201710944

(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 201710944 A

(43)公開日： 中華民國 106 (2017) 年 03 月 16 日

(21)申請案號：105107215 (22)申請日： 中華民國 105 (2016) 年 03 月 09 日

(51)Int. Cl.： *G06F21/60 (2013.01)* *G06F21/31 (2013.01)*

(30)優先權：2015/09/01 中國大陸 201510551943.8

(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：郭棟 (CN) ；原攀峰 (CN) ；劉鑫 (CN) ；陳廷梁 (CN)

(74)代理人：林志剛

申請實體審查：無 申請專利範圍項數：16 項 圖式數：5 共 38 頁

(54)名稱

鑒權方法及鑒權裝置

(57)摘要

本案實施例揭露了一種鑒權方法及鑒權裝置，所述方法包括：接收終端發送的攜帶使用者資訊及待鑒權的許可權點資訊的鑒權請求；根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；確定與所述使用者資訊相關聯的至少一個上層主體資訊；根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；將所述第一集合與所述第二集合的交集確定為鑒權集合；判斷所述待鑒權的許可權點資訊是否在所述鑒權集合中；若是，則判定鑒權通過。本案實施例可以實現包含多個主體的應用的許可權管理。

指定代表圖：

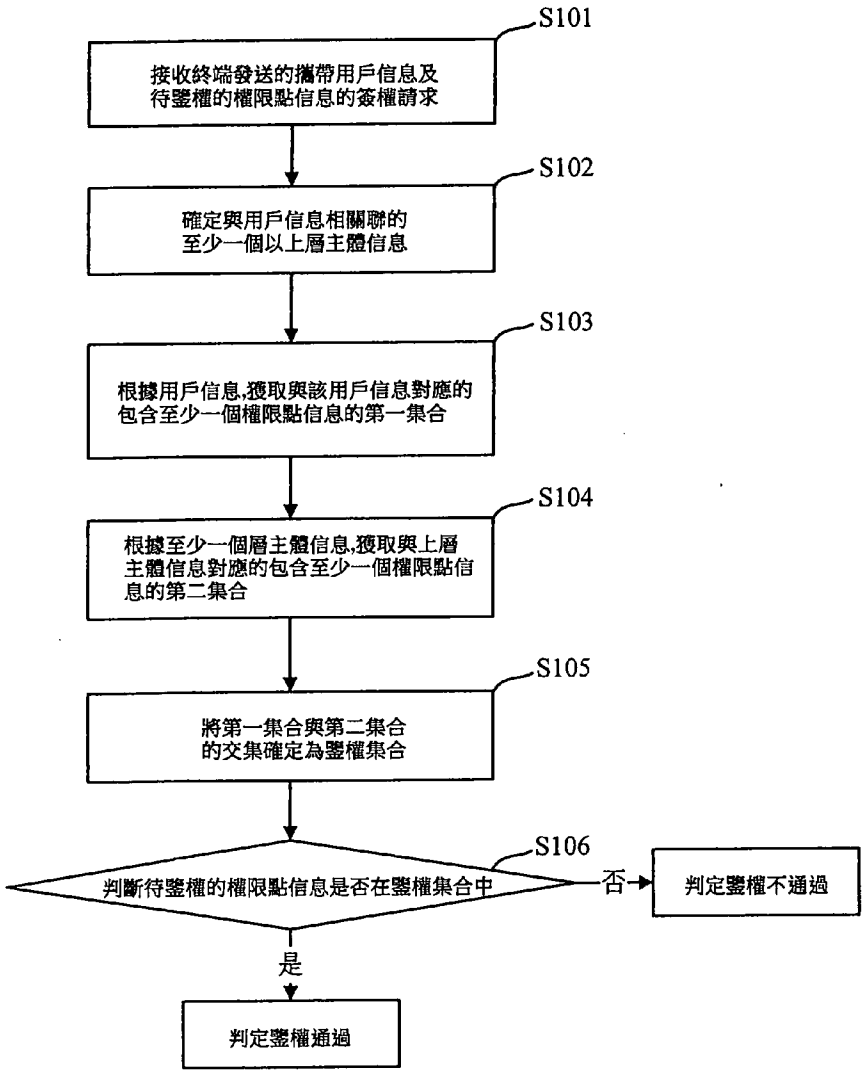
S101
接收終端發送的攜帶用戶信息及待鑒權的權限點信息的簽權請求
S102
確定與用戶信息相關聯的至少一個以上層主體信息
S103
根據用戶信息,獲取與該用戶信息對應的包含至少一個權限點信息的第一集合
S104
根據至少一個層主體信息,獲取與上層主體信息對應的包含至少一個權限點信息的第二集合
S105
將第一集合與第二集合的交集確定為鑒權集合
S106
判斷待鑒權的權限點信息是否在鑒權集合中
否
判定鑒權不通過
是
判定鑒權通過

圖 2

201710944

發明摘要

※申請案號：105107215

※申請日：105 年 03 月 09 日　　※IPC 分類：

G06F 21/60 (2013.01)

G06F 21/31 (2013.01)

【發明名稱】(中文/英文)

鑒權方法及鑒權裝置

【中文】

本案實施例揭露了一種鑒權方法及鑒權裝置，所述方法包括：接收終端發送的攜帶使用者資訊及待鑒權的許可權點資訊的鑒權請求；根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；確定與所述使用者資訊相關聯的至少一個上層主體資訊；根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；將所述第一集合與所述第二集合的交集確定為鑒權集合；判斷所述待鑒權的許可權點資訊是否在所述鑒權集合中；若是，則判定鑒權通過。本案實施例可以實現包含多個主體的應用的許可權管理。

【英文】

【代表圖】

【本案指定代表圖】：第(２)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

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)

鑒權方法及鑒權裝置

【技術領域】

本案涉及電腦技術領域，特別涉及一種鑒權方法及鑒權裝置。

【先前技術】

許可權管理，一般指根據系統設置的安全規則或者安全性原則，使用者可以訪問而且只能訪問自己被授權的資源。許可權管理技術是管理應用系統中的主體訪問客體的許可權的技術，其可以應用與任何藉由使用者帳戶及密碼進行登陸的應用系統中。

現有技術中，上述主體可以是各個用戶，上述客體可以是系統中的各種資源，如：各個模組下的資源、資料服務資源等。應用系統藉由預先為每個使用者分配相應的許可權資訊，並將這些許可權資訊與各個使用者的 ID 進行映射並存儲，從而在系統鑒權的過程中，根據使用者登陸的 ID 查詢到該使用者所具備的許可權資訊，實現許可權管理。

在一些特殊的應用系統（如：大數據平台）中，一般還可以根據實際需求，系統中可以根據實際需求設置其他

的主體，比如：租戶、項目等。在這些包括多種主體的應用系統中，可以將各個用戶劃分到相應的專案或租戶中來實現管理，對於不同的專案、或租戶而言，訪問系統資源的許可權也不盡相同。

在實現本案的過程中，發明人發現現有技術至少存在以下問題：

目前還沒有實現包括多種主體的應用系統的許可權管理的技術。

【發明內容】

本案實施例的目的是提供一種鑒權方法及鑒權裝置，以實現解決現有技術無法實現包括多種主體的應用系統的許可權管理的問題。

為解決上述技術問題，本案實施例提供的鑒權方法及裝置是這樣實現的：

一種鑒權方法，包括：

接收終端發送的攜帶使用者資訊及待鑒權的許可權點資訊的鑒權請求；

確定與所述使用者資訊相關聯的至少一個上層主體資訊；

根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；

根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；

將所述第一集合與所述第二集合的交集確定為鑒權集合；

判斷所述待鑒權的許可權點資訊是否在所述鑒權集合中；

若是，則判定鑒權通過。

一種鑒權方法，包括：

接收終端發送的攜帶使用者資訊及待鑒權資訊集合的鑒權請求；其中，所述待鑒權資訊集合包含至少一個待鑒權的許可權點資訊；

確定與所述使用者資訊相關聯的至少一個上層主體資訊；

根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；

根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；

將所述第一集合與所述第二集合的交集確定為鑒權集合；

判斷所述待鑒權資訊集合與所述鑒權集合是否有交集；

若是，將所述待鑒權資訊集合與所述鑒權集合的交集確定為與當前的鑒權請求對應的鑒權通過的許可權點資訊的集合。

一種鑒權裝置，包括：

接收單元，用於接收終端發送的攜帶使用者資訊及待

鑒權的許可權點資訊的鑒權請求；

第一確定單元，用於確定與所述使用者資訊相關聯的至少一個上層主體資訊；

第一獲取單元，用於根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；

第二獲取單元，用於根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；

第二確定單元，用於將所述第一集合與所述第二集合的交集確定為鑒權集合；

判斷單元，用於判斷所述待鑒權的許可權點資訊是否在所述鑒權集合中，若是，則判定鑒權通過。

一種鑒權裝置，包括：

接收單元，用於接收終端發送的攜帶使用者資訊及待鑒權資訊集合的鑒權請求；其中，所述待鑒權資訊集合包含至少一個待鑒權的許可權點資訊；

第一確定單元，用於確定與所述使用者資訊相關聯的至少一個上層主體資訊；

第一獲取單元，用於根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；

第二獲取單元，用於根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點

資訊的第二集合；

第二確定單元，用於將所述第一集合與所述第二集合的交集確定為鑒權集合；

鑒權確定單元，用於判斷所述待鑒權資訊集合與所述鑒權集合是否有交集；若是，將所述待鑒權資訊集合與所述鑒權集合的交集確定為與當前的鑒權請求對應的鑒權通過的許可權點資訊的集合。

由以上本案實施例提供的技術方案可見，本案實施例藉由接收終端發送的包含使用者資訊的鑒權請求，根據使用者資訊獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；之後確定與上述使用者資訊相關聯的至少一個上層主體資訊，並獲取與該上層主體資訊對應的包含至少一個許可權點資訊的第二集合；最終，根據獲取到的第一集合和第二集合，將第一集合、第二集合的交集確定為鑒權集合，根據該鑒權集合來判定終端發送的鑒權請求是否通過。從而基於以上過程，本案實施例可以實現包含多個主體的應用的許可權管理。

【圖式簡單說明】

為了更清楚地說明本案實施例或現有技術中的技術方案，下面將對實施例或現有技術描述中所需要使用的附圖作簡單地介紹，顯而易見地，下面描述中的附圖僅僅是本案中記載的一些實施例，對於本領域普通技術人員來講，在不付出創造性勞動性的前提下，還可以根據這些附圖獲

得其他的附圖。

圖 1 為示出了本案實施例中包含多個主體的應用系統的架構；

圖 2 為本案一實施例中鑒權方法的流程圖；

圖 3 為本案另一實施例中鑒權方法的流程圖；

圖 4 為本案一實施例中鑒權裝置的模組圖；

圖 5 為本案另一實施例中鑒權裝置的模組圖。

【實施方式】

為了使本技術領域的人員更好地理解本案中的技術方案，下面將結合本案實施例中的附圖，對本案實施例中的技術方案進行清楚、完整地描述，顯然，所描述的實施例僅僅是本案一部分實施例，而不是全部的實施例。基於本案中的實施例，本領域普通技術人員在沒有作出創造性勞動前提下所獲得的所有其他實施例，都應當屬於本案保護的範圍。

圖 1 為示出了本案實施例中包含多個主體的應用系統的架構，該架構的主體可以包括用戶及與各個用戶對應的上層主體，這些上層主體可以是租戶、或項目。在系統架構中，還可以包括平台管理級的主體，比如：平台管理人員。一般地，這個應用系統可以包含一個或多個租戶，每個租戶下可以包含一個或多個專案，每個專案中又可以包含一個或多個用戶。其中，定義上述租戶是使用上述應用系統的資源（可以是存儲資源、運算資源、開發資源等）

的客戶群體（如：公司），定義上述項目是從屬於上述租戶的子群體，每個項目可以對應於一個項目空間，該項目空間可以定義為使用者對資料進行加工處理的場所，使用者可以按照不同的產品線來劃分不同的項目空間。

通常，應用系統可以為系統中的每個主體分配相應的角色。這些角色可以包括用戶的角色、專案的角色、租戶的角色及管理級成員的角色。其中，使用者的角色還可以根據該使用者所屬的專案和租戶，分為用戶在項目級的角色、用戶在租戶級的角色。舉例而言，在圖 1 中，每個租戶中的角色包括租戶的擁有者、管理員及各個成員，成員的角色可以包括租戶級經理、租戶級科長、租戶級工程師等，成員的角色可以由管理員來管理，租戶的擁有者可以添加/刪除管理員。每個租戶可以創建專案，每個專案中的角色也可以包括專案的擁有者、管理員及各個成員，成員的角色可以包括項目級經理、項目級科長、項目級工程師等，成員的角色可以由管理員來管理，租戶的擁有者可以添加/刪除管理員。此外，平台管理級的成員的角色可以包括平台管理員等，平台管理員可以管理平台級的角色和管理許可權點資訊。所謂許可權點資訊是由客體（資源）+操作組成，例如：管理員的創建操作、管理員列表的查看操作、項目的創建操作、SQL 的發佈操作、使用者自訂函數的發佈操作、某個資料服務的使用操作等。

在上述應用系統中，每個租戶、項目作為一個群體，也具備相應的角色。比如：應用系統包括 1000 個租戶，

可以根據租戶的級別劃分租戶的角色，租戶的角色可以包括：{ZHRole 1、ZHRole 2、.....、ZHRole n}，那麼可以根據租戶的級別將上述 1000 個租戶分別與這 n 個租戶的角色：{ZHRole 1、ZHRole 2、.....、ZHRole n}進行映射。同理，租戶也可以根據需要為其下的各個專案劃分相應的許可權。假設某個租戶包括 100 個項目，項目的角色可以包括：{XMRole 1、XMRole 2、.....、XMRole m}，那麼可以將上述 100 個項目分別與這 m 個項目的角色：{XMRole 1、XMRole 2、.....、XMRole m}進行映射。當然，應用平台上的其他租戶下的項目也可以與上述項目的角色：{XMRole 1、XMRole 2、.....、XMRole m}進行映射。

上述應用平台可以根據將角色資訊與相應的一個或多個許可權點資訊（本文可以稱包含至少一個許可權點資訊的集合）進行映射。對於各個租戶而言，應用系統的伺服器上可以存儲各個租戶資訊與相應的租戶角色資訊的映射關係，以及各個租戶角色資訊與一個或多個許可權點資訊的映射關係。對於各個專案而言，應用系統的伺服器上可以存儲各個專案資訊與相應的專案角色資訊的映射關係，以及各個專案角色資訊與一個或多個許可權點資訊的映射關係。對應各個使用者而言，應用系統的伺服器上可以存儲各個使用者資訊與使用者角色資訊的映射關係（包括用戶在專案級別的角色資訊、使用者在租戶級別的角色資訊），以及各個使用者角色資訊與一個或多個許可權點資

訊的映射關係。

值得提及的是，本案的上層主體並不限於上述實施例介紹的租戶或項目，還可以是其他形式的主體，如：集團、歸屬於該集團下的至少一個子公司、歸屬於上述至少一個子公司下的至少一個部門等，並且，該應用系統包括的主體的數目也不受限制，如：可以包括三層主體或三層以上的主體。本文將以兩層上層主體為例來介紹本案的技術方案。

圖 2 為本案一實施例中鑒權方法的流程圖。上述鑒權方法的執行主體可以是應用系統的伺服器。基於上述應用系統的架構，本實施例的鑒權方法包括：

S101：接收終端發送的攜帶使用者資訊及待鑒權的許可權點資訊的鑒權請求。

上述終端可以是訪問上述伺服器的電腦、或智慧無線終端、或伺服器等。

使用者可以藉由上述終端採用使用者資訊及密碼的形式進行登陸，登陸成功後，根據登陸的使用者資訊向伺服器發送包含該使用者資訊及待鑒權的許可權點資訊的鑒權請求。其中，待鑒權的許可權點資訊可以根據使用者資訊來確定，該許可權點資訊可以是一個或者多個。當然，待鑒權的許可權點資訊也可以根據使用者的具體操作來確定，如：登陸終端的使用者在嘗試執行某個操作時，需通過鑒權過程來確定當前用戶是否具備這樣操作的許可權。

S102：確定與使用者資訊相關聯的至少一個上層主體

資訊。

舉例而言，若所述上層主體資訊包括兩個，分別是租戶資訊、專案資訊，則上述步驟 S102 可以具體包括：

確定與所述使用者資訊相關聯的租戶資訊；

確定與所述使用者資訊相關聯的、且歸屬於所述租戶資訊下的專案資訊；

在上述應用系統中，每個使用者會預先被劃分到相應的上層主體（租戶、專案）下。例如：使用者資訊可以是：“張三”，該使用者資訊“張三”所歸屬的上層主體資訊可以是：“X 租戶”、“X 租戶下的 Y 項目”。

S103：根據使用者資訊獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合。

本實施例中，所述第一集合 A 所包含的許可權點資訊可以對應於各個使用者的許可權，即許可權主體的是用戶。

如上所述，該步驟 S103 可以具體包括：

查詢與所述使用者資訊映射的第一角色資訊；其中，所述第一角色資訊用以標識所述使用者資訊對應的使用者在所述上層主體資訊對應的上層主體中的角色；

查詢與所述第一角色資訊映射的包含至少一個許可權點資訊的第一集合 A。

舉例而言，對於上述包括租戶、專案的應用系統而言，與使用者資訊相映射的第一角色資訊可以包括該使用者在租戶級的用戶角色、及該用戶在項目級的用戶角色。

假設根據使用者資訊：“張三”，確定到該用戶在租戶級的用戶角色例如是：“租戶級的經理”，確定到該用戶在專案級的用戶角色例如是：“項目總監”。根據上述使用者在不同的上層主體中的用戶角色：“租戶級的經理”和“項目總監”，可以分別藉由查詢得到與上述用戶角色對應的兩個包含至少一個許可權點資訊的集合 A1 和 A2，也就是說，這兩個集合 A1、A2 分別表示該用戶在租戶級別、項目級別所擁有的許可權。其中，第一集合 A 可以是上述兩個集合 A1 和 A2 的交集。假設 A1={許可權點 Q1、許可權點 Q2、許可權點 Q3、許可權點 Q4}，A2={許可權點 Q1、許可權點 Q3、許可權點 Q5、許可權點 Q4}，則藉由取交集，可以得到第一集合 A=A1∩A2={許可權點 Q1、許可權點 Q3、許可權點 Q4}。

值得述及的是，本案其他實施例中，應用系統中的上層主體可以只是租戶，而租戶下面沒有劃分項目，則只需獲取用戶在該租戶級別的角色資訊及其相應的許可權集合即可。另外，若應用系統包含較多數量的上層主體，當其中一個或多個上層主體空缺後，為確保最終得到的許可權交集不為空集，上述空缺的一個或多個上層主體所對應的許可權集合中可以包含所有可能擁有的許可權點。

S104：根據至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合。

如上所述，對於應用系統中的各個上層主體而言，其也具備相應的許可權。本案實施例中，若所述上層主體資

訊包括至少兩個，則上述步驟 S104 包括：

分別獲取與各個上層主體資訊對應的包括至少一個許可權點資訊的許可權集合；並將與各個上層主體資訊對應的許可權集合的交集確定為所述第二集合。

本案實施例中，該步驟 S104 可以具體包括：

查詢與所述上層主體資訊映射的第二角色資訊；其中，所述第二角色資訊用以標識該上層主體資訊對應的上層主體在應用系統中的角色；

查詢與所述第二角色資訊映射的包含至少一個許可權點資訊的第二集合 B。

對於包含租戶、專案的應用系統而言，上層主體資訊可以包括租戶資訊、專案資訊，則相應的第二角色資訊也包括該租戶在應用系統中角色資訊、及該專案在應用系統中角色資訊。則，獲取上述第二集合 B 的具體過程可以包括：

獲取與所述租戶資訊對應的包含至少一個許可權點資訊的許可權集合 B1；

獲取與所述專案資訊對應的包含至少一個許可權點資訊的許可權集合 B2；

將許可權集合 B1 與許可權集合 B2 的交集確定為所述第二集合 B。

舉例而言，對於使用者資訊：“張三”，藉由查詢用戶-上層主體映射表，可以得到其對應的專案資訊例如是：“X 租戶下的 Y 專案”，其對應的租戶資訊例如

是：“X 租戶”。藉由查詢上層主體-主體角色映射表，可以得到上述專案資訊：“X 租戶下的 Y 專案”對應的角色資訊是：“XMRole 11”，得到上述租戶資訊：“X 租戶”對應的角色資訊是：“ZHRole 12”。最終，藉由查詢主體角色資訊-許可權點資訊的映射表，可以得到上述角色資訊：“XMRole 11”對應的許可權集合 B1={許可權點 Q1、許可權點 Q2、許可權點 Q3、許可權點 Q4、許可權點 Q5、許可權點 Q6、許可權點 Q8、許可權點 Q10}，得到上述角色資訊“ZHRole 12”對應的許可權集合 B2={許可權點 Q2、許可權點 Q3、許可權點 Q4、許可權點 Q5、許可權點 Q6、許可權點 Q9、許可權點 Q10}，則，藉由取交集，得到第二集合 B=B1∩B2={許可權點 Q2、許可權點 Q3、許可權點 Q4、許可權點 Q5、許可權點 Q6、許可權點 Q10}。

S105：將第一集合 A 與第二集合 B 的交集 A∩B 確定為鑒權集合 C。

本案實施例中，第一集合 A 表示使用者在各個上層主體中的許可權點資訊集合。第二集合 B 表示使用者所屬的各個上層主體所具備的許可權點資訊集合。由於在上述應用系統的許可權管理機制中，下層主體所對應的許可權點資訊集合可以是上層主體所對應的許可權點資訊集合的子集。舉例而言，用戶是專案、租戶的下層主體，專案、租戶是用戶的上層主體，則用戶所對應的許可權點資訊集合是各個租戶、專案所對應的許可權點資訊集合的子集。

故，需要藉由將第一集合 A 與第二集合 B 的交集 A∩B 確定為鑒權集合 C，以確定該用戶最終能夠擁有的許可權。

S106：判斷待鑒權的許可權點資訊是否在鑒權集合 C 中。

繼續沿用上述例子，假設第一集合 A={許可權點 Q1、許可權點 Q3、許可權點 Q4}，第二集合 B={許可權點 Q2、許可權點 Q3、許可權點 Q4、許可權點 Q5、許可權點 Q6、許可權點 Q10}，則確定的鑒權集合 C=A∩B={許可權點 Q3、許可權點 Q4}。

若終端發送的鑒權請求中攜帶的待鑒權的許可權點資訊是：Q3、或 Q4、或{Q3、Q4}，由於這些許可權點資訊在鑒權集合 C 中，則判定鑒權通過，該終端的使用者具備相應的訪問應用系統的資源的許可權。相反地，若終端發送的鑒權資訊中攜帶的待鑒權的許可權點資訊不在上述鑒權集合 C 中，如：Q5，則判定鑒權不通過，該終端的使用者不具備相應的訪問應用系統的資源的許可權。

圖 3 為本案另一實施例中鑒權方法的流程圖。上述鑒權方法的執行主體可以是應用系統的伺服器。基於上述應用系統的架構，本實施例的鑒權方法包括：

S201：接收終端發送的攜帶使用者資訊及待鑒權資訊集合的鑒權請求；其中，所述待鑒權資訊集合包含至少一個待鑒權的許可權點資訊。

S202：根據使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合 A。

S203：確定與使用者資訊相關聯的至少一個上層主體資訊。

S204：根據至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合 B。

S205：將第一集合 A 與第二集合 B 的交集確定為鑒權集合 C。

上述步驟 S201~S205 可以參照上述步驟 S101~S105 的內容，定義該待鑒權資訊集合 D。

S206：判斷待鑒權資訊集合 D 與所述鑒權集合 C 是否有交集。

S207：若是，將所述待鑒權資訊集合 D 與所述鑒權集 C 合的交集確定為與當前的鑒權請求對應的鑒權通過的許可權點資訊的集合 E。

本案實施例中，若集合 E=D∩C=D，則表明待鑒權資訊集合 D 是鑒權集 C 的一個子集，也就是說，待鑒權資訊集合 D 包含的各個待鑒權的許可權點資訊全部落在最終確定的鑒權集合 C 中，可以判定鑒權完全通過；若集合 E=D∩C=空集，則表明待鑒權資訊集合 D 包含的各個待鑒權的許可權點資訊沒有一個落在最終確定的鑒權集合 C 中，可以判定鑒權完全不通過；若集合 E=D∩C 不是空集，而是集合 D 的子集，則表明待鑒權資訊集合 D 包含的各個待鑒權的許可權點資訊部分落在最終確定的鑒權集合 C 中，可以判定鑒權部分通過。

藉由上述過程，可以根據集合 E=D∩C 所包含的許可

權點資訊，來確定使用終端的使用者最終鑒權通過的許可權。

圖 4 為本案一實施例中鑒權裝置的模組圖。本實施例的鑒權裝置，包括：

接收單元 301，用於接收終端發送的攜帶使用者資訊及待鑒權的許可權點資訊的鑒權請求；

第一確定單元 302，用於確定與所述使用者資訊相關聯的至少一個上層主體資訊；

第一獲取單元 303，用於根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；

第二獲取單元 304，用於根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；

第二確定單元 305，用於將所述第一集合與所述第二集合的交集確定為鑒權集合；

判斷單元 306，用於判斷所述待鑒權的許可權點資訊是否在所述鑒權集合中，若是，則判定鑒權通過。

本案實施例中，所述第二獲取單元 304 具體用於：

若所述上層主體資訊包括至少兩個，則分別獲取與各個上層主體資訊對應的包括至少一個許可權點資訊的許可權集合；

將與各個上層主體資訊對應的許可權集合的交集確定為所述第二集合。

本案實施例中，若所述上層主體資訊包括租戶資訊、專案資訊，則，所述第一確定單元 302 具體用於：

確定與所述使用者資訊相關聯的租戶資訊；

確定與所述使用者資訊相關聯的、且歸屬於所述租戶資訊下的專案資訊；

則，所述第二獲取單元 304 具體用於：

獲取與所述租戶資訊對應的包含至少一個許可權點資訊的許可權集合；

獲取與所述專案資訊對應的包含至少一個許可權點資訊的許可權集合；

將所述租戶資訊對應的的許可權集合與所述專案資訊對應的許可權集合的交集確定為所述第二集合。

本案實施例中，所述第一獲取單元 302 具體用於：

查詢與所述使用者資訊映射的第一角色資訊；其中，所述第一角色資訊用以標識所述使用者資訊對應的使用者在所述上層主體資訊對應的上層主體中的角色；

查詢與所述第一角色資訊映射的包含至少一個許可權點資訊的第一集合；

所述第二獲取單元 304 具體用於：

查詢與至少一個上層主體資訊映射的至少一個第二角色資訊；其中，所述第二角色資訊用以標識該上層主體資訊對應的上層主體在應用系統中的角色；

查詢與至少一個第二角色資訊映射的包含至少一個許可權點資訊的第二集合。

圖 5 為本案另一實施例中鑒權裝置的模組圖。本實施例的鑒權裝置，包括：

接收單元 401，用於接收終端發送的攜帶使用者資訊及待鑒權資訊集合的鑒權請求；其中，所述待鑒權資訊集合包含至少一個待鑒權的許可權點資訊；

第一確定單元 402，用於確定與所述使用者資訊相關聯的至少一個上層主體資訊；

第一獲取單元 403，用於根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；

第二獲取單元 404，用於根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；

第二確定單元 405，用於將所述第一集合與所述第二集合的交集確定為鑒權集合；

鑒權確定單元 406，用於判斷所述待鑒權資訊集合與所述鑒權集合是否有交集；若是，將所述待鑒權資訊集合與所述鑒權集合的交集確定為與當前的鑒權請求對應的鑒權通過的許可權點資訊的集合。

本案實施例中，所述第二獲取單元 304 具體用於：

若所述上層主體資訊包括至少兩個，則分別獲取與各個上層主體資訊對應的包括至少一個許可權點資訊的許可權集合；

將與各個上層主體資訊對應的許可權集合的交集確定

為所述第二集合。

本案實施例中，若所述上層主體資訊包括租戶資訊、專案資訊，則，所述第一確定單元 302 具體用於：

確定與所述使用者資訊相關聯的租戶資訊；

確定與所述使用者資訊相關聯的、且歸屬於所述租戶資訊下的專案資訊；

則，所述第二獲取單元 304 具體用於：

獲取與所述租戶資訊對應的包含至少一個許可權點資訊的許可權集合；

獲取與所述專案資訊對應的包含至少一個許可權點資訊的許可權集合；

將所述租戶資訊對應的許可權集合與所述專案資訊對應的許可權集合的交集確定為所述第二集合。

本案實施例中，所述第一獲取單元 302 具體用於：

查詢與所述使用者資訊映射的第一角色資訊；其中，所述第一角色資訊用以標識所述使用者資訊對應的使用者在所述上層主體資訊對應的上層主體中的角色；

查詢與所述第一角色資訊映射的包含至少一個許可權點資訊的第一集合；

所述第二獲取單元 304 具體用於：

查詢與至少一個上層主體資訊映射的至少一個第二角色資訊；其中，所述第二角色資訊用以標識該上層主體資訊對應的上層主體在應用系統中的角色；

查詢與至少一個第二角色資訊映射的包含至少一個許

可權點資訊的第二集合。

綜上，本案實施例藉由接收終端發送的包含使用者資訊的鑒權請求，根據使用者資訊獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；之後確定與上述使用者資訊相關聯的至少一個上層主體資訊，並獲取與該上層主體資訊對應的包含至少一個許可權點資訊的第二集合；最終，根據獲取到的第一集合和第二集合，將第一集合、第二集合的交集確定為鑒權集合，根據該鑒權集合來判定終端發送的鑒權請求是否通過。從而基於以上過程，本案實施例可以實現包含多個主體的應用的許可權管理。

為了描述的方便，描述以上裝置時以功能分為各種單元分別描述。當然，在實施本案時可以把各單元的功能在同一個或多個軟體和/或硬體中實現。

本領域內的技術人員應明白，本發明的實施例可提供為方法、系統、或電腦程式產品。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電腦可用程式碼的電腦可用存儲媒體（包括但不限於磁碟記憶體、CD-ROM、光學記憶體等）上實施的電腦程式產品的形式。

本發明是參照根據本發明實施例的方法、設備（系統）、和電腦程式產品的流程圖和/或方塊圖來描述的。應理解可由電腦程式指令實現流程圖和/或方塊圖中的每

一流程和/或方塊、以及流程圖和/或方塊圖中的流程和/或方塊的結合。可提供這些電腦程式指令到通用電腦、專用電腦、嵌入式處理機或其他可程式設計資料處理設備的處理器以產生一個機器，使得藉由電腦或其他可程式設計資料處理設備的處理器執行的指令產生用於實現在流程圖一個流程或多個流程和/或方塊圖一個方塊或多個方塊中指定的功能的裝置。

這些電腦程式指令也可存儲在能引導電腦或其他可程式設計資料處理設備以特定方式工作的電腦可讀記憶體中，使得存儲在該電腦可讀記憶體中的指令產生包括指令裝置的製造品，該指令裝置實現在流程圖一個流程或多個流程和/或方塊圖一個方塊或多個方塊中指定的功能。

這些電腦程式指令也可裝載到電腦或其他可程式設計資料處理設備上，使得在電腦或其他可程式設計設備上執行一系列操作步驟以產生電腦實現的處理，從而在電腦或其他可程式設計設備上執行的指令提供用於實現在流程圖一個流程或多個流程和/或方塊圖一個方塊或多個方塊中指定的功能的步驟。

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，本案的實施例可提供為方法、系統或電腦程式產品。因此，本案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，本案可採用在一個或多個其中包含有電腦可用程式碼的電腦可用存儲媒體（包括但不限於磁碟記憶體、CD-ROM、光學記憶體等）上實施的電腦程式產品的形式。

本案可以在由電腦執行的電腦可執行指令的一般上下文中描述，例如程式模組。一般地，程式模組包括執行特定任務或實現特定抽象資料類型的常式、程式、物件、元件、資料結構等等。也可以在分散式運算環境中實踐本案，在這些分散式運算環境中，由通過通信網路而被連接的遠端處理設備來執行任務。在分散式運算環境中，程式模組可以位於包括存放裝置在內的本地和遠端電腦存儲媒體中。

本說明書中的各個實施例均採用漸進的方式描述，各個實施例之間相同相似的部分互相參見即可，每個實施例重點說明的都是與其他實施例的不同之處。尤其，對於系統實施例而言，由於其基本相似於方法實施例，所以描述的比較簡單，相關之處參見方法實施例的部分說明即可。

以上所述僅為本案的實施例而已，並不用於限制本案。對於本領域技術人員來說，本案可以有各種更改和變

化。凡在本案的精神和原理之內所作的任何修改、等同替換、改進等，均應包含在本案的申請專利範圍之內。

【符號說明】

301：接收單元

302：第一獲取單元

303：第一確定單元

304：第二獲取單元

305：第二確定單元

306：判斷單元

401：接收單元

402：第一獲取單元

403：第一確定單元

404：第二獲取單元

405：第二確定單元

406：鑒權確定單元

申請專利範圍

1. 一種鑒權方法，其特徵在於，包括：

接收終端發送的攜帶使用者資訊及待鑒權的許可權點資訊的鑒權請求；

確定與所述使用者資訊相關聯的至少一個上層主體資訊；

根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；

根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；

將所述第一集合與所述第二集合的交集確定為鑒權集合；

判斷所述待鑒權的許可權點資訊是否在所述鑒權集合中；

若是，則判定鑒權通過。

2. 根據申請專利範圍第 1 項所述的方法，其中，根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合，包括：

若所述上層主體資訊包括至少兩個，則分別獲取與各個上層主體資訊對應的包括至少一個許可權點資訊的許可權集合；

將與各個上層主體資訊對應的許可權集合的交集確定為所述第二集合。

3. 根據申請專利範圍第 1 或 2 項所述的方法，其

中，若所述上層主體資訊包括租戶資訊、專案資訊，則，所述確定與所述使用者資訊相關聯的至少一個上層主體資訊，包括：

確定與所述使用者資訊相關聯的租戶資訊；

確定與所述使用者資訊相關聯的、且歸屬於所述租戶資訊下的專案資訊；

則，所述根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合，包括：

獲取與所述租戶資訊對應的包含至少一個許可權點資訊的許可權集合；

獲取與所述專案資訊對應的包含至少一個許可權點資訊的許可權集合；

將所述租戶資訊對應的許可權集合與所述專案資訊對應的許可權集合的交集確定為所述第二集合。

4. 根據申請專利範圍第 1 項所述的方法，其中，根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合，包括：

查詢與所述使用者資訊映射的第一角色資訊；其中，所述第一角色資訊用以標識所述使用者資訊對應的使用者在所述上層主體資訊對應的上層主體中的角色；

查詢與所述第一角色資訊映射的包含至少一個許可權點資訊的第一集合；

所述根據所述至少一個上層主體資訊，獲取與上層主

體信息對應的包含至少一個許可權點資訊的第二集合，包括：

查詢與至少一個所述上層主體資訊映射的至少一個第二角色資訊；其中，所述第二角色資訊用以標識各上層主體資訊對應的該上層主體在應用系統中的角色；

查詢與至少一個所述第二角色資訊映射的包含至少一個許可權點資訊的第二集合。

5. 一種鑒權方法，其特徵在於，包括：

接收終端發送的攜帶使用者資訊及待鑒權資訊集合的鑒權請求；其中，所述待鑒權資訊集合包含至少一個待鑒權的許可權點資訊；

確定與所述使用者資訊相關聯的至少一個上層主體資訊；

根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；

根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；

將所述第一集合與所述第二集合的交集確定為鑒權集合；

判斷所述待鑒權資訊集合與所述鑒權集合是否有交集；

若是，將所述待鑒權資訊集合與所述鑒權集合的交集確定為與當前的鑒權請求對應的鑒權通過的許可權點資訊的集合。

6. 根據申請專利範圍第 5 項所述的方法，其中，根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合，包括：

若所述上層主體資訊包括至少兩個，則分別獲取與各個上層主體資訊對應的包括至少一個許可權點資訊的許可權集合；

將與各個上層主體資訊對應的許可權集合的交集確定為所述第二集合。

7. 根據申請專利範圍第 5 或 6 項所述的方法，其中，若所述上層主體資訊包括租戶資訊、專案資訊，則，所述確定與所述使用者資訊相關聯的至少一個上層主體資訊，包括：

確定與所述使用者資訊相關聯的租戶資訊；

確定與所述使用者資訊相關聯的、且歸屬於所述租戶資訊下的專案資訊；

則，所述根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合，包括：

獲取與所述租戶資訊對應的包含至少一個許可權點資訊的許可權集合；

獲取與所述專案資訊對應的包含至少一個許可權點資訊的許可權集合；

將所述租戶資訊對應的許可權集合與所述專案資訊對應的許可權集合的交集確定為所述第二集合。

8. 根據申請專利範圍第 5 項所述的方法，其中，所述根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合，包括：

查詢與所述使用者資訊映射的第一角色資訊；其中，所述第一角色資訊用以標識所述使用者資訊對應的使用者在所述上層主體資訊對應的上層主體中的角色；

查詢與所述第一角色資訊映射的包含至少一個許可權點資訊的第一集合；

所述根據所述至少一個上層主體資訊，獲取與上層主體信息對應的包含至少一個許可權點資訊的第二集合，包括：

查詢與至少一個所述上層主體資訊映射的至少一個第二角色資訊；其中，所述第二角色資訊用以標識該上層主體資訊對應的上層主體在應用系統中的角色；

查詢與至少一個所述第二角色資訊映射的包含至少一個許可權點資訊的第二集合。

9. 一種鑒權裝置，其特徵在於，包括：

接收單元，用於接收終端發送的攜帶使用者資訊及待鑒權的許可權點資訊的鑒權請求；

第一確定單元，用於確定與所述使用者資訊相關聯的至少一個上層主體資訊；

第一獲取單元，用於根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集合；

第二獲取單元，用於根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；

第二確定單元，用於將所述第一集合與所述第二集合的交集確定為鑒權集合；

判斷單元，用於判斷所述待鑒權的許可權點資訊是否在所述鑒權集合中，若是，則判定鑒權通過。

10. 根據申請專利範圍第 9 項所述的裝置，其中，所述第二獲取單元具體用於：

若所述上層主體資訊包括至少兩個，則分別獲取與各個上層主體資訊對應的包括至少一個許可權點資訊的許可權集合；

將與各個上層主體資訊對應的許可權集合的交集確定為所述第二集合。

11. 根據申請專利範圍第 9 或 10 項所述的裝置，其中，若所述上層主體資訊包括租戶資訊、專案資訊，則，所述第一確定單元具體用於：

確定與所述使用者資訊相關聯的租戶資訊；

確定與所述使用者資訊相關聯的、且歸屬於所述租戶資訊下的專案資訊；

則，所述第二獲取單元具體用於：

獲取與所述租戶資訊對應的包含至少一個許可權點資訊的許可權集合；

獲取與所述專案資訊對應的包含至少一個許可權點資

訊的許可權集合；

將所述租戶資訊對應的許可權集合與所述專案資訊對應的許可權集合的交集確定為所述第二集合。

12. 根據申請專利範圍第 9 項所述的裝置，其中，所述第一獲取單元具體用於：

查詢與所述使用者資訊映射的第一角色資訊；其中，所述第一角色資訊用以標識所述使用者資訊對應的使用者在所述上層主體資訊對應的上層主體中的角色；

查詢與所述第一角色資訊映射的包含至少一個許可權點資訊的第一集合；

所述第二獲取單元具體用於：

查詢與至少一個所述上層主體資訊映射的至少一個第二角色資訊；其中，所述第二角色資訊用以標識該上層主體資訊對應的上層主體在應用系統中的角色；

查詢與至少一個所述第二角色資訊映射的包含至少一個許可權點資訊的第二集合。

13. 一種鑒權裝置，其特徵在於，包括：

接收單元，用於接收終端發送的攜帶使用者資訊及待鑒權資訊集合的鑒權請求；其中，所述待鑒權資訊集合包含至少一個待鑒權的許可權點資訊；

第一確定單元，用於確定與所述使用者資訊相關聯的至少一個上層主體資訊；

第一獲取單元，用於根據所述使用者資訊，獲取與該使用者資訊對應的包含至少一個許可權點資訊的第一集

合；

第二獲取單元，用於根據所述至少一個上層主體資訊，獲取與該上層主體信息對應的包含至少一個許可權點資訊的第二集合；

第二確定單元，用於將所述第一集合與所述第二集合的交集確定為鑒權集合；

鑒權確定單元，用於判斷所述待鑒權資訊集合與所述鑒權集合是否有交集；若是，將所述待鑒權資訊集合與所述鑒權集合的交集確定為與當前的鑒權請求對應的鑒權通過的許可權點資訊的集合。

14. 根據申請專利範圍第 13 項所述的裝置，其中，所述第二獲取單元具體用於：

若所述上層主體資訊包括至少兩個，則分別獲取與各個上層主體資訊對應的包括至少一個許可權點資訊的許可權集合；

將與各個上層主體資訊對應的許可權集合的交集確定為所述第二集合。

15. 根據申請專利範圍第 13 或 14 項所述的裝置，其中，若所述上層主體資訊包括租戶資訊、專案資訊，則，所述第一確定單元具體用於：

確定與所述使用者資訊相關聯的租戶資訊；

確定與所述使用者資訊相關聯的、且歸屬於所述租戶資訊下的專案資訊；

則，所述第二獲取單元具體用於：

獲取與所述租戶資訊對應的包含至少一個許可權點資訊的許可權集合；

獲取與所述專案資訊對應的包含至少一個許可權點資訊的許可權集合；

將所述租戶資訊對應的許可權集合與所述專案資訊對應的許可權集合的交集確定為所述第二集合。

16. 根據申請專利範圍第 13 項所述的裝置，其中，所述第一獲取單元具體用於：

查詢與所述使用者資訊映射的第一角色資訊；其中，所述第一角色資訊用以標識所述使用者資訊對應的使用者在所述上層主體資訊對應的上層主體中的角色；

查詢與所述第一角色資訊映射的包含至少一個許可權點資訊的第一集合；

所述第二獲取單元具體用於：

查詢與至少一個所述上層主體資訊映射的至少一個第二角色資訊；其中，所述第二角色資訊用以標識該上層主體資訊對應的上層主體在應用系統中的角色；

查詢與至少一個所述第二角色資訊映射的包含至少一個許可權點資訊的第二集合。

圖式

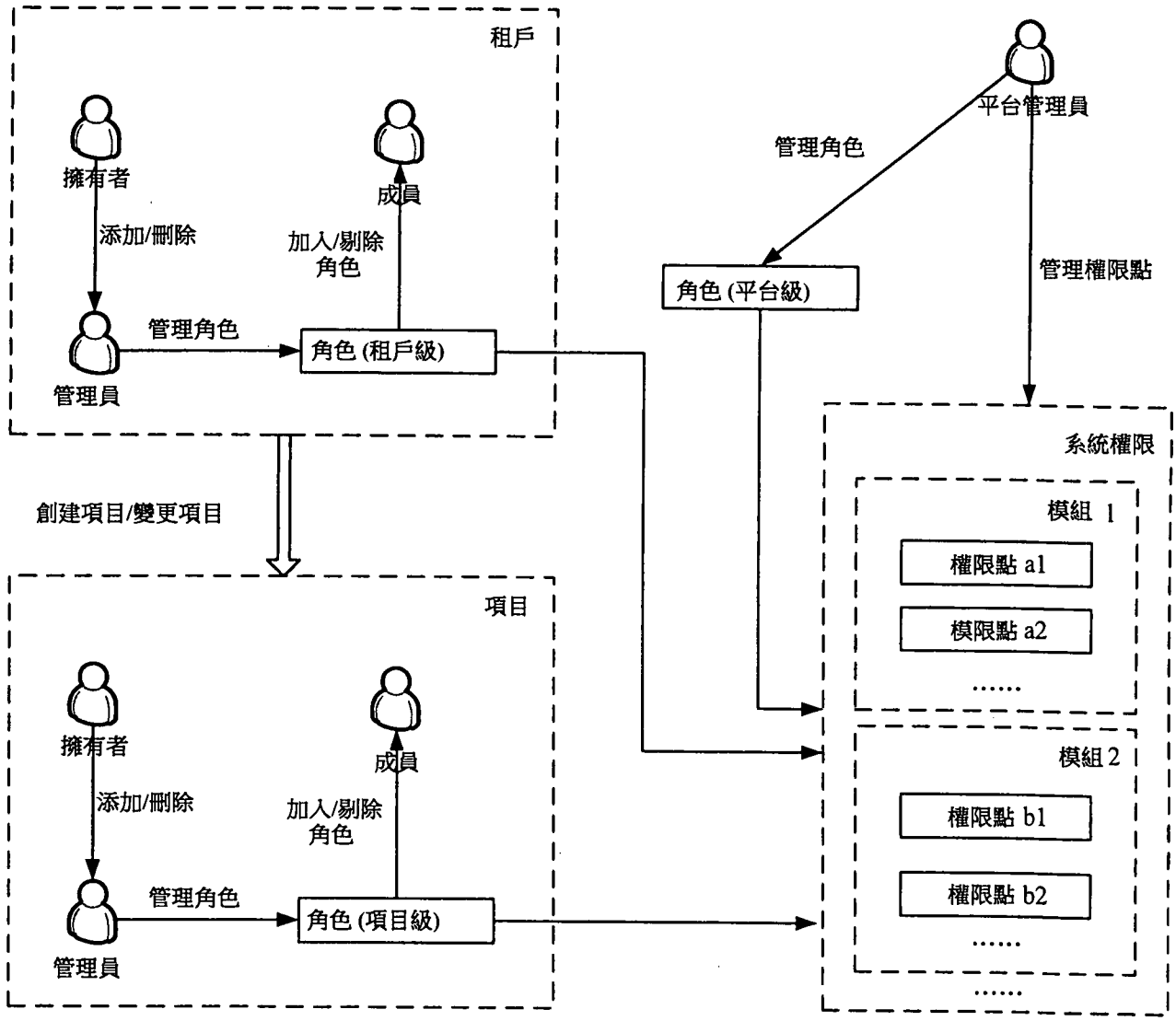
租戶
擁有者
添加/刪除
管理角色
管理員
成員
加入/剔除
角色
角色 (租戶級)
創建項目/變更項目
項目
擁有者
添加/刪除
管理角色
管理員
成員
加入/剔除
角色
角色 (項目級)
平台管理員
管理角色
角色 (平台級)
管理權限點
系統權限
模組 1
權限點 a1
模限點 a2
.....
模組 2
權限點 b1
權限點 b2
.....
.....

圖 1

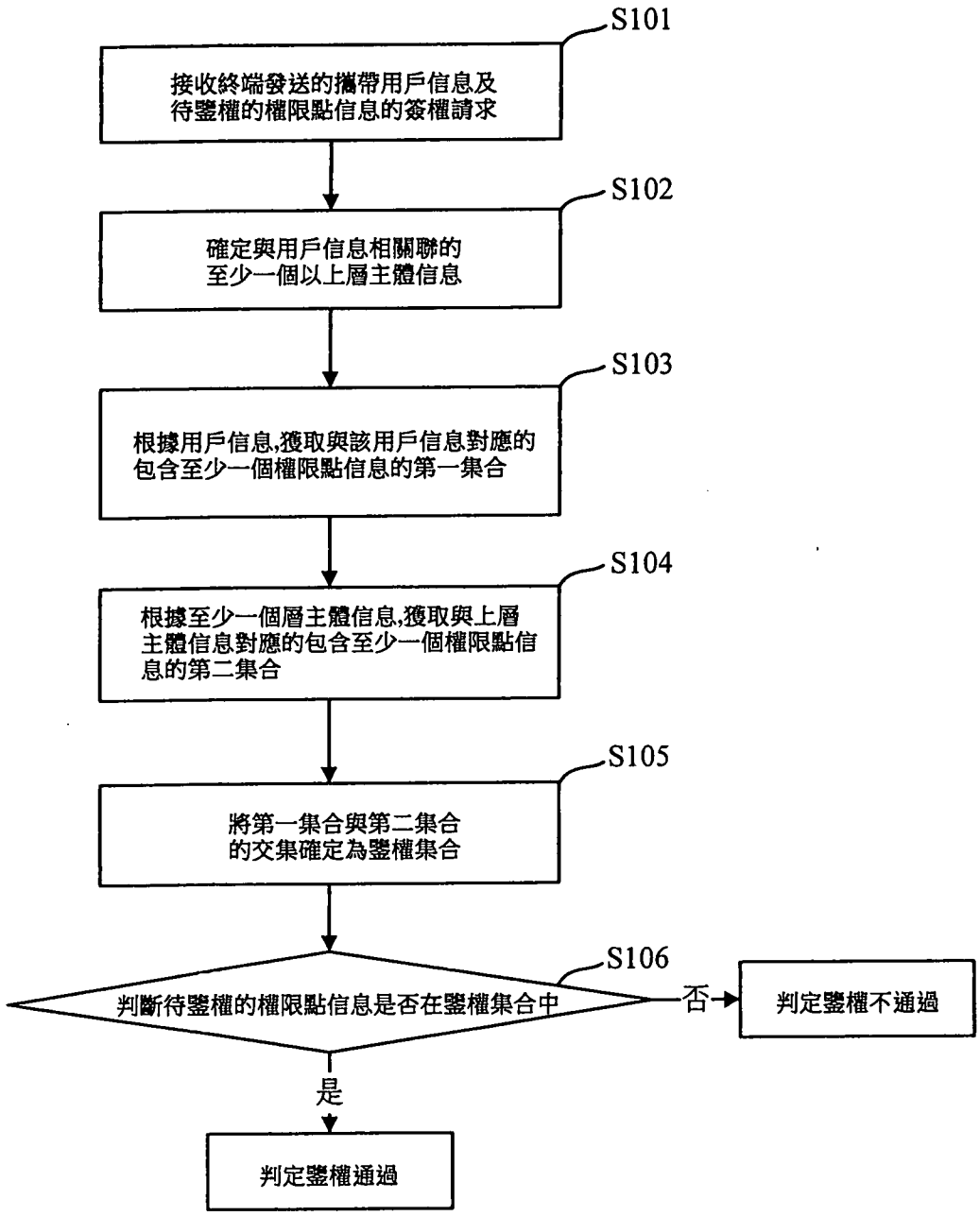
S101
接收終端發送的攜帶用戶信息及待鑒權的權限點信息的簽權請求
S102
確定與用戶信息相關聯的至少一個以上層主體信息
S103
根據用戶信息,獲取與該用戶信息對應的包含至少一個權限點信息的第一集合
S104
根據至少一個層主體信息,獲取與上層主體信息對應的包含至少一個權限點信息的第二集合
S105
將第一集合與第二集合的交集確定為鑒權集合
S106
判斷待鑒權的權限點信息是否在鑒權集合中
否
判定鑒權不通過
是
判定鑒權通過

圖 2

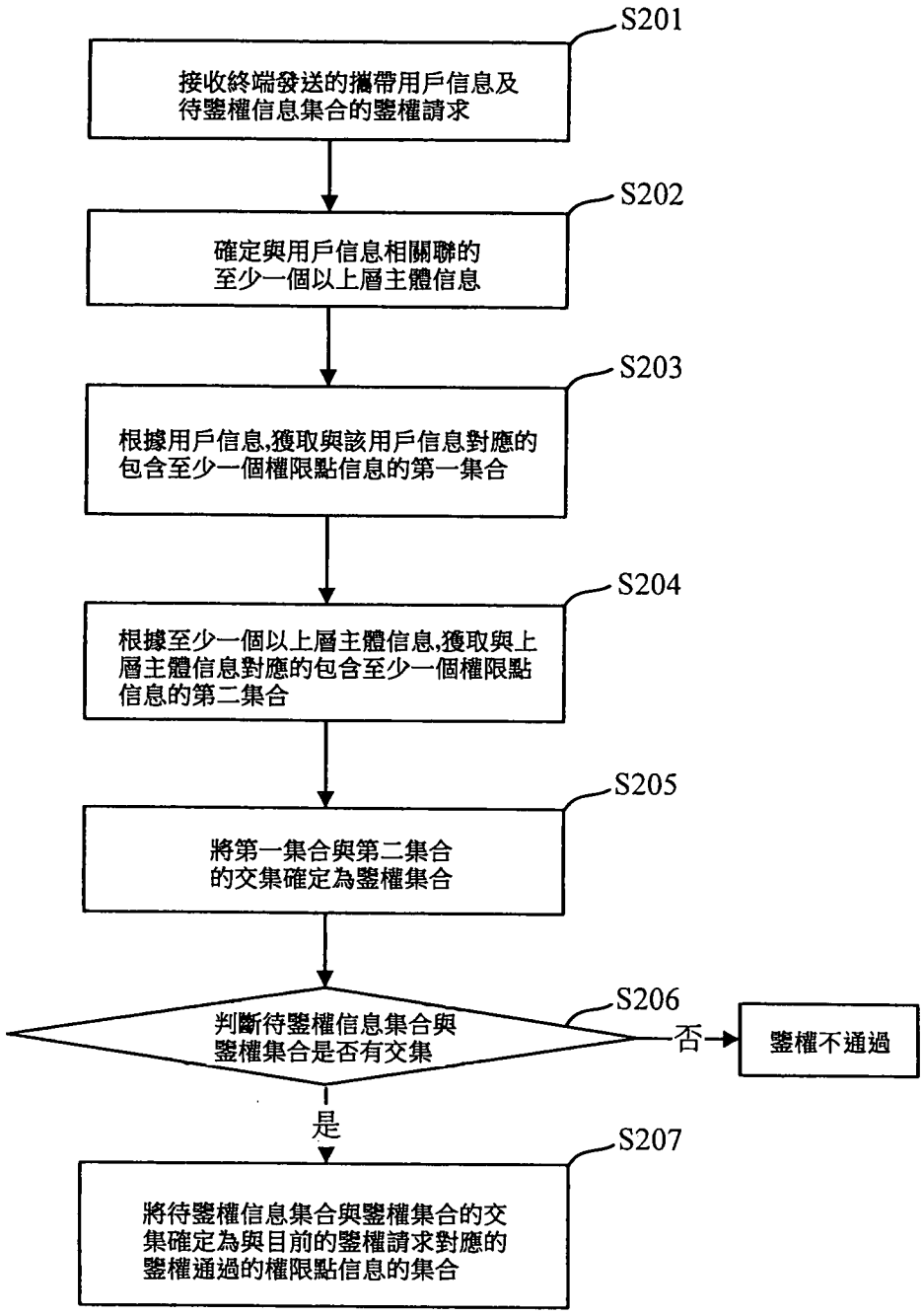
S201
接收終端發送的攜帶用戶信息及待鑒權信息集合的鑒權請求
S202
確定與用戶信息相關聯的至少一個以上層主體信息
S203
根據用戶信息,獲取與該用戶信息對應的包含至少一個權限點信息的第一集合
S204
根據至少一個以上層主體信息,獲取與上層主體信息對應的包含至少一個權限點信息的第二集合
S205
將第一集合與第二集合的交集確定為鑒權集合
S206
判斷待鑒權信息集合與鑒權集合是否有交集
否
鑒權不通過
是
S207
將待鑒權信息集合與鑒權集合的交集確定為與目前的鑒權請求對應的鑒權通過的權限點信息的集合

圖 3

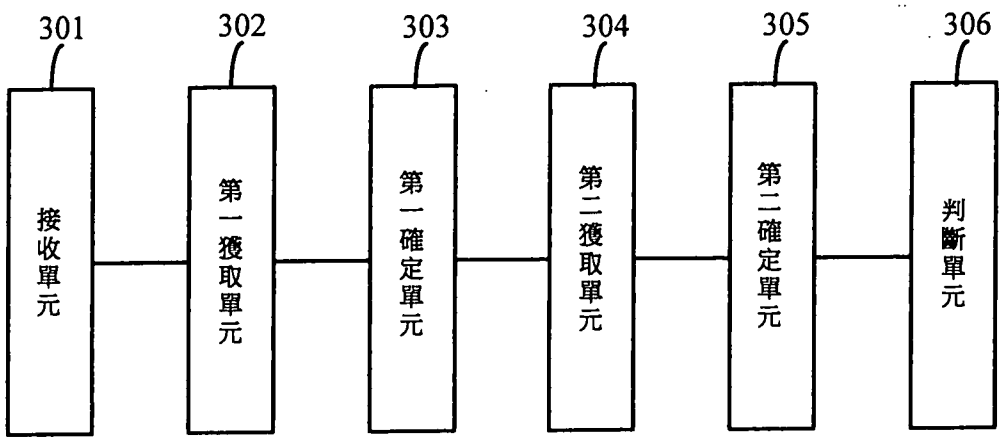
301
302
303
304
305
306
接收單元
第一獲取單元
第一確定單元
第二獲取單元
第二確定單元
判斷單元

圖 4

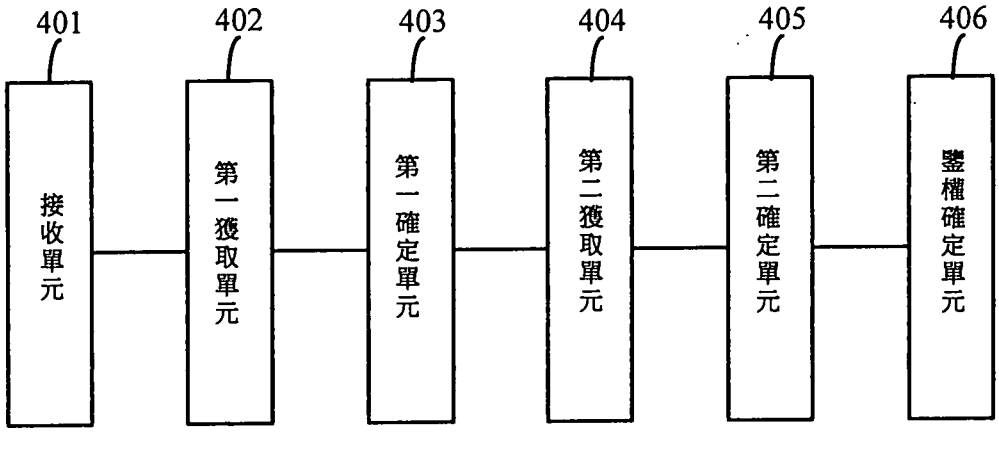
401
402
403
404
405
406
接收單元
第一獲取單元
第一確定單元
第二獲取單元
第二確定單元
鑒權確定單元

圖 5