M563003

(19)中華民國智慧財產局

(12)新型說明書公告本 **(11)證書號數：TW M563003 U**

(45)公告日： 中華民國 107 (2018) 年 07 月 01 日

(21)申請案號：107201165 (22)申請日： 中華民國 107 (2018) 年 01 月 24 日

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

(71)申請人：南山人壽保險股份有限公司(中華民國) NAN SHAN LIFE INSURANCE CO., LTD. (TW)

臺北市信義區莊敬路 168 號

(72)新型創作人：林振宇 LIN, CHEN YU (TW)

(74)代理人：何愛文；王仁君

申請專利範圍項數：10 項 圖式數：4 共 15 頁

(54)名稱

內部網路之多重驗證授權系統

(57)摘要

本創作關於一種用於一內部網路之多重驗證授權系統，其包括：至少一個客戶端裝置，其包含至少一個裝置識別碼；一身份資料庫，其包含該內部網路之一或多個使用者的帳戶資料；一網路交換器，其係與至少一個客戶端裝置連接；一第一驗證伺服器，其係與該網路交換器連接；以及一第二驗證伺服器，其分別與該第一驗證伺服器和該身份資料庫連接。

指定代表圖：

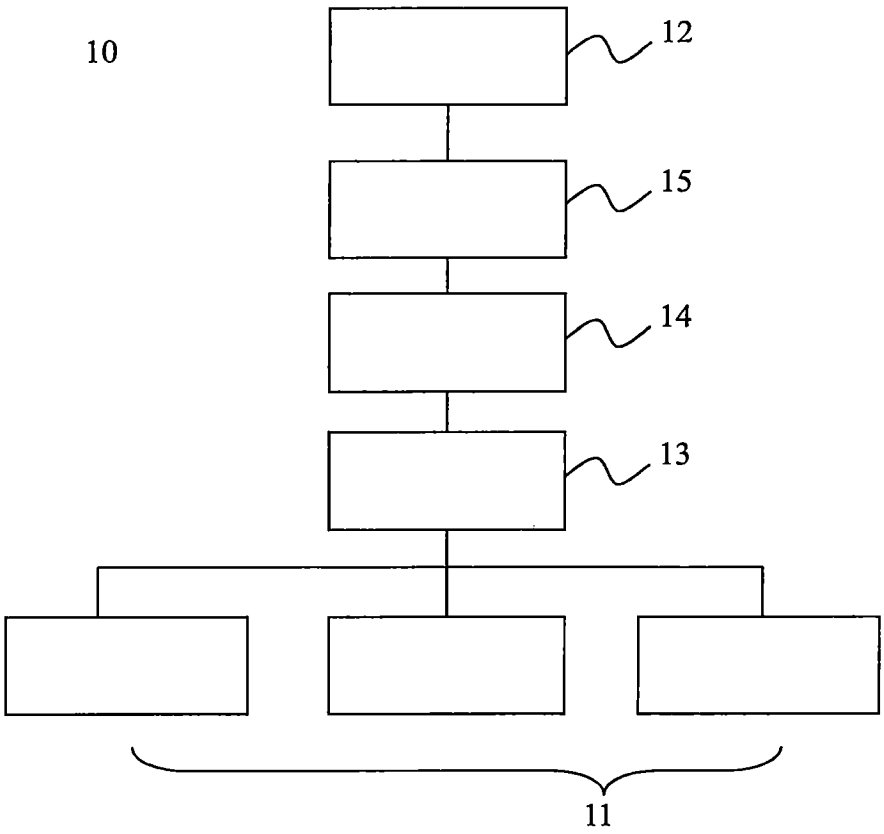

圖 1

符號簡單說明：

10・・・多重驗證授權系統

11・・・客戶端裝置

12・・・身份資料庫

13・・・網路交換器

14・・・第一驗證伺服器

15・・・第二驗證伺服器

新型專利說明書

（本說明書格式、順序，請勿任意更動）

【新型名稱】（中文/英文）

內部網路之多重驗證授權系統

【技術領域】

本創作關於一種網路存取的授權系統，除了驗証使用者登入電腦的帳號外，特別還加入裝置的驗証及授權，限制通過驗證之裝置有使用內部網路的權限。

【先前技術】

以往，電腦裝置在接上企業內網路的交換器之後，即可使用企業內部網路，並不會要求電腦裝置之使用者提供身份資訊，因此增加了企業內部網路被駭客入侵的風險。

因此，企業為了提高企業的資安防護強度，企業會利用電腦裝置之使用者的身份資訊（例如帳號及密碼）來管控企業內部網路之使用權限。然而，僅利用使用者的身份資訊（例如帳號及密碼）來管控權限，仍會有外來或未符規定被授權使用(不合規)的電腦或裝置得與進入企業的內部網路，使得企業內部網路的安全仍存在著不少的資安風險。

因此，為提高企業資安防護強度，除了識別使用者的身份資訊外，如何提供一種避免外來或不合規的電腦進入企業內部網路的系統，來提升其安全性，乃是目前資訊安全產業所欲積極尋求的目標。

【新型內容】

為了達成上述目標，本創作人乃積極苦思研究，以期可解決上述企業內部網路之資安風險的相關問題，經過不斷的努力及研究，終於研發出本創作。

本創作提出一實施例，一種用於一內部網路之多重驗證授權系統，其包括：至少一個客戶端裝置，其包含至少一個裝置識別碼；一身份資料庫，其包含該內部網路之一或多個使用者的帳戶資料；一網路交換器，其係與該至少一個客戶端裝置連接；一第一驗證伺服器，其係與該網路交換器連接，並驗證該至少一個裝置識別碼是否已被認

證；以及一第二驗證伺服器，其分別與該第一驗證伺服器和該身份資料庫連接，其中該網路交換器與各裝置之連接係基於至少一種網際網路協定(Internet Protocol；IP)、傳輸控制通訊協定(Transmission Control Protocol；TCP)及用戶資料通訊協定(User Datagram Protocol；UDP)等協定進行資料傳輸或連接。

依據本創作之另一實施例，該至少一個客戶端裝置中已被認證為可使用該內部網路，該第一驗證伺服器儲存或能讀取其所包含該至少一個裝置識別碼，而該至少一個裝置識別碼包含MAC位址(Media Access Control Address)。

依據本創作之另一實施例，該至少一個客戶端裝置可為個人電腦、筆記型電腦、平板電腦、行動裝置或智慧型穿戴裝置其中之一者。

依據本創作之另一實施例，該至少一個客戶端裝置為僅提供語音封包之網路電話裝置時，該網路交換器直接提供該網路電話裝置於該內部網路之使用。

依據本創作之另一實施例，該多重驗證授權系統更包含一第三驗證伺服器，該第三驗證伺服器分別與該第二驗證伺服器和該身份資料庫連接，且利用該一或多個使用者之至少一個生物特徵進行辨識，其中該至少一個生物特徵為語音、臉部、指紋、手掌紋、虹膜及視網膜之一或多者。

依據本創作之另一實施例，該一或多個使用者將該至少一個客戶端裝置(例如個人電腦、筆記型電腦、平板電腦、行動裝置或智慧型穿戴裝置其中之一者)以網路連接至該多重驗證授權系統後，該多重驗證授權系統進行下述步驟：步驟S101，要求該至少一個客戶端裝置提供該至少一個裝置識別碼及該一或多個使用者的帳戶資料至該網路交換器；步驟S102，該網路交換器提交該至少一個裝置識別碼及該一或多個使用者的帳戶資料至該第一驗證伺服器；步驟S103，該第一驗證伺服器驗證該至少一個裝置識別碼是否為合規，產生一第一驗證結果，並將該一或多個使用者的帳戶資料提交至該第二驗證伺服器；步驟S104，該第二驗證伺服器向該身份資料庫獲取及驗證該一或多個使用者的帳戶資料是否正確，產生一第二驗證結果，並將該第二驗證結

果回覆該第一驗證伺服器；步驟S105，該第一驗證伺服器將該第一驗證結果及該第二驗證結果回覆至該網路交換器；以及步驟S106，該網路交換器依據該第一驗證結果及該第二驗證結果配置存取一控制列表，以提供該至少一個客戶端裝置是否可使用該內部網路之一訊息。

依據本創作之另一實施例，該一或多個使用者將該至少一個客戶端裝置（例如網路監視器、列表機、影印機或掃描器其中之一者）網路連接至該多重驗證授權系統後，該多重驗證授權系統進行下述步驟：步驟S201，要求該至少一個客戶端裝置提供該至少一個裝置識別碼至該網路交換器；步驟S202，該網路交換器提交該至少一個裝置識別碼至該第一驗證伺服器；步驟S203，該第一驗證伺服器驗證該至少一個裝置識別碼是否為合規，產生一第三驗證結果，並將該第三驗證結果回覆該網路交換器；以及步驟S204，該網路交換器依據該第三驗證結果配置存取一控制列表，以提供該至少一個客戶端裝置是否可使用該內部網路之一訊息。

相較於習知技術，本創作之多重驗證授權系統可藉由客戶端裝置、裝置識別碼、身份資料庫、網路交換器及一或多個驗證伺服器彼此協同運作，可在驗證使用者的身份資訊之外，進一步藉由驗證客戶端裝置來提供客戶端裝置是否可使用企業內部網路，藉此避免外來或不合規的裝置進入企業內部網路，以提升企業的資訊安全。

【圖式簡單說明】

圖1係顯示本創作一種多重驗證授權系統的概略結構方塊圖。

圖2係顯示本創作另一實施例之多重驗證授權系統的概略結構方塊圖。

圖3係顯示本創作使用方式之實施範例流程圖。

圖4係顯示本創作使用方式之另一實施範例流程圖。

【實施方式】

參看所附之圖式，就本創作之具體形態來加以說明。

如圖1所示，本創作係一種用於內部網路的多重驗證授權系統10，多重驗證授權系統10包含至少一個客戶端裝置11（例如個人電腦、筆記型電腦、平板電腦、行動裝置、智慧型穿戴裝置、網路監視器、

列表機、影印機或掃描器），且至少一個客戶端裝置11具有至少一個裝置識別碼，其中至少一個裝置識別碼係為MAC位址（Media Access Control Address）；一身份資料庫12儲存有一或多個使用者的帳戶資料，各個使用者被個別授權使用內部網路，其中各使用者的使用權限可相同或不相同；一網路交換器13係與至少一個客戶端裝置11連接，其可基於至少一種網際網路協定（Internet Protocol；IP）、傳輸控制通訊協定（Transmission Control Protocol；TCP）及用戶資料通訊協定（User Datagram Protocol；UDP）等協定與至少一個客戶端裝置11進行資料傳輸或連接至網際網路；一第一驗證伺服器14係與網路交換器13連接，第一驗證伺服器14用於驗證至少一個裝置識別碼是否已被多重驗證授權系統10所認證；以及一第二驗證伺服器15分別與第一驗證伺服器14和身份資料庫12連接。

另外，至少一個客戶端裝置11中包含有已被認證或被授權可使用內部網路之合規裝置，第一驗證伺服器14能儲存及/或讀取合規裝置所包含的裝置識別碼（例如MAC位址）。

另外，至少一個客戶端裝置11為僅提供語音封包之網路電話裝置時，網路交換器13直接提供網路電話裝置於內部網路使用。

另外，如圖2所示，多重驗證授權系統10更包含一第三驗證伺服器16，第三驗證伺服器16分別與第二驗證伺服器15和身份資料庫12連接，第三驗證伺服器16係利用一或多個使用者之至少一個生物特徵進行辨識及驗證使用者，其中生物特徵包含有語音、臉部、指紋、手掌紋、虹膜及視網膜之一或多者。

參看圖3所示，以下便針對本創作使用時之使用方式的實施範例流程來加以說明。

進行流程前，身份資料庫12已儲存了一或多個使用者的帳戶資料，各使用者被個別授權使用內部網路，其中各使用者的使用權限可相同或不相同。各使用者將至少一個客戶端裝置以網路連接至多重驗證授權系統10後，該多重驗證授權系統10首先進行步驟S101，要求至少一個客戶端裝置11提供至少一個裝置識別碼（例如MAC位址）及一或多個使用者的帳戶資料至網路交換器13；接著進行步驟S102，使網

路交換器13提交至少一個裝置識別碼及一或多個使用者的帳戶資料至第一驗證伺服器14；接著進行步驟S103，使第一驗證伺服器14驗證至少一個裝置識別碼是否為合規，並產生一第一驗證結果，並將一或多個使用者的帳戶資料提交至第二驗證伺服器15；再進行步驟S104，使第二驗證伺服器15向身份資料庫12獲取及驗證一或多個使用者的帳戶資料是否正確，並產生一第二驗證結果，並將第二驗證結果回覆第一驗證伺服器14；之後則進行步驟S105，使第一驗證伺服器14將第一驗證結果及第二驗證結果回覆至網路交換器13；再進行步驟S106，使網路交換器13依據第一驗證結果及第二驗證結果配置存取一控制列表，用於提供至少一個客戶端裝置11是否可使用內部網路之一訊息。

另外，上述客戶端裝置11可為個人電腦、筆記型電腦、平板電腦、行動裝置或智慧型穿戴裝置其中之一者，其用於連接至內部網路。

參看圖4所示，以下便針對本創作使用時之使用方式的另一實施範例流程來加以說明。

進行流程前，身份資料庫12同樣已儲存了一或多個使用者的帳戶資料，各使用者被個別授權使用內部網路，其中各使用者的使用權限可相同或不相同。各使用者將至少一個客戶端裝置11以網路連接至多重驗證授權系統10後，多重驗證授權系統10首先進行步驟S201，要求至少一個客戶端裝置11提供至少一個裝置識別碼至網路交換器13；接著進行步驟S202，使網路交換器13提交至少一個裝置識別碼至第一驗證伺服器14；接著進行步驟S203，使第一驗證伺服器14驗證至少一個裝置識別碼是否為合規，產生一第三驗證結果，並將第三驗證結果回覆網路交換器13；再進行步驟S204，使網路交換器13依據第三驗證結果配置存取一控制列表，用以提供至少一個客戶端裝置11是否可使用內部網路之一訊息。

另外，上述客戶端裝置11可為網路監視器、列表機、影印機或掃描器其中之一者。

以上所述僅為本創作的較佳具體實施例，其並不用以限制本創作，凡在本創作的精神和原則之內，所作的任何修改、等同拆換、改進等，均應包含在本創作的保護範圍之內。

【符號說明】

10　多重驗證授權系統

11　客戶端裝置

12　身份資料庫

13　網路交換器

14　第一驗證伺服器

15　第二驗證伺服器

16　第三驗證伺服器

S101-S106 步驟

S201-S204 步驟

公告本

新型摘要

【新型名稱】(中文/英文)

內部網路之多重驗證授權系統

【中文】

本創作關於一種用於一內部網路之多重驗證授權系統，其包括：至少一個客戶端裝置，其包含至少一個裝置識別碼；一身份資料庫，其包含該內部網路之一或多個使用者的帳戶資料；一網路交換器，其係與至少一個客戶端裝置連接；一第一驗證伺服器，其係與該網路交換器連接；以及一第二驗證伺服器，其分別與該第一驗證伺服器和該身份資料庫連接。

【英文】

無

申請專利範圍

1. 一種用於一內部網路之多重驗證授權系統，其包括：
至少一個客戶端裝置，其包含至少一個裝置識別碼；
一身份資料庫，其包含該內部網路之一或多個使用者的帳戶資料；
一網路交換器，其係與該至少一個客戶端裝置連接；
一第一驗證伺服器，其係與該網路交換器連接，並驗證該至少一個裝置識別碼是否已被認證；以及
一第二驗證伺服器，其分別與該第一驗證伺服器和該身份資料庫連接。

2. 如申請範圍第 1 項之多重驗證授權系統，其中該至少一個客戶端裝置中已被認證為可使用該內部網路，該第一驗證伺服器儲存或能讀取其所包含該至少一個裝置識別碼。

3. 如申請範圍第 2 項之多重驗證授權系統，其中該至少一個裝置識別碼包含 MAC 位址（Media Access Control Address）。

4. 如申請範圍第 1 項之多重驗證授權系統，其中更包含一第三驗證伺服器，該第三驗證伺服器分別與該第二驗證伺服器和該身份資料庫連接，且利用該一或多個使用者之至少一個生物特徵進行辨識。

5. 如申請範圍第 4 項之多重驗證授權系統，其中該至少一個生物特徵為語音、臉部、指紋、手掌紋、虹膜及視網膜之一或多者。

6. 如申請專利範圍第 1 至 3 項之其中一項之多重驗證授權系統，其中該一或多個使用者將該至少一個客戶端裝置以網路連接至該多重驗證授權系統後，該多重驗證授權系統進行下述步驟：
步驟 S101，要求該至少一個客戶端裝置提供該至少一個裝置識別

碼及該一或多個使用者的帳戶資料至該網路交換器；

步驟 S102，該網路交換器提交該至少一個裝置識別碼及該一或多個使用者的帳戶資料至該第一驗證伺服器；

步驟 S103，該第一驗證伺服器驗證該至少一個裝置識別碼是否為合規，產生一第一驗證結果，並將該一或多個使用者的帳戶資料提交至該第二驗證伺服器；

步驟 S104，該第二驗證伺服器向該身份資料庫獲取及驗證該一或多個使用者的帳戶資料是否正確，產生一第二驗證結果，並將該第二驗證結果回覆該第一驗證伺服器；

步驟 S105，該第一驗證伺服器將該第一驗證結果及該第二驗證結果回覆至該網路交換器；以及

步驟 S106，該網路交換器依據該第一驗證結果及該第二驗證結果配置存取一控制列表，以提供該至少一個客戶端裝置是否可使用該內部網路之一訊息。

7. 如申請專利範圍第 6 項之多重驗證授權系統，其中該至少一個客戶端裝置可為個人電腦、筆記型電腦、平板電腦、行動裝置或智慧型穿戴裝置其中之一者。

8. 如申請專利範圍第 1 至 3 項之其中一項之多重驗證授權系統，其中該一或多個使用者將該至少一個客戶端裝置網路連接至該多重驗證授權系統後，該多重驗證授權系統進行下述步驟：

步驟 S201，要求該至少一個客戶端裝置提供該至少一個裝置識別碼至該網路交換器；

步驟 S202，該網路交換器提交該至少一個裝置識別碼至該第一驗證伺服器；

步驟 S203，該第一驗證伺服器驗證該至少一個裝置識別碼是否為合規，產生一第三驗證結果，並將該第三驗證結果回覆該網路交換器；以及

步驟 S204，該網路交換器依據該第三驗證結果配置存取一控制列

表，以提供該至少一個客戶端裝置是否可使用該內部網路之一訊息。

9. 如申請專利範圍第 8 項之多重驗證授權系統，其中該至少一個客戶端裝置可為網路監視器、列表機、影印機或掃描器其中之一者。

10. 如申請專利範圍第 1 至 3 項之其中一項之多重驗證授權系統，其中該至少一個客戶端裝置為僅提供語音封包之網路電話裝置時，該網路交換器直接提供該網路電話裝置於該內部網路之使用。

圖式

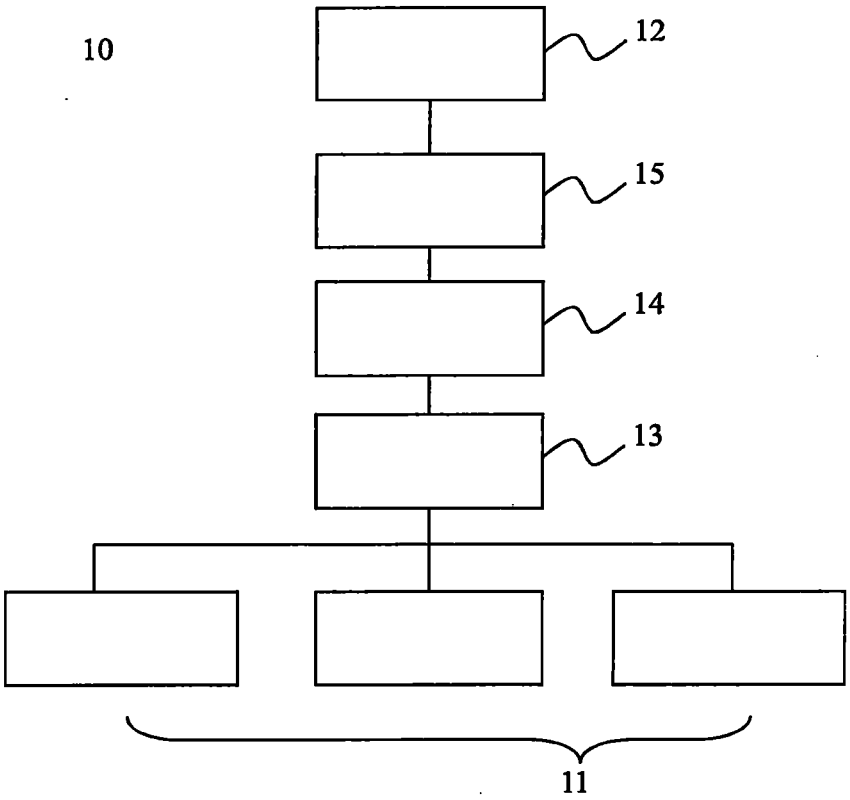

圖 1

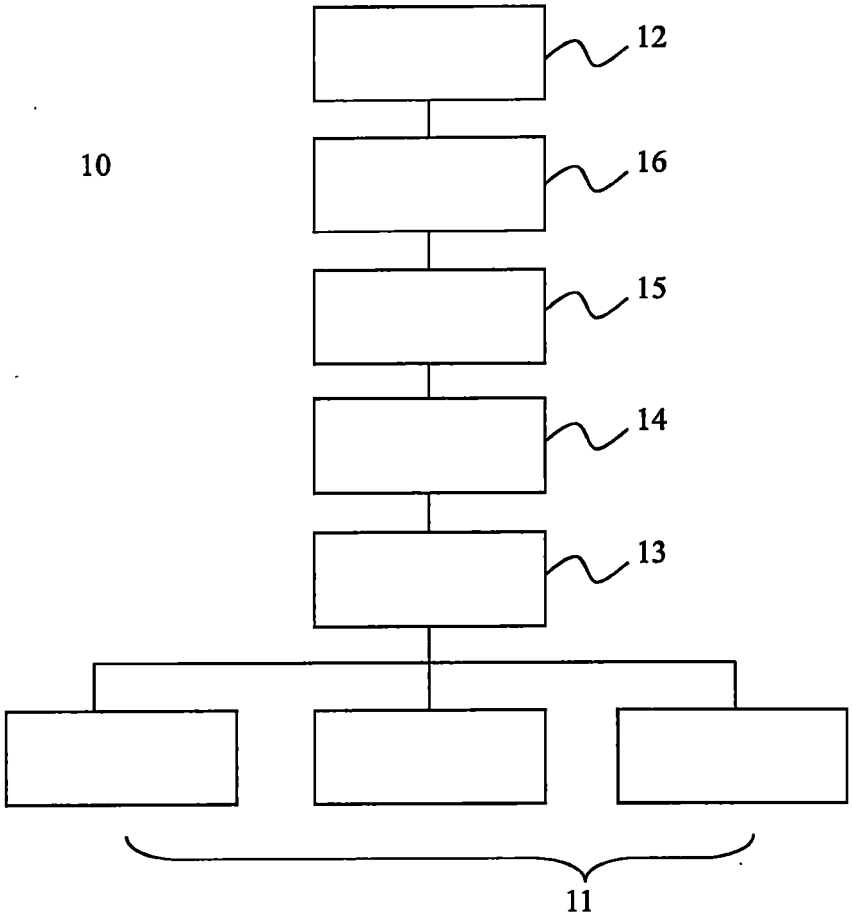

圖 2

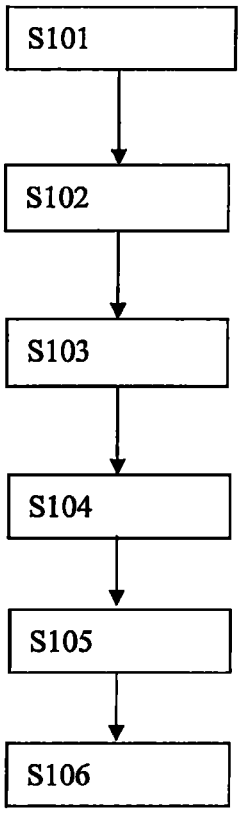

圖 3

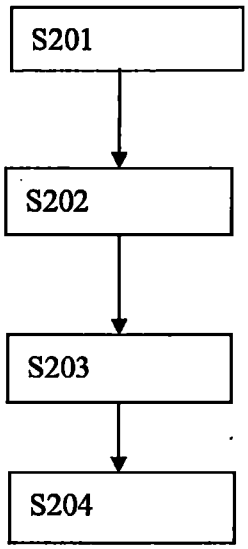

圖 4

【代表圖】

【本案指定代表圖】：圖1。

【本代表圖之符號簡單說明】：

10　多重驗證授權系統

11　客戶端裝置

12　身份資料庫

13　網路交換器

14　第一驗證伺服器

15　第二驗證伺服器