M665802

(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 M665802 U**

(45)公告日： 中華民國 114 (2025) 年 01 月 21 日

(21)申請案號：113210182 (22)申請日： 中華民國 113 (2024) 年 09 月 19 日

(51)Int. Cl.： ***G06F21/64 (2013.01)*** ***G06F21/62 (2013.01)***

G06Q50/00 (2024.01)

(71)申請人：國泰金融控股股份有限公司(中華民國) CATHAY FINANCIAL HOLDING CO., LTD. (TW)

臺北市大安區仁愛路 4 段 296 號

(72)新型創作人：江崑成 CHIANG, KUN-CHENG (TW)；廖銘宏 LIAO, MING-HUNG (TW)

(74)代理人：何美瑩

(NOTE)備註： 相同的創作已於同日申請發明專利(Another patent application for invention in respect of the same creation has been filed on the same date)

申請專利範圍項數：7 項 圖式數：9 共 33 頁

(54)名稱

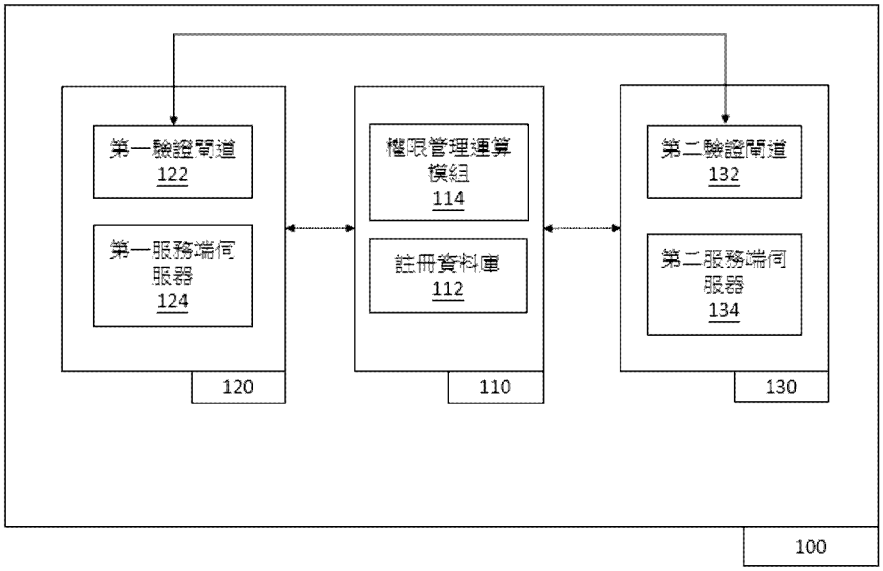
多站點驗證授權之資料交換系統

(57)摘要

本揭示內容是關於一種多站點驗證授權之資料交換系統及方法，所述系統包含一主伺服器和複數個服務裝置，其中各該服務裝置設有服務端伺服器及驗證閘道用以控制所述服務端伺服器之訪問。所述主伺服器設有一註冊資料庫，其儲存有各該服務裝置的索引資料，且該些索引資料同步於各個驗證閘道中。因此，本新型透過主伺服器與各該驗證閘道調控所建立的交換平台，能夠以任一服務裝置作為中介，再以轉導機制向目標服務裝置取得特定資料，並蒐集提供與用戶端，使得資料交換的驗證過程更佳便利。

Disclosed herein is a system and method for data exchange. The system includes a main server and multiple service devices, each of which is equipped with a service server and a gateway for authentication and authorization. The gateway is configured to control access to the service server. The main server is equipped with a registration database that stores index data for each service device, which is synchronized and stored in the gateways. Therefore, the present invention provides an exchange platform regulated by the main server and the gateways for authentication and authorization, enabling any service device to act as an intermediary to retrieve specific data from a target service device through a relay mechanism and then collect and provide the data to a user end, thereby making the authentication and authorization process for data exchange more convenient.

指定代表圖：



第 1 圖

符號簡單說明：

100:多站點驗證授權之資料交換系統

110:主伺服器

112:註冊資料庫

114:權限管理運算模組

120:第一服務裝置

122:第一驗證閘道

124:第一服務端伺服器

130:第二服務裝置

132:第二驗證閘道

134:第二服務端伺服器

M665802

【新型摘要】

【中文新型名稱】 多站點驗證授權之資料交換系統

【英文新型名稱】 SYSTEMS FOR MULTI-SITE AUTHENTICATION-AUTHORIZATION ANDDATA EXCHANGE

【中文】本揭示內容是關於一種多站點驗證授權之資料交換系統及方法，所述系統包含一主伺服器和複數個服務裝置，其中各該服務裝置設有服務端伺服器及驗證閘道用以控制所述服務端伺服器之訪問。所述主伺服器設有一註冊資料庫，其儲存有各該服務裝置的索引資料，且該些索引資料同步於各個驗證閘道中。因此，本新型透過主伺服器與各該驗證閘道調控所建立的交換平台，能夠以任一服務裝置作為中介，再以轉導機制向目標服務裝置取得特定資料，並蒐集提供與用戶端，使得資料交換的驗證過程更佳便利。

【英文】

Disclosed herein is a system and method for data exchange. The system includes a main server and multiple service devices, each of which is equipped with a service server and a gateway for authentication and authorization. The gateway is configured to control access to the service server. The main server is equipped with a registration database that stores index data for each service device, which is synchronized and stored in the gateways. Therefore, the present invention provides an exchange platform regulated by the main server and the gateways for authentication and authorization, enabling any service device to act as an intermediary to retrieve specific data from a target service device through a relay mechanism and then collect and provide the data

to a user end, thereby making the authentication and authorization process for data exchange more convenient.

【指定代表圖】　　第1圖

【代表圖之符號簡單說明】

100	多站點驗證授權之資料交換系統
110	主伺服器
112	註冊資料庫
114	權限管理運算模組
120	第一服務裝置
122	第一驗證閘道
124	第一服務端伺服器
130	第二服務裝置
132	第二驗證閘道
134	第二服務端伺服器

【新型說明書】

【中文新型名稱】　多站點驗證授權之資料交換系統

【英文新型名稱】　SYSTEMS FOR MULTI-SITE AUTHENTICATION-AUTHORIZATION AND DATA EXCHANGE

【技術領域】

【0001】　本揭示內容是關於資料交換的系統及方法，特別是一種透過驗證閘道的設置，完成資料傳輸過程達到單點接收及多點跳轉之系統及方法。

【先前技術】

【0002】　現今之數據資料交換缺乏統一的交換平台，各裝置/系統間往往採用不同的資料交換方法，且通常依賴個別裝置/系統之間的串接及複雜的驗證機制，然而串接機制各不相同，導致資料傳輸過程中產生許多不便，導致交換效率低下。

【0003】　此外，不同的串接機制在安全性方面也存在顯著差異。因無統一規格的情況下，部分裝置/系統可能具備較高的安全措施，如加密和身份驗證機制，但部分裝置/系統則可能相對簡單，這使得資料在傳輸過程中暴露於潛在的安全風險之中。裝置/系統間的安全性差異不僅增加了敏感資料洩漏的風險，也讓使用者對資料傳輸安全性產生疑慮。

【0004】　有鑑於此，為了先前技術所存在的缺陷導致資訊無法得到充分整合和有效利用，使得裝置/系統之間的資料交換過程變得冗長且低效。最終，這些問題給使用者帶來了極大的不便，減低了整體醫療服務的效率，並可能延誤了醫療決策的作出。因此，如何解決現有技術中的這些問題，提供一個統一且安全的資料交換平台，成為了現代醫療服務領域中的一個重要課題。

【0005】 有鑑於此，本領域亟需一種改良的多站點驗證授權之資料交換系統及方法，能夠達到整合及有效率地且安全地傳送系統/裝置間的資料。

【新型內容】

【0006】 新型內容旨在提供本揭示內容的簡化摘要，以使閱讀者對本揭示內容具備基本的理解。此新型內容並非本揭示內容的完整概述，且其用意並非在指出本新型實施例的重要/關鍵元件或界定本新型的範圍。

【0007】 為解決先前技術所存在的問題，本系統提出一種新穎的多站點驗證授權之資料交換系統及方法，能夠有效率地進行資料交換，提升資料交換的安全性及效率。

【0008】 本新型之一態樣是關於一種多站點驗證授權之資料交換系統，運作於分散式運算設備內，用以與一用戶端通訊連接。本新型之系統設有主伺服器、第一服務裝置、第二服務裝置彼此通訊連接，其中主伺服器包含一註冊資料庫，所述第一服務裝置和第二服務裝置分別包含有服務端伺服器（即，第一服務端伺服器和第二服務端伺服器）和驗證閘道（即，第一驗證閘道和第二驗證閘道）用以控制伺服器之訪問。本系統透過該些驗證閘道進行通訊連接及資料交換，且該些驗證閘道同步儲存有該些索引資訊。再者，該些驗證閘道經配置用以執行一驗證指令和一授權指令。在實際操作的過程中，所述第一服務端伺服器透過第一驗證閘道接收來自用戶端之服務請求，其中所述服務請求包含一服務資訊和一授權資訊，第一驗證閘道依據服務請求相對應之索引資訊透過該第二驗證閘道呼叫第二服務端伺服器，經第二驗證閘道驗證後，第一服務端伺服器向第二服務端伺服器取得相應所述服務資訊的至少一服務資料。

【0009】 依據本新型一實施方式，所述多站點驗證授權之資料交換系統更包含第三服務裝置與所述主伺服器通訊連接。所述第三服務裝置配置上包含一

第三服務端伺服器與一第三驗證閘道彼此通訊連接，其中所述第三服務端伺服器於主伺服器進行註冊，產生第三服務端伺服器之一索引資訊於註冊資料庫中，且所述第三驗證閘道，用以控制第三服務端伺服器之訪問，且同步儲存有該些索引資訊。在本實施方式實際操作的過程中，第一服務端伺服器透過該第一驗證閘道接收來自該用戶端之一服務請求，其中所述服務請求包含一服務資訊和一授權資訊，接著，第一驗證閘道依據該服務請求傳送一授權憑證和一資料索引至第三驗證閘道，以及第三驗證閘道依據授權憑證和資料索引，呼叫第一伺服器提供相應服務資訊的至少一服務資料至第三服務端伺服器。在可任選的實施方式中，所述至少一服務資料係由第一服務端伺服器和/或第二服務端伺服器所提供。此外，在本多站點驗證授權之資料交換系統中，所述用戶端亦可透過QR碼形式提供授權憑證和資料索引至第三驗證閘道。

【0010】　依據本新型一較佳的實施方式，本新型多站點驗證授權之資料交換系統中的主伺服器、第一服務裝置和二服務端裝置之間係以快捷式醫療照護互通操作資源(Fast Healthcare Interoperability Resources，FHIR)標準之複數筆FHIR規範資料進行交換。

【0011】　此外，在本新型一實施方式中，所述主伺服器更包含一權限管理運算模組，藉由執行以下步驟來對該些FHIR規範資料進行權限管理，包括：

(a) 分別取得來自第一服務裝置之一第一公鑰及一第一私鑰，以及來自第二服務裝置之一第二公鑰與一第二私鑰；

(b) 基於步驟(a)之第一私鑰及第二公鑰之組合，產生一密鑰；

(c) 以步驟(b)之密鑰加密FHIR規範資料，以產生一加密FHIR規範資料；

(d) 基於第一私鑰對步驟(c)加密FHIR規範資料進行簽章，以產生一簽章FHIR規範資料；

(e) 基於第一公鑰對步驟(d)簽章FHIR規範資料進行驗章，以解除簽章，恢復步驟(c)之加密FHIR規範資料；以及

(f) 基於步驟(a)之第二私鑰及該第一公鑰之組合產生步驟(b)之密鑰，以解密步驟(e)之加密FHIR規範資料，以取得解密後的FHIR規範資料。

【0012】 本新型另一態樣是關於一種利用上述任一實施方式所示之多站點驗證授權之資料交換系統所執行的方法，包含以下步驟：

(1-A) 第一服務端伺服器透過第一驗證閘道接收來自用戶端之服務請求，其中所述服務請求包含一服務資訊和一授權資訊；

(1-B) 第一驗證閘道依據服務請求向第一服務端伺服器取得相對應該服務資訊之一第一服務資料；以及

(1-C) 第一驗證閘道依據該服務請求透過第二驗證閘道向第二服務端伺服器取得相對應該服務資訊之一第二服務資料，並由第一驗證閘道將第一服務資料和第二服務資料提供至用戶端。

【0013】 依據本新型另一態樣，利用本新型之多站點驗證授權之資料交換系統所執行的方法，包含以下步驟：

(2-A) 第一服務裝置透過第一驗證閘道接收來自用戶端所提供的服務請求，其中該服務請求包含一服務資訊和一授權資訊；

(2-B) 第一驗證閘道依據服務請求傳送一授權憑證和一資料索引至該第三驗證閘道；以及

(2-C) 第三驗證閘道依據該授權憑證和該資料索引，呼叫該第一伺服器提供相應該服務資訊的至少一服務資料至該第三服務端伺服器，其中該至少一服務資料係由所述第一服務端伺服器和/或所述第二服務端伺服器所提供。

【0014】 在參閱下文實施方式後，本新型所屬技術領域中具有通常知識者當可輕易瞭解本新型之基本精神及其他新型目的，以及本新型所採用之技術手段與實施態樣。

【圖式簡單說明】

【0015】 為讓本新型的上述與其他目的、特徵、優點與實施方式能更明顯易懂，所附圖式之說明如下。

第1圖為依據本新型一實施方式所示之多站點驗證授權之資料交換系統100的示意圖；

第2圖為依據本新型一實施方式所示利用第1圖所示之多站點驗證授權之資料交換系統100所執行的方法流程圖；

第3圖為依據本新型另一實施方式所示之利用本新型多站點驗證授權之資料交換系統所執行的方法流程圖；

第4圖為依據本新型多站點驗證授權之資料交換系統200於醫療領域的配置示意圖；

第5圖為第4圖所示之多站點驗證授權之資料交換系統200於執行醫療資料交換的方法流程圖；

第6圖為依據本新型另一實施方式所示之多站點驗證授權之資料交換系統300於醫療領域的配置示意圖；

第7圖為第6圖所示之多站點驗證授權之資料交換系統300以電子處方籤執行領藥方法之流程圖；

第8圖為依據本新型另一實施方式所示之多站點驗證授權之資料交換系統400於醫療領域的配置示意圖；以及

第9圖為第8圖所示之多站點驗證授權之資料交換系統400執行領藥和運動療程之方法流程圖。

【0016】 根據慣常的作業方式，圖中各種特徵與元件並未依比例繪製，其繪製方式是為了以最佳的方式呈現與本新型相關的具體特徵與元件。此外，在不同圖式間，以相同或相似的元件符號來指稱相似的元件/部件。

【實施方式】

【0017】 為了使本揭示內容的敘述更加詳盡與完備，下文針對了本新型的實施態樣與具體實施例提出了說明性的描述；但這並非實施或運用本新型具體實施例的唯一形式。實施方式中涵蓋了多個具體實施例的特徵以及用以建構與操作這些具體實施例的方法步驟與其順序。然而，亦可利用其他具體實施例來達成相同或均等的功能與步驟順序。

【0018】 I. 定義

【0019】 為方便起見，本說明書、實施例及所附申請專利範圍中所使用的特定專有名詞集中在此。除非本說明書另有定義，此處所使用的科學與技術詞彙的含義與本新型所屬技術領域中具有通常知識者所理解與慣用的意義相同。並且，在和上下文不相衝突的情形下，本說明書所使用的單數名詞涵蓋該名詞的複數型，而所使用的複數名詞時亦涵蓋該名詞的單數型。具體而言，在本說明書與申請專利範圍中，單數形式「一」(a及an)包括複數參考值，但依據上下文而另有指示者除外。此外，在本說明書與申請專利範圍中，「至少一」(at least one)與「一或多」(one or more)表述方式的意義相同，兩者都代表包含了一、二、三或更多。

【0020】 所述「服務端」或「用戶端」包含任何能夠與至少一伺服器通訊連接訪問系統資源或服務的計算機裝置，其中所述通訊連接不限於有線或無線

網路連接。依據本新型一實施方式，所述「服務端」或「用戶端」包含至少一圖形顯示裝置(graphical display device)和圖形化使用者介面(graphical user interfaces)，讓使用者能夠透過圖形化使用者介面的應用程式、工具、服務或軟體查看訊息及互動。在本揭示內容中，對應服務端的使用者可以是任何人。再者，在可任選的實施方式中，所述「服務端」或「用戶端」可以是桌上型電腦、伺服器電腦、手持式或膝上型裝置、個人數位助理、多處理器系統、基於微處理器之系統、機上盒、可程式化消費性電子產品、行動裝置（特別是智慧型手機）、網路電腦、迷你電腦、主機電腦、包含任何上述系統或裝置之分散式運算環境及與其相似者。在一具體的實施方式中，所述「服務端」為伺服器電腦，而「用戶端」為行動裝置，其中使用者透過運行於行動裝置上的應用程式，與本系統通訊連接，運行在此所示之多站點驗證授權及資料交換之方法。

【0021】　在本揭示內容中，所述「系統」較佳係藉由複數個計算裝置所組成之分散式運算環境及與其相似者所運作，包含複數個通訊連接的伺服器，每個伺服器均配置特定的功能模組，用於實現系統的整體功能。本系統中的伺服器通過網絡協議（如HTTP、HTTP或TCP/IP等）進行資料交換，以協同完成資料處理、用戶請求響應、以及數據管理等任務，以執行本新型任一實施方式所示之多站點驗證授權、索引及交換之方法。

【0022】　當可理解，所述的「伺服器」通常具備至少某種形式的儲存媒體、通訊單元和處理單元。所述的儲存媒體包含依電性、及非依電性、可移除及不可移除媒體，可運用適當的方法或技術，使上述媒體能用於儲存所欲資訊（如：電腦可讀取指令、資料結構、應用程式模組、及其他資料）。儲存單元包含但不限於：RAM、ROM、EEPROM、快閃記憶體、或其他記憶體技術、CD-ROM、數位多功能影音光碟（DVD）、或其他光學

儲存器、磁匣、磁帶、磁碟片儲存器、以及其他磁性儲存裝置、或任何能夠用以儲存所需資訊且可供處理器存取之其他媒體。一般而言，通訊單元可將電腦可讀取指令、資料、結構、應用程式模組及其他資料具體實作成各種資料訊號，且可透過任何通訊媒體傳遞之。作為例示而非限制，通訊單元包含有線媒體（如有線網路或直接有線連線）及無線媒體（如音波、紅外線、無線電、微波、展頻技術、及其他無線媒體技術）。此外，通訊單元是採用通訊晶片進行實作，通訊晶片例如為支援乙太網路、光纖通訊網路、電信電纜網路、全球行動通信(Global System for Mobile communication, GSM)、個人手持式電話系統(Personal Handy-phone System, PHS)、碼多重擷取(Code Division Multiple Access, CDMA)系統、寬頻碼分多址(Wideband Code Division Multiple Access, WCDMA)系統、長期演進(Long Term Evolution, LTE)系統、全球互通微波存取(Worldwide interoperability for Microwave Access, WiMAX)系統、無線保真(Wireless Fidelity, Wi-Fi)系統、藍牙的信號傳輸的元件或或者其他支援電機電子工程師學會（Institute of Electrical and Electronics Engineers，IEEE）制定的標準通訊規格的晶片。處理單元與通訊單元和儲存單元通訊連接，用以運行商業險核保風險評估方法的必要運算與必要功能。在本揭露的一實施例中，處理單元例如為，採用中央處理單元(Central Processing Unit，CPU)，或是其他可程式化之一般用途或特殊用途的微處理器(Microprocessor)、數位信號處理器(Digital Signal Processor，DSP)、可程式化控制器、特殊應用積體電路(Application Specific Integrated Circuit，ASIC)或其他類似元件或上述元件的組合，本揭露不限於此。

【0023】　在其他實施方式中，所述的「系統」亦可藉由計算機裝置所運作，可以是伺服器電腦、桌上型電腦、手持式或膝上型裝置、個人數位助理、多處理器系統、基於微處理器之系統、機上盒、可程式化消費性電子

產品、行動電話（特別是智慧型手機）、網路電腦、迷你電腦、主機電腦、包含任何上述系統或裝置之分散式運算環境及與其相似者。

【0024】 在本揭示內容中，「快捷式醫療照護互通操作資源」(Fast Healthcare Interoperability Resources, FHIR）一詞係指由國際健康資訊交換第七層協定協會公佈的電子醫療資訊交換準則，用以改善不同醫療系統之間資料戶通及操作性。具體來說，FHIR針對醫療過程中包含臨床及非臨床資料（例如：電子病歷、臨床記錄、影像資料、處方、患者資訊）的結構進行標準化定義，亦即定義資料中的欄位、屬性以及兩者之間的關聯性，使每個欄位都有特定的資料類型和格式，確保不同系統間能夠按照一致的結構和標準來交換和共用醫療資訊，便於醫療機構之間或者是與保險機構之間的資料互通。

【0025】 本文所述的「權限管理」一詞是指一種組織和管理數據、系統或資源存取的程式，目的在於確保只有被授權的用戶或實體能夠訪問特定的資源、功能或數據。一般來說，「權限管理」包含使用者身分識別及驗證、授與權限、權限審核和監控、權限分級管理等。在本揭示內容例示性實施方式中，本新型醫療資料交換及理賠服務系統藉由加密傳輸以及設置傳輸簽章來對醫療資訊進行存取得權限管理。再者，所述權限管理運算模組是由處理器、記憶體與儲存媒體所實現。

【0026】 II. 具體實施方式

【0027】 為改善先前技術的缺陷，本新型所提出的多站點驗證授權之資料交換系統及方法，能夠以任一服務裝置，作為資料存取的匯集點，完成單點接收多點跳轉之目的，讓資料交換的過程更有效率。

【0028】 第1圖為依據本新型一實施方式所示之多站點驗證授權之資料交換系統100。本新型多站點驗證授權之資料交換系統100設有主伺服器110、第一服務裝置120、第二服務裝置130彼此通訊連接。本新型之主伺服器110包含一註

冊資料庫112及情況設有權限管理運算模組114，所述第一服務裝置120和第二服務裝置130分別包含有服務端伺服器（即，第一服務端伺服器124和第二服務端伺服器134）和驗證閘道（即，第一驗證閘道122和第二驗證閘道132）與該些伺服器通訊連接，用以控制該些伺服器之訪問。需要注意的是本新型的技術特徵在於服務裝置分別設有各自的驗證閘道，基於該些驗證閘道彼此及與主伺服器通訊連接，用以協助本多站點驗證授權之資料交換系統中的服務裝置透過驗證閘道進行授權、驗證和資料驗證等，以改善來自不同服務端資料傳輸間驗證的複雜性及不便性。

【0029】 本新型之多站點驗證授權之資料交換系統100中第一服務裝置120之第一服務端伺服器124和第二服務裝置130第二服務端伺服器134分別於主伺服器110進行註冊，產生相對於該些伺服器之索引資訊於註冊資料庫112中，且該些索引資訊同步儲存於驗證閘道中。在其他實施方式中，本新型多站點驗證授權之資料交換系統100中的服務裝置為複數個，且可視實際使用需求進行增減，多站點驗證授權之資料交換系統100中的服務裝置皆須經向主伺服器註冊後，將會即時同步更新索引資料，至各個服務裝置內的驗證閘道中。此外，本新型之服務裝置係由相同或不同的服務端所提供，用戶端可任意的訪問任一服務裝置，以執行本新型所揭示的資料方法。

【0030】 請同時參見第2圖，第2圖為依據本新型一實施方式所示利用第1圖所示之多站點驗證授權之資料交換系統100所執行的方法流程圖。在實際操作的過程中，所述第一服務裝置120之第一服務端伺服器124透過第一驗證閘道122接收來自用戶端之服務請求，其中所述服務請求包含一服務資訊和一授權資訊（步驟501）。本新型所屬技術領域中具有通常知識者應當可以理解，所述服務資訊和授權資訊可以根據實際使用目的選擇並執行相應的指令，其中所述服務資訊涵蓋服務項目及相對應的索引資訊，使得各該驗證閘道可透過該些資訊內

容呼叫對應系統中特定索引標的（如，第一服務端伺服器124或第二服務端伺服器134），透過授權資訊進行伺服器的訪問或使該伺服器提供相對應的服務資料。在本實施方式中，所述服務請求中的請求項目跨越兩個不同的裝置，分別為第一服務裝置120和第二服務裝置130，因此，依據服務請求使第一服務裝置120提供相應服務請求之第一服務資料（步驟S503），第一驗證閘道122依據該服務請求透過第二驗證閘道132向第二服務端伺服器134取得相對應服務請求之一第二服務資料（步驟S505），接著，再由第一服務裝置120將第一服務資料和第二服務資料提供至所述用戶端105（步驟S507）。由此可見，本新型所提供的方法系以用戶端所訪問之第一服務端伺服器124作為中介層，使第一服務端伺服器124過第一驗證閘道122、第二驗證閘道132與第二服務端伺服器134通訊連接，取得第二服務端伺服器134所提供的資料。以此類推，若所述服務請求對應複數個服務裝置，仍是以收到用戶端之服務請求之服務裝置作為中介層，由其透過驗證閘道向其他服務裝置通訊連接並取得相關資料後，再將蒐集到的所有資料傳送至用戶端，達成單點接收並進行多點跳轉之目的。

【0031】 第3圖為依據本新型另一實施方式所示之利用本新型多站點驗證授權之資料交換系統所執行的方法流程圖。在非限制的實施方式中，本新型的多站點驗證授權之資料交換系統可包括複數個服務裝置，任一服務裝置皆設有彼此通訊連接的驗證閘道和服務端伺服器。在本實施方式中，本新型除了原第1圖所揭露的系統配置外，更包含有第三服務裝置，其包含有一彼此通訊連接之第三驗證閘道和一第三服務端伺服器。所述第三服務裝置同樣先行於主伺服器註冊後，產生相對應的索引資訊並儲存於註冊資料庫112中，且該些索引資訊將同步更新並儲存於各該驗證閘道中（如，第一驗證閘道、第二驗證閘道和第三驗證閘道）。

【0032】 在本實施方式所執行的方法中，首先，第一服務裝置透過第一驗證閘道接收來該用戶端所提供的服務請求（步驟S601），所述服務請求包括服務資訊和授權資訊。接著，第一驗證閘道依據服務請求傳送一授權憑證和一資料索引至第三驗證閘道（步驟S603A）。在另一實施方式中，所述授權憑證和資料索引係由用戶端所提供至第三驗證閘道（步驟S603B），例如，透過QR碼或其他方式。第三驗證閘道依據授權憑證和資料索引，透過第一驗證閘道呼叫第一伺服器提供相應所述服務資訊的至少一服務資料至第三服務端伺服器（步驟S605）。

【0033】 第4圖為依據本新型多站點驗證授權之資料交換系統200於醫療領域的配置示意圖，圖中所示之各裝置通訊連接，且箭頭僅用於舉例說明各該裝置資料傳輸的方向性，本新型並不限於此。

【0034】 在此實施方式中，本新型的多站點驗證授權之資料交換系統200包含主伺服器210、醫院A服務裝置220（即，第一服務裝置）和醫院B服務裝置230（即，第二服務裝置），各該伺服器和服務裝置之配置原則上與第1圖所示之系統示意圖相同，故相同之處不另贅述。

【0035】 請同時參見第5圖，其為第4圖所示之多站點驗證授權之資料交換系統於執行醫療資料交換的方法流程圖。在本實施方式中，醫院A服務裝置220（即，第一服務裝置）透過第一驗證閘道接收來用戶端所提供的病歷調閱請求（步驟S701）。所述病歷調閱請求包含但不限於就醫資訊、就醫場所、就醫科別、就醫時間等以及授權資訊。在本實施方式中，所述病歷調閱請求欲調閱兩家醫院的就診記錄，故醫院A服務裝置220依據病歷調閱請求提供相應病歷調閱請求之第一就醫記錄（步驟S703），同時醫院A服務裝置220之第一驗證閘道依據病歷調閱請求透過第二驗證閘道使醫院B服務裝置230提供相應病歷調閱請求之第二就醫記錄至醫院A服務裝置220（步驟S705）。在此實施方式中，所述醫院A服務裝置220呼叫醫院B服務裝置230的過程中經第二驗證閘道驗證/認證程序後，使

醫院B服務裝置提供相應病歷調閱請求之第二就醫記錄至醫院A服務裝置220。接著由醫院A服務裝置220將第一就醫記錄和第二就醫記錄提供至用戶端205（步驟S707）。

【0036】 第6圖為依據本新型另一實施方式所示之多站點驗證授權之資料交換系統300於醫療領域的配置示意圖，圖中所示之各裝置通訊連接，且箭頭僅用於舉例說明各該裝置資料傳輸的方向性，本新型並不限於此。請同時參見第7圖，其為第6圖所示之多站點驗證授權之資料交換系統300以電子處方籤執行領藥方法之流程圖。在本實施方式中，除了主伺服器310外更包含有經註冊之醫院A服務裝置320、醫院B服務裝置340、醫院C服務裝置350和藥局A服務裝置330。在本實施方式中，各該服務裝置通訊連接，且依照實際使用目的各服務裝置分別透過驗證閘道進行資料驗證、認證和交換。第7圖所示之領藥方法係以主伺服器310、醫院A服務裝置320和藥局A服務裝置330所完成，其中所述醫院A服務裝置320作為第一服務裝置，藥局A服務裝置330作為第二服務裝置。

【0037】 首先，使用者透過用戶端305向醫院A服務裝置320傳送領藥請求，其包含領藥資訊和授權資訊，其中領藥資訊包含但不限於領藥藥局、領藥資訊或處方籤資訊等，且所述授權資訊用以領藥資訊授權至領藥藥局A。醫院A服務裝置320透過第一驗證閘道接收來用戶端所提供的領藥請求，其中領藥請求包含領藥資訊和授權資訊，基於此產生一授權憑證和資料索引，並傳送至藥局A服務裝置330之第二驗證閘道（步驟S803），接著藥局A服務裝置330透過第二驗證閘道依據授權憑證和資料索引，呼叫醫院A伺服器320提供相應所述領藥請求的處方籤資料至藥局A伺服器（步驟S805），最終，使用者至藥局A完成領藥作業（步驟S807），例如，可藉由使用者之健保卡透過藥局A服務裝置330之第二驗證閘道完成使用者驗證程序完成領藥作業。

【0038】 第8圖為依據本新型另一實施方式所示之多站點驗證授權之資料交換系統400於醫療領域的配置示意圖，圖中所示之各裝置通訊連接，且箭頭僅用於舉例說明各該裝置資料傳輸的方向性，本新型並不限於此。請同時參見第9圖，其為第8圖所示之多站點驗證授權之資料交換系統執行領藥和運動療程之方法流程圖。本新型多站點驗證授權之資料交換系統400除了主伺服器410外，可包含複數個由醫療機構或照護機構所提供之服務裝置，例如，主伺服器410、醫院A服務裝置420、醫院B服務裝置440、醫院C服務裝置450、藥局A服務裝置430和健身房A服務裝置460，所述服務裝置的數量可無限地擴充。

【0039】 第9圖所示之執行領藥和運動療程方法係以主伺服器410、醫院A服務裝置420、藥局A服務裝置430和健身房A服務裝置460所完成，為方便說明其中所述醫院A服務裝置420作為第一服務裝置，藥局A服務裝置430作為第二服務裝置和健身房A服務裝置460作為第三服務裝置。

【0040】 醫院A服務裝置420透過第一驗證閘道接收來用戶端所提供的服務請求，其中所述服務請求同時包含有二種服務項目資訊，分別為領藥請求和運動請求（步驟S901）。舉例而言，領藥請求包含領藥資訊和相應的授權資訊，以及運動請求包含運動療程資訊和相應的授權資訊。醫院A服務裝置420透過第一驗證閘道分別依據領藥請求和運動請求產生一第一授權憑證和第一資料索引至藥局A服務裝置430，以及第二授權憑證和第二資料索引至健身房A服務裝置460（步驟S903、S905），藥局A服務裝置430透過第二驗證閘道依據第一授權憑證和第一資料索引，呼叫醫院A服務裝置420提供相應領藥請求的處方籤資料（步驟S907），健身房A服務裝置460透過三驗證閘道依據第二授權憑證和第二資料索引，呼叫醫院A服務裝置420提供相應運動請求的處方籤資料，最終使用者分別至藥局A完成領藥作業和健身房A完成領藥作業及運動療程（步驟S911、S913）。

【0041】 根據本新型的較佳實施方式，所述多站點驗證授權之資料交換系統可基於FHIR規範進行統一格式的資料交換，作為系統的基礎架構，以確保本新型系統符合國際醫療資訊標準。根據需要，本新型之系統還可結合多對多的傳輸簽章加解密機制。此技術內容已於本案申請人先前於2023年09月19日提出之臺灣新型專利申請（申請號112135699）中揭露，其內容在此併入作為參考，並作為本說明書之一部份。

【0042】 在本新型多站點驗證授權之資料交換系統所傳輸的資料可能包含許多個人資訊及敏感的健康訊息，若在交換過程被攔截，可能會導致個人隱私曝露導致身份冒用，或是不法份子偽造病歷進行醫療詐欺等後果。據此，本新型之主伺服器110可設置權限管理運算模組114分別與其他服務端所提供之服務裝置通訊連接，用以管理傳輸資料/FHIR規範資料的存取權限，確保資料的安全性及正確性。

【0043】 所述權限管理運算模組114是用以執行以下步驟：

(a) 分別取得來自該第一服務裝置之一第一公鑰及一第一私鑰，以及來自該第二服務裝置之一第二公鑰與一第二私鑰；

(b) 基於步驟(a)之該第一私鑰及該第二公鑰之組合，產生一密鑰；

(c) 以步驟(b)之該密鑰加密該FHIR規範資料，以產生一加密FHIR規範資料；

(d) 基於該第一私鑰對步驟(c)該加密FHIR規範資料進行簽章，以產生一簽章FHIR規範資料；

(e) 基於該第一公鑰對步驟(d)該簽章FHIR規範資料進行驗章，以解除該簽章，恢復步驟(c)之該加密FHIR規範資料；以及

(f) 基於步驟(a)之該第二私鑰及該第一公鑰之組合產生步驟(b)之該密鑰，以解密步驟(e)之該加密FHIR規範資料，以取得解密後的該FHIR規範資料。

【0044】 具體來說，每個服務裝置（如，醫療機構或保險機構）分別具有一公鑰以及一私鑰，用以加密欲交換之檔案，其中公鑰是公開於資料交換平台或系統中流通，而私鑰則由各機構分別保管。在一較佳的實施方式中，當服務裝置於本多站點驗證授權之資料交換系統註冊時，會產生一組公鑰和私鑰，其中公鑰上傳至主伺服器，完成註冊作業。

【0045】 所述權限管理運算模組即是藉由結合傳送方及接收方的公鑰及/或私鑰進行加解密以及簽驗章，以確認資料來源的正確性，以及管理FHIR規範資料之存取權。在本新型之多站點驗證授權之資料交換系統中，各服務裝置係透過一公鑰向主伺服器進行註冊。

【0046】 以第5圖為例，本新型多站點驗證授權之資料交換系統之主伺服器先分別取得代表醫院A服務裝置的第一公鑰及第一私鑰，醫院B服務裝置的第二公鑰及第二私鑰，以進行後續加密步驟。接著，以醫院A服務裝置的第一私鑰及醫院B服務裝置的第二公鑰之組合，經過運算後產生一密鑰。在非限制性實施方式中，所述密鑰可以是矩陣、字串或其他形式的數據，具體格式和類型取決於所使用的加密演算法和應用場景。

【0047】 以上述步驟產生的密鑰對欲傳送的FHIR規範資料進行加密，加密過程使用特定的演算法和密鑰來對資料進行處理，產生加密FHIR規範資料，使得未經授權的人無法輕易解讀數據的內容，只有擁有相應私鑰的一方（亦即，具有第二私鑰的保險機構）才能進行解密，還原為可讀的原始內容。

【0048】 此外，為了確保是來自於特定服務裝置，在步驟S705中，醫院B服務裝置在傳送加密FHIR規範資料（如，第二就醫記錄）前進一步以第二私鑰進行簽章，以產生簽章FHIR規範資料，由於第二私鑰未於公開平台流通，因此醫院A服務裝置可藉由檢視接收到的資料是否包含第二私鑰產生的簽章，來確認該資料是否來自該醫院B。

【0049】 在步驟S705中，醫院A服務裝置利用以第二公鑰進行驗章，據以解除簽章，並獲得加密FHIR規範資料。若接收到的資料並非來自於醫院B之伺服器，則無法以第二公鑰解除該簽章，亦無法獲得加密FHIR規範資料。在醫院A服務裝置獲得加密FHIR規範資料後，醫院A進一步以其持有的第一私鑰與該醫院B的第二公鑰結合，產生與上述所產生之密鑰相同的密鑰來解密該加密FHIR規範資料，據以將加密內容還原為人類可讀之格式，取得所述FHIR規範資料。

【0050】 非必要的，本新型之多站點驗證授權之資料交換系統更包含在形成加密FHIR規範資料之後，及/或形成簽章FHIR規範資料後，將加密FHIR規範資料、簽章FHIR規範資料或其組合傳遞至一區塊鏈資料庫。依據本揭示內容某些較佳的實施方式，所述權限管理運算模組還用以執行以下步驟：在形成加密FHIR規範資料之後，及/或形成簽章FHIR規範資料後後，以特定的數學函數與加密FHIR規範資料進行運算，以得到一由特定長度的字元所組成的雜湊值，並將該雜湊值傳送至區塊鏈資料庫。在另一實施方式中，各該服務裝置之服務端伺服器更配置一資料校驗單元，與區塊鏈資料庫通訊連接，用以計算來自區塊鏈資料庫的加密FHIR規範資料，以得到一校驗雜湊值，並將校驗雜湊值與區塊鏈資料庫中的該雜湊值進行比對，若比對結果一致，表示接收到的加密FHIR規範資料與來源加密FHIR規範資料相同；若比對結果不一致，則表示接收到的加密FHIR規範資料與最初的加密FHIR規範資料不同，於交換過程中可能曾被竄改內容。綜上，藉由上述進行加解密及簽驗章的權限管理程序，可確保資料在傳遞的過程中，若被第三方截取也無法讀取原始資料的內容，亦可確認接收到的資料是來自指定的服務端。

【0051】 綜上所述，本新型之多站點驗證授權之資料交換系統透過驗證閘道的設置解決先前技術資料傳輸技術的困難，以單點驗證及多點轉倒機制，讓服務請求指向正確的目標服務裝置（如，醫療機構、藥局或保健機構等）。再者，

本新型之交換系統亦可應用在FHIR規範資料及搭配獨特的權限管理程序，能夠提升資料交換的安全性，並符合國際醫療資訊標準。

【0052】 應當理解的是，前述對實施方式的描述僅是以實施例的方式給出，且本領域所屬技術領域中具有通常知識者可進行各種修改。以上說明書、實施例及實驗結果提供本新型之例示性實施方式之結構與用途的完整描述。雖然上文實施方式中揭露了本新型的各種具體實施例，然其並非用以限定本新型，本新型所屬技術領域中具有通常知識者，在不悖離本新型之原理與精神的情形下，當可對其進行各種更動與修飾，因此本新型之保護範圍當以附隨申請專利範圍所界定者為準。

【符號說明】

【0053】 本新型主要元件符號列示如下：

100、200、300、400	多站點驗證授權之資料交換系統
105、205、305、405	用戶端
110、210、310、410	主伺服器
112	註冊資料庫
114	權限管理運算模組
120	第一服務裝置
122	第一驗證閘道
124	第一服務端伺服器
130	第二服務裝置
132	第二驗證閘道
134	第二服務端伺服器
220、320、420	醫院A服務裝置

230、340、440	醫院B服務裝置
330、430	藥局A服務裝置
350、450	醫院C服務裝置
460	健身房A服務裝置

【新型申請專利範圍】

【請求項1】 一種多站點驗證授權之資料交換系統，運作於一分散式運算設備內，用以與一用戶端通訊連接，包含：

一主伺服器，包含一註冊資料庫；

一第一服務裝置，與該主伺服器通訊連接，包含：

一第一服務端伺服器，於該主伺服器註冊，產生相對於該第一服務端伺服器之一索引資訊於該註冊資料庫中；

一第一驗證閘道，與該第一服務端伺服器通訊連接，用以控制該第一服務端伺服器之訪問；以及

一第二服務裝置，與該主伺服器通訊連接，包含：

一第二服務端伺服器，於該主伺服器註冊，產生相對於該第二服務端伺服器之一索引資訊於該註冊資料庫中；

一第二驗證閘道，與該第二服務端伺服器通訊連接，用以控制該第二服務端伺服器之訪問，且該第一驗證閘道和該第二驗證閘道彼此通訊連接，且同步儲存有該些索引資訊；

其中該第一服務端伺服器透過該第一驗證閘道接收來自該用戶端之一服務請求，其中該服務請求包含一服務資訊和一授權資訊，該第一驗證閘道依據該服務請求相對應之該索引資訊透過該第二驗證閘道呼叫該第二服務端伺服器，經該第二驗證閘道驗證後，該第一服務端伺服器向該第二服務端伺服器取得相應該服務資訊的至少一服務資料。

【請求項2】 如請求項 1 所述之多站點驗證授權之資料交換系統，其中該第一驗證閘道或該第二驗證閘道經配置用以執行一驗證指令和一授權指令。

【請求項3】 如請求項 1 所述之多站點驗證授權之資料交換系統，更包含：

一第三服務裝置，與該主伺服器通訊連接，包含：

一第三服務端伺服器，於該主伺服器進行註冊，產生相對於該第三服務端伺服器之一索引資訊於該註冊資料庫中；

一第三驗證閘道，與該第三服務端伺服器通訊連接，用以控制該第三服務端伺服器之訪問，且同步儲存有該些索引資訊；

其中該第一服務端伺服器透過該第一驗證閘道接收來自該用戶端之一服務請求，其中該服務請求包含一服務資訊和一授權資訊，該第一驗證閘道依據該服務請求傳送一授權憑證和一資料索引至該第三驗證閘道，以及該第三驗證閘道依據該授權憑證和該資料索引，呼叫該第一服務端伺服器提供相應該服務資訊的至少一服務資料至該第三服務端伺服器，其中該至少一服務資料係由該第一服務端伺服器和/或該第二服務端伺服器所提供。

【請求項4】 如請求項 3 所述之多站點驗證授權之資料交換系統，其中該服務資料係由該第一服務端伺服器和該第二服務端伺服器所提供。

【請求項5】 如請求項 3 所述之多站點驗證授權之資料交換系統，其中該用戶端係透過一 QR 碼形式提供該授權憑證和該資料索引至該第三驗證閘道。

【請求項6】 如請求項 1 所述之多站點驗證授權之資料交換系統，其中該主伺服器、該第一服務裝置和該二服務端裝置之間係以快捷式醫療照護互通操作資源(Fast Healthcare Interoperability Resources，FHIR)標準之複數筆 FHIR 規範資料進行交換。

【請求項7】 如請求項 6 所述之多站點驗證授權之資料交換系統，其中該主伺服器更包含一權限管理運算模組，藉由執行以下步驟來對該些 FHIR 規範資料進行權限管理，包括：

(a) 分 別取得來自該第一服務裝置之一第一公鑰及一第一私鑰，以及來自該第二服務裝置之一第二公鑰與一第二私鑰；

(b) 基於步驟(a)之該第一私鑰及該第二公鑰之組合，產生一密鑰；

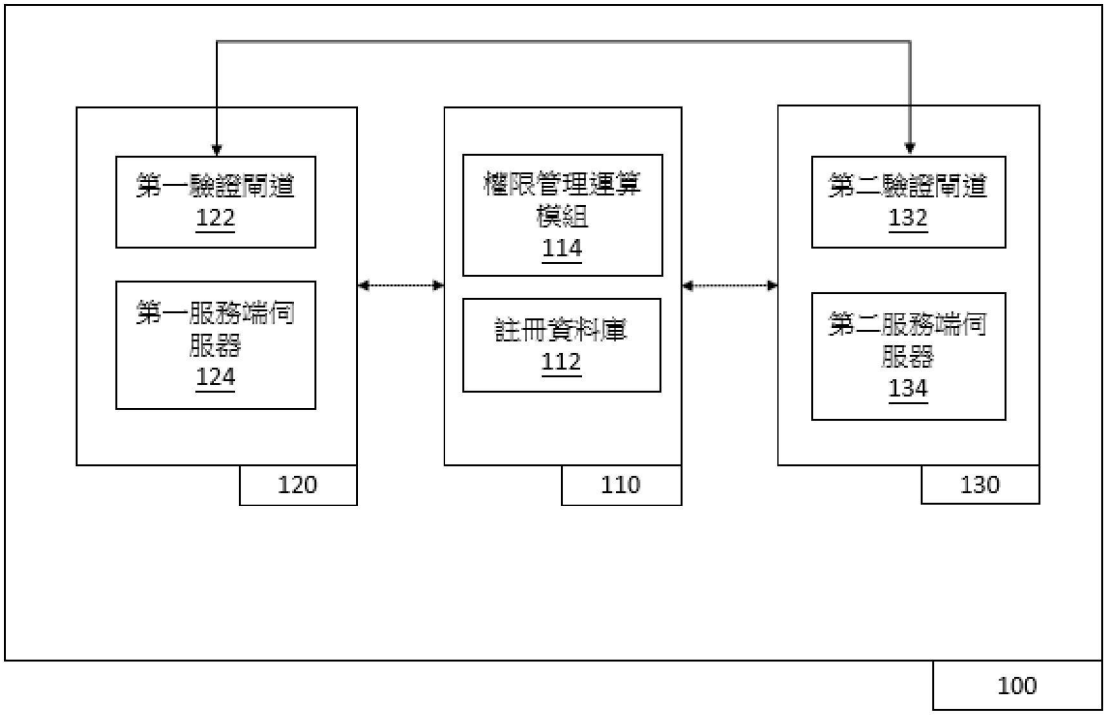
(c) 以步驟(b)之該密鑰加密該FHIR規範資料，以產生一加密FHIR規範資料；

(d) 基於該第一私鑰對步驟(c)該加密FHIR規範資料進行簽章，以產生一簽章FHIR規範資料；

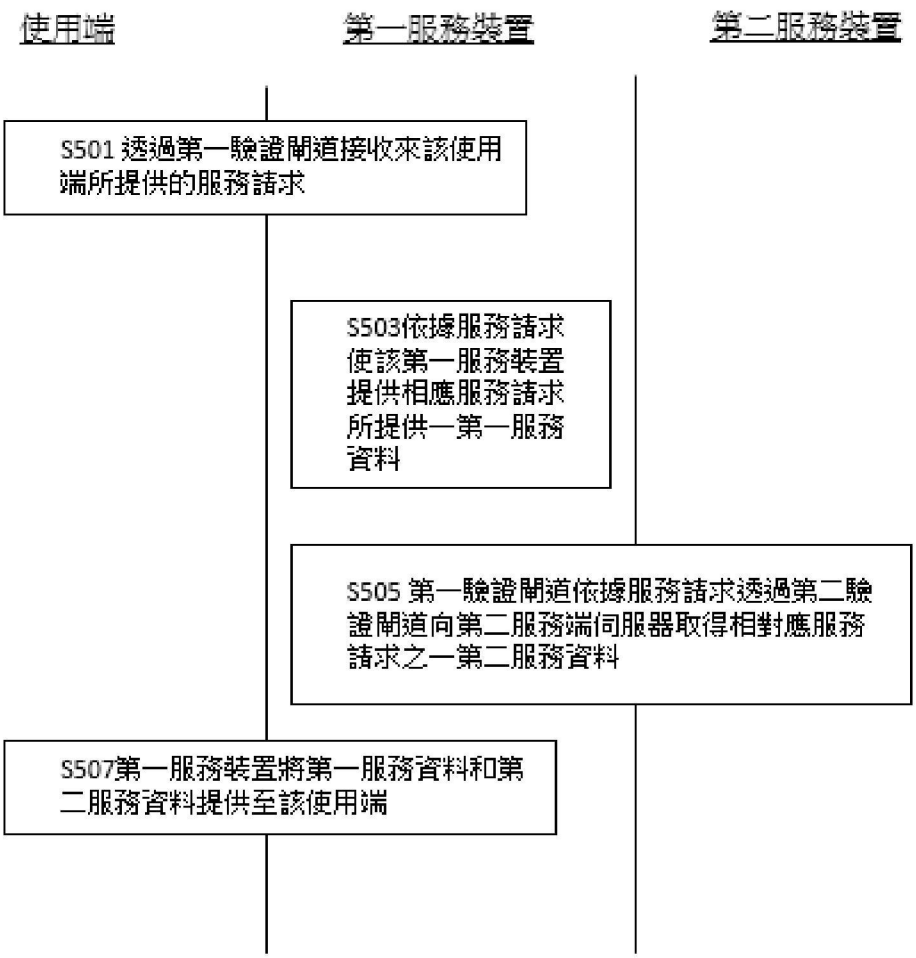
(e) 基於該第一公鑰對步驟(d)該簽章FHIR規範資料進行驗章，以解除該簽章，恢復步驟(c)之該加密FHIR規範資料；以及

(f) 基於步驟(a)之該第二私鑰及該第一公鑰之組合產生步驟(b)之該密鑰，以解密步驟(e)之該加密FHIR規範資料，以取得解密後的該FHIR規範資料。

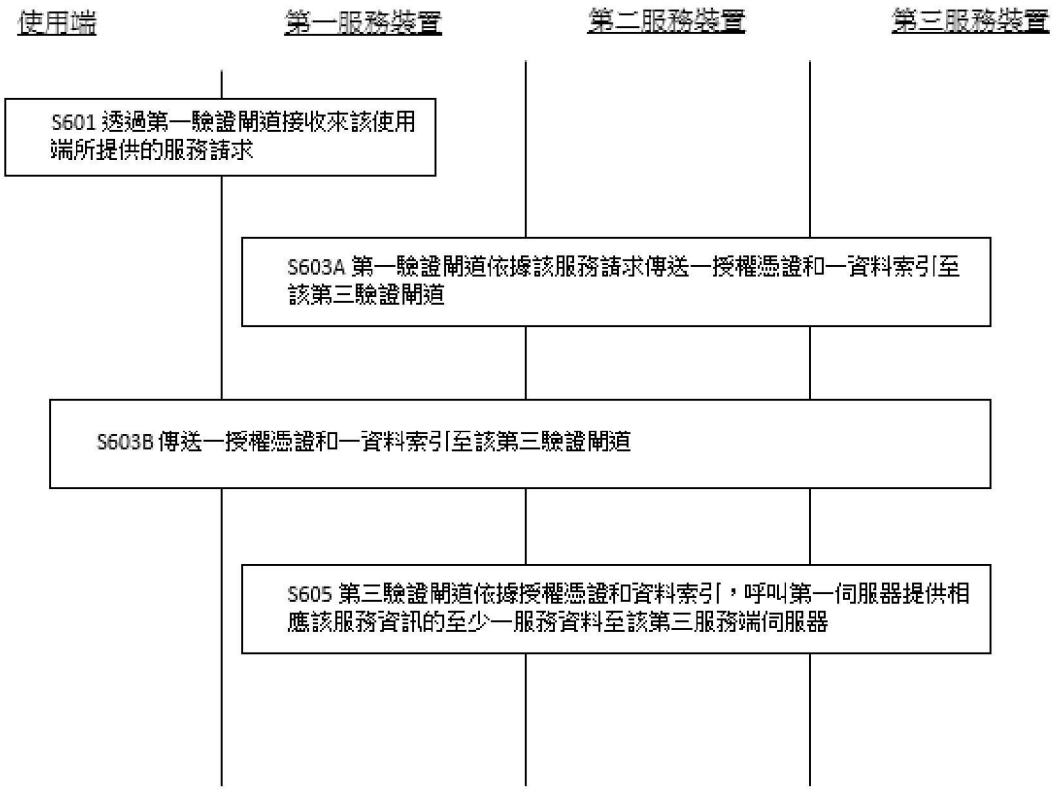
【新型圖式】


第一驗證閘道
122
第一服務端伺服器
124
120
權限管理運算模組
114
註冊資料庫
112
110
第二驗證閘道
132
第二服務端伺服器
134
130
100

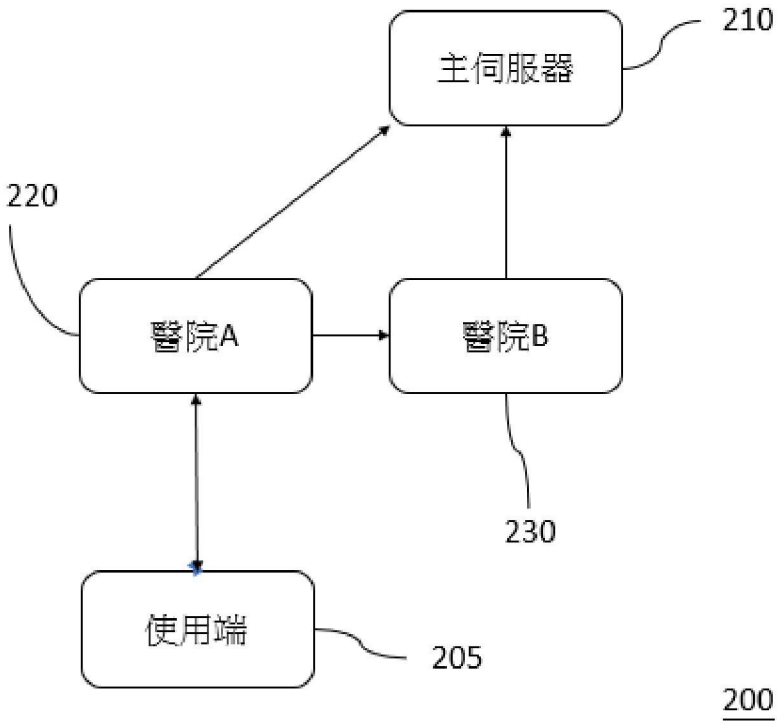
第 1 圖


使用端
第一服務裝置
第二服務裝置
S501 透過第一驗證閘道接收來該使用端所提供的服務請求
S503依據服務請求使該第一服務裝置提供相應服務請求所提供一第一服務資料
S505 第一驗證閘道依據服務請求透過第二驗證閘道向第二服務端伺服器取得相對應服務請求之一第二服務資料
S507第一服務裝置將第一服務資料和第二服務資料提供至該使用端

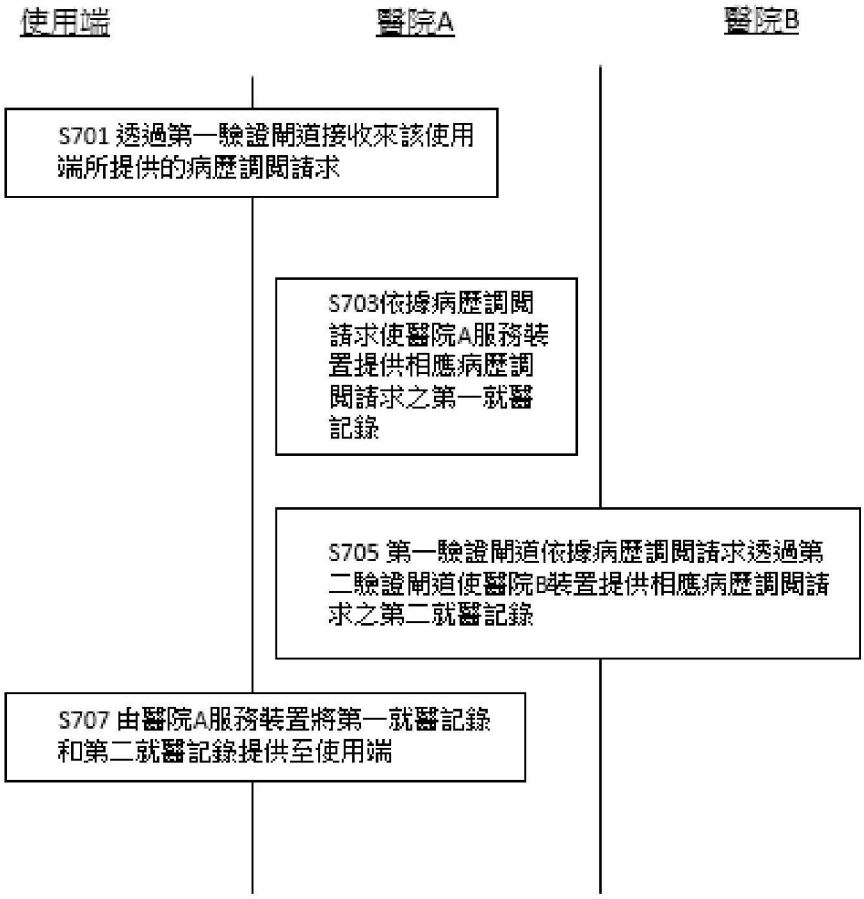
第 2 圖


使用端
第一服務裝置
第二服務裝置
第三服務裝置
S601 透過第一驗證閘道接收來該使用端所提供的服務請求
S603A 第一驗證閘道依據該服務請求傳送一授權憑證和一資料索引至該第三驗證閘道
S603B 傳送一授權憑證和一資料索引至該第三驗證閘道
S605 第三驗證閘道依據授權憑證和資料索引，呼叫第一伺服器提供相應該服務資訊的至少一服務資料至該第三服務端伺服器

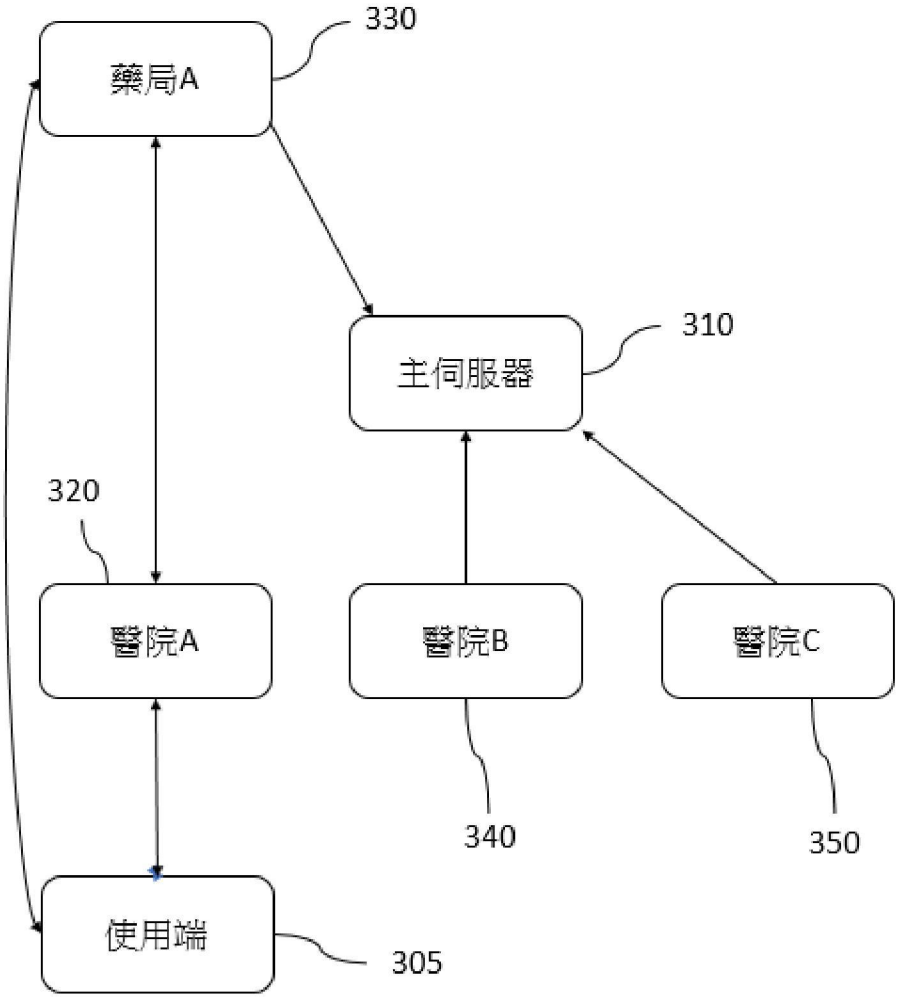
第 3 圖



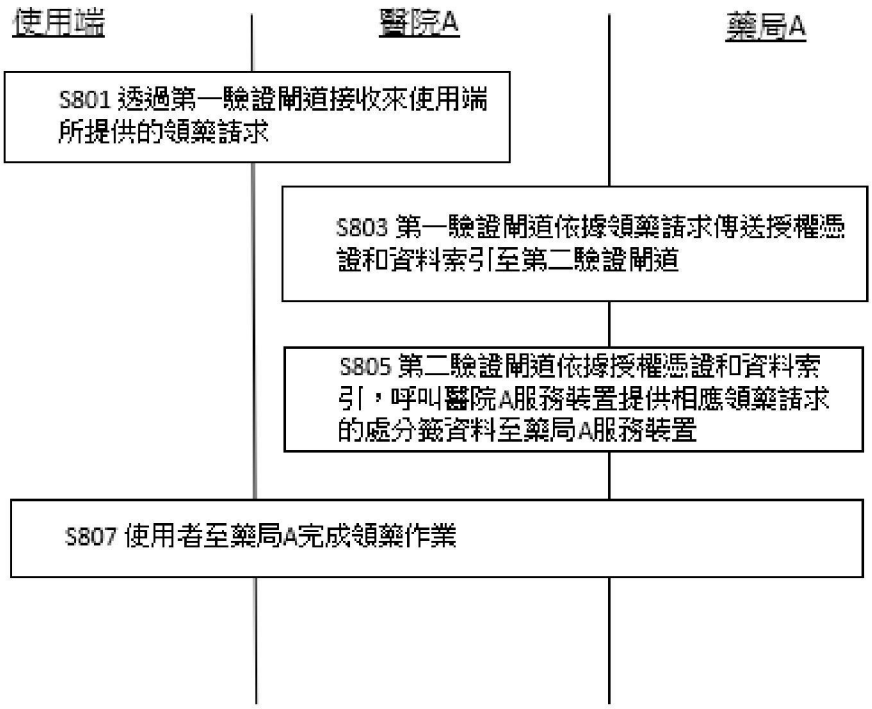
第 4 圖


使用端
醫院A
醫院B
S701 透過第一驗證閘道接收來該使用端所提供的病歷調閱請求
S703依據病歷調閱請求使醫院A服務裝置提供相應病歷調閱請求之第一就醫記錄
S705 第一驗證閘道依據病歷調閱請求透過第二驗證閘道使醫院B裝置提供相應病歷調閱請求之第二就醫記錄
S707 由醫院A服務裝置將第一就醫記錄和第二就醫記錄提供至使用端

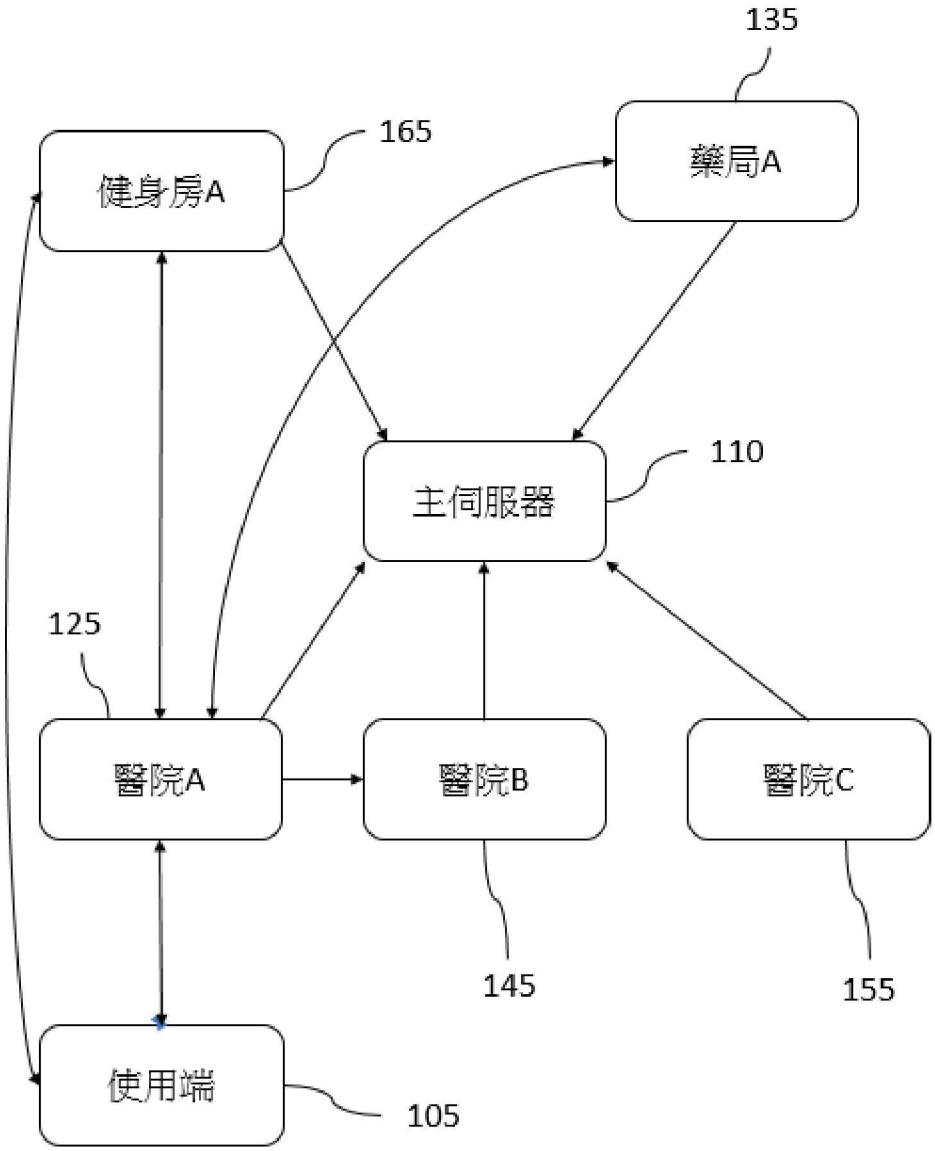
第 5 圖



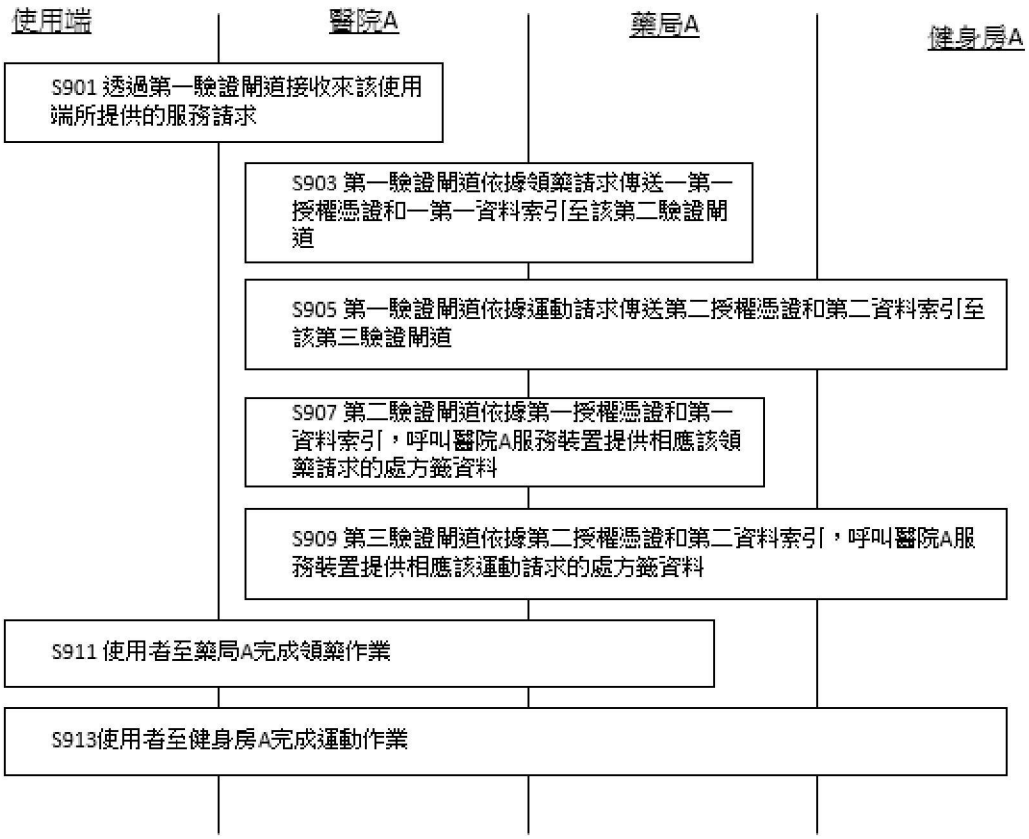
第 6 圖


使用端
醫院A
藥局A
S801 透過第一驗證閘道接收來使用端所提供的領藥請求
S803 第一驗證閘道依據領藥請求傳送授權憑證和資料索引至第二驗證閘道
S805 第二驗證閘道依據授權憑證和資料索引，呼叫醫院A服務裝置提供相應領藥請求的處分簽資料至藥局A服務裝置
S807 使用者至藥局A完成領藥作業

第 7 圖



第 8 圖


使用端
醫院A
藥局A
健身房A
S901 透過第一驗證閘道接收來該使用端所提供的服務請求
S903 第一驗證閘道依據領藥請求傳送一第一授權憑證和一第一資料索引至該第二驗證閘道
S905 第一驗證閘道依據運動請求傳送第二授權憑證和第二資料索引至該第三驗證閘道
S907 第二驗證閘道依據第一授權憑證和第一資料索引，呼叫醫院A服務裝置提供相應該領藥請求的處方箋資料
S909 第三驗證閘道依據第二授權憑證和第二資料索引，呼叫醫院A服務裝置提供相應該運動請求的處方箋資料
S911 使用者至藥局A完成領藥作業
S913使用者至健身房A完成運動作業

第 9 圖