求時，確定該資料交互請求對應的風險等級；

其中，在該資料交互請求對應的風險等級高於預設等級時，獲取該用戶端的用戶的第一用戶識別碼。

3. 如申請專利範圍第 1 項所述的身分驗證方法，其中，該獲取該用戶端的用戶的第一用戶識別碼，具體包括：

從用戶資料庫中提取該用戶端的用戶的第一用戶識別碼。

4. 如申請專利範圍第 1 項所述的身分驗證方法，其中，該獲取該用戶端的用戶的第一用戶識別碼，具體包括：

向該用戶端發送用戶識別碼輸入請求，以使該用戶端的用戶輸入該第一用戶識別碼。

5. 如申請專利範圍第 1 項所述的身分驗證方法，還包括：

接收該驗證伺服器發送的該呼叫過程中的交互記錄；

根據該驗證結果交互記錄對該用戶端的用戶進行身分驗證。

6. 一種身分驗證方法，其特徵在於，包括以下步驟：

接收業務伺服器發送的第一用戶識別碼；

為該第一用戶識別碼分配對應的中間號碼；

將所述中間號碼返回至該業務伺服器，以透過該業務伺服器將該中間號碼提供給用戶的用戶端；

從電話通信網路獲取向該中間號碼發起該呼叫的第二用戶識別碼；

驗證該第一用戶識別碼與該第二用戶識別碼是否一致，並將驗證結果返回至該業務伺服器。

7. 如申請專利範圍第 6 項所述的身分驗證方法，其中，該為該第一用戶識別碼分配對應的中間號碼，包括：

從預設的號碼池中隨機選擇一個臨時號碼，並將該臨時號碼作為該第一用戶識別碼對應的中間號碼。

8. 如申請專利範圍第 6 項所述的身分驗證方法，其中，該為該第一用戶識別碼分配對應的中間號碼，包括：

將預設的號碼作為該第一用戶識別碼對應的中間號碼。

9. 一種業務伺服器，其特徵在於，包括：

第一獲取模組，用於當透過網路接收到用戶端發送的資料交互請求時，獲取該用戶端對應的第一用戶識別碼；

第一發送模組，用於將該第一用戶識別碼發送至驗證伺服器；

第二獲取模組，用於從該驗證伺服器獲取與該第一用戶識別碼對應的中間號碼；

第二發送模組，用於將該中間號碼發送至該用戶端，以使該用戶端的用戶透過電話通信網路向該中間號碼發起呼叫請求；

第一接收模組，用於接收驗證伺服器根據該呼叫請求回饋的該身分驗證的驗證結果；

處理模組，用於根據該驗證結果處理該資料交互請求。

10. 如申請專利範圍第 9 項所述的業務伺服器，還包括：

確定模組，用於當透過網路接收到用戶端發送的資料交互請求時，確定該資料交互請求對應的風險等級；

其中，該第一獲取模組用於在該資料交互請求對應的風險等級高於預設等級時，獲取該用戶端的用戶的第一用

戶識別碼。

11. 如申請專利範圍第 9 項所述的業務伺服器，其中，該第一獲取模組用於：

從用戶資料庫中提取該用戶端的用戶的第一用戶識別碼。

12. 如申請專利範圍第 9 項所述的業務伺服器，其中，該第一獲取模組用於：

向該用戶端發送用戶識別碼輸入請求，以使該用戶端的用戶輸入該第一用戶識別碼。

13. 如申請專利範圍第 9 項所述的業務伺服器，還包括：

第二接收模組，用於接收該驗證伺服器發送的該呼叫過程中的交互記錄；

驗證模組，用於根據該交互記錄對該用戶端的用戶進行身分驗證。

14. 一種驗證伺服器，其特徵在於，包括：

接收模組，用於接收業務伺服器發送的第一用戶識別碼；

分配模組，用於為該第一用戶識別碼分配對應的中間號碼；

返回模組，用於將該中間號碼返回至該業務伺服器，以透過該業務伺服器將該中間號碼提供給用戶的用戶端；

獲取模組，用於從電話通信網路獲取向該中間號碼發起該呼叫的第二用戶識別碼；

驗證模組，用於驗證該第一用戶識別碼與該第二用戶識別碼是否一致，並將驗證結果返回至該業務伺服器。

15. 如申請專利範圍第 14 項所述的驗證伺服器，其中，該分配模組用於：

從預設的號碼池中隨機選擇一個臨時號碼，並將該臨時號碼作為該第一用戶識別碼對應的中間號碼。

16. 如申請專利範圍第 14 項所述的驗證伺服器，其中，該分配模組用於：

將預設的號碼作為該第一用戶識別碼對應的中間號碼。

17. 一種身分驗證系統，其特徵在於，包括：

用戶端；

如申請專利範圍第 9-13 項中任一項所述的業務伺服器；以及

如申請專利範圍第 14-16 項中任一項所述的驗證伺服器。

圖式

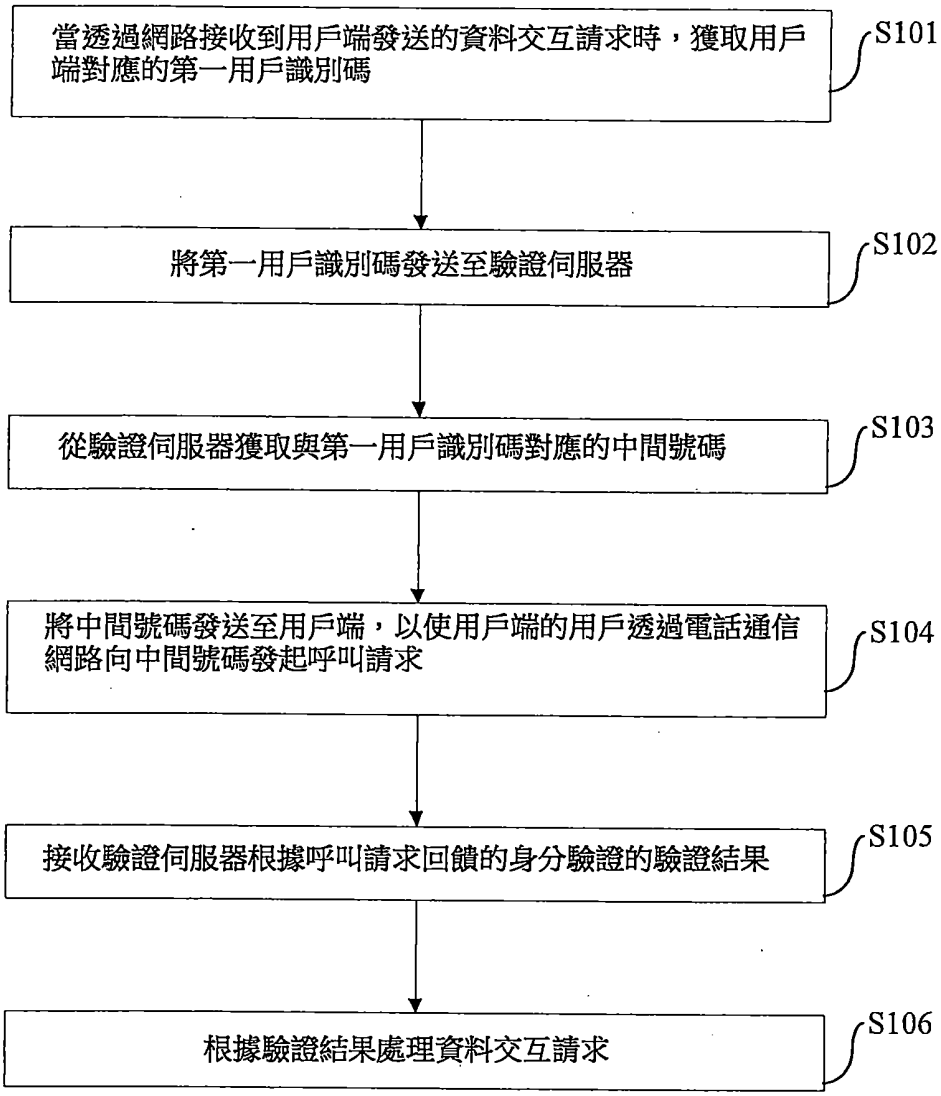
當透過網路接收到用戶端發送的資料交互請求時，獲取用戶端對應的第一用戶識別碼
S101
將第一用戶識別碼發送至驗證伺服器
S102
從驗證伺服器獲取與第一用戶識別碼對應的中間號碼
S103
將中間號碼發送至用戶端，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫請求
S104
接收驗證伺服器根據呼叫請求回饋的身分驗證的驗證結果
S105
根據驗證結果處理資料交互請求
S106

圖 1

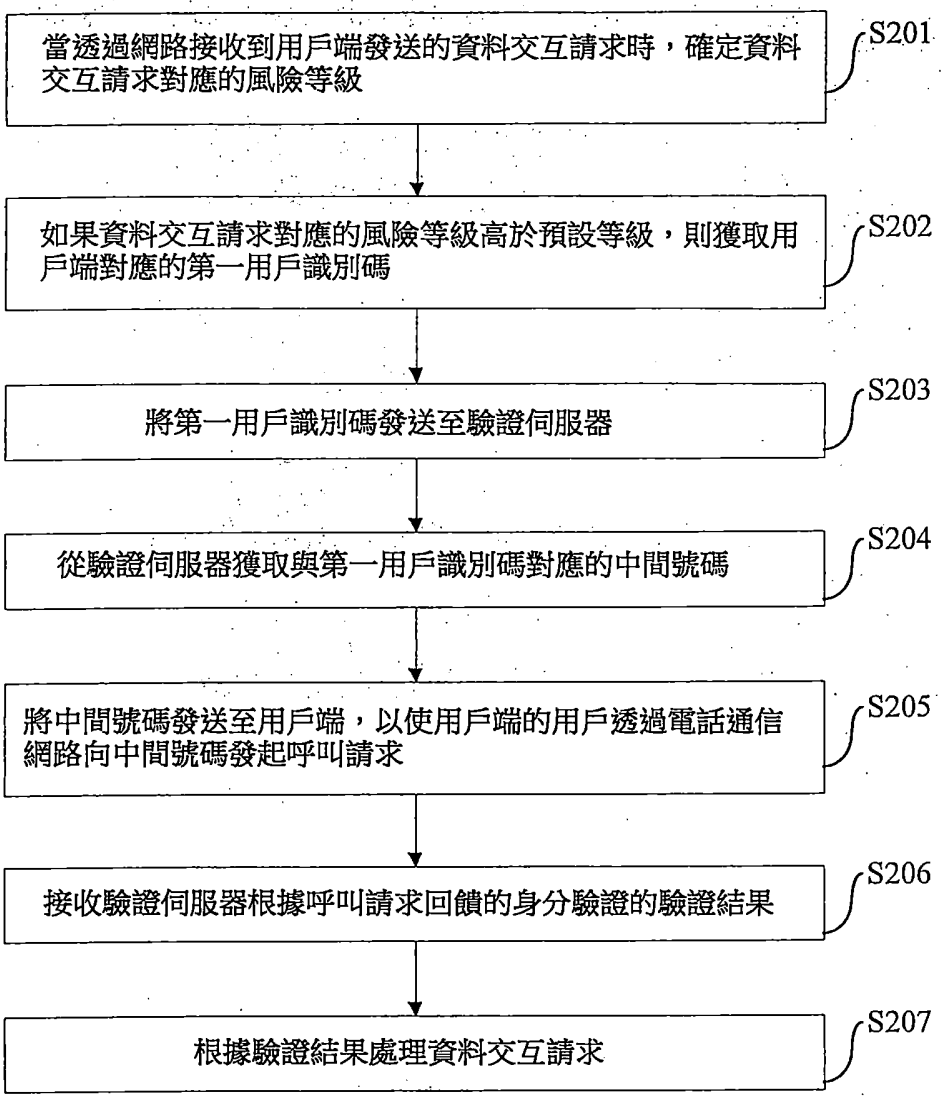
當透過網路接收到用戶端發送的資料交互請求時，確定資料交互請求對應的風險等級
S201
如果資料交互請求對應的風險等級高於預設等級，則獲取用戶端對應的第一用戶識別碼
S202
將第一用戶識別碼發送至驗證伺服器
S203
從驗證伺服器獲取與第一用戶識別碼對應的中間號碼
S204
將中間號碼發送至用戶端，以使用戶端的用戶透過電話通信網路向中間號碼發起呼叫請求
S205
接收驗證伺服器根據呼叫請求回饋的身分驗證的驗證結果
S206
根據驗證結果處理資料交互請求
S207

圖 2

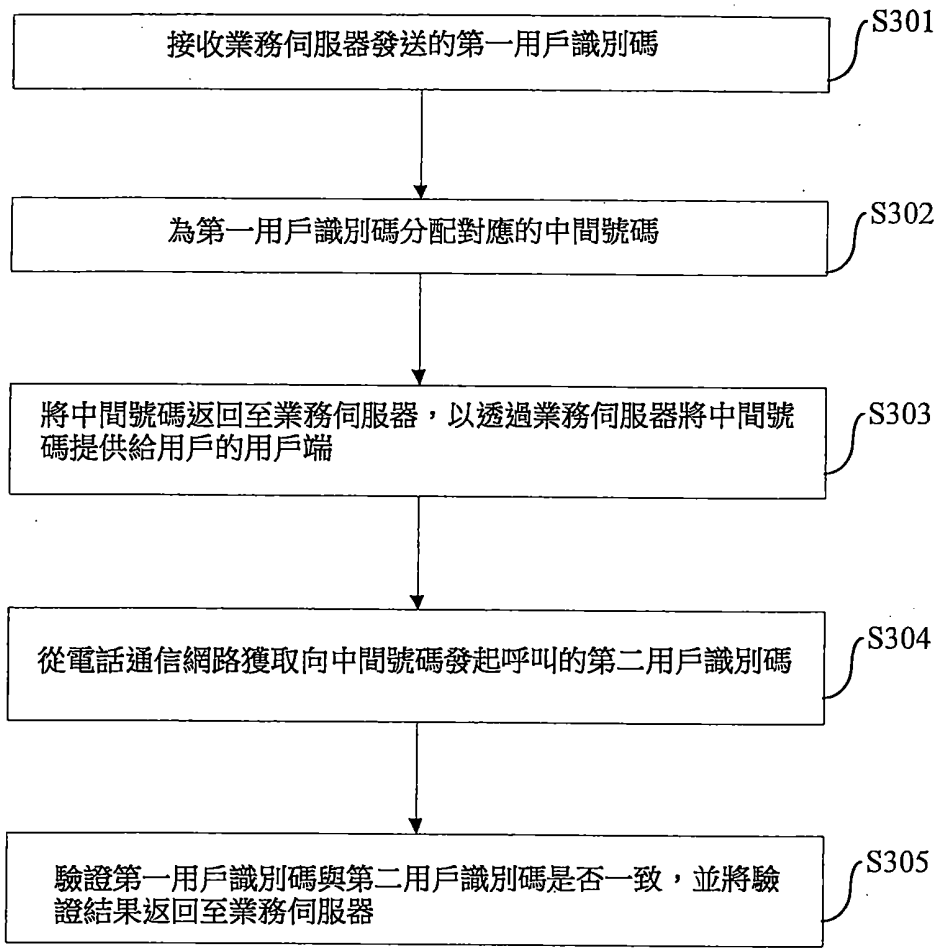
接收業務伺服器發送的第一用戶識別碼
S301
為第一用戶識別碼分配對應的中間號碼
S302
將中間號碼返回至業務伺服器，以透過業務伺服器將中間號碼提供給用戶的用戶端
S303
從電話通信網路獲取向中間號碼發起呼叫的第二用戶識別碼
S304
驗證第一用戶識別碼與第二用戶識別碼是否一致，並將驗證結果返回至業務伺服器
S305

圖 3

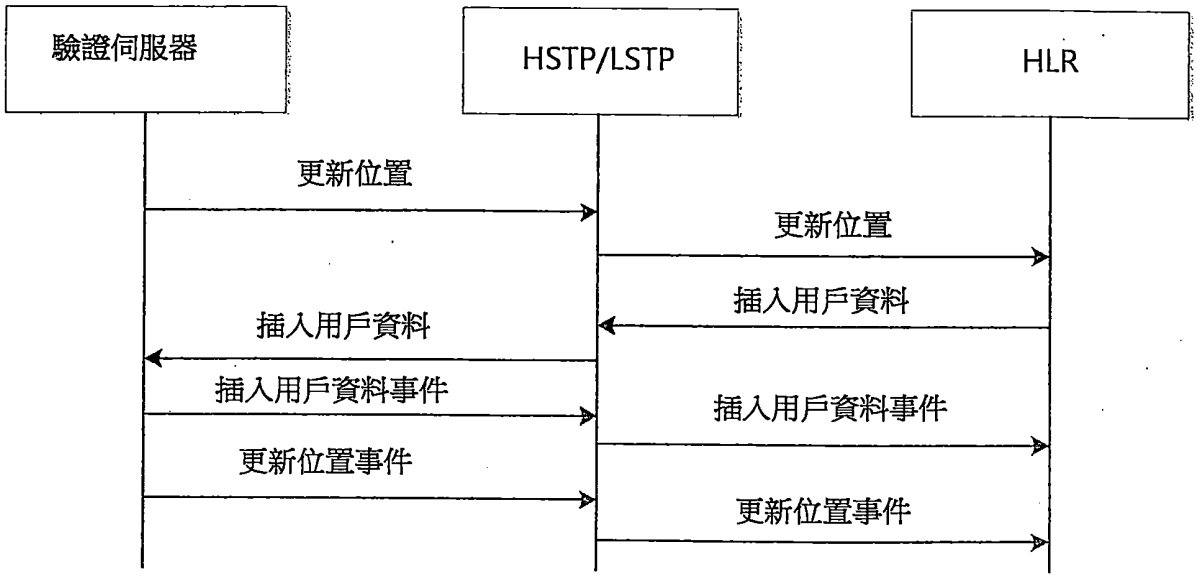
驗證伺服器
HSTP/LSTP
HLR
更新位置
更新位置
插入用戶資料
插入用戶資料
插入用戶資料事件
插入用戶資料事件
更新位置事件
更新位置事件

圖 4

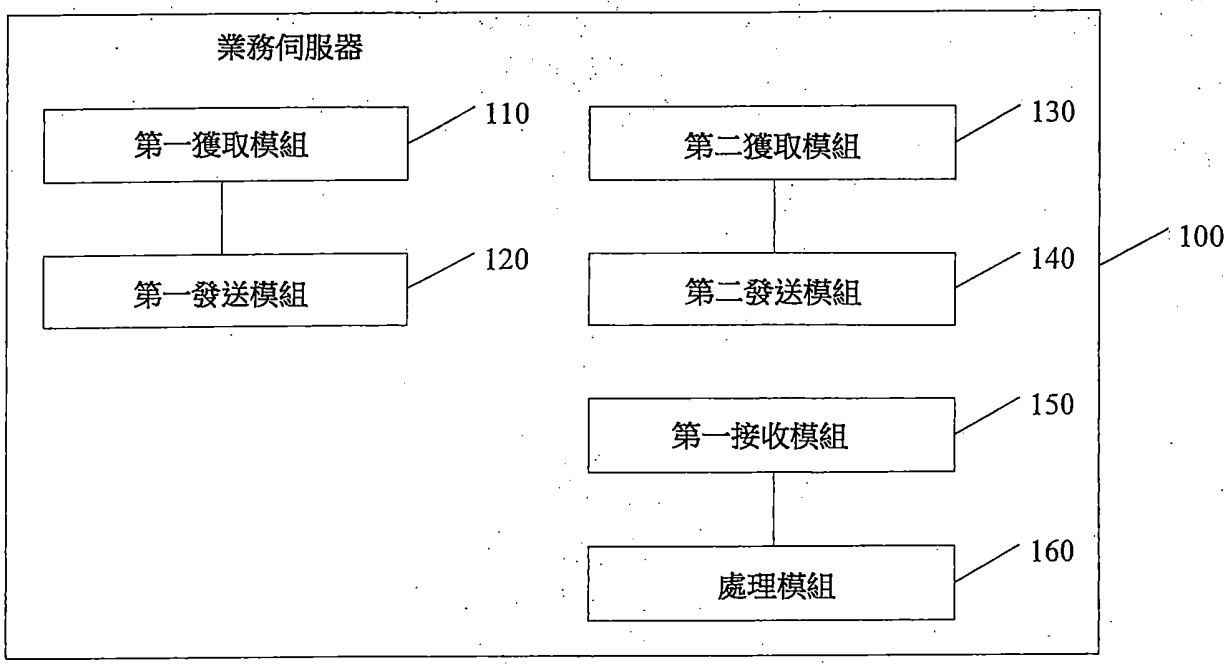
業務伺服器
第一獲取模組
110
第一發送模組
120
第二獲取模組
130
第二發送模組
140
第一接收模組
150
處理模組
160
100

圖 5

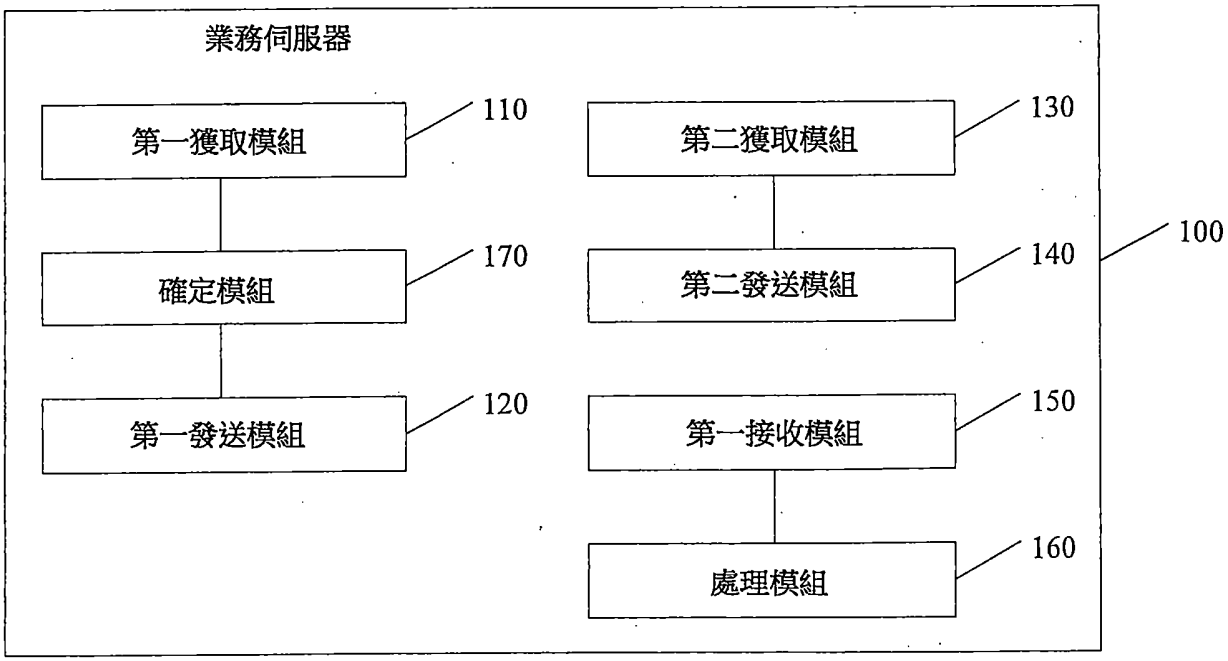
業務伺服器
第一獲取模組
110
確定模組
170
第一發送模組
120
第二獲取模組
130
第二發送模組
140
第一接收模組
150
處理模組
160
100

圖 6

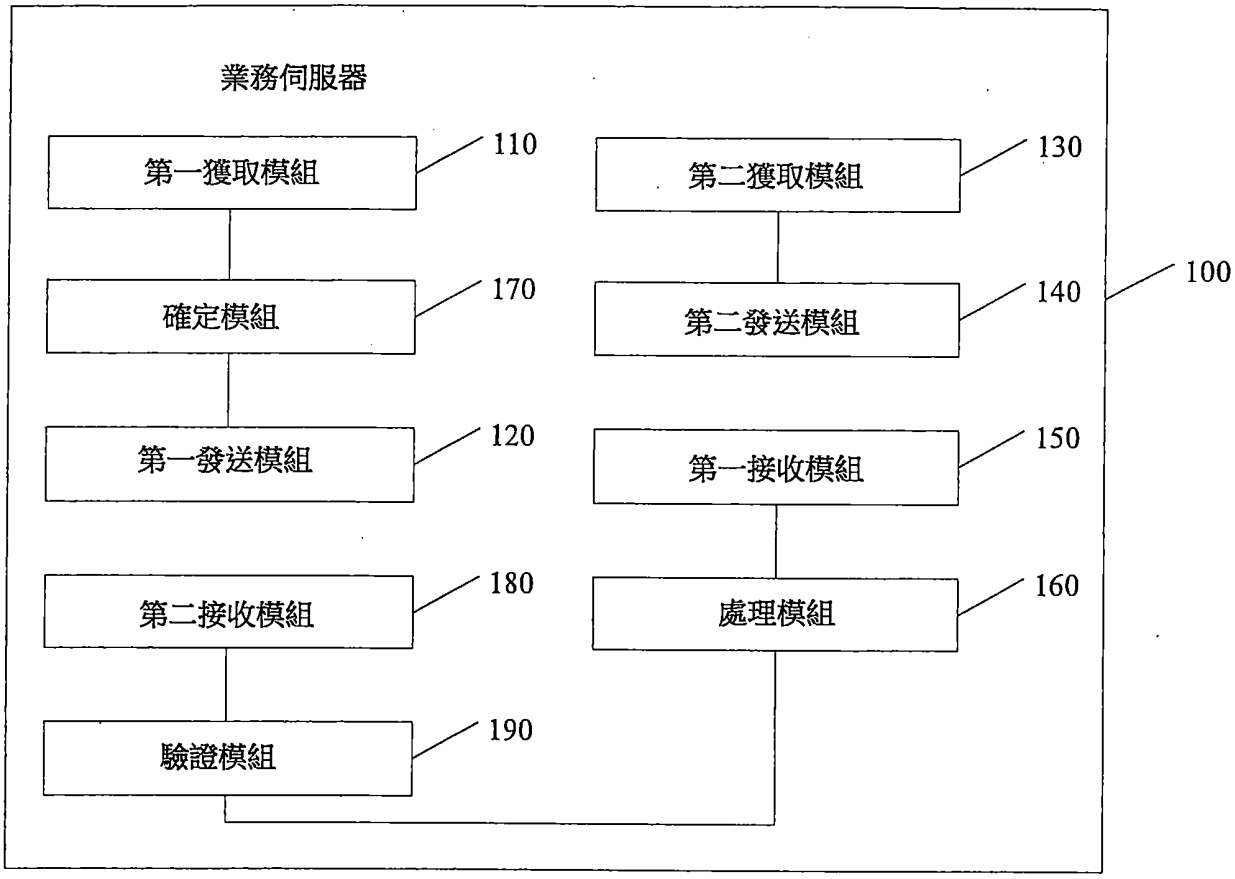
業務伺服器
第一獲取模組
110
第二獲取模組
130
確定模組
170
第二發送模組
140
100
第一發送模組
120
第一接收模組
150
第二接收模組
180
處理模組
160
驗證模組
190

圖 7

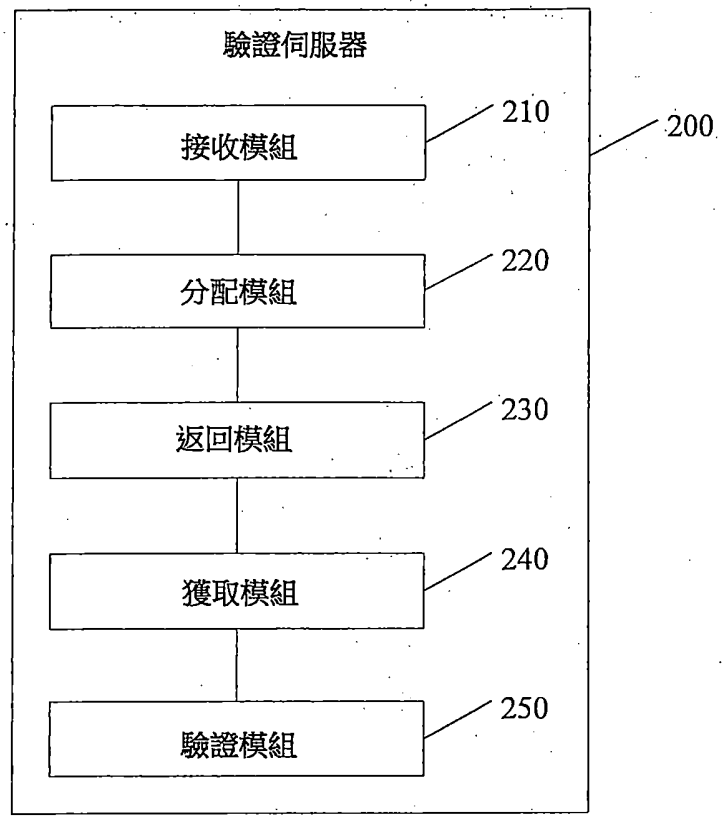
驗證伺服器
接收模組
210
200
分配模組
220
返回模組
230
獲取模組
240
驗證模組
250

圖 8

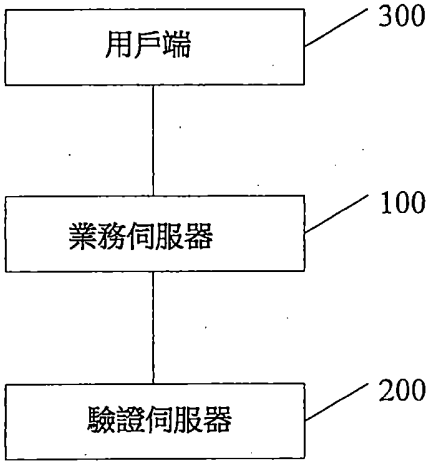
用戶端
300
業務伺服器
100
驗證伺服器
200

圖 9