



(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 I755580 B

(45)公告日：中華民國 111 (2022) 年 02 月 21 日

(21)申請案號：108100521

(22)申請日：中華民國 108 (2019) 年 01 月 07 日

(51)Int. Cl. : G07C9/00 (2020.01)

H04L29/06 (2006.01)

H04W12/06 (2021.01)

H04L9/32 (2006.01)

H04B5/00 (2006.01)

H04L29/08 (2006.01)

(30)優先權：2018/03/21 中國大陸

201810234267.5

(71)申請人：開曼群島商創新先進技術有限公司(開曼群島)ADVANCED NEW TECHNOLOGIES CO., LTD. (KY)

開曼群島

(72)發明人：廖暉(CN)；李京(CN)；周凡(CN)

(74)代理人：林志剛

(56)參考文獻：

CN 103971435B

CN 107154115A

審查人員：謝宏榮

申請專利範圍項數：8 項 圖式數：5 共 28 頁

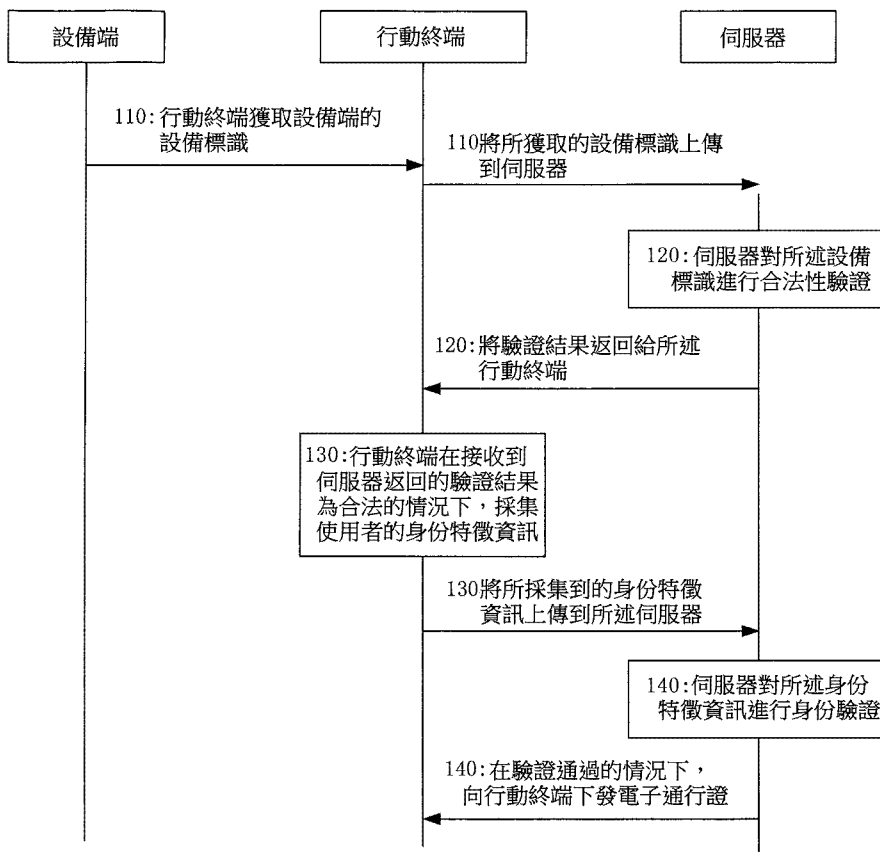
(54)名稱

身份驗證的方法及裝置和電子設備

(57)摘要

本說明書實施例提供一種身份驗證的方法及裝置和電子設備，所述方法包括：行動終端獲取設備端的設備標識，並將所獲取的設備標識上傳到伺服器；所述伺服器對所述設備標識進行合法性驗證，並將驗證結果返回給所述行動終端；所述行動終端在接收到所述伺服器返回的驗證結果為合法的情況下，採集使用者的身份特徵資訊，並將所採集到的身份特徵資訊上傳到所述伺服器；所述伺服器對所述身份特徵資訊進行身份驗證，並在驗證透過的情況下，向所述行動終端下發電子通行證；其中，所述電子通行證用於獲取所述設備端提供的服務。

指定代表圖：



【圖 2】

**【發明摘要】****【中文發明名稱】**

身份驗證的方法及裝置和電子設備

**【中文】**

本說明書實施例提供一種身份驗證的方法及裝置和電子設備，所述方法包括：行動終端獲取設備端的設備標識，並將所獲取的設備標識上傳到伺服器；所述伺服器對所述設備標識進行合法性驗證，並將驗證結果返回給所述行動終端；所述行動終端在接收到所述伺服器返回的驗證結果為合法的情況下，採集使用者的身份特徵資訊，並將所採集到的身份特徵資訊上傳到所述伺服器；所述伺服器對所述身份特徵資訊進行身份驗證，並在驗證透過的情況下，向所述行動終端下發電子通行證；其中，所述電子通行證用於獲取所述設備端提供的服務。

【指定代表圖】第(2)圖。  
【代表圖之符號簡單說明】無

【特徵化學式】無

## 【發明說明書】

### 【中文發明名稱】

身份驗證的方法及裝置和電子設備

### 【技術領域】

本說明書實施例涉及網際網路技術領域，尤其涉及一種身份驗證的方法及裝置和電子設備。

### 【先前技術】

隨著網際網路的不斷發展，透過行動終端實現電子通行證或者電子鑰匙的場景越來越多，例如行動支付、酒店登記、上班打卡、智慧門鎖等。

以智慧門鎖為例，使用者可以使用行動終端開鎖。具體地，智慧門鎖需要對使用者的身份進行驗證，在身份驗證通過後，行動終端才可以獲取電子通行證或者電子鑰匙。也就是說，行動終端獲取電子通行證或者電子鑰匙之前，需要設備端對使用者身份進行核實。可以看出，由於設備端需要進行身份核實，因此設備端需要具有一定的軟體和/或硬體上的要求。例如採用人臉識別進行身份驗證時，軟體方面設備端需要有一定的計算能力，硬體方面設備端需要有攝影鏡頭。

需要提供一種適用設備端性能要求不高的身份驗證的方案。

**【發明內容】**

本說明書實施例提供的一種身份驗證的方法及裝置和電子設備：

根據本說明書實施例的第一方面，提供一種身份驗證的方法，所述方法包括：

行動終端獲取設備端的設備標識，並將所獲取的設備標識上傳到伺服器；

所述伺服器對所述設備標識進行合法性驗證，並將驗證結果返回給所述行動終端；

所述行動終端在接收到所述伺服器返回的驗證結果為合法的情況下，採集使用者的身份特徵資訊，並將所採集到的身份特徵資訊上傳到所述伺服器；

所述伺服器對所述身份特徵資訊進行身份驗證，並在驗證通過的情況下，向所述行動終端下發電子通行證；其中，所述電子通行證用於獲取所述設備端提供的服務。

根據本說明書實施例的第二方面，提供一種身份驗證的方法，所述方法應用於行動終端，所述方法包括：

獲取設備端的設備標識；

將所述設備標識上傳到伺服器，以使所述伺服器對所述設備標識進行合法性驗證；

在接收到所述伺服器返回的驗證結果為合法的情況下，採集使用者的身份特徵資訊；

將所述身份特徵資訊上傳到所述伺服器，以使所述伺服器對所述身份特徵資訊進行身份驗證；

獲取所述伺服器在身份驗證通過時下發的電子通行證；其中，所述電子通行證用於獲取所述設備端提供的服務。

根據本說明書實施例的第三方面，提供一種身份驗證的裝置，所述裝置應用於行動終端，所述裝置包括：

第一獲取單元，獲取設備端的設備標識；

第一上傳單元，將所述設備標識上傳到伺服器，以使所述伺服器對所述設備標識進行合法性驗證；

採集單元，在接收到所述伺服器返回的驗證結果為合法的情況下，採集使用者的身份特徵資訊；

第二上傳單元，將所述身份特徵資訊上傳到所述伺服器，以使所述伺服器對所述身份特徵資訊進行身份驗證；

第二獲取單元，獲取所述伺服器在身份驗證通過時下發的電子通行證；其中，所述電子通行證用於獲取所述設備端提供的服務。

根據本說明書實施例的第四方面，提供一種電子設備，包括：

處理器；

用於儲存處理器可執行指令的記憶體；

其中，所述處理器被配置為實現上述任一項所述的身份驗證的方法。

本說明書實施例，將原本需要由設備端完成的身份驗證轉由伺服器完成，從而可以降低設備端對軟體、硬體方面的需求，從而也可以適用於性能不高的設備端。

**【圖式簡單說明】**

圖 1 是本說明書一實施例提供的實現身份驗證的系統架構概念圖；

圖 2 是本說明書一實施例提供的身份驗證的方法的流程圖；

圖 3 是本說明書一實施例提供的身份驗證的方法的流程圖；

圖 4 是本說明書一實施例提供的身份驗證的裝置的硬體結構圖；

圖 5 是本說明書一實施例提供的身份驗證的裝置的模組示意圖。

**【實施方式】**

這裡將詳細地對示例性實施例進行說明，其示例表示在附圖中。下面的描述涉及附圖時，除非另有表示，不同附圖中的相同數字表示相同或相似的要素。以下示例性實施例中所描述的實施方式並不代表與本說明書相一致的所有實施方式。相反，它們僅是與如所附申請專利範圍中所詳述的、本說明書的一些方面相一致的裝置和方法的例子。

在本說明書使用的術語是僅僅出於描述特定實施例的目的，而非旨在限制本說明書。在本說明書和所附申請專利範圍中所使用的單數形式的“一種”、“所述”和“該”也旨

在包括多數形式，除非上下文清楚地表示其他含義。還應當理解，本文中使用的術語“和/或”是指並包含一個或多個相關聯的列出專案的任何或所有可能組合。

應當理解，儘管在本說明書可能採用術語第一、第二、第三等來描述各種資訊，但這些資訊不應限於這些術語。這些術語僅用來將同一類型的資訊彼此區分開。例如，在不脫離本說明書範圍的情況下，第一資訊也可以被稱為第二資訊，類似地，第二資訊也可以被稱為第一資訊。取決於語境，如在此所使用的詞語“如果”可以被解釋成為“在……時”或“當……時”或“回應於確定”。

如前所述，一方面，由於設備端需要進行身份核實，因此設備端需要具有一定的軟體和/或硬體上的要求。例如採用人臉識別進行身份驗證時，軟體方面設備端需要有一定的計算能力，硬體方面設備端需要有攝影鏡頭。另一方面，某些設備端設計時，對能耗要求比較嚴格，例如採用電池供電的低功耗設備，這些設備由於普遍採用了低功耗模組，無法長期進行複雜的計算需求；同樣以智慧門鎖為例，智慧門鎖普遍採用電池供電，為了達到長時間使用，採用的是低功耗模組。

本說明書可以涉及一個或多個系統。以下請參考圖 1 示出了本說明書中可以適用的示例性的系統架構概念圖。所述系統架構概念圖可以包括設備端 11、行動終端 12 和伺服器 13。

所述設備端 11 可以是指進行需要電子通行證或者電子

鑰匙的設備。不同場景中，設備端對應了具體不同的設備；例如酒店入住場景，設備端可以為用於入住登記的自助終端。開鎖場景中，設備端可以是智慧門鎖。

所述行動終端11可以是指使用者使用的客戶端。該客戶端可以是指安裝有應用的終端；例如安裝有應用APP的手機。

所述伺服器13可以是指與所述設備端11和行動終端12通訊的應用伺服器、伺服器集群或者基於伺服器集群構建的雲端平臺。所述伺服器13可以用於進行身份驗證。

在實際應用中，當使用者需要獲取設備端11提供的服務時，可以透過行動終端12獲取設備端11的設備標識以及採集使用者的身份特徵資訊，並由伺服器13進行驗證，最終獲取伺服器13下發的電子通行證；然後行動終端12可以基於該電子通行證來獲取設備端11提供的服務。

以下可以結合圖2所示的例子介紹本說明書一種實現身份驗證的方法的實施例，如圖2所示，該方法可以包括以下步驟：

步驟110：行動終端獲取設備端的設備標識，並將所獲取的設備標識上傳到伺服器。

在一實施例中，所述設備標識包括靜態的設備標識和/或動態的設備標識。

以靜態的設備標識為例，所述設備標識具有唯一性，即每一個設備端都可以對應有一個唯一的設備標識。例如，設備出廠時的設備編號，ID等。

以動態的設備標識為例，所述設備標識可以包括動態符記，例如 token。所述動態符記可以是指一串加密的字串，可以是由預設的演算法生成的。一般的，動態符記是動態變化的，例如行動終端每次獲取的動態符記都是不同的；或者設備端週期性生成新的符記。

在一實施例中，所述行動終端獲取設備端的設備標識，具體包括：

行動終端透過與設備端建立短距離無線通訊，從而獲取所述設備端傳輸的設備標識。

具體地，所述短距離無線通訊包括藍牙通訊、紅外線通訊、無線局域網、WIFI、超寬頻通訊、紫峰通訊、近場通訊的一種。

在實施例中，所述設備端中可以集成有適用於短距離無線通訊的模組，如藍牙(Bluetooth)模組、紅外線(IrDA)模組、無線局域網(WI-FI或WLAN，大多採用802.11系列協定)模組、WIFI直連(Wi-Fi Direct)模組、超寬頻通訊(Ultra Wide Band)模組、紫峰(Zigbee)模組、近場通訊(Near Field Communication，NFC)模組等，以實現短距離無線信號的收發。同樣地，行動終端中也可以集成有同樣的適用於短距離無線通訊的模組。

在一實施例中，以藍牙技術為例進行說明。

藍牙技術作為取代資料電纜的短距離無線通訊技術，可以支援點對點以及點對多點的通訊，從而在設備間實現快捷而方便的資訊交互。

設備端可以透過藍牙模組發出包含自身的標識(UUID)的廣播信號。藍牙技術中，藍牙模組可以透過“全球唯一識別碼”(Universally Unique Identifier, UUID)來標識。每一個這樣的UUID都在時空上保證藍牙服務的唯一性。UUID具體可以是短整形(16或32位)和長整形(128位)。UUID可以透過藍牙廣播信號發送。

較佳地，所述藍牙技術，可以採用低功耗藍牙技術(Bluetooth Low Energy, BLE)。更優地，可以採用iBeacon技術。iBeacon技術是一種基於BLE開發的技術，具有成本低，擴展廣，定制靈活的特點。這種iBeacon技術可以使一個智慧手機或其他裝置在一個iBeacon基地的感應範圍內能夠執行相應的命令。例如本實施例中，收款設備可以為iBeacon基地。iBeacon已由蘋果公司於2013年9月發佈的行動設備用OS(iOS7)上配備。

BLE的通訊方式一般包括兩種：advertising(廣告)和connecting(連接)。廣告(Advertising)是一種單向的發送機制，屬於廣播模式的一種。想要被搜索到的設備(如iBeacon基地，收款設備)可以以20毫秒到10秒鐘的時間間隔發送一段資料包。使用的時間間隔越短，電池消耗的越快，設備被發現的速度也就會快。資料包長度最多47個位元組，一般可以由以下部分組成：

1 byte : preamble(1位元組做標頭)

4 byte : access address(4位元組做地址)

39 bytes : advertising channel PDU(39個位元組用於

PDU資料包)

3 bytes : CRC(3個位元組用於CRC資料校驗)

BLE設備可以運行在單一的不可連接的廣告模式中(在這種模式下所有的資訊都包含在廣告資料包中);此外, BLE設備也可以運行在可被連接的模式下(即connecting模式)。

本實施例中的設備端,可以運行在單一的不可連接的廣告模式中。這樣,設備端主要是將自身的設備標識透過廣告模式發送出去。具體的,所述設備端的設備標識,可以承載於上述PDU資料包中。

行動終端可以透過掃描廣播的藍牙信號發現設備端的UUID。具體的,安裝於行動終端上的應用可以透過調用底層應用程式設計介面(Application Programming Interface, API),驅動行動終端對無線信號的掃描。進而,可以掃描到設備端發出的無線信號,例如透過廣播方式發出的藍牙信號。由於設備端發出的藍牙信號包含其自身的設備標識資訊UUID,因此,行動終端可以透過掃描的藍牙廣播信號中發現該UUID。

在一實施例中,所述行動終端獲取設備端的設備標識,具體包括:

行動終端透過掃描設備端提供的圖形碼,從而獲取所述設備端的設備標識。

該實施例中,設備端可以展示出包含設備標識的圖形碼。行動終端中可以集成有用於掃描圖形碼的模組,例如

攝影鏡頭、掃碼器等，以實現掃描圖形碼從而獲取設備標識。

在一實施例中，以攝影鏡頭為例進行說明。

行動終端可以透過開啟攝影鏡頭，當攝影鏡頭採集到圖形碼的圖像後，透過行動終端本地解析軟體或者遠端伺服器解析出所述圖形碼包含的設備標識。

在一實施例中，所述圖形碼可以包括二維碼、條碼等。

步驟 120：所述伺服器對所述設備標識進行合法性驗證，並將驗證結果返回給所述行動終端。

在一實施例中，所述伺服器對所述設備標識進行合法性驗證，具體可以包括：

判斷所述設備標識對應的設備是否已在伺服器上註冊；

在所述設備標識對應的設備已在伺服器上註冊的情況下，確定驗證結果為合法。

一般的，設備端的生產商可以在設備端出廠時，可以在伺服器上完成註冊，從而在伺服器上可以儲存有設備標識與設備之間的對應關係，並且還有已註冊記錄。

在一實施例中，針對動態的設備標識，伺服器具有與設備端相同的用於生成動態符記的演算法。透過該演算法，伺服器可以驗證行動終端上傳的動態符記是否正確，並在正確的情況下，確定驗證結果為合法。

伺服器在確定了驗證結果後，就可以將驗證結果返回

給行動終端。

步驟 130：所述行動終端在接收到所述伺服器返回的驗證結果為合法的情況下，採集使用者的身份特徵資訊，並將所採集到的身份特徵資訊上傳到所述伺服器。

在一實施例中，所述身份特徵資訊可以包括生物特徵資訊。

所述生物特徵資訊包括指紋、掌紋、虹膜、眼紋、人臉、聲波、腦電波中的至少一種。對應的，所述行動終端中需要集成有採集生物特徵資訊的模組，例如透過攝影鏡頭可以採集使用者的人臉圖像；透過指紋模組可以採集使用者的指紋；透過聲波模組可以採集使用者聲波資訊等等。

在一實施例中，所述身份特徵資訊也可以包括使用者輸入的密碼資訊。

步驟 140：所述伺服器對所述身份特徵資訊進行身份驗證，並在驗證通過的情況下，向所述行動終端下發電子通行證；其中，所述電子通行證用於獲取所述設備端提供的服務。

本實施例中，所述伺服器中保存有使用者預留的身份特徵資訊。當伺服器收到行動終端上傳的身份特徵資訊後，可以與所述預留的身份特徵資訊進行比對，如果一致，則說明當前使用者為本人；反之，則說明當前使用者不是本人。

伺服器在驗證通過的情況下，進而可以向所述行動終

端下發電子通行證。所述電子通行證可以是設備端認可的，行動終端可以使用該電子通行證獲取設備端提供的服務。

以智慧門鎖場景為例，當行動終端獲取到電子通行證後，使用該電子通行證就可以打開智慧門鎖。

以酒店入住場景為例，當行動終端獲取到電子通行證後，使用該電子通行證就可以完成登記入住。

本說明書實施例，將原本需要由設備端完成的身份驗證轉由伺服器完成，從而可以降低設備端對軟體、硬體方面的需求，從而也可以適用於性能不高的設備端。另一方面，透過身份驗證，可以確定當前使用者是否為本人，防止冒用的情況出現，提升了可靠性。

在一實施例中，行動終端使用電子通行證，具體可以為：

行動終端將電子通行證發送給設備端。這裡，參考步驟 110 所示，可以是基於短距離無線通訊實現的。之後，設備端可以在本地對電子通行證進行校驗，待校驗通過後才可以提供服務。或者，設備端可以將電子通行證上傳到伺服器，由伺服器進行校驗，待伺服器返回的校驗結果為通過後才可以提供服務。

以下結合圖 3 介紹本申請以行動終端為主體的方法實施例，該實施例可以對應圖 2：

步驟 210：獲取設備端的設備標識；

步驟 220：將所述設備標識上傳到伺服器，以使所述

伺服器對所述設備標識進行合法性驗證；

步驟 230：在接收到所述伺服器返回的驗證結果為合法的情況下，採集使用者的身份特徵資訊；

步驟 240：將所述身份特徵資訊上傳到所述伺服器，以使所述伺服器對所述身份特徵資訊進行身份驗證；

步驟 250：獲取所述伺服器在身份驗證通過時下發的電子通行證；其中，所述電子通行證用於獲取所述設備端提供的服務。

在一實施例中，所述獲取設備端的設備標識，具體包括：

透過與設備端建立短距離無線通訊，從而獲取所述設備端傳輸的設備標識；

或者，

透過掃描設備端提供的圖形碼，從而獲取所述設備端的設備標識。

在一實施例中，所述短距離無線通訊包括藍牙通訊、紅外線通訊、無線局域網、WIFI、超寬頻通訊、紫峰通訊、近場通訊的一種。

在一實施例中，所述身份特徵資訊包括生物特徵資訊。

在一實施例中，所述生物特徵資訊包括指紋、掌紋、虹膜、眼紋、人臉、聲波、腦電波中的至少一種。

在一實施例中，所述設備標識包括靜態的設備標識和/或動態的設備標識。

在一實施例中，所述動態的設備標識包括動態符記。

與前述身份驗證的方法實施例相對應，本說明書還提供了身份驗證的裝置的實施例。所述裝置實施例可以透過軟體實現，也可以透過硬體或者軟硬體結合的方式實現。以軟體實現為例，作為一個邏輯意義上的裝置，是透過其所在設備的處理器將非易失性記憶體中對應的電腦程式指令讀取到記憶體中運行形成的。從硬體層面而言，本說明書身份驗證的裝置所在設備的一種硬體結構如圖4所示可以包括處理器、網路介面、記憶體以及非易失性記憶體之外，實施例中裝置所在的設備通常根據該身份驗證的實際功能，還可以包括其他硬體，對此不再贅述。

請參見圖5，為本說明書一實施例提供的身份驗證的裝置的模組圖，所述裝置包括：

第一獲取單元310，獲取設備端的設備標識；

第一上傳單元320，將所述設備標識上傳到伺服器，以使所述伺服器對所述設備標識進行合法性驗證；

採集單元330，在接收到所述伺服器返回的驗證結果為合法的情況下，採集使用者的身份特徵資訊；

第二上傳單元340，將所述身份特徵資訊上傳到所述伺服器，以使所述伺服器對所述身份特徵資訊進行身份驗證；

第二獲取單元350，獲取所述伺服器在身份驗證通過時下發的電子通行證；其中，所述電子通行證用於獲取所述設備端提供的服務。

在一個可選的實施例中：

所述第一獲取單元310，具體包括：

第一獲取子單元，透過與設備端建立短距離無線通訊，從而獲取所述設備端傳輸的設備標識；

或者，

第二獲取子單元，透過掃描設備端提供的圖形碼，從而獲取所述設備端的設備標識。

在一個可選的實施例中：

所述短距離無線通訊包括藍牙通訊、紅外線通訊、無線局域網、WIFI、超寬頻通訊、紫峰通訊、近場通訊的一種。

在一個可選的實施例中：

所述身份特徵資訊包括生物特徵資訊。

在一個可選的實施例中：

所述生物特徵資訊包括指紋、掌紋、虹膜、眼紋、人臉、聲波、腦電波中的至少一種。

在一個可選的實施例中：

所述設備標識包括靜態的設備標識和/或動態的設備標識。

在一個可選的實施例中：

所述動態的設備標識包括動態符記。

上述實施例闡明的系統、裝置、模組或單元，具體可以由電腦晶片或實體實現，或者由具有某種功能的產品來實現。一種典型的實現設備為電腦，電腦的具體形式可以

是個人電腦、膝上型電腦、蜂巢式電話、相機電話、智慧型電話、個人數位助理、媒體播放機、導航設備、電子郵件收發設備、遊戲控制台、平板電腦、可穿戴設備或者這些設備中的任意幾種設備的組合。

上述裝置中各個單元的功能和作用的實現過程具體詳見上述方法中對應步驟的實現過程，在此不再贅述。

對於裝置實施例而言，由於其基本對應於方法實施例，所以相關之處參見方法實施例的部分說明即可。以上所描述的裝置實施例僅僅是示意性的，其中所述作為分離部件說明的單元可以是或者也可以不是物理上分開的，作為單元顯示的部件可以是或者也可以不是物理單元，即可以位於一個地方，或者也可以分佈到多個網路單元上。可以根據實際的需要選擇其中的部分或者全部模組來實現本說明書方案的目的。本領域普通技術人員在不付出進步性勞動的情況下，即可以理解並實施。

以上圖 5 描述了身份驗證的裝置的內部功能模組和結構示意，其實質上的執行主體可以為一種電子設備，包括：

處理器；

用於儲存處理器可執行指令的記憶體；

獲取設備端的設備標識；

將所述設備標識上傳到伺服器，以使所述伺服器對所述設備標識進行合法性驗證；

在接收到所述伺服器返回的驗證結果為合法的情況

下，採集使用者的身份特徵資訊；

將所述身份特徵資訊上傳到所述伺服器，以使所述伺服器對所述身份特徵資訊進行身份驗證；

獲取所述伺服器在身份驗證通過時下發的電子通行證；其中，所述電子通行證用於獲取所述設備端提供的服務。

可選的，所述獲取設備端的設備標識，具體包括：

透過與設備端建立短距離無線通訊，從而獲取所述設備端傳輸的設備標識；

或者，

透過掃描設備端提供的圖形碼，從而獲取所述設備端的設備標識。

可選的，所述短距離無線通訊包括藍牙通訊、紅外線通訊、無線局域網、WIFI、超寬頻通訊、紫峰通訊、近場通訊的一種。

可選的，所述身份特徵資訊包括生物特徵資訊。

可選的，所述生物特徵資訊包括指紋、掌紋、虹膜、眼紋、人臉、聲波、腦電波中的至少一種。

可選的，所述設備標識包括靜態的設備標識和/或動態的設備標識。

可選的，所述動態的設備標識包括動態符記。

在上述電子設備的實施例中，應理解，該處理器可以是中央處理單元(英文：Central Processing Unit，簡稱：CPU)，還可以是其他通用處理器、數位訊號處理器(英

文：Digital Signal Processor，簡稱：DSP)、專用積體電路(英文：Application Specific Integrated Circuit，簡稱：ASIC)等。通用處理器可以是微處理器或者該處理器也可以是任何常規的處理器等，而前述的記憶體可以是唯讀記憶體(英文：read-only memory，縮寫：ROM)、隨機存取記憶體(英文：random access memory，簡稱：RAM)、快閃記憶體、硬碟或者固態硬碟。結合本發明實施例所公開的方法的步驟可以直接體現為硬體處理器執行完成，或者用處理器中的硬體及軟體模組組合執行完成。

本說明書中的各個實施例均採用遞進的方式描述，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，對於電子設備實施例而言，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。

本領域技術人員在考慮說明書及實踐這裡公開的發明後，將容易想到本說明書的其它實施方案。本說明書旨在涵蓋本說明書的任何變型、用途或者適應性變化，這些變型、用途或者適應性變化遵循本說明書的一般性原理並包括本說明書未公開的本技術領域中的公知常識或慣用技術手段。說明書和實施例僅被視為示例性的，本說明書的真正範圍和精神由下面的申請專利範圍指出。

應當理解的是，本說明書並不局限於上面已經描述並在附圖中示出的精確結構，並且可以在不脫離其範圍進行

各種修改和改變。本說明書的範圍僅由所附的申請專利範圍來限制。

**【符號說明】**

11：設備端

12：行動終端

13：伺服器

310：第一獲取單元

320：第一上傳單元

330：採集單元

340：第二上傳單元

350：第二獲取單元

## 【發明申請專利範圍】

### 【第1項】

一種身份驗證的方法，所述方法包括：

行動終端獲取智慧門鎖的動態符記，並將所獲取的動態符記上傳到伺服器；

所述伺服器利用與所述智慧門鎖相同的用於生成動態符記的演算法，驗證所述行動終端上傳的動態符記是否正確，並將驗證結果返回給所述行動終端；

所述行動終端在接收到所述伺服器返回的驗證結果為正確的情況下，採集使用者的身份特徵資訊，並將所採集到的身份特徵資訊上傳到所述伺服器；

所述伺服器對所述身份特徵資訊進行身份驗證，並在驗證通過的情況下，向所述行動終端下發電子通行證；其中，所述電子通行證用於打開所述智慧門鎖。

### 【第2項】

一種身份驗證的方法，所述方法應用於行動終端，所述方法包括：

獲取智慧門鎖的動態符記；

將所述動態符記上傳到伺服器，以使所述伺服器利用與所述智慧門鎖相同的用於生成動態符記的演算法，驗證所述行動終端上傳的動態符記是否正確；

在接收到所述伺服器返回的驗證結果為正確的情況下，採集使用者的身份特徵資訊；

將所述身份特徵資訊上傳到所述伺服器，以使所述伺

服器對所述身份特徵資訊進行身份驗證；

獲取所述伺服器在身份驗證通過時下發的電子通行證；其中，所述電子通行證用於打開所述智慧門鎖。

**【第3項】**

根據申請專利範圍第2項所述的方法，所述獲取智慧門鎖的動態符記，具體包括：

透過與智慧門鎖建立短距離無線通訊，從而獲取所述智慧門鎖傳輸的動態符記；

或者，

透過掃描智慧門鎖提供的圖形碼，從而獲取所述智慧門鎖的動態符記。

**【第4項】**

根據申請專利範圍第3項所述的方法，所述短距離無線通訊包括藍牙通訊、紅外線通訊、無線局域網、WIFI、超寬頻通訊、紫峰通訊、近場通訊的一種。

**【第5項】**

根據申請專利範圍第2項所述的方法，所述身份特徵資訊包括生物特徵資訊。

**【第6項】**

根據申請專利範圍第5項所述方法，所述生物特徵資訊包括指紋、掌紋、虹膜、眼紋、人臉、聲波、腦電波中的至少一種。

**【第7項】**

一種身份驗證的裝置，所述裝置包括：

第一獲取單元，獲取智慧門鎖的動態符記；

第一上傳單元，將所述動態符記上傳到伺服器，以使所述伺服器利用與所述智慧門鎖相同的用於生成動態符記的演算法，驗證所述行動終端上傳的動態符記是否正確；

採集單元，在接收到所述伺服器返回的驗證結果為正確的情況下，採集使用者的身份特徵資訊；

第二上傳單元，將所述身份特徵資訊上傳到所述伺服器，以使所述伺服器對所述身份特徵資訊進行身份驗證；

第二獲取單元，獲取所述伺服器在身份驗證通過時下發的電子通行證；其中，所述電子通行證用於打開所述智慧門鎖。

**【第8項】**

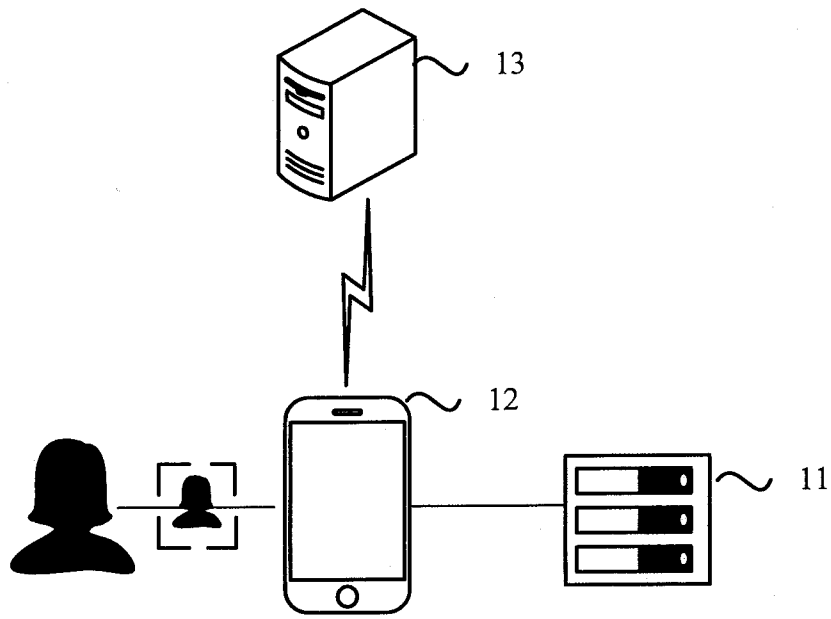
一種電子設備，包括：

處理器；

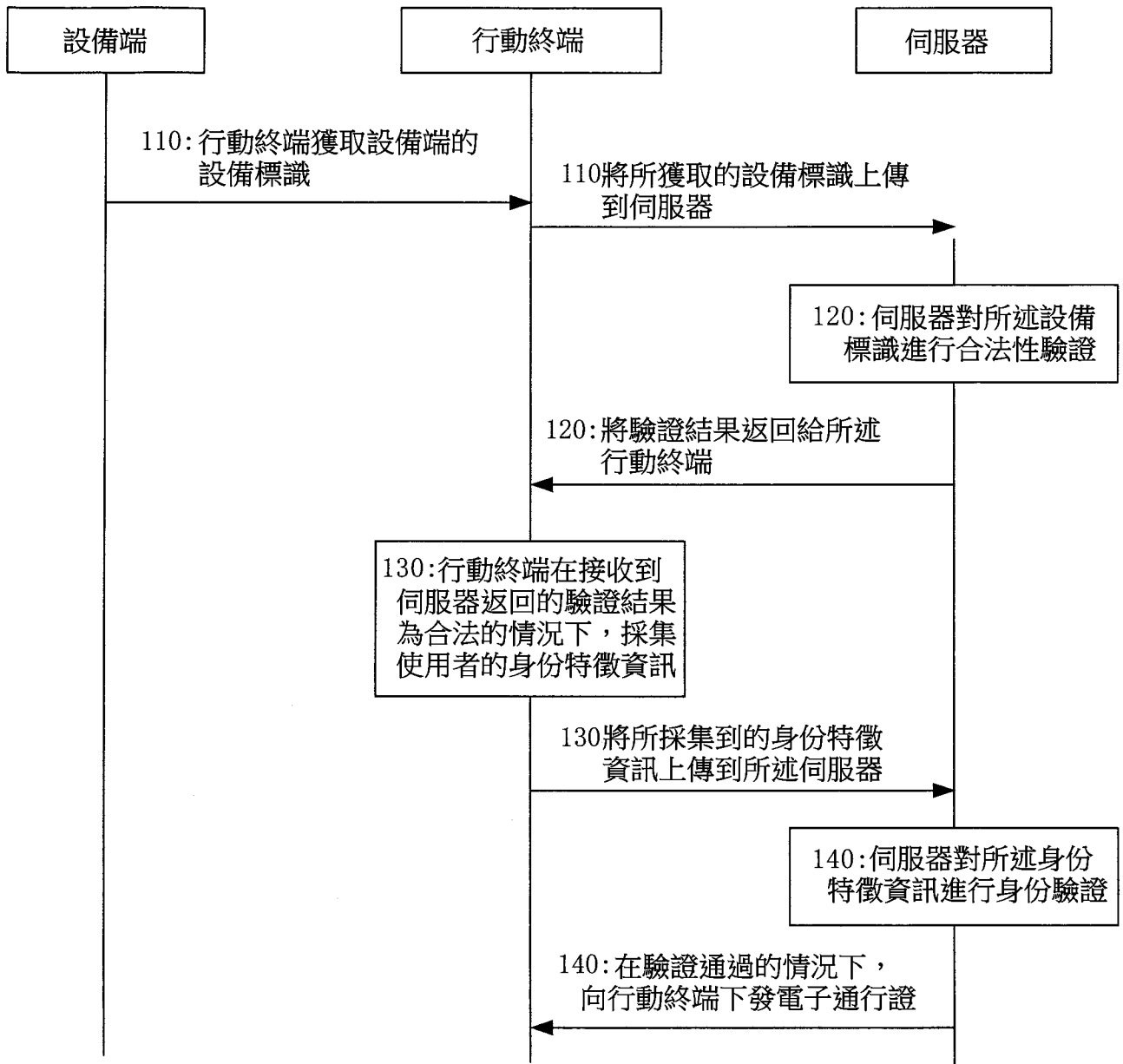
用於儲存處理器可執行指令的記憶體；

其中，所述處理器被配置為實現上述申請專利範圍第1-6項中之任一項所述的方法。

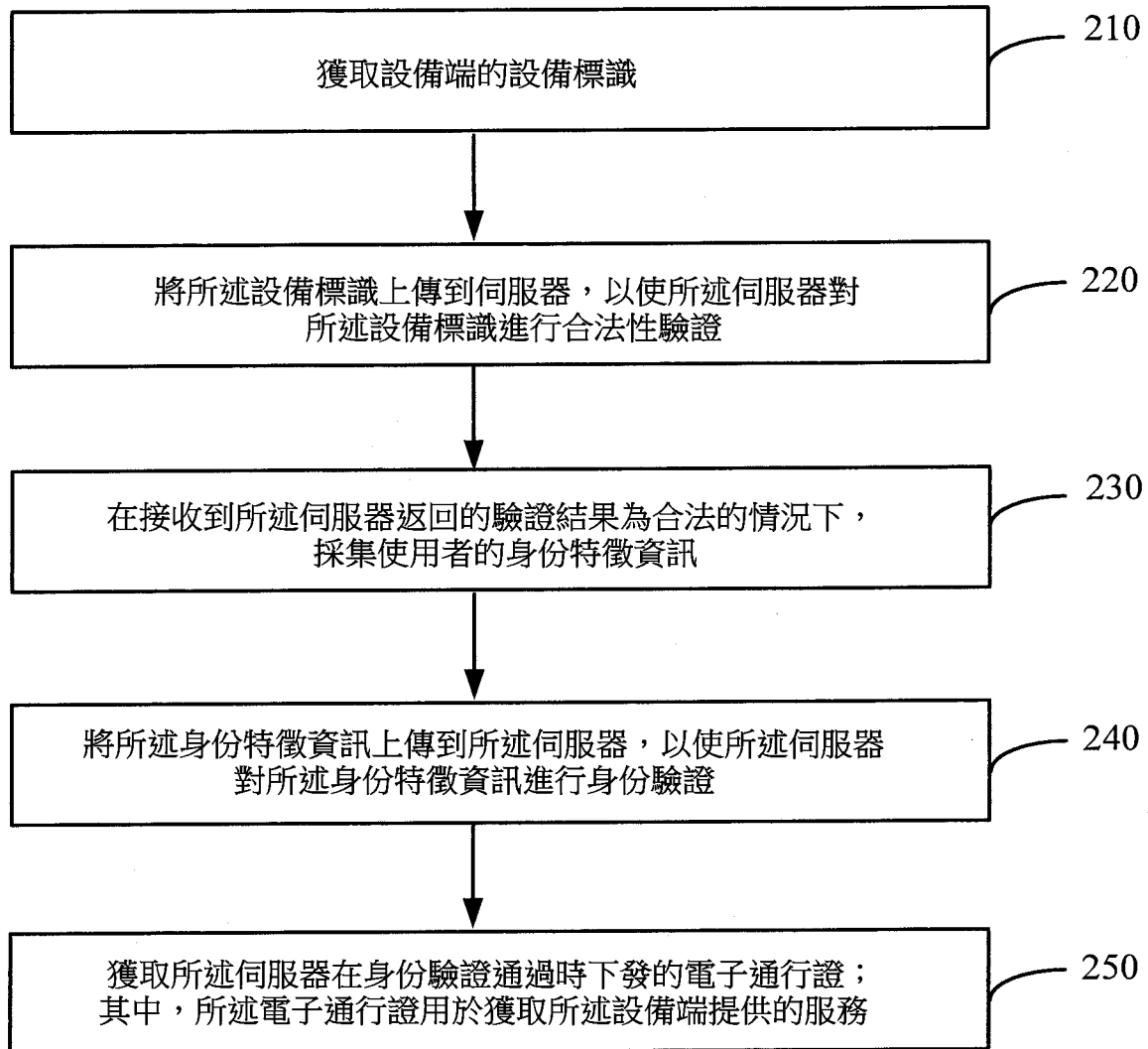
【發明圖式】



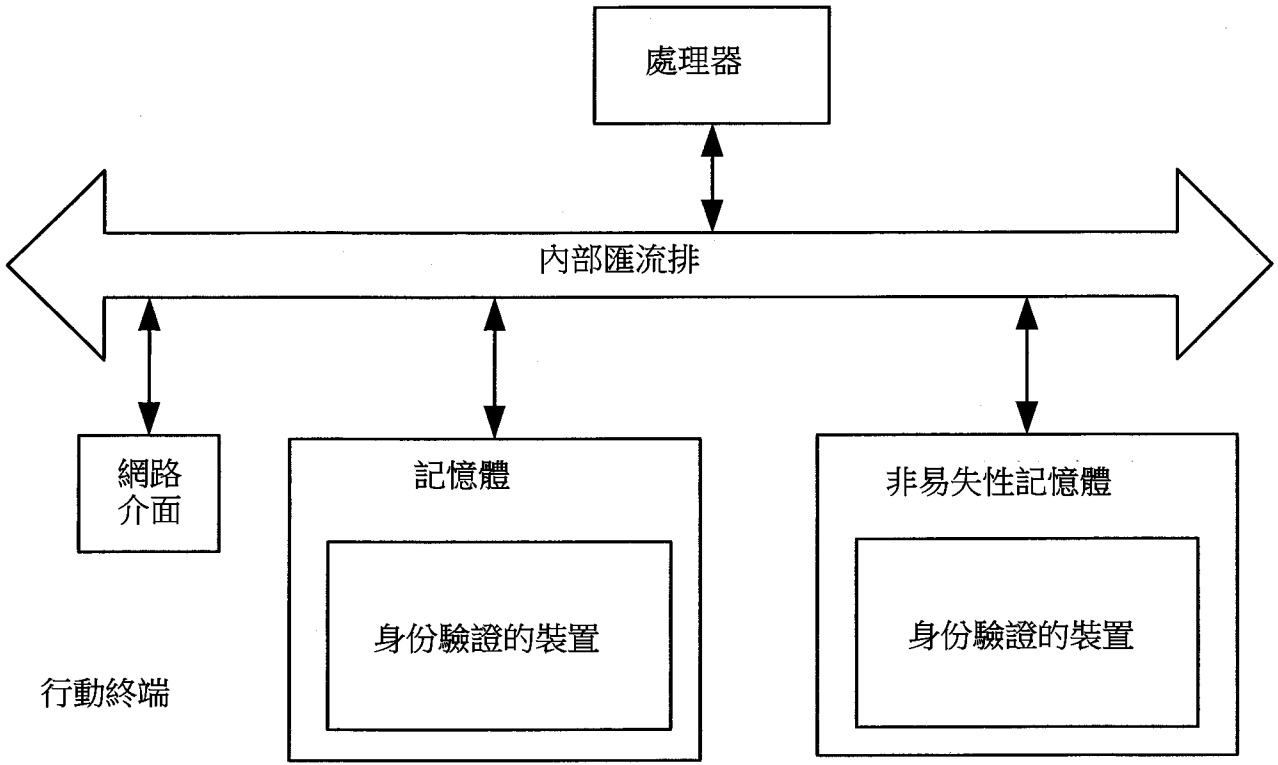
【圖 1】



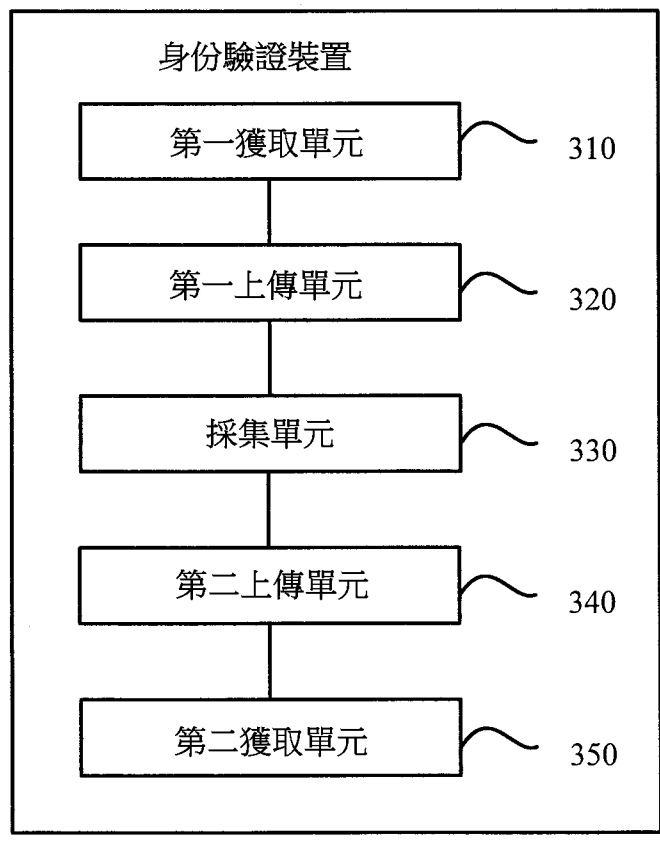
【圖 2】



【圖 3】



【圖 4】



【圖 5】